Integer linear programming techniques for constant dimension codes and related structures

Von der Universität Bayreuth
zur Erlangung des Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

von

Daniel Heinlein

aus Kronach

1. Gutachter: Prof. Dr. Michael Stoll
2. Gutachter: apl. Prof. Dr. Sascha Kurz
3. Gutachter: apl. Prof. Dr. Alfred Wassermann
4. Gutachter: Prof. Dr. Leo Storme

Tag der Einreichung: 12.04.2018
Tag des Kolloquiums: 13.11.2018

Techniken der ganzzahligen linearen Optimierung für constant dimension codes und verwandte Strukturen

Der Verband der Untervektorräume eines endlichdimensionalen Vektorraumes über einem endlichen Körper ist versehen mit der so genannten subspace distance oder der injection distance ein metrischer Raum. Eine Teilmenge dieses metrischen Raumes heißt subspace code. Falls ein subspace code ausschließlich Elemente, so genannte Codeworte, derselben Dimension beinhaltet, nennt man ihn constant dimension code, abgekürzt CDC. Die Minimaldistanz ist der kleinste paarweise Abstand von Elementen eines subspace codes. Im Falle von CDCs ist die Minimaldistanz äquivalent zu einer oberen Schranke an die Dimension des Durchschnitts von je zwei Codewörtern.

Subspace codes spielen eine entscheidende Rolle im Kontext von random linear network coding, bei dem Daten zwischen einem Sender und mehreren Empfängern übertragen werden, so dass Teilnehmer der Kommunikation zufällige Linearkombinationen der Daten weitersenden.

Zwei wichtige Probleme des subspace coding sind die Bestimmung der Kardinalität größter subspace codes und der Klassifikation von subspace codes.

Diese Arbeit gibt unter Zuhilfenahme von Techniken der ganzzahligen linearen Optimierung und Symmetrie teilweise Antworten auf obige Fragen mit dem Fokus auf CDCs.

Mit der coset construction und der improved linkage construction geben wir zwei allgemeine Konstruktionen an, die die beste bekannte untere Schranke an die Kardinalität in vielen Fällen verbessern.

Ein als Baustein für aufwändige CDCs oft genutzter und sehr strukturierter CDC ist der lifted maximum rank distance code, abgekürzt LMRD. Wir verallgemeinern obere Schranken für CDCs die einen LMRD beinhalten, so genannte LMRD bounds. Dies liefert eine neue Methode um einen LMRD mit weiteren Codewörtern zu erweitern. In sporadischen Fällen liefert diese Technik neue beste untere Schranken an die Kardinalität von größten CDCs. Die improved linkage construction wird genutzt, um eine unendliche Serie von CDCs deren Kardinalität die LMRD bound übertrifft, zu konstruieren.

Eine weitere Konstruktion, die einen LMRD beinhaltet, gepaart mit einer asymptotischen Analyse in dieser Arbeit, beschränkt das Verhältnis zwischen bester bekannter unterer Schranke und bester bekannter oberer Schranke auf mindestens 61,6% für alle Parameter.

Des Weiteren vergleichen wir bekannte obere Schranken und zeigen neue Beziehungen zwischen ihnen auf.

Diese Arbeit beschreibt zudem eine computergestützte Klassifikation von größten binären CDCs in Dimension acht, Codewortdimension vier und Minimaldistanz sechs. Dies ist, für nichttriviale Parameter, die zusätzlich nicht den Spezialfall von partial spreads parametrisieren, der dritte Parametersatz, bei dem die maximale Kardinalität festgestellt wurde und der zweite Parametersatz, bei dem eine Klassifikation aller größten Codes vorliegt.

Einige Symmetriegruppen können beweisbar nicht Automorphismengruppen von großen CDCs sein. Wir geben zusätzlich einen Algorithmus an, der alle Untergruppen einer endlichen Gruppe nach einer vorgegebenen, mit Einschränkungen wählbaren, Eigenschaft

durchsucht. Im Kontext von CDCs liefert dieser Algorithmus zum einen eine Liste von Untergruppen, die als Kandidaten von Automorphismengruppen von großen Codes infrage kommen und zum anderen können hierdurch gefundene Codes mit viel Symmetrie weiterverarbeitet und vergrößert werden. Dies liefert einen neuen größten Code in dem kleinsten offenen Fall, nämlich in der Situation des binären Analogons der Fano Ebene.

Integer linear programming techniques for constant dimension codes and related structures

The lattice of subspaces of a finite dimensional vector space over a finite field is combined with the so-called subspace distance or the injection distance a metric space. A subset of this metric space is called subspace code. If a subspace code contains solely elements, so-called codewords, with equal dimension, it is called constant dimension code, which is abbreviated as CDC. The minimum distance is the smallest pairwise distance of elements of a subspace code. In the case of a CDC, the minimum distance is equivalent to an upper bound on the dimension of the pairwise intersection of any two codewords.

Subspace codes play a vital role in the context of random linear network coding, in which data is transmitted from a sender to multiple receivers such that participants of the communication forward random linear combinations of the data.

The two main problems of subspace coding are the determination of the cardinality of largest subspace codes and the classification of subspace codes.

Using integer linear programming techniques and symmetry, this thesis answers partially the questions above while focusing on CDCs.

With the coset construction and the improved linkage construction, we state two general constructions, which improve on the best known lower bound of the cardinality in many cases.

A well-structured CDC which is often used as building block for elaborate CDCs is the lifted maximum rank distance code, abbreviated as LMRD. We generalize known upper bounds for CDCs which contain an LMRD, the so-called LMRD bounds. This also provides a new method to extend an LMRD with additional codewords. This technique yields in sporadic cases best lower bounds on the cardinalities of largest CDCs. The improved linkage construction is used to construct an infinite series of CDCs whose cardinalities exceed the LMRD bound.

Another construction which contains an LMRD together with an asymptotic analysis in this thesis restricts the ratio between best known lower bound and best known upper bound to at least 61.6% for all parameters.

Furthermore, we compare known upper bounds and show new relations between them.

This thesis describes also a computer-aided classification of largest binary CDCs in dimension eight, codeword dimension four, and minimum distance six. This is, for non-trivial parameters which in addition do not parametrize the special case of partial spreads, the third set of parameters of which the maximum cardinality is determined and the second set of parameters with a classification of all maximum codes.

Provable, some symmetry groups cannot be automorphism groups of large CDCs. Additionally, we provide an algorithm which examines the set of all subgroups of a finite group for a given, with restrictions selectable, property. In the context of CDCs, this algorithm provides on the one hand a list of subgroups, which are eligible for automorphism groups of large codes and on the other hand codes having many symmetries which are found by this method can be enlarged in a postprocessing step. This yields a new largest code in the smallest open case, namely the situation of the binary analogue of the Fano plane.

Acknowledgments

My deep gratitude goes to my supervisors Sascha Kurz and Alfred Wassermann for introducing me into this research area and giving me this opportunity and together with Michael Kiermaier and Thomas Honold for many interesting discussions and helpful comments.

I would also like to thank Michael Stoll and Leo Storme for reviewing this thesis and Jörg Rambau for being a member of the examination board.

Next, I want to thank the German Research Foundation for their financial support in our project "Integer Linear Programming Models for Subspace Codes and Finite Geometry" ("Ganzzahlige Optimierungsmodelle für Subspace Codes und endliche Geometrie", KU 2430/3-1, WA 1666/9-1) and the EU COST Action project IC1104 "Random Network Coding and Designs over GF(q)" for many beautiful conferences.

Furthermore, I would like to thank Andreas Herán, Stefan Müller, and Thomas Heinlein for proof-reading of and remarks on this thesis.

I thank my family for their steady support without whom this work definitely would not have been possible.

Contents

1 Introduction

In network coding, the goal is to transmit information from a source (sender) to at least one sink (receiver) through a network, such that the participating nodes may use coding on the data that they received. This setting is called multicast.

More formally, a network is a finite, connected, and directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ with vertices in $\mathcal{V}$ and arcs in $\mathcal{A}$ such that each arc has a capacity of $c : \mathcal{A} \to \mathbb{Z}_{\geq 0}$. $\mathcal{V}$ contains the special vertices S, the sender, and the receivers R_i for $i = 1, \dots, r$. Vertices are called *nodes* and arcs are called *links* in the following. A link $b \in \mathcal{A}$ is called ingoing, respective outgoing, of a node n if $b = (m, n)$, respective $b = (n, m)$, for $m \in \mathcal{V}$.

In the classical case, in which no coding but simple replication and forwarding (store-and-forward) of information at the intermediate nodes, i.e., $\mathcal{V} \setminus (\{S\} \cup \{R_i \mid i = 1, \dots, r\})$, is allowed, there are examples showing that given capacities are not achieved. The default example is the so-called butterfly network, see Figure 1. In this case, S wants to send the information x_1 and x_2 to both receivers R_1 and R_2. Using store-and-forward, V_1 can only send x_1 on both outgoing links and therefore V_3 and R_1 both know x_1, and the same is true for x_2, V_2, V_3, and R_2. Now V_3 has two possibilities: send either x_1 or x_2 to V_4. In both cases, the information which was not sent can only be sent after transmitting the first information, introducing a delay in time. If we allow coding at the nodes of this network, then V_3 gains the ability to combine x_1 and x_2, e.g., using binary vectors x_1 and x_2 and $+$ in $\mathbb{F}_2^v$, which is equal to xor, for the newly crafted information $\alpha = \beta_1 = \beta_2 = x_1 + x_2$. α is then sent instead of x_1 or x_2. Then, R_1 computes $\alpha + x_1 = x_2$ and R_2 computes $\alpha + x_2 = x_1$, so both receivers know both informations. This effectively reduces the overall time to sent two informations to two receivers through this specific network.

Although using two sources, another standard example is depicted in Figure 2. This network should be interpreted as wireless connections of two clients SR_1 and SR_2 to a base station V_1, such that neither of the clients can send or receive information from each other, but both can communicate over V_1. For example, SR_1 wants to send x_1 to SR_2 and SR_2 wants to send x_2 to SR_1 fast while V_1 can only get data from one sender in one time slot. Being wireless, V_1 sends the same information to both SR_1 and SR_2, and cannot send two distinct information to the clients. The catch is again that by using $x_1, x_2 \in \mathbb{F}_2^v$ and the linear combination $x_1 + x_2$, we can reduce the total time for the exchange of the data by $1/4$. The actions of the three participating nodes are listed in Table 1. Conceptually, this can be modeled via hypergraphs, in which each arc has one source and a set of vertices as receiver. Neither hypergraphs nor multiple senders, so-called multisource problems, are handled in this thesis.

The capacity of a network, i.e., the maximum flow in respective the minimum cut of a network, can be achieved by linear network coding, cf. [LYC03]. In this context, information is interpreted as vectors in the row vector space $V = \mathbb{F}_q^v$ and coding at all

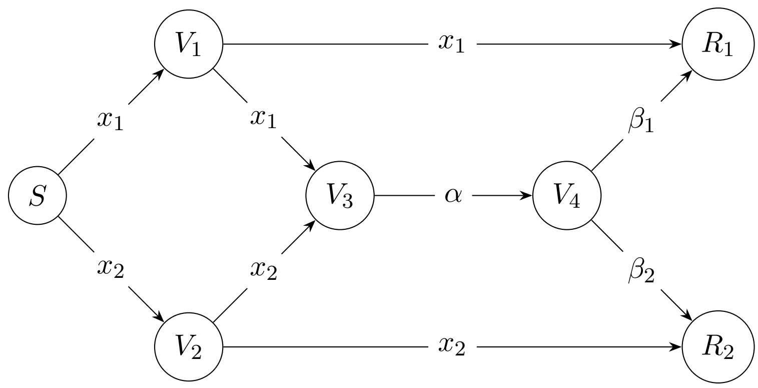


Figure 1: Butterfly network to demonstrate that store-and-forward introduces a time delay when sending information to both receivers. All capacities are one and the depicted x_1 and x_2 is the information to send. The α, β_1, and β_2 are x_1 or x_2 if store-and-forward is applied and for example $x_1 + x_2$ for binary vectors if linear network coding is applied.

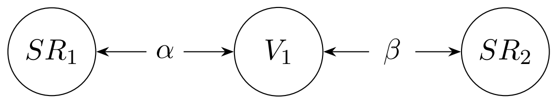


Figure 2: Wireless network with two senders to demonstrate the advantage of network coding. See Table 1 for the usage of this network.

time	store-and-forward		linear network coding	
slot	α	β	α	β
1	$SR_1 \to x_1 \to V_1$	–	$SR_1 \to x_1 \to V_1$	–
2	–	$V_1 \leftarrow x_2 \leftarrow SR_2$	–	$V_1 \leftarrow x_2 \leftarrow SR_2$
3	$SR_1 \leftarrow x_1 \leftarrow V_1$	$V_1 \to x_1 \to SR_2$	$SR_1 \leftarrow x_1 + x_2 \leftarrow V_1$	$V_1 \to x_1 + x_2 \to SR_2$
4	$SR_1 \leftarrow x_2 \leftarrow V_1$	$V_1 \to x_2 \to SR_2$	–	–

Table 1: Actions of the participants in Figure 2 using store-and-forward and linear network coding.

nodes, not only intermediate ones, is to build a linear combination of the received vectors, which can be different for each outgoing link throughout the whole network.

If there is a malicious node in the network, it may insert rogue vectors which are then processed by the nodes in the described way. In fact, we have up to $\#\mathcal{A}$ erroneous vectors, one for each link in the network.

Assume that the sender wants to send only $x_1, \ldots, x_k \in V$, a so-called *generation*. Multiple generations can be implemented by labeling each sent vector with the generation number, which then is only linearly combined with vectors having the same label. Assume further, that there is only one receiver, i.e., $r = 1$. The method below can also be applied in a scenario with multiple receivers.

Then, independent of any structural information about the network, the receiver observes K vectors, $y_1, \ldots, y_K \in V$, which are linear combinations of the valid vectors $x_1, \ldots, x_k$ and the erroneous vectors $e_1, \ldots, e_{\#\mathcal{A}} \in V$. Since V consists of row vectors, the receiver gets

$$\begin{pmatrix} y_1 \\ \vdots \\ y_K \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{K,1} & \cdots & a_{K,k} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} + \begin{pmatrix} b_{1,1} & \cdots & b_{1,\#\mathcal{A}} \\ \vdots & \ddots & \vdots \\ b_{K,1} & \cdots & b_{K,\#\mathcal{A}} \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ \vdots \\ e_{\#\mathcal{A}} \end{pmatrix}.$$

We will abbreviate this so-called *channel* as $Y = A \cdot X + B \cdot E$ with $Y \in \mathbb{F}_q^{K \times v}$, $A \in \mathbb{F}_q^{K \times k}$, $X \in \mathbb{F}_q^{k \times v}$, $B \in \mathbb{F}_q^{K \times (\#\mathcal{A})}$, and $E \in \mathbb{F}_q^{(\#\mathcal{A}) \times v}$.

By choosing the linear combination in each node randomly, we end up by the so-called random linear network coding [Ho+03] in which no information about A and B is available at all. Nevertheless, it is known that the decoding probability converges to 1 by increasing the field size $q \to \infty$. This increases the motivation to not use A and B in the reasoning of the decoding.

Another advantage is, that the network may have cycles or delays [SKK08] and even nodes may join or leave the network at will. In all of these scenarios, the receiver gets $Y = AX + BE$.

As Kötter and Kschischang observed in [KK08b, Section 2], see also [SKK08, Section 3.A], if E is the all-zero matrix $\mathbf{0} \in \mathbb{F}_q^{(\#\mathcal{A}) \times v}$, then the row-space of X contains the row-space of Y as a subspace. This observation leads to the idea to study subspaces instead of single vectors and that it does not matter which basis is received. Hence, by sending an arbitrary k-dimensional basis of U as $x_1, \ldots, x_k$, the receiver gets K vectors that span a subspace W. If $E = \mathbf{0}$, then $K \leq k$. Let E' be the row-space of $B \cdot E$ and $\mathcal{H}_{l'}(U)$ be an l'-dimensional subspace of U, then we have $W = \mathcal{H}_{l'}(U) + E'$. Next, E' can be split into $E' = E'' \oplus Z$ with $E'' \leq U$, $\dim(Z \cap U) = 0$, and $l' \leq l$. The interpretation is that errors which lie in the span of U are no errors at all. Hence, the final channel, called random linear network coding channel (RLNCC), is

$$W = \mathcal{H}_l(U) \oplus Z,$$

such that $\dim(Z \cap U) = 0$ and in which $t = \dim(Z)$ errors and $p = \max\{0, \max\{\dim(U) \mid U \in C\} - l\}$ erasures occur for a given set of subspaces C.

A set of subspaces of V is called *subspace code*.

By introducing a metric $\mathrm{d_x}$ on the set of subspaces of V, it can be proved that the *minimum distance decoder*, i.e., $\operatorname{argmin}\{\mathrm{d_x}(W,B) \mid B \in C\}$, can reconstruct U using only W and C if the number of errors and erasures which occurred in the transmission is small.

Although there are two well-known metrics on the set of subspaces of V, the subspace distance $\mathrm{d_s}(U,W) = \dim(U+W) - \dim(U \cap W)$ and the injection distance $\mathrm{d_i}(U,W) = \max\{\dim(U), \dim(W)\} - \dim(U \cap W)$, we mainly consider the subspace distance.

The vital property to guarantee a successful decoding is the *minimum distance* of the subspace code C, which shall be large and in turn decreases the cardinality of C. Conversely, it is also preferable to increase the information that each symbol which is transmitted carries. This corresponds to a large cardinality of C and hence there is a trade-off between the amount of transmitted data and resistance against errors or erasures.

Hence, for fixed parameters V and d the question to determine the maximum cardinality of C and to classify subspace codes up to symmetry arises.

While focusing on the so-called constant dimension case in which all elements of C have the same dimension, this thesis develops new general constructions, sporadic codes, bounds in special cases and the second classification of a set of parameters which is non-trivial and not of maximum distance.

The homepage `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16] was developed together with this thesis. It lists numerical values for lower and upper bounds of the sizes of subspace codes and constant dimension codes. There are also codes to download, for some parameters even all codes up to isomorphism. The parameters are bounded by field size ≤ 9 and ambient space ≤ 19 and only the subspace distance is considered.

In Chapter 2, we introduce the notation and basic facts which we will use at various places in this work. Chapter 3 continues with additional basic facts about the structure of subspaces in a vector space and it particularly introduces a binary linear programming formulation called DefaultCDCBLP, which is able to determine the maximum size of a subspace code with constant dimension for fixed other parameters and will be applied frequently, sometimes slightly modified. Chapter 4 states the well-known connection between the Hamming distance of pivot vectors and the subspace distance of corresponding subspaces. This chapter also states the well-known Echelon-Ferrers construction which we use as building block for some elaborate constructions as the coset construction in Chapter 5, which generalizes the original coset construction from [HK17c]. An often used constant dimension code (CDC) is the lifted maximum rank distance code (LMRD). Chapter 6 generalizes known upper bounds for CDCs containing LMRDs. This bound is called LMRD bound and the proof is used to get sporadic codes whose cardinalities exceed the corresponding best known largest codes for these parameters. This chapter describes the paper [Hei18] in more detail. Chapter 7 discusses the best known upper bounds for the cardinalities of constant dimension codes and shows new relations between bounds. One of the best recursive constructions, the linkage construction, is improved in Chapter 8 and numerical computations for small parameters listed in `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16] suggest that this is the best lower bound in most sets of parameters. The limit behaviour of ratios of lower and upper bounds and an infinite series of parameters in which the LMRD bound is surpassed are studied in Chapter 9. The chapters 7, 8, and 9 state and partially generalize or continue the work of the paper [HK17b]. Some symmetries are not feasible for large codes and can be handled in theory in Chapter 10. They can also be handled with computer calculations and Chapter 11 shows a general technique which is also implemented in `Magma` [BCP97] in the appendix. This yields a set S of subgroups of the $\mathrm{GL}(\mathbb{F}_2^7)$ with the property that all groups which are not in the conjugacy classes of elements of S under the $\mathrm{GL}(\mathbb{F}_2^7)$ are automorphism groups of CDCs in this setting with small cardinality. As a byproduct, we get a new largest code in this setting. This chapter and also the appendix provide the algorithm and the details of [Hei+17c]. In Chapter 12 we determine the third exact value of maximum cardinalities of CDCs and second classification of non-trivial parameters with non-maximum distance. This chapter generalizes the theory of [Hei+17a] and lists a classification of [HK17a]. We conclude this thesis in Chapter 13 with a list of open problems.

2 Preliminaries

Let $\mathbb{F}_q$ be the up to isomorphism unique finite field with q elements and denote $V \cong \mathbb{F}_q^v$ the up to isomorphism unique v-dimensional row vector space over $\mathbb{F}_q$. The i-th unit vector is commonly denoted as u_i. The vector space of matrices which have m rows, n columns and entries in $\mathbb{F}_q$ is $\mathbb{F}_q^{m\times n}$. If $M \in \mathbb{F}_q^{m\times n}$, then $M_{i,*}$ is the i-th row for $1 \le i \le m$, $M_{*,j}$ is the j-th column for $1 \le j \le n$, and consequently $M_{i,j}$ is the element in the i-th row and j-th column. We abbreviate $[n] = \{1, 2, \ldots, n\}$, if and only if as "iff", with respect to as "wrt.", and without loss of generality as "wlog.".

Grassmannian and q-binomial coefficients By $\begin{bmatrix} V \\ k \end{bmatrix}$ we denote the set of all k-dimensional subspaces in V, which is also called Grassmannian and denoted as $G_q(v,k)$ or $\mathcal{G}_q(v,k)$ in other literature.

Its size is given by the q-binomial coefficient $\begin{bmatrix} v \\ k \end{bmatrix}_q$, which is also called Gaussian binomial coefficient.

We refer to [AAR99; And76; Ber10; Ext83] and in particular to [BKW18b] for further reading.

1 Lemma
Let $q \ge 2$ be a prime power and k and v integers. Then

$$\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^v - q^i}{q^k - q^i} = \prod_{i=0}^{k-1} \frac{q^{v-i} - 1}{q^{k-i} - 1} = \prod_{i=1}^{k} \frac{q^{v-k+i} - 1}{q^i - 1}$$

if $0 \le k \le v$ and $\begin{bmatrix} v \\ k \end{bmatrix}_q = 0$ otherwise.

Proof
The first equality is proved by a simple counting argument. For the i-th basis vector of an ordered basis of a k-dimensional subspace of $\mathbb{F}_q^v$, we have $q^v - q^i$ $(i = 0, \ldots, k-1)$ possibilities, whereas, by the very same counting argument, $(q^k - q^0)(q^k - q^1) \cdot \ldots \cdot (q^k - q^{k-1})$ ordered bases span the same k-dimensional vector space. The remaining equations are simple transformations. □

For a prime power $q \ge 2$ and a non-negative integer n, we also define the q-number $[n]_q = \frac{q^n - 1}{q-1} = \sum_{i=0}^{n-1} q^i \in \mathbb{Z}_{\ge 0}$ and the q-factorial $[n]_q! = \prod_{i=1}^{n} [i]_q$ together with $[0]_q! = 1$. We also apply the notation of $[n]_q = \sum_{i=0}^{n-1} q^i$ for an arbitrary positive integer q. These

q-numbers are very useful in proofs containing q-binomial coefficients, due to the following correspondence.

2 Lemma
For $q \geq 2$ prime power and $0 \leq k \leq v$ integers, we have

$$\left[{v \atop k}\right]_q = \frac{[v]_q!}{[k]_q![v-k]_q!}.$$

Proof

$$\begin{aligned}\left[{v \atop k}\right]_q &= \prod_{i=1}^{k} \frac{q^{v-k+i}-1}{q^i-1} = \prod_{i=1}^{k} \frac{(q^{v-k+i}-1)/(q-1)}{(q^i-1)/(q-1)} = \prod_{i=1}^{k} \frac{[v-k+i]_q}{[i]_q} \\ &= \frac{\prod_{i=v-k+1}^{v}[i]_q}{\prod_{i=1}^{k}[i]_q} = \frac{\prod_{i=1}^{v}[i]_q}{\prod_{i=1}^{k}[i]_q \cdot \prod_{i=1}^{v-k}[i]_q} = \frac{[v]_q!}{[k]_q![v-k]_q!}.\end{aligned}$$ □

Particularly, Lemma 2 shows that the q-binomial coefficient is symmetric, i.e., $\left[{v \atop k}\right]_q = \left[{v \atop v-k}\right]_q$ and that the following two q-Pascal identities hold:

3 Lemma
For $q \geq 2$ prime power and $1 \leq k \leq v-1$ integers, we have

$$\left[{v \atop k}\right]_q = \left[{v-1 \atop k}\right]_q \cdot q^k + \left[{v-1 \atop k-1}\right]_q \quad \text{and} \quad \left[{v \atop k}\right]_q = \left[{v-1 \atop k}\right]_q + \left[{v-1 \atop k-1}\right]_q \cdot q^{v-k}.$$

Proof
Since $q^v - 1 = (q^{v-k}-1)q^k + (q^k-1) = (q^{v-k}-1) + (q^k-1)q^{v-k}$, dividing by $q-1$ yields $[v]_q = [v-k]_q q^k + [k]_q = [v-k]_q + [k]_q q^{v-k}$. Due to $1 \leq k \leq v-1$, we can divide this by $([k]_q[v-k]_q)$ to obtain $\frac{[v]_q}{[k]_q[v-k]_q} = \frac{1}{[k]_q}q^k + \frac{1}{[v-k]_q} = \frac{1}{[k]_q} + \frac{1}{[v-k]_q}q^{v-k}$. Multiplying with $\frac{[v-1]_q!}{[k-1]_q![v-k-1]_q!}$ yields

$$\frac{[v]_q!}{[k]_q![v-k]_q!} = \frac{[v-1]_q!}{[k]_q![v-k-1]_q!}q^k + \frac{[v-1]_q!}{[k-1]_q![v-k]_q!} = \frac{[v-1]_q!}{[k]_q![v-k-1]_q!} + \frac{[v-1]_q!}{[k-1]_q![v-k]_q!}q^{v-k},$$

which concludes the proof with Lemma 2. □

Moreover, the q-binomial coefficient can be written as a sum:

4 Lemma
For q prime power and $k \leq v$ integers, we have:

$$\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q = \sum_{l=0}^{k} c(q,k,l) q^{lv},$$

where

$$c(q,k,l) = \frac{(-1)^{k-l} \sum_{w \in \mathbb{F}_2^k, ||w||_1 = l} q^{\sum_{j=1}^{k} j \cdot w_j}}{q^{lk} \prod_{j=1}^{k}(q^j - 1)}$$

does not depend on v.

Proof
If $k < 0$, then both sides are zero, hence we assume $0 \leq k$. Let $w \in \mathbb{F}_2^k$ iterate over all summands of the evaluation of $\prod_{j=1}^{k}(q^{v-k+j} - 1)$ such that $w_j = 1$ chooses q^{v-k+j} and $w_j = 0$ chooses -1, i.e.,

$$\begin{aligned}
\prod_{j=1}^{k}(q^{v-k+j} - 1) &= \sum_{w \in \mathbb{F}_2^k} \prod_{j=1}^{k} (q^{v-k+j} w_j + (-1)(1 - w_j)) \\
&= \sum_{w \in \mathbb{F}_2^k} (-1)^{k - ||w||_1} q^{\sum_{j=1}^{k} w_j (v-k+j)} = \sum_{l=0}^{k} \sum_{w \in \mathbb{F}_2^k, ||w||_1 = l} (-1)^{k-l} q^{l(v-k) + \sum_{j=1}^{k} j \cdot w_j} \\
&= \sum_{l=0}^{k} \left((-1)^{k-l} q^{l(v-k)} \sum_{w \in \mathbb{F}_2^k, ||w||_1 = l} q^{\sum_{j=1}^{k} j \cdot w_j} \right).
\end{aligned}$$

Hence, this can be inserted in the equation for the q-binomial coefficient:

$$\begin{aligned}
\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q = \prod_{j=1}^{k} \frac{q^{v-k+j} - 1}{q^j - 1} &= \frac{\sum_{l=0}^{k} \left((-1)^{k-l} q^{l(v-k)} \sum_{w \in \mathbb{F}_2^k, ||w||_1 = l} q^{\sum_{j=1}^{k} j \cdot w_j} \right)}{\prod_{j=1}^{k}(q^j - 1)} \\
&= \sum_{l=0}^{k} \frac{(-1)^{k-l} \sum_{w \in \mathbb{F}_2^k, ||w||_1 = l} q^{\sum_{j=1}^{k} j \cdot w_j}}{q^{lk} \prod_{j=1}^{k}(q^j - 1)} q^{lv} = \sum_{l=0}^{k} c(q,k,l) q^{lv}. \qquad \square
\end{aligned}$$

The following inequality will be applied multiple times to bound quotients of q-numbers.

5 Lemma
For $1 < b$ and a real numbers, we have $\frac{a-1}{b-1} \circ \frac{a}{b}$ for $a \circ b$ with $\circ \in \{<, \leq, =, \geq, >\}$. Hence, we have $\frac{[x]_q}{[y]_q} \circ q^{x-y}$ for $q \geq 2$ prime power and integers x and y with $1 \leq y$ and $x \circ y$.

Divisions of two q-binomial coefficients can be computed straight forward:

6 Lemma (cf. [HKK16b, Lemma 2.4])
For $q \geq 2$ prime power and $1 \leq k \leq v$, we have

$$\frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v \\ k-1 \end{bmatrix}_q} = \frac{[v-k+1]_q}{[k]_q} = \frac{q^{v-k+1}-1}{q^k-1}.$$

Proof
This is an application of Lemma 2.

$$\frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v \\ k-1 \end{bmatrix}_q} = \frac{[v]_q![k-1]_q![v-k+1]_q!}{[k]_q![v-k]_q![v]_q!} = \frac{[v-k+1]_q}{[k]_q}.$$

□

The following lemma simplifies the comparison of the Anticode bound (Theorem 107) to the Compact Johnson bound (Corollary 117) later.

7 Lemma
For $q \geq 2$ prime power and integers a, b, c with $0 \leq b \leq c \leq a$, we have:

$$\frac{\begin{bmatrix} a \\ b \end{bmatrix}_q}{\begin{bmatrix} c \\ b \end{bmatrix}_q} = \frac{\begin{bmatrix} a \\ c \end{bmatrix}_q}{\begin{bmatrix} a-b \\ c-b \end{bmatrix}_q}.$$

Proof
This is also an application of Lemma 2.

$$\frac{\begin{bmatrix} a \\ b \end{bmatrix}_q}{\begin{bmatrix} c \\ b \end{bmatrix}_q} = \frac{[a]_q![b]_q![c-b]_q!}{[b]_q![a-b]_q![c]_q!} = \frac{[a]_q![c-b]_q![a-c]_q!}{[c]_q![a-c]_q![a-b]_q!} = \frac{\begin{bmatrix} a \\ c \end{bmatrix}_q}{\begin{bmatrix} a-b \\ c-b \end{bmatrix}_q}.$$

□

The determination of the exact value of $\begin{bmatrix} v \\ k \end{bmatrix}_q$ can be cumbersome and is not always required since an approximation is often sufficient. To this end, Kötter and Kschischang proved in [KK08b, Lemma 4] that $1 < \begin{bmatrix} v \\ k \end{bmatrix}_q / q^{k(v-k)} < 4$ for a prime power q and $0 < k < v$. In fact, using the q-Pochhammer symbol, which is defined as $(a;q)_n = \prod_{i=0}^{n-1}(1-aq^i)$, in the special case $(1/q;1/q)_n = \prod_{i=1}^{n}(1-q^{-i})$ together with the limit $(1/q;1/q)_\infty = \prod_{i=1}^{\infty}(1-q^{-i})$, their proof shows a more exact estimation:

8 Lemma (cf. [KK08b, Lemma 4])
For $q \geq 2$ prime power and $0 < k < v$, we have

$$1 < \begin{bmatrix} v \\ k \end{bmatrix}_q / q^{k(v-k)} < (1/q;1/q)_k^{-1} < (1/q;1/q)_\infty^{-1} \leq (1/2;1/2)_\infty^{-1} \approx 3.4627.$$

We will use $\mu(q) := (1/q; 1/q)_\infty^{-1}$ as an abbreviation. $\mu(q)$ is monotonically decreasing in q and some approximated values for small q are given in Table 2. In particular, a coarse upper bound involving only exponents is $\mu(q) \leq 4 \leq q^2$ for all $q \geq 2$ prime power and $\mu(q) \leq 3 \leq q$ for all $q \geq 3$ prime power.

q	2	3	4	5	7	8	9
$\mu(q)$	3.46	1.79	1.45	1.32	1.20	1.16	1.14
$\log_q(\mu(q))$	1.79	0.53	0.27	0.17	0.09	0.07	0.06

Table 2: Values for $\mu(q)$ and $\log_q(\mu(q))$ for small q.

We perform a similar analysis concerning the limit behavior of $q^{ab} / \left[\begin{smallmatrix} a+b \\ b \end{smallmatrix}\right]_q$.

9 Lemma (cf. [HK17b, Lemma 5])
For $q \geq 2$ prime power and a, b positive integers, we have $\lim_{a\to\infty} q^{ab} / \left[\begin{smallmatrix} a+b \\ b \end{smallmatrix}\right]_q = (1/q; 1/q)_b$ and this convergence is strictly monotonically decreasing.

Moreover, we have

$$\begin{array}{lllllll} (1/q;1/q)_b & > & (1/q;1/q)_\infty & \geq & (1/2;1/2)_\infty & > & 0.288788 \text{ and} \\ (1/q;1/q)_b & \geq & (1/2;1/2)_b & > & (1/2;1/2)_\infty & > & 0.288788. \end{array}$$

Proof
The definition of q-binomial coefficients and q-Pochhammer symbols yields

$$\lim_{a\to\infty} \frac{q^{ab}}{\left[\begin{smallmatrix} a+b \\ b \end{smallmatrix}\right]_q} = \lim_{a\to\infty} \frac{q^{ab}}{\prod_{i=1}^{b} \frac{q^{a+i}-1}{q^i-1}} = \lim_{a\to\infty} \prod_{i=1}^{b} \frac{q^i - 1}{q^i - q^{-a}} = \prod_{i=1}^{b} (1 - q^{-i}) = (1/q; 1/q)_b.$$

The monotonicity follows from

$$\frac{q^{ab} / \left[\begin{smallmatrix} a+b \\ b \end{smallmatrix}\right]_q}{q^{(a+1)b} / \left[\begin{smallmatrix} a+1+b \\ b \end{smallmatrix}\right]_q} = \frac{[a+1+b]_q! [b]_q! [a]_q!}{[b]_q! [a+1]_q! [a+b]_q!} q^{-b} = \frac{[a+1+b]_q}{[a+1]_q} q^{-b} > q^b q^{-b} = 1.$$

The inequalities follow from $1-q^{-i} < 1$ and $1-2^{-i} \leq 1-q^{-i}$ and $\prod_{i=1}^{b}(1-q^{-i}) > \prod_{i=1}^{\infty}(1-q^{-i}) \geq \prod_{i=1}^{\infty}(1-2^{-i})$ in the upper and $\prod_{i=1}^{b}(1-q^{-i}) \geq \prod_{i=1}^{b}(1-2^{-i}) > \prod_{i=1}^{\infty}(1-2^{-i})$ in the lower case. □

Although both series of inequalities in the lemma seem to form a single series, the critical part is not comparable: $(1/2;1/2)_b \not> (1/q;1/q)_\infty$, e.g., $b = 1$ and $q = 3$ yield $(1/2;1/2)_b = 0.5$ and $(1/q;1/q)_\infty \approx 0.56$.

Moreover, we need to count the number of subspaces which lie in a given subspace and only intersect another given subspace trivially. This number is well-known in a more general setting.

10 Lemma ([BKW18b, Lemma 1])
Let $B \leq U \leq W \leq V$ with $\dim(B) = b$, $\dim(U) = u$, and $\dim(W) = w$ and c an integer. Then
$$\#\{A \leq W \mid \dim(A) = c \text{ and } A \cap U = B\} = q^{(u-b)(c-b)} \begin{bmatrix} w-u \\ c-b \end{bmatrix}_q .$$
Both sides of the equation are zero iff $c < b$ or $w - u < c - b$.

The usage of $B = \{0\}$ in the last lemma implies:

11 Definition
Let W and U be subspaces of V. The set of all c-dimensional subspaces that are in W and intersect U trivially is
$$\begin{bmatrix} W \backslash U \\ c \end{bmatrix} := \{A \leq W \mid \dim(A) = c \text{ and } A \cap U = \{0\}\}.$$
For $w = \dim(W)$ and $u = \dim(U \cap W)$ its cardinality is denoted as $\begin{bmatrix} w \backslash u \\ c \end{bmatrix}_q$ which can be computed:
$$\begin{bmatrix} w \backslash u \\ c \end{bmatrix}_q = \prod_{i=0}^{c-1} \frac{q^w - q^{u+i}}{q^c - q^i} = q^{uc} \prod_{i=0}^{c-1} \frac{q^{w-u} - q^i}{q^c - q^i} = q^{uc} \begin{bmatrix} w-u \\ c \end{bmatrix}_q$$
for $0 \leq c \leq w - u$ and 0 otherwise.

This allows to count the number of l-subspaces of V that are incident to a specific k-subspace.

12 Corollary
Let V be a subspace, $0 \leq k \leq v$, $0 \leq l \leq v$ integers, and $U \in \begin{bmatrix} V \\ k \end{bmatrix}$. Then $\#\{W \in \begin{bmatrix} V \\ l \end{bmatrix} \mid W \leq U\} = \begin{bmatrix} k \\ l \end{bmatrix}_q$ if $l \leq k$ and $\#\{W \in \begin{bmatrix} V \\ l \end{bmatrix} \mid U \leq W\} = \begin{bmatrix} v-k \\ l-k \end{bmatrix}_q$ if $k \leq l$.

Proof
If $l \leq k$, then $\#\{W \in \begin{bmatrix} V \\ l \end{bmatrix} \mid W \leq U\} = \#\{W \in \begin{bmatrix} U \\ l \end{bmatrix}\} = \begin{bmatrix} k \\ l \end{bmatrix}_q$ by Lemma 1. If $k \leq l$ then each subspace in $\{W \in \begin{bmatrix} V \\ l \end{bmatrix} \mid U \leq W\}$ is determined by basis extension as $W = Z \oplus U$ for $Z \in \begin{bmatrix} V \backslash U \\ l-k \end{bmatrix}$ while each $Z \in \begin{bmatrix} W \backslash U \\ l-k \end{bmatrix}$ determines the same subspace W. As $\# \begin{bmatrix} V \backslash U \\ l-k \end{bmatrix} = \begin{bmatrix} v \backslash k \\ l-k \end{bmatrix}_q$ and $\# \begin{bmatrix} W \backslash U \\ l-k \end{bmatrix} = \begin{bmatrix} l \backslash k \\ l-k \end{bmatrix}_q$, which is in particular independent of U and

W, Definition 11 provides

$$\#\{W \in \begin{bmatrix} V \\ l \end{bmatrix} \mid U \le W\} = \frac{\begin{bmatrix} v\backslash k \\ l-k \end{bmatrix}_q}{\begin{bmatrix} l\backslash k \\ l-k \end{bmatrix}_q} = \frac{\begin{bmatrix} v-k \\ l-k \end{bmatrix}_q q^{k(l-k)}}{\begin{bmatrix} l-k \\ l-k \end{bmatrix}_q q^{k(l-k)}} = \begin{bmatrix} v-k \\ l-k \end{bmatrix}_q. \qquad \square$$

The rows of any matrix $M \in \mathbb{F}_q^{k\times v}$ having rank k, i.e., $1 \le k \le v$ integers, span a subspace S in $\begin{bmatrix} V \\ k \end{bmatrix}$. In this context, the matrix M is called generator matrix of S. Since the application of the Gaussian elimination algorithm on the rows of M does not change its row-space, any matrix obtained via basic row operations is a generator matrix of S which is especially true for the unique matrix in reduced row echelon form (RREF), cf. [Gor16, Proposition 8.2]. A matrix B in $\mathbb{F}^{r\times s}$, $\mathbb{F}$ is a field, has RREF iff B has $\mathrm{rk}(B)$ non-zero rows at the top and $r - \mathrm{rk}(B)$ zero rows at the bottom, the first non-zero entry from the left in each row is a 1, the so called leading 1, the corresponding column is a unit column, and if a non-zero row i has its first entry in position j then the row $i+1$ has at least j zeros in the beginning. Conversely, any basis of S, written as the rows of a matrix N produce a generator matrix N of S. Although $S \in \begin{bmatrix} V \\ k \end{bmatrix}$ has $\#\,\mathrm{GL}(S) = \#\,\mathrm{GL}(\mathbb{F}_q^k) = \prod_{i=0}^{k-1}(q^k - q^i)$ ordered bases and $\#\,\mathrm{GL}(\mathbb{F}_q^k)/k!$ unordered bases, it has exactly one basis whose rows form a matrix in RREF and in particular the requirement of being in RREF only chooses a *canonical* basis of S. Hence the bijection

$$\tau_{q,k,v} : \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \to \{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k, A \text{ is in RREF}\}$$

and surjective map

$$\mathrm{RREF}_{q,k,v} : \{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k\} \to \{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k, A \text{ is in RREF}\}$$

will be applied multiple times. If q, v, and k are clear from the context, we will abbreviate $\tau_{q,k,v}$ with τ and $\mathrm{RREF}_{q,k,v}$ with RREF. For a matrix $M \in \mathbb{F}^{r\times s}$ in RREF, a pivot column c is a column of M such that there is a row that has its leading 1 in c. Note that any pivot column is a unit vector, M has the $\mathrm{rk}(M)$ pivot columns $u_1, u_2, \dots, u_{\mathrm{rk}(M)} \in \mathbb{F}^r$, and if column i and $j > i$ are indices of pivot columns of M with $M_{*,i} = u_x$ and $M_{*,j} = u_y$, then $x < y$. Using the weight of a vector $\mathrm{wt}(u) = \#\{j \in \{1, \dots, v\} \mid u_j \ne 0\}$ for $u \in \mathbb{F}^v$, the maps

$$\mathrm{p}_{q,v,k} : \begin{cases} \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} & \to \{u \in \mathbb{F}_2^v \mid \mathrm{wt}(u) = k\} \\ U & \mapsto u, \text{ such that } u_j = 1 \text{ iff } j \text{ is a pivot column of } \tau(U) \end{cases}$$

and

$$\mathrm{p}_{q,v,k} : \begin{cases} \{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k, A \text{ is in RREF}\} & \to \{u \in \mathbb{F}_2^v \mid \mathrm{wt}(u) = k\} \\ M & \mapsto \mathrm{p}(\tau^{-1}(M)) \end{cases}$$

for $k = 0, 1, \dots, v$ will be useful in the remaining text. If the context implies q, v, and k, we abbreviate $\mathrm{p}_{q,v,k}$ with p. The image of p is called the pivot vector of U or M.

13 Example
Denoting u_i as the i-th unit vector, the subspace $\langle u_1, u_2\rangle \le \mathbb{F}_2^3$, which contains the vectors $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, and $(1,1,0)$, fulfills $\tau(\langle u_1, u_2\rangle) = \left(\begin{smallmatrix}1&0&0\\0&1&0\end{smallmatrix}\right)$. Conversely, the rows of any given matrix $M \in \mathbb{F}_q^v$ with $\operatorname{rk}(M) = k$, i.e., not necessary in RREF, span W, a k-dimensional subspace in $\mathbb{F}_q^v$, and in particular $\tau(W)$ is the RREF of M.
Here, we have $\mathrm{p}(\langle u_1, u_2\rangle) = (1,1,0)$ and $\mathrm{p}(\left(\begin{smallmatrix}1&0&0\\0&1&0\end{smallmatrix}\right)) = (1,1,0)$.

Using $\begin{bmatrix}V\\k\end{bmatrix}$ as vertex set of a graph, we obtain the so-called *Grassmann graph* [BCN89, Chapter 9.3], in which two vertices are adjacent iff the intersection of the two corresponding subspaces has dimension $k-1$. The Grassmann graph is $q[k]_q[v-k]_q$-regular (Corollary 103 and [BCN89, Theorem 9.3.3]) and even *distance-regular*, i.e., for two vertices v_1 and v_2 and integers d_1 and d_2, the number of vertices with distance d_1 from v_1 and d_2 from v_2 only depends on d_1, d_2, and the distance between v_1 and v_2 but not on the specific choice of v_1 and v_2 [BCN89, Chapter 4.1].

Metric spaces and subspace distance The set of all subspaces of V, $\mathcal{L}(V) = \bigcup_{i=0}^{v} \begin{bmatrix}V\\i\end{bmatrix}$, forms a metric space associated with the so-called subspace distance $\mathrm{d_s}(U,W) = \dim(U+W) - \dim(U\cap W)$, cf. [KK08b, Lemma 1]. As a short notation, we will use $U \le V$ for $U \in \mathcal{L}(V)$.

Depending on the situation, another reformulation of $\mathrm{d_s}(U,W)$ may be useful. Applying $\dim(U+W) = \dim(U) + \dim(W) - \dim(U\cap W)$, we get:

$$\begin{aligned}\mathrm{d_s}(U,W) &= \dim(U+W) - \dim(U\cap W) = \dim(U) + \dim(W) - 2\dim(U\cap W)\\ &= 2\dim(U+W) - \dim(U) - \dim(W) = 2\operatorname{rk}\left(\begin{pmatrix}\tau(U)\\ \tau(W)\end{pmatrix}\right) - \dim(U) - \dim(W).\end{aligned}$$

The metric space $(\mathcal{L}(V), \mathrm{d_s})$ may be viewed as a q-analogue of the Hamming space $(\mathbb{F}_2^v, \mathrm{d_h})$ used in conventional coding theory via the subset-subspace analogy [Knu71].

In the notation of projective geometry, the elements of $\mathcal{L}(V)$ are the flats of $\mathrm{PG}(V) \cong \mathrm{PG}(\mathbb{F}_q^v) \cong \mathrm{PG}(v-1,q)$ and in some literature $\mathcal{L}(V)$ is denoted as $\mathcal{P}_q(v)$. In particular, we use always the vector space dimension. A survey on Galois geometries and coding theory can be found in [ES16], see also [CPS18]. Subspaces of small (algebraic) dimension or co-dimension get special names according to Table 3. A vector space of dimension k is also abbreviated as k-space or k-subspace. If $U \le W$ or $W \le U$ for $U, W \le V$, then we call U and W incident or U incident to W or W incident to U.

$\dim(U)$	1	2	3	4	$v-1$
name	point	line	plane	solid	hyperplane

Table 3: Names for subspaces according to their dimensions.

Moreover, $\mathcal{L}(V)$ is a lattice – the so-called subspace lattice. A possible visualization is therefore a Hasse diagram, e.g, Figure 3, which shows a Hasse diagram of $\mathcal{L}(\mathbb{F}_2^4)$.

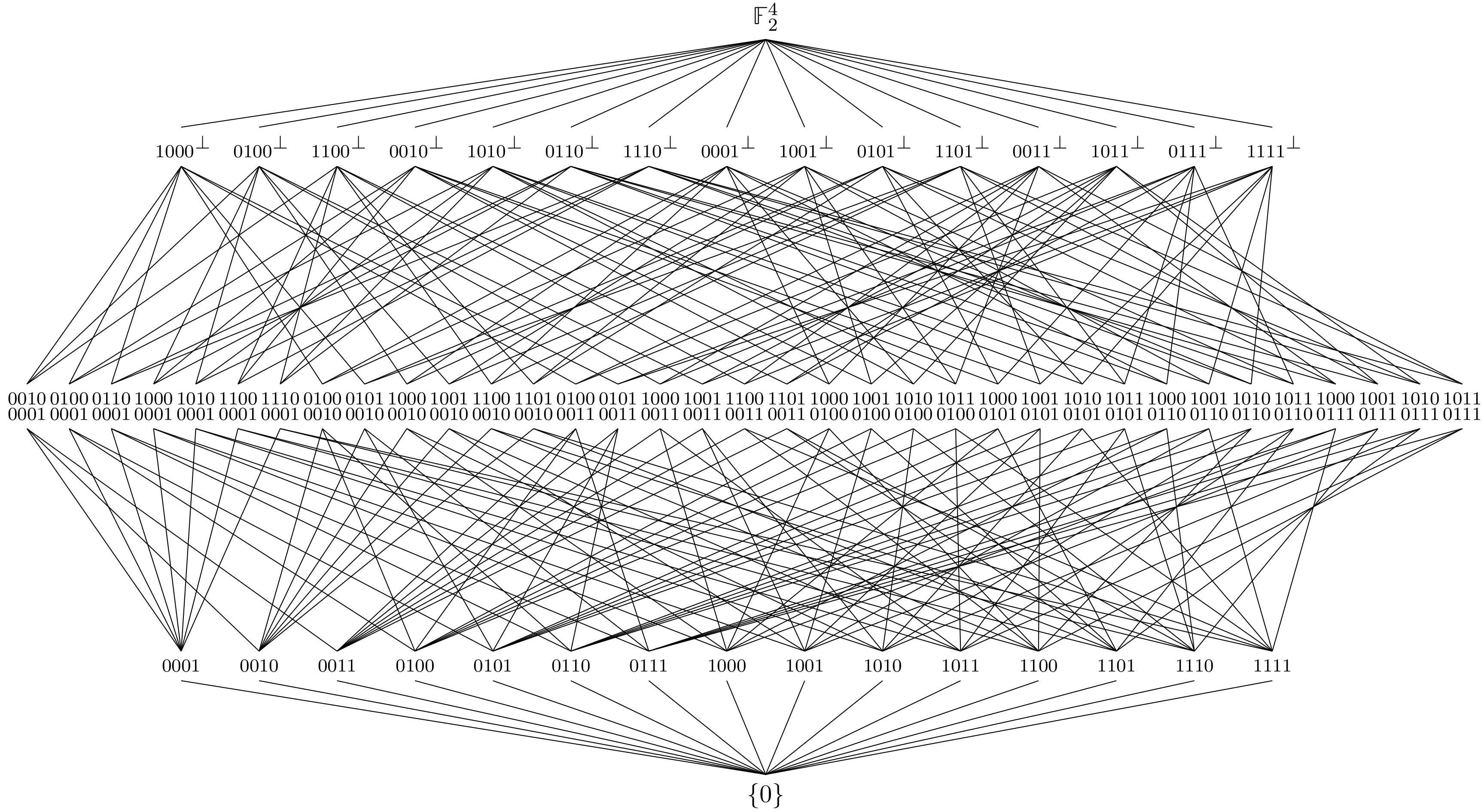
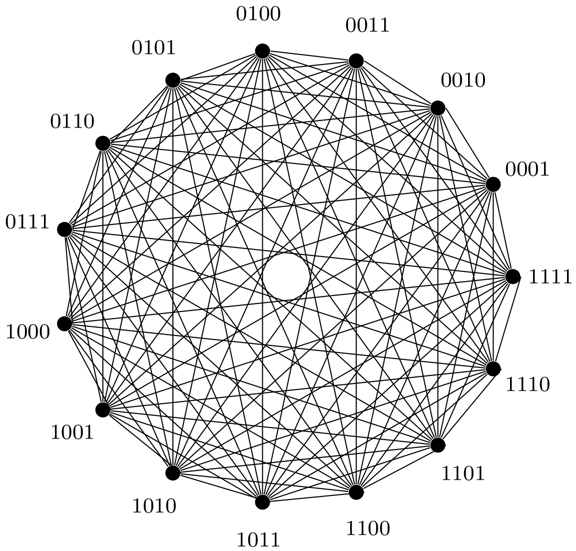
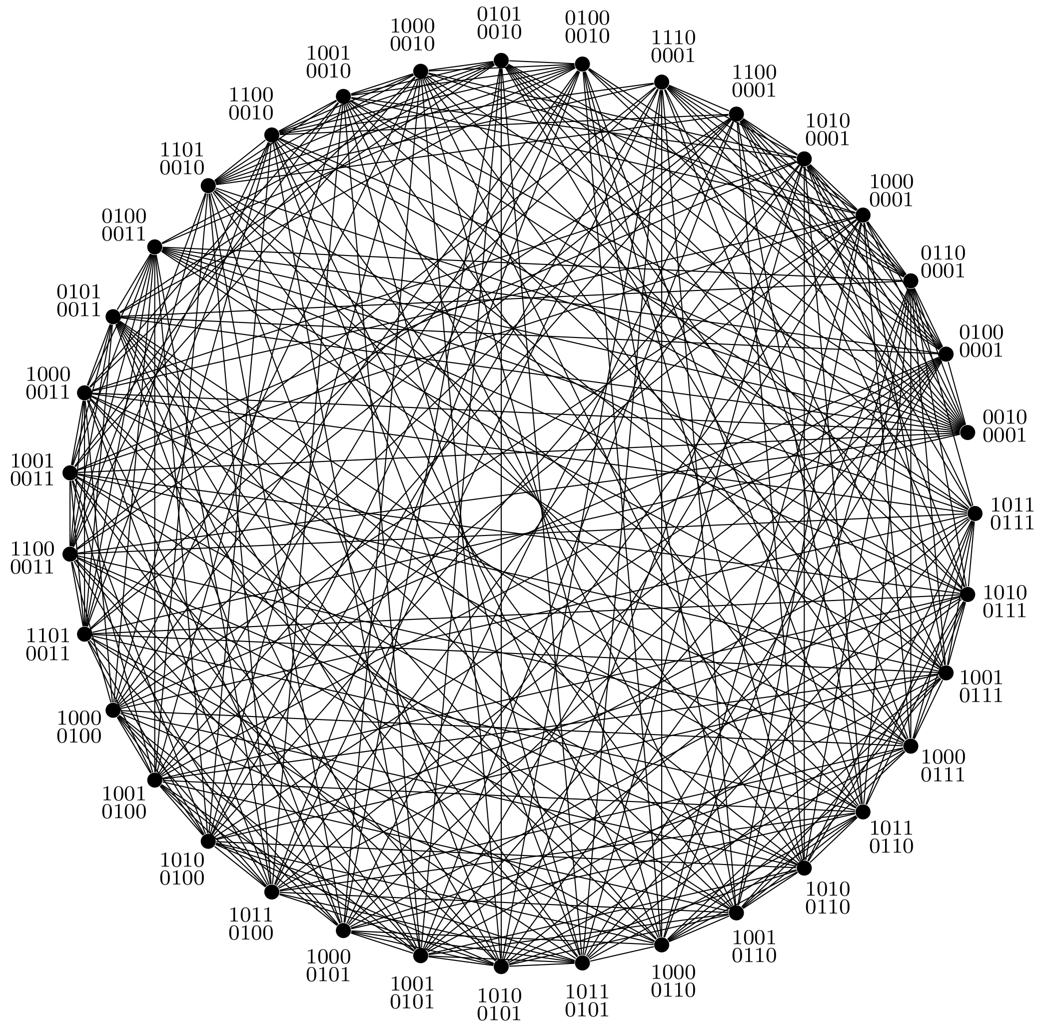


Figure 3: Hasse diagram of $\mathcal{L}(\mathbb{F}_2^4)$. Any subspace U of $\mathbb{F}_2^4$ is denoted as $\tau(U)$ where we omit the brackets and the orthogonal space is wrt. the standard inner product.



(a) Grassmann graph of $\begin{bmatrix} \mathbb{F}_2^4 \\ 1 \end{bmatrix}$. Two 1-subspaces are adjacent iff their intersection has dimension zero, i.e., the graph is complete.



(b) Grassmann graph of $\begin{bmatrix} \mathbb{F}_2^4 \\ 2 \end{bmatrix}$. Two 2-subspaces are adjacent iff their intersection has dimension one, hence this is an 18-regular graph.

Figure 4: Grassmann graphs of $\begin{bmatrix} \mathbb{F}_2^4 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} \mathbb{F}_2^4 \\ 2 \end{bmatrix}$.

Injection distance Another metric on $\mathcal{L}(V)$ is the so-called injection distance $\mathrm{d_i}$ (cf. [SK09]) which is defined by

$$\begin{aligned}\mathrm{d_i}(U,W) &= \max\{\dim(U),\dim(W)\} - \dim(U\cap W)\\ &= \dim(U+W) - \min\{\dim(U),\dim(W)\}.\end{aligned}$$

For $U, W \in \mathcal{L}(V)$, we have

$$\begin{aligned}\mathrm{d_s}(U,W) &= \mathrm{d_i}(U,W) + \min\{\dim(U),\dim(W)\} - \dim(U\cap W)\\ &= \mathrm{d_i}(U,W) + \dim(U+W) - \max\{\dim(U),\dim(W)\}\\ &= 2\mathrm{d_i}(U,W) - |\dim(U) - \dim(W)|.\end{aligned}$$

This can be bounded with

$$\mathrm{d_i}(U,W) \leq \mathrm{d_s}(U,W) \leq 2\mathrm{d_i}(U,W).$$

The first relation is an equality iff $U \leq W$ or $W \leq U$ and the second is an equality iff $\dim(U) = \dim(W)$, hence $\mathrm{d_s}$ and $\mathrm{d_i}$ are equivalent on $\begin{bmatrix} V \\ k \end{bmatrix}$ for each $k = 0, \ldots, v$.

The injection distance $\mathrm{d_i}(U,W)$ equals the graph distance of the vertices corresponding to U and W in the Grassmann graph.

$\mathcal{H}_k(U)$ is an arbitrary k-dimensional subspace of a vector space U, cf. [KK08b, before Definition 1].

Using the RLNCC $W = \mathcal{H}_l(U) \oplus Z$ Kötter and Kschischang prove that, for a sent U, a received W can be successfully decoded by a minimum distance decoder, i.e., $\operatorname{argmin}\{\mathrm{d_x}(W,B) \mid B \in C\}$, $\mathrm{x} \in \{\mathrm{i},\mathrm{s}\}$, if the distance is large enough. The proof involving the injection distance is analogous to the proof involving the subspace distance, since $\mathrm{d_s}(X,U) = \mathrm{d_i}(X,U)$ for all U with $X \leq U$. Additional notation will be defined in the paragraph "Subspace codes".

14 Theorem (cf. [KK08b, Theorem 2])
Let C be a subspace code, $\mathrm{x} \in \{\mathrm{i},\mathrm{s}\}$, $U \in C$, and $W = \mathcal{H}_l(U) \oplus Z$ with $t = \dim(Z)$ and $p = \max\{0, \max\{K(C)\} - l\}$. If $t + p < \mathrm{D_x}(C)/2$, then $U = \operatorname{argmin}\{\mathrm{d_x}(W,B) \mid B \in C\}$.

Proof
Let $X = \mathcal{H}_l(U)$. Since $X \leq U$ and $X \leq W$, we have $\mathrm{d_x}(X,U) = \dim(U) - \dim(X) \leq p$ and $\mathrm{d_x}(X,W) = \dim(W) - \dim(X) = t$, which then shows $\mathrm{d_x}(U,W) \leq p + t < \mathrm{D_x}(C)/2$ with the triangle inequality. Next, for $Y \neq U \in C$, we have $\mathrm{D_x}(C) \leq \mathrm{d_x}(Y,U) \leq \mathrm{d_x}(Y,W) + \mathrm{d_x}(W,U)$ again by the triangle inequality, i.e., $\mathrm{d_x}(Y,W) \geq \mathrm{D_x}(C) - \mathrm{d_x}(W,U) > 2\mathrm{d_x}(W,U) - \mathrm{d_x}(W,U) = \mathrm{d_x}(W,U)$. □

This theorem justifies that the subspace distance and the injection distance is studied in the context of subspace coding.

Groups Let G be a group and U be a subgroup, denoted $U \leq G$. The *right coset of g with respect to U* is $Ug = \{ug \mid u \in U\}$. The set of right cosets is $U \backslash G$. The *left coset of g with respect to U* is analogously $gU = \{gu \mid u \in U\}$. The set of left cosets is G/U. Finally, $\#U\backslash G = \#G/U = (G : U)$ is also called the *index of U in G*.

15 Lemma (Lagrange's theorem, [KS04, 1.1.7])
If G is a finite group and $U \leq G$, then $\#U \cdot (G : U) = \#G$.

Let G be a group, $U \leq G$ a subgroup and $g, h \in G$ elements. The *conjugation of h with g* is $h^g = g^{-1}hg$, the *conjugation class of h in G* is $h^G = \{h^g \mid g \in G\}$, the *conjugation of U with g* is $U^g = g^{-1}Ug = \{g^{-1}ug \mid u \in U\}$, and the *conjugation class of U in G* is $U^G = \{U^g \mid g \in G\}$.

For two groups A and B with $A \leq B$ let $N_B(A)$ denote the normalizer of A in B, i.e., $N_B(A) = \{b \in B \mid A^b = A\}$, and let $A \trianglelefteq B$ denote that A is a normal subgroup in B, i.e., $A^b = A$ for all $b \in B$.

For a finite group G and a prime p, a *p-subgroup of G* is a subgroup of G of order p^i for an i and a *Sylow p-subgroup of G* is a subgroup of G that is not properly contained in any p-subgroup of G.

The following theorem resembles [KM79, Theorem 11.1.1] and the fact about the index is from [KS04, 3.2.3].

16 Theorem (Sylow's theorem, [KM79, Theorem 11.1.1], [KS04, 3.2.3])
Let G be a finite group and p be a prime with $p \mid \#G$.

1. For each i with $p^i \mid \#G$ there is a subgroup of G of order p^i.
2. If $p^{i+1} \mid \#G$, then each subgroup of G of order p^i is contained in a subgroup of G of order p^{i+1}. In particular, if j is maximal with $p^j \mid \#G$ then any Sylow p-subgroup of G has order p^j and conversely any subgroup of order p^j is a Sylow p-subgroup of G.
3. The Sylow p-subgroups of G are conjugate in G.
4. The number r of Sylow p-subgroups of G fulfills $r \equiv 1 \pmod p$ and $r = (G : N_G(P))$ for a Sylow p-subgroup P of G. In particular $r \mid \#G$.

A consequence of this lemma of particular interest is:

17 Corollary
Let G be a finite group and p be a prime with $p \mid \#G$. Then any Sylow p-group contains a conjugate of any p-group.

The trivial group and 0-subspace is denoted as $\langle\rangle$ or $\{0\}$.

18 Definition ([KM79, Page 33, 134f], [Tho68], cf. [PS00])
A *subnormal series* of a group G is a series of subgroups $(G_1, \ldots, G_k)$ such that $\langle\rangle = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k \trianglelefteq G_{k+1} = G$.

A group G is called *solvable* if it has a subnormal series $\langle\rangle = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_k \trianglelefteq G_{k+1} = G$ whose quotient groups are abelian, i.e., G_i/G_{i-1} is abelian for all $i \in [k+1]$.

A *solvable number* is a positive integer n such that any group of order n is solvable. The negation is called *non-solvable number*.

19 Lemma ([Tho68], cf. [PS00])
The positive integer n is non-solvable number iff $d \mid n$ for $d \in A \cup B \cup C \cup D \cup E$ with
$A = \{2^p(2^{2p} - 1) \mid p \text{ prime}\}$,
$B = \{3^p(3^{2p} - 1)/2 \mid p \geq 3 \text{ prime}\}$,
$C = \{p(p^2 - 1)/2 \mid p \geq 7 \text{ prime}, p^2 + 1 \equiv 0 \pmod 5\}$,
$D = \{5616\}$, and
$E = \{2^{2p}(2^{2p} + 1)(2^p - 1) \mid p \geq 3 \text{ prime}\}$.

This shows a generalization of the famous Feit-Thompson theorem [Koc70, 2.8.1], which states that any finite group with odd order is solvable and hence any positive and odd integer is a solvable number.

20 Corollary
Any non-solvable number is divisible by 12 or 20.

Proof
Using $4 \mid 2^p$ and $3^{2p} - 1 = 9^p - 1 \equiv 1^p - 1 = 0 \pmod 8$ for any prime p, $2 \mid p - 1 \wedge 4 \mid p + 1$ or $4 \mid p - 1 \wedge 2 \mid p + 1$ for any odd prime p, $5616 = 4 \cdot 1404$, and $4 \mid 2^{2p} = 4^p$ for any prime p, Lemma 19 shows that any non-solvable number is a multiple of 4.

Since $2^{2p} \equiv 1 \pmod 3$, $3 \mid 3^p$, and $3 \mid (p-1)p(p+1)$ for all primes p, $5616 = 3 \cdot 1872$, and $2^{2p} \equiv -1 \pmod 5$ for odd primes p, Lemma 19 shows that any non-solvable number is a multiple of 3 in the cases A, B, C, D and a multiple of 5 in the case E. $\square$

In particular, the difference of any two non-solvable numbers is at least 12 and this is attained between e.g. 168 and 180 as the first non-solvable numbers $60, 120, 168, 180, 240, 300, 336, 360, 420, 480, 504, 540, 600, 660, 672, 720, 780, 840, 900, 960, 1008$ (cf. `https://oeis.org/A056866`) show.

For a finite group G and a set of primes π, a *Hall π-subgroup of G* is a subgroup of G such that any prime that divides its order is contained in π and vice versa and its order is coprime to its index in G.

For example, Theorem 16 shows that any Sylow p-subgroup of the finite group G is a Hall π-subgroup of G with $\pi = \{p\}$. Although for $\pi = \{p\}$ a Hall π-subgroup always exist by Theorem 16, in general this is not true, e.g., the alternating group on five elements, A_5, contains a Hall $\{2, 3\}$-subgroup, i.e., $A_4 \leq A_5$, but neither a non-trivial Hall $\{3, 5\}$-subgroup nor a non-trivial Hall $\{2, 5\}$-subgroup [KS04, Page 135].

A positive divisor d of an integer n is called *Hall divisor* if $\mathrm{GCD}(d, n/d) = 1$, i.e., d and n/d are coprime.

Although the following theorem resembles [KM79, Theorem 20.1.1], the version in e.g. [Koc70, 11.1.1] contains additional facts about the number of Hall π-subgroups of G.

21 Theorem (Hall's theorem, [KM79, Theorem 20.1.1])
Let G be a finite solvable group, m be a Hall divisor of $\#G$, and π be the set of primes dividing m.

1. G contains at least one Hall π-subgroup, which then has order m.
2. The Hall π-subgroups of G are conjugate in G.
3. Any subgroup of G whose order divides m is contained in a Hall π-subgroup of G.

The orders of a set of groups are abbreviated as a string $1^{n_1}2^{n_2}\ldots$ such that there are n_i groups of order i in the set and we omit the cases with $n_i = 0$.

Occasionally, we will mention *abstract types* of groups. We use C_n for the cyclic group, D_n for the dihedral group, Q_n for the quaternion group of order n, A_n for the alternating group, and S_n for the symmetric group on n elements. $\times$ denotes a direct product and $\rtimes$ denotes a (not necessarily unique) semidirect product of groups.

The `Small Groups Library` [BEO], which is implemented in the computer algebra system `Magma` [BCP97] and `GAP` [GAP18], provides precise information of the abstract types of groups with small order. It contains among others all abstract types of groups of order ≤ 2000 without 1024.

If X is a finite set and G a finite group acting on X, then the *group action* is commonly a right operation and denoted as $\circ$ or without a symbol. For $x \in X$, the *orbit of x under G* is $xG = \{xg \mid g \in G\}$, the *stabilizer of x in G* is $\mathrm{Stab}_G(x) = \{g \in G \mid xg = x\}$, which is a subgroup of G, the *orbit space of X under G* is $X/G = \{xG \mid x \in X\}$, and a *transversal of X under G* is a subset T of X such that there is exactly one representative in T for each orbit in X/G.

22 Lemma (Orbit-Stabilizer theorem, [KS04, 3.1.5])
Let G be a finite group which operates on the finite set X. Then for any $x \in X$ we have $xG = (G : \mathrm{Stab}_G(x)) = \#G/\#\,\mathrm{Stab}_G(x)$. In particular the size of any orbit under G divides $\#G$.

There is a connection between conjugation and stabilizers.

23 Lemma ([KS04, 3.1.3])
Let G be a finite group which operates on the finite set X. Then for any $x \in X$ and $g \in G$ we have $\mathrm{Stab}_G(x)^g = \mathrm{Stab}_G(xg)$.

$x \in X$ is called *fixed under* G or *fixed point under* G, if $xG = \{x\}$ and any orbit of size $\#G$ is called *full-length*. A group operation is called *transitive*, if $X = xG$ for an arbitrary $x \in X$, which is only possible if $\#X \mid \#G$.

The *orbit type* of X/G is a string $1^{n_1}2^{n_2}\ldots$ such that there are n_i orbits of size i in X/G and we omit the cases with $n_i = 0$.

After prescribing a symmetry group $U \leq G$ some symmetry is given by the normalizer of U in G operating on the orbits.

24 Lemma
Let G be a group, X a set, and $f(x, g) = x \circ g$ for $x \in X$, $g \in G$ a right operation of G on X. Let $U \leq G$ be a subgroup. Then $N_G(U)$ operates on X/U via $F(xU, n) = xU \circ n = (xn)U = (x \circ n)U = f(x, n)U$ for $xU \in X/U$, $n \in N_G(U)$.

Proof
Let $xU = x'U \in X/U$, $n, n' \in N_G(U)$, and $e \in N_G(U)$ the trivial element. F is closed, since $F(xU, n) = xU \circ n = (xn)U \in X/U$. F is well-defined, since $xU = x'U \Leftrightarrow \exists u \in U : x' = x \circ u$ and $n \in N_G(U)$ implies the existence of $u' \in U$ with $un = nu'$, hence $F(xU, n) = xU \circ n = xnU = xnu'U = xunU = x'nU = x'U \circ n = F(x'U, n)$. The group operation properties of F are then induced by f: $F(xU, e) = f(x, e)U = xU$ and $F(xU, gh) = xU \circ gh = (xgh)U = f(x, gh)U = f(f(x, g), h)U = f(x, g)Uh = (xUg)h = F(F(xU, g), h)$, which concludes the proof. $\square$

Let G be a finite group and $H \leq G$ a subgroup. Analogously to [Rom12, Theorem 4.19], we consider the group operation $\varphi : G \to \mathcal{S}_{G/H}$ of G on the left cosets of H in G via left multiplication. Its kernel is $\ker(\varphi) = \{g \in G \mid g(aH) = aH\,\forall a \in G\} = \bigcap_{a\in G} H^a$, being the kernel of a group homomorphism, $\bigcap_{a\in G} H^a$ is normal, and for any normal subgroup $N \trianglelefteq G$ which is contained in H, we have $N = N^a \leq H^a$, i.e., $\bigcap_{a\in G} H^a$ is the largest normal subgroup in H. Hence, we define $H^\circ = \bigcap_{a\in G} H^a$, the *core* of H. Since the quotient group G/H° is embedded in $\mathcal{S}_{G/H}$ by the isomorphism theorem for groups, we get the following theorem.

25 Theorem (Strong Cayley theorem, cf. [Rom12, Theorem 4.20])
Let G be a finite group and $H \leq G$. Then $G/H^\circ \to \mathcal{S}_{G/H}$ is an injective group homomorphism and $(G : H^\circ) \mid (G : H)!$. If $\mathrm{GCD}(\#H, ((G : H) - 1)!) = 1$, then $H \trianglelefteq G$.

The condition $\mathrm{GCD}(\#H, ((G : H) - 1)!) = 1$ is fulfilled iff all primes p dividing $\#H$ are $\geq (G : H)$. This is in particular true if $(G : H)$ is the smallest prime dividing $\#G$:

26 Corollary
Let G be a finite group and p the smallest prime that divides $\#G$. Then any subgroup of G with index p is normal in G.

The choice of $H = \langle\rangle$, i.e., the identity group of G, in Theorem 25 implies the Cayley theorem (here in the finite case), cf. [Cay54], which states that any group G is isomorphic to a subgroup of $\mathcal{S}_G$.

Let L/K be a field extension. Then $\mathrm{Aut}(L)$ is the group of all automorphisms of L and $\mathrm{Aut}(L/K) = \{g \in \mathrm{Aut}(L) \mid g(k) = k \,\forall k \in K\}$ is the subset of automorphisms that fixes K element-wise.

Isometries and automorphisms An isometry of $\mathcal{L}(V)$, i.e., a distance-preserving map, ι of the metric space $(\mathcal{L}(V), \mathrm{d_s})$ maps $\mathcal{L}(V)$ to $\mathcal{L}(V)$ and fulfills $\mathrm{d_s}(U, W) = \mathrm{d_s}(\iota(U), \iota(W))$ for all $U, W \in \mathcal{L}(V)$.

Let β be a fixed non-degenerate symmetric bilinear form on V and $\pi : \mathcal{L}(V) \to \mathcal{L}(V), U \mapsto U^\perp = \{v \in V \mid \beta(v, u) = 0 \,\forall u \in U\}$, where $U^\perp$ denotes the orthogonal space of U with respect to β, see also [SK09, Remark after Lemma 1] for $\mathrm{d_s}(U^\perp, W^\perp) = \mathrm{d_s}(U, W)$.

Note that although the dimensions are complementary: $\dim(U) + \dim(U^\perp) = \dim(V)$, we have no complementary subspaces in general, e.g., $U = \langle u_1 + u_2\rangle$ has $U^\perp = \langle u_1 + u_2, u_3\rangle$ in $\mathbb{F}_2^3$ with the standard bilinear form $\beta(x, y) = x \cdot y^T = x_1y_1 + x_2y_2$.

Each element in the general linear group $\mathrm{GL}(V)$ induces an isometry on $(\mathcal{L}(V), \mathrm{d_s})$. For $M \in \mathrm{GL}(V)$ this map is $g_M : \mathcal{L}(V) \to \mathcal{L}(V)$ and $g_M(U) = \{u \cdot M \mid u \in U\}$, noting that V contains row vectors. Since two matrices that are scalar multiples, i.e., $M = \lambda M'$ for an $\lambda \in \mathbb{F}_q^*$, induce the same map $g_M = g'_M$[1], we factor the center of the group, $\mathrm{Z}(\mathrm{GL}(V)) = \{\lambda I_v \mid \lambda \in \mathbb{F}_q^*\}$, where I_v is the $v \times v$ identity matrix, out and get the projective linear group $\mathrm{PGL}(V) = \mathrm{GL}(V)/\mathrm{Z}(\mathrm{GL}(V))$.

[1]The maps are different if applied to vectors in V, but for subspaces of V both maps are equal.

Next, a field automorphism f also induces an isometry on $(\mathcal{L}(V), \mathrm{d_s})$, i.e., $f : \mathcal{L}(V) \to \mathcal{L}(V)$ and $f(U) = \{(f(u_1), \ldots, f(u_v)) \mid u \in U\}$, i.e., component-wise. All field automorphisms of $\mathbb{F}_{p^m}$ are multiple applications of the so-called Frobenius automorphism $x \mapsto x^p$, i.e., $x \mapsto x^{p^i}$ for $i = 0, \ldots, m-1$, cf. [Lan90, Theorem 2.4].

The semidirect product of both groups, $\mathrm{P\Gamma L}(\mathbb{F}_q^v) = \mathrm{PGL}(\mathbb{F}_q^v) \rtimes \mathrm{Aut}(\mathbb{F}_q)$, is known as the projective semilinear group.

For $3 \leq \dim(V)$ these are all isometries:

27 Theorem (cf. [HKK16b, Theorem 2.1], see also [Tra13c, Theorem 5])
For $3 \leq \dim(V)$, the automorphism group of $(\mathcal{L}(V), \mathrm{d_s})$ is $\langle \mathrm{P\Gamma L}(V), \pi \rangle \cong \mathrm{P\Gamma L}(V) \rtimes \langle \pi \rangle$.

The proof involves the *Fundamental Theorem of Projective Geometry* and this in turn imposes the restriction on the dimension.

For a prime p and integers $v \geq 1$ and $m \geq 1$:

$$\#\langle \mathrm{P\Gamma L}(\mathbb{F}_{p^m}^v), \pi \rangle = \# \mathrm{GL}(\mathbb{F}_{p^m}^v) \cdot 2m/(p^m - 1) = \prod_{i=0}^{v-1} (p^{vm} - p^{im}) \cdot 2m/(p^m - 1).$$

Hence, for a subspace $U \leq V$ and an automorphism $g = (M \cdot \mathrm{Z}(\mathrm{GL}(V)), \alpha) \in (\mathrm{GL}(V)/\mathrm{Z}(\mathrm{GL}(V)), \mathrm{Aut}(\mathbb{F}_q)) \cong \mathrm{P\Gamma L}(V)$ the operation is

$$Ug = U \circ g = \alpha(\tau^{-1}(\mathrm{RREF}(\tau(U) \cdot M))).$$

For classifications of subsets of $\begin{bmatrix} V \\ k \end{bmatrix}$ up to isomorphism, the acting group is $\mathrm{P\Gamma L}(V)$.

28 Example
Consider $\mathbb{F}_9 \cong \mathbb{F}_3(\alpha)$ with $\alpha^2 = 2$ and the usual scalar product $\beta(x, y) = xy$. Using $f(x) = x^3 \in \mathrm{Aut}(\mathbb{F}_9)$, I_3 as the 3×3 identity matrix, and id as the identity map, the operation of

$$\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_9^3)), f, \pi \right) \in \langle \mathrm{P\Gamma L}(\mathbb{F}_9^3), \pi \rangle \qquad \text{on} \qquad \langle (1, \alpha, 0) \rangle \in \mathcal{L}(\mathbb{F}_9^3)$$

can be computed:

$$\langle (1, \alpha, 0) \rangle \circ \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_9^3)), f, \pi \right) = \langle (1, 0, \alpha) \rangle \circ \left(I_3 \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_9^3)), f, \pi \right)$$
$$= \langle (1, 0, 2\alpha) \rangle \circ \left(I_3 \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_9^3)), \mathrm{id}, \pi \right) = \tau^{-1} \begin{pmatrix} 1 & 0 & 2\alpha \\ 0 & 1 & 0 \end{pmatrix} \circ \left(I_3 \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_9^3)), \mathrm{id}, \mathrm{id} \right) = \tau^{-1} \begin{pmatrix} 1 & 0 & 2\alpha \\ 0 & 1 & 0 \end{pmatrix}.$$

Subspace codes A subspace code C is a subset of $\mathcal{L}(V)$. In this context the elements of C are called codewords and V the ambient space on C. The so-called minimum (subspace) distance $\mathrm{D_s}(C)$ of C is the smallest distance between pairs of codewords, i.e., $\mathrm{D_s}(C) = \min\{\mathrm{d_s}(U,W) \mid U \neq W \in C\}$, the same is true for the minimum (injection) distance $\mathrm{D_i}(C)$. Another property is the dimension distribution $\delta(C)$ of C. $\delta(C)$ is a vector with $v+1$ non-negative integral entries $\delta(C) = (\delta_0, \delta_1, \ldots, \delta_v)$ such that δ_i is the number of i-dimensional subspaces in C, cf. [HKK16b]. Occasionally, $\delta(C)$ is abbreviated as a string $0^{n_0}1^{n_1}\ldots$ such that the number of contained i-dimensional codewords is n_i and entries with $n_i = 0$ are commonly omitted. $K(C) = \{\dim(U) \mid U \in C\} \subseteq \{0,1,\ldots,v\}$ is the set of dimensions for the codewords in C, i.e., $\delta_i = 0$ for all $i \in \{0,1,\ldots,v\} \setminus K(C)$.

An automorphism φ of a subspace code C is an isometry of $(\mathcal{L}(V), \mathrm{d_s})$ such that $\varphi(C) = C$, i.e., $\varphi(U) \in C$ for all $U \in C$. Using this, the automorphism group of C is $\mathrm{Aut}(C) = \{\varphi \in \langle \mathrm{P\Gamma L}(V), \pi\rangle \mid \varphi(C) = C\}$. A subgroup of $\mathrm{Aut}(C)$ is denoted as *an* automorphism group of C. If G is an automorphism group of C, then C is called G-invariant and the largest group G with the property that C is G-invariant is $\mathrm{Aut}(C)$. Moreover, C is called self-dual, if $\pi(C) = C^\perp = C$ and in particular $C^\perp = \pi(C) = \{U^\perp \mid U \in C\}$ is called the orthogonal code of C. Up to isomorphism of subspace codes, the code $C^\perp$ does not depend on the exact choice of the bilinear form β. Some literature denote $C^\perp$ as the dual of C.

For $q \geq 2$ prime power, non-negative integers v, M, d, $K \subseteq \{0,1,\ldots,v\}$, $\mathrm{x} \in \{\mathrm{s},\mathrm{i}\}$, and $U \leq \langle \mathrm{P\Gamma L}(\mathbb{F}_q^v), \pi\rangle$ a $(v,M,d;K;U)_q^{\mathrm{x}}$ *subspace code* is a subspace code $C \subseteq \mathcal{L}(\mathbb{F}_q^v)$ such that $\mathrm{D_x}(C) \geq d$, $K(C) \subseteq K$, $\#C = M$, and $U \leq \mathrm{Aut}(C)$. Note that although all v-dimensional $\mathbb{F}_q$-vector spaces are isomorphic, it is sometimes convenient to embed C in a non-standard ambient space.

The two extremal cases of K are commonly denoted as constant dimension code (CDC) if $K = \{k\}$, in this case we write the integer k instead of the set K in $(v,M,d;K;U)_q^{\mathrm{x}}$, and mixed dimension code (MDC) if $K = \{0,1,\ldots,v\}$ is unrestricted, and hence K is omitted in $(v,M,d;K;U)_q^{\mathrm{x}}$.

If $(v,M,d;K;U)_q^{\mathrm{x}}$ denotes a CDC, then $\mathrm{D_s}(C) = 2\mathrm{D_i}(C)$ and we always use $\mathrm{x} = \mathrm{s}$. Moreover, if x is omitted, then we assume the subspace distance, i.e., $\mathrm{x} = \mathrm{s}$, also in the general case.

If U is omitted, then we assume no restriction which defaults to U equals the identity in $\langle \mathrm{P\Gamma L}(\mathbb{F}_q^v), \pi\rangle$.

If C is a $(v,M,d;K)_q^{\mathrm{s}}$ subspace code, then $C^\perp$ is a $(v,M,d;v-K)_q^{\mathrm{s}}$ subspace code where $v - K = \{v-k \mid k \in K\}$.

The determination of the maximum size, or at least suitable bounds, of M for fixed $q, v, d, K, U, \mathrm{x}$ and the classification of maximum codes is known as the *main problem of subspace coding* since it forms a q-analogue of the *main problem of classical coding theory* (cf. [MS77a, Page 23]). In analogy to the classical block codes, we use the symbol $\mathrm{A}_q^{\mathrm{x}}(v,d;K;U)$ for the maximum cardinality of an $(v,M,d;K;U)_q^{\mathrm{x}}$ subspace code and the defaults of the parameters apply as well.

The numbers $\mathrm{A}_q(v,d;k)$ are known for a wide range of parameters. By definition, $\mathrm{A}_q(v,d;k) = 0$ for $k < 0$ or $v < k$ with the unique maximum code $C = \emptyset$. If $d \leq 2$, then

$\mathrm{A}_q(v,d;k) = \left[{v \atop k}\right]_q$ and $d = 2$ with the unique maximum code $C = \left[{V \atop k}\right]$. If $2k < d$, then for $U \neq W \in \left[{V \atop k}\right]$ we have $\mathrm{d_s}(U,W) = 2(k - \dim(U \cap W)) < d$, or if $2(v-k) < d$, then for $U \neq W \in \left[{V \atop k}\right]$ we have $\mathrm{d_s}(U,W) = 2(\dim(U+W) - k) < d$, and consequently any code with minimum distance greater than $\min\{2k, 2(v-k)\}$ has at most one element. In fact each subset of $\left[{V \atop k}\right]$ of cardinality one defines a maximum code, but they are all isomorphic in the $\mathrm{P\Gamma L}(\mathbb{F}_q^v)$.[2] Since π is an isometry, we have $\mathrm{A}_q(v,d;k) = \mathrm{A}_q(v,d;v-k)$, allowing the assumption $k \leq v-k$ without loss of generality. Any isomorphism class of CDCs of codeword dimension k corresponds to a unique isomorphism class of CDCs of codeword dimension $v-k$, which is only of interest for $3 \leq v$. Next, note that the subspace distance in the CDC case is always even. Therefore we occasionally use the assumption $2 \leq d/2 \leq k \leq v-k$ in the CDC case.

Also, the numbers $\mathrm{A}_q(v,d)$ are known for some parameters. If $v < d$, then $\mathrm{d_s}(U,W) = \dim(U+W) - \dim(U \cap W) \leq v < d$ implies that each code has at most one element. Moreover, each subset of $\mathcal{L}(V)$ of cardinality one defines a maximum code, but applying $\mathrm{GL}(V)$ and π, which are in the potentially unknown automorphism group, yields exactly one isomorphism class for each codeword dimension $k = 0, \ldots, \lfloor v/2 \rfloor$. If $d \leq 1$, then $\mathrm{A}_q(v,d) = \sum_{i=0}^{v} \left[{v \atop i}\right]_q$ with the unique maximum code $C = \mathcal{L}(V)$. Moreover, $\mathrm{A}_q(2,2) = q+1$ with the unique maximum code $C = \left[{V \atop 1}\right]$. The other maximal code is $C = \{\{0\}, V\}$ which is smaller than $q+1$ for all prime powers $q \geq 2$. Hence, we occasionally assume $2 \leq d \leq v$ and $3 \leq v$ in the MDC case with the subspace distance.

This settles the drawback of $3 \leq v$ in Theorem 27 in the context of the main problem of subspace coding for arbitrary $K \subseteq \{0,1,\ldots,v\}$.

More bounds and isomorphism types for subspace codes can be found e.g. in [HKK16b] and [HK18].

Note that for $U \neq W$ in a $(v, \#C, d; k)_q$ CDC C, the subspace distance yields $\dim(U \cap W) \leq k - d/2$. Therefore, any at least $(k-d/2+1)$-dimensional subspace of V is contained in at most one codeword.

By relaxing the restrictions on K, d or U and applying Lemma 23 we obtain the following connections.

29 Lemma
Let $q \geq 2$ be a prime power and $v, d, d' \in \mathbb{Z}$, $0 \leq v$, $K, K' \subseteq \{0,1,\ldots,v\}$, $U, U' \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$, $g \in \mathrm{P\Gamma L}(\mathbb{F}_q^v)$, and $\mathrm{x} \in \{\mathrm{s}, \mathrm{i}\}$. If $K \subseteq K'$, $d \geq d'$, or $U \geq U'$, then $\mathrm{A}_q^{\mathrm{x}}(v,d;K;U) \leq \mathrm{A}_q^{\mathrm{x}}(v,d';K';U')$. Moreover, we have $\mathrm{A}_q^{\mathrm{x}}(v,d;K;U^g) = \mathrm{A}_q^{\mathrm{x}}(v,d;K;U)$.

In Chapter 12 we prove $\mathrm{A}_2(8,6;4) = 257$ and use the following theorem.

[2] Although the exact automorphism group is unknown for $v \leq 2$, this statement solely uses the transitivity of $\mathrm{GL}(V)$, which is a subgroup of the automorphism group.

30 Theorem ([HKK16b, Theorem 3.3(i)])
If $v = 2k \geq 8$ is even, then $\mathrm{A}_q(v, v-2) = \mathrm{A}_q(v, v-2; k)$.

The online tables `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16] list numerical values of the known lower and upper bounds of the sizes of CDCs and MDCs.

Rank metric codes For matrices $M, N \in \mathbb{F}_q^{m\times n}$ where m and n are positive integers the rank distance is defined via $\mathrm{d_r}(M, N) = \mathrm{rk}(M - N)$, cf. [Gab85], which in turn yields the metric space $(\mathbb{F}_q^{m\times n}, \mathrm{d_r})$. A rank metric code C is a subset of $\mathbb{F}_q^{m\times n}$. Its minimum rank distance is the rank distance between pairs of distinct codewords or ∞ for rank metric codes of size at most one. The parameters of C with minimum rank distance d are commonly abbreviated as $(m \times n, \#C, d)_q$. If C is a subspace of $\mathbb{F}_q^{m\times n}$, then C is called *linear*, its cardinality is a power of q, and the parameters of C are denoted as $[m \times n, \log_q(\#C), d]_q$.

The maximum achievable size for rank-metric codes is known for all parameters by a Singleton-like argument. The concatenation of the maps $f : A \to B$ and $g : B \to C$ is denoted as $g \circ f : A \to C$.

31 Theorem (cf. [Gab85])
Let $1 \leq d \leq \min\{m, n\}$ be integers, q a prime power, and $C \subseteq \mathbb{F}_q^{m\times n}$ be a rank-metric code with minimum rank distance d. Then $\#C \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$.

Proof
Let wlog. $n \leq m$ (otherwise transpose), then the so-called puncturing

$$f_l : \begin{cases} \mathbb{F}_q^{m\times l} \to \mathbb{F}_q^{m\times(l-1)} \\ (M_{*,1}, M_{*,2}, \ldots, M_{*,l}) \mapsto (M_{*,1}, M_{*,2}, \ldots, M_{*,l-1}) \end{cases}$$

fulfills $\mathrm{d_r}(A, B) - \mathrm{d_r}(f_l(A), f_l(B)) \in \{0, 1\}$ for $A, B \in \mathbb{F}_q^{m\times l}$. Thus, $f = f_{n-d+2} \circ f_{n-d+3} \circ \ldots \circ f_n$ is injective, since the minimum rank distance is not zero: $\mathrm{d_r}(f(A), f(B)) \geq \mathrm{d_r}(A, B) - d + 1 \geq d - d + 1 = 1$. Hence, $\#f(C) = \#\{f(M) \mid M \in C\} \leq \#\mathbb{F}_q^{m\times(n-d+1)} = q^{m(n-d+1)}$. □

If $1 \leq \min\{m, n\} < d$, then only $\#C = 1$ is possible, which can be achieved by e.g. a zero matrix. Both bounds can be combined to give a single upper bound $\#C \leq \lceil q^{\max\{m,n\}(\min\{m,n\}-d+1)} \rceil$.

Rank metric codes attaining this upper bound are called maximum rank distance (MRD) codes. Linear MRD codes exist for all positive integral choices of the parameters

m, n, and d. The following construction for linear MRD codes was independently found in [Del78a; Gab85; Rot91]. They are called *Gabidulin MRD codes.*

Let wlog. $n \le m$ (otherwise transpose) and consider $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$. Then $C = \mathbb{F}_{q^m}^k \cdot M = \{u \cdot M \mid u \in \mathbb{F}_q^k\} \subseteq \mathbb{F}_{q^m}^n$ with

$$M = \begin{pmatrix} g_1^{q^0} & g_2^{q^0} & \cdots & g_n^{q^0} \\ g_1^{q^1} & g_2^{q^1} & \cdots & g_n^{q^1} \\ & & \vdots & \\ g_1^{q^{k-1}} & g_2^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times n}$$

is via the isomorphism $\mathbb{F}_{q^m}^n \cong \mathbb{F}_q^{m \times n}$ the $[m \times n, mk, d]_q$ Gabidulin MRD code ($d = n-k+1$), cf. [HM17, Definition 2.4].

A survey of general constructions and properties of MRD codes can be found in [GR18; OÖ18].

Moreover, for consistency, we allow $m = 0$ or $n = 0$ with $C = \emptyset$, and $d = 1$ with $C = \mathbb{F}_q^{m \times n}$.

In the context of $(m \times n, \#C, d)_q$ rank metric codes, we often use the lifting map

$$\Lambda_{q,m,n} \colon \mathbb{F}_q^{m \times n} \to \begin{bmatrix} \mathbb{F}_q^{m+n} \\ m \end{bmatrix}, M \mapsto \tau^{-1}(I_m \mid M).$$

If the parameterization of $\Lambda_{q,m,n}$ is clear from the context, we abbreviate this symbol with Λ. The $m \times n$-matrix consisting entirely of zeros is denoted as $\mathbf{0}_{m \times n}$ or simply $\mathbf{0}$ if the dimension is obvious. Λ is injective and its image is given by all m-subspaces of $\mathbb{F}_q^{m+n}$ having trivial intersection with the special subspace $S = \tau^{-1}(\mathbf{0}_{n \times m} \mid I_n) \le \mathbb{F}_q^{m+n}$. In fact, Λ is an isometry $(\mathbb{F}_q^{m \times n}, 2\mathrm{d}_\mathrm{r}) \to (\mathbb{F}_q^{m+n}, \mathrm{d}_\mathrm{s})$. Of particular interest are the LMRD codes, which are CDCs of fairly large, though not maximum size, cf. Chapter 4.

Further notation and statements Successive zeros and ones are abbreviated:

$$1_l = \underbrace{1 \ldots 1}_{l} \quad \text{and} \quad 0_l = \underbrace{0 \ldots 0}_{l}.$$

$\mathcal{S}_X$ is the symmetric group of the set X and $\mathcal{S}_n = \mathcal{S}_{[n]}$.

The horizontal concatenation of two matrices A and B having the same number of rows is denoted as $A \mid B$.

If $b < a$ then we assume $\{a, a+1, \ldots, b\} = \emptyset$.

For a matrix A and vectors x and b of suitable dimension, $Ax \le b$ is defined as $A_{i,*}x \le b_i$ for all i.

For a set X the set of all unordered pairs of X is called $\binom{X}{2} = \{\{x, y\} \in X \times X \mid x \ne y\}$.

We will call two subspaces $A, B \le V$ *disjoint*, if their intersection has dimension zero.

If U is a subspace of W, we write $U \le W$, if H is subgroup of G, we also write $H \le G$.

The greatest common divisor is called GCD.

$\mathbb{1}_\varphi \in \{0, 1\}$ which is 1 iff φ is true is called *indicator function* and given a set S we call $\mathbb{1}_S(x) \in \{0, 1\}$ with $\mathbb{1}_S(x) = 1 \Leftrightarrow x \in S$ *characteristic function* of S.

For a set X the powerset is $2^X = \{A \subseteq X\}$.

A set of at least three points is called *collinear* if there is a line containing all points and four points in a plane such that no three of them are collinear form a *quadrangle*, cf. [Cox74].

Splitting a large problem into multiple subproblems may be an advantage depending on the situation.

32 Lemma

Let X be a finite set and $f : 2^X \to \{0,1\}$ be a function. A bijection $\pi : X \to X$ is called an automorphism (with respect to f) if $f(S) = f(\pi(S))$ for all $S \subseteq X$. Let Γ be a group of automorphisms, $T = \{t_1, \ldots, t_m\}$ be a transversal of Γ acting on X, where the corresponding orbit sizes are in decreasing ordering, and $\tau : X \to \{1, \ldots, m\}$ such that $x \in X$ is in the same orbit as $t_{\tau(x)}$. If $\tilde{S} \subseteq X$ and $i = \min\{\tau(x) \mid x \in \tilde{S}\}$, then there exists an automorphism $\gamma \in \Gamma$ with $t_i \in \gamma(\tilde{S})$, $f(\tilde{S}) = f(\gamma(\tilde{S}))$, and $\min\{\tau(x) \mid x \in \gamma(\tilde{S})\} = i$.

Proof

Choose $x \in \tilde{S}$ with $\tau(x) = i$ and $\gamma \in \Gamma$ with $\gamma(x) = t_i$. Note that $\tau(\gamma'(x')) = \tau(x')$ for all $\gamma' \in \Gamma$ and all $x' \in X$. □

In general, we label the elements of T in decreasing size of the corresponding orbit lengths, since large orbits admit small stabilizers and forbid many elements from X in the subsequent subproblems, i.e., we get few rather asymmetrical large subproblems and many small subproblems.

33 Lemma (Bézout's identity, [JJ98, Theorem 1.7 and 1.8])

Let $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$, then there are $s, t \in \mathbb{Z}$ with $as + bt = \mathrm{GCD}(a, b)$. Moreover, $\mathrm{GCD}(a, b) \mid as' + bt'$ for all $s', t' \in \mathbb{Z}$.

Linear programming See e.g. [BK92; DT03; DT97]. The underlying set for linear programming is a *polyhedron*, i.e., $P(A, b) = \{x \in \mathbb{R}^n \mid Ax \leq b\}$ for an $A \in \mathbb{R}^{m \times n}$ and $b \in \mathbb{R}^m$ and column vectors x, it is easy to observe that $P(A, b)$ is convex. Its *dimension* $\dim(P(A, b))$ is the maximum number of affinely independent[3] vectors in $P(A, b)$ minus one. If $\dim(P(A, b)) = n$ then the polyhedron is called *full-dimensional* and if it is bounded it is called *polytope*. A polyhedron $P(A, b)$ is a *formulation* for $X \subseteq \mathbb{Z}^n$ if $X = P(A, b) \cap \mathbb{Z}^n$. For two formulations $P(A, b)$ and $P(A', b')$ of X, $P(A, b)$ is called *better* than $P(A', b')$ if $P(A, b) \subsetneq P(A', b')$ and it is called *optimal* if $P(A, b) = \mathrm{conv}(X)$, i.e., the convex hull of X. An inequality $s^T x \leq t$ is called *valid* for $P(A, b)$ if $P(A, b) \subseteq \{x \in \mathbb{R}^n \mid s^T x \leq t\}$. For a valid inequality $s^T x \leq t$ of $P(A, b)$ the set $F = \{x \in P(A, b) \mid s^T x = t\}$ is called

[3]The vectors $\{x_1, \ldots, x_l\}$ are affinely independent iff $\{x_2 - x_1, \ldots, x_l - x_1\}$ is linearly independent.

face of $P(A, b)$. Although $\emptyset$ and $P(A, b)$ are faces, any face that is neither $\emptyset$ nor $P(A, b)$ is called *proper face*. Faces are polyhedrons and *facets* F are faces of $P(A, b)$ with $\dim(P(A, b)) = \dim(F) + 1$. Hence, facets are faces that are not contained in another proper faces.

A theoretically important polyhedron is the stable set polytope [PS93]. For an undirected, connected, and simple graph $G = (V, E)$ the stable set polytope is

$$\mathrm{Stab}(G) = \mathrm{conv}(\{x \in \{0, 1\}^{\#V} \mid x_a + x_b \leq 1 \ \forall \{a, b\} \in E\}).$$

The set of constraints $x_a + x_b \leq 1 \ \forall \{a, b\} \in E$ is called *edge constraints*. This polytope is full-dimensional since $\emptyset$ and any subset of V of cardinality one is an independent set, yielding $\#V + 1$ affine independent points contained in the polytope. Any clique $L \subseteq V$ implies a valid inequality $\sum_{a \in L} x_a \leq 1$ for $\mathrm{Stab}(G)$ which is a facet iff L is maximal with respect to inclusion. These constraints are called *clique constraints*.

The *LP-relaxation* of the variable $x \in [a, b] \cap \mathbb{Z}$ is $x \in [\lceil a \rceil, \lfloor b \rfloor]$. If all integral variables are exchanged to their corresponding LP-relaxed counterparts, then an integer linear program is called *LP-relaxed*.

Subspace designs and q-Steiner systems See e.g. [BKW18a; BKW18b] for the notation of this paragraph.

Let $q \geq 2$ be a prime power and $0 \leq t \leq k \leq v$ and $0 \leq \lambda$ integers. A pair (V, B) is called $t - (v, k, \lambda)_q$ *subspace design*, if B is a multiset of k-subspaces of $V = \mathbb{F}_q^v$, the elements of B are called *blocks*, and each t-subspace of $\mathbb{F}_q^v$ is contained in exactly λ blocks. The design is called *simple*, if B is a set.

If the condition "contained in exactly λ blocks" of the definition of a subspace design is changed to "contained in at most λ blocks" then it is called *subspace packing design* and if it is changed to "contained in at least λ blocks", it is known as *subspace covering design*.

Hence, subspace packing designs with $\lambda = 1$ are CDCs and vice versa.

A simple $t - (v, k, 1)_q$ design is also known as *q-Steiner system* and abbreviated as $S(t, k, v)_q$. Therefore, any $S(t, k, v)_q$ q-Steiner system is a $\left(v, \left[\begin{smallmatrix} v \\ t \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} k \\ t \end{smallmatrix}\right]_q, 2(k - t + 1); k\right)_q$ CDC and vice versa. Any $S(t, k, v)_q$ q-Steiner system attains the Anticode bound, cf. Theorem 107, i.e., it is a maximum CDC. Next to the trivial cases with $t = k$ ($S = \left[\begin{smallmatrix} \mathbb{F}_q^v \\ k \end{smallmatrix}\right]$) and $k = v$ ($S = \{\mathbb{F}_q^v\}$) and the spreads (see below) with $t = 1$, only one additional set of parameters of a q-Steiner system is known: $S(2, 3, 13)_2$, cf. [Bra+16].

The smallest non-resolved q-Steiner system would have the parameters $S(2, 3, 7)_2$, i.e., it would be a $(7, 381, 4; 3)_2$ CDC. The corresponding structure in the set case is the well-known Fano plane, cf. Figure 5, which has 7 points and 7 blocks, each block consists of 3 points such that any two blocks meet in exactly 1 point.

Vector space partitions, (partial) spreads, parallelisms Closely related structures to subspace codes are vector space partitions, partial spreads, and spreads, which are used to build parallelisms.

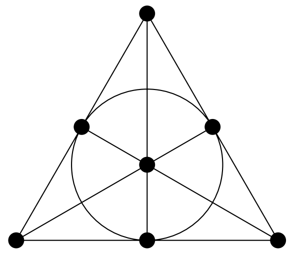


Figure 5: The Fano plane.

A *vector space partition* of V is a subset $P \subseteq \mathcal{L}(V) \setminus \{\{0\}\}$ such that any non-zero vector in V is contained in exactly one element of P, cf. [Hed12]. P is said to be of type $v^{n_v}(v-1)^{n_{v-1}} \ldots 1^{n_1}$ if P contains exactly n_i subspaces of dimension i, where entries with $n_i = 0$ are commonly omitted. One-dimensional elements of P are called *holes*. Each covering of non-zero vectors, i.e., a subset of $\mathcal{L}(V)$ such that a non-zero vector is contained at most one time, can trivially be extended to a vector space partition by adding the non-covered points, i.e., one-dimensional subspaces, cf. Table 3. Although the intersection of any pair $U \neq W$ of elements of P is zero-dimensional and therefore we have $\mathrm{d_s}(U,W) = \dim(U+W) = \dim(U) + \dim(W)$, the minimum subspace distance of P considered as MDC can be as low as two, e.g. if P contains two points. On the other hand, the minimum distance $d = v$ restricts an MDC to only contain subspaces with pairwise trivial intersection and therefore such an MDC can be extended to a vector space partition.

A *partial k-spread* in V is a subset $S \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ such that each non-zero vector is contained in at most one element in S. Therefore, S can be extended in a unique way to a $k^{\#S}1^{n_1}$ vector space partition with $n_1 = \begin{bmatrix} v \\ 1 \end{bmatrix}_q - \begin{bmatrix} k \\ 1 \end{bmatrix}_q \#S = (q^v - 1 - (q^k-1)\#S)/(q-1)$. Since $\mathrm{d_s}(U,W) = 2k$ for $U \neq W \in S$, S is also a $(v, \#S, 2k; k)_q$ CDC. A special case is given if S is already a vector space partition, i.e., all non-zero vectors of V are partitioned into subspaces in S. In this case, S is called *spread* and has $\begin{bmatrix} v \\ 1 \end{bmatrix}_q / \begin{bmatrix} k \\ 1 \end{bmatrix}_q = (q^v-1)/(q^k-1)$ elements. Spreads are known to exist iff $k \mid v$ (cf. Theorem 124), i.e., $\mathrm{A}_q(v, 2k; k) = (q^v-1)/(q^k-1)$ if $k \mid v$.

On the one hand, writing $v = lk + r$ with $0 \le r < k$, we have $q^v - 1 \equiv q^r - 1 \pmod{q^k-1}$ which is $0 \pmod{q^k-1}$ iff $r = 0$. On the other hand, $S = \begin{bmatrix} \mathbb{F}_{q^k}^{v/k} \\ 1 \end{bmatrix}$ is a spread, the so-called *Desarguesian spread*, in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$, since $\#S = ((q^k)^{v/k}-1)/(q^k-1) = (q^v-1)/(q^k-1)$, the elements of S intersect only trivially, any element $U \in S$ has q^k vectors, and using $U = \langle u \rangle = \{\alpha u \mid \alpha \in \mathbb{F}_{q^k}\}$, U is $\mathbb{F}_{q^k}$-linear, and in particular $\mathbb{F}_q$-linear. As observed in [Tra13c, Theorem 10], different Desarguesian spreads arise through different isomorphisms between $\mathbb{F}_{q^k}^{v/k}$ and $\mathbb{F}_q^v$, but all of them are linear maps and therefore the linear maps between these isomorphisms show that all Desarguesian spreads are isomorphic, which allows to speak of *the* Desarguesian spread for given parameters.

Bounds on partial spreads may be found in Section 7.1.

For an arbitrary set X, a *packing* Q of X is a set of subsets of X such that each pair of elements of Q is pairwise disjoint. Using this definition, a *parallelism* in $\begin{bmatrix} V \\ k \end{bmatrix}$ is a packing of the power set of $\begin{bmatrix} V \\ k \end{bmatrix}$ that consists entirely of spreads. Parallelisms in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ are known to exist, cf. [ES16], in the following cases:

- $q = 2$, $v \geq 4$ even, and $k = 2$,
- all q, $v = 2^m$ for $m \geq 2$, and $k = 2$,
- $q \equiv 2 \pmod 3$, $v = 4$, and $k = 2$,
- $q = 3$, $v = 6$, and $k = 2$, or
- $q = 2$, $v = 6$, and $k = 3$.

Block Codes The Hamming distance is defined as $\mathrm{d_h}(u, w) = \#\{i \in \{1, 2, \ldots, v\} \mid u_i \neq w_i\}$ for $u, w \in \mathbb{F}^v$, where $\mathbb{F}$ is a field. A *block code* C is a subset of $\mathbb{F}_q^v$. If its minimum distance, i.e., the minimum Hamming distance of pairs of C, is lower bounded by d, then C is called $(v, \#C, d)_q$ block code and if additionally C is a linear subspace of $\mathbb{F}_q^v$ of dimension k, then its parameters are denoted with $[v, k, d]_q$. To dissociate the usage of block codes from subspace codes, we will indicate their appearance by the term block code. The weight of u, $w(u) = \mathrm{d_h}(u, \mathbf{0})$, is the number of non-zero entries of $u \in \mathbb{F}_q^v$. A special case is given, if each element of C has the same weight, in which case the block code is called *constant weight code*.

Graphs and Cliques If $G = (V, E)$ is an undirected, connected, and simple graph and $w : V \to \mathbb{Z}_{\geq 1}$ are weights, then we call the tuple (G, w) *weighted graph*. For $S \subseteq V$ is $G|_S$ the *induced subgraph*. A *clique* C in G is a subset of V such that $G|_C$ is a complete graph and a *maximum weight clique* in (G, w) is a clique C with $w(C) \geq w(C')$ for any clique C' of G. We abbreviate $w(S) = \sum_{v \in S} w(v)$ for $S \subseteq V$. With $\omega(G, w) := \max\{w(C) \mid C \text{ clique in } (G, w)\}$ we denote the *clique number* in (G, w). If $w(v) = 1$ for all $v \in V$ we omit the reference to w and $w(S) = \#S$ for $S \subseteq V$. We refer to $\omega(G, w)$ with $w(v) = 1$ for all $v \in V$ with the term *unweighted clique number* $\omega(G)$.

For a map $f : A \to B$ and $b \in B$ the map $(f/b) : A \to B$ is defined via $(f/b)(a) = f(a)/b$ for all $a \in A$.

The following lemma allows to find substructures of maximum cliques, provided that the weights are exponential.

34 Lemma
Let $G = (V, E)$ be a graph with weights $w : V \to \mathbb{Z}_{\geq 1}$.

1. If there is a map $W : V \to \mathbb{Z}_{\geq 0}$ and integers $c \geq 1$ and $T \geq 0$ with $w(v) = c^{W(v)}$ for all $v \in V$ and $t = c^T$, $Z = \{v \in V \mid t \leq w(v)\}$, $Y = V \setminus Z$, $\omega(G|_Y, w|_Y) < t$, and C is a maximum weight clique in (G, w), then $C \cap Z$ is a maximum weight clique in $(G|_Z, w|_Z)$.

2. If $A, B \subseteq V$ with $V = A \cup B$ (not necessarily a partition) then $\omega(G, w) \leq \omega(G|_A, w|_A) + \omega(G|_B, w|_B) \leq w(A) + \omega(G|_B, w|_B)$.

3. If there is a map $W : V \to \mathbb{Z}_{\geq 0}$ and integers $c \geq 1$ and $0 \leq L \leq T$ with $w(v) = c^{W(v)}$ for all $v \in V$, $t = c^T$, and $l = c^L$, $V(i,j) = \{v \in V \mid i \leq w(v) < j\}$ for $1 \leq i < j$, $\omega(G|_{V(l,t)}, w|_{V(l,t)}/l) < t/l - \#V/c$, and C is a maximum weight clique in (G, w), then $C \cap V(t, \infty)$ is a maximum weight clique in $(G|_{V(t,\infty)}, w|_{V(t,\infty)})$.

Proof

1. If $C \cap Z$ is no maximum weight clique in $(G|_Z, w|_Z)$ then there is a clique C' in $(G|_Z, w|_Z)$ with

$$\begin{aligned} & w(C \cap Z) < w(C') \Leftrightarrow \sum_{v \in C \cap Z} c^{W(v)-T} < \sum_{v \in C'} c^{W(v)-T} \\ & \Leftrightarrow \sum_{v \in C \cap Z} c^{W(v)-T} + 1 \leq \sum_{v \in C'} c^{W(v)-T} \Leftrightarrow \sum_{v \in C \cap Z} c^{W(v)} + c^T \leq \sum_{v \in C'} c^{W(v)} \\ & \Leftrightarrow w(C \cap Z) + t \leq w(C'). \end{aligned}$$

   Consequently, $w(C) - w(C \cap Z) = w(C \cap Y) \leq \omega(G|_Y, w|_Y) < t \leq w(C') - w(C \cap Z)$ proofs that C is no maximum weight clique in (G, w), a contradiction.

2. Let C be a maximum weight clique in (G, w), then $\omega(G, w) = w(C) \leq w(C \cap A) + w(C \cap B) \leq \omega(G|_A, w|_A) + \omega(G|_B, w|_B)$. The last inequality follows from the definition of cliques.

3. We have $\max\{w(v) \mid v \in V(1, l)\} \leq l/c$ since $w(v) < l \Leftrightarrow c^{W(v)} < c^L \Leftrightarrow c^{W(v)} \leq c^{L-1} \Leftrightarrow w(v) \leq l/c$ for any $v \in V(1, l)$.

   By $\omega(G|_{V(l,t)}, w|_{V(l,t)}/l) \cdot l = \omega(G|_{V(l,t)}, w|_{V(l,t)})$, the application of (2) yields

$$\begin{aligned} & \omega(G|_{V(1,t)}, w|_{V(1,t)}) \leq \omega(G|_{V(1,l)}, w|_{V(1,l)}) + \omega(G|_{V(l,t)}, w|_{V(l,t)}) \\ & \leq w(V(1,l)) + \omega(G|_{V(l,t)}, w|_{V(l,t)}/l)l < \#V(1,l)l/c + (t/l - \#V/c)l \\ & \leq \#V c^{L-1} + (c^{T-L} - \#V/c)c^L = c^T = t \end{aligned}$$

   which in turn shows that the preconditions of (1) are fulfilled. □

Matroids and their connection to the Greedy Algorithm In each iteration, the greedy algorithm (Algorithm 1) takes the next best element and does not backtrack to find better solutions. Usually this leads to solutions which are arbitrarily far away from an optimal value, but the structures on which this algorithm yields the optimal solution are characterized.

35 Definition ([Pit14, Definition 3.1 and 3.5])
Let X be a finite set and $I \subseteq 2^X$, then (X, I) is called *independence system* iff

1. $\emptyset \in I$ and
2. if $U \in I$ and $W \subseteq U$, then $W \in I$.

If additionally

3. if $U, W \in I$ and $\#W < \#U$ then there is a $u \in U \setminus W$ such that $W \cup \{u\} \in I$,

then (X, I) is called *matroid*. The sets in I are called *independent*. A *basis* of an independence system is a maximal independent set.

Let $w : X \to \mathbb{R}$ be a function and $w(U) = \sum_{u \in U} w(u)$ for all $U \subseteq X$. This function will be interpreted as objective function of a maximization problem.

Algorithm 1 Greedy algorithm using an independence system, cf. [Pit14, Algorithm 3.1].

Require: (X, I) is an independence system, $w : X \to \mathbb{R}$
procedure GREEDY($(X, I), w$)
    Sort X such that we assume $w(x_1) \geq w(x_2) \geq \ldots \geq w(x_{\#X})$
    $R \leftarrow \emptyset$
    for $i = 1, \ldots, \#X$ **do**
        if $R \cup \{x_i\} \in I$ **then**
            $R \leftarrow R \cup \{x_i\}$
        end if
    end for
    return R
end procedure

36 Theorem ([Pit14, Definition 3.11])
Let (X, I) be an independence system and B the set of all bases. Then (X, I) is a matroid iff the output of Greedy (Algorithm 1) is optimal for $\max\{w(U) \mid U \in B\}$.

A well-known example is the minimum spanning tree of a undirected, connected, and simple graph.

37 Example ([Pit14, Page 38f])
Let $G = (V, E)$ be a connected, undirected, and simple graph. Then with $X = V$, $I = \{U \subseteq V \mid U \text{ contains no cycle}\}$ we have a matroid (X, I) ([Pit14, Proposition 2.3])

and for any $w : X \to \mathbb{R}$ a maximal cycle free subset of V for that w attains its maximum can be computed by Algorithm 1.

Association schemes and Delsarte's linear programming bound This paragraph uses mainly the notation of [BCN89, Chapter 2] with some influences of [MS77b, Chapter 21].

An association scheme is simply a finite set on which multiple relations are defined simultaneously.

38 Definition ([BCN89, Chapter 2.1] and [MS77b, Chapter 21.2])
Let X be a finite set of size n. An *association scheme with d classes* is a pair $(X, \{R_0, R_1, \ldots, R_d\})$ such that

1. $\{R_0, R_1, \ldots, R_d\}$ is a partition of X^2,
2. $R_0 = \{(x, x) \mid x \in X\}$,
3. $(x, y) \in R_i \Rightarrow (y, x) \in R_i$ for all $i \in \{0, 1, \ldots, d\}$, and
4. there are p_{ij}^k with $p_{ij}^k = \#\{z \in X \mid (x, z) \in R_i \wedge (z, y) \in R_j\}$ for all $(x, y) \in R_k$.

The numbers p_{ij}^k are called *intersection numbers* of the scheme and $n_i = p_{ii}^0$ is called *valency* of R_i.

Clearly, we have $n_0 = 1$ and $n = \#X = \sum_{i=0}^d n_i$.

An association scheme may be interpreted as complete, undirected graph with loops, such that any edge $\{x, y\}$ is labeled with the weight i where i is the index of the relation R_i with $(x, y) \in R_i$. Due to the partition there is exactly one such relation. Then, p_{ij}^k may be interpreted as the number of vertices with distance i to x and distance j to y, where x and y are some vertices with distance k.

Using the adjacency matrix $A_i \in \{0, 1\}^{n \times n}$ of the relation R_i with $(A_i)_{x,y} = 1$ iff $(x, y) \in R_i$, the $n \times n$ identity matrix I, and the $n \times n$ all-one matrix J, the four properties in Definition 38 translate to:

1. $\sum_{i=0}^d A_i = J$,
2. $A_0 = I$,
3. $A_i = A_i^T$ for all $i \in \{0, 1, \ldots, d\}$, and
4. $A_i A_j = \sum_{k=0}^d p_{ij}^k A_k$ for all $i, j \in \{0, 1, \ldots, d\}$.

The subspace $\mathcal{A} = \langle A_0, A_1, \ldots, A_d \rangle_{\mathbb{R}} \leq \mathbb{R}^{n \times n}$ is called *Bose-Mesner algebra*. It has dimension $d+1$, since the A_i are linearly independent, consists of symmetric matrices, and any two matrices in $\mathcal{A}$ commute, since $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k = \sum_{k=0}^{d} p_{ji}^k A_k = A_j A_i$.

Since the A_i are symmetric and commute, they can be diagonalized simultaneously (cf. [Gan59, Chapter 9.15]), i.e., there is an $S \in \mathbb{R}^{n \times n}$ such that $S^{-1} A_i S$ is a diagonal matrix for all $i \in \{0, 1, \ldots, d\}$ and the $\mathbb{R}^{n \times n}$ can be decomposed into $d+1$ eigenspaces with dimension f_i ($i \in \{0, 1, \ldots, d\}$). These f_i are called *multiplicities* of the association scheme. Therefore, $\mathcal{A}$ is semisimple and has a unique basis of primitive idempotents $\{E_0, E_1, \ldots, E_d\}$, $f_i = \operatorname{rk}(E_i)$, in which wlog. $E_0 = n^{-1} J$ and hence $f_0 = 1$. They fulfill $E_i^2 = E_i$ ($i \in \{0, 1, \ldots, d\}$), $E_i E_j = \mathbf{0}_{n \times n}$ ($i \neq j \in \{0, 1, \ldots, d\}$), and $\sum_{i=0}^{d} E_i = I$.

Hence, the unique matrices $P \in \mathbb{R}^{n \times n}$ and $n^{-1} Q \in \mathbb{R}^{n \times n}$ map one basis to another, i.e., $A_j = \sum_{i=0}^{d} P_{ij} E_i$ and $E_j = n^{-1} \sum_{i=0}^{d} Q_{ij} A_i$. P and Q are called *eigenmatrices* of the association scheme, since $A_j E_i = P_{ij} E_i$.

Let $Y \subseteq X$ and $\mathbb{1}_Y$ be its characteristic row vector. The *outer distribution of* Y is the matrix $B \in \mathbb{Z}^{n \times (d+1)}$ with $B_{xi} = (A_i \mathbb{1}_Y^T)_x = \#\{y \in Y \mid (x, y) \in R_i\}$. The *inner distribution of* Y is the vector $a = (\#Y)^{-1} \mathbb{1}_Y B \in \mathbb{Q}^{d+1}$, i.e., $a_i = (\#Y)^{-1} \mathbb{1}_Y A_i \mathbb{1}_Y^T = (\#Y)^{-1} \#(R_i \cap Y^2)$. Clearly, we have $a_0 = 1$, $\sum_{i=0}^{d} a_i = \#Y$, $a \geq 0$, and $B \geq 0$.

The next theorem is due to Delsarte.

39 **Theorem ([BCN89, Proposition 2.5.2], [MS77b, Chapter 21.7, Theorem 12])**
Let $(X, \{R_0, R_1, \ldots, R_d\})$ be an association scheme, $Y \subseteq X$ be non-empty and a, B the inner and outer distribution of Y. Then $aQ \geq 0$ and if $(aQ)_j = 0$ then $(BQ)_{xj} = 0$ for all $x \in X$.

The linear programming method uses the linear program

$$\max \left\{ \sum_{i=0}^{d} a_i \;\middle|\; a_0 = 1 \wedge aQ \geq 0 \wedge a \geq 0 \wedge a \in \mathbb{Q}^{d+1} \right\}$$

with additional and situation dependent constraints to upper bound the size of any subset of the association scheme fulfilling these situation dependent constraints.

Delsarte's generalization of the Anticode bound is:

40 **Theorem ([BCN89, Proposition 2.5.3])**
Let $(X, \{R_0, R_1, \ldots, R_d\})$ be an association scheme, $Y, Z \subseteq X$ both non-empty, and a_Y, a_Z be the inner distributions of Y and Z, respectively. If $I_Y \dot\cup I_Z$ is a partition of $\{1, 2, \ldots, d\}$, $(a_Y)_i = 0$ for all $i \in I_Y$, and $(a_Z)_i = 0$ for all $i \in I_Z$, then $\#Y \cdot \#Z \leq \#X$ and equality holds iff for all $i \in \{1, 2, \ldots, d\}$ we have $(a_Y Q)_i = 0$ or $(a_Z Q)_i = 0$.

An association scheme $(X, \{R_0, R_1, \ldots, R_d\})$ with an ordering of its relations is called *metric*, if $p_{ij}^k \neq 0 \Rightarrow k \leq i + j$ and $p_{ij}^{i+j} \neq 0$ for all $i, j, k \in \{0, 1, \ldots, d\}$, cf. [BCN89, Chapter 2.7] and [MS77b, Chapter 21.4].

If $(X, \{R_0, R_1, \dots, R_d\})$ is a metric association scheme, then (X, R_1) is a distance-regular graph and $x, y \in X$ have distance i in the graph iff $(x, y) \in R_i$. Conversely, if $G = (V, E)$ is a distance-regular graph of diameter l, then $(V, \{R_0, R_1, \dots, R_l\})$ with $(x, y) \in R_i$ iff x and y have distance i in the graph.

The *q-Johnson scheme* is the metric association scheme of the Grassmann graph. Its parameters are computed in [Del76a, Theorem 10], [Del78b] [Del76b, Page 269], cf. [ZJX11]:

- $n_i = q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} v-k \\ i \end{bmatrix}_q$,
- $f_i = \begin{bmatrix} v \\ i \end{bmatrix}_q - \begin{bmatrix} v \\ i-1 \end{bmatrix}_q$,
- $P_{ji} = \sum_{m=0}^{i} (-1)^{i-m} q^{\binom{i-m}{2}+jm} \begin{bmatrix} k-m \\ k-i \end{bmatrix}_q \begin{bmatrix} k-j \\ m \end{bmatrix}_q \begin{bmatrix} v-k-j+m \\ m \end{bmatrix}_q$, and
- $Q_{ij} = \frac{f_j}{n_i} P_{ji}$.

$P_{ji} = P_i(j)$ is a q-Hahn polynomial [BPV13; Del78b].

3 Structure of subspaces in a vector space

In order to describe some structural properties of a CDC and to give bounds, we will consider incidences with fixed subspaces. Therefore, let $V = \mathbb{F}_q^v$ and $\mathcal{I}(S, X)$ be the set of subspaces in $S \subseteq \mathcal{L}(V)$ that are incident to $X \in \mathcal{L}(V)$, i.e.,

$$\mathcal{I}(S, X) = \{U \in S \mid U \leq X\} \cup \{U \in S \mid X \leq U\}.$$

41 Lemma
Let C be a $(v, \#C, d; k)_q$ CDC and $X \leq V$. Then we have

$$\#\mathcal{I}(C, X) \leq \begin{cases} \mathrm{A}_q(\dim(X), d; k) & \text{if } \dim(X) \geq k, \\ \mathrm{A}_q(v - \dim(X), d; k - \dim(X)) & \text{if } \dim(X) < k. \end{cases}$$

Proof
If $\dim(X) \geq k$, then $\mathcal{I}(C, X)$ is a $(\dim(X), \#\mathcal{I}(C, X), d; k)_q$ CDC and hence its cardinality is bounded by $\mathrm{A}_q(\dim(X), d; k)$. If $\dim(X) < k$, then we write $V = X \oplus V'$ and $U_i = X \oplus U_i'$ for all $U_i \in \mathcal{I}(C, X)$. With this, we have $\mathrm{d_s}(U_i, U_j) = 2k - 2\dim(U_i \cap U_j) \leq 2(k - \dim(X)) - 2\dim(U_i' \cap U_j') = \mathrm{d_s}(U_i', U_j')$ and hence $\{U_i' \mid U_i \in \mathcal{I}(C, X)\}$ is a $(v - \dim(X), \#\mathcal{I}(C, X), d'; k)_q$ CDC with $d \leq d'$. □

In general we have no equality in the inequality $\mathrm{d_s}(U_i, U_j) \leq \mathrm{d_s}(U_i', U_j')$ in the proof: For the unit vectors u_1 and u_2 and $A = \langle u_1 \rangle$, $B = \langle u_2 \rangle$, and $X = \langle u_1 + u_2 \rangle$ the subspace $\langle u_1 + u_2 \rangle = (A \cap B) \oplus X < (A \oplus X) \cap (B \oplus X) = \langle u_1, u_2 \rangle$ is proper.

If $\#\mathcal{I}(C, X)$ is small, then we can state the following upper bound on $\#C$:

42 Lemma
Let C be a $(v, \#C, d; k)_q$ CDC and $0 \leq l \leq v$. If $\#\mathcal{I}(C, X) \leq b$ for all $X \in \begin{bmatrix} V \\ l \end{bmatrix}$, then

$$\#C \leq \begin{cases} b \cdot \begin{bmatrix} v \\ l \end{bmatrix}_q / \begin{bmatrix} k \\ l \end{bmatrix}_q & \text{if } l \leq k, \\ b \cdot \begin{bmatrix} v \\ l \end{bmatrix}_q / \begin{bmatrix} v-k \\ l-k \end{bmatrix}_q & \text{if } k < l. \end{cases}$$

Proof
Double counting $\mathcal{T} = \{(U, X) \in C \times \left[{V \atop l}\right] \mid U \le X \text{ or } X \le U\}$ yields $\#\mathcal{T} = \sum_X \#\mathcal{I}(C, X) \le \sum_X b = \left[{v \atop l}\right]_q b$ on the one hand and $\#\mathcal{T} = \left[{k \atop l}\right]_q \cdot \#C$ if $l \le k$ and $\#\mathcal{T} = \left[{v-k \atop l-k}\right]_q \cdot \#C$ if $k < l$. □

Now, we specialize our considerations to CDCs with $v = 2k$ and minimum subspace distance $d = 2k - 2$. Using the two well known facts $\mathrm{A}_q(v, 2k; k) = \frac{q^v - q}{q^k - 1} - q + 1$ for $v \equiv 1 \pmod k$ and $2 \le k \le v$, cf. Theorem 126, and $\mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; v - k)$, due to the properties of orthogonal codes, we conclude:

43 **Corollary**
Let C be a $(2k, \#C, 2k - 2; k)_q$ CDC for $k \ge 1$ and $b \in \mathbb{Z}$. Then $\#\mathcal{I}(C, H) \le q^k + 1$ for all hyperplanes H and $\#\mathcal{I}(C, P) \le q^k + 1$ for all points P. Moreover, if $\#\mathcal{I}(C, H) \le b$ for all hyperplanes H or $\#\mathcal{I}(C, P) \le b$ for all points P, then $\#C \le (q^k + 1)b$.

Proof
Lemma 41 gives $\#\mathcal{I}(C, P) \le \mathrm{A}_q(2k - 1, 2k - 2; k - 1) = q^k + 1$ and $\#\mathcal{I}(C, H) \le \mathrm{A}_q(2k - 1, 2k - 2; k) = \mathrm{A}_q(2k - 1, 2k - 2; k - 1) = q^k + 1$. Applying Lemma 42 with $l = 1$ respective $l = v - 1$ completes the proof. □

Corollary 43 will be applied in Chapter 12 in order to deduce $\mathrm{A}_2(8, 6; 4) \le 272$.

44 **Lemma ([HKK16b, Lemma 2.8.i])**
Let C be a $(v, \#C, d; K)_q^{\mathrm{s}}$ subspace code, $P \in \left[{V \atop 1}\right]$, $H \in \left[{V \atop v-1}\right]$ with $P \not\le H$, and $d \ge 2$. Then the so-called *shortened code*

$$S(C, P, H) = \{U \cap H \mid U \in \mathcal{I}(C, P)\} \cup \mathcal{I}(C, H)$$

is a $(v - 1, \#\mathcal{I}(C, P) + \#\mathcal{I}(C, H), d'; K')_q^{\mathrm{s}}$ subspace code with $d' \ge d - 1$ and $K' \subseteq (K \cup \{k - 1 \mid k \in K\}) \cap \{0, 1, \ldots, v\}$.

Applying Lemma 44 for a $(v, \#C, d; k)_q$ CDC C gives a

$$(v - 1, \#\mathcal{I}(C, P) + \#\mathcal{I}(C, H), d'; K')_q^{\mathrm{s}}$$

subspace code, where $d' \ge d - 1$ and $K' = \{k - 1, k\} \cap \{0, 1, \ldots, v\}$. For a more refined analysis we will consider incidences of codewords with pairs of points and hyperplanes.

The following proposition is valid for all subsets $S \subseteq \left[{V \atop k}\right]$, not only CDCs.

45 Proposition
Let $S \subseteq \left[{V \atop k}\right]$, $1 \le k \le v-1$, and $b \in \mathbb{N}$. If $\#S > \frac{(q^v-1)(b-1)}{q^{v-k}+q^k-2}$, then there is a hyperplane $\bar{H}$ and a point $\bar{P} \not\le \bar{H}$ with $\#\mathcal{I}\left(S, \bar{H}\right) + \#\mathcal{I}\left(S, \bar{P}\right) \ge b$.

Proof
Let $\#\mathcal{I}(S,H) + \#\mathcal{I}(S,P) \le b-1$ for all pairs of points and hyperplanes (P,H) with $P \not\le H$. Double counting the set $\mathcal{T}$ of triples (P,H,U), where $U \in \mathcal{I}(S,H) \cup \mathcal{I}(S,P)$ and $P \not\le H$, gives

$$\begin{aligned}\#\mathcal{T} &= \sum_{U \in S}\left(\sum_{H \in \mathcal{I}\left(\left[{V \atop v-1}\right],U\right)} \#\left\{P \in \left[{V \atop 1}\right] \mid P \not\le H\right\} + \sum_{P \in \mathcal{I}\left(\left[{V \atop 1}\right],U\right)} \#\left\{H \in \left[{V \atop v-1}\right] \mid P \not\le H\right\}\right)\\ &= \#S \cdot \left(\left[{v-k \atop v-1-k}\right]_q \left(\left[{v \atop 1}\right]_q - \left[{v-1 \atop 1}\right]_q\right) + \left[{k \atop 1}\right]_q \left(\left[{v \atop v-1}\right]_q - \left[{v-1 \atop v-1-1}\right]_q\right)\right)\\ &= \#S([v-k]_q + [k]_q)([v]_q - [v-1]_q))\end{aligned}$$

and

$$\begin{aligned}\#\mathcal{T} &= \sum_{P} \sum_{H \in \left[{V \atop v-1}\right] \setminus \mathcal{I}\left(\left[{V \atop v-1}\right],P\right)} (\#\mathcal{I}(S,H) + \#\mathcal{I}(S,P))\\ &\le \left[{v \atop 1}\right]_q \left(\left[{v \atop v-1}\right]_q - \left[{v-1 \atop v-1-1}\right]_q\right)(b-1) = [v]_q([v]_q - [v-1]_q)(b-1),\end{aligned}$$

where we use $\mathcal{I}\left(\left[{V \atop k}\right], H\right) \cap \mathcal{I}\left(\left[{V \atop k}\right], P\right) = \emptyset$, due to $P \not\le H$ and $\#\mathcal{I}(S,H) + \#\mathcal{I}(S,P) \le b-1$. Hence, we obtain

$$\#S([v-k]_q + [k]_q)([v]_q - [v-1]_q)) \le [v]_q([v]_q - [v-1]_q)(b-1),$$

so that $\#S \le \frac{[v]_q(b-1)}{[v-k]_q+[k]_q} = \frac{(q^v-1)(b-1)}{q^{v-k}+q^k-2}$, which is a contradiction. □

Again, we specialize our considerations to CDCs with $v = 2k$ and minimum distance $d = 2k-2$.

46 Corollary
Let C be a $(2k, \#C, 2k-2; k)_q$ CDC with $k \ge 3$. If $\#C > (q^k+1)(q^k+1-(c+1)/2)$ for some $c \in \mathbb{N}$, then there is a hyperplane $\bar{H}$ and a point $\bar{P}$ with $\#\mathcal{I}\left(C, \bar{H}\right) + \#\mathcal{I}\left(C, \bar{P}\right) \ge 2(q^k+1) - c$ and $\bar{P} \not\le \bar{H}$.

Proof
The statement follows from Proposition 45 using $b = 2(q^k+1) - c$. □

3.1 DefaultCDCBLP

The following binary linear program (BLP) is the canonical formulation of the main problem of subspace coding in the constant dimension case and therefore deserves the name DefaultCDCBLP. We will use it regularly in exactly this or slightly modified versions, which we denote at the specific text passages.

47 **Definition**
Let $q \geq 2$ be a prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers. Then DefaultCDCBLP(q, v, d, k) is the following BLP:

$$\begin{array}{llll}
\max \sum\limits_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} x_U \quad \text{st} & & & \\
\sum\limits_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U \leq \mathrm{A}_q(v-w, d; k-w) & \forall W \in \begin{bmatrix} \mathbb{F}_q^v \\ w \end{bmatrix} & \forall w \in \{1, \ldots, k-d/2\} \\
\sum\limits_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U \leq 1 & \forall W \in \begin{bmatrix} \mathbb{F}_q^v \\ k-d/2+1 \end{bmatrix} & \\
\sum\limits_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U \leq 1 & \forall W \in \begin{bmatrix} \mathbb{F}_q^v \\ k+d/2-1 \end{bmatrix} & \\
\sum\limits_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U \leq \mathrm{A}_q(w, d; k) & \forall W \in \begin{bmatrix} \mathbb{F}_q^v \\ w \end{bmatrix} & \forall w \in \{k+d/2, \ldots, v-1\} \\
x_U \in \{0, 1\} & \forall U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} &
\end{array}$$

The importance lies in the following connection:

48 **Lemma**
For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers, we have:
On the one hand, for any $(v, N, d; k)_q$ CDC C the characteristic vector

$$(x_U)_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} = (\mathbb{1}_{\{U \in C\}})_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}}$$

is feasible for DefaultCDCBLP(q, v, d, k).
On the other hand, for a feasible characteristic vector $(x_U)_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}}$ of DefaultCDCBLP(q, v, d, k) the set

$$C = \left\{ U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \;\middle|\; x_U = 1 \right\}$$

is a $(v, N, d; k)_q$ CDC.

In both cases $N = \sum_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} x_U$ and in particular, $\mathrm{A}_q(v, d; k) = \textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$.

Proof

Let C be a $(v, N, d; k)_q$ CDC and $(x_U)_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} = (\mathbb{1}_{\{U \in C\}})_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}}$ its characteristic vector. Then the sizes match $N = \sum_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} x_U$. For $W \le \mathbb{F}_q^v$ with $\dim(W) = w$ we have $\#\mathcal{I}(C, W) = \sum_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U$ and hence with Lemma 41:

$$\sum_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U = \#\mathcal{I}(C, W) \le \begin{cases} \mathrm{A}_q(w, d; k) & \text{if } w \ge k, \\ \mathrm{A}_q(v - w, d; k - w) & \text{if } w < k. \end{cases}$$

Since $\mathrm{A}_q(v', d; k') = 1$ if $d/2 > \min\{k', v' - k'\}$ we have $\mathrm{A}_q(w, d; k) = 1$ if $k \le w < k + d/2$ and $\mathrm{A}_q(v - w, d; k - w) \le 1$ if $k - d/2 < w < k$. Hence, (x_U) is feasible for all constraints of $\textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$.

Let $(x_U)_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}}$ be feasible for $\textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$ and $C = \left\{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \,\middle|\, x_U = 1\right\}$ a subset of $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$. Again the sizes match $N = \sum_{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}} x_U$.

The second set of constraints in $\textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$ are $\sum_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, W\right)} x_U \le 1$ for all $W \in \begin{bmatrix} \mathbb{F}_q^v \\ k - d/2 + 1 \end{bmatrix}$ and hence any $U \ne U' \in C$ have $\dim(U \cap U') \le k - d/2$ which implies the minimum subspace distance $\mathrm{d_s}(U, U') = 2(k - \dim(U \cap U')) \ge d$. □

The constraints with $\dim(W) \in \{k - d/2 + 2, \ldots, k + d/2 - 2\}$ are implied by the two sets of constraints with $\dim(W) \in \{k - d/2 + 1, k + d/2 - 1\}$ and hence are redundant, i.e., any (x_U) with $0 \le x_U \le 1$ (instead of $x_U \in \{0, 1\}$) for all $U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ which is feasible for both sets of constraints with $\dim(W) \in \{k - d/2 + 1, k + d/2 - 1\}$ is automatically feasible for the constraints with $\dim(W) \in \{k - d/2 + 2, \ldots, k + d/2 - 2\}$.

If C is a $(v, \#C, d; k)_q$ CDC, then its corresponding feasible vector in $\textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$ fulfills exactly $\#C \cdot \begin{bmatrix} k \\ k - d/2 + 1 \end{bmatrix}_q$ constraints having $\dim(W) = k - d/2 + 1$ and $\#C \cdot \begin{bmatrix} k + d/2 - 1 \\ k \end{bmatrix}_q$ constraints having $\dim(W) = k + d/2 - 1$ with equality.

At first glance, any constraint with $\dim(W) \ne k - d/2 + 1$ is redundant. This is only true for integral (x_U) and since the solving process of a binary linear program usually depends on LP-relaxations, one can profit by using these additional constraints.

$\textsc{Default}\mathrm{CDCBLP}(q, v, d, k)$ may be changed by removing some constraints. An analogous proof as the proof of Lemma 48 shows the same facts also for the following

BLP:

$$
\begin{aligned}
\mathrm{A}_q(v,d;k) = \max & \sum_{U \in \left[\begin{smallmatrix}\mathbb{F}_q^v\\ k\end{smallmatrix}\right]} x_U & & \\
\text{st} & \sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}\mathbb{F}_q^v\\ k\end{smallmatrix}\right], W\right)} x_U \le 1 & & \forall W \in \left[\begin{smallmatrix}\mathbb{F}_q^v\\ k-d/2+1\end{smallmatrix}\right] \\
& x_U \in \{0,1\} & & \forall U \in \left[\begin{smallmatrix}\mathbb{F}_q^v\\ k\end{smallmatrix}\right]
\end{aligned}
$$

On the one hand, this BLP is inferior to DefaultCDCBLP(q,v,d,k) in terms of the set of feasible points in the LP-relaxation and consequently the quality of the LP-relaxations in the solving process of the branch & bound method ([Dak65]) are also inferior, but it is superior in terms of computation speed of LP-iterations, since all intermediate computation steps operate on smaller structures. Moreover, using $V = \mathbb{F}_q^v$, any subset of constraints $\mathcal{P}$ with

$$
\left\{ x_U \;\middle|\; \sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right], W\right)} x_U \le 1 \;\forall W \in \left[\begin{smallmatrix}V\\ k-d/2+1\end{smallmatrix}\right] \right\}
$$

$$\subseteq \mathcal{P} \subseteq$$

$$
\left\{ x_U \;\middle|\; \begin{aligned}
&\sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right], W\right)} x_U \le \mathrm{A}_q(v-w,d;k-w) \;\forall W \in \left[\begin{smallmatrix}V\\ w\end{smallmatrix}\right] \;\forall w \in \{1,\ldots,k-d/2\} \wedge \\
&\sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right], W\right)} x_U \le 1 \;\forall W \in \left[\begin{smallmatrix}V\\ k-d/2+1\end{smallmatrix}\right] \wedge \\
&\sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right], W\right)} x_U \le 1 \;\forall W \in \left[\begin{smallmatrix}V\\ k+d/2-1\end{smallmatrix}\right] \wedge \\
&\sum_{U \in \mathcal{I}\left(\left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right], W\right)} x_U \le \mathrm{A}_q(w,d;k) \;\forall W \in \left[\begin{smallmatrix}V\\ w\end{smallmatrix}\right] \;\forall w \in \{k+d/2,\ldots,v-1\}
\end{aligned} \right\}
$$

can be used for a BLP

$$
\max \left\{ \sum_{U \in \left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right]} x_U \;\middle|\; x_U \in \mathcal{P} \wedge x_U \in \{0,1\} \;\forall U \in \left[\begin{smallmatrix}V\\ k\end{smallmatrix}\right] \right\}
$$

whose optimal value is also equal to $\mathrm{A}_q(v,d;k)$ using the same proof as Lemma 48.

	q	v	d	k	number of maximal cliques	number of maximum cliques	$\left[{v \atop k-d/2+1}\right]_q$	$\left[{v \atop k+d/2-1}\right]_q$
$k < v/2$	2	5	4	2	186	31	31	155
	2	6	4	2	1458	63	63	1395
	2	7	4	2	?	127	127	11811
$k = v/2$	2	4	4	2	30	30	15	15
	2	6	4	3	1302	1302	651	651
	2	6	6	3	?	126	63	63

Table 4: Number of inclusion maximal and maximum cliques of the stable set polytopes $\mathrm{Stab}(G)$ for small CDC parameters. The computation of the entries labeled with "?" are aborted after 260 hours of wall-time.

It is quite difficult to give an advice which set of constraints $\mathcal{P}$ is advisable in the general case since this depends on the conditions of use.

The set of constraints $\mathcal{P}$, together with $-x_U \le 0$ for all $U \in \left[{\mathbb{F}_q^v \atop k}\right]$, implies a better formulation if it is larger and DefaultCDCBLP(q, v, d, k) uses the best of these formulations.

The connection between CDCs and stable set polytopes uses the graph

$$G' = \left(\left[{\mathbb{F}_q^v \atop k}\right], \left\{\{U, W\} \in \binom{\left[{\mathbb{F}_q^v \atop k}\right]}{2} \,\middle|\, \mathrm{d_s}(U, W) < d\right\}\right).$$

Then

$$\mathrm{A}_q(v, d; k) = \max\left\{\sum_{U \in \left[{\mathbb{F}_q^v \atop k}\right]} x_U \,\middle|\, x \in \mathrm{Stab}(G')\right\}.$$

In particular, the set of constraints $x_U + x_W \le 1$ for all $U \ne W \in \left[{\mathbb{F}_q^v \atop k}\right]$ with $\mathrm{d_s}(U, W) < d$ hence are called *edge constraints*. $\sum_{U \in \mathcal{I}\left(\left[{\mathbb{F}_q^v \atop k}\right], W\right)} x_U \le 1$ for all $W \in \left[{\mathbb{F}_q^v \atop k-d/2+1}\right]$ respectively $\sum_{U \in \mathcal{I}\left(\left[{\mathbb{F}_q^v \atop k}\right], W\right)} x_U \le 1$ for all $W \in \left[{\mathbb{F}_q^v \atop k+d/2-1}\right]$ are *clique constraints*.

Frankl and Wilson proved in [FW86, Theorem 1] that the maximum cardinality of $A \subseteq \left[{\mathbb{F}_q^v \atop k}\right]$ with $\mathrm{d_s}(U, W) < d$ for all $U \ne W \in A$ is $\max\left\{\left[{v-(k-d/2+1) \atop k-(k-d/2+1)}\right]_q, \left[{k+d/2-1 \atop k}\right]_q\right\}$ if $k + d/2 - 1 \le v$ and therefore at least one of the two sets of clique constraints of the last paragraph are facets.

Table 4 lists the numbers of inclusion maximal and maximum cliques of the stable set polytopes $\mathrm{Stab}(G')$ for small parameters of CDCs computed with `Cliquer`. For $k = v/2$, each maximal clique attains the cardinality of the respective clique number, i.e., is a maximum clique. For $k < v/2$ the number of maximum cliques still corresponds with $\left[{v \atop k-d/2+1}\right]_q$, i.e., the number of constraints in DefaultCDCBLP(q, v, d, k) induced by

W of dimension $k-d/2+1$. Although in this case the constraints induced by the $(k+d/2-1)$-dimensional subspaces are not maximum cliques, they are inclusion maximal and according to the table these are all maximal cliques.

Adding inequalities to a formulation may remove the property of a face being a facet as the following simple example shows. The full-dimensional polytope $P=\{x\in\mathbb{R}\mid 0\le x\le 1.5\}$ is a formulation for $X=\{0,1\}$ and the valid inequality $x\le 1.5$ implies the facet $F=\{x\in\mathbb{R}\mid x=1.5\}$. By adding the inequality $x\le 1$ to P the formulation $P'=\{x\in\mathbb{R}\mid 0\le x\le 1\}$ is better than P. It is even optimal. But $x\le 1.5$ implies the face $F'=\{x\in\mathbb{R}\mid x=1.5\le 1\}=\emptyset$ which is still a face but no facet.

The next lemma will show that the clique constraints are even facets in the polytope of the LP-relaxation of DefaultCDCBLP(q,v,d,k), i.e., $0\le x_U\le 1$ instead of $x_U\in\{0,1\}$ for $U\in\begin{bmatrix}\mathbb{F}_q^v\\k\end{bmatrix}$.

49 Lemma

Let $q\ge 2$ be a prime power, $2\le d/2\le k\le v-k$ integers, P be the polytope of the LP-relaxation of DefaultCDCBLP(q,v,d,k), and $P_{\text{opt}}=\operatorname{conv}\left(P\cap\mathbb{Z}^{\left[{v\atop k}\right]_q}\right)$. Then:

1. $\dim(P)=\left[{v\atop k}\right]_q$ and hence P_{opt} is full-dimensional, which implies that P is full-dimensional,
2. $0\le x_U$ defines a facet of P_{opt} for all $U\in\begin{bmatrix}\mathbb{F}_q^v\\k\end{bmatrix}$, which implies that these inequalities define facets of P as well,
3. $\sum_{U\in\mathcal{I}\left(\begin{bmatrix}\mathbb{F}_q^v\\k\end{bmatrix},W\right)}x_U\le 1$ defines a facet of P for all $W\in\begin{bmatrix}\mathbb{F}_q^v\\k-d/2+1\end{bmatrix}$, and
4. $\sum_{U\in\mathcal{I}\left(\begin{bmatrix}\mathbb{F}_q^v\\k\end{bmatrix},W\right)}x_U\le 1$ defines a facet of P for all $W\in\begin{bmatrix}\mathbb{F}_q^v\\k+d/2-1\end{bmatrix}$.

Proof

We abbreviate $\mathcal{G}=\begin{bmatrix}\mathbb{F}_q^v\\k\end{bmatrix}$.

1 The CDCs $C_0=\emptyset$ and $C_{U'}=\{U'\}$ for all $U'\in\mathcal{G}$ yield feasible vectors $(x_U)_{U\in\mathcal{G}}=\mathbf{0}$ and $(x_U)_{U\in\mathcal{G}}=\mathbb{1}_{\{U=U'\}}$ for P_{opt} via Lemma 48. They are affinely independent and the dimension of P_{opt} is exactly $\left[{v\atop k}\right]_q$ because $P\subseteq\mathbb{R}^{\left[{v\atop k}\right]_q}$.

2 Fix an $\bar{U}\in\mathcal{G}$ and thereby the inequality $0\le x_{\bar{U}}$ and the face $F=\{x\in P_{\text{opt}}\mid x_{\bar{U}}=\mathbf{0}\}$. The CDCs C_0 and $C_{U'}$ for $U'\in\mathcal{G}\setminus\{\bar{U}\}$ yield vectors in F which are again affinely independent and in particular $\dim(F)=\left[{v\atop k}\right]_q-1=\dim(P)-1$.

3 We fix a $W\in\begin{bmatrix}\mathbb{F}_q^v\\k-d/2+1\end{bmatrix}$ and the inequality $\sum_{U\in\mathcal{G}:W\le U}x_U\le 1$. The number of k-spaces in $\mathbb{F}_q^v$ that contain W is $\lambda=\begin{bmatrix}v-k+d/2-1\\d/2-1\end{bmatrix}_q$. Moreover let $U_0\in\mathcal{G}$ be a fixed subspace with $W\le U_0$. Next, we will define $\left[{v\atop k}\right]_q$ affinely independent vectors

$(y_U)^{\bar{U}}_{U\in\mathcal{G}}$ for all $\bar{U} \in \mathcal{G}$ in $F = \{x \in P \mid \sum_{U\in\mathcal{G}:W\le U} x_U = 1\}$ which then in turn prove $\dim(F) = \left[{v \atop k}\right]_q - 1 = \dim(P) - 1$:

$$(y_U)^{\bar{U}}_{U\in\mathcal{G}} = \begin{cases} \mathbb{1}_{\{U=\bar{U}\}} & \text{if } W \le \bar{U} \ne U_0, \\ \mathbb{1}_{\{W\le U\}}/\lambda & \text{if } U_0 = \bar{U}, \text{ and} \\ \mathbb{1}_{\{W\le U \text{ or } U=\bar{U}\}}/\lambda & \text{if } W \not\le \bar{U}. \end{cases}$$

All three cases fulfill $\sum_{U\in\mathcal{G}:W\le U} x_U \le 1$ with equality.

They are affinely independent iff $\{(y_U)^{\bar{U}}_{U\in\mathcal{G}} - (y_U)^{U_0}_{U\in\mathcal{G}} \mid \bar{U} \ne U_0\}$ is linearly independent:

$$\begin{aligned} 0 &= \sum_{\bar{U}\in\mathcal{G}\setminus\{U_0\}} \mu_{\bar{U}}((y_U)^{\bar{U}}_{U\in\mathcal{G}} - (y_U)^{U_0}_{U\in\mathcal{G}}) = \sum_{\bar{U}\in\mathcal{G}\setminus\{U_0\}} \mu_{\bar{U}}(y_U)^{\bar{U}}_{U\in\mathcal{G}} + (-\sum_{\bar{U}\in\mathcal{G}\setminus\{U_0\}} \mu_{\bar{U}})(y_U)^{U_0}_{U\in\mathcal{G}} \\ &= \sum_{W\le\bar{U}\ne U_0} \mu_{\bar{U}}\mathbb{1}_{\{U=\bar{U}\}} + (-\sum_{\bar{U}\in\mathcal{G}\setminus\{U_0\}} \mu_{\bar{U}})\mathbb{1}_{\{W\le U\}}/\lambda + \sum_{W\not\le\bar{U}} \mu_{\bar{U}}\mathbb{1}_{\{W\le U \text{ or } U=\bar{U}\}}/\lambda. \end{aligned}$$

Since the vectors $\mathbb{1}_{\{\cdot\}}$ are linearly independent, this implies $\mu_{\bar{U}} = 0$ for $W \le \bar{U} \ne U_0$, $(-\sum_{\bar{U}\in\mathcal{G}\setminus\{U_0\}} \mu_{\bar{U}})/\lambda = 0$, and $\mu_{\bar{U}}/\lambda = 0$ for $W \not\le \bar{U}$, i.e., $\mu_{\bar{U}}$ for $\bar{U} \ne U_0$.

Next, each $(y_U)^{\bar{U}}_{U\in\mathcal{G}}$ is contained in P: Since $\mathrm{A}_q(v', d; k') \ge 2$ iff $1 \le k' \le v' - 1$ and $d/2 \le \min\{k', v' - k'\}$, $2 \le d/2 \le k \le v - k$ implies that the right hand side of the inequalities of $\textsc{Default}$CDCBLP(q, v, d, k) which are of the form $\mathrm{A}_q(v', d; k')$ are at least 2. Since $\sum_{U\in\mathcal{G}}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le 1 + 1/\lambda \le 2$ for all $\bar{U} \in \mathcal{G}$, all these vectors are feasible for the constraints. Any subset $L \in \binom{\mathcal{G}}{\lambda}$ of cardinality λ implies $\sum_{U\in L}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le 1$ for all $\bar{U} \in \mathcal{G}$ and in particular these vectors are feasible for any constraint with $\dim(W') = k - d/2 + 1$. For any $Z \in \left[{\mathbb{F}_q^v \atop k+d/2-1}\right]$, we distinguish the following cases. If $W \not\le Z$, then $\sum_{U\le Z}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le 1/\lambda \le 1$ for all $\bar{U} \in \mathcal{G}$. If $W \le \bar{U} \ne U_0$, then $\sum_{U\le Z}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le 1$. Else there are $\left[{(k+d/2-1)-(k-d/2+1) \atop k-(k-d/2+1)}\right]_q = \left[{2(d/2-1) \atop d/2-1}\right]_q$ k-spaces U with $W \le U \le Z$ and we have

$$\begin{aligned} &\sum_{U\le Z}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le \left(\left[{2(d/2-1) \atop d/2-1}\right]_q + 1\right)/\lambda \le 1 \\ \Leftrightarrow &\left[{2(d/2-1) \atop d/2-1}\right]_q < \left[{v-k+d/2-1 \atop d/2-1}\right]_q \Leftrightarrow 2(d/2-1) < v - k + d/2 - 1 \end{aligned}$$

which is implied by $2 \le d/2 \le k \le v - k$.

4 An analogous reasoning as in **3** can be applied for a fixed $Z \in \left[{\mathbb{F}_q^v \atop k+d/2-1}\right]$. We only have to replace $W \le U$, $W \le U_0$, and $W \le \bar{U}$ with $U \le Z$, $U_0 \le Z$, and $\bar{U} \le Z$, respectively as well as $\lambda = \left[{k+d/2-1 \atop d/2-1}\right]_q$. Then an analogous definition of $(y_U)^{\bar{U}}_{U\in\mathcal{G}}$ provides $\left[{v \atop k}\right]_q$ affinely independent vectors contained in the face. The only difference is to show that for fixed $W \in \left[{\mathbb{F}_q^v \atop k-d/2+1}\right]$ and $\bar{U} \in \mathcal{G}$ the vector $(y_U)^{\bar{U}}_{U\in\mathcal{G}}$ is feasible for the inequality $\sum_{U\ge W} x_U \le 1$: If $W \not\le Z$ then $\sum_{U\ge W}(y_U)^{\bar{U}}_{U\in\mathcal{G}} \le 1/\lambda \le 1$ and if $U_0 \ne \bar{U} \le Z$ then

$\sum_{U \ge W} (y_U)^{\bar{U}}_{U \in \mathcal{G}} \le 1$, else there are again $\begin{bmatrix} 2(d/2-1) \\ d/2-1 \end{bmatrix}_q$ k-spaces between W and Z. Hence:

$$\sum_{U \ge W} (y_U)^{\bar{U}}_{U \in \mathcal{G}} \le \left(\begin{bmatrix} 2(d/2-1) \\ d/2-1 \end{bmatrix}_q + 1 \right) / \lambda \le 1$$
$$\Leftrightarrow \begin{bmatrix} 2(d/2-1) \\ d/2-1 \end{bmatrix}_q < \begin{bmatrix} k+d/2-1 \\ d/2-1 \end{bmatrix}_q \Leftrightarrow 2(d/2-1) < k + d/2 - 1$$

which is again implied by $2 \le d/2 \le k \le v - k$. □

The following statements imply some additional structure that large codes must have and, as byproduct, allow to upper bound the slack of some inequalities of the DefaultCDCBLP.

50 **Lemma**
Let $q \ge 2$ be a prime power, $2 \le d/2 \le \min\{k, v-k\}$ integers and C be a $(v, \#C, d; k)_q$ CDC. Then we have $\#C - \#\mathcal{I}(C, H) \le q^{v-k} \operatorname{A}_q(v-1, d; k-1)$ and $\#C - \#\mathcal{I}(C, P) \le q^k \operatorname{A}_q(v-1, d; k)$ for any point P and hyperplane H in $\mathbb{F}_q^v$.

Proof
Let $H \le \mathbb{F}_q^v$ be a fixed hyperplane and $\mathcal{P}$ the set of points in $\mathbb{F}_q^v$ that are not incident to H. Double counting of the set $\{(U, P) \in C \times \mathcal{P} \mid P \le U\}$ yields

$$(\#C - \#\mathcal{I}(C, H))(\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q) = \sum_{P \in \mathcal{P}} \#\mathcal{I}(C, P)$$

and the right hand side is estimated with Lemma 41 to $\le (\begin{bmatrix} v \\ 1 \end{bmatrix}_q - \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q) \operatorname{A}_q(v-1, d; k-1)$, which proofs the first part. The second part can be proved in exactly the same way interchanging points and hyperplanes – or by applying orthogonality, i.e., we also interchange points and hyperplanes as well as k and $v-k$. □

This lemma has the consequence for DefaultCDCBLP(q, v, d, k) that it allows to bound the slack of the inequalities with $w = 1$ and $w = v-1$. The *slack* s of an inequality $f(x) \le g$ is defined as $s = g - f(x)$, which is therefore non-negative, and in particular we have $f(x) \le g \Leftrightarrow f(x) + s = g \wedge s \ge 0$. Hence, the slack for the inequality corresponding to the point P is $s(P) = \operatorname{A}_q(v-1, d; k-1) - \sum_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, P\right)} x_U = \operatorname{A}_q(v-1, d; k-1) - \#\mathcal{I}(C, P)$ and to the hyperplane H it is $s(H) = \operatorname{A}_q(v-1, d; k) - \sum_{U \in \mathcal{I}\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, H\right)} x_U = \operatorname{A}_q(v-1, d; k) - \#\mathcal{I}(C, H)$.

51 **Corollary**
Let $q \ge 2$ be a prime power, $2 \le d/2 \le \min\{k, v-k\}$ integers and C be a $(v, \#C, d; k)_q$ CDC. Then we have $s(H) \le q^{v-k} \operatorname{A}_q(v-1, d; k-1) + \operatorname{A}_q(v-1, d; k) - \#C$ and $s(P) \le q^k \operatorname{A}_q(v-1, d; k) + \operatorname{A}_q(v-1, d; k-1) - \#C$ for any point P and hyperplane H in $\mathbb{F}_q^v$.

For example Lemma 50 implies for any $(6, \#C, 4; 3)_2$ CDC C: $\#C - \#\mathcal{I}(C, H) \leq 8 \cdot \mathrm{A}_2(5, 4; 2) = 8 \cdot 9$ and $\#C - \#\mathcal{I}(C, P) \leq 8 \cdot \mathrm{A}_2(5, 4; 3) = 8 \cdot 9$ for any point P and hyperplane H in $\mathbb{F}_2^6$, i.e.,

$$\#C \leq 72 + \min\left\{\min\left\{\#\mathcal{I}(C, P) \;\middle|\; P \in \begin{bmatrix}\mathbb{F}_2^6\\1\end{bmatrix}\right\}, \min\left\{\#\mathcal{I}(C, H) \;\middle|\; H \in \begin{bmatrix}\mathbb{F}_2^6\\5\end{bmatrix}\right\}\right\}$$

In particular, if $\#C = 77$, then $5 \leq \#\mathcal{I}(C, P)$ and $5 \leq \#\mathcal{I}(C, H)$ for any point P and hyperplane H in $\mathbb{F}_2^6$.

Alternatively, Corollary 51 upper bounds the slack: $s(P) \leq 81 - \#C$ and $s(H) \leq 81 - \#C$ for any point P and hyperplane H in $\mathbb{F}_2^6$ which is of particular interest if the right hand side is ≤ 8, i.e., $\#C \geq 73$, since the left hand side is bounded by 9 due to Lemma 41.

In fact, Table 6 in [HKK15] shows that there is a point which is incident to exactly 5 codewords for any $(6, 77, 4; 3)_2$ CDC.

4 The connection between subspaces and pivot vectors

For $u \in \mathbb{F}_2^v$ let $\operatorname{EF}_q(u) = \{M \in \mathbb{F}_q^{\operatorname{wt}(u)\times v} \mid M \text{ in RREF and } \operatorname{p}(M) = u\}$. In particular we have $\#\operatorname{EF}_q((u_1, u_2, \ldots, u_v)) = q^{\sum_{i=1}^{v}(1-u_i)\cdot\sum_{j=1}^{i-1} u_j}$ and $\sum_{u\in\mathbb{F}_2^v,\operatorname{wt}(u)=k} \#\operatorname{EF}_q(u) = \left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q$.

A *Ferrers diagram* is a graphical representation of a partition of an integer. Let $n = s_1 + s_2 + \ldots + s_l$ for positive integers $s_1, s_2, \ldots, s_l$ with $s_1 \ge s_2 \ge \ldots \ge s_l$, cf. [And76]. The $l \times s_1$ array with s_i dots in the i-th row which are all aligned to the right is the Ferrers diagram of the partition $n = s_1 + s_2 + \ldots + s_l$. Note that some literature aligns the dots to the left.

For an $m \times \eta$ Ferrers diagram $\mathcal{F}$, a Ferrers diagram rank metric code (FDRMC) $(\mathcal{F}, \#C, d)_q$ is a $(m \times \eta, \#C, d)_q$ rank metric code C such that each matrix in C has non-zeros only in the positions where $\mathcal{F}$ has dots.

The Echelon-Ferrers diagram of $u \in \mathbb{F}_2^v$ is the Ferrers diagram consisting of dots in the positions in which $\operatorname{EF}_q(u)$ has variables, which is independent of q, cf. [ES09; Etz+16].

52 **Example**
For $u = (1, 0, 1, 1, 0) \in \mathbb{F}_2^5$ we have

$$\operatorname{EF}_q(u) = \left\{ \begin{pmatrix} 1 & b_1 & 0 & 0 & b_2 \\ 0 & 0 & 1 & 0 & b_3 \\ 0 & 0 & 0 & 1 & b_4 \end{pmatrix} \in \mathbb{F}_q^{3\times 5} \;\middle|\; b_1, b_2, b_3, b_4 \in \mathbb{F}_q \right\}.$$

Here, we have $\#\operatorname{EF}_q(u) = q^4$ and the Echelon-Ferrers diagram uses $n = 4$, $s_1 = 2$, $s_2 = s_3 = 1$, and is $\begin{smallmatrix} \bullet & \bullet \\ & \bullet \\ & \bullet \end{smallmatrix}$.

The subspace distance between two subspaces with the same set of pivot columns can be computed by the rank distance of the corresponding generator matrices.

53 **Lemma ([SE11, Corollary 3])**
For all $U, W \in \mathcal{L}(V)$ with $\operatorname{p}(U) = \operatorname{p}(W)$, we have $\operatorname{d_s}(U, W) = 2\operatorname{d_r}(\tau(U), \tau(W))$.

Moreover, one can lower bound the subspace distance of two arbitrary matrices $U \in \operatorname{EF}_q(u)$ and $W \in \operatorname{EF}_q(w)$ by only considering u and w.

54 Lemma ([ES09, Lemma 2])
For two subspaces $U, W \in \mathcal{L}(V)$, we have $\mathrm{d_h}(\mathrm{p}(U), \mathrm{p}(W)) \leq \mathrm{d_s}(U, W)$.

Note that u and w may have different weight, i.e., U and W may have different dimension.

The Echelon-Ferrers construction from [ES09], see also [HR18], works as follows: To construct a $(v, M, d)_q$ MDC, we choose a block code $B \subseteq \mathbb{F}_2^v$ with minimum Hamming distance at least d. B is called skeleton code in this context. For each $b \in B$, we take a $C_b \subseteq \mathrm{EF}_q(b)$ with minimum rank distance of at least $d/2$. Then, by Lemma 53 and Lemma 54, $C = \bigcup_{b \in B}\{\tau^{-1}(A) \mid A \in C_b\}$ has the desired properties and $M = \sum_{b \in B} \#C_b$.

Moreover, to construct a $(v, M, d; k)_q$ CDC, the same construction as before with the restriction of B being a constant weight code in which each vector has weight k can be applied.

Hence, the two main questions that arise from this construction are how to choose the skeleton code and how to choose a rank metric code in $\mathrm{EF}_q(u)$ for given $u \in \mathbb{F}_2^v$.

To give a partial answer to the second question, let $\dim(\mathcal{F}, \delta)$ be the maximum dimension of a linear FDRMC with the Ferrers diagram $\mathcal{F}$ and minimum rank distance $1 \leq \delta$. Then we have an upper bound on $\dim(\mathcal{F}, \delta)$.

55 Theorem ([ES09, Theorem 1])
Let $\mathcal{F}$ be a $m \times \eta$ Ferrers diagram and $1 \leq \delta$ an integer. Let ν_i be the number of dots in $\mathcal{F}$, which are not contained in the first i rows and not contained in the rightmost $\delta - 1 - i$ columns for $0 \leq i \leq \delta - 1$, then $\dim(\mathcal{F}, \delta) \leq \min\{\nu_i \mid i \in \{0, 1, \ldots, \delta - 1\}\}$.

The authors of [ES09] conjectured that this upper bound is tight for all reasonable parameters. This conjecture is still unrefuted and valid in many cases, cf. [Etz+16].

If $u \in \mathbb{F}_2^v$ has k consecutive 1's and is 0 else, i.e., $u = (0_{v-k-c} 1_k 0_c)$ for $0 \leq c \leq v - k$, then its Echelon-Ferrers diagram has k rows and c columns and is full, i.e., it is the partition of $n = k \cdot c$ with $s_1 = s_2 = \ldots = s_k = c$ if $1 \leq c$ or else it contains no dot. Any element in the set $\mathrm{EF}_q(u)$ therefore has $v - k - c$ zero columns, then k pivot columns, and then c variable columns yielding a cardinality of q^{kc}. In this case, omitting these $v - c$ columns in the beginning yields $\mathbb{F}_q^{k \times c}$ in which we look for a rank metric code with minimum distance at least $d/2$. Embedding such a rank metric code again in $\mathrm{EF}_q(u)$ then yields a desired subcode C_u. Moreover, the cardinality of each rank metric code is equal to the cardinality of the embedded code in $\mathrm{EF}_q(u)$ and vice versa and therefore, focusing on constructing large codes, we take an $(k \times c, \lceil q^{\max\{k,c\}(\min\{k,c\}-d/2+1)} \rceil, d/2)_q$ MRD code, cf. Theorem 31, such that $\#C_u = \lceil q^{\max\{k,c\}(\min\{k,c\}-d/2+1)} \rceil$. Hence, in these cases the bound of Theorem 55 is tight.

For special subclasses explicit formulae for the sizes of the corresponding codes have been obtained, see [Ska10]. Additional refinements to the Echelon-Ferrers construction have been proposed recently, see [ES13; Etz+16; ST15].

A prominent special case is the so called lifted maximum rank code (LMRD), cf. [SKK08, Proposition 4]. It arises by taking the skeleton code $B = \{(1_k 0_{v-k})\}$ in the Echelon-Ferrers construction. Therefore an LMRD code is a $(v, \lceil q^{\max\{k,v-k\}(\min\{k,v-k\}-d/2+1)} \rceil, d; k)_q$ CDC, which simplifies, using $2 \le d/2 \le k \le v-k$, to a $(v, q^{(v-k)(k-d/2+1)}, d; k)_q$ CDC. Using this special pivot vector, all RREF matrices of codewords of an LMRD have a $k \times k$ identity matrix in the beginning. In other words, for an $(k \times (v-k), \lceil q^{\max\{k,v-k\}(\min\{k,v-k\}-d/2+1)} \rceil, d/2)_q$ MRD M, the set $\{\Lambda(A) \mid A \in M\}$ is an LMRD.

The arising question of upper bounds on sizes for CDCs which contain an LMRD as subset was partly answered by Etzion and Silberstein in [ES13, Theorem 10 and Theorem 11].

56 Theorem (cf. [ES13, Theorems 10 and 11])
Let C be a $(v, \#C, d; k)_q$ CDC that contains an LMRD for $2 \le d/2 \le k \le v-k$.

- If $d = 2(k-1)$ and $k \ge 3$, then $\#C \le q^{2(v-k)} + \mathrm{A}_q(v-k, 2(k-2); k-1)$,
- if $d = k$ even, then $\#C \le q^{(v-k)(k/2+1)} + \begin{bmatrix} v-k \\ k/2 \end{bmatrix}_q \frac{q^v - q^{v-k}}{q^k - q^{k/2}} + \mathrm{A}_q(v-k, k; k)$.

The paper [Hei18] and also this thesis in Chapter 6 generalize both bounds in Proposition 88 and Proposition 91 such that both bounds together cover the parameter range $2k < 3d$ together with $2 \le d/2 \le k \le v-k$.

57 Proposition (Proposition 99 and [Hei18, Proposition 1])
For $2 \le d/2 \le k \le v-k$ let C be a $(v, \#C, d; k)_q$ CDC that contains an LMRD code.

If $k < d \le 2/3v$ we have

$$\#C \le q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v-k, 2(d-k); d/2).$$

If additionally $d = 2k$, $r \equiv v \pmod{k}$, $0 \le r < k$, and $[r]_q < k$, then the right hand side is equal to $\mathrm{A}_q(v, d; k)$ and achievable in all cases.

If $(v, d, k) \in \{(6+3l, 4+2l, 3+l), (6l, 4l, 3l) \mid l \ge 1\}$, then there is a CDC containing an LMRD with these parameters whose cardinality achieves the bound.

If $k < d$ and $v < 3d/2$ we have

$$\#C \le q^{(v-k)(k-d/2+1)} + 1$$

and this cardinality is achieved.

If $d \le k < 3d/2$ we have

$$\#C \le q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v-k, 3d-2k; d) + \begin{bmatrix} v-k \\ d/2 \end{bmatrix}_q \begin{bmatrix} k \\ d-1 \end{bmatrix}_q q^{(k-d+1)(v-k-d/2)} / \begin{bmatrix} k-d/2 \\ d/2-1 \end{bmatrix}_q .$$

Another interesting special case for generating a $(v, \#C, d'; k)_q$ CDC C with $d \le d'$ $2 \le d/2 \le k \le v-k$ is given by the restriction to only use pivot vectors with k consecutive ones, cf. [Tra13a]. Then, as seen before, the maximum code in $\mathrm{EF}_q(u)$ for $u = (0_{v-k-c}1_k0_c) \in \mathbb{F}_2^v$ has $\lceil q^{\max\{k,c\}(\min\{k,c\}-d/2+1)}\rceil$ elements, answering the second question arising in the context of the Echelon-Ferrers construction, which was how the rank metric code should be chosen. In this case, also the first question can be answered thoroughly by taking the skeleton code $B = \{(0_{id/2}1_k0_{v-k-id/2}) \mid i \in \{0,1,\ldots,\lfloor (v-k)/(d/2)\rfloor\}\}$. Note that the Hamming distance between two arbitrary elements of B is at least d and hence Lemma 54 guarantees a subspace distance of at least d and that any other choice of B consisting entirely of vectors with k consecutive ones yields a final CDC of at most the same size. Therefore,

$$\#C = \sum_{i=0}^{\lfloor (v-k)/(d/2)\rfloor} \lceil q^{\max\{k,v-k-id/2\}(\min\{k,v-k-id/2\}-d/2+1)}\rceil,$$

which can be simplified using $x = \lfloor (v-2k)/(d/2)\rfloor$, $y = \lfloor (v-k-d/2+1)/(d/2)\rfloor$, and $z = \lfloor (v-k)/(d/2)\rfloor$. Note that $k \le v-k-id/2 \Leftrightarrow i \le x$ and $0 \le v-k-id/2-d/2+1 \Leftrightarrow i \le y$ and $0 \le v-2k \le v-k-d/2+1 \le v-k$ implies $0 \le x \le y \le z$ and $d \le k+1$ implies $x+1 \le y$. Hence:

$$= \sum_{i=0}^{x} q^{(v-k-id/2)(k-d/2+1)} + \sum_{i=x+1}^{z} \lceil q^{k(v-k-id/2-d/2+1)}\rceil$$
$$= \sum_{i=0}^{x} q^{(v-k-id/2)(k-d/2+1)} + \sum_{i=x+1}^{y} q^{k(v-k-id/2-d/2+1)} + \sum_{i=y+1}^{z} 1.$$

For the last sum, $z - y = \lfloor (v-k)/(d/2)\rfloor - \lfloor (v-k+1)/(d/2)\rfloor + 1 \in \{0,1\}$, by applying $\alpha - 1 < \lfloor \alpha \rfloor \le \alpha$ for $\alpha \in \mathbb{R}$, and $z - y = 0$ iff $v-k < ld/2 = v-k+1$ for an $l \in \mathbb{Z}$ iff $d/2 \mid v-k+1$. For the first sum, we apply the geometric series to get:

$$q^{(v-k)(k-d/2+1)} \sum_{i=0}^{x} \left(q^{(-d/2)(k-d/2+1)}\right)^i$$
$$= q^{(v-k)(k-d/2+1)} \frac{1-q^{(-d/2)(k-d/2+1)(x+1)}}{1-q^{(-d/2)(k-d/2+1)}}$$
$$= q^{(v-k)(k-d/2+1)} \frac{q^{d/2(k-d/2+1)} - q^{d/2(k-d/2+1)(-x)}}{q^{d/2(k-d/2+1)}-1}$$
$$= \frac{q^{(v-k+d/2)(k-d/2+1)} - q^{(v-k-xd/2)(k-d/2+1)}}{q^{d/2(k-d/2+1)}-1}.$$

For the second sum, we have 0 if $x = y$ and else we apply also the geometric series to get:

$$q^{k(v-k-d/2+1)} \sum_{i=x+1}^{y} \left(q^{k(-d/2)}\right)^i = q^{k(v-k-d/2+1)} \frac{q^{k(-d/2)(x+1)} - q^{k(-d/2)(y+1)}}{1-q^{k(-d/2)}}$$
$$= q^{k(v-k-d/2+1)} \frac{q^{kd/2(-x)} - q^{kd/2(-y)}}{q^{kd/2}-1} = \frac{q^{k(v-k+1-d/2(x+1))} - q^{k(v-k+1-d/2(y+1))}}{q^{kd/2}-1}.$$

Moreover, note that C contains a LMRD and hence its cardinality is restricted by Theorem 56 and Proposition 99 and particularly, its minimum distance is equal to d.

This results in the following

58 **Theorem (cf. [Tra13a, Corollary 6])**
For q prime power and integers v, d, and k with $2 \le d/2 \le k \le v-k$ as well as $x = \lfloor (v-2k)/(d/2) \rfloor$ and $y = \lfloor (v-k-d/2+1)/(d/2) \rfloor$ we have:

$$\begin{aligned} \mathrm{A}_q(v,d;k) \ge\; & \frac{q^{(v-k+d/2)(k-d/2+1)} - q^{(v-k-xd/2)(k-d/2+1)}}{q^{d/2(k-d/2+1)}-1} \\ & + \mathbb{1}_{x<y} \frac{q^{k(v-k+1-d/2(x+1))} - q^{k(v-k+1-d/2(y+1))}}{q^{kd/2}-1} \\ & + \mathbb{1}_{d/2 \nmid v-k+1}. \end{aligned}$$

Fixing $d = 2k$, we derive another special case from the Echelon-Ferrers construction. Here, $x = \lfloor v/k \rfloor - 2$ and $z = \lfloor v/k \rfloor - 1$, i.e., $x+1 = z$, rendering y unnecessary. Then, by writing $r \equiv v \pmod k$ for $0 \le r < k$, we have $z = (v-r)/k - 1$ and particularly $kz = v-k-r$ and $xk = zk - k = v - 2k - r$. The first sum can be further evaluated to

$$\sum_{i=0}^{x} q^{v-k-ik} = \frac{q^v - q^{v-k-xk}}{q^k-1} = \frac{q^v - q^{v-k-v+2k+r}}{q^k-1} = \frac{q^v - q^{k+r}}{q^k-1}$$

The second sum becomes also easier by applying $r+1-k \le 0$:

$$\sum_{i=x+1}^{z} \lceil q^{k(v-2k-ik+1)} \rceil = \lceil q^{k(v-2k-zk+1)} \rceil = \lceil q^{k(v-2k-v+k+r+1)} \rceil = \lceil q^{k(r+1-k)} \rceil = 1.$$

Hence, the constructed code of the last paragraph has a size of

$$\frac{q^v - q^{k+r}}{q^k-1} + 1 = \frac{q^v - q^{k+r} + q^k - 1}{q^k-1}, \tag{4.1}$$

which is equal to Theorem 126 and is optimal if $[r]_q < k$, i.e., $\mathrm{A}_q(v,2k;k) = \frac{q^v - q^{k+r}}{q^k-1} + 1$ with $r \equiv v \pmod k$, $0 \le r < k$, and $[r]_q < k$, cf. Theorem 131.

The main ingredients of the last construction were pivot vectors with k consecutive ones. This can be improved by considering pivot vectors with at most *two* blocks of consecutive ones, such that these pivot vectors still have k ones in total. Although the maximum cardinality of FDRMCs is still an open question, the following lemma settles many cases.

59 Theorem ([ES09, Theorem 2], transposed version)
Let $\mathcal{F}$ be an $m \times \eta$, $m \leq \eta$, Ferrers diagram and δ a positive integer such that the uppermost $\delta - 1$ rows of $\mathcal{F}$ contain η dots. Then there is a FDRMC of cardinality $\sum_{i=\delta}^{m} r_i$ in $\mathbb{F}_q^{m\times\eta}$ for all $q \geq 2$ prime power, where r_i is the number of dots in the i-th row of $\mathcal{F}$ for $i \in \{1, \ldots, m\}$. This FDRMC size achieves the bound of Theorem 55.

In particular, for all integers $1 \leq \delta = d/2 \leq k - d/2$ there is a bound achieving FDRMC for $\mathcal{F} = \left(\begin{smallmatrix} A & B \\ & C \end{smallmatrix}\right)$ such that A, B, and C are full Ferrers diagrams with the shapes $(k - d/2) \times (\lambda d/2)$, $(k - d/2) \times (v - k - \lambda d/2)$, and $(d/2) \times (v - k - \lambda d/2)$ for $\lambda \in \{0, \ldots, \lceil 2(v - k)/d \rceil\}$.

60 Lemma
Let $q \geq 2$ be a prime power and $2 \leq d/2 \leq k \leq v - k$ integers. If additionally $d \leq k + 1$, then there is a $(v, N, d; k)_q$ CDC with

$$N = q^{(v-k)(k-d/2+1)} \frac{q^{(d/2)^2(M+1)} - 1}{q^{(d/2)^2} - 1} q^{-(d/2)^2 M}$$

with $M = \lceil 2(v - k)/d \rceil$.

Proof
Let $p_\lambda = (1_{k-d/2} 0_{\lambda d/2} 1_{d/2} 0_{v-k-\lambda d/2})$ for $\lambda \in \{0, \ldots, M\}$. Then $p_\lambda \in \mathbb{F}_2^v$ is of weight k for all $\lambda \in \{0, \ldots, M\}$ and $\mathrm{d_h}(p_\lambda, p_{\lambda'}) = d$ for all $\lambda \neq \lambda' \in \{0, \ldots, M\}$. Hence, p_λ gives rise to a Ferrers diagram with four blocks $\left(\begin{smallmatrix} A & B \\ & C \end{smallmatrix}\right)$ such that A, B, and C have the shapes $(k - d/2) \times (\lambda d/2)$, $(k - d/2) \times (v - k - \lambda d/2)$, and $(d/2) \times (v - k - \lambda d/2)$, respectively. A, B, and C are full Ferrers diagrams, i.e., using m and η of Theorem 59, we have $m = k$ and $\eta = v - k$ and therefore $m \leq \eta$. For $\delta = d/2$ the uppermost $\delta - 1$ rows have each η dots since $d \leq k + 1$ is equivalent to $d/2 - 1 \leq k - d/2$.

Consequently, the FDRMC corresponding to p_λ has the dimension $(d/2)(v-k-\lambda d/2) + (k - d + 1)(v - k)$ for all $\lambda \in \{0, \ldots, M\}$ and by Lemma 54 the CDC has cardinality

$$\begin{aligned} N &= \sum_{\lambda=0}^{M} q^{(d/2)(v-k-\lambda d/2)+(k-d+1)(v-k)} = q^{(v-k)(k-d/2+1)} \sum_{\lambda=0}^{M} q^{-(d/2)^2\lambda} \\ &= q^{(v-k)(k-d/2+1)} \frac{q^{-(d/2)^2(M+1)} - 1}{q^{-(d/2)^2} - 1} = q^{(v-k)(k-d/2+1)} \frac{q^{(d/2)^2(M+1)} - 1}{q^{(d/2)^2} - 1} q^{-(d/2)^2 M}. \quad \square \end{aligned}$$

Note that p_0 is the pivot vector of an LMRD and in fact the first factor of the cardinality, i.e., $q^{(v-k)(k-d/2+1)}$, is the size of an LMRD. Hence this construction improves on the size of an LMRD by a factor of $\frac{q^{(d/2)^2(M+1)}-1}{q^{(d/2)^2}-1} q^{-(d/2)^2 M}$.

Another construction of FDRMC is given by the next lemma. It will be applied to prove Lemma 97 and Lemma 98.

61 Lemma (cf. [Etz+16, Theorem 9])
Let A be an $[a \times a', l, d_a]_q$ and B a $[b \times b', l, d_b]_q$ rank metric code. Then there is an $[(a+b) \times (a'+b'), l, d_a + d_b]_q$ rank metric code such that each codeword contains a zero matrix of size $b \times a'$ in the bottom left corner.

5 The Coset Construction

The *coset construction* is a parameterized construction for CDCs. One property is that the minimum subspace distance of constructed sets can be bounded in terms of the parameters. Not surprisingly, the size of these sets is also dependent on the parameters and hence we try to create large codes with this new method. To achieve this, we show that it is possible to extend a given coset constructed set with another coset constructed set, depending on the parameterization of both codes, or an arbitrary codeword, only depending on its pivot vector. This allows to combine the coset construction with the Echelon-Ferrers construction, since the latter incorporates large sets of codewords having predefined pivot vectors.

The classical coset construction in [HK17c] generalizes [ES13, Construction III], which is only applicable for $(8, N, 4; 4)_q$ CDCs, to arbitrary parameters $(v_1 + v_2, N, d; k_1 + k_2)_q$ using two *blocks*. Here we describe an evolved version of this construction which involves an arbitrary number b of blocks for $(\sum_{i=1}^{b} v_i, N, d; \sum_{i=1}^{b} k_i)_q$ CDCs.

5.1 The coset construction

First, we need to introduce a *padding* for matrices which adds zero-columns into a given matrix. Let $M \in \mathbb{F}_q^{m\times n}$ be a matrix and $p \in \mathbb{F}_2^s$ be a vector for $n + \operatorname{wt}(p) = s$. $\varphi_p(M)$ is the matrix $M' \in \mathbb{F}_q^{m\times s}$ with

$$M'_i = \begin{cases} \mathbf{0}_{m\times 1} & \text{if } p_i = 1 \\ M_{i-\sum_{j=1}^{i} p_j} & \text{else} \end{cases}.$$

For example, we have $\varphi_{(010001)}((\begin{smallmatrix} 1&0&1&1 \\ 0&1&1&0 \end{smallmatrix})) = (\begin{smallmatrix} 1&0&0&1&1&0 \\ 0&0&1&1&0&0 \end{smallmatrix})$.

Next, for a positive integer b and $0 \le k_i \le v_i$ integers for $i \in [b]$, let $\mathcal{F}_{(k_i,v_i)_{i\in[b]}}$ be the Ferrers diagram consisting of k_i rows with $\sum_{j=i+1}^{b}(v_j - k_j)$ dots for each $i = 1, \ldots, b-1$, i.e.:

$$\mathcal{F}_{(k_i,v_i)_{i\in[b]}} = \begin{array}{cccc}
k_1\left\{\begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \underbrace{\bullet\dots\bullet}_{v_2-k_2}\end{array}\right. & \begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \bullet\dots\bullet\end{array} & & \begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \bullet\dots\bullet\end{array}\\
 & k_2\left\{\begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \underbrace{\bullet\dots\bullet}_{v_3-k_3}\end{array}\right. & & \begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \bullet\dots\bullet\end{array}\\
 & & \ddots & \vdots\\
 & & & k_{b-1}\left\{\begin{array}{c}\bullet\dots\bullet\\ \vdots\\ \underbrace{\bullet\dots\bullet}_{v_b-k_b}\end{array}\right.
\end{array}.$$

For $b \geq 1$, $C_i \in \begin{bmatrix}\mathbb{F}_q^{v_i}\\ k_i\end{bmatrix}$, $i = 1, \dots, b$, and M in an $(\mathcal{F}_{(k_i,v_i)_{i\in[b]}}, N, \delta)_q$ FDRMC ($1 \leq N$, $1 \leq \delta$), we introduce the abbreviation

$$C(C_1, \dots, C_b, M) :=$$
$$\begin{pmatrix}\tau(C_1) & & & \mathbf{0}\\ & \tau(C_2) & & \\ & & \ddots & \\ \mathbf{0} & & & \tau(C_b)\end{pmatrix} + \begin{pmatrix}\mathbf{0}_{(\sum_{i=1}^{b-1} k_i)\times v_1} & \varphi_{(\mathrm{p}(C_2)|\dots|\mathrm{p}(C_b))}(M)\\ & \\ \mathbf{0}_{k_b\times v_1} & \mathbf{0}_{k_b\times(\sum_{i=2}^{b} v_i)}\end{pmatrix}$$

which is the matrix in RREF that arises if one builds the diagonal block matrix with the RREF matrices corresponding to $C_1, \dots, C_b$ and embeds the Echelon-Ferrers diagram matrix M in the top right part with an embedding, such that the pivot columns of $C_2, \dots, C_b$ are also pivot columns in $C(C_1, \dots, C_b, M)$. Using this definition, $\mathcal{F}_{(k_i,v_i)_{i\in[b]}}$ is the Echelon-Ferrers diagram of $(1_{k_1} \mid \mathrm{p}(C_2) \mid \dots \mid \mathrm{p}(C_b))$, and it is in particular independent of $C_2, \dots, C_b$ for only their ambient space and subspace dimension is needed.

62 Lemma (Coset construction, cf. [HK17c, Lemma 3])
Let $q \geq 2$ be a prime power, l and b be positive integers, $1 \leq k_i \leq v_i$ for $i \in [b]$ be integers, $\emptyset \neq \mathcal{C}_i^j \subseteq \begin{bmatrix}\mathbb{F}_q^{v_i}\\ k_i\end{bmatrix}$ for $i \in [b]$ and $j \in [l]$ and $\mathcal{C}_i^j \cap \mathcal{C}_i^{j'} = \emptyset$ for $i \in [b]$ and $j \neq j' \in [l]$. Let $\mathcal{M}$ be a non-empty $(\mathcal{F}_{(k_i,v_i)_{i\in[b]}}, \#\mathcal{M}, 1)_q$ FDRMC. Then

$$\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}) := \dot{\bigcup}_{j\in[l]} \{\tau^{-1}(C(C_1, \dots, C_b, M)) \mid C_i \in \mathcal{C}_i^j\ \forall i \in [b], M \in \mathcal{M}\}$$

is a subset of $\begin{bmatrix}\mathbb{F}_q^{\sum_{i=1}^b v_i}\\ \sum_{i=1}^b k_i\end{bmatrix}$ of size $\#\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}) = \#\mathcal{M} \cdot \sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j$.

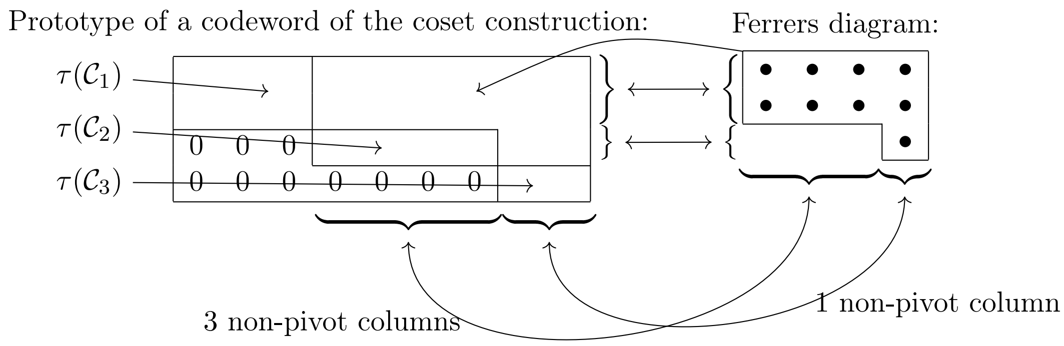


Figure 6: Prototype of a CDC codeword and connection to the Ferrers diagram in the setting of Example 63.

Proof

For a fixed $j \in [l]$ and $C_i \in \mathcal{C}_i^j$ for $i \in [b]$, $\tau(C_i)$ is a $k_i \times v_i$ matrix over $\mathbb{F}_q$ of rank k_i for all $i \in [b]$. For $M \in \mathcal{M}$, $\varphi_{(\mathrm{p}(C_2)|\ldots|\mathrm{p}(C_b))}(M)$ fits in terms of dimensions into the matrix $C(C_1, \ldots, C_b, M)$ and has zero columns to the top of the pivot columns of C_i for $2 \le i \le b$. Hence, $C(C_1, \ldots, C_b, M)$ has rank $\sum_{i=1}^b k_i$ and therefore $\tau^{-1}(C(C_1, \ldots, C_b, M))$ is a $\sum_{i=1}^b k_i$ dimensional subspace in $\mathbb{F}_q^{\sum_{i=1}^b v_i}$. Counting $\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M})$ completes the proof. $\square$

63 **Example**

Let $b = 3$ and $k_1 = 2$, $v_1 = 3$, $k_2 = 1$, $v_2 = 4$, and $k_3 = 1$, $v_3 = 2$. Then $\tau(\mathcal{C}_1)$ consists of 2×3 matrices, $\tau(\mathcal{C}_2)$ consists of 1×4 matrices, and $\tau(\mathcal{C}_3)$ consists of 1×2 matrices, such that each matrix has full (row) rank. Any CDC codeword, considered as matrix in RREF, which is constructed by the coset construction using these building blocks, has dimension 4×9 and full (row) rank. Figure 6 shows a graphical representation of such a codeword as RREF matrix and the relationship with a properly sized Ferrers diagram, i.e., in this example the Ferrers diagram partitions the number 9 into $4 + 4 + 1$ and has therefore shape 3×4.

The name *coset construction* reflects the fact that any vector $u = (\lambda_1, \ldots, \lambda_b) \cdot C(C_1, \ldots, C_b, M)$ with $\lambda_i \in \mathbb{F}_q^{k_i}$ for $i \in [b]$ is divided into parts which lie in cosets of $C_1, \ldots, C_b$. With $v_i' = \sum_{j=2}^{i-1} v_j + 1$, $v_i'' = \sum_{j=2}^{i} v_j$, and $o_i = (\lambda_1, \ldots, \lambda_b) \cdot \varphi_{\mathrm{p}(C_i)}(M_{*,(v_i', \ldots, v_i'')})$ for $i \in \{2, \ldots, b\}$ and $o_1 = 0$, we can split u into $(u_1 \mid \ldots \mid u_b)$ where $u_i = o_i + \lambda_i \cdot \tau(C_i)$ for $i \in [b]$. Hence, u_i is in the coset $o_i + C_i$ for $i \in [b]$.

The parameter l is called the *length* and $(\mathcal{C}_i^j)_{i,j}, \mathcal{M}$ are called *components* of the construction.

There are some special cases. If $b = 1$, then $\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}) = \dot{\bigcup}_{j \in [l]} \mathcal{C}_1^j$. If $k_i = v_i$ for an $\bar{i} \in [b]$, then $\mathcal{C}_{\bar{i}}^j = \{\tau^{-1}(I_{k_{\bar{i}}})\} = \{\mathbb{F}_q^{k_{\bar{i}}}\}$.

5.2 The minimum subspace distance of the coset construction and rearranging of the components

We can bound the subspace distance of the constructed code.

64 **Lemma (cf. [HK17c, Lemma 4])**
Let q, b, v_i, and k_i for $i \in [b]$ satisfy the conditions of Lemma 62, $C_i, C'_i \in \begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ for $i \in [b]$ and M, M' in an $(\mathcal{F}_{(k_i,v_i)_{i\in[b]}}, N, 1)_q$ FDRMC $(2 \le N)$.

1. If $p(C_i) = p(C'_i)$ for all $i \in [b]$, then

$$2\mathrm{d_r}(M, M') \le \mathrm{d_s}(C(C_1, \ldots, C_b, M), C(C'_1, \ldots, C'_b, M'))$$

with equality if $C_i = C'_i$ for all $i \in [b]$ and

2.

$$\sum_{i=1}^{b} \mathrm{d_s}(C_i, C'_i) \le \mathrm{d_s}(C(C_1, \ldots, C_b, M), C(C'_1, \ldots, C'_b, M')).$$

Proof
We use the reformulation

$$\mathrm{d_s}(C(C_1, \ldots, C_b, M), C(C'_1, \ldots, C'_b, M')) = 2\left(\mathrm{rk}\begin{pmatrix} C(C_1,\ldots,C_b,M) \\ C(C'_1,\ldots,C'_b,M') \end{pmatrix} - \sum_{i=1}^{b} k_i\right).$$

1. Let $p(C_i) = p(C'_i)$ for $i \in [b]$, then

$$\varphi_{(\mathrm{p}(C'_2)|\ldots|\mathrm{p}(C'_b))}(M') = \varphi_{(\mathrm{p}(C_2)|\ldots|\mathrm{p}(C_b))}(M')$$

and

$$\varphi_{(\mathrm{p}(C_2)|\ldots|\mathrm{p}(C_b))}(M') - \varphi_{(\mathrm{p}(C_2)|\ldots|\mathrm{p}(C_b))}(M) = \varphi_{(\mathrm{p}(C_2)|\ldots|\mathrm{p}(C_b))}(M' - M).$$

Moreover, $\tau(C'_i) - \tau(C_i)$ has zero columns at the positions of the ones of $\mathrm{p}(C_i)$ and we apply

$$\mathrm{rk}\begin{pmatrix} \mathbf{0}_1 & & A \\ & \ddots & \\ & & \mathbf{0}_b \end{pmatrix} \le \mathrm{rk}\begin{pmatrix} B_1 & & A \\ & \ddots & \\ & & B_b \end{pmatrix}$$

which is true for any choice of $A, B_1, \ldots, B_b$, using $\mathbf{0}$ as a zero matrix with appropriate dimension. Note that the rank of a matrix is invariant under permutations of rows or columns, respectively. Hence, the rank in the reformulation is equal to

$$\operatorname{rk}\begin{pmatrix} \tau(C_1) & \varphi_{(\mathrm{p}(C_2)|\dots|\mathrm{p}(C_b))}(M) \\ & \ddots \\ \mathbf{0} & \tau(C_b) \\ \tau(C_1')-\tau(C_1) & \varphi_{(\mathrm{p}(C_2)|\dots|\mathrm{p}(C_b))}(M'-M) \\ & \ddots \\ \mathbf{0} & \tau(C_b')-\tau(C_b) \end{pmatrix} = \operatorname{rk}\begin{pmatrix} I_{\sum_{i=1}^b k_i} & & \\ & B_1 & M'-M \\ \mathbf{0} & & \ddots \\ & & B_b \end{pmatrix}$$
$$\geq \sum_{i=1}^{b} k_i + \operatorname{rk}(M'-M).$$

We get the first part of the claim by inserting this in the reformulation.

2. Here, we apply $\operatorname{rk}(\begin{smallmatrix} X & \mathbf{0} \\ \mathbf{0} & Z \end{smallmatrix}) \leq \operatorname{rk}(\begin{smallmatrix} X & Y \\ \mathbf{0} & Z \end{smallmatrix})$ $b-1$ times, which is also true for all X, Y, Z of appropriate dimension. Hence, the rank in the reformulation can be bounded by

$$\geq \operatorname{rk}\begin{pmatrix} \tau(C_1) & \mathbf{0} \\ & \ddots \\ \mathbf{0} & \tau(C_b) \\ \tau(C_1') & \mathbf{0} \\ & \ddots \\ \mathbf{0} & \tau(C_b') \end{pmatrix} = \sum_{i=1}^{b} \operatorname{rk}\begin{pmatrix} \tau(C_i) \\ \tau(C_i') \end{pmatrix} = \sum_{i=1}^{b} (\mathrm{d_s}(C_i, C_i')/2 + k_i).$$

The last equality follows from $\mathrm{d_s}(C_i, C_i') = 2\left(\operatorname{rk}\begin{pmatrix} \tau(C_i) \\ \tau(C_i') \end{pmatrix} - k_i\right)$. Inserting this in the reformulation concludes the proof. □

It is also possible to deduce some constraints for the components of a coset construction, if the resulting code shall fulfill a given minimum distance.

65 **Lemma ([HK17c, Lemma 7])**
Under the same preconditions as Lemma 62 and $\mathbf{0} \in \mathcal{M}$, we have for all $i \in [b]$ and $j \in [l]$

$$\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M})) \leq \mathrm{D_s}(\mathcal{C}_i^j)$$

and

$$\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M})) \leq 2\mathrm{D_r}(\mathcal{M}).$$

Proof
For an $\bar{i} \in [b]$ and $\bar{j} \in [l]$ let $C_{\bar{i}} \neq C_{\bar{i}}' \in \mathcal{C}_{\bar{i}}^{\bar{j}}$ and $C_i \in \mathcal{C}_i^{\bar{j}}$ for $i \in [b]$, $i \neq \bar{i}$. Then

$$\mathrm{d_s}(C(C_1, \dots, C_{\bar{i}-1}, C_{\bar{i}}, C_{\bar{i}+1}, \dots, C_b, \mathbf{0}), C(C_1, \dots, C_{\bar{i}-1}, C_{\bar{i}}', C_{\bar{i}+1}, \dots, C_b, \mathbf{0})) = \mathrm{d_s}(C_{\bar{i}}, C_{\bar{i}}')$$

which is lower bounded by the minimum subspace distance, i.e., $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$.

For the second part, we take a $\bar{j} \in [l]$ and let $C_i \in \mathcal{C}_i^{\bar{j}}$ for $i \in [b]$ and $M \neq M' \in \mathcal{M}$. Then the equality in Lemma 64 shows

$$\mathrm{d_s}(C(C_1, \dots, C_b, M), C(C_1, \dots, C_b, M')) = 2\mathrm{d_r}(M, M')$$

which is again lower bounded by the minimum distance, completing the proof. □

Both, Lemma 64 and Lemma 65 together verify the intuition that the best choice for $\mathrm{D_r}(\mathcal{M})$ is $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))/2$ to achieve large codes. Moreover, both lemmata show that the best choice for $\mathrm{D_s}(\mathcal{C}_i^j)$ for any $i \in [b]$ and $j \in [l]$ is exactly $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$ and this automatically fulfills the Condition 2 in Lemma 64. Note that the left hand side of Condition 2 in Lemma 64, i.e., $\sum_{i=1}^b \mathrm{d_s}(C_i, C_i')$, is at least $2b$ for $C_i^j \in \mathcal{C}_i^j$ and $C_i^{j'} \in \mathcal{C}_i^{j'}$ for $i \in [b]$ and $j \neq j' \in [l]$. Hence, if both necessary conditions in Lemma 65 and the conditions of Lemma 62 are fulfilled we have $2b \leq \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$.

The next example shows that it is in general not feasible to lower bound the subspace distances of $\dot\bigcup_{j=1}^l \mathcal{C}_i^j$ in terms of $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$.

66 Example
Let $U_1 = \tau^{-1}\left(\begin{smallmatrix}1&0&1&0\\0&1&0&0\end{smallmatrix}\right)$, $U_2 = \tau^{-1}\left(\begin{smallmatrix}1&0&1&1\\0&1&0&1\end{smallmatrix}\right)$, and $U_3 = \tau^{-1}\left(\begin{smallmatrix}0&0&1&0\\0&0&0&1\end{smallmatrix}\right)$. Then with $b = 2$, $l = 3$, $\mathcal{M} = \{\mathbf{0}\}$, $\mathcal{C}_1^1 = \{U_1\}$, $\mathcal{C}_1^2 = \{U_2\}$, $\mathcal{C}_1^3 = \{U_3\}$, $\mathcal{C}_2^1 = \{U_1\}$, $\mathcal{C}_2^2 = \{U_3\}$, and $\mathcal{C}_2^3 = \{U_2\}$, the code constructed by Lemma 62 is $\mathcal{C} = \{W_1, W_2, W_3\}$ with $W_1 = \tau^{-1}\left(\begin{smallmatrix}U_1&\mathbf{0}\\\mathbf{0}&U_1\end{smallmatrix}\right)$, $W_2 = \tau^{-1}\left(\begin{smallmatrix}U_2&\mathbf{0}\\\mathbf{0}&U_3\end{smallmatrix}\right)$, and $W_3 = \tau^{-1}\left(\begin{smallmatrix}U_3&\mathbf{0}\\\mathbf{0}&U_2\end{smallmatrix}\right)$. Note that $\mathrm{d_s}(U_1, U_2) = 2$, $\mathrm{d_s}(U_1, U_3) = \mathrm{d_s}(U_2, U_3) = 4$, $\mathrm{d_s}(W_1, W_2) = \mathrm{d_s}(W_1, W_3) = 6$, and $\mathrm{d_s}(W_2, W_3) = 8$ and in particular we have $6 = \mathrm{D_s}(\mathcal{C}) \not\leq \sum_{i=1}^b \mathrm{D_s}\left(\dot\bigcup_{j=1}^l \mathcal{C}_i^j\right) = 2 + 2$.

Next, we will rearrange the components in order to construct larger codes. This may decrease the minimum subspace distance, as the following example shows.

67 Example
Continuing Example 66 with the permutations $\sigma_1 = () \in \mathcal{S}_{[3]}$ and $\sigma_2 = (2,3) \in \mathcal{S}_{[3]}$, we see that $\mathcal{C}((\mathcal{C}_{i,\sigma_i(j)})_{i,j}, \mathcal{M}) = \{W_1', W_2', W_3'\}$ with $W_1' = W_1$, $W_2' = \tau^{-1}\left(\begin{smallmatrix}U_2&\mathbf{0}\\\mathbf{0}&U_2\end{smallmatrix}\right)$, and $W_3' = \tau^{-1}\left(\begin{smallmatrix}U_3&\mathbf{0}\\\mathbf{0}&U_3\end{smallmatrix}\right)$. In particular $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_{i,\sigma_i(j)})_{i,j}, \mathcal{M})) = 4$, since $\mathrm{d_s}(W_1', W_2') = 4$ and $\mathrm{d_s}(W_1', W_3') = \mathrm{d_s}(W_2', W_3') = 8$.

Although permuting the components of a code of Lemma 62 may change the minimum distance, which is nevertheless lower bounded by $2b$, it can increase the size of constructed codes.

68 Lemma
Under the same preconditions as Lemma 62, $\#\mathcal{C}_i^1 \ge \#\mathcal{C}_i^2 \ge \ldots \ge \#\mathcal{C}_i^l$, and $\sigma_i \in \mathcal{S}_{[l]}$ arbitrary for all $i \in [b]$, we have

$$\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^{\sigma_i(j)} \le \sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^{j}.$$

Proof
For $X > x$ and $Y > y$ we have $XY + xy > Xy + xY$ since $XY + xy - Xy - xY = (X-x)(Y-y) > 0$. Hence, we can rearrange the factors while not decreasing the value of the sum. For $1 \le j < j' \le l$ let

- $X = \prod_{i \in [b], \sigma_i(j) < \sigma_i(j')} \#\mathcal{C}_i^{\sigma_i(j)}$,
- $y = \prod_{i \in [b], \sigma_i(j) > \sigma_i(j')} \#\mathcal{C}_i^{\sigma_i(j)}$,
- $x = \prod_{i \in [b], \sigma_i(j) < \sigma_i(j')} \#\mathcal{C}_i^{\sigma_i(j')}$, and
- $Y = \prod_{i \in [b], \sigma_i(j) > \sigma_i(j')} \#\mathcal{C}_i^{\sigma_i(j')}$.

Note that $\#\mathcal{C}_i^{\sigma_i(j)} \ge \#\mathcal{C}_i^{\sigma_i(j')} \Leftrightarrow \sigma_i(j) < \sigma_i(j')$. Applying the stated fact shows that $\sigma_i' \in \mathcal{S}_{[l]}$ defined as

$$\sigma_i'(w) = \begin{cases} \sigma_i(w) & \text{if } w \notin \{j, j'\} \\ \sigma_i(j) & \text{if } w \in \{j, j'\} \text{ and } \sigma_i(j) < \sigma_i(j') \\ \sigma_i(j') & \text{if } w \in \{j, j'\} \text{ and } \sigma_i(j) > \sigma_i(j') \end{cases}$$

for all $i \in [b]$ yields $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^{\sigma_i(j)} \le \sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^{\sigma_i'(j)}$. Performing this for all pairs j, j' with $1 \le j < j' \le l$ transforms σ_i into the identity for all $i \in [b]$. □

The next example shows that the coset construction is able to prove that some subspaces are feasible together in the same CDC, whereas the Echelon-Ferrers construction cannot deduce this fact. Note that CDCs with subspace distance 2 are well-known and considered trivial.

69 Example
Let $d \in \mathbb{Z}_{\ge 4}$ even, $b \in \mathbb{Z}_{\ge 2}$, $1 \le k_i \le v_i$ integers for $i \in [b]$, $A_1, A_1' \in \mathbb{F}_q^{(k_1-1)\times(v_1-k_1-1)}$, $A_i, A_i' \in \mathbb{F}_q^{k_i \times (v_i - k_i)}$ for $i \in [b] \setminus \{1\}$, $B_1, B_1' \in \mathbb{F}_q^{1 \times (v_1-k_1-1)}$, and M, M' in an

$(\mathcal{F}_{(k_i,v_i)_{i\in[b]}}, N, 1)_q$ FDRMC $(2 \le N)$ such that $\sum_{i=1}^{b} \mathrm{d_r}(A_i, A'_i) \ge d/2 - 1$. We define subspaces as follows:

$$C_1 = \begin{pmatrix} I_{k_1-1} & 0 & 0 & A_1 \\ \mathbf{0}_{1\times(k_1-1)} & 1 & 0 & B_1 \end{pmatrix}$$
$$C'_1 = \begin{pmatrix} I_{k_1-1} & 0 & 0 & A'_1 \\ \mathbf{0}_{1\times(k_1-1)} & 0 & 1 & B'_1 \end{pmatrix}$$

and for $2 \le i \le b$:

$$C_i = \begin{pmatrix} I_{k_i} & A_i \end{pmatrix}$$
$$C'_i = \begin{pmatrix} I_{k_i} & A'_i \end{pmatrix}.$$

Then, we have $\mathrm{d_h}(\mathrm{p}(\tau^{-1}(C(C_1,\ldots,C_b,M))), \mathrm{p}(\tau^{-1}(C(C'_1,\ldots,C'_b,M')))) = 2$ and hence both subspaces may not appear together in a non-trivial code constructed by the Echelon-Ferrers construction. But since $\mathrm{rk}\begin{pmatrix} C_1 \\ C'_1 \end{pmatrix} = k_1 + 1 + \mathrm{d_r}(A_1, A'_1)$ and $\mathrm{rk}\begin{pmatrix} C_i \\ C'_i \end{pmatrix} = k_i + \mathrm{d_r}(A_i, A'_i)$ for $i \in [b]$, we have $\mathrm{d_s}(\tau^{-1}(C(C_1,\ldots,C_b,M)), \tau^{-1}(C(C'_1,\ldots,C'_b,M'))) \ge \sum_{i=1}^{b} \mathrm{d_s}(C_i, C'_i) = \sum_{i=1}^{b} 2\left(\mathrm{rk}\begin{pmatrix} C_i \\ C'_i \end{pmatrix} - k_i\right) = 2\left(\sum_{i=1}^{b} \mathrm{d_r}(A_i, A'_i)\right) + 2 \ge d$ by Lemma 64.

5.3 Extending the coset construction

It is possible to extend a code which is created by the coset construction with further codewords by only considering their pivot columns. This is especially useful for the combination of the coset construction with the Echelon-Ferrers construction [ES09].

70 **Lemma (cf. [HK17c, Lemma 5])**
Under the same preconditions as Lemma 62 and with a subspace $U \le \mathbb{F}_q^{\sum_{i=1}^{b} v_i}$ such that

$$s_i = \sum_{\eta=\sum_{j=1}^{i-1} v_j + 1}^{\sum_{j=1}^{i} v_j} \mathrm{p}(U)_\eta$$

for $i \in [b]$, we have $\sum_{i=1}^{b} |k_i - s_i| \le \mathrm{d_s}(U, W)$ where $W \in \mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M})$.

Proof
Since $\mathrm{d_h}(a|a', b|b') = \mathrm{d_h}(a, b) + \mathrm{d_h}(a', b')$ and $\mathrm{d_h}(a, a') \ge \left| ||a||_1 - ||a'||_1 \right|$ for $a, b \in \mathbb{F}_2^\eta$ and $a', b' \in \mathbb{F}_2^\nu$, we have $\sum_{i=1}^{b} |k_i - s_i| \le \mathrm{d_h}(\mathrm{p}(U), \mathrm{p}(W)) \le \mathrm{d_s}(U, W)$ where the last inequality follows from Lemma 54. □

Two CDCs arising both by the coset constructions for different parameters can also be combined.

71 Lemma
Let $2 \le q$ prime power, $1 \le b^j$, and $1 \le k_i^j \le v_i^j$ ($v_1^j \ne 1$) be integers given for $i \in [b^j]$, $j \in [2]$ with $\sum_{i=1}^{b^1} v_i^1 = \sum_{i=1}^{b^2} v_i^2$.

Let W^j be a codeword of a CDC arising by an application of the coset construction with parameters q, b^j, k_i^j, v_i^j for $i \in [b^j]$ and $j \in [2]$. The other parameters and sets involved in both constructions may be arbitrary, as long as they fit in the preconditions of Lemma 62.

Let $N_i^j = \sum_{r=1}^{i} v_r^j$ for $i \in [b^j]$, $j \in [2]$, $\{M_1, \ldots, M_m\} = \{N_1^1, \ldots, N_{b^1}^1, N_1^2, \ldots, N_{b^2}^2\}$, such that $1 = M_0 < M_1 < \ldots < M_m$.

Let $x_i^j = \sum_{r=M_{i-1}}^{M_i} \mathrm{p}(W^j)_r$ for $i \in [m]$ and $j \in [2]$.

Then we have $\sum_{i=1}^{m} |x_i^1 - x_i^2| \le \mathrm{d_s}(W^1, W^2)$ and additionally $\max\{b^1, b^2\} \le m \le b^1 + b^2$, $0 \le x_i^j \le M_i - M_{i-1}$ for $i \in [m]$, $j \in [2]$, and $k_i^j = \sum_{r=1:N_{i-1}^j < M_r \le N_i^j}^{m} x_r^j$ for $i \in [b^j]$, $j \in [2]$ where we assume $N_0^j = 0$ for $j \in [2]$.

Proof
We have $\sum_{i=1}^{m} |x_i^1 - x_i^2| \le \mathrm{d_h}(\mathrm{p}(W^1), \mathrm{p}(W^2)) \le \mathrm{d_s}(W^1, W^2)$, where the last inequality follows from Lemma 54. The remaining statements follows simply by counting and using the definitions. □

The last lemma can be reformulated to a minimization problem, i.e.,

$$
\begin{aligned}
z^* = \min \sum_{i=1}^{m} |x_i^1 - x_i^2| & & \\
\text{st } k_i^j = \sum_{r=1:N_{i-1}^j < M_r \le N_i^j}^{m} x_r^j & & \forall i \in [b^j]\, \forall j \in [2] \\
0 \le x_i^j \le M_i - M_{i-1} & & \forall i \in [m]\, \forall j \in [2] \\
x_i^j \in \mathbb{Z} & & \forall i \in [m]\, \forall j \in [2],
\end{aligned}
$$

then $z^* \le \mathrm{d_s}(W^1, W^2)$.

An application of the triangle inequality in the special case of $b = 2$ will provide an explicit criterion.

72 Corollary (cf. [HK17c, Lemma 6])
Let $2 \le q$ prime power, $b^j = 2$, and $1 \le k_i^j \le v_i^j$ ($v_1^j \ne 1$) be integers given for $i, j \in [2]$ with $v_1^1 + v_2^1 = v_1^2 + v_2^2$. Additionally, we assume $v_1^1 \le v_1^2$.

Let W^j be a codeword of a CDC arising by an application of the coset construction with parameters q, b^j, k_i^j, v_i^j for $i, j \in [2]$, the other parameters and sets involved in both constructions may be arbitrary, as long as they fit in the preconditions of Lemma 62.

If $v_1^1 = v_1^2$, let $z = |k_1^1 - k_1^2| + |k_2^1 - k_2^2|$, else, i.e., $v_1^1 < v_1^2$, let $\alpha_1 = \max\{0, k_1^2 - v_1^2 + v_1^1\}$, $\beta_1 = \min\{v_1^1, k_1^2\}$, $\alpha_2 = \max\{0, k_2^1 - v_1^2 + v_1^1\}$, and $\beta_2 = \min\{v_2^2, k_2^1\}$, and

$$\begin{aligned} z_1 &= \min\{|x - k_1^1| + |x - (k_1^2 + k_2^2 - k_2^1)| : x \in \{\alpha_1, \beta_1, k_1^1\} \cap [\alpha_1, \beta_1]\}, \\ z_2 &= \min\{|x - k_2^2| + |x - (k_1^1 + k_2^1 - k_1^2)| : x \in \{\alpha_2, \beta_2, k_2^2\} \cap [\alpha_2, \beta_2]\}, \end{aligned}$$

and $z = \max\{z_1, z_2\}$. Then $z \le \mathrm{d_s}(W^1, W^2)$.

Proof

If $v_1^1 < v_1^2$, then we have, using the notation of Lemma 71:

$$\begin{aligned} \min\, & |x_1^1 - x_1^2| + |x_2^1 - x_2^2| + |x_3^1 - x_3^2| \\ \text{st}\, & k_1^1 = x_1^1, k_2^1 = x_2^1 + x_3^1, k_1^2 = x_1^2 + x_2^2, k_2^2 = x_3^2 \\ & 0 \le x_1^1, x_1^2 \le v_1^1, 0 \le x_2^1, x_2^2 \le v_1^2 - v_1^1, 0 \le x_3^1, x_3^2 \le v_2^2 \\ & x_1^1, x_2^1, x_3^1, x_1^2, x_2^2, x_3^2 \in \mathbb{Z}, \end{aligned}$$

which can be simplified to

$$\begin{aligned} = \min\, & |k_1^1 - x_1^2| + |k_2^1 - x_3^1 - k_1^2 + x_1^2| + |x_3^1 - k_2^2| \\ \text{st}\, & \max\{0, k_1^2 - v_1^2 + v_1^1\} \le x_1^2 \le \min\{v_1^1, k_1^2\} \\ & \max\{0, k_2^1 - v_1^2 + v_1^1\} \le x_3^1 \le \min\{v_2^2, k_2^1\} \\ & x_3^1, x_1^2 \in \mathbb{Z}. \end{aligned}$$

Note that $\max\{0, k_1^2 - v_1^2 + v_1^1\} \le \min\{v_1^1, k_1^2\}$ and $\max\{0, k_2^1 - v_1^2 + v_1^1\} \le \min\{v_2^2, k_2^1\}$. Using the triangle inequality, we can lower bound the objective in two ways:

1. $|k_2^1 - x_3^1 - k_1^2 + x_1^2| + |x_3^1 - k_2^2| \ge |x_1^2 - (k_1^2 + k_2^2 - k_2^1)|$ yields

$$\begin{aligned} \ge \min\, & |x_1^2 - k_1^1| + |x_1^2 - (k_1^2 + k_2^2 - k_2^1)| \\ \text{st}\, & \max\{0, k_1^2 - v_1^2 + v_1^1\} \le x_1^2 \le \min\{v_1^1, k_1^2\}, x_1^2 \in \mathbb{Z} \text{ and} \end{aligned}$$

2. $|k_1^1 - x_1^2| + |k_2^1 - x_3^1 - k_1^2 + x_1^2| \ge |x_3^1 - (k_1^1 + k_2^1 - k_1^2)|$ yields:

$$\begin{aligned} \ge \min\, & |x_3^1 - (k_1^1 + k_2^1 - k_1^2)| + |x_3^1 - k_2^2| \\ \text{st}\, & \max\{0, k_2^1 - v_1^2 + v_1^1\} \le x_3^1 \le \min\{v_2^2, k_2^1\}, x_3^1 \in \mathbb{Z}. \end{aligned}$$

In both cases, the objective is a convex function and hence its minimum is attained on the boundaries or the constant part intersected with the boundaries.

If $v_1^1 = v_1^2$, then we have, using the notation of Lemma 71:

$$\begin{aligned} \min\, & |x_1^1 - x_1^2| + |x_2^1 - x_2^2| \\ \text{st}\, & k_1^1 = x_1^1, k_2^1 = x_2^1, k_1^2 = x_1^2, k_2^2 = x_2^2 \\ & 0 \le x_1^1, x_1^2 \le v_1^1, 0 \le x_2^1, x_2^2 \le v_2^2 \\ & x_1^1, x_2^1, x_1^2, x_2^2 \in \mathbb{Z}, \end{aligned}$$

which is feasible with minimum $|k_1^1 - k_1^2| + |k_2^1 - k_2^2|$.

The conclusion follows in both cases from Lemma 71. □

5.4 Bounds and constructions for the components of the coset construction

The next lemmata show bounds on $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j$, which is one part that determines the size of codes which are constructed by Lemma 62. The other part is $\#\mathcal{M}$. Latter is studied in the literature [ES09; Etz+16; TR10], see also Chapter 4.

73 **Lemma (cf. [HK17c, Corollary 1])**
Under the same preconditions as Lemma 62 and $d \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$ we have:

1. $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j \le l \cdot \prod_{i=1}^{b} \mathrm{A}_q(v_i, d; k_i)$ and
2. $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j \le \begin{bmatrix} v_{\bar{i}} \\ k_{\bar{i}} \end{bmatrix}_q \cdot \prod_{i=1, i \ne \bar{i}}^{b} \mathrm{A}_q(v_i, d; k_i)$ for all $\bar{i} \in [b]$.

Proof
Using Lemma 65, we have $d \le \mathrm{D_s}(\mathcal{C}_i^j)$ for all $i \in [b]$ and $j \in [l]$. Hence, $\mathcal{C}_i^j$ is a $(v_i, \#\mathcal{C}_i^j, d_i^j; k_i)_q$ CDC with $d \le d_i^j$ and $\#\mathcal{C}_i^j \le \mathrm{A}_q(v_i, d_i^j; k_i) \le \mathrm{A}_q(v_i, d; k_i)$ for all $i \in [b]$, $j \in [l]$. Therefore we fix an $\bar{i} \in [b]$ and compute

$$\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j = \sum_{j=1}^{l} \left(\#\mathcal{C}_{\bar{i}}^j \prod_{i=1, i \ne \bar{i}}^{b} \#\mathcal{C}_i^j \right) \le \prod_{i=1, i \ne \bar{i}}^{b} \mathrm{A}_q(v_i, d; k_i) \cdot \sum_{j=1}^{l} \#\mathcal{C}_{\bar{i}}^j.$$

Hence, the first part results via

$$\prod_{i=1, i \ne \bar{i}}^{b} \mathrm{A}_q(v_i, d; k_i) \cdot \sum_{j=1}^{l} \#\mathcal{C}_{\bar{i}}^j \le \prod_{i=1, i \ne \bar{i}}^{b} \mathrm{A}_q(v_i, d; k_i) \cdot \sum_{j=1}^{l} \mathrm{A}_q(v_{\bar{i}}, d; k_{\bar{i}})$$

and the second part uses $\dot{\bigcup}_{j=1}^{l} \mathcal{C}_{\bar{i}}^j \subseteq \begin{bmatrix} \mathbb{F}_q^{v_{\bar{i}}} \\ k_{\bar{i}} \end{bmatrix}$ concluding the proof. □

Note that the upper bound of the first part of Lemma 73 is better than the second part of this lemma iff $l \cdot \mathrm{A}_q(v_{\bar{i}}, d; k_{\bar{i}}) < \begin{bmatrix} v_{\bar{i}} \\ k_{\bar{i}} \end{bmatrix}_q$ for all $\bar{i} \in [b]$.

Another upper bound is given by an optimal solution of a non-linear integer maximization problem.

74 Lemma
Let $b, l, b_i, u_i \in \mathbb{Z}_{\geq 1}$ with $l \leq b_i$ for $i \in [b]$. Then

$$x_i^* = (\underbrace{\underbrace{u_i, \ldots, u_i}_{\alpha_i^*}, \underbrace{\beta_i^*}_{1}, \underbrace{1, \ldots, 1}_{\gamma_i^*}}_{l})_{j \in [l]} \quad \forall i \in [b]$$

is an optimal solution for

$$\begin{aligned} \max \sum_{j=1}^{l} \prod_{i=1}^{b} x_{i,j} & \\ \text{st} \sum_{j=1}^{l} x_{i,j} \leq b_i & \qquad \forall i \in [b] \\ 1 \leq x_{i,j} \leq u_i & \qquad \forall i \in [b]\, \forall j \in [l] \\ x_{i,j} \in \mathbb{Z} & \qquad \forall i \in [b]\, \forall j \in [l] \end{aligned}$$

with either

- $\alpha_i^* = l - 1$, $\beta_i^* = u_i$, and $\gamma_i^* = 0$, if $lu_i \leq b_i$, or
- $\beta_i^* \equiv b_i + 1 - l \pmod{u_i - 1}$ and $1 \leq \beta_i^* \leq u_i - 1$, which is therefore unique, $\alpha_i^* = \frac{b_i + 1 - l - \beta_i^*}{u_i - 1}$, and $\gamma_i^* = l - 1 - \alpha_i^*$, if $b_i < lu_i$

for all $i \in [b]$.

Proof
This maximization problem is feasible since $x_{i,j} = 1$ for all $i \in [b]$ and $j \in [l]$ is feasible with objective value l and it is bounded since all variables are bounded. Therefore the maximum exists.

Let $x'_{i,j}$ for $i \in [b]$ and $j \in [l]$ denote an optimal solution.

Then $\sum_{j=1}^{l} x'_{i,j} = \min\{b_i, lu_i\}$ for $i \in [b]$ since otherwise at least one $x'_{i,j}$ could be increased while strictly increasing the objective value since all coefficients are positive, which is a contradiction to the optimality of $x'_{i,j}$.

Since for real-valued $a \leq A$ and $b \leq B$ we have $0 \leq (A - a)(B - b)$ and hence $Ab + aB \leq AB + ab$ we can assume wlog. that $x'_{i,1} \geq x'_{i,2} \geq \ldots \geq x'_{i,l}$ for $i \in [b]$.

Furthermore, since for real-valued $x \le X$ and $0 < \varepsilon$, as well as $a, a' \in \mathbb{R}$ we have $0 \le X\varepsilon - x\varepsilon$ and hence $Xa + xa' \le X(a+\varepsilon) + x(a'-\varepsilon)$ we can assume wlog. that all but at most one index $\bar{j}$ fulfill either $x'_{i,j} = 1$ or $x'_{i,j} = u_i$.

Hence, $(x'_{i,j})_{j\in[l]}$ has the form $(u_i, \ldots, u_i, \lambda, 1, \ldots, 1)$ with $1 \le \lambda \le u_i$, which is then defined via $\sum_{j=1}^{l} x'_{i,j} = \min\{b_i, lu_i\}$. In particular, this implies $\lambda \in \mathbb{Z}$ and $x^*_{i,j}$ as defined above is an optimal solution. □

75 Lemma
Under the same preconditions as Lemma 62 and $d \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$ we have:

$$\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j \le \max_{d \ge d_i \in 2\mathbb{Z}_{\ge 1}\ \forall i \in [b] \wedge l = \min\{\mathrm{A}_q(v_i, d_i; k_i) \mid i \in [b]\}} \sum_{j=1}^{l} \prod_{i=1}^{b} x_{i,j},$$

where the $x_{i,j}$ are given by Lemma 74 for $b_i = \mathrm{A}_q(v_i, d_i; k_i)$ and $u_i = \mathrm{A}_q(v_i, d; k_i)$ for $i \in [b]$.

Proof
The possible values for the length l are part of the stated optimization formulation. Note that smaller l would strictly decrease the maximum value and hence are omitted. For each $j \in [l]$ we have $\#\mathcal{C}_i^j \le \mathrm{A}_q(v_i, d; k_i) = u_i$ due to the lower bound for the minimum distance of Lemma 65. Applying Lemma 74 completes the proof. □

We need a technical lemma before we can state a lower bound.

76 Lemma (cf. [ES13, Lemma 5])
For positive integers m, n, and $d \le d'$ and $2 \le q$ prime power, any $[m \times n, \max\{m,n\}(\min\{m,n\} - d + 1), d]_q$ Gabidulin MRD code contains an $[m \times n, \max\{m,n\}(\min\{m,n\} - d' + 1), d']_q$ Gabidulin MRD code as subspace.

Proof
We can wlog. assume that $n \le m$ since the rank of a matrix is invariant under transposition and let $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ be the isomorphism between a finite field and the corresponding $\mathbb{F}_q$-vector space after choosing a basis. To ease the notation, we will apply φ component-wise.

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be $\mathbb{F}_q$-linear independent. We use $M_\kappa = \begin{pmatrix} g_1^{q^0} & g_2^{q^0} & \cdots & g_n^{q^0} \\ g_1^{q^1} & g_2^{q^1} & \cdots & g_n^{q^1} \\ & \vdots & & \\ g_1^{q^{\kappa-1}} & g_2^{q^{\kappa-1}} & \cdots & g_n^{q^{\kappa-1}} \end{pmatrix}$ for $\kappa \in \{k, k'\}$. Let $C = \mathbb{F}_{q^m}^k \cdot M_k$ such that $\varphi(C)$ is the $[m \times n, mk, d]_q$ Gabidulin MRD code with $k = n - d + 1$. Then with $C' = \mathbb{F}_{q^m}^{k'} \cdot M_{k'}$ the set $\varphi(C')$ is a $[m \times n, mk', d']_q$ Gabidulin MRD code with $k' = n - d' + 1$. Since $C' \le C$, the statement follows. □

77 **Lemma (cf. [HK17c, Lemma 13])**
Under the same preconditions as Lemma 62 and $d_1, \ldots, d_b$ even positive integers, there are sets $\mathcal{C}_i^j \subseteq \begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ for $i \in [b]$ and $j \in [l]$ such that

1. $d := \sum_{i=1}^b d_i$,
2. $d \le \mathrm{D_s}(\mathcal{C}_i^j)$ for $i \in [b]$ and $j \in [l]$,
3. $d_i \le \mathrm{D_s}(\dot\bigcup_{j=1}^l \mathcal{C}_i^j)$ for $i \in [b]$,
4. $d \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$ if $d \le \mathrm{D_r}(\mathcal{M})$,
5. $l = \min_{i=1}^b \{q^{\max\{k_i, v_i-k_i\}(d-d_i)/2}\} = q^{\min_{i=1}^b \{\max\{k_i,v_i-k_i\}(d-d_i)\}/2}$,
6. $\#\mathcal{C}_i^j = q^{\max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d/2+1)}$ for $i \in [b]$ and $j \in [l]$, and
7.
$$\begin{aligned}\sum_{j=1}^l \prod_{i=1}^b \#\mathcal{C}_i^j &= l \cdot \prod_{i=1}^b q^{\max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d/2+1)} \\ &= l \cdot q^{\sum_{i=1}^b \max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d/2+1)}.\end{aligned}$$

Proof
Let $L_i = \Lambda_{q,k_i,v_i-k_i}$ be the lifting map, which shall also be applied to sets via $L_i(S) = \{L_i(M) \mid M \in S\}$, for $i \in [b]$.

For each $i \in [b]$, we choose $\dot\bigcup_{j=1}^l \mathcal{C}_i^j \subseteq L_i(B_i)$ for a linear $[k_i \times (v_i - k_i), \max\{k_i, v_i - k_i\}(\min\{k_i, v_i-k_i\} - d_i/2+1), d_i/2]_q$ Gabidulin MRD code B_i and for each $j \in [l]$ we choose $\mathcal{C}_i^j$ specifically as lifting of different cosets of a linear $[k_i \times (v_i - k_i), \max\{k_i, v_i - k_i\}(\min\{k_i, v_i-k_i\} - d/2+1), d/2]_q$ Gabidulin MRD code B_i^j, which is chosen as subspace of B_i by Lemma 76.

Then, by Lemma 53 and $\mathrm{d_r}(A+C, B+C) = \mathrm{d_r}(A,B)$ for matrices $A, B, C \in \mathbb{F}_q^{a \times b}$, we have $d \le \mathrm{D_s}(\mathcal{C}_i^j)$ for $i \in [b]$, $j \in [l]$, $d_i \le \mathrm{D_s}(\dot\bigcup_{j=1}^l \mathcal{C}_i^j)$ for all $i \in [b]$, and by Lemma 64 we have $d \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$.

The length l of the construction is upper bounded by the number of cosets for each $i \in [b]$, i.e.,

$$l \le \frac{q^{\max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d_i/2+1)}}{q^{\max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d/2+1)}}$$

and aiming for large codes, we choose l to be as large as possible.

The size of each coset of B_i^j is $\#B_i^j = q^{\max\{k_i,v_i-k_i\}(\min\{k_i,v_i-k_i\}-d/2+1)}$, which is by definition also the size of $\mathcal{C}_i^j$ for all $i \in [b]$ and $j \in [l]$.

The final size results since the size of each coset is equal for each $j \in [l]$. $\square$

Another construction involves parallelisms and is able to attain the upper bound.

78 **Lemma (cf. [HK17c, Theorem 9])**
Under the same preconditions as Lemma 62, if there is a parallelism in $\begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ and $b \le k_i$ for all $i \in [b]$, there are sets $\mathcal{C}_i^j \subseteq \begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ for $i \in [b]$, $j \in [l]$ such that

1. $2b \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$ if $2b \le \mathrm{D_r}(\mathcal{M})$,
2. $l = \min_{i=1}^b \left\{ \frac{\begin{bmatrix} v_i \\ k_i \end{bmatrix}_q (q^{k_i}-1)}{q^{v_i}-1} \right\}$,
3. $\#\mathcal{C}_i^j = \frac{q^{v_i}-1}{q^{k_i}-1}$ for $i \in [b]$, $j \in [l]$,
4. $\sum_{j=1}^l \prod_{i=1}^b \#\mathcal{C}_i^j = l \cdot \prod_{i=1}^b \frac{q^{v_i}-1}{q^{k_i}-1}$, and
5. $\sum_{j=1}^l \prod_{i=1}^b \#\mathcal{C}_i^j$ attains both bounds of Lemma 73 with equality if $b = k_i$ for all $i \in [b]$.

Proof
Let P_i be a parallelism in $\begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ for $i \in [b]$. For each $i \in [b]$, we choose $\dot{\bigcup}_{j=1}^l \mathcal{C}_i^j \subseteq P_i$ and for each $j \in [l]$ we choose $\mathcal{C}_i^j$ as different spreads in P_i.

Then, $\mathrm{D_s}(\mathcal{C}_i^j) = 2k_i$ for $i \in [b]$ and $j \in [l]$, which upper bounds $\mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M})$ by Lemma 65. Since $2 \le \mathrm{D_s}(\dot{\bigcup}_{j=1}^l \mathcal{C}_i^j)$ for $i \in [b]$, Lemma 64 shows $2b \le \mathrm{D_s}(\mathcal{C}((\mathcal{C}_i^j)_{i,j}, \mathcal{M}))$.

Each $\mathcal{C}_i^j$ is a spread in $\begin{bmatrix} \mathbb{F}_q^{v_i} \\ k_i \end{bmatrix}$ and therefore has cardinality $\frac{q^{v_i}-1}{q^{k_i}-1}$ for $i \in [b]$ and $j \in [l]$. Hence, each P_i contains exactly $\frac{\begin{bmatrix} v_i \\ k_i \end{bmatrix}_q (q^{k_i}-1)}{q^{v_i}-1}$ spreads for all $i \in [b]$ and aiming for large codes, we choose $l \le \#P_i$ for $i \in [b]$ to be as large as possible.

For the last statement, we use $\mathrm{A}_q(\nu k, 2k; k) = \frac{q^{\nu k}-1}{q^k-1}$ for ν positive integer, cf. Corollary 125. Using Lemma 73 with $d = 2b$ directly yields the first upper bound. For the second upper bound we choose $\bar{i}$ such that $l = \#P_{\bar{i}}$. This concludes the proof. $\square$

5.5 Example of the coset construction: $(18, N, 6; 9)_2$ CDCs

The next example applies Lemma 78 to parallelisms in $\begin{bmatrix} \mathbb{F}_2^6 \\ 3 \end{bmatrix}$, which are the only known parallelisms with $k = 3$ and hence allow to choose $b = 3$.

	pivot vector	dimension of FDRMC	details if MRD
$s_1 = 6$	111111|111000|000000	63	9×9 MRD, the lifted MRD
	111111|000111|000000	54	
	111111|000000|111000	45	
	111111|000000|000111	36	6×9 MRD
$s_2 = 6$	111000|111111|000000	45	
	000111|111111|000000	36	9×6 MRD
	000000|111111|111000	9	9×3 MRD
	000000|111111|000111	6	6×3 MRD
$s_3 = 6$	111000|000000|111111	9	3×9 MRD
	000111|000000|111111	6	3×6 MRD
	000000|111000|111111	3	3×3 MRD
	000000|000111|111111	0	0×0 MRD

Table 5: Pivot vectors used by the Echelon-Ferrers construction for $(18, N, 6; 9)_2$ CDCs.

79 Example
Let $q = 2$, $b = 3$, $v_1 = v_2 = v_3 = 6$, and $k_1 = k_2 = k_3 = 3$.

Then we apply Lemma 78 to obtain $l = 155$, $\#\mathcal{C}_i^j = 9$ for $i \in [3]$, $j \in [155]$ and $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j = 155 \cdot 9^3 = 112\,995$.

Choosing an $(\mathcal{F}, 2^{15}, 3)_2$ FDRMC $\mathcal{M}$ with

$$\mathcal{F} = \begin{array}{cccccc} \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\ & & & \bullet & \bullet & \bullet \\ & & & \bullet & \bullet & \bullet \\ & & & \bullet & \bullet & \bullet \end{array}$$

is possible by Theorem 59 and even bound achieving by Theorem 55.

Putting both parts together, the coset construction in Lemma 62 yields an $(18, N, d; 9)_2$ CDC $\mathcal{C}_{\text{coset}}$ with $N = 112\,995 \cdot 2^{15} = 3\,702\,620\,160 \approx 2^{31.8}$ and $6 \leq d$.

N is small compared to the cardinality of an LMRD with parameters $(18, 2^{63}, 6; 9)_2$, but Lemma 70 with $s_1 = 6$, $s_2 = 3$, $s_3 = 0$, and $\sum_{i=1}^{b} |k_i - s_i| = 6$ shows that combining both codes is also feasible for these parameters.

More general, any subspace U with $\dim(U) = 9$ and $s_i = \sum_{\eta=6i-5}^{6i} \mathrm{p}(U)_\eta$ for $i \in [3]$ can be added to $\mathcal{C}_{\text{coset}}$ to build a $(18, N', 6; 9)_2$ CDC via Lemma 70 if $6 \leq |s_1 - 3| + |s_2 - 3| + |s_3 - 3|$, $s_1 + s_2 + s_3 = 9$, and $0 \leq s_i \leq 6$ for $i \in [3]$. This is fulfilled iff either $s_{\bar{i}} = 6$ for an $\bar{i} \in [3]$ or $\{s_1, s_2, s_3\} = \{0, 4, 5\}$. Hence a possibility to choose pivot vectors, fulfilling the constraints on s_1, s_2, and s_3, that additionally has a pairwise Hamming distance of at least 6 is shown in Table 5.

Note that the dimension of the three FDRMCs which are not rectangular MRD codes is determined exactly by Theorem 59.

This set of pivot vectors is the unique possibility if one iteratively and greedily takes the remaining pivot vectors according to the largest dimension.

Hence, combining the corresponding codewords of the Echelon-Ferrers construction with $\mathcal{C}_{\text{coset}}$ yields an $(18, N', 6; 9)_2$ CDC with $N' = 3\,702\,620\,160 + 2^{63} + 2^{54} + 2^{45} + 2^{36} + 2^{45} + 2^{36} + 2^{9} + 2^{6} + 2^{9} + 2^{6} + 2^{3} + 2^{0} = 9\,241\,456\,945\,250\,010\,249 \approx 9.24 \cdot 10^{18}$.

This is larger than the code constructed by the multicomponent construction of Theorem 58 ($\approx 9.22 \cdot 10^{18}$), the improved linkage construction of Theorem 136 ($\approx 9.22 \cdot 10^{18}$), or the construction in Lemma 60 ($2^{63-27} \cdot (2^{36}-1)/(2^{9}-1) = 9\,241\,421\,688\,455\,823\,360$).

The improved linkage construction builds an $(18, N, 6; 9)_2$ code with $N \le \max\{\mathrm{A}_2(m, 6; 9) \cdot 2^{9(16-m)} + \mathrm{A}_2(24-m, 6; 9) \mid m = 9, \ldots, 15\}$, which is upper bounded by $9\,223\,372\,124\,661\,828\,921 \approx 9.22 \cdot 10^{18}$, if one takes the exact value $\mathrm{A}_2(i, 6; 9) = 1$ for $9 \le i \le 11$, $\mathrm{A}_2(12, 6; 9) = 585$, and the Anticode bound in the remaining necessary cases: $\mathrm{A}_2(13, 6; 9) \le 319\,449$, $\mathrm{A}_2(14, 6; 9) \le 168\,823\,644$, and $\mathrm{A}_2(15, 6; 9) \le 87\,807\,053\,113$.

Note that Lemma 34 with $c = 2$, W the upper bound on the dimension of an FDRMC, cf. Theorem 55, $L = 48$, and $T = 60$ on the graph G, consisting of the 1200 pivot vectors with $s_{\bar{i}} = 6$ for an $\bar{i} \in [3]$ or $\{s_1, s_2, s_3\} = \{0, 4, 5\}$ such that two pivot vectors are connected with an edge iff their Hamming distance is at least 6, uses $3072 = \omega(G|_{V(l,t)}, w|_{V(l,t)}/l) < t/l - \#V/c = 3496$ and consequently any maximum weight clique in G has to contain a maximum weight clique on the seven pivot vectors with $60 \le W(.)$ (for $W(.)$ from Lemma 34), i.e., it has to contain the pivot vector of an LMRD. Applying this lemma again with $L = 40$ and $T = 52$ for the induced subgraph G' of (111111111000000000) with 947 vertices uses $3361 = \omega(G'|_{V(l,t)}, w|_{V(l,t)}/l) < t/l - \#V/c = 3623$ and hence any maximum weight clique contains in addition to the pivot vector of an LMRD also a maximum weight clique on the seven pivot vectors which have Hamming distance at least 6 to the pivot vector of an LMRD and $52 \le W(.)$, i.e, the pivot vector (111111000111000000). The 820 remaining pivot vectors in the induced subgraph G'' that have Hamming distance at least 6 to both forced pivot vectors in a maximum weight clique have all an upper bound on the dimension of their FDRMCs of 45 and the unweighted clique number of G'' is 16, i.e., any maximum weight clique in G'' is bounded by $2^{45} \cdot 16 = 2^{49}$ and hence any maximum weight clique in G is bounded by $2^{63} + 2^{54} + 2^{49} \approx 9.2419 \cdot 10^{18}$. This is therefore an upper bound on the size of any code constructed by the Echelon-Ferrers construction involving only these 1200 pivot vectors. The LMRD bound of Proposition 99 is not applicable for these parameters.

5.6 Algorithms and problem formulations for computing good components

The question how to find good components, i.e., components with large $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j$ while having a large minimum subspace distance, will be tackled in this section. First, an intuitive greedy version is presented which has the drawback that it may not find maximum cardinalities. Second, a formulation as weighted independent set with an additional restriction is shown that may be solved optimally by e.g. an integer linear programming approach.

5.6.1 Matroids and the Greedy algorithm in the setting of the coset construction

In order to choose the $\mathcal{C}_i^j$, one can apply a greedy like approach, i.e., take multiple CDCs in the same ambient space, until it suffices or there is no further fitting code. More detailed, fix a prime power $q \geq 2$, an positive integer b and $1 \leq k_i \leq v_i$ integers and even $d_i \geq 2$ for $i \in [b]$, and an even integral $d \geq 2$, such that $d \leq \sum_{i=1}^{b} d_i$. Then Algorithm 2 computes a selection of the components.

Algorithm 2 Greedy strategy for computing the components of the coset construction, cf. [HK17c, Algorithm 8].

procedure GreedyComponents(q, d, b, $v_1, \ldots, v_b$, $d_1, \ldots, d_b$, $k_1, \ldots, k_b$)
  for $i \in \{1, \ldots, b\}$ **do**
    $\mathcal{C}_i \leftarrow$ GreedyComponentsHelper(q, v_i, d, d_i, k_i)
  end for
  $l \leftarrow \min\{\mathcal{C}_i \mid i \in [b]\}$
  return $(\mathcal{C}_1, \ldots, \mathcal{C}_b)$, l
end procedure
procedure GreedyComponentsHelper(q, v, d, d', k)
  $\mathcal{R} \leftarrow \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$
  $j \leftarrow 0$
  while $\mathcal{R} \neq \emptyset$ **do**
    $j \leftarrow j + 1$
    select CDC $\mathcal{A}_j$ of maximum cardinality in $\mathcal{R}$ with $\mathrm{D_s}(\mathcal{A}_j) \geq d$
    $\mathcal{R} \leftarrow \{U \in \mathcal{R} \mid \mathrm{D_s}(\mathcal{A}_j \cup \{U\}) \geq d'\}$
  end while
  return $(\mathcal{A}_1, \ldots, \mathcal{A}_j)$
end procedure

Although this approach seems to be rather intuitive, it is in general not able to provide a choice of $(\mathcal{C}_i^j)_{i,j}$ that maximizes $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j$. This can be seen since the underlying structure is no matroid, cf. Definition 35. For prime power $q \geq 2$, integers $1 \leq k \leq v-1$, and even $d \geq 2$, we define $X := \{$ all CDCs in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with subspace distance d $\}$ and $I := \{$ disjoint subsets of X $\}$. Clearly, (X, I) is an independence system. For $U \neq W \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with $\mathrm{d_s}(U, W) \geq d$ we now have $\{U\}, \{W\}, \{U, W\} \in X$ and $\{\{U\}, \{W\}\}, \{\{U, W\}\} \in I$. Since it is not possible to add an element from $\{\{U\}, \{W\}\}$ to $\{U, W\}$ such that the resulting set is in I, the third property of Definition 35 is not fulfilled and (X, I) is no matroid. Therefore the greedy approach may not yield a solution of maximum size.

5.6.2 A clique formulation for the components

The inequality $\sum_{i=1}^{b} \mathrm{d_s}(C_i, C_i') \leq \mathrm{d_s}(C(C_1, \ldots, C_b, M), C(C_1', \ldots, C_b', M'))$ of Lemma 64 is fulfilled, if we choose even $d_i \geq 2$ for $i \in [b]$, such that the target minimum distance d

lower bounds $\sum_{i=1}^{b} d_i$ and in turn each d_i lower bounds $\mathrm{d_s}(C_i, C_i')$. Hence, after fixing the d_i, the problem to find $(\mathcal{C}_i^j)_{i,j}$ is decoupled into finding $(\mathcal{C}_i^j)_j$ for each $i \in [b]$. Moreover, $\dot{\bigcup}_{j\in[l]}\mathcal{C}_i^j$ is a $(v_i, N, d_i; k_i)_q$ CDC for suitable parameters. Therefore, we can start by taking an integer $1 \le \kappa_i \le \mathrm{A}_q(v_i, d; k_i)$, a $(v_i, \#\mathcal{A}_i, d_i; k_i)_q$ CDC $\mathcal{A}_i$, and split it into all cardinality restricted subsets $\mathcal{S}(\mathcal{A}_i, \kappa_i) = \{U \subseteq \mathcal{A}_i \mid \#U \le \kappa_i \wedge d \le \mathrm{D_s}(U)\}$. Then, any $\dot{\bigcup}_{j\in[l]}\mathcal{C}_i^j$ with $\#\mathcal{C}_i^j \le \kappa_i$ is equivalent to a clique in a graph having vertex set $\mathcal{S}(\mathcal{A}_i, \kappa_i)$. Two vertices $S_1 \neq S_2$ are connected with an edge iff $S_1 \cap S_2 = \emptyset$. The goal is to maximize the weighted clique, where the weights are given by the cardinalities of the vertices and that the length l of the coset construction restricts the number of vertices in the clique. One possibility is to involve `Cliquer` [NÖ03]. Another possibility is to utilize a BLP:

$$
\begin{aligned}
\max \sum_{S\in\mathcal{S}(\mathcal{A}_i,\kappa_i)} & \#S \cdot x_S & \\
\text{st} \sum_{S\in\mathcal{S}(\mathcal{A}_i,\kappa_i)} & x_S = l & \\
& x_{S_1} + x_{S_2} \le 1 & \forall\ S_1 \neq S_2 \in \mathcal{S}(\mathcal{A}_i, \kappa_i) : S_1 \cap S_2 \neq \emptyset \\
& x_S \in \{0, 1\} & \forall\ S \in \mathcal{S}(\mathcal{A}_i, \kappa_i)
\end{aligned}
$$

Then we use Lemma 68 to combine cliques for different $i \in [b]$. Lemma 64 guarantees a minimum subspace distance of $\sum_{i=1}^{b} d_i \ge d$ for the coset constructed code that uses these cliques as components.

5.7 Further Examples

In this section, we apply the coset construction to some parameters in order to achieve or surpass the best known lower bound of $\mathrm{A}_q(v, d; k)$ at the time of the writing of the paper [HK17c].

5.7.1 $(8, N, 4; 4)_q$ CDCs

An improvement beyond the Echelon-Ferrers construction was Construction III in [ES13] giving $\mathrm{A}_2(8, 4; 4) \ge 4797$. The coset construction generalizes [ES13, Construction III]. Note that also [CP17, Theorem 4.1] achieves the same cardinality $N = q^{12} + \left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_q (q^2 + 1)q^2 + 1$ using a different approach, cf. [CPS18]. Moreover the code constructed in [ES13, Construction III], as well as our coset construction, contain an LMRD code and N is upper bound achieving, cf. Proposition 99.

We apply the coset construction with $q \ge 2$ prime power, $b = 2$, $k_1 = k_2 = 2$, and $v_1 = v_2 = 4$. Since $\left[\begin{smallmatrix}\mathbb{F}_q^4\\2\end{smallmatrix}\right]$ admits parallelisms (cf. Page 39), we therefore use Lemma 78 to obtain $l = \frac{\left[\begin{smallmatrix}4\\2\end{smallmatrix}\right]_q}{q^2+1} = q^2 + q + 1$ and sets $\mathcal{C}_i^j$, $i \in [b]$ and $j \in [l]$, each of size $q^2 + 1$. Moreover, since $b = 2$ the FDRMC part of the construction is in fact an ordinary $(2 \times 2, q^2, 2)_q$ MRD code. Hence, the coset construction produces an $(8, q^2(q^2+q+1)(q^2+1)^2, 4; 4)_q$ CDC $\mathcal{C}_{\text{coset}}$. Now we apply Lemma 70 for codewords having a pivot vector of (11110000) or (00001111).

Since both have a Hamming distance of at least 4 to any codeword in $\mathcal{C}_{\text{coset}}$ and have Hamming distance of 8 with each other, we can extend $\mathcal{C}_{\text{coset}}$ with an $(8, q^{12}, 4; 4)_q$ LMRD and the single codeword $\tau^{-1}(\mathbf{0}_{4\times 4} \mid I_4)$ to get an $(8, q^{12}+q^2(q^2+q+1)(q^2+1)^2+1, 4; 4)_q$ CDC.

5.7.2 $(3k, N, 2k; k+1)_q$ CDCs

80 **Theorem (cf. [HK17c, Theorem 11])**
Let $q \geq 2$ be a prime power and $k \geq 3$ an integer. Then $\mathrm{A}_q(3k, 2k; k+1) \geq q^{4k-2}+q^k+1$. This achieves the bound for CDCs that contain an LMRD of Proposition 99.

Proof
Apply the coset construction with $b = 2$, $k_1 = 1$, $d_1 = 2$, $v_1 = k+1$, $k_2 = k$, $d_2 = 2k-2$, and $v_2 = 2k-1$. Then $\mathrm{A}_q(k+1, 2; 1) = \left[\begin{smallmatrix} k+1 \\ 1 \end{smallmatrix}\right]_q = \frac{q^{k+1}-1}{q-1}$ and using orthogonality $\mathrm{A}_q(2k-1, 2k-2; k) = \mathrm{A}_q(2k-1, 2k-2; k-1)$ which is the maximum size of a partial spread with $2k-1 \equiv 1 \pmod{k-1}$, i.e., it is known to be $\frac{q^{2k-1}-q}{q^{k-1}-1} - q + 1 = q^k + 1$ (cf. Theorem 126). Since $q^k + 1 < \frac{q^{k+1}-1}{q-1}$, we can choose $l = 1$, $\mathcal{C}_1^1 = \{U\}$ with an $U \in \left[\begin{smallmatrix} \mathbb{F}_q^{k+1} \\ 1 \end{smallmatrix}\right]$, a $(2k-1, q^k+1, 2k-2; k)_q$ CDC $\mathcal{C}_2^1$ and an MRD code $(1 \times (k-1), 1, k)_q$ for $\mathcal{M}$, i.e., $\mathcal{M} = \{\mathbf{0}_{1\times(k-1)}\}$. Using the coset construction and Lemma 64, this produces a $(3k, q^k+1, 2k; k+1)_q$ CDC $\mathcal{C}_{\text{coset}}$. Using Lemma 70, the common pivot vector of an LMRD, i.e., $(1_{k+1}0_{2k-1})$ has a Hamming distance of $2k$ to any pivot vector of a subspace in $\mathcal{C}_{\text{coset}}$, the code $\mathcal{C}_{\text{coset}}$ can be extended with any $(3k, q^{4k-2}, 2k; k+1)_q$ LMRD. □

For $k = 3$ is this:

81 **Corollary (cf. [HK17c, Theorem 10])**
Let $q \geq 2$ be a prime power. Then $\mathrm{A}_q(9, 6; 4) \geq q^{10} + q^3 + 1$ and this achieves the bound for CDCs that contain an LMRD of Proposition 99.

5.7.3 $(10, 4173, 6; 4)_2$ CDCs

The coset construction is able to utilize the previously found $(6, 77, 4; 3)_2$ CDCs of [HKK15] to produce a $(10, 4173, 6; 4)_2$ CDC. We apply the search strategy of Section 5.6.2 to find distinct sets inside of a $(6, 77, 4; 3)_2$ code.

82 **Theorem ([HKK15, Theorem 1 and Table 6])**
$\mathrm{A}_2(6, 4; 3) = 77$ and there exist exactly 5 isomorphism classes of optimal $(6, 77, 4; 3)_2$ CDCs under the action of $\mathrm{GL}(\mathbb{F}_2^6)$.

type	size automorphism group	duality respective π
A	168	self-dual
B	48	self-dual
C	2	self-dual
D	2	dual of E
E	2	dual of D

A simple computation shows that the size of a maximum subset of a $(6, 77, 4; 3)_2$ CDC of type B, C, D or E, having subspace distance of 6, is at most 5. In the case of type A, it is however 7. More precisely let $\mathcal{A}$ be a $(6, 77, 4; 3)_2$ CDC of type A and $\mathcal{S}_i = \{\mathcal{U} \subseteq \mathcal{A} \mid \#\mathcal{U} = i \wedge 6 \le \mathrm{D_s}(U)\}$. Then another simple calculation computes all the sets in $\mathcal{S}_i$ for all $i \in [9]$. Their cardinalities are:

$i =$	1	2	3	4	5	6	7	8	$9 = \mathrm{A}_2(6, 6; 3)$
$\#\mathcal{S}_i =$	77	840	2240	1792	560	112	16	0	0

Applying and extending the coset construction yields a $(10, 4173, 6; 4)_2$ CDC that surpasses any CDC that the Echelon-Ferrers construction produces: An extensive computer search shows that the Echelon-Ferrers construction yields codes of maximum size 4167 in this case.

83 **Theorem (cf. [HK17c, Theorem 13])**
$\mathrm{A}_2(10, 6; 4) \ge 4173$ and this achieves the LMRD bound of Proposition 99.

Proof
First, the coset construction produces a $(10, 76, 6; 4)_2$ CDC $\mathcal{C}_{\text{coset}}$. Therefore, we choose $b = 2$, $k_1 = 1$, $d_1 = 2$, $v_1 = 4$, $k_2 = 3$, $d_2 = 4$, and $v_2 = 6$. Since $\mathrm{A}_2(4, 2; 1) = \left[{4 \atop 1}\right]_2 = 15$, we have $l \le 15$. Applying the search strategy of Section 5.6.2 allows to split the $(6, 77, 4; 3)_2$ CDC $\mathcal{C}$ of type A into 15 pairwise disjoint subsets of cardinality $7^2 5^{10} 4^3$. Hence, fixing $l = 15$, choosing $\mathcal{C}_1^j = \{U_j\}$ for different $U_j \in \begin{bmatrix} \mathbb{F}_2^4 \\ 1 \end{bmatrix}$ $(j \in [l])$, and $\mathcal{C}_2^j$ specifically as these 15 distinct subsets in $\mathcal{C}$ for $j \in [l]$, we have $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j = 7 \cdot 2 + 5 \cdot 10 + 4 \cdot 3 = 76$. $\mathcal{M}$ is an ordinary $(1 \times 3, 1, 3)_2$ MRD, i.e., $\mathcal{M} = \{\mathbf{0}_{1 \times 3}\}$. Hence, the coset construction in Lemma 62 and Lemma 64 yield a $(10, 76, 6; 4)_2$ CDC $\mathcal{C}_{\text{coset}}$. The Hamming distance between (1111000000) and the pivot vector of an arbitrary subspace in $\mathcal{C}_{\text{coset}}$ is exactly 6 and using Lemma 70 any $(10, 2^{12}, 6; 4)_2$ LMRD is a feasible extension for $\mathcal{C}_{\text{coset}}$. A computer search showed that this extended $(10, 2^{12} + 76, 6; 4)_2$ CDC is not maximal and can be further extended by another codeword, yielding an $(10, 4173, 6; 4)_2$ CDC. □

If we take subsets of an $(6, 77, 4; 3)_2$ CDC of type B, C, D or E, we have at most $\sum_{j=1}^{l} \prod_{i=1}^{b} \#\mathcal{C}_i^j \le l \cdot 5 \le 15 \cdot 5 = 75$, which is too small compared to the target cardinality of 76. The last extension by one subspace cannot be achieved if one only considers pivot vectors, since any possible pivot vector either has Hamming distance of at most 4 to a codeword in $\mathcal{C}_{\text{coset}}$ or has Hamming distance of 0 to any codeword in an LMRD.

A possible start to generalize this to $(10, N, 6; 4)_q$ is again to take $b = 2$, $k_1 = 1$, $d_1 = 2$, $v_1 = 4$, $k_2 = 3$, $d_2 = 4$, and $v_2 = 6$. Then $l = \left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_q = q^3 + q^2 + q + 1$ and $\mathcal{C}_1^j = \{U_j\}$ for different $U_j \in \left[\begin{smallmatrix}\mathbb{F}_q^4\\1\end{smallmatrix}\right]$ for $j \in [l]$. In [HKK15, Theorem 2 and Section 4], the $(6, 77, 4; 3)_2$ CDC of type A was generalized to a $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ CDC for all prime powers $q \geq 2$. This seems to be the canonical choice for the CDC that shall be split into l subsets. This last step has to be performed analytically, since even for $q = 3$ it contains already 754 subspaces and enumerating all subsets up to cardinality $\kappa \leq \mathrm{A}_q(6, 6; 3) = q^3 + 1$ is computationally infeasible.

6 The LMRD bound and naturally arising code constructions

In this chapter, we study a bound for constant dimension codes which contain a lifted maximum rank distance code. This particular bound is therefore called LMRD bound, cf. Proposition 99. At first, there were two LMRD bounds, each for disjoint but small sets of parameters, introduced by Etzion and Silberstein in [ES13, Theorems 10 and 11]. The results of this chapter, which were previously published in [Hei18], generalize both bounds to one single bound, while increasing the range of applicable parameters such that [ES13, Theorems 10 and 11] arise as special cases.

Analogously to the style of the tables in `http://subspacecodes.uni-bayreuth.de`, cf. [Hei+16], Figure 7 visualizes for fixed q and v the parameter regions of d and k in which which if clause of Proposition 99 is applicable.

First, we will generalize [ES13, Theorem 10] in Proposition 88 and [ES13, Theorem 11] in Proposition 91 respectively, the latter in a parameterized scheme. Second, we will show the optimal choice for parameters of Proposition 91 and also the superiority of Proposition 88 compared to Proposition 91, where both are applicable. Last, the proof of Proposition 88 can be exploited to get a new code construction. The codewords of a given CDC can be extended such that the arising new CDC is compatible to any LMRD in higher ambient space dimension. Note that the beauty lies in the fact that this new CDC is compatible to any LMRD having the same parameters q, v, d, and k and therefore the usually hard question how to combine CDCs or which CDCs are compatible is trivial in our setting.

Since the writing of [ES13] there are some works that can profit of a generalized LMRD bound. First of all Etzion asked in Research Problem 5 of his survey of 100 open problems [Etz13] and the authors of [HK17c] asked in the conclusion for a generalization of the LMRD bound. Next the expurgation-augmentation method of Honold et al. [AHL16; LH14] often surpasses the LMRD bound and is therefore stronger than all constructions that include an LMRD as subset. The homepage `http://subspacecodes.uni-bayreuth.de`, cf. [Hei+16] lists some explicit calculations of lower and upper bounds and particularly the LMRD bound for small parameters, i.e., $q \le 9$ and $v \le 19$. Finally, there are multiple papers that use the LMRD bound and can profit of this generalization [ES16; HK17a; HK17b; HKK15; ST13; ST15].

By

$$\Gamma_{q,k,v} = \tau^{-1}(\mathbf{0}_{(v-k)\times k} \mid I_{v-k})$$

we denote the $(v-k)$-dimensional subspace of V that contains all vectors which start

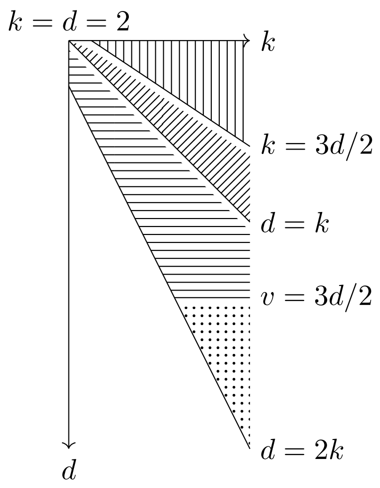


Figure 7: For fixed q and v the image shows the general knowledge about LMRD bounds in analogy to the tables in `http://subspacecodes.uni-bayreuth.de`, cf. [Hei+16]. From top to bottom: No LMRD bound is known for parameters in the area with vertical lines (|||), Below, for parameters in (////) the tightest currently known LMRD bound is Theorem 91. For parameters in (≡) Theorem 88 is the currently tightest LMRD bound, and the LMRD bound is trivial in the dotted area (⁝⁝⁝).

with k zeros. We use this to partition the vector space $V = \mathbb{F}_q^v$

$$V = \Gamma_{q,k,v} \dot\cup \Delta_{q,k,v}.$$

Hence, $\Delta_{q,k,v}$ contains all $q^v - q^{v-k}$ vectors of V whose first k entries are not 0_k each.

Note that the authors of [HKK15] denote $\Gamma_{q,k,v}$ *special flat* and that we drop the reference to q, v, and k if it is clear from the context, similarly to the definition of τ and p in Chapter 2.

6.1 Bounds on CDCs containing LMRDs

In general, any $(k - d/2 + 1)$-dimensional subspace of V is contained in at most one codeword of a $(v, \#C, d; k)_q$ CDC C. If C contains an LMRD M, then all $(k - d/2 + 1)$-subspaces in Δ are covered by codewords in M. More precisely:

84 Lemma ([ES13, Lemma 4])
Using $2 \leq d/2 \leq k \leq v - k$, each $(k - d/2 + 1)$-dimensional subspace of V, whose non-zero vectors are in Δ, is a subspace of exactly one element of a $(v, q^{(v-k)(k-d/2+1)}, d; k)_q$ LMRD code.

Proof
The number of $(k-d/2+1)$-dimensional subspaces in Δ is

$$\#\begin{bmatrix} V\backslash\Gamma \\ k-d/2+1 \end{bmatrix} = \begin{bmatrix} v\backslash v-k \\ k-d/2+1 \end{bmatrix}_q = q^{(v-k)(k-d/2+1)} \begin{bmatrix} k \\ k-d/2+1 \end{bmatrix}_q .$$

The cardinality of any LMRD code with these parameters is $q^{(v-k)(k-d/2+1)}$. It contains only non-zero vectors from Δ, and, since each $(k-d/2+1)$-dimensional subspace is contained in exactly one codeword while each k-dimensional subspace contains $\begin{bmatrix} k \\ k-d/2+1 \end{bmatrix}_q$ $(k-d/2+1)$-dimensional subspaces, the statement follows. □

85 Lemma
Any subspace U of V contains a $(\dim(U)-\dim(U\cap\Gamma))$-dimensional subspace, whose non-zero vectors are in Δ.

Proof
By definition of Δ all vectors in $U\setminus(U\cap\Gamma)$ are in Δ. Then by basis extension there is a $W \in \begin{bmatrix} U\backslash\Gamma \\ \dim(U)-\dim(U\cap\Gamma) \end{bmatrix}$ with $U = W \oplus (U\cap\Gamma)$ and $(W\setminus\{0\}) \subseteq \Delta$. □

These two lemmata will now show that CDCs containing LMRDs have to have a large intersection with Γ, which is of course not true for general CDCs.

86 Lemma
Using $2 \le d/2 \le k \le v-k$, any $(v, \#C, d; k)_q$ CDC C that contains an LMRD code M can be partitioned into

$$C = M \,\dot\cup\, \dot{\bigcup}_{t=d/2}^{k} S_t,$$

where $S_t = \{U \in C \mid \dim(U\cap\Gamma) = t\}$, and

$$\mathrm{d_s}(A\cap\Gamma, B\cap\Gamma) \ge \mathrm{d_s}(A,B) - 2k + a + b$$

for $A \in S_a$ and $B \in S_b$.

Proof
A subspace $U \in C$ with $\dim(U\cap\Gamma) \le d/2-1$ contains an at least $(k-d/2+1)$-dimensional subspace W with non-zero vectors in Δ via Lemma 85. Then Lemma 84 shows that $W_0 = \mathcal{H}_{k-d/2+1}(W)$ is contained in exactly one codeword in M, i.e., $U \in M$. Moreover, using the minimum distance, W_0 is in at most one element of C.

For $A \in S_a$ and $B \in S_b$ we have $\dim(A\cap B\cap\Gamma) \le \dim(A\cap B) = k - \mathrm{d_s}(A,B)/2$, hence $\mathrm{d_s}(A\cap\Gamma, B\cap\Gamma) = a + b - 2\dim(A\cap B\cap\Gamma) \ge \mathrm{d_s}(A,B) - 2k + a + b$. □

Note that $M = S_0$ and the inequality $\mathrm{d_s}(A \cap \Gamma, B \cap \Gamma) \geq \mathrm{d_s}(A, B) - 2k + a + b$ is also valid if A or B is in M.

Using this lemma, we can upper bound the size of a $(v, \#C, d; k)_q$ CDC C that contains an LMRD M, for $2 \leq d/2 \leq k \leq v - k$, via

$$\#C = \#M + \sum_{t=d/2}^{k} \#S_t = q^{(v-k)(k-d/2+1)} + \sum_{t=d/2}^{k} \#S_t.$$

The following trick may be observed in [AA09, Theorem 3].

87 Lemma
Let $l < 2m$ be an integer and $A_i \subseteq \begin{bmatrix} V \\ i \end{bmatrix}$ for $m \leq i \leq M$ such that $\mathrm{d_s}(U, W) \geq \dim(U) + \dim(W) - l$ for $U \neq W \in \bigcup_{i=m}^{M} A_i$. Then

$$\# \bigcup_{i=m}^{M} A_i \leq \mathrm{A}_q(v, 2m - l; m).$$

Proof
For each $m \leq i \leq M$, we define $B_i = \{\mathcal{H}_m(U) \mid U \in A_i\}$. Then the set $C = \bigcup_{i=m}^{M} B_i$ is a $(v, \# \bigcup_{i=m}^{M} A_i, 2m - l; m)_q$ CDC. The cardinality follows from the minimum distance, i.e., for $\tilde{U} \neq \tilde{W} \in C$ such that $U \in A_u$ yielded $\tilde{U}$ and $W \in A_w$ yielded $\tilde{W}$, we have $u + w - l \leq \mathrm{d_s}(U, W) = u + w - 2\dim(U \cap W) \Rightarrow \dim(\tilde{U} \cap \tilde{W}) \leq \dim(U \cap W) \leq l/2$ and $\mathrm{d_s}(\tilde{U}, \tilde{W}) = 2(m - \dim(\tilde{U} \cap \tilde{W})) \geq 2(m - l/2) > 0$. $\square$

Now we are ready to state the first LMRD bound:

88 Proposition (cf. [ES13, Theorem 10])
For $2 \leq d/2 \leq k \leq v - k$ and $k < d$ let C be a $(v, \#C, d; k)_q$ CDC that contains an LMRD code. Then

$$\#C \leq q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v - k, 2(d - k); d/2).$$

Proof
Let C_M be the LMRD code which is contained in C and $C = C_M \dot{\cup} \dot{\bigcup}_{t=d/2}^{k} S_t$ the partition of Lemma 86. Let $A_i = \{U \cap \Gamma \mid U \in S_i\} \subseteq \begin{bmatrix} \Gamma \\ i \end{bmatrix}$, $m = d/2$, $M = k$, and $l = 2k - d$. Then $k < d$ is equivalent to $l < 2m$ and we have $\mathrm{d_s}(U \cap \Gamma, W \cap \Gamma) \geq \mathrm{d_s}(U, W) - 2k + \dim(U \cap \Gamma) + \dim(W \cap \Gamma) \geq \dim(U \cap \Gamma) + \dim(W \cap \Gamma) - l$ by Lemma 86. In particular, $\dim(U \cap \Gamma) + \dim(W \cap \Gamma) - l \geq 2m - l > 0$ shows $\# \bigcup_{i=m}^{M} A_i = \# \bigcup_{i=m}^{M} S_i$. Applying Lemma 87 provides $\# \bigcup_{i=m}^{M} A_i \leq \mathrm{A}_q(\dim(\Gamma), 2m - l; m) = \mathrm{A}_q(v - k, 2(d - k); d/2)$, which completes the proof. $\square$

The special case of $d = 2(k-1)$ and $k \geq 3$ was already proved in [ES13, Theorem 10]. Next, we generalize [ES13, Theorem 11] and therefore need two technical lemmata.

89 Lemma
Let c, k, q, t, t_0, and y be integers, where q is a prime power, $y \neq 0$, and $c \leq k - t$ as well as $t_0 \leq t$. Then

$$\begin{bmatrix} k\backslash t_0 \\ c \end{bmatrix}_q \begin{bmatrix} t_0 \\ y \end{bmatrix}_q \leq \begin{bmatrix} k\backslash t \\ c \end{bmatrix}_q \begin{bmatrix} t \\ y \end{bmatrix}_q .$$

Proof
Since $t_0 = t$, $c < 0$, $y < 0$, $t_0 < y$ or $c = 0$ are obvious, we assume $1 \leq c$ and $1 \leq y \leq t_0 < t$. Using the reformulations from Definition 11, Lemma 2, and Lemma 5, we obtain

$$\frac{\begin{bmatrix} k\backslash t_0 \\ c \end{bmatrix}_q \begin{bmatrix} t_0 \\ y \end{bmatrix}_q}{\begin{bmatrix} k\backslash t \\ c \end{bmatrix}_q \begin{bmatrix} t \\ y \end{bmatrix}_q} q^{c(t-t_0)} = \frac{\begin{bmatrix} k-t_0 \\ c \end{bmatrix}_q \begin{bmatrix} t_0 \\ y \end{bmatrix}_q}{\begin{bmatrix} k-t \\ c \end{bmatrix}_q \begin{bmatrix} t \\ y \end{bmatrix}_q} = \frac{[k-t_0]_q![t_0]_q![k-t-c]_q![t-y]_q!}{[k-t]_q![t]_q![k-t_0-c]_q![t_0-y]_q!}$$

$$= \prod_{i=t_0+1}^{t} \frac{[k-i+1]_q[i-y]_q}{[k-i-c+1]_q[i]_q} \leq \prod_{i=t_0+1}^{t} \left(\frac{[k-i+1]_q}{[k-i-c+1]_q} q^{-y} \right).$$

Then, by abbreviating $g_i = k - i + 1 - c \geq 1$ for all $i \leq t$, we get

$$\frac{[g_i + c]_q}{[g_i]_q} \leq \frac{q^{g_i+c}}{q^{g_i} - 1} = q^c \frac{1}{1 - q^{-g_i}} \leq q^c \frac{1}{1 - q^{-1}} = q^c \frac{q}{q-1} \leq q^{c+1}.$$

Inserting this in the first inequality yields

$$\prod_{i=t_0+1}^{t} \left(\frac{[k-i+1]_q}{[k-i-c+1]_q} q^{-y} \right) \leq \prod_{i=t_0+1}^{t} \left(q^{c+1} q^{-y} \right) = q^{(c+1-y)(t-t_0)} \leq q^{c(t-t_0)},$$

which completes the proof. □

The restriction $t_0 \leq t$ is the reason for the fixation $t_0 = d/2$ later in this section.

90 Lemma
Using the notation of Lemma 86, let c, t, and y be integers with $0 \leq y \leq k$, $d/2 \leq t \leq k$, and $k - d/2 + 1 \leq c + y$. Let $N_{t,Y} = \{U \in S_t \mid Y \leq U\} = \mathcal{I}(S_t, Y)$ for each $Y \in \begin{bmatrix} \Gamma \\ y \end{bmatrix}$ with $0 \leq y \leq k$ and $d/2 \leq t \leq k$. Then:

$$\sum_{Y \in \begin{bmatrix} \Gamma \\ y \end{bmatrix}} \#N_{t,Y} = \#S_t \cdot \begin{bmatrix} t \\ y \end{bmatrix}_q .$$

Moreover for all $Y \in \begin{bmatrix} \Gamma \\ y \end{bmatrix}$:

$$\sum_{t=d/2}^{k-c} \#N_{t,Y} \cdot \begin{bmatrix} k\backslash t \\ c \end{bmatrix}_q \leq \begin{bmatrix} v\backslash v-k \\ c \end{bmatrix}_q .$$

Proof
The equation follows from double-counting the set $\{(Y,U) \in \left[{\Gamma \atop y}\right] \times S_t \mid Y \le U\}$.

For the inequality, we have 0 on the left hand side if $c < 0$ or $k - d/2 < c$, i.e., we assume $0 \le c \le k - d/2$. The statement follows from counting

$$\dot{\bigcup}_{t=d/2}^{k} \dot{\bigcup}_{U \in N_{t,Y}} \left[{U \backslash \Gamma \atop c}\right] \subseteq \left[{V \backslash \Gamma \atop c}\right].$$

The left hand side is disjoint, because for fixed Y there is, using $\dim(\langle Y, R\rangle) = y + c \ge k - d/2 + 1$, at most one element $W \in C$ with $\langle Y, R\rangle \le W$, where $R \in \left[{V \backslash \Gamma \atop c}\right]$.

Furthermore $\left[{U \backslash \Gamma \atop c}\right] = \emptyset$ for $k - c < t$ and $U \in N_{t,Y}$. □

Note that we use deliberately $t < y \le k$ with $N_{t,Y} = \emptyset$.

In particular, we have:

$$\#N_{t_0,Y} \le \frac{\left[{v \backslash v-k \atop c}\right]_q - \sum_{t=d/2, t \ne t_0}^{k-c} \#N_{t,Y} \cdot \left[{k \backslash t \atop c}\right]_q}{\left[{k \backslash t_0 \atop c}\right]_q}$$

for all integers c, t_0, and y with $0 \le y \le k$, $k - d/2 + 1 \le c + y$, $Y \in \left[{\Gamma \atop y}\right]$, and $d/2 \le t_0 \le k$, as well as $0 \le c \le k - t_0$.

In the successive discussion, we fix $t_0 = d/2$ (cf. Lemma 89), to ease the notation significantly while maintaining the same level of detail: The second summand of the last part of the proof of the next proposition would not vanish for other t_0.

Now we can state the second LMRD bound.

91 **Proposition (cf. [ES13, Theorem 11])**
For $2 \le d/2 \le k \le v - k$ let C be a $(v, \#C, d; k)_q$ CDC that contains an LMRD code for integers c and y, such that $1 \le y \le d/2$, $1 \le c \le \min\{k - d/2, d/2\}$, and $k - d/2 + 1 \le c + y$. Then

$$\#C \le q^{(v-k)(k-d/2+1)} + \frac{\left[{v-k \atop y}\right]_q \left[{k \atop c}\right]_q}{\left[{k-d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q} q^{c(v-k-d/2)} + \mathrm{A}_q(v-k, d-2(c-1); k-c+1).$$

Proof
Using Lemma 86 we only have to upper bound $\#S_{d/2} + \sum_{t=d/2+1}^{k} \#S_t$. Applying Lemma 90, we get:

$$\begin{aligned}\#S_{d/2} &= \frac{\sum_{Y \in \left[{\Gamma \atop y}\right]} \#N_{d/2,Y}}{\left[{d/2 \atop y}\right]_q} \le \sum_{Y \in \left[{\Gamma \atop y}\right]} \frac{\left[{v \backslash v-k \atop c}\right]_q - \sum_{t=d/2+1}^{k-c} \#N_{t,Y} \left[{k \backslash t \atop c}\right]_q}{\left[{k \backslash d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q} \\ &= \frac{\left[{v-k \atop y}\right]_q \left[{v \backslash v-k \atop c}\right]_q - \sum_{t=d/2+1}^{k-c} \#S_t \left[{t \atop y}\right]_q \left[{k \backslash t \atop c}\right]_q}{\left[{k \backslash d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q}.\end{aligned}$$

Hence

$$\#S_{d/2} + \sum_{t=d/2+1}^{k} \#S_t$$
$$\leq \frac{\left[{v-k \atop y}\right]_q \left[{v\backslash v-k \atop c}\right]_q}{\left[{k\backslash d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q} + \frac{\sum_{t=d/2+1}^{k-c} \#S_t \left(\left[{k\backslash d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q - \left[{t \atop y}\right]_q \left[{k\backslash t \atop c}\right]_q \right)}{\left[{k\backslash d/2 \atop c}\right]_q \left[{d/2 \atop y}\right]_q} + \sum_{t=k-c+1}^{k} \#S_t.$$

Now we apply Lemma 89 for $1 \leq y$, $t_0 = d/2$, and $d/2+1 \leq t \leq k-c$, and thereby upper bound the second summand with zero.

The last summand can be upper bounded by again utilizing Lemma 87 with $A_i = \{U \cap \Gamma \mid U \in S_i\} \subseteq \left[{\Gamma \atop i}\right]$, $m = k-c+1$, $M = k$, which is possible since $1 \leq c$, and $l = 2k-d$ (cf. Lemma 86), using $0 < 2m - l = d - 2(c-1) \Leftrightarrow c \leq d/2$. This upper bounds the last summand with $\mathrm{A}_q(v-k, d-2(c-1); k-c+1)$. □

The special case of $d = k$ even, $c = 1$, $y = d/2$ was already proved in [ES13, Theorem 11].

6.2 Comparison of the bounds

Having Proposition 88 and Proposition 91 at hand, we aim to clarify for which values of y and c Proposition 91 is best and, using this knowledge, we compare the strongest version of Proposition 91 with Proposition 88 to see that Proposition 88 is always stronger wherever the parameters q, v, d, and k allow the application of both bounds.

The easy part is to eliminate y in Proposition 91, since smaller $y(c)$ are always better.

92 Remark
Using $2 \leq d/2 \leq k \leq v-k$, the function $f(y) = \left[{v-k \atop y}\right]_q / \left[{d/2 \atop y}\right]_q = \prod_{i=0}^{y-1} \frac{q^{v-k}-q^i}{q^{d/2}-q^i}$ is monotonically increasing for $1 \leq y \leq d/2$. Hence, the optimal choice for y is $\max\{1, k-d/2+1-c\}$ for a fixed c, which implies $\max\{1, k-d+1\} \leq c \leq \min\{k-d/2, d/2\}$. Note that such a c exists iff $d/2 < k < 3d/2$.

Hence, the 2-dimensional polytope, in which the possible parameters (c, y) lie, therefore is only 1-dimensional, but $y(c)$ depends on c.

It is harder to find a good choice for c. Fortunately it suffices to consider the three summands in Proposition 91 separately and the first is independent of y and c. As we will see, a smaller c is better. Next, we compare the third summand of Proposition 91 for different c.

93 **Lemma (cf. Theorem 108 with $t = 1$ and $m = v$)**
For a prime power $q \geq 2$ and integers $v \geq 0$ and $k \neq 0$, we have

$$\mathrm{A}_q(v, d; k) \leq \mathrm{A}_q(v, d-2; k-1).$$

Proof
The statement is obvious for the separated cases $k < 0$, $v < k$, $2k < d$, $v \leq 1$, or $d \leq 2$. For odd d we can use $\tilde{d} = d+1$ due to $\mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d+1; k)$. Hence, we assume $2 \leq d/2 \leq k \leq v$ integers. We estimate the left hand side with the Singleton bound (Theorem 109) and the right hand side with the size of an LMRD code. Since both bounds depend on whether $k \leq v/2$, we have these three cases:

If $k \leq v/2$, then

$$\mathrm{A}_q(v, d; k) \leq \begin{bmatrix} v-d/2+1 \\ v-k \end{bmatrix}_q \leq \mu(q) q^{(v-k)(k-d/2+1)} \leq q^{(v-k+1)(k-d/2+1)} \leq \mathrm{A}_q(v, d-2; k-1),$$

which is true for $q \geq 3$, since $\mu(q) \leq q \leq q^{k-d/2+1}$, and $q = 2$ with $2 \leq k - d/2 + 1$. For $q = 2$ and $d = 2k$, the Singleton bound is $\begin{bmatrix} v-k+1 \\ 1 \end{bmatrix}_2 = 2^{v-k+1} - 1$ yielding the result.

If $v/2 \leq k-1$, then

$$\begin{aligned} \mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; v-k) &\leq \begin{bmatrix} v-d/2+1 \\ k \end{bmatrix}_q \leq \mu(q) q^{k(v-k-d/2+1)} \\ &\leq q^{(k-1)(v-k-d/2+3)} \leq \mathrm{A}_q(v, d-2; v-k+1) = \mathrm{A}_q(v, d-2; k-1), \end{aligned}$$

which is true, since $\mu(q) \leq q^2 \leq q^{3k-3-v+d/2}$, i.e., $v+5 \leq 2k+3 \leq 2k+1+d/2 \leq 3k+d/2$.

If v is odd and $k = (v+1)/2$, then

$$\begin{aligned} \mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; (v+1)/2) = \mathrm{A}_q(v, d; (v-1)/2) &\leq \begin{bmatrix} v-d/2+1 \\ (v+1)/2 \end{bmatrix}_q \\ &\leq \mu(q) q^{((v-1)/2-d/2+1)(v+1)/2} \leq q^{((v-1)/2-d/2+2)(v+1)/2} \\ &\leq \mathrm{A}_q(v, d-2; (v-1)/2) = \mathrm{A}_q(v, d-2; k-1), \end{aligned}$$

which is true for $3 \leq v$ since $\mu(q) \leq q^2 \leq q^{(v+1)/2}$. □

Next, we compare the second summand of Proposition 91 for different c, but thereby we have to consider the dependence of $y(c)$ of c:

94 **Lemma**
For integers c, d, k, q, v, and $y(c)$ such that $q \geq 2$ is a prime power, $2 \leq d/2 \leq k \leq v-k$ integers, $0 \leq c \leq k - d/2 - 1$, and $0 \leq y(c) \leq d/2$, let

$$f(c) = \frac{\begin{bmatrix} v-k \\ y(c) \end{bmatrix}_q \begin{bmatrix} k \\ c \end{bmatrix}_q}{\begin{bmatrix} k-d/2 \\ c \end{bmatrix}_q \begin{bmatrix} d/2 \\ y(c) \end{bmatrix}_q} q^{c(v-k-d/2)}.$$

If $y(c+1) = y(c)$ or $y(c+1) = y(c) - 1 \geq 0$, then $f(c) \leq f(c+1)$.

Proof
The term

$$\lambda = \frac{[d/2 - y(c)]_q!}{[d/2 - y(c+1)]_q!} \cdot \frac{[v-k-y(c+1)]_q!}{[v-k-y(c)]_q!}$$

is 1 if $y(c+1) = y(c)$ and

$$\frac{[v-k-y(c)+1]_q}{[d/2 - y(c)+1]_q} \le \mu(q) q^{v-k-d/2}$$

if $y(c+1) = y(c) - 1$. Using the q-factorial version of the q-binomial coefficient, one gets:

$$\begin{aligned}
\frac{f(c)}{f(c+1)} &= \frac{q^{k-d/2-c}-1}{q^{k-c}-1} \cdot q^{-(v-k-d/2)} \cdot \lambda \\
&\le q^{-d/2} \cdot q^{-(v-k-d/2)} \cdot \lambda \\
&\le \begin{cases} q^{-(v-k)} & \text{if } y(c+1) = y(c) \\ \mu(q) q^{-(d/2)} \le q^{2-(d/2)} & \text{else} \end{cases} \\
&\le 1
\end{aligned}$$

□

Since smaller values for y and c are preferable, we compare Proposition 88 with Proposition 91 to see that Proposition 88 is always tighter, if both are applicable. Since the size of the LMRD subcode is equal in both bounds, it remains to compare the second summand of Proposition 88 with the sum of the second and the third summand of Proposition 91. Luckily, a simplified estimation, only involving the second summand of Proposition 91 and a crude lower bound of $c = 1$, yields the desired result.

95 Lemma
Let d, k, q, and v be integers such that $q \ge 2$ is a prime power, $2 \le d/2 \le k \le v-k$, $k < d$, $1 \le k - d/2$, $c = 1$, and $y = k - d/2$. Then

$$\mathrm{A}_q(v-k, 2(d-k); d/2) \le \frac{\begin{bmatrix} v-k \\ y \end{bmatrix}_q \begin{bmatrix} k \\ c \end{bmatrix}_q}{\begin{bmatrix} k-d/2 \\ c \end{bmatrix}_q \begin{bmatrix} d/2 \\ y \end{bmatrix}_q} q^{c(v-k-d/2)}.$$

Proof
The right hand side is alwasy at least one by Lemma 5:

$$\begin{aligned}
&\frac{\begin{bmatrix} v-k \\ y \end{bmatrix}_q \begin{bmatrix} k \\ c \end{bmatrix}_q}{\begin{bmatrix} k-d/2 \\ c \end{bmatrix}_q \begin{bmatrix} d/2 \\ y \end{bmatrix}_q} q^{c(v-k-d/2)} = \frac{\begin{bmatrix} v-k \\ y \end{bmatrix}_q}{\begin{bmatrix} d/2 \\ y \end{bmatrix}_q} \frac{[k]_q}{[k-d/2]_q} q^{v-k-d/2} \\
&= \prod_{i=1}^{y} \frac{q^{v-k-y+i}-1}{q^{d/2-y+i}-1} \frac{[k]_q}{[k-d/2]_q} q^{v-k-d/2} \ge \prod_{i=1}^{y} q^{v-k-d/2} q^{d/2} q^{v-k-d/2} \ge q^{v-k} \ge 1.
\end{aligned}$$

Hence, we assume wlog. $2 \leq \mathrm{A}_q(v-k, 2(d-k); d/2)$ and in particular $3d/2 \leq v$ which allows in turn the application of the Singleton bound of Theorem 109:

$$\mathrm{A}_q(v-k, 2(d-k); d/2) \leq \begin{bmatrix} v-d+1 \\ v-k-d/2 \end{bmatrix}_q \leq \mu(q) q^{(v-k-d/2)(k-d/2+1)} \leq q^{(v-k-d/2)(k-d/2+1)+d/2}$$

$$= q^{(v-k-d/2)(k-d/2)} \cdot q^{d/2} \cdot q^{v-k-d/2} \leq \prod_{i=1}^{y} \frac{[v-k-y+i]_q}{[d/2-y+i]_q} \cdot \frac{[k]_q}{[k-d/2]_q} \cdot q^{v-k-d/2}$$

$$= \frac{[v-k]_q![k]_q![k-d/2-c]_q![d/2-y]_q!}{[v-k-y]_q![k-c]_q![k-d/2]_q![d/2]_q!} \cdot q^{v-k-d/2} = \frac{\begin{bmatrix} v-k \\ y \end{bmatrix}_q \begin{bmatrix} k \\ c \end{bmatrix}_q}{\begin{bmatrix} k-d/2 \\ c \end{bmatrix}_q \begin{bmatrix} d/2 \\ y \end{bmatrix}_q} q^{c(v-k-d/2)}. \qquad \square$$

6.3 The LMRD bound

Before we state the LMRD bound, which is the combination of both single LMRD bounds, we look at some parameters q, v, d, and k in which Proposition 88 is tight.

The Echelon-Ferrers construction yields some partial spread parameters, in which Proposition 88 is tight and, even more, $\mathrm{A}_q(v, 2k; k)$ is met.

96 **Remark**

For $2 \leq d/2 \leq k \leq v-k$, as well as $k < d \leq 2v/3$, we have:

If $d = 2k$, then $\mathrm{A}_q(v-k, 2(d-k); d/2)$ corresponds to a partial spread and if in addition $r \equiv v \pmod{k}$, $0 \leq r < k$, and $[r]_q < k$ then $\mathrm{A}_q(v-k, 2(d-k); d/2) = \frac{q^{v-k}-q^{k+r}}{q^k-1} + 1$, cf. Theorem 131. Hence, the bound in Proposition 88 is $\#C \leq q^{v-k} + \frac{q^{v-k}-q^{k+r}}{q^k-1} + 1 = \frac{q^v-q^{k+r}}{q^k-1} + 1 = \mathrm{A}_q(v, d; k)$. An optimal CDC containing an LMRD can be constructed with Equation 4.1, as a special case of the Echelon-Ferrers construction, cf. Chapter 4.

If $v = 3d/2$, then $\mathrm{A}_q(v-k, 2(d-k); d/2)$ corresponds to an orthogonal partial spread and if in addition $d-k \mid d/2$, it corresponds to a spread of size $(q^{3d/2-k}-1)/(q^{d-k}-1)$, cf. Corollary 125.

Next, we list two infinite families of parameters such that Proposition 88 is tight. The first was not known before and the second is listed for completeness.

97 **Lemma**

For integral $l \geq 1$ and prime power q, there is a $(6l, q^{3l(l+1)} + q^{2l} + q^l + 1, 4l; 3l)_q$ CDC C that contains an LMRD. This cardinality achieves the bound of Proposition 88.

Proof

The bound of Proposition 88 can be computed via Remark 96.

C is constructed with the Echelon-Ferrers construction, cf. Chapter 4, and these pivot vectors:

$(1_l 1_l 1_l 0_l 0_l 0_l)$ (i.e., an LMRD of size $q^{3l(l+1)}$)
$(1_l 0_l 0_l 1_l 1_l 0_l)$
$(0_l 1_l 0_l 1_l 0_l 1_l)$
$(0_l 0_l 1_l 0_l 1_l 1_l)$ (i.e., a subcode with 1 element)

Note that the Hamming distances between these four constant weight codewords is always $4l$ which implies the subspace distance of at least $4l$ via Lemma 54. The size of the subcode, corresponding to the second constant weight codeword, is q^{2l} and can be constructed with Lemma 61 and an $[l \times 2l, 2l, l]_q$ MRD. The third constant weight codeword gives rise to the q^l codewords of C using the same technique and an $[l \times l, l, l]_q$ MRD. □

Previously, only the optimality for $l = 1$ was known [ES13, Theorem 10].

Another series of LMRD bound achieving parameters is:

98 Lemma
For integral $l \geq 1$ and prime power q, there is a $(6+3l, q^{6+4l}+q^{2+l}+1, 4+2l; 3+l)_q$ CDC C that contains an LMRD. This cardinality achieves the bound of Proposition 88.

Proof
First, the bound is given by $\#C \leq q^{6+4l} + \mathrm{A}_q(3+2l, 2+2l; 2+l)$. The second summand is, due to orthogonal codes and $3+2l \equiv 1 \pmod{1+l}$ for $l \geq 1$, known, cf. Theorem 126, and equal to $q^{2+l}+1$.

Second, C can be constructed with the Echelon-Ferrers construction, cf. Chapter 4, and these pivot vectors:

$(1_1 1_{1+l} 1_1 0_{1+l} 0_1 0_{1+l})$ (i.e., an LMRD of size q^{6+4l})
$(1_1 0_{1+l} 0_1 1_{1+l} 1_1 0_{1+l})$
$(0_1 0_{1+l} 1_1 0_{1+l} 1_1 1_{1+l})$ (i.e., a subcode with 1 element)

Note that the Hamming distances between these three constant weight codewords is always $4+2l$ which implies the subspace distance of at least $4+2l$ via Lemma 54. The size of the subcode, corresponding to the second constant weight codeword, is q^{2+l} and can be constructed with Lemma 61, a $[1 \times (2+l), 2+l, 1]_q$ MRD and a $[(2+l) \times (1+l), 2+l, 1+l]_q$ MRD. □

For all prime powers q and integral $l \geq 1$, this bound was previously known [ES13, Theorem 10] as well as the construction [ES09] and it is listed here for completeness.

99 Proposition ([Hei18, Proposition 1])
For $2 \leq d/2 \leq k \leq v-k$ let C be a $(v, \#C, d; k)_q$ CDC that contains an LMRD code.

If $k < d \leq 2v/3$ we have

$$\#C \leq q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v-k, 2(d-k); d/2).$$

If additionally $d = 2k$, $r \equiv v \pmod{k}$, $0 \le r < k$, and $[r]_q < k$, then the right hand side is equal to $\mathrm{A}_q(v, d; k)$ and achievable in all cases.

If $(v, d, k) \in \{(6+3l, 4+2l, 3+l), (6l, 4l, 3l) \mid l \ge 1\}$, then there is a CDC containing an LMRD with these parameters whose cardinality achieves the bound.

If $k < d$ and $v < 3d/2$ we have

$$\#C \le q^{(v-k)(k-d/2+1)} + 1$$

and this cardinality is achieved.

If $d \le k < 3d/2$ we have

$$\begin{aligned}\#C \le\ & q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v-k, 3d-2k; d) \\ & + \begin{bmatrix} v-k \\ d/2 \end{bmatrix}_q \begin{bmatrix} k \\ d-1 \end{bmatrix}_q q^{(k-d+1)(v-k-d/2)} / \begin{bmatrix} k-d/2 \\ d/2-1 \end{bmatrix}_q .\end{aligned}$$

Proof

First, we discuss the optimal choice of y and c. Remark 92 shows that the optimal choice for y is $\max\{1, k-d/2+1-c\}$. Then, for $\max\{1, k-d+1\} \le c \le \min\{k-d/2, d/2\}$ we compare the second summand and the third summand of the statement in Proposition 91 separately. The third summand, i.e., $\mathrm{A}_q(v-k, d-2(c-1); k-c+1)$ is monotonically decreasing in c as seen in Lemma 93. The second summand, in which we have to consider $y(c)$, i.e.,

$$\frac{\begin{bmatrix} v-k \\ y(c) \end{bmatrix}_q \begin{bmatrix} k \\ c \end{bmatrix}_q}{\begin{bmatrix} k-d/2 \\ c \end{bmatrix}_q \begin{bmatrix} d/2 \\ y(c) \end{bmatrix}_q} q^{c(v-k-d/2)}$$

is also monotonically decreasing in c by Lemma 94. Hence, the smallest c yields the smallest upper bound and therefore $\max\{1, k-d+1\}$ is the optimal choice for c.

Second, we compare the bound of Proposition 91 to the bound of Proposition 88 where both bounds are applicable, i.e., $d/2 < k < d$. The second summand of Proposition 91, utilizing the optimal choice of y and c, is already larger than the second summand of Proposition 88 by Lemma 95.

Hence, we only apply Proposition 91 for $d \le k < 3d/2$ and in particular $d \le k$ shows $c = k-d+1 \ge 1$ and $y = d/2 \ge 2$.

Third, we consider the cases in which Proposition 88 is tight.

The restriction $v < 3d/2$ is equivalent to $2(v-k-d/2) < 2(d-k)$, i.e., any two codewords $U \ne W$ in an orthogonal $(v-k, \#C, 2(d-k); d/2)_q$ code have $\mathrm{d_s}(U, W) \le 2(v-k-d/2) < 2(d-k)$, hence $\#C \le 1$. Moreover a code attaining this bound can be constructed by extending a $(v, \#M, d; k)_q$ LMRD with the codeword $Z = \tau^{-1}((\mathbf{0}_{v-k} \mid I_k))$, since $2k \le v$ implies that Z intersects each other codeword trivially.

Two additional families of parameters such that Proposition 88 is tight are given by Lemma 97 and Lemma 98.

Proposition 88 is tight in some partial spread cases via Remark 96 and even meets the bound $\mathrm{A}_q(v, 2k; k)$. □

Therefore, Proposition 99 implies the parameter regions in Figure 7.

6.4 Improved code sizes

Since Lemma 86 states that any $(v, \#C, d; k)_q$ CDC that contains an LMRD M can be partitioned into $C = M \mathbin{\dot\cup} S_{d/2} \mathbin{\dot\cup} \ldots \mathbin{\dot\cup} S_k$, we know that any codeword in $C \setminus M$ has an at least $d/2$-dimensional intersection with Γ. Hence, we describe a promising approach to find large codes C by considering $E \subseteq \begin{bmatrix} \Gamma \\ d/2 \end{bmatrix}$. If $k < d$, i.e., $k - d/2 + 1 \le d/2$, then any codeword in $C \setminus M$ contains different elements of E. Moreover, Lemma 86 also states, that the minimum distance of E has to be at least $2(d - k)$, cf. Proposition 88. With other words, E is a $(v - k, \#E, 2(d - k); d/2)_q$ CDC embedded in Γ. On the one hand, it is natural to consider already large CDCs, which for example are listed here: `http://subspacecodes.uni-bayreuth.de` [Hei+16] and try to extend them. On the other hand, a given $(v', N', d'; k')_q$ CDC can be used to build a $(v'+2k'-d'/2, N', 2k'; 2k'-d'/2)_q$ CDC that is compatible to any LMRD that respects these parameters.

Moreover, if $k < d$, then a $(v, \#C, d; k)_q$ CDC C that contains an LMRD M implies a $(v - k, \#C - \#M, 2(d - k); d/2)_q$ CDC $C' = \{\mathcal{H}_{d/2}(U \cap \Gamma) \mid U \in C \setminus M\}$, which in turn shows that generating a large C is at least as difficult as generating C'.

Next, the number of subspaces in $C \setminus M$ having a large intersection with Γ is limited by $\#S_t \le \mathrm{A}_q(v - k, d - 2(k - t); t)$ for $\max\{d/2, k - d/2 + 1\} \le t \le k$ as an application of Lemma 87, $m = M = t$, $l = 2k - d$, $A_t = \{U \cap \Gamma \mid U \in S_t\} \subseteq \left[\begin{smallmatrix} \Gamma \\ t \end{smallmatrix}\right]$, with $\#A_t = \#S_t$, and the minimum distance $\mathrm{d_s}(U \cap \Gamma, W \cap \Gamma) \ge \mathrm{d_s}(U, W) - 2k + 2t \ge d - 2k + 2t > 0$ shows.

For a given subcode E, Algorithm 3 shows our applied search strategy. The argument $r_{\max}$ controls the level of detail of each of the independent $n_{\max}$ runs. Also, we do not precompute the set of extensions for each subspace in E, although it may be useful to save computation time if $r_{\max}$ is large compared to the size of the set of extensions, i.e. $\begin{bmatrix} v-d/2 \\ k-d/2 \end{bmatrix}_q$, and $n_{\max}$ is at least two.

Table 6 lists improved sizes of CDCs for small fixed parameters q, v, d, and k. The size of the LMRD with these parameters is $\#M$ and the successive columns only show the extended cardinality without the corresponding LMRD size. Therefore LMRD-B$-\#M$ is the size of the LMRD bound, PBKLB$-\#M$ is the previously best known lower bound, E is the used subcode up to embedding in Γ, and BKLB$-\#M$ is the current best known lower bound, i.e., the code size constructed with our described method. The codes can be downloaded from `http://subspacecodes.uni-bayreuth.de`, see also [Hei+16].

A further improvement of the second code, i.e. $(q, v, d, k) = (2, 11, 6, 4)$, such that it still contains an LMRD, would imply a $(7, \#E, 4; 3)_2$ CDC E with $333 < \#E$.

The situation of the first code, i.e., $(q, v, d, k) = (2, 10, 6, 5)$, is a special case, since $\#S_3 \le 155$, $\#S_4 \le 1$, and $S_5 \subseteq \{\Gamma\}$.

If $\#S_5 = 1$, then $\#S_3 = \#S_4 = 0$, because any subspace $U \in S_3 \cup S_4$ has $\mathrm{d_s}(U, \Gamma) \le 4$, hence we set $S_5 = \emptyset$.

If $\#S_4 = 1$, then $\#S_3 \le 140$, because for $U \in S_4$ we have $\#\{W \in S_3 \mid \dim((U \cap \Gamma) \cap (W \cap \Gamma)) = 3\} = \left[\begin{smallmatrix} 4 \\ 3 \end{smallmatrix}\right]_2 = 15$, i.e., the elements in this set have $\mathrm{d_s}(U, W) = 2(5 - 3) = 4$

Algorithm 3 Random search strategy for extending an arbitrary LMRD

Require: E is a $(v-k, \#E, 2(d-k); d/2)_q$ CDC embedded in Γ, $1 \le n_{\max}$, and $1 \le r_{\max}$

procedure $\textsc{Search}(E, n_{\max}, r_{\max})$
  $T \leftarrow \left\{ \tau(U) \;\middle|\; U \in \begin{bmatrix} \mathbb{F}_q^{v-d/2} \\ k-d/2 \end{bmatrix} \right\}$ ▷ as an array, so T_i is the i-th element
  $C_{\max} \leftarrow \{\}$
  for $n \in \{1, \ldots, n_{\max}\}$ **do**
    $C \leftarrow \{\}$
    for $U \in E$ **do**
      $B \in \begin{bmatrix} V \\ v-d/2 \end{bmatrix}$ ▷ such that $B \oplus U = V$
      $M \leftarrow \tau(B)$
      $\sigma \leftarrow \text{random}(\mathcal{S}_{\#T})$
      for $r \in \{1, \ldots, \min\{r_{\max}, \#T\}\}$ **do**
        $W \leftarrow U \oplus \tau^{-1}(T_{\sigma(r)} \cdot M)$
        for $Z \in C$ **do**
          if $\dim(Z \cap W) > k - d/2$ **then**
            continue r
          end if
        end for
        $C \leftarrow C \cup \{W\}$
        if $k < d$ **then**
          continue U
        end if
      end for
    end for
    if $\#C > \#C_{\max}$ **then**
      $C_{\max} \leftarrow C$
    end if
  end for
  return $C_{\max}$
end procedure

q	v	d	k	$\#M$	LMRD-B $-\#M$	PBKLB $-\#M$	E	BKLB $-\#M$
2	10	6	5	2^{15}	155	122 [SE11, Ex. 4]	$\left[{\Gamma \atop 3}\right]$	155
2	11	6	4	2^{14}	$\mathrm{A}_2(7,4;3) \leq 381$	285 [ES09; Hei+16]	$(7,333,4;3)_2$ [Hei+16]	333
2	11	6	5	2^{18}	1395	852 [ES09; Hei+16]	$\left[{\Gamma \atop 3}\right]$	1334
2	12	6	4	2^{16}	$\mathrm{A}_2(8,4;3) \leq 1493$	1144 [ES09; Hei+16]	$(8,1326,4;3)_2$ [BÖW16]	1303
2	12	6	5	2^{21}	11811	7232 [ES09; Hei+16]	$\left[{\Gamma \atop 3}\right]$	7925
2	13	6	4	2^{18}	$\mathrm{A}_2(9,4;3) \leq 6205$	4747 [ST15]	$(9,5986,4;3)_2$ [BÖW16]	5753

Table 6: New lower bounds on some CDC parameters

and, aiming for large code sizes, we set $S_4 = \emptyset$.

Therefore, a code with these parameters that contain an LMRD and achieves the LMRD bound has to contain a subcode S_3 of cardinality 155, i.e., all subspaces $\left[{\Gamma \atop 3}\right]$ have to be extended with subspaces in $\left[{V \setminus \Gamma \atop 2}\right]$ such that the minimum distance constraint is fulfilled. The subspace distance of any codeword $U \in M$ and $W \in S_3 = C \setminus M$ is at least 6 and therefore only the minimum distance of S_3 is in question.

There are, for each subspace in $\left[{\Gamma \atop 3}\right]$, $\left[{10-3 \atop 5-3}\right]_2 = 2667$ extensions to 5 dimensions, of which $\left[{10\setminus 5 \atop 2}\right]_2 / \left[{5\setminus 3 \atop 2}\right]_2 = 2480$ have a trivial intersection with Γ.

Hence, by prescribing the following subgroup of order 31 of the stabilizer of Γ, i.e., the cyclic group generated by a block diagonal matrix consisting of twice the same generator of a Singer cycle in Γ,

$$G = \left\langle \begin{pmatrix} 0&0&0&0&1&&&&& \\ 1&0&0&0&0&&&&& \\ 0&1&0&0&1&&&&& \\ 0&0&1&0&0&&&&& \\ 0&0&0&1&0&&&&& \\ &&&&&0&0&0&0&1 \\ &&&&&1&0&0&0&0 \\ &&&&&0&1&0&0&1 \\ &&&&&0&0&1&0&0 \\ &&&&&0&0&0&1&0 \end{pmatrix} \right\rangle,$$

we partition the set $\left\{U \in \left[{\mathbb{F}_2^{10} \atop 5}\right] \,\middle|\, \dim(U \cap \Gamma) = 3\right\}$ of size $2480 \cdot 155 = 384\,400$ into 12400 orbits of length 31 under the action of G. 3100 of these orbits contain a pair of subspaces that has an intersection of at least dimension 3 and hence these orbits cannot be subset of a $(10, N, 6; 5)_2$ CDC. The remaining 9300 orbits are then considered as vertices of a graph in which two vertices $O_1 \neq O_2$ share an edge iff $\dim(U \cap W) \leq 2$ for all $U \in O_1$ and $W \in O_2$. Clearly, the clique number is upper bounded by $5 = \# \left[{\Gamma \atop 3}\right] / \#G$ since each 3-dimensional subspaces in Γ may be contained at most once without violating the minimum distance. A greedy clique search provides a clique of size 5. With other words these five orbits are an extension of any $(10, 2^{15}, 6; 5)_2$ LMRD of size 155 achieving the

LMRD bound of Proposition 99. Representatives in RREF of these five orbits are

$$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&0&1&1&1&0&0&0&1&0\\ &&&&&1&0&0&0&0\\ &&&&&0&1&1&0&0\\ &&&&&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&1&0&0&0\\ &&&&&1&0&0&0&0\\ &&&&&0&0&1&0&0\\ &&&&&0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&1\\ &&&&&1&0&0&0&1\\ &&&&&0&1&0&1&0\\ &&&&&0&0&1&0&1 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&0&0&1&1&0&0&0&1&0\\ &&&&&1&0&0&0&1\\ &&&&&0&1&0&1&1\\ &&&&&0&0&1&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&1&1\\ &&&&&1&0&0&0&0\\ &&&&&0&1&0&0&1\\ &&&&&0&0&1&1&1 \end{pmatrix},$$

in which the omitted parts are zeros, since the corresponding rows are RREF matrices of the 3-dimensional intersection with Γ.

An approach with a BLP

The problem of extending a large embedded CDC to one that can be joined with an LMRD can be formulated as BLP:

100 Lemma
Let C' be a $(v', N', d'; k')_q$ CDC embedded in $\Gamma = \Gamma_{q,k,v}$, where $v = v' + 2k' - d'/2$, $k = 2k' - d'/2$, $s = k' - d'/2 + 1$, and $V = \mathbb{F}_q^v$. Moreover we use a $(v, q^{v's}, 2k'; k)_q$ LMRD M and $E(U) = \{W \in \left[\begin{smallmatrix} V \\ k \end{smallmatrix}\right] \mid U \le W\}$ for $U \in C'$. Then, for any feasible $X = \{x_{U,W} \in \{0,1\} \mid U \in C', W \in E(U)\}$ of the BLP below and $C = \{W \mid x_{U,W} = 1, U \in C', W \in E(U)\}$, we have that $M \cup C$ is a $(v, q^{v's} + \#C, 2k'; k)_q$ CDC.

$$\begin{aligned} \max & \sum_{U \in C'} \sum_{W \in E(U)} x_{U,W} \\ \text{st} & \\ & \sum_{W \in E(U)} x_{U,W} \le 1 && \forall\, U \in C' \\ & \sum_{U \in C'} \sum_{W \in E(U): B \le W} x_{U,W} \le 1 && \forall\, B \in \left[\begin{smallmatrix} V \\ s \end{smallmatrix}\right] \\ & x_{U,W} \in \{0,1\} && \forall\, U \in C', W \in E(U) \end{aligned}$$

Proof
The first constraint of the BLP ensures that each $U \in C'$ is extended to at most one codeword $W \in C$, whereas the second constraint ensures that the minimum distance of C is large enough: $\dim(X \cap Y) < s$ implies $\mathrm{d_s}(X, Y) > 2(k - s) = 2((2k' - d'/2) - (k' - d'/2 + 1)) = 2(k' - 1)$. □

Note that this BLP is a subset of DefaultCDCBLP(q, v, d, k) (Definition 47) in terms of W-variables. Since $\#E(U) = \left[\begin{smallmatrix} v-k' \\ k-k' \end{smallmatrix}\right]_q$ for all $U \in C'$, the number of variables of the

BLP in Lemma 100 is $\#C' \cdot \begin{bmatrix} v-k' \\ k-k' \end{bmatrix}_q$, which is considerably smaller than the number of variables in DefaultCDCBLP(q, v, d, k) (Definition 47), i.e., $\begin{bmatrix} v \\ k \end{bmatrix}_q$.

As an example, we apply this to $(q, v, d, k) = (2, 10, 6, 5)$. We additionally know that any C with $\#C \geq 142$ fulfills $W \cap \Gamma = U$ for all $U \in \begin{bmatrix} \Gamma \\ 3 \end{bmatrix}$ and $W \in E(U)$. Therefore, we can add the restrictions to these W's to the BLP of Lemma 100 by either adding the additional constraints $x_{U,W} = 0$ for all $U \in \begin{bmatrix} \Gamma \\ 3 \end{bmatrix}$ and $W \in E(U)$ with $W \cap \Gamma \neq U$, or by restricting the set $E(U)$ to $E(U)' = \{W \in E(U) \mid W \cap \Gamma = U\}$, which in turn has 2480 elements for all $U \in \begin{bmatrix} \Gamma \\ 3 \end{bmatrix}$. This adapted BLP has then $155 \cdot 2480 = 384\,400$ variables – compared to $\begin{bmatrix} 10 \\ 5 \end{bmatrix}_2 = 109\,221\,651$ variables of DefaultBLP (Definition 47) and to the original version in Lemma 100 with $155 \cdot 2667 = 413\,385$ variables. Unfortunately, trying to solve this adapted BLP, `Gurobi` ([Gur16]) cannot even compute the LP-relaxation of the whole problem, i.e., in the branch & bound ([Dak65]) root node, due to the lack of memory.

7 Known upper bounds

Contents of this chapter were previously published in [HK17b].

The list of known upper bounds has not changed much since [EV11a; KSK09]. Comparisons of the bounds are distributed in the literature and even commentaries, cf. [BPV13]. Unfortunately, some results are wrong and this chapter is dedicated to provide a complete picture of upper bounds for CDCs and comparisons between them, to the best of our knowledge.

Interestingly, most upper bounds for CDCs for $2 \le d/2 < k \le v-k$ integers are dominated by the improved Johnson bound, which in turn refers back to more elaborate upper bounds on partial spreads.

Besides these general upper bounds, the only two sporadic improvements for $2 \le d/2 < k \le v-k$, i.e., no partial spreads, are $\mathrm{A}_2(6,4;3) = 77 < 81$ [HKK15] and $\mathrm{A}_2(8,6;4) = 257 < 289$, cf. Theorem 191.

See `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16] for numerical values of the known lower and upper bounds of the sizes of general subspace codes and CDCs for small parameters.

The structural results of Lemma 41 imply an upper bound which in turn is able to prove many known bounds, such as the Anticode bound, Johnson IIa, and Johnson IIb.

101 Lemma

For $q \ge 2$ prime power, $2 \le d/2 \le \min\{k, v-k\}$ integers, and $0 \le x \le v$, we have

$$\mathrm{A}_q(v,d;k) \le \begin{cases} \frac{\mathrm{A}_q(x,d;k)\left[{v \atop x}\right]_q}{\left[{v-k \atop x-k}\right]_q} = \frac{\mathrm{A}_q(x,d;k)\left[{v \atop k}\right]_q}{\left[{x \atop k}\right]_q} & \text{if } k \le x, \\ \frac{\mathrm{A}_q(v-x,d;k-x)\left[{v \atop x}\right]_q}{\left[{k \atop x}\right]_q} = \frac{\mathrm{A}_q(v-x,d;k-x)\left[{v \atop k}\right]_q}{\left[{v-x \atop k-x}\right]_q} & \text{if } x < k. \end{cases}$$

Proof

Let C be a $(v,N,d;k)_q$ CDC and $k \le x$. Double counting $\{(U,X) \in C \times \left[{\mathbb{F}_q^v \atop x}\right] \mid U \le X\}$ and applying Lemma 41 yields $N\left[{v-k \atop x-k}\right]_q = \sum_{X \in \left[{\mathbb{F}_q^v \atop x}\right]} \#\mathcal{I}(C,X) \le \left[{v \atop x}\right]_q \mathrm{A}_q(x,d;k)$.

For $x < k$ we count $\{(U,X) \in C \times \left[{\mathbb{F}_q^v \atop x}\right] \mid X \le U\}$ and apply again Lemma 41 to get $N\left[{k \atop x}\right]_q = \sum_{X \in \left[{\mathbb{F}_q^v \atop x}\right]} \#\mathcal{I}(C,X) \le \left[{v \atop x}\right]_q \mathrm{A}_q(v-x,d;k-x)$.

The application of Lemma 7 proves the equalities. □

Anticode type bounds A large class of upper bounds for CDCs is given by a similar technique.

In general an anticode of diameter e is a subset of a metric space whose elements have pairwise distance of at most e.

In the next lemma we count the number of k-spaces in $\mathbb{F}_q^v$ which have a large intersection with a fixed m-dimensional subspace in $\mathbb{F}_q^v$.

102 **Lemma ([HK17b, Lemma 2])**
For $q \geq 2$ prime power and t, k, v, m integers, such that $t \leq k \leq v$, we have for all $W \in \begin{bmatrix} \mathbb{F}_q^v \\ m \end{bmatrix}$

$$\#\left\{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \mid \dim(U \cap W) \geq k-t\right\} = \sum_{i=0}^{t} q^{(m+i-k)i} \begin{bmatrix} m \\ k-i \end{bmatrix}_q \begin{bmatrix} v-m \\ i \end{bmatrix}_q.$$

Moreover, the cardinality is non-zero if $0 \leq t \leq k \leq v$ and $k-t \leq m \leq v$.

Proof
Both sides of the equation are zero if $t < 0$, $v < m$, or $m < k-t$ and hence we assume wlog. $0 \leq t \leq k \leq v$ and $k-t \leq m \leq v$.

Consider an $U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with $\dim(U \cap W) = k-i$ for $\max\{0, k-m\} \leq i \leq \min\{t, v-m\}$. Then, the number of choices of U can be counted via $(U \cap W) \oplus U'$. We have $U \cap W \in \begin{bmatrix} W \\ k-i \end{bmatrix}$ and $U' \in \begin{bmatrix} \mathbb{F}_q^v \backslash W \\ i \end{bmatrix}$, whereas $\begin{bmatrix} k \backslash k-i \\ i \end{bmatrix}_q$ choices of U' span the same subspace U. Hence,

$$\begin{aligned}\left\{U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \middle| \dim(U \cap W) = k-i\right\} &= \begin{bmatrix} m \\ k-i \end{bmatrix}_q \cdot \begin{bmatrix} v \backslash m \\ i \end{bmatrix}_q / \begin{bmatrix} k \backslash k-i \\ i \end{bmatrix}_q \\ &= \begin{bmatrix} m \\ k-i \end{bmatrix}_q \cdot \begin{bmatrix} v-m \\ i \end{bmatrix}_q q^{im} / \left(\begin{bmatrix} k-(k-i) \\ i \end{bmatrix}_q q^{i(k-i)} \right) = \begin{bmatrix} m \\ k-i \end{bmatrix}_q \cdot \begin{bmatrix} v-m \\ i \end{bmatrix}_q q^{i(m-k+i)}.\end{aligned}$$

Finally, applying the convention $\begin{bmatrix} a \\ b \end{bmatrix}_q = 0$ for integers with $b < 0$ or $b > a$ and summing over $i = 0, 1, \ldots, t$ yields the result. $\square$

The size is independent of the choice of $W \in \begin{bmatrix} \mathbb{F}_q^v \\ m \end{bmatrix}$. Moreover $\dim(U \cap W) \geq k-t$ is equivalent to $\mathrm{d_s}(U, W) \leq m-k+2t$, and therefore using $m = k$, we get the size of a sphere $S(W, k, t) = \left\{U \in \begin{bmatrix} V \\ k \end{bmatrix} \mid \mathrm{d_s}(U, W) \leq 2t\right\}$, i.e., a sphere in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with radius $2t$ and center $W \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$, cf. [KK08b, Definition 4].

103 **Corollary (cf. [KK08b, Theorem 5])**
For $q \geq 2$ prime power, integers $0 \leq t \leq k \leq v$, and $W \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ we have

$$\#S(W, k, t) = \sum_{i=0}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} v-k \\ i \end{bmatrix}_q.$$

An anticode in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with diameter e is a subset $A \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ such that $e = \max\{\mathrm{d_s}(U, W) \mid U \neq W \in A\}$, i.e., its *maximum* distance is bounded, whereas in the case of CDCs the *minimum* distance is bounded. Hence, $S(W, k, t)$ is an anticode in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with diameter $4t$ by the triangle inequality $\mathrm{d_s}(X, Y) \leq \mathrm{d_s}(X, W) + \mathrm{d_s}(W, Y) \leq 2t + 2t$ for all $X, Y \in S(W, k, t)$.

104 Lemma ([AA09, Lemma 1], cf. [AAK01, Theorem 1'])
Let $G = (V, E)$ be a graph that admits a transitive group of automorphisms $\mathrm{Aut}(G)$ and let A, B be arbitrary subsets of the vertex set V. Then, there exists a group element $g \in \mathrm{Aut}(G)$ such that

$$\frac{\#A}{\#V} \leq \frac{\#(g(A) \cap B)}{\#B}.$$

Proof
We count $T = \{(a, f) \in A \times \mathrm{Aut}(G) \mid f(a) \in B\}$ in two ways.

First, we have $\#T = \sum_{f \in \mathrm{Aut}(G)} \#\{a \in A \mid f(a) \in B\} = \sum_{f \in \mathrm{Aut}(G)} \#(f(A) \cap B)$.

Second, let $a \in A$ be fixed and for fixed $b \in B$ there is, by applying the transitivity of the action of $\mathrm{Aut}(G)$, a $h_b \in \mathrm{Aut}(G)$ such that $h_b(a) = b$. Then, we can express the set of group elements which map a to b by a coset of the stabilizer of a in $\mathrm{Aut}(G)$:

$$\begin{aligned}
&\{f \in \mathrm{Aut}(G) \mid f(a) = b\} = \{f \in \mathrm{Aut}(G) \mid f(a) = h_b(a)\} \\
&= \{f \in \mathrm{Aut}(G) \mid h_b^{-1} \circ f(a) = a\} = \{h_b \circ f \mid f \in \mathrm{Aut}(G) \wedge f(a) = a\} \\
&= h_b\{f \in \mathrm{Aut}(G) \mid f(a) = a\} = h_b \, \mathrm{Stab}_{\mathrm{Aut}(G)}(a).
\end{aligned}$$

By the Orbit-Stabilizer theorem (Lemma 22) we know $\#(a \, \mathrm{Aut}(G)) \cdot \# \, \mathrm{Stab}_{\mathrm{Aut}(G)}(a) = \# \, \mathrm{Aut}(G)$ and the transitivity of $\mathrm{Aut}(G)$ implies $a \, \mathrm{Aut}(G) = V$.

Therefore:

$$\begin{aligned}
\#T &= \sum_{a \in A} \#\{f \in \mathrm{Aut}(G) \mid f(a) \in B\} = \sum_{a \in A} \# \left(\dot{\bigcup}_{b \in B} \{f \in \mathrm{Aut}(G) \mid f(a) = b\} \right) \\
&= \sum_{a \in A} \sum_{b \in B} \# \left(h_b \, \mathrm{Stab}_{\mathrm{Aut}(G)}(a) \right) = \sum_{a \in A} \sum_{b \in B} \# \, \mathrm{Stab}_{\mathrm{Aut}(G)}(a) \\
&= \sum_{a \in A} \sum_{b \in B} \# \, \mathrm{Aut}(G)/\#V = \#A \cdot \#B \cdot \# \, \mathrm{Aut}(G)/\#V.
\end{aligned}$$

Both ways of counting $\#T$ imply:

$$\frac{\sum_{f \in \mathrm{Aut}(G)} \#(f(A) \cap B)}{\# \, \mathrm{Aut}(G)} = \frac{\#A \cdot \#B}{\#V}$$

such that the left hand side is the average size of images of A in B and hence there is a $g \in \mathrm{Aut}(G)$ with the desired property. □

105 Corollary ([AA09, Corollary 1], cf. [AAK01, Theorem 1])
Let C be a $(v, \#C, d; k)_q$ CDC with pairwise subspace distances in $D \subseteq \{d, d+2, \ldots\}$. Then, for any $B \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$, there exists a CDC $C^* \subseteq B$ with distances in D such that

$$\#C \le \frac{\#C^* \cdot \left[{v \atop k} \right]_q}{\#B}.$$

In particular, if C has the minimum subspace distance d and B is an anticode in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ with diameter $d-2$, we have $\#C^* \le 1$ and $\#C \le \frac{\left[{v \atop k} \right]_q}{\#B}$. Using the spheres $S(W, k, \lfloor (d/2-1)/2 \rfloor)$ as B, we obtain the *Sphere-packing bound*. Another approach to prove this bound is to use the distance-regularity of the Grassmann graph.

106 Theorem (Sphere-packing bound, cf. [KK08b, Theorem 6])
For $q \ge 2$ prime power and $2 \le d/2 \le \min\{k, v-k\}$ integers, we have

$$\mathrm{A}_q(v, d; k) \le \frac{\left[{v \atop k} \right]_q}{\sum_{i=0}^{\lfloor (d/2-1)/2 \rfloor} q^{i^2} \left[{k \atop i} \right]_q \left[{v-k \atop i} \right]_q}.$$

Let $V = \mathbb{F}_q^v$ and $W \in \begin{bmatrix} V \\ k-d/2+1 \end{bmatrix}$ be a fixed subspace. Then the set $B = \{U \in \left[{V \atop k} \right] \mid W \le U\}$ is an anticode in $\left[{V \atop k} \right]$ of diameter $d-2$ and size $\#B = \begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q$.

Similarly, by orthogonality, if $W \in \begin{bmatrix} V \\ k+d/2-1 \end{bmatrix}$ is a fixed subspace, then the set $B = \{U \in \left[{V \atop k} \right] \mid U \le W\}$ is an anticode in $\left[{V \atop k} \right]$ of diameter $d-2$ and size $\#B = \begin{bmatrix} k+d/2-1 \\ d/2-1 \end{bmatrix}_q$.

Frankl and Wilson proved in [FW86, Theorem 1] that these anticodes have the largest possible size, which implies the tightest Anticode-type bound. We will speak of *the anticode bound*. This is also derived by considering Theorem 40 for the q-Johnson scheme.

107 Theorem (Anticode bound, [WXS03, Theorem 5.2], [EV11a, Theorem 1])
For $q \ge 2$ prime power and $2 \le d/2 \le \min\{k, v-k\}$ integers we have

$$\mathrm{A}_q(v, d; k) \le \frac{\left[{v \atop k} \right]_q}{\begin{bmatrix} \max\{k, v-k\}+d/2-1 \\ d/2-1 \end{bmatrix}_q} = \min \left\{ \underbrace{\frac{\left[{v \atop k} \right]_q}{\begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q}}_{= \frac{\left[{v \atop k-d/2+1} \right]_q}{\left[{k \atop k-d/2+1} \right]_q}}, \underbrace{\frac{\left[{v \atop k} \right]_q}{\begin{bmatrix} k+d/2-1 \\ d/2-1 \end{bmatrix}_q}}_{= \frac{\left[{v \atop v-k+d/2-1} \right]_q}{\left[{v-k \atop v-k+d/2-1} \right]_q}} \right\}.$$

Proof
Applying Lemma 101 with $x = k - d/2 + 1$ yields $\mathrm{A}_q(v, d; k) \le \left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} v-k+d/2-1 \\ d/2-1 \end{smallmatrix}\right]_q$ and with $x = k + d/2 - 1$ we get $\mathrm{A}_q(v, d; k) \le \left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} k+d/2-1 \\ d/2-1 \end{smallmatrix}\right]_q$. The minimum of both right hand sides is $\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} \max\{k,v-k\}+d/2-1 \\ d/2-1 \end{smallmatrix}\right]_q$. Applying Lemma 7 yields the transformation. □

Another possibility to use Corollary 105, in which $\#C^*$ does not have to be one, is given by the next theorem.

108 **Theorem ([AA09, Theorem 3], [KSK09, Theorem 8], [HK17b, Theorem 8])**
For $q \ge 2$ prime power, $2 \le d/2 \le \min\{k, v - k\}$, $0 \le t < d/2$, and $k - t \le m \le v$ integers we have

$$\mathrm{A}_q(v, d; k) \le \frac{\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q \mathrm{A}_q(m, d - 2t; k - t)}{\sum_{i=0}^{t} q^{i(m+i-k)} \left[\begin{smallmatrix} m \\ k-i \end{smallmatrix}\right]_q \left[\begin{smallmatrix} v-m \\ i \end{smallmatrix}\right]_q}.$$

Proof
Let $W \in \left[\begin{smallmatrix} \mathbb{F}_q^v \\ m \end{smallmatrix}\right]$ be a fixed subspace and define $B = \left\{ U \in \left[\begin{smallmatrix} \mathbb{F}_q^v \\ k \end{smallmatrix}\right] \;\middle|\; \dim(U \cap W) \ge k - t \right\}$, so that $\#B = \sum_{i=0}^{t} q^{(m+i-k)i} \left[\begin{smallmatrix} m \\ k-i \end{smallmatrix}\right]_q \left[\begin{smallmatrix} v-m \\ i \end{smallmatrix}\right]_q$ is given by Lemma 102.

Let C^* be an arbitrary $(v, \#C^*, d; k)_q$ CDC with $C^* \subseteq B$.

Applying Lemma 87 with $A_i = \{U \in C^* \mid \dim(U \cap W) = i\} \subseteq \left[\begin{smallmatrix} W \\ i \end{smallmatrix}\right]$ for $m = k - t \le i \le k = M$ and $\mathrm{d_s}(X \cap W, Y \cap W) \ge \dim(X \cap W) + \dim(Y \cap W) - l$ with $l = 2k - d$, which is implied by $\dim(X \cap Y) \le k - d/2$, shows that $\# \bigcup_{i=k-t}^{k} A_i \le \mathrm{A}_q(m, d - 2t; k - t)$, since $d - 2t > 0$. Moreover, $\mathrm{d_s}(X \cap W, Y \cap W) \ge d - 2t > 0$ implies $\#C^* = \# \bigcup_{i=k-t}^{k} A_i \le \mathrm{A}_q(m, d - 2t; k - t)$. Applying Corollary 105 with $D = \{d, d+1, \ldots, v\}$ yields the bound. □

If $v - m < i$, then the corresponding summands in the denominator are all zero and hence the right hand side only increases. Focusing on strong bounds allows therefore to assume additionally $t \le v - m$.

Some allocations of the parameters in Theorem 108 may be interpreted. Choosing $m = v$ gives the bound $\mathrm{A}_q(v, d; k) \le \mathrm{A}_q(v, d - 2t; k - t)$, cf. Lemma 93. For $t = 0$ and $m \le v - 1$, we obtain $\mathrm{A}_q(v, d; k) \le \mathrm{A}_q(m, d; k) \left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} m \\ k \end{smallmatrix}\right]_q$. This is exactly the application of Johnson IIb (Inequality (7.2) in Theorem 113) $v - m$ times and omitting the rounding and hence, for fixed $t = 0$, the optimal choice for m is $m = v - 1$. In this case, Theorem 108 is equivalent to Johnson IIb (Inequality (7.2) in Theorem 113). It is not known whether there are parameters such that Theorem 108 strictly improves on Theorem 113 at all. For $t = 1$ and $m = v - 1$ the bound can be rewritten via Lemma 3 to $\mathrm{A}_q(v, d; k) \le \mathrm{A}_q(v - 1, d - 2; k - 1)$.

Numerical computations for small parameters, i.e., $2 \le q \le 9$ prime power, $4 \le v \le 100$, $2 \le d/2 \le k \le v-k$ integers, indicate that in all cases with $d/2 < k$, i.e., non-partial spread cases, there are no proper improvements compared to Theorem 113. If $d = 2k$, i.e., partial spreads which are mainly treated in the next subsection, then there are improvements compared to Corollary 125 of which some are summarized in Proposition 134. The other improvements are inferior compared to Theorem 130 and Theorem 132.

Puncturing and the Singleton bound Let $U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ be a subspace and $H \in \begin{bmatrix} \mathbb{F}_q^v \\ v-1 \end{bmatrix}$ be a hyperplane. The operation

$$\operatorname{punct} : \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \to \begin{bmatrix} H \\ k-1 \end{bmatrix}, U \mapsto \mathcal{H}_{k-1}(U \cap H)$$

is called *puncturing operation.* Using the definition of $\mathcal{H}$, see Page 27, $\operatorname{punct}(U) = U \cap H$ if $U \not\leq H$ and one of the $\begin{bmatrix} k \\ k-1 \end{bmatrix}_q$ arbitrary chosen $(k-1)$-subspaces of U otherwise. Although punct is no map, it has the property that $\operatorname{punct}(U) \leq U$ and therefore, for $U, W \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$,

$$\begin{aligned} \mathrm{d_s}(\operatorname{punct}(U), \operatorname{punct}(W)) &= 2(k - 1 - \dim(\operatorname{punct}(U) \cap \operatorname{punct}(W))) \\ &\geq 2(k - \dim(U \cap W)) - 2 = \mathrm{d_s}(U, W) - 2. \end{aligned}$$

Applying punct $d/2-1$ times to a $(v, \#C, d; k)_q$ CDC C yields a $(v-d/2+1, \#C, d'; k-d/2+1)_q$ CDC D with $2 \leq d'$, which proves $\#C = \#D$, whereas D has at most $\begin{bmatrix} v-d/2+1 \\ k-d/2+1 \end{bmatrix}_q$ elements. Considering either the code or its orthogonal code gives:

109 Theorem (Singleton bound [KK08b, Theorem 9])
For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers we have

$$\mathrm{A}_q(v, d; k) \leq \begin{bmatrix} v-d/2+1 \\ \max\{k,v-k\} \end{bmatrix}_q = \min\left\{ \begin{bmatrix} v-d/2+1 \\ k \end{bmatrix}_q, \begin{bmatrix} v-d/2+1 \\ v-k \end{bmatrix}_q \right\}.$$

The equality follows from $0 \leq x$ and $0 \leq y$ imply $|x-y| \leq |x+y|$, hence for $y = a-b$: $|\frac{a+b-x}{2} - b| \leq |\frac{a+b-x}{2} - a|$, i.e, $\begin{bmatrix} a+b-x \\ b \end{bmatrix}_q \geq \begin{bmatrix} a+b-x \\ a \end{bmatrix}_q$.

In [XF09, Section 4] Xia and Fu verified that the Anticode bound is always stronger than the Singleton bound for $2 \leq d/2 \leq k \leq v-k$.

Referring to [KK08b] the authors of [KSK09, Section 3.1] state that even a relaxation of the Singleton bound is always stronger than the sphere packing bound for non-trivial codes. However, on the one hand, for $q = 2$, $v = 8$, $d = 6$, and $k = 4$, the Sphere-packing bound gives an upper bound of $200\,787/451 \approx 445.2$ while the Singleton bound gives an upper bound of $\begin{bmatrix} 6 \\ 4 \end{bmatrix}_2 = 651$. On the other hand, for $q = 2$, $v = 8$, $d = 4$, and $k = 4$, the Singleton bound gives $\begin{bmatrix} 7 \\ 3 \end{bmatrix}_2 = 11811$ and the Sphere-packing bound gives $\begin{bmatrix} 8 \\ 4 \end{bmatrix}_2 = 200\,787$. Examples in which the Singleton bound dominates the Sphere-packing bound are easy to find. For $d = 2$ both bounds coincide and for $d = 4$ the Singleton bound is always stronger than the Sphere-packing bound since $\begin{bmatrix} v-1 \\ k \end{bmatrix}_q < \begin{bmatrix} v \\ k \end{bmatrix}_q$.

110 Lemma
The Sphere-packing bound (Theorem 106) is strictly tighter than the Singleton bound (Theorem 109) if $q = 2$, $v = 2k$, $d = 6$, and $3 \le k$ integer.

Proof
For these parameters, the Singleton bound is $\begin{bmatrix} 2k-2 \\ k-2 \end{bmatrix}_2$ and the Sphere-packing bound is $\begin{bmatrix} 2k \\ k \end{bmatrix}_2 / (1 + 2([k]_2)^2)$. Hence,

$$\frac{\begin{bmatrix} 2k \\ k \end{bmatrix}_2}{1 + 2([k]_2)^2} < \begin{bmatrix} 2k-2 \\ k-2 \end{bmatrix}_2 \Leftrightarrow \frac{[2k]_2!}{([k]_2!)^2(1 + 2([k]_2)^2)} < \frac{[2k-2]_2!}{[k-2]_2![k]_2!}$$
$$\Leftrightarrow \frac{[2k]_2[2k-1]_2}{[k]_2[k-1]_2(1 + 2([k]_2)^2)} < 1.$$

Using the inequalities $[x]_2 = 2^x - 1 < 2^x$ and $0 < 1$ we get

$$\Leftarrow \frac{2^{4k-1}}{2(2^k - 1)^3(2^{k-1} - 1)} \le 1$$

which is true for all $3 \le k$. □

In fact, for $q \le 9$ and $v \le 19$ even the conversion is true, as the entries of `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16] show. The asymptotic bounds [KK08b, Corollaries 7 and 10], using normalized parameters, and [KK08b, Figure 1] suggest that there is only a small range of parameters where the Sphere-packing bound can be superior to the Singleton bound.

Johnson I Transferring the classical Johnson bounds for constant weight codes regarding the Hamming distance [Joh62; Ton98] to the CDC case, Xia and Fu proved:

111 Theorem (Johnson I [XF09, Theorem 2])
For $q \ge 2$ prime power and $2 \le d/2 \le \min\{k, v-k\}$ integers with $\left(q^k - 1\right)^2 > (q^v - 1)\left(q^{k-d/2} - 1\right)$, we have

$$\mathrm{A}_q(v, d; k) \le \frac{\left(q^k - q^{k-d/2}\right)(q^v - 1)}{\left(q^k - 1\right)^2 - (q^v - 1)\left(q^{k-d/2} - 1\right)}.$$

However, the required condition of Theorem 111 is rather restrictive and can be simplified considerably.

112 **Proposition ([HK17b, Proposition 1])**
For $q \geq 2$ prime power and integers $0 \leq k < v$ and $2 \leq d/2 \leq \min\{k, v-k\}$, the bound in Theorem 111 is applicable iff $d/2 = \min\{k, v-k\}$ and $1 \leq k$. Then, it is equivalent to

$$\mathrm{A}_q(v,d;k) \leq \frac{q^v - 1}{q^{\min\{k,v-k\}} - 1}.$$

If $k = v$ then the bound is equivalent to $\mathrm{A}_q(v,d;k) \leq 1$.

Proof
If $k = 0$ we have $\left(q^k - 1\right)^2 = 0$, so that we assume $k \geq 1$ in the following. If $k \leq v-k$ and $d/2 \leq k-1$, then

$$(q^v - 1)\left(q^{k-d/2} - 1\right) \geq \left(q^{2k} - 1\right)(q-1) \geq q^{2k} - 1 > q^{2k} - 2q^k + 1 = \left(q^k - 1\right)^2.$$

If $k \geq v-k+1$ and $d/2 \leq v-k-1$, then applying $v - d/2 \geq k+1$, $k \geq v-k$, $1 \geq q^{-d/2}$, and $q \geq 2$ shows

$$\begin{aligned}(q^v - 1)\left(q^{k-d/2} - 1\right) \geq \left(q^k - 1\right)^2 &\Leftrightarrow q^{v-d/2} + 2 \geq q^k + q^{v-k} + q^{-d/2}\\ &\Leftarrow q^{k+1} + 2 \geq 2q^k + 1 \Leftrightarrow (q-2)q^k + 1 \geq 0.\end{aligned}$$

If $d/2 = \min\{k, v-k\}$, $q \geq 2$, and $k \geq 1$, then it can be easily checked that the condition of Theorem 111 is satisfied and we obtain the proposed formula after simplification. □

Proposition 112 corresponds in fact to the simplest bound on partial spreads Corollary 125, which is tight in the spread case. In Section 7.1 we will list more elaborate bounds on partial spreads.

Johnson II Although Proposition 112 as generalization of the first Johnson bound is rather weak, generalizing [Joh62, Inequality (5)], see [XF09], leads to strong upper bounds.

113 **Theorem (Johnson II [XF09, Theorem 3], [EV11a, Theorem 4,5])**
For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers, we have

$$\mathrm{A}_q(v,d;k) \leq \frac{q^v - 1}{q^k - 1} \mathrm{A}_q(v-1,d;k-1) \text{ and} \tag{7.1}$$

$$\mathrm{A}_q(v,d;k) \leq \frac{q^v - 1}{q^{v-k} - 1} \mathrm{A}_q(v-1,d;k). \tag{7.2}$$

Proof
Applying Lemma 101 with $x = 1$ yields $\mathrm{A}_q(v, d; k) \leq \mathrm{A}_q(v-1, d; k-1) \left[{v \atop 1}\right]_q / \left[{k \atop 1}\right]_q$. The same lemma with $x = v-1$ yields $\mathrm{A}_q(v, d; k) \leq \mathrm{A}_q(v-1, d; k) \left[{v \atop v-1}\right]_q / \left[{v-k \atop v-1-k}\right]_q$. □

We call Inequality (7.1) *Johnson IIa* and Inequality (7.2) *Johnson IIb*.

For partial spreads, i.e., $d = 2k$, Inequality (7.1) gives $\mathrm{A}_q(v, 2k; k) \leq \left\lfloor \frac{q^v-1}{q^k-1} \right\rfloor$ which is Corollary 125 and similarly, for $d = 2(v-k)$, Inequality (7.2) gives $\mathrm{A}_q(v, 2v-2k; k) \leq \left\lfloor \frac{q^v-1}{q^{v-k}-1} \right\rfloor$. This correspondence involving orthogonality is analyzed in the next lemma.

Some literature omits Inequality 7.2 and only state Inequality 7.1, e.g., [XF09, Theorem 3]. An analogous behavior may be observed in the classical case of constant weight codes, in which e.g. [MS77b, Theorem 4 on page 527] omits one of the two bounds and formulates Problem (2) on page 528 with the hint that ones should be replaced by zeros as exercise for the reader.

114 Proposition (cf. [EV11a, Section III, Lemma 13], [HK17b, Proposition 2])
Johnson IIa and Johnson IIb are equivalent using orthogonality.

Proof
We have

$$\mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; v-k) \overset{(7.1)}{\leq} \frac{q^v-1}{q^{v-k}-1} \mathrm{A}_q(v-1, d; v-k-1) = \frac{q^v-1}{q^{v-k}-1} \mathrm{A}_q(v-1, d; k),$$

which is Johnson IIb, and

$$\mathrm{A}_q(v, d; k) = \mathrm{A}_q(v, d; v-k) \overset{(7.2)}{\leq} \frac{q^v-1}{q^k-1} \mathrm{A}_q(v-1, d; v-k) = \frac{q^v-1}{q^k-1} \mathrm{A}_q(v-1, d; k-1),$$

which is Johnson IIa. □

The two bounds in Theorem 113 may be applied recursively. In the classical case it is not settled which of the two corresponding bounds is stronger, cf. [MS77b, Research Problem 17.1]. Let $A(n, d, w)$ be the maximum size of a binary constant weight code of length n, Hamming distance d and weight w. Then the two corresponding inequalities to Theorem 113 are $A(n, d, w) \leq \lfloor n/w \cdot A(n-1, d, w-1) \rfloor$ and $A(n, d, w) \leq \lfloor n/(n-w) \cdot A(n-1, d, w) \rfloor$. Applying the first bound yields

$$A(28, 8, 13) \leq \lfloor 28/13 \cdot A(27, 8, 12) \rfloor \leq \lfloor 28/13 \cdot 10547 \rfloor = 22716$$

while applying the second bound yields

$$A(28, 8, 13) \leq \lfloor 28/15 \cdot A(27, 8, 13) \rfloor \leq \lfloor 28/15 \cdot 11981 \rfloor = 22364$$

using the numerical bounds from `http://webfiles.portal.chalmers.se/s2/research/kit/bounds/cw.html`, cf. [AVZ00]. The authors of [EV11a; KSK09] state that the optimal choice of Inequality (7.1) or Inequality (7.2) also is not settled. We are able to answer this particular question for CDCs.

115 **Proposition ([HK17b, Proposition 3])**
For $q \ge 2$ prime power and integers $0 \le k \le v-k$ and $2 \le d/2 \le \min\{k, v-k\}$, we have

$$\left\lfloor \frac{q^v-1}{q^k-1} \mathrm{A}_q(v-1,d;k-1) \right\rfloor \le \left\lfloor \frac{q^v-1}{q^{v-k}-1} \mathrm{A}_q(v-1,d;k) \right\rfloor .$$

Moreover, the equality holds iff $v = 2k$.

Proof
By considering orthogonal codes, we obtain equality for $v = 2k$. Now we assume $k < v/2$ and show

$$\frac{q^v-1}{q^k-1} \mathrm{A}_q(v-1,d;k-1) + 1 \le \frac{q^v-1}{q^{v-k}-1} \mathrm{A}_q(v-1,d;k), \tag{7.3}$$

which implies the proposed statement. Considering the size of an LMRD code, we can lower bound the right hand side of Inequality (7.3) to

$$\frac{q^v-1}{q^{v-k}-1} \mathrm{A}_q(v-1,d;k) \ge \frac{q^v-1}{q^{v-k}} \cdot q^{(v-k-1)(k-d/2+1)}.$$

Since

$$\frac{\begin{bmatrix} v-1 \\ k-1 \end{bmatrix}_q}{\begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q} = \frac{\prod_{i=1}^{k-1} \frac{q^{v-k+i}-1}{q^i-1}}{\prod_{i=1}^{d/2-1} \frac{q^{v-k+i}-1}{q^i-1}} \le \prod_{i=d/2}^{k-1} \frac{q^{v-k+i}}{q^i-1} = q^{(v-k)(k-d/2)} \prod_{i=d/2}^{k-1} \frac{1}{1-q^{-i}}$$

we can use the Anticode bound to upper bound the left hand side of Inequality (7.3) to

$$\frac{q^v-1}{q^k-1} \mathrm{A}_q(v-1,d;k-1) + 1 \le \frac{q^v-1}{q^k-1} \cdot q^{(v-k)(k-d/2)} \cdot \mu(k-1,d/2,q) + 1,$$

where $\mu(a,b,q) := \prod_{i=b}^{a} \left(1-q^{-i}\right)^{-1}$. Thus, it suffices to verify

$$\frac{q^{k-d/2+1}}{q^k-1} \cdot \mu(k-1,d/2,q) + \frac{1}{f} \le 1, \tag{7.4}$$

where we have divided by

$$f := \frac{q^v-1}{q^{v-k}} \cdot q^{(v-k-1)(k-d/2+1)} = \frac{q^v-1}{q} \cdot q^{(v-k-1)(k-d/2)}.$$

Since $d \geq 4$, we have $\mu(k-1, d/2, q) \leq \prod_{i=2}^{\infty} \left(1 - q^{-i}\right)^{-1} \leq \prod_{i=2}^{\infty} \left(1 - 2^{-i}\right)^{-1} < 1.74$. Since $v \geq 4$ and $q \geq 2$, we have $\frac{1}{f} \leq \frac{2}{15}$. Since $k \geq 2$, we have $\frac{q^{k-d/2+1}}{q^k-1} \leq \frac{q}{q^2-1}$, which is at most $\frac{3}{8}$ for $q \geq 3$. Thus, Inequality (7.4) is valid for all $q \geq 3$.

If $d \geq 6$ and $q = 2$, then $\mu(k-1, d/2, q) \leq \prod_{i=3}^{\infty} \left(1 - 2^{-i}\right)^{-1} < 1.31$ and $\frac{q^{k-d/2+1}}{q^k-1} \leq \frac{1}{3}$, so that Inequality (7.4) is satisfied.

In the remaining part of the proof we assume $d = 4$ and $q = 2$. If $k = 2$, then $\mu(k-1, d/2, q) = 1$ and $\frac{q^{k-d/2+1}}{q^k-1} = \frac{2}{3}$. If $k = 3$, then $\mu(k-1, d/2, q) = \frac{4}{3}$ and $\frac{q^{k-d/2+1}}{q^k-1} = \frac{4}{7}$. If $k \geq 4$, then $\frac{q^{k-d/2+1}}{q^k-1} \leq \frac{8}{15}$, $\mu(k-1, d/2, q) \leq 1.74$, and $\frac{1}{f} \leq \frac{2}{255}$ due to $v \geq 2k \geq 8$. Thus, Inequality (7.4) is valid in all cases. □

Since Proposition 115 states that Johnson IIa dominates Johnson IIb if $k \leq v - k$, we can now initially assume $k \leq v - k$ and apply Johnson IIa recursively, which is then the optimal choice between these two inequalities in contrast to the lack of knowledge in the classical case.

116 Corollary (Recursive Johnson IIa)
For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers, we have

$$\mathrm{A}_q(v, d; k) \leq \left\lfloor \frac{q^v - 1}{q^k - 1} \left\lfloor \frac{q^{v-1} - 1}{q^{k-1} - 1} \left\lfloor \ldots \left\lfloor \frac{q^{v-k+d/2+1} - 1}{q^{d/2+1} - 1} \mathrm{A}_q(v - k + d/2, d; d/2) \right\rfloor \ldots \right\rfloor \right\rfloor \right\rfloor .$$

For example [EV11a, Theorem 6], [KSK09, Theorem 7], and [XF09, Corollary 3] list this bound in an explicit version by inserting $\mathrm{A}_q(v - k + d/2, d; d/2) \leq \left\lfloor \frac{q^{v-k+d/2}-1}{q^{d/2}-1} \right\rfloor$, which is the simplest partial spread bound, cf. Corollary 125.

If, in addition to inserting Corollary 125, also the rounding in each step is omitted, we obtain the sometimes called *Compact Johnson bound*:

117 Corollary (Compact Johnson bound, [ZJX11, Proposition 1])
For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers, we have

$$\mathrm{A}_q(v, d; k) \leq \frac{\begin{bmatrix} v \\ k-d/2+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-d/2+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v-k+d/2-1 \\ d/2-1 \end{bmatrix}_q}.$$

This is exactly the Anticode bound of Theorem 107 for $k \leq v/2$ by applying Lemma 7 and in particular Inequality 7.1 dominates the Anticode bound if $k \leq v - k$.

The Johnson bound could be improved in [KK17] by considering multisets of points which are q^r-divisible, i.e., a multiset $\mathcal{P}$ of points in $\mathbb{F}_q^v$ is called q^r-divisible for $1 \le r \le v-1$, iff $\#\mathcal{P} \equiv \#(\mathcal{P} \cap H) \pmod{q^r}$ for any hyperplane $H \le \mathbb{F}_q^v$, where $\mathcal{P} \cap H$ is also a multiset and contains exactly the points of $\mathcal{P}$ which are in H. The authors of [KK17] show that the multiset of points corresponding to a $(v, N, d; k)_q$ CDC with $2 \le k$ is q^{k-1}-divisible.

Here we use a modified notation which was applied in e.g. [Hei+17a], too.

118 **Definition (cf. [Hei+17a])**
Let $q \ge 2$ be a prime power and a and k positive integers. Then

$$\left\{\frac{a}{[k]_q}\right\}_k := \max\left\{b \in \mathbb{Z} \;\middle|\; \exists a_1, \ldots, a_k \in \mathbb{Z}_{\ge 0} : a - b[k]_q = \sum_{i=1}^{k} a_i q^{k-i}[i]_q\right\}.$$

This allows to state the *Improved Johnson bound.*

119 **Theorem (Improved Johnson bound, [KK17, Theorem 3 and 4])**
For $q \ge 2$ prime power and $2 \le d/2 \le k \le v-k$ integers, we have

$$\mathrm{A}_q(v, d; k) \le \left\{\frac{q^v - 1}{q^k - 1}\,\mathrm{A}_q(v-1, d; k-1)\right\}_k.$$

As an example, we have $\mathrm{A}_2(9, 6; 4) \le \left\{\frac{[9]_2\,\mathrm{A}_2(8,6;3)}{[4]_2}\right\}_4 = \left\{\frac{17374}{[4]_2}\right\}_4 = 1156$ with $\mathrm{A}_2(8, 6; 3) = 34$, cf. Theorem 127 since $17374 - 1156 \cdot 15 = 34 = 8 + 12 + 14$ but neither $17374 - 1157 \cdot 15 = 19$ nor $17374 - 1158 \cdot 15 = 4$ can be written as non-negative integer combination of 8, 12, 14, and 15. This improves on Johnson IIa (Inequality 7.1 in Theorem 113) by two. In [KK17] is an easy algorithm to verify whether a given integer can be represented as $\sum_{i=1}^{k} a_i q^{k-i}[i]_q$ in Definition 118.

Similar to Corollary 116 the bound of Theorem 119 can also be applied recursively. This bound is called *Recursive Improved Johnson bound.*

120 **Corollary (Recursive Improved Johnson bound, cf. [KK17])**
For $q \ge 2$ prime power and $2 \le d/2 \le k \le v-k$ integers, we have

$$\mathrm{A}_q(v, d; k) \le \left\{\frac{q^v - 1}{q^k - 1}\left\{\frac{q^{v-1} - 1}{q^{k-1} - 1}\left\{\ldots\left\{\frac{q^{v'+1} - 1}{q^{\frac{d}{2}+1} - 1}\,\mathrm{A}_q(v', d; \frac{d}{2})\right\}_{\frac{d}{2}+1} \ldots\right\}_{k-2}\right\}_{k-1}\right\}_k,$$

where $v' = v - k + d/2$ and $\{a/[k]_q\}_k$ is defined in Definition 118.

Linear Programming Bound Applying Theorem 39 to the q-Johnson scheme allows to use the linear programming method, described in Chapter 2. However, numerical computations indicate that it is not better than the Anticode bound (Theorem 107) which is called Compact Johnson bound (Corollary 117).

In the case of the q-Johnson scheme $\left(\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}, \{R_0, R_1, \ldots, R_k\}\right)$, we have $(U, W) \in R_i$ iff $\mathrm{d_s}(U, W) = 2i$ for $U, W \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ and hence the inner distribution a of any $(v, \#C, d; k)_q$ CDC C fulfills $a_i = 0$ for all $1 \le i \le d/2 - 1$. Therefore, the linear programming method involving these additional constraints and parameters ($Q_{i,j}$ and f_j) below Theorem 39 is:

121 Theorem (Linear Programming bound [ZJX11, Proposition 3])
For $q \ge 2$ prime power and $2 \le d/2 \le \min\{k, v-k\}$ integers, we have

$$\begin{aligned}
&\mathrm{A}_q(v, d; k) \\
&\le 1 + \max\left\{ \sum_{i=d/2}^{k} x_i \;\middle|\; \sum_{i=d/2}^{k} -Q_{i,j} x_i \le f_j \,\forall j \in [k] \wedge x_i \ge 0 \,\forall i \in \{d/2, \ldots, k\} \right\} \\
&= 1 + \min\left\{ \sum_{j=1}^{k} y_j f_j \;\middle|\; \sum_{j=1}^{k} Q_{i,j} y_j \le -1 \,\forall i \in \{d/2, \ldots, k\} \wedge y_j \ge 0 \,\forall j \in [k] \right\}
\end{aligned}$$

The authors of [ZJX11] proved that the Compact Johnson Bound (Corollary 117) can be interpreted as feasible solution for the constraints of the minimization linear program in Theorem 121. Therefore, the Linear Programming bound yields a stronger upper bound than the Compact Johnson bound, but numerical computations for small parameters ($q \le 9$ and $v \le 30$) indicate that both bounds are equal, i.e., $\begin{bmatrix} v \\ k-d/2+1 \end{bmatrix}_q / \begin{bmatrix} k \\ k-d/2+1 \end{bmatrix}_q$ is assumed to be the optimal value for any linear program in Theorem 121 for these parameters.

Sporadic cases In only two non-partial spread cases, the upper bound could be further improved:

122 Theorem ([HKK15, Theorem 1])
$\mathrm{A}_2(6, 4; 3) = 77$.

123 Proposition (Theorem 191 and [HK17a])
$\mathrm{A}_2(8, 6; 4) = 257$.

Unfortunately, these two improved upper bounds do not tighten Corollary 116 for any set of parameters as Lemma 198 shows.

7.1 Upper bounds for partial spreads

In the case of partial spreads, i.e., CDCs with maximum possible subspace distance $d = 2k$, more elaborate upper bounds are known. Interestingly, they involve the remainder $r \equiv v \pmod{k}$ with $0 \le r < k$. The question of the best upper bound in the subclass of spreads, i.e., $r = 0$, is completely settled.

124 **Theorem ([Seg64, §VI])**
Let $q \ge 2$ be a prime power and $1 \le k \le v$ be integers. Then $\mathbb{F}_q^v$ contains a spread iff $k \mid v$.

Since a k-spread in $\mathbb{F}_q^v$ is a $(v, (q^v - 1)/(q^k - 1), 2k; k)_q$ CDC, it fulfills the simplest of all upper bounds for partial spreads with equality:

125 **Corollary**
For $q \ge 2$ prime power and $2 \le k \le v - k$ integers, we have $\mathrm{A}_q(v, 2k; k) \le \frac{q^v-1}{q^k-1}$ which is equality iff $k \mid v$. Moreover, using $v = tk + r$, $2 \le t$, and $0 \le r < k$ integers, we have $\left\lfloor \frac{q^v-1}{q^k-1} \right\rfloor = \frac{q^v-q^{k+r}}{q^k-1} + q^r$.

Proof
Since the minimum distance is $2k$, any point in $\mathbb{F}_q^v$ is in at most one codeword. There are $\begin{bmatrix} v \\ 1 \end{bmatrix}_q = \frac{q^v-1}{q-1}$ points in $\mathbb{F}_q^v$, and $\begin{bmatrix} k \\ 1 \end{bmatrix}_q = \frac{q^k-1}{q-1}$ points in any codeword, so the first statement follows immediately.

The last statement follows from $\left\lfloor \frac{q^v-1}{q^k-1} \right\rfloor = q^{k+r} \underbrace{\frac{q^{k(t-1)} - 1}{q^k - 1}}_{\in \mathbb{Z}} + q^r + \underbrace{\left\lfloor \frac{q^r - 1}{q^k - 1} \right\rfloor}_{=0}$. □

Note that this is also the Anticode bound Theorem 107 applied to $d/2 = k$.

Superior upper bounds are known if one focuses on partial spreads with $k \nmid v$. If the remainder r is one then the question of the best upper bound is also settled.

126 **Theorem ([Beu75])**
For $q \ge 2$ prime power and integers $v = tk + r$, $2 \le t$, $0 \le r < k$, we have $\mathrm{A}_q(v, 2k; k) \ge \frac{q^v-q^{k+r}}{q^k-1} + 1$ with equality for $r \le 1$.

This construction provides codes of the same size as Theorem 58.

By a computer search described in [ElZ+10], an $(8, 34, 6; 3)_2$ CDC was found, which improves on the construction of Theorem 126 by exactly one. Applying the upper bound of Theorem 129, one gets $\mathrm{A}_2(8, 6; 3) = 34$ and recursively $\mathrm{A}_2(8+3l, 6; 3)$ for $l \geq 0$. Besides these parameters, no partial spread exceeding the lower bound from Theorem 126 is known. This also settled the determination of the best upper bound if $q = 2 \wedge v \equiv 2 \pmod 3$ ($6 \leq v$ integer).

127 Theorem ([ElZ+10, Theorem 5])
For $2 \leq t$ we have $\mathrm{A}_2(3t+2, 6; 3) = \frac{2^{3t+2}-2^5}{2^3-1} + 2$.

For the remaining values of k, i.e., $q = 2 \wedge v \equiv 2 \pmod k$ for arbitrary $4 \leq k \leq v-k$ integers, the question of the best upper bound could also be answered. They match the cardinality of the construction in Theorem 126.

128 Theorem ([Kur17a, Theorem 4.3])
For $2 \leq t$ and $4 \leq k$ we have $\mathrm{A}_2(tk+2, 2k; k) = \frac{2^{tk+2}-2^{k+2}}{2^k-1} + 1$.

For almost 30 years the best general upper bound was given by Drake and Freeman.

129 Theorem ([DF79, Corollary 8], cf. [BB52])
For $q \geq 2$ prime power and integers $v = tk + r$, $2 \leq t$, $1 \leq r < k$, and $\theta = \lfloor (\sqrt{1+4q^k(q^k-q^r)} - (2q^k - 2q^r + 1))/2 \rfloor$ we have $\mathrm{A}_q(v, 2k; k) \leq \frac{q^v - q^{k+r}}{q^k-1} + q^r - 1 - \theta$.

Quite recently this bound could be improved by considering the non-covered points of a partial spread as columns of a generator matrix of a linear, projective, and divisible code together with the linear programming method, cf. [Hei+17b; HKK18a; HKK18b]. In fact Theorem 129 is a special case of Theorem 130 for $y = k$.

130 Theorem ([Kur17b, Theorem 2.10] and [DF79] for $y = k$)
For $q \geq 2$ prime power and integers $v = tk + r$, $2 \leq t$, $1 \leq r < k$, $0 \leq z = [r]_q + 1 - k$, and $\max\{r, 2\} \leq y \leq k$, we have

$$\mathrm{A}_q(v, 2k; k) \leq \frac{q^v - q^{k+r}}{q^k - 1} + \left\lceil q^y - \frac{1}{2} - \frac{1}{2}\sqrt{1 + 4q^y(q^y - (z+y-1)(q-1) - 1)} \right\rceil.$$

The next theorem shows that the construction of Theorem 126 is asymptotically optimal, i.e., if k is much larger than the remainder of the division of v by k.

131 **Theorem ([NS17, Theorem 5])**
For $q \geq 2$ prime power and integers $v = tk + r$, $2 \leq t$, $1 \leq r < k$, and $[r]_q < k$, we have $\mathrm{A}_q(v, 2k; k) = \frac{q^v - q^{k+r}}{q^k - 1} + 1$.

Since $[2]_2 = 3 < k$, Theorem 131 contains Theorem 128 as special case.

Applying similar techniques, the result was generalized to $k \leq [r]_q$. In fact, Theorem 131 is a special case of Theorem 132 with $z = 0$ and the upper bound of Theorem 127 is a special case of Theorem 132 with $z = 1$.

132 **Theorem ([Kur17b, Theorem 2.9] and [NS17] for $z = 0$)**
For $q \geq 2$ prime power and integers $v = tk + r$, $2 \leq t$, $1 \leq r < k$, and $z = \max\{0, [r]_q + 1 - k\} \leq [r]_q/2$ we have $\mathrm{A}_q(v, 2k; k) \leq \frac{q^v - q^{k+r}}{q^k - 1} + 1 + z(q - 1)$.

Using Theorem 130 the restriction $z \leq [r]_q/2$ can be removed from Theorem 132, cf. [HKK18a].

There are also 21 sporadic series that are better by exactly one compared to Theorem 130 and Theorem 132.

133 **Theorem ([Kur17b, Appendix])**
Let $2 \leq t$. Then

$\mathrm{A}_2(4t + 3, 8; 4) \leq 2^4 \cdot \frac{2^{4t-1} - 2^3}{2^4 - 1} + 4$
$\mathrm{A}_2(6t + 4, 12; 6) \leq 2^6 \cdot \frac{2^{6t-2} - 2^4}{2^6 - 1} + 8$
$\mathrm{A}_2(6t + 5, 12; 6) \leq 2^6 \cdot \frac{2^{6t-1} - 2^5}{2^6 - 1} + 18$
$\mathrm{A}_3(4t + 3, 8; 4) \leq 3^4 \cdot \frac{3^{4t-1} - 3^3}{3^4 - 1} + 14$
$\mathrm{A}_3(5t + 3, 10; 5) \leq 3^5 \cdot \frac{3^{5t-2} - 3^5}{3^3 - 1} + 13$
$\mathrm{A}_3(5t + 4, 10; 5) \leq 3^5 \cdot \frac{3^{5t-1} - 3^4}{3^5 - 1} + 44$
$\mathrm{A}_3(6t + 4, 12; 6) \leq 3^6 \cdot \frac{3^{6t-2} - 3^4}{3^6 - 1} + 41$
$\mathrm{A}_3(6t + 5, 12; 6) \leq 3^6 \cdot \frac{3^{6t-1} - 3^5}{3^6 - 1} + 133$
$\mathrm{A}_3(7t + 4, 14; 7) \leq 3^7 \cdot \frac{3^{7t-3} - 3^4}{3^7 - 1} + 40$
$\mathrm{A}_4(5t + 3, 10; 5) \leq 4^5 \cdot \frac{4^{5t-2} - 4^3}{4^5 - 1} + 32$
$\mathrm{A}_4(6t + 3, 12; 6) \leq 4^6 \cdot \frac{4^{6t-3} - 4^3}{4^6 - 1} + 30$
$\mathrm{A}_4(6t + 5, 12; 6) \leq 4^6 \cdot \frac{4^{6t-1} - 4^5}{4^6 - 1} + 548$
$\mathrm{A}_4(7t + 4, 14; 7) \leq 4^7 \cdot \frac{4^{7t-3} - 4^4}{4^7 - 1} + 128$
$\mathrm{A}_5(5t + 2, 10; 5) \leq 5^5 \cdot \frac{5^{5t-3} - 5^2}{5^5 - 1} + 7$
$\mathrm{A}_5(5t + 4, 10; 5) \leq 5^5 \cdot \frac{5^{5t-1} - 5^4}{5^5 - 1} + 329$
$\mathrm{A}_7(5t + 4, 10; 5) \leq 7^5 \cdot \frac{7^{5t-1} - 7^2}{7^5 - 1} + 1246$
$\mathrm{A}_8(4t + 3, 8; 4) \leq 8^4 \cdot \frac{8^{4t-1} - 8^3}{8^4 - 1} + 264$
$\mathrm{A}_8(5t + 2, 10; 5) \leq 8^5 \cdot \frac{8^{5t-3} - 8^2}{8^5 - 1} + 25$
$\mathrm{A}_8(6t + 2, 12; 6) \leq 8^6 \cdot \frac{8^{6t-4} - 8^2}{8^6 - 1} + 21$
$\mathrm{A}_9(3t + 2, 6; 3) \leq 9^3 \cdot \frac{9^{3t-1} - 9^2}{9^3 - 1} + 41$
$\mathrm{A}_9(5t + 3, 10; 5) \leq 9^5 \cdot \frac{9^{5t-2} - 9^3}{9^5 - 1} + 365$

Currently, Corollary 125 (in the spread case), Theorem 130, Theorem 132, and Theorem 133 constitute the tightest parametric bounds for partial spreads.

Theorem 108 improves on the upper bound of partial spreads compared to Corollary 125.

134 Proposition
For $q \geq 2$ prime power, $2 \leq k$, $1 \leq w$, and $q^w+3 \leq k$ integers, we have $\mathrm{A}_q(2k+w, 2k; k) \leq \mathrm{A}_q(2k+w-1, 2k-2; k-1)$ and this is tighter then $\mathrm{A}_q(2k+w, 2k; k) \leq \left\lfloor \frac{q^{2k+w}-1}{q^k-1} \right\rfloor = q^{k+w} + q^w$, which is implied by Corollary 125.

Proof
Note that $q^w + 3 \leq k \Rightarrow w < k$. The first inequality follows from Theorem 108 with $m = 2k + w - 1$ and $t = 1$ involving Lemma 3 and the equality from $q^{2k+w} - 1 = (q^{k+w} + q^w)(q^k - 1) + q^w - 1$. We have $[w+1]_q = [w]_q + q^w$ by the definition of the q-number (or by Lemma 3) and $q^w + 3 \leq k \Leftrightarrow [w]_q \leq (k-4)/(q-1)$. In particular, $[w+1]_q = [w]_q + q^w \leq q^w + (k-4)/(q-1) \leq (k-3)+(k-4) \leq 2k-4 \Leftrightarrow [w+1]_q + 1 - (k-1) \leq [w+1]_q/2$ is needed for the existence of a suitable z in Theorem 132 with $t = 2$ and $r = w + 1$, which in turn shows

$$\mathrm{A}_q(2k + w - 1, 2k - 2; k - 1) \leq \frac{q^{2k+w-1} - q^{k+w}}{q^{k-1} - 1} + 1 + z(q-1) = q^{k+w} + 1 + z(q-1).$$

Finally, $z \leq [w+1]_q + 1 - (k-1) = [w]_q - k + 2 + q^w < [w]_q$ implies

$$q^{k+w} + 1 + z(q-1) < q^{k+w} + 1 + [w]_q(q-1) = q^{k+w} + q^w. \qquad \square$$

7.2 Overview

For $q \geq 2$ prime power and $2 \leq d/2 \leq k \leq v - k$ integers, an overview of dominance relations between upper bounds is depicted here. An arrow $A \to B$ means in this context, that the bound A is at most the value of the bound B on all parameters on which both are defined that fulfill $q \geq 2$ prime power and $2 \leq d/2 \leq k \leq v - k$ integers. If this is a tie then $A \to B$ means that the parameters on which A is defined is a superset of the parameters on which B is defined.

Figure 8 shows the dominance relations for $d/2 < k$ without the two sporadic cases in Theorem 122 and Proposition 123 and Figure 9 shows the dominance relations for $d/2 = k$ without the 21 sporadic series in Theorem 133 and without the spread case, i.e., $k \mid v$.

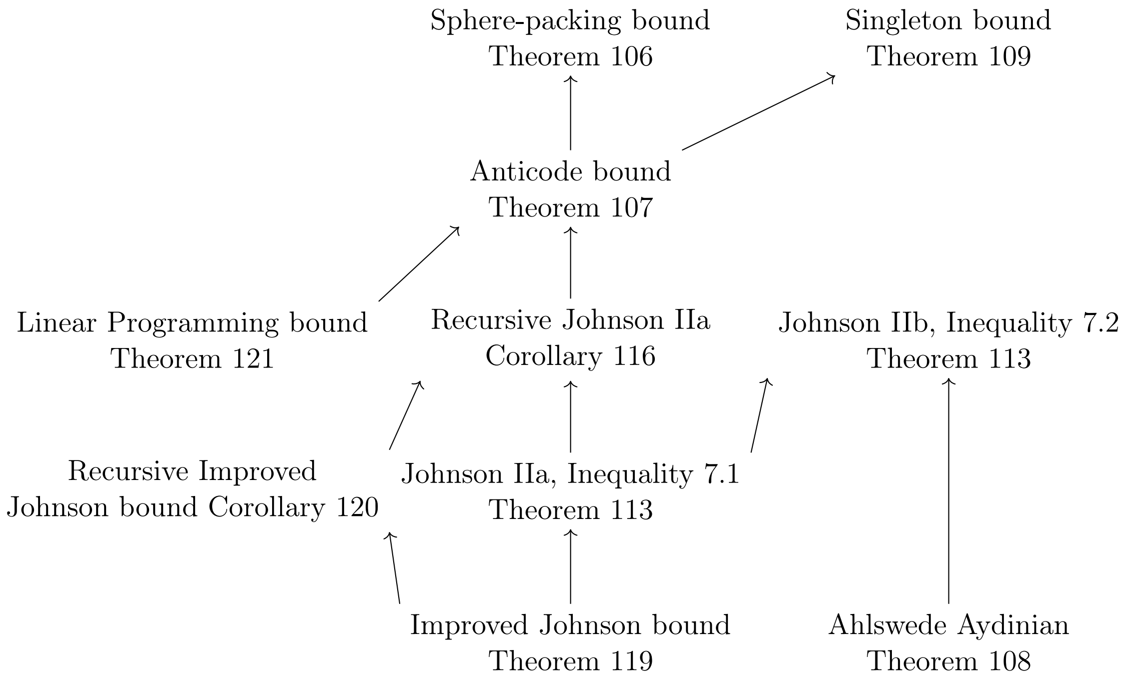


Figure 8: Dominance relations of upper bounds for non-partial spread CDCs, without the two sporadic cases.

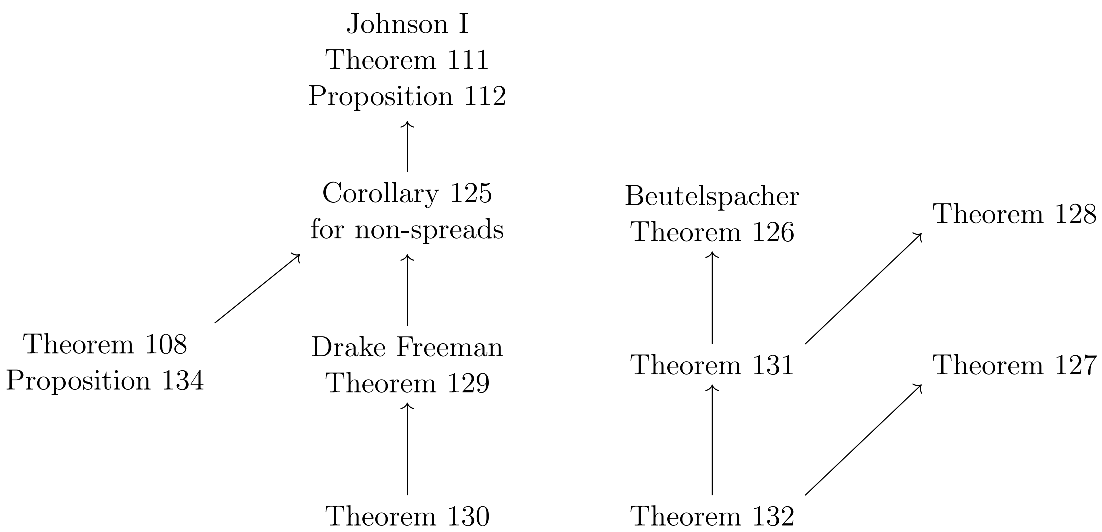


Figure 9: Dominance relations of upper bounds for partial spreads, without the 21 sporadic series and spreads.

8 The improved linkage construction

Contents of this chapter were previously published in [HK17b].

We slightly improve the so-called linkage construction by Gluesing-Luerssen, Troha / Morrison [GMT15; GT16] and Silberstein, Trautmann [ST15], which yields the best known lower bounds for $\mathrm{A}_q(v, d; k)$ for many parameters, see e.g. `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16].

In [GT16] Gluesing-Luerssen and Troha introduced the so-called linkage construction which uses two constant dimension codes of the same codeword-dimension k, subspace distance d, and field size q. These two CDCs may still differ in their ambient vector space and cardinality. Together with a *fitting* rank metric code, the linkage construction embeds both CDCs in a larger common ambient space while padding one of the two CDCs with the matrices of the rank metric code. This idea leads to a recursive lower bound for $\mathrm{A}_q(v, d; k)$ which is one of the largest for general parameters.

The same method was invented independently by Silberstein and Trautmann as a Corollary to their Construction D in [ST15] and also appeared in [GMT15, Theorem 5.1] for cyclic orbit codes and in [EV11a, Theorem 11] for spreads.

135 Theorem ([GT16, Theorem 2.3], cf. [ST15, Corollary 39])
For $q \geq 2$ prime power, $0 \leq k \leq v_i$ integers, d_i even integer ($i \in \{1, 2\}$), and an integer d_r, let C_i be a non-empty $(v_i, N_i, d_i; k)_q$ CDC for $i \in \{1, 2\}$ and let C_r be a non-empty $[k \times v_2, n_r, d_r]_q$ linear rank metric code. Then

$$\{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\} \cup \{\tau^{-1}(\mathbf{0}_{k\times v_1} \mid \tau(W)) : W \in C_2\}$$

is a $(v_1 + v_2, N_1 q^{n_r} + N_2, \min\{d_1, d_2, 2d_r\}; k)_q$ CDC.

Since the generated CDC depends on the choice of C_1, C_2, and C_r and in particular their representatives within isomorphism classes, one typically obtains many isomorphism classes of CDCs with the same parameters.

[ST15, Theorem 37] corresponds to the weakened version of Theorem 135 in which $C_2 = \emptyset$, cf. [GMT15, Theorem 5.1]. In [ST15, Corollary 39] Silberstein and Trautmann obtain the same cardinality, by assuming $d_1 = d_2 = 2d_r$ which is indeed the optimal choice, and $3k \leq v$, which is no restriction since for $2k \leq v \leq 3k - 1$ the optimal choice of Δ in [ST15, Corollary 39] is given by $\Delta = v - k$ and in that case the constructed CDC is an LMRD code extended with a $(v - k, N, d; k)_q$ CDC. For $v - k < \Delta \leq v$ the constructed code is an embedded $(\Delta, N, d; k)_q$ CDC.

The main aspect about the last theorem is that the pivot vectors of any codeword in $\{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\}$ and the pivot vector for any codeword in $\{\tau^{-1}(\mathbf{0}_{k\times v_1} \mid \tau(W)) : W \in C_2\}$ have their ones in distinct positions. Hence, Lemma 54 guarantees that their subspace distance is large enough. Applying the very same lemma can increase the size of the constructed code by allowing the second CDC to be in a larger ambient space, i.e., the ones in the pivot vectors may overlap. This in turn shows that Theorem 135 is a special case involving $d = 2k$ and linearity of the rank metric codes of the following theorem.

136 **Theorem ([HK17b, Theorem 18])**
For $q \ge 2$ prime power, $0 \le k \le v_i$ integers, $2 \le d_i$ even integer ($i \in \{1, 2\}$), $1 \le d_r \in \mathbb{Z}$, and $2 \le d$ even integer, let C_i be a non-empty $(v_i, N_i, d_i; k)_q$ CDC for $i \in \{1, 2\}$ and let C_r be a non-empty $(k \times (v_2 - k + d/2), N_r, d_r)_q$ rank metric code. Then

$$\{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\} \cup \{\tau^{-1}(\mathbf{0}_{k\times(v_1-k+d/2)} \mid \tau(W)) : W \in C_2\}$$

is a $(v_1 + v_2 - k + d/2, N_1N_r + N_2, \min\{d_1, d_2, 2d_r, d\}; k)_q$ CDC.

Proof
Denote the sets with $\mathcal{C}_1 = \{\tau^{-1}(\tau(U) \mid M) : U \in C_1, M \in C_r\}$, $\mathcal{C}_2 = \{\tau^{-1}(\mathbf{0}_{k\times(v_1-k+d/2)} \mid \tau(W)) : W \in C_2\}$, and $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$. The dimension of the ambient space and the codewords of $\mathcal{C}$ directly follow from the construction. Since the constructed matrices are all in RREF and pairwise distinct, $\mathcal{C}$ is well defined and we have $\#\mathcal{C} = N_1N_r + N_2$. It remains to lower bound the minimum subspace distance of $\mathcal{C}$.

Let $A, C \in C_1$ and $B, D \in C_r$. If $A \ne C$, then

$$\begin{aligned}\mathrm{d_s}(\tau^{-1}(\tau(A) \mid B), \tau^{-1}(\tau(C) \mid D)) &= 2\left(\mathrm{rk}\begin{pmatrix}\tau(A) & B\\ \tau(C) & D\end{pmatrix} - k\right)\\ &\ge 2\left(\mathrm{rk}\begin{pmatrix}\tau(A)\\ \tau(C)\end{pmatrix} - k\right) = \mathrm{d_s}(A, C) \ge d_1.\end{aligned}$$

If $A = C$ but $B \ne D$, we have

$$\begin{aligned}\mathrm{d_s}(\tau^{-1}(\tau(A) \mid B), \tau^{-1}(\tau(C) \mid D)) = 2\left(\mathrm{rk}\begin{pmatrix}\tau(A) & B\\ \tau(C) & D\end{pmatrix} - k\right)\\ = 2\left(\mathrm{rk}\begin{pmatrix}\tau(A) & B\\ \mathbf{0} & D-B\end{pmatrix} - k\right) = 2(k + \mathrm{rk}(D - B) - k) \ge 2d_r.\end{aligned}$$

For $A' \ne C' \in C_2$,

$$\mathrm{d_s}(\tau^{-1}(\mathbf{0}_{k\times(v_1-k+d/2)} \mid \tau(A')), \tau^{-1}(\mathbf{0}_{k\times(v_1-k+d/2)} \mid \tau(C'))) = \mathrm{d_s}(A', C') \ge d_2.$$

At last, for two codewords $U \in \mathcal{C}_1$ and $W \in \mathcal{C}_2$, we apply Lemma 54. The pivot vector $\mathrm{p}(U)$ has its k ones in the first v_1 positions and the pivot vector $\mathrm{p}(W)$ has its k ones not in the first $v_1 - k + d/2$ positions, so that the ones can coincide at most at the positions $\{v_1 - k + d/2 + 1, \ldots, v_1\}$. Thus, $\mathrm{d_s}(U, W) \ge \mathrm{d_h}(\mathrm{p}(U), \mathrm{p}(W)) \ge k - (k - d/2) + k - (k - d/2) = d$. □

The next example shows a case in which Theorem 136 improves on Theorem 135.

137 **Example ([HK17b])**
Consider $(7, N, 4; 3)_2$ CDCs.

On the one hand, applying Theorem 135 implies $(v_1, v_2) \in \{(3,4),(4,3)\}$ and $4 \le \min\{d_1, d_2, 2d_r\}$. We have $\#C_1 \le \mathrm{A}_2(v_1, d_1; 3) = 1$ and $\#C_2 \le \mathrm{A}_2(v_2, d_2; 3) = 1$ in both cases. Hence, the size of the constructed code is bounded by $N \le 1 \cdot 2^{2v_2} + 1 \le 257$.

On the other hand, Theorem 136 allows to choose $d = 4$, i.e., the pivot-ones may overlap in exactly one position. This allows to choose $(v_1, v_2) = (3, 5)$, $d_1 = d_2 = 2d_r = 4$, $\#C_1 = \mathrm{A}_2(3, 4; 3) = 1$, and $\#C_2 = \mathrm{A}_2(5, 4; 3) = 9$. Using a $(3 \times 4, 2^8, 2)_2$ MRD code allows to construct a CDC of size $N = 1 \cdot 2^8 + 9 = 265$.

For $(7, N, 4; 3)_2$ CDCs, Theorem 136 is inferior compared to the best known lower bound 333, cf. Theorem 171. This situation changes in general. For $2 \le q \le 9$ prime power, $2 \le d/2 \le k \le v - k$, and $v \le 19$ integers Theorem 135 provides the best known lower bound for $\mathrm{A}_q(v, d; k)$ in 42.1% of the cases, while Theorem 136 provides the best known lower bound in 69.1% of the cases, see `http://subspacecodes.uni-bayreuth.de/cdctoplist/` associated with [Hei+16] for details. Since Theorem 135 is a special case of Theorem 136 the set of parameters for which Theorem 135 gives the best known lower bound is a subset of the set of parameters where Theorem 136 yields the best known lower bound.

Although Theorem 136 has some degrees of freedom, some of its parameters are obvious, if one wants to construct codes of largest possible size. First, both involved CDCs have to be maximum CDCs of cardinality $\mathrm{A}_q(v_i, d_i; k)$ or a reasonable lower bound, if the exact value is unknown. Second, the rank metric code has to be an MRD code of size $\lceil q^{\max\{k,v_2-k+d/2\}(\min\{k,v_2-k+d/2\}-d_r+1)} \rceil$. Third, $d_1 = d_2 = 2d_r \le d$, since otherwise it would be possible to increase the sizes of the involved rank metric codes or CDCs and therefore the size of the constructed code, until this condition is achieved. Fourth, the condition can be sharpened to $d_1 = d_2 = 2d_r = d$ as the following lemma shows. By increasing d, the ambient space dimension of the constructed CDC increases together with N_r and N_2, but for a larger ambient space a more tailored application of Theorem 136 allows larger CDCs.

138 **Lemma**
For $q \ge 2$ prime power, $k, v_i, d_i, d_r, d, l \in \mathbb{Z}$ $(i \in \{1,2\})$ and $0 \le k \le v_i$, $2 \le d_i$ even $(i \in \{1,2\})$, $1 \le d_r \in \mathbb{Z}$, $2 \le d$ even, and $2 \le l$ even, we have

$$\mathrm{A}_q(v_1, d; k) \cdot \left\lceil q^{\max\{k,v_2-k+(d+l)/2\}(\min\{k,v_2-k+(d+l)/2\}-d/2+1)} \right\rceil + \mathrm{A}_q(v_2, d; k) \le$$
$$\mathrm{A}_q(v_1, d; k) \cdot \left\lceil q^{\max\{k,(v_2+l/2)-k+d/2\}(\min\{k,(v_2+l/2)-k+d/2\}-d/2+1)} \right\rceil + \mathrm{A}_q((v_2 + l/2), d; k).$$

Proof
Since $v_2 - k + (d+l)/2 = (v_2 + l/2) - k + d/2$ both first summands are equal and $\mathrm{A}_q(v_2, d; k) \le \mathrm{A}_q((v_2 + l/2), d; k)$ concludes the proof. □

This discussion provides the following two corollaries of Theorem 136.

139 **Corollary ([HK17b, Corollary 3])**
For $q \ge 2$ prime power, $0 \le k \le \min\{v_1, v_2\}$ integers, and $2 \le d$ even, we have

$$\begin{aligned}&\mathrm{A}_q(v_1 + v_2 - k + d/2, d; k)\\ &\ge \mathrm{A}_q(v_1, d; k) \cdot \left\lceil q^{\max\{k, v_2-k+d/2\}(\min\{k,v_2-k+d/2\}-d/2+1)} \right\rceil + \mathrm{A}_q(v_2, d; k).\end{aligned}$$

By a variable substitution:

140 **Corollary ([HK17b, Corollary 4])**
For $q \ge 2$ prime power, $0 \le k \le m \le v - d/2$ integers, and $2 \le d$ even, we have

$$\begin{aligned}&\mathrm{A}_q(v, d; k)\\ &\ge \mathrm{A}_q(m, d; k) \cdot \left\lceil q^{\max\{k, v-m\}(\min\{k,v-m\}-d/2+1)} \right\rceil + \mathrm{A}_q(v - m + k - d/2, d; k).\end{aligned}$$

Not all possible values of m are of interest. In fact cardinalities for small values of m are exceeded by the choice $m^* = k$.

141 **Lemma**
For $q \ge 2$ prime power, $2 \le d/2 \le k \le v - k$ integers, $k \le m \le \min\{d/2 + k - 1, v - k\}$, and $m^* = k$ we have

$$\begin{aligned}&\mathrm{A}_q(m, d; k) \cdot \left\lceil q^{\max\{k, v-m\}(\min\{k,v-m\}-d/2+1)} \right\rceil + \mathrm{A}_q(v - m + k - d/2, d; k)\\ &\le \mathrm{A}_q(m^*, d; k) \cdot \left\lceil q^{\max\{k, v-m^*\}(\min\{k,v-m^*\}-d/2+1)} \right\rceil + \mathrm{A}_q(v - m^* + k - d/2, d; k)\\ &= q^{(v-k)(k-d/2+1)} + \mathrm{A}_q(v - d/2, d; k)\end{aligned}$$

and the corresponding CDC contains an LMRD.

Proof
First, $\mathrm{A}_q(m, d; k) = 1$ iff $0 \le k \le m$ and $d/2 > \min\{k, m-k\}$. The latter is implied by $m \le k + d/2 - 1$. Hence, using $k \le v - m$, $\mathrm{A}_q(m, d; k) \cdot \left\lceil q^{\max\{k,v-m\}(\min\{k,v-m\}-d/2+1)} \right\rceil +$ $\mathrm{A}_q(v - m + k - d/2, d; k)$ simplifies to $q^{\lambda(k-d/2+1)} + \mathrm{A}_q(\lambda + k - d/2, d; k)$ with $\lambda = v - m$. This term is maximal if λ is maximal, i.e., m is minimal which is the case for $m^* = k$. □

142 Example

For the parameters of $\mathrm{A}_2(9,4;3)$ we can apply Corollary 140 for all $m \in \{3,\dots,7\}$. The following table lists

$$\mathrm{A}_2(9,4;3) \geq \mathrm{A}_2(m,4;3) \cdot 2^{\max\{3,9-m\}(\min\{3,9-m\}-1)} + \mathrm{A}_2(10-m,4;3)$$

for all $m \in \{3,\dots,7\}$. As implied by Lemma 141, $m = 3$ is superior to $m = 4$ but the best lower bound of this method uses $m = 6$.

m	$\mathrm{A}_2(m,4;3)$	$2^{\max\{3,9-m\}(\min\{3,9-m\}-1)}$	$\mathrm{A}_2(10-m,4;3)$	$\mathrm{A}_2(9,4;3) \geq$
3	1	$2^{6\cdot 2}$	≥ 333	4429
4	1	$2^{5\cdot 2}$	77	1101
5	9	$2^{4\cdot 2}$	9	2313
6	77	$2^{3\cdot 2}$	1	4929
7	≥ 333	$2^{3\cdot 1}$	1	2665

The next question is to examine the case when there is no other possibility for m that is not covered by Lemma 141.

143 Corollary

For $q \geq 2$ prime power, $2 \leq k \leq v-k$ integers with $v \leq 3k-1$, and $d = 2k$, the improved linkage construction is equivalent to an extended LMRD, i.e., $\mathrm{A}_q(v,2k;k) \geq q^{v-k}+1$, which is also the upper bound for CDCs containing an LMRD for these parameters.

Proof

Using $v - d/2 \leq \min\{d/2+k-1, v-k\} \Leftrightarrow v \leq 3k-1$, the lower bound of the improved linkage construction of Corollary 140 is maximized by Lemma 141 for all possible m.

The last part follows with $\mathrm{A}_q(v-k,2k;k) = 1$ iff $0 \leq k \leq v-k$ and $d/2 = k > \min\{k, v-2k\}$, i.e., $2k \leq v < 3k$ and Proposition 99. □

Although the last statement is valid for many partial spreads, we can analyze the spread case in more detail.

144 Lemma ([HK17b, Lemma 4])

If $d = 2k$ and $k \mid v$, then Corollary 140 gives $\mathrm{A}_q(v,d;k) \geq \frac{q^v-1}{q^k-1}$ for all $m = k, 2k, \dots, v-k$ and smaller sizes otherwise.

Proof
Using Corollary 125, we get $\mathrm{A}_q(v', 2k; k) = (q^{v'} - 1)/(q^k - 1)$ for all integers v' being divisible by k and obtain

$$\begin{aligned}\mathrm{A}_q(v, 2k; k) &\geq \mathrm{A}_q(m, 2k; k) \cdot \left\lceil q^{\max\{k, v-m\}(\min\{k, v-m\}-k+1)} \right\rceil + \mathrm{A}_q(v-m, 2k; k) \\ &= \frac{q^m - 1}{q^k - 1} \cdot q^{v-m} + \frac{q^{v-m} - 1}{q^k - 1} = \frac{q^v - 1}{q^k - 1}\end{aligned}$$

if k divides m. Otherwise, $\mathrm{A}_q(m, 2k; k) < \frac{q^m-1}{q^k-1}$ and $\mathrm{A}_q(v-m, 2k; k) < \frac{q^{v-m}-1}{q^k-1}$ imply for the right hand side

$$\mathrm{A}_q(m, 2k; k) \cdot q^{v-m} + \mathrm{A}_q(v-m, 2k; k) < \frac{q^m - 1}{q^k - 1} \cdot q^{v-m} + \frac{q^{v-m} - 1}{q^k - 1} = \frac{q^v - 1}{q^k - 1}. \qquad \square$$

Algorithm 4 Dynamic programming approach for the tightest application of Corollary 140.

Require: $q \geq 2$ prime power, $0 \leq k$, $0 \leq v_{\max}$ integers, and $2 \leq d$ even, $f : \mathbb{Z}_{\geq k+d/2} \to \mathbb{Z}$ such that $f(v) \leq \mathrm{A}_q(v, d; k)$.
Ensure: $a(v) \leq \mathrm{A}_q(v, d; k)$ for all integral $v \leq v_{\max}$.

for $v \in \{-\infty, \ldots, k-1\}$ **do**
  $a(v) \leftarrow 0$
end for
for $v \in \{k, \ldots, k + d/2 - 1\}$ **do**
  $a(v) \leftarrow 1$
end for
for $v \in \{k + d/2, \ldots, v_{\max}\}$ **do**
  $a(v) \leftarrow f(v)$
  for $m \in \{k, \ldots, v - d/2\}$ **do**
    if $k < m \leq \min\{k + d/2 - 1, v - k\}$ **then**
      ▷ By Lemma 141 these m are inferior to $m^* = k$.
      continue
    end if
    $t \leftarrow a(m) \left\lceil q^{\max\{k, v-m\}(\min\{k, v-m\} - d/2 + 1)} \right\rceil + a(v - m + k - d/2)$
      ▷ only uses $a(i)$ for $i \leq v - d/2$
    $a(v) \leftarrow \max\{a(v), t\}$
  end for
end for
return $a(\cdot)$

The tightest evaluation of Corollary 140 can be computed with a dynamic programming approach, as depicted in Algorithm 4. This algorithm also uses an oracle f which incorporates additional lower bounds of $\mathrm{A}_q(v, d; k)$ in order to strengthen the computed lower bounds.

By arithmetic progressions of step size s, we can apply Corollary 140 recursively such that only two starting values are necessary.

145 Proposition ([HK17b, Proposition 6])
For $q \geq 2$ prime power and integers $0 \leq k \leq v_0$, $1 \leq d/2 \leq s$, and $0 \leq l$, we have

$$\mathrm{A}_q(v_0 + ls, d; k) \geq \mathrm{A}_q(v_0, d; k) \cdot b^l + \mathrm{A}_q(s + k - d/2, d; k)[l]_b$$

with $b = \left\lceil q^{\max\{k,s\}(\min\{k,s\}-d/2+1)} \right\rceil$.

If additionally $2k \leq v_0 + d/2$ and $d/2 \leq k + 1$, then we have

$$\mathrm{A}_q(v_0 + ls, d; k) \geq \mathrm{A}_q(s + k - d/2, d; k) \cdot \left(q^{k-d/2+1}\right)^{v_0-k+d/2} [l]_{q^{s(k-d/2+1)}} + \mathrm{A}_q(v_0, d; k).$$

Proof
Both sides of both parts of the proposition are equal if $l = 0$ and hence we assume wlog. $1 \leq l$. Next, we abbreviate $a(x) = \mathrm{A}_q(x, d; k)$ and $b(x) = \left\lceil q^{\max\{k,x\}(\min\{k,x\}-d/2+1)} \right\rceil$. Using this shortened notation, Corollary 140 is simply: $a(v) \geq a(m)b(v-m) + a(v-m+k-d/2)$ for all $m \in \{k, \ldots, v - d/2\}$.

Let $v = v_0 + ls$ and $m = v_0 + (l-1)s$. Since $1 \leq l$, $k \leq v_0$, and $d/2 \leq s$, we have $k \leq m \leq v - d/2$. Then applying Corollary 140 yields

$$a(v_0 + ls) \geq a(v_0 + (l-1)s) \cdot b(s) + a(s + k - d/2)$$

and by induction

$$a(v_0 + ls) \geq a(v_0 + (l-i)s) \cdot b(s)^i + a(s + k - d/2)[i]_{b(s)}$$

for all $i \in \{0, \ldots, l\}$ which is the first part of the proposition for $i = l$.

For the second part, applying Corollary 140 with $v = v_0 + ls$ and $m = s + k - d/2$, again with $k \leq m \leq v - d/2$, gives

$$a(v_0 + ls) \geq a(s + k - d/2) \cdot b(v_0 + (l-1)s - k + d/2) + a(v_0 + (l-1)s),$$

and by induction for all $i \in \{0, \ldots, l\}$:

$$a(v_0 + ls) \geq a(s + k - d/2) \cdot \sum_{j=1}^{i} b(v_0 + (l-j)s - k + d/2) + a(v_0 + (l-i)s).$$

If $2k \leq v_0 + d/2$ and $d/2 \leq k + 1$, then

$$b(v_0 + (l-j)s - k + d/2) = \left(q^{k-d/2+1}\right)^{v_0+(l-j)s-k+d/2},$$

so that

$$\sum_{j=1}^{l} b(v_0 + (l-j)s - k + d/2) = \sum_{j=1}^{l} \left(q^{k-d/2+1}\right)^{v_0+(l-j)s-k+d/2} =$$

$$\left(q^{k-d/2+1}\right)^{v_0-k+d/2} \sum_{r=0}^{l-1} \left(q^{s(k-d/2+1)}\right)^{r} = \left(q^{k-d/2+1}\right)^{v_0-k+d/2} [l]_{q^{s(k-d/2+1)}}. \qquad \square$$

146 Example ([HK17b, Example 1])
Using $\mathrm{A}_2(13,4;3) = 1597245$ [Bra+16] and $\mathrm{A}_2(7,4;3) \geq 333$ [Hei+16], the application of Proposition 145 with $s = 6$ gives

$$\mathrm{A}_2(13+6l,4;3) \geq 4096^l \cdot 1597245 + 333 \cdot \frac{4096^l - 1}{4095}$$

and

$$\mathrm{A}_2(13+6l,4;3) \geq 333 \cdot 16777216 \cdot \frac{4096^l - 1}{4095} + 1597245$$

for all $l \geq 0$.

Proposition 155 shows that the first lower bound almost meets the Anticode bound, cf. Theorem 107 asymptotically.

It is easy to generalize Theorem 136 to more than two involved CDCs.

147 Corollary ([HK17b, Corollary 5])
For $q \geq 2$ prime power and integers $1 \leq k \leq v_i$, $2 \leq m$, and $i \in \{1,\ldots,m\}$, let

- C_i be a non-empty $(v_i, N_i, d_i; k)_q$ CDC,
- C_i^R be a non-empty $(k \times v_i^R, N_i^R, d_i^R)_q$ rank metric code,
- $v_1^R = 0$, $C_1^R = \emptyset$, $N_1^R = 1$, $d_1^R = \infty$, and
- $\delta_i \in \mathbb{Z}$, $\delta_i \leq k-1$, $\delta_m = 0$, $v_i^R = \sum_{j=1}^{i-1}(v_j - \delta_j)$ for $i \neq 1$.

Then

$$\bigcup_{i=1}^{m} \left\{ \tau^{-1}(\mathbf{0}_{k\times(v-v_i-v_i^R)} \mid \tau(U_i) \mid M_i) : U_i \in C_i, M_i \in C_i^R \right\}$$

is a $(v, N, d; k)_q$ CDC with

- $v = \sum_{i=1}^{m}(v_i - \delta_i)$,
- $N = \sum_{i=1}^{m} N_i \cdot N_i^R$, and
- $d = \min\{d_i, 2d_i^R, 2(k-\delta_i) \mid i = 1,\ldots,m\}$.

Proof
By inductively applying Theorem 136 up to $m-1$ times, we prove that for all $m' \in \{1,\ldots,m\}$ there is a

$$\left(v_{m'}+v_{m'}^R, \sum_{i=1}^{m'} N_i \cdot N_i^R, \min\{d_{m'}, 2d_{m'}^R, \min\{d_i, 2d_i^R, 2(k-\delta_i)|i \in \{1,\ldots,m'-1\}\}\}; k\right)_q$$

CDC

$$C_{\{1,\ldots,m'\}} = \bigcup_{i=1}^{m'} \left\{\tau^{-1}(\mathbf{0}_{k\times(v_{m'}+v_{m'}^R-v_i-v_i^R)} \mid \tau(U_i) \mid M_i) : U_i \in C_i, M_i \in C_i^R\right\},$$

which then concludes the prove for $m'=m$.

This claim is trivially valid for $m'=1$ with $C_{\{1\}}=C_1$ and for $m'=2$ applying Theorem 136 for C_1, C_2, and C_2^R with $d=2(k-\delta_1)\ge 2$ yields a $(v_1+v_2-\delta_1, N_1+N_2\cdot N_2^R, \min\{d_1,d_2,2d_2^R,2(k-\delta_1)\};k)_q$ CDC $C_{\{1,2\}}$.

Let $\iota_n : 2^{\begin{bmatrix}\mathbb{F}_q^{v'}\\ k\end{bmatrix}} \to 2^{\begin{bmatrix}\mathbb{F}_q^{n}\\ k\end{bmatrix}}$ with $v' \le n$ and $\iota_n(S) = \{\tau^{-1}(\mathbf{0}_{k\times(n-v')} \mid \tau(U)) : U \in S)\}$ be an embedding of subspaces in an ambient space of dimension n.

If $C_{\{1,\ldots,m'\}}$ has the stated properties, then using Theorem 136 with $C_{\{1,\ldots,m'\}}$, $C_{m'+1}$, $C_{m'+1}^R$, and $d=2(k-\delta_{m'})\ge 2$, we construct a

$$\left(v_{m'+1}+v_{m'+1}^R, \sum_{i=1}^{m'+1} N_i \cdot N_i^R, D; k\right)_q$$

CDC

$$C_{\{1,\ldots,m'+1\}} = \iota_{v_{m'+1}+v_{m'+1}^R}(C_{\{1,\ldots,m'\}}) \cup \{\tau^{-1}(\tau(U) \mid M) : U \in C_{m'+1}, M \in C_{m'+1}^R\}$$

with

$$\begin{aligned} D =& \min\{d_{m'+1}, \min\{d_{m'}, 2d_{m'}^R, \min\{d_i, 2d_i^R, 2(k-\delta_i) \mid i \in \{1,\ldots,m'-1\}\}\}, \\ & 2d_{m'+1}^R, 2(k-\delta_{m'})\} \\ =& \min\{d_{m'+1}, 2d_{m'+1}^R, \min\{d_i, 2d_i^R, 2(k-\delta_i) \mid i \in \{1,\ldots,m'\}\}\}. \end{aligned}$$

□

The sizes of the codes of Corollary 147 are inferior compared to the dynamic programming approach, since its proof consists also of multiple applications of Theorem 136. However, it can be used to prove:

148 Corollary ([HK17b, Corollary 6], cf. [GT16, Theorem 4.6])
For $q \ge 2$ prime power and integers $1 \le k \le \min\{v_1, v_2\}$, $2 \le d/2$, a $[k\times(v_1+v_2), n, d/2]_q$ linear MRD code C^R and $(v_{i-2}, N_i, d; k)_q$ CDCs C_i for $i \in \{3,4\}$. Then

$$\begin{aligned} &\{\tau^{-1}(I_{k\times k} \mid M) : M \in C^R\} \\ \cup&\{\tau^{-1}(\mathbf{0}_{k\times k} \mid \tau(U) \mid \mathbf{0}_{k\times v_2}) : U \in C_3\} \\ \cup&\{\tau^{-1}(\mathbf{0}_{k\times k} \mid \mathbf{0}_{k\times v_1} \mid \tau(U)) : U \in C_4\} \end{aligned}$$

is a $(v_1+v_2+k, q^{(v_1+v_2)(k-d/2+1)}+N_3+N_4, d; k)_q$ CDC.

Proof
Applying Corollary 147 with

- $m=3$
- $\bar{C}_1 = C_4$, $\bar{C}_2 = C_3$,
- $\bar{C}_3 = \{\tau^{-1}(I_{k\times k})\}$ (i.e., an $(k,1,\infty;k)_q$ CDC)
- $\delta_1=\delta_2=\delta_3=0$
- $\bar{C}_1^R = \emptyset$
- $\bar{C}_2^R = \{\mathbf{0}_{k\times v_2}\}$ (i.e., an $(k\times v_2, 1, \infty)_q$ rank metric code)
- $\bar{C}_3^R = C^R$

yields the $(v_1+v_2+k, q^{(v_1+v_2)(k-d/2+1)}+N_3+N_4, d; k)_q$ CDC in question. $\square$

Interestingly, Corollary 148 constructs not necessarily the same codes as [GT16, Theorem 4.6]. Although they have the same cardinality, since the latter constructions involves matrices $A \mid B$ such that $d_r \le \min\{\mathrm{rk}(A), \mathrm{rk}(B)\}$, while our construction involves matrices C of the same size as $A \mid B$ with $d_r \le \mathrm{rk}(C)$.

This is not equivalent as the following small example shows: It is not possible to split $C = \left(\begin{smallmatrix} I_{k-1} \\ \mathbf{0}\end{smallmatrix} \mid \mathbf{0} \mid \ldots \mid \mathbf{0} \mid w\right)$, where w is a non-zero column, in two matrices $A = \left(\begin{smallmatrix} I_{k-1} \\ \mathbf{0}\end{smallmatrix} \mid \mathbf{0} \mid \ldots \mid \mathbf{0}\right)$ and $B = (\mathbf{0} \mid \ldots \mid \mathbf{0} \mid w)$ both having rank at least d_r for $2 \le d_r \le k$.

Conclusively, we remark that an application of Corollary 140 with $2k \le m \le v-k$ using an LMRD in the CDC C_1 cannot generate a CDC that exceeds the LMRD bound of Proposition 99.

149 **Lemma ([HK17b, Lemma 6])**
For $q \ge 2$ prime power, $0 \le k \le v_i$ integers, $2 \le d_i$ even integer ($i \in \{1,2\}$), $1 \le d_r \in \mathbb{Z}$, and $2 \le d$ even let C_i be a $(v_i, N_i, d_i; k)_q$ CDC for $i \in \{1,2\}$ and let C_r be a $(k \times (v_2-k+d/2), N_r, d_r)_q$ rank metric code.

If additionally $k \le \min\{v_1/2, (v_1+v_2+d/2)/3\}$, $d_r = d_1/2$, $d_1 \le d_2$, $d_1 \le d$, C_r is MRD, and C_1 contains an LMRD in $\begin{bmatrix} \mathbb{F}_q^{v_1} \\ k \end{bmatrix}$, then the CDC constructed in Theorem 136 contains an LMRD in $\begin{bmatrix} \mathbb{F}_q^{v_1+v_2-k+d/2} \\ k \end{bmatrix}$.

Proof

Let $\{\tau^{-1}(I_{k\times k} \mid M) : M \in R\} \subseteq C_1$ be the lifted MRD code in C_1. Since R is a $(k \times (v_1 - k), \#R, d_1/2)_q$ MRD code, we have $\#R = q^{(v_1-k)(k-d_1/2+1)}$. The first set of the construction contains

$$\{\tau^{-1}(I_{k\times k} \mid M \mid A) : M \in R, A \in C_r\}$$

in which $\{(M \mid A) : M \in R, A \in C_r\}$ forms a $(k \times (v_1 + v_2 - 2k + d/2), N, d_r)_q$ rank metric code of size $N = q^{(v_1-k)(k-d_1/2+1)} \cdot q^{(v_2-k+d/2)(k-d_r+1)} = q^{(v_1+v_2-2k+d/2)(k-d_r+1)}$, hence it is an MRD code. $\square$

9 Asymptotic bounds

Contents of this chapter were previously published in [HK17b].

For $q \geq 2$ prime power and $2 \leq d/2 \leq \min\{k, v-k\}$ integers the ratio "LMRD / Singleton" is at least 1/4 and converges to 1 for increasing q Lemma 8, cf. [KK08b]:

$$\frac{q^{\max\{k,v-k\}(\min\{k,v-k\}-d/2+1)}}{\begin{bmatrix} v-d/2+1 \\ \max\{k,v-k\} \end{bmatrix}_q} \geq \frac{q^{\max\{k,v-k\}(\min\{k,v-k\}-d/2+1)}}{\mu(q) \cdot q^{\max\{k,v-k\}(\min\{k,v-k\}-d/2+1)}} = \mu(q)^{-1} > \frac{1}{4}.$$

In this chapter, we tighten this analysis to get a ratio "best known lower bound / best known upper bound" of at least 0.616081 for all $q \geq 2$ prime power and $2 \leq d/2 \leq k \leq v-k$ integers and in fact, using the q-Pochhammer symbol, cf. Page 20,

$$\frac{(1/q;1/q)_k}{(1-q^{-(d/2)^2} \cdot \mathbb{1}_{d \leq k+1})(1/q;1/q)_{d/2-1}}$$

is the largest known general lower bound of this ratio that we will derive in this chapter. This might be improved as [ES13, Table 2], only exemplarily for $d=4$, indicates.

An asymptotic result involving the non-constructive probabilistic method was applied for fixed d and k (or fixed $v-k$ due to orthogonal codes) to show that the ratio of "best known lower bound / best known upper bound" tends to 1 for increasing v, cf. [FR85, Theorem 4.1], which is implied by a more general result of Frankl and Rödl on hypergraphs or [BE12, Theorem 1] for an explicit error term.

If the parameter k can vary with the dimension v, then our asymptotic analysis implies that there is still a gap of almost $1.6 \approx 0.616081^{-1}$ of the ratio of "best known upper bound / best known lower bound" of the code sizes for $q=2$, $d=4$ and $k=\lfloor v/2 \rfloor$, which is the worst case.

Using the asymptotic result in Lemma 9, we can compare the size of the lifted MRD codes to the Singleton and the Anticode bound for all interesting parameters. The monotonicity is of particular interest, since it shows that the limit is the worst case lower bound of the ratios "LMRD / Singleton" or "LMRD / Anticode" in both cases.

150 **Proposition ([HK17b, Proposition 7])**
For $q \geq 2$ prime power and integers $2 \leq d/2 \leq k \leq v-k$ the ratio of the size of an LMRD code divided by the size of the Singleton bound converges for $v \to \infty$ strictly monotonically decreasing to $(1/q;1/q)_{k-d/2+1}$ and we have

$$\begin{array}{lllllll} (1/q;1/q)_{k-d/2+1} & > & (1/q;1/q)_\infty & \geq & (1/2;1/2)_\infty & > & 0.288788 \text{ and} \\ (1/q;1/q)_{k-d/2+1} & \geq & (1/2;1/2)_{k-d/2+1} & > & (1/2;1/2)_\infty & > & 0.288788. \end{array}$$

Proof
With $z = k - d/2 + 1$ and $s = v - k$ the LMRD has size q^{sz} and the Singleton bound is $\begin{bmatrix} s+z \\ z \end{bmatrix}_q$. Therefore, the ratio is $q^{sz}/\begin{bmatrix} s+z \\ z \end{bmatrix}_q$, so that Lemma 9 gives the proposed limit, monotonicity, and the inequalities. $\square$

151 **Proposition ([HK17b, Proposition 8])**
For $q \geq 2$ prime power and integers $2 \leq d/2 \leq k \leq v - k$ the ratio of the size of an LMRD code divided by the size of the Anticode bound converges for $v \to \infty$ strictly monotonically decreasing to $\frac{(1/q;1/q)_k}{(1/q;1/q)_{d/2-1}} \geq \frac{q}{q-1} \cdot (1/q;1/q)_k$ and we have

$$\begin{array}{lclclcll} \frac{q}{q-1}(1/q;1/q)_k & > & \frac{q}{q-1}(1/q;1/q)_\infty & \geq & 2(1/2;1/2)_\infty & > & 0.577576 & \text{and} \\ \frac{q}{q-1}(1/q;1/q)_k & \geq & 2(1/2;1/2)_k & > & 2(1/2;1/2)_\infty & > & 0.577576. & \end{array}$$

Proof
With $z = d/2 - 1$ and $s = v - k$ the LMRD has size $q^{s(k-z)}$. The Anticode bound is $\begin{bmatrix} s+k \\ k \end{bmatrix}_q / \begin{bmatrix} s+z \\ z \end{bmatrix}_q$. Therefore, the ratio is

$$\frac{q^{sk}}{\begin{bmatrix} s+k \\ k \end{bmatrix}_q} \cdot \left(\frac{q^{sz}}{\begin{bmatrix} s+z \\ z \end{bmatrix}_q} \right)^{-1}.$$

From Lemma 9 we conclude

$$\lim_{s\to\infty} \frac{q^{sk}}{\begin{bmatrix} s+k \\ k \end{bmatrix}_q} = (1/q;1/q)_k \quad \text{and} \quad \lim_{s\to\infty} \frac{q^{sz}}{\begin{bmatrix} s+z \\ z \end{bmatrix}_q} = (1/q;1/q)_z,$$

so that the limit follows. The subsequent inequalities follow from $2 \leq d/2$, the monotonicity of $(1/q;1/q)_n$, $q \geq 2$, and Lemma 9.

In particular, $f(q) = \frac{q}{q-1}(1/q;1/q)_\lambda \geq \frac{2}{2-1}(1/2;1/2)_\lambda$ for $\lambda \in \{k, \infty\}$ is implied by $\frac{1-q^{-i}}{1-(q+1)^{-i}} \leq 1$ for all $1 \leq i$ and

$$\frac{f(q)}{f(q+1)} = \frac{q^2}{q^2-1} \prod_{i=1}^{\lambda} \frac{1-q^{-i}}{1-(q+1)^{-i}} = \frac{q^2}{q^2-1} \frac{q-1}{q} \prod_{i=2}^{\lambda} \frac{1-q^{-i}}{1-(q+1)^{-i}} \leq \frac{q}{q+1} \leq 1.$$

The monotonicity can be computed directly using q-factorials

$$\begin{aligned} &\frac{q^{s(k-z)} \begin{bmatrix} s+z \\ z \end{bmatrix}_q}{\begin{bmatrix} s+k \\ k \end{bmatrix}_q} \cdot \frac{\begin{bmatrix} s+1+k \\ k \end{bmatrix}_q}{q^{(s+1)(k-z)} \begin{bmatrix} s+1+z \\ z \end{bmatrix}_q} \\ &= \frac{[s+z]_q![s+1+k]_q![k]_q![s]_q![z]_q![s+1]_q!}{[z]_q![s]_q![k]_q![s+1]_q![s+k]_q![s+1+z]_q!} q^{z-k} \\ &= \frac{[s+1+k]_q}{[s+1+z]_q} q^{z-k} > q^{k-z} q^{z-k} = 1 \end{aligned}$$

and hence

$$\frac{q^{s(k-z)}}{\left[\begin{smallmatrix} s+k \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} s+z \\ z \end{smallmatrix}\right]_q} > \frac{q^{(s+1)(k-z)}}{\left[\begin{smallmatrix} s+1+k \\ k \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} s+1+z \\ z \end{smallmatrix}\right]_q}.$$

□

The coarser lower bound of the ratio "LMRD / Anticode" of $\frac{(1/q;1/q)_\infty}{(1/q;1/q)_{d/2-1}}$ was already proved in [ES13, Lemma 9].

In particular, the best known lower L and upper U bounds on $\mathrm{A}_q(v,d;k)$ for all parameters fulfill $L/U > 0.577576$ and the most challenging parameters are given by $q=2$, $d=4$, and $k=\lfloor v/2 \rfloor$.

This can be slightly improved by Lemma 60 instead of the LMRD bound for $d \le k+1$.

152 Proposition

For $q \ge 2$ prime power and integers $2 \le d/2 \le k \le v-k$ with $d \le k+1$ the ratio of the size of the code constructed in Lemma 60 divided by the size of the Anticode bound converges for $v \to \infty$ strictly monotonically decreasing to $\frac{(1/q;1/q)_k}{(1-q^{-(d/2)^2})(1/q;1/q)_{d/2-1}} \ge \frac{q^4}{q^4-1} \cdot \frac{q}{q-1} \cdot (1/q;1/q)_k$ and we have

$$\frac{q^4}{q^4-1}\frac{q}{q-1}(1/q;1/q)_k > \frac{q^4}{q^4-1}\frac{q}{q-1}(1/q;1/q)_\infty \ge (32/15)(1/2;1/2)_\infty > 0.616081 \text{ and}$$

$$\frac{q^4}{q^4-1}\frac{q}{q-1}(1/q;1/q)_k \ge (32/15)(1/2;1/2)_k > (32/15)(1/2;1/2)_\infty > 0.616081.$$

Proof

From Proposition 151 we know that the size of an LMRD code divided by the size of the Anticode bound converges for $v \to \infty$ strictly monotonically decreasing to $\frac{(1/q;1/q)_k}{(1/q;1/q)_{d/2-1}}$ and the code in Lemma 60 has cardinality $\mu = \frac{q^{(d/2)^2(M+1)}-1}{q^{(d/2)^2 M}(q^{(d/2)^2}-1)} = \frac{1-q^{-(d/2)^2(M+1)}}{1-q^{-(d/2)^2}}$ times the size of an LMRD, where $M = \lceil (v-k)/d \rceil$. Hence, $\lim_{v\to\infty} \mu = \lim_{M\to\infty} \mu = 1/(1-q^{-(d/2)^2})$ shows the limit.

To show that the convergence is monotonically decreasing, we abbreviate $\delta = d/2$ and $\lambda = (v-k)/(2\delta)$ and use $M(v) = \lceil \lambda \rceil$, which fulfills $M(v+1) - M(v) \in \{0,1\}$ and $M(v+1) - M(v) = 1$ iff $2\delta \mid v-k$. In that case, we have $M(v) = \lambda$ and $M(v+1) = \lambda + 1$.

For a $(v,N,d;k)_q$ CDC let the ratio of the size of Lemma 60 divided by the size of the Anticode bound be $f(v)$, i.e.,

$$f(v) = \frac{\mu q^{(v-k)(k-\delta+1)} \left[\begin{smallmatrix} v-k+\delta-1 \\ \delta-1 \end{smallmatrix}\right]_q}{\left[\begin{smallmatrix} v \\ k \end{smallmatrix}\right]_q} = \frac{(q^{\delta^2(M(v)+1)}-1) q^{(v-k)(k-\delta+1)} [k]_q! [v-k+\delta-1]_q!}{q^{\delta^2 M(v)}(q^{\delta^2}-1)[v]_q! [\delta-1]_q!},$$

so that

$$\frac{f(v+1)}{f(v)} = \frac{q^{\delta^2(M(v+1)+1)}-1}{q^{\delta^2(M(v)+1)}-1} \frac{[v-k+\delta]_q}{[v+1]_q} \frac{q^{k-\delta+1}}{q^{\delta^2(M(v+1)-M(v))}}.$$

If $M(v+1)-M(v)=0$, applying Lemma 5 with $d \le k+1 \Leftrightarrow \delta-k \le -\delta+1 \le -1 < 1$ shows

$$\frac{f(v+1)}{f(v)} = \frac{[v-k+\delta]_q}{[v+1]_q} q^{k-\delta+1} < q^{-k+\delta-1} q^{k-\delta+1} = 1.$$

If $M(v+1)-M(v)=1$, we write $M(v)=\lambda$ and $M(v+1)=\lambda+1$:

$$\frac{f(v+1)}{f(v)} = \frac{q^{\delta^2(\lambda+2)}-1}{q^{\delta^2(\lambda+1)}-1} \frac{[v-k+\delta]_q}{[v+1]_q} \frac{q^{k-\delta+1}}{q^{\delta^2}} = \frac{q^{\delta^2(\lambda+2)}-1}{q^{\delta^2(\lambda+2)}-q^{\delta^2}} \frac{q^v-q^{k-\delta}}{q^v-q^{-1}}.$$

This is ≤ 1 iff

$$\begin{aligned}
&(q^{\delta^2(\lambda+2)}-1)(q^v-q^{k-\delta}) \le (q^{\delta^2(\lambda+2)}-q^{\delta^2})(q^v-q^{-1}) \\
&\Leftrightarrow -q^{\delta^2(\lambda+2)+k-\delta} - q^v + q^{k-\delta} \le -q^{\delta^2(\lambda+2)-1} - q^{\delta^2+v} + q^{\delta^2-1} \\
&\Leftrightarrow q^{k-\delta} + q^v(q^{\delta^2}-1) \le q^{\delta^2(\lambda+2)}(q^{k-\delta}-q^{-1}) + q^{\delta^2-1}.
\end{aligned}$$

Now we use the estimations $k-\delta \le v$ on the left hand side and $q^{k-\delta}-q^{-1} \ge q^{k-\delta-1}$ as well as $\delta^2-1 \ge 0$ on the right hand side to obtain:

$$\Leftarrow q^{v+\delta^2} \le q^{\delta^2(\lambda+2)+k-\delta-1} \Leftrightarrow v \le \delta^2(\lambda+1)+k-\delta-1.$$

Since $\delta^2\lambda = (v-k)\delta/2$ we have

$$\Leftrightarrow v \le (v-k)\delta/2 + \delta^2 + k - \delta - 1 \Leftrightarrow 0 \le (v-k)(\delta/2-1) + \delta^2 - \delta - 1,$$

so that $0 \le v-k$ and $0 \le \delta/2-1$ together with $0 \le \delta^2-\delta-1$ for all $2 \le \delta$ shows the monotonicity.

For the first inequality, we abbreviate

$$g(\delta) = \frac{(1/q;1/q)_k}{(1-q^{-\delta^2})(1/q;1/q)_{\delta-1}}$$

and show that g is monotonically increasing so that the minimum is at $\delta=2$. Hence, using the q-Pochhammer symbol $(1/q;1/q)_x = \prod_{i=1}^{x}(1-q^{-i})$, cf. Page 20, and the inequality from Lemma 5, we get

$$\begin{aligned}
\frac{g(\delta)}{g(\delta+1)} &= \frac{(1-q^{-(\delta+1)^2})(1/q;1/q)_\delta}{(1-q^{-\delta^2})(1/q;1/q)_{\delta-1}} = \frac{(1-q^{-(\delta+1)^2})(1-q^{-\delta})}{(1-q^{-\delta^2})} \\
&= \frac{(q^{(\delta+1)^2}-1)(q^\delta-1)q^{\delta^2}}{(q^{\delta^2}-1)q^{(\delta+1)^2}q^\delta} < \frac{(q^{(\delta+1)^2}-1)q^{\delta^2}}{q^{(\delta+1)^2}q^\delta} q^{\delta-\delta^2} = \frac{q^{(\delta+1)^2}-1}{q^{(\delta+1)^2}} < 1.
\end{aligned}$$

The inequality $(1/q;1/q)_k > (1/q;1/q)_\infty$ for all $q \ge 2$ is implied by $1-q^{-i} < 1$.

Last, we show that for any k

$$h(q) = \frac{q^4}{q^4-1} \frac{q}{q-1} (1/q;1/q)_k$$

is monotonically increasing so that the minimum is attained at $q = 2$. Therefore, we use $\frac{1-q^{-i}}{1-(q+1)^{-i}} < 1$ for $q \geq 2$ and additionally $d \leq k+1 \Rightarrow 3 \leq k$:

$$\begin{aligned}
\frac{h(q)}{h(q+1)} &= \frac{q^4 q((q+1)^4-1)q(1/q;1/q)_k}{(q^4-1)(q-1)(q+1)^4(q+1)(1/(q+1);1/(q+1))_k} \\
&= \frac{q^6((q+1)^4-1)}{(q^4-1)(q-1)(q+1)^5} \prod_{i=1}^{2} \frac{1-q^{-i}}{1-(q+1)^{-i}} \prod_{i=3}^{k} \underbrace{\frac{1-q^{-i}}{1-(q+1)^{-i}}}_{<1} \\
&< \frac{q^6((q+1)^4-1)}{(q^4-1)(q-1)(q+1)^5} \frac{(q-1)^2(q+1)^4}{q^5(q+2)} = \frac{q((q+1)^4-1)(q-1)}{(q^4-1)(q+1)(q+2)} \\
&< \frac{q(q+1)^4(q-1)}{(q^4-q)(q+1)(q+2)} = \frac{(q+1)^3}{(q^2+q+1)(q+2)} = \frac{(q+1)^3}{(q+1)^3+1} < 1.
\end{aligned}$$

This concludes the proof. $\square$

An analogous improvement of the "LMRD / Anticode" ratio was tried in [ES13, Table 2].
Given Proposition 152 it is possible to improve the estimation of Proposition 151 to get "lower bound / Anticode" ≥ 0.616081 for all reasonable parameters. Since Proposition 152 is applicable for $d \leq k+1$, we can assume $k+2 \leq d \Leftrightarrow \lceil k/2 \rceil \leq d/2-1$ in Proposition 151. Therefore the tightest bound $\frac{(1/q;1/q)_k}{(1/q;1/q)_{d/2-1}}$ of Proposition 151 can be estimated to

$$\begin{aligned}
&\frac{(1/q;1/q)_k}{(1/q;1/q)_{d/2-1}} \geq \frac{(1/q;1/q)_k}{(1/q;1/q)_{\lceil k/2 \rceil}} = \prod_{i=\lceil k/2 \rceil+1}^{k} (1-q^{-i}) \\
\geq &\prod_{i=\lceil k/2 \rceil+1}^{k} (1-2^{-i}) \geq (1-2^{-\lceil k/2 \rceil-1})^{\lfloor k/2 \rfloor} \geq (1-2^{-k/2-1})^{k/2}
\end{aligned}$$

and $(1-2^{-k/2-1})^{k/2}$ has its minimum on $2 \leq k$ at $k^* \approx 2.566$ with $(1-2^{-k^*/2-1})^{k^*/2} \approx 0.744 > 0.616081$.

Replacing the Anticode bound by the (recursive) improved Johnson bound of Corollary 120 does not change the limit behavior of Proposition 151 or Proposition 152 for $v \to \infty$ and since this bound surpasses the Johnson bound of Corollary 116, the Johnson bound does not change this limit behavior either. Since the improved and standard Johnson bound refer back to bounds for partial spreads, we first need the following auxiliary lemma.

153 **Lemma ([HK17b])**
For $q \geq 2$ prime power and integers $2 \leq d/2 = k \leq v-k$ the ratio of the best known lower bound divided by the best known upper bound converges to 1 for $v \to \infty$.

Proof
For the integers t and r we write $v = tk + r$ with $2 \le t$ and $0 \le r < k$. Theorem 126 yields the lower bound $\frac{q^v - q^{k+r}}{q^k - 1} + 1$ for these parameters and $(q^v - 1)/(q^k - 1)$ is a trivial upper bound for spreads, cf. Corollary 125.

$$\lim_{t\to\infty} \frac{(q^{tk+r} - q^{k+r})/(q^k - 1) + 1}{(q^{tk+r} - 1)/(q^k - 1)} = \lim_{t\to\infty} \frac{q^{tk+r} - q^{k+r} + q^k - 1}{q^{tk+r} - 1}$$
$$= \lim_{t\to\infty} \frac{1 - q^{k-tk} + q^{k-tk-r} - q^{-tk-r}}{1 - q^{-tk-r}} = 1$$ □

154 Lemma
Using the notation of Definition 118, we have $\left\{\frac{a}{[k]_q}\right\}_k \ge \frac{a}{[k]_q} - kq$.

Proof
By definition, $\{a/[k]_q\}_k$ is the maximal $b \in \mathbb{N}$ such that there are non-negative integers $a_0, \ldots, a_{k-1}$ with $a - b \cdot [k]_q = \sum_{i=0}^{k-1} a_i \cdot q^{k-1-i} \cdot \frac{q^{i+1}-1}{q-1}$. By [KK17, Theorem 4] this is equivalent to the existence of a q^{k-1}-divisible multiset of points of cardinality $a - b \cdot [k]_q$ and by [KK17, Proposition 1] and the definition of $F(q, r)$ beforehand, there are q^{k-1}-divisible multisets of points of cardinality n for all $n > (k-1)q^k - [k]_q$. Using $n := a - b \cdot [k]_q$ there is a q^{k-1}-divisible multisets of points of cardinality $a - b \cdot [k]_q$ if $a - b \cdot [k]_q > (k-1)q^k - [k]_q \Leftrightarrow \frac{a-(k-1)q^k}{[k]_q} + 1 > b$. Hence, by Lemma 8, $\{a/[k]_q\}_k \ge \frac{a-(k-1)q^k}{[k]_q} = \frac{a}{[k]_q} - \frac{(k-1)q^k}{[k]_q} \ge \frac{a}{[k]_q} - \frac{(k-1)q^k}{q^{k-1}} \ge \frac{a}{[k]_q} - kq$. □

Now we will show that the ratio between the Improved Johnson bound (Corollary 120) and the Anticode bound (Theorem 107) tends also to 1 as v tends to infinity for $2 \le d/2 \le k \le v - k$. Therefore we abbreviate $v' = v - k + d/2$ and $a_i = (q^{v'+i} - 1)/(q^{d/2+i} - 1) > 1$ for $i = 0, \ldots, k - d/2$ and note that

$$\prod_{i=j}^{k-d/2} a_i = \prod_{i=j}^{k-d/2} \frac{[v'+i]_q}{[d/2+i]_q} = \frac{[v]_q![d/2+j-1]_q![v-k]_q!}{[v'+j-1]_q![k]_q![v-k]_q!} = \frac{\begin{bmatrix} v \\ k \end{bmatrix}_q}{\begin{bmatrix} v'+j-1 \\ d/2+j-1 \end{bmatrix}_q}$$

for $j \in \{0, 1\}$.

Hence, Corollary 120 and the statements of Lemma 153 and Lemma 154, as well as the estimation from Lemma 8, yield

$$
\begin{aligned}
&\frac{\left[{v \atop k}\right]_q}{\left[{v'-1 \atop d/2-1}\right]_q} \\
&\geq \left\{ \frac{q^v-1}{q^k-1} \left\{ \frac{q^{v-1}-1}{q^{k-1}-1} \left\{ \ldots \left\{ \frac{q^{v'+1}-1}{q^{d/2+1}-1} \cdot \left\lfloor \frac{q^{v'}-1}{q^{d/2}-1} \right\rfloor \right\}_{d/2+1} \ldots \right\}_{k-2} \right\}_{k-1} \right\}_k \\
&= \{a_{k-d/2}\{a_{k-d/2-1}\{\ldots\{a_1\lfloor a_0\rfloor\}_{d/2+1}\ldots\}_{k-2}\}_{k-1}\}_k \\
&\geq a_{k-d/2}(a_{k-d/2-1}(\ldots(a_1(a_0-1)-(d/2+1)q)\ldots)-(k-1)q)-kq \\
&\geq a_{k-d/2}(a_{k-d/2-1}(\ldots(a_1(a_0-kq)-kq)\ldots)-kq)-kq \\
&= \prod_{i=0}^{k-d/2} a_i - kq\left(\sum_{j=1}^{k-d/2}\prod_{l=j}^{k-d/2} a_l + 1\right) \geq \prod_{i=0}^{k-d/2} a_i - kq(k-d/2+1)\prod_{i=1}^{k-d/2} a_i \\
&= \frac{\left[{v \atop k}\right]_q}{\left[{v'-1 \atop d/2-1}\right]_q} - kq(k-d/2+1)\frac{\left[{v \atop k}\right]_q}{\left[{v' \atop d/2}\right]_q} = \frac{\left[{v \atop k}\right]_q}{\left[{v'-1 \atop d/2-1}\right]_q}\left(1-kq(k-d/2+1)\frac{\left[{v'-1 \atop d/2-1}\right]_q}{\left[{v' \atop d/2}\right]_q}\right) \\
&\geq \frac{\left[{v \atop k}\right]_q}{\left[{v'-1 \atop d/2-1}\right]_q}\left(1-kq(k-d/2+1)\frac{\mu(q)q^{(d/2-1)(v-k)}}{q^{(d/2)(v-k)}}\right) \\
&= \frac{\left[{v \atop k}\right]_q}{\left[{v'-1 \atop d/2-1}\right]_q}\left(1-\frac{kq(k-d/2+1)\mu(q)}{q^{v-k}}\right).
\end{aligned}
$$

Hence, we have $1 \geq$ "Improved Johnson bound / Anticode bound" $\geq z_v$, where z_v is a series with $\lim_{v\to\infty} z_v = 1$, and thus the sqeeze theorem [Soh14, Theorem 3.3.6] shows that the Improved Johnson bound does not tighten the limit behaviour compared to the Anticode bound.

Next, we consider the ratio between the lower bound from the first arithmetic progression of the improved linkage construction of Proposition 145 and the Anticode bound Theorem 107 for $l \to \infty$.

155 Proposition ([HK17b, Proposition 9])
For $q \geq 2$ prime power and integers $k \leq v_0 - k$, $1 \leq d/2 \leq k \leq s$, and $0 \leq l$, we have

$$
\begin{aligned}
&\lim_{l\to\infty} \frac{\mathrm{A}_q(v_0, d; k)b^l + \mathrm{A}_q(s+k-d/2, d; k)[l]_b}{\left[{v_0+ls \atop k}\right]_q / \left[{v_0+ls-k+d/2-1 \atop d/2-1}\right]_q} \\
&= \frac{(\mathrm{A}_q(v_0, d; k) + \mathrm{A}_q(s+k-d/2, d; k)/(b-1))(1/q;1/q)_k}{q^{(v_0-k)(k-d/2+1)}(1/q;1/q)_{d/2-1}}
\end{aligned}
$$

with $b = q^{s(k-d/2+1)}$.

Proof
We abbreviate $X = \mathrm{A}_q(v_0, d; k)$ and $Y = \mathrm{A}_q(s + k - d/2, d; k)$.
The numerator can be rewritten as

$$Xb^l + Y\frac{b^l - 1}{b - 1} = \left(X + Y\frac{1 - b^{-l}}{b - 1}\right) b^l$$

and therefore we use the convergence

$$\lim_{l\to\infty} X + Y\frac{1 - b^{-l}}{b - 1} = X + Y/(b - 1).$$

Next we apply Lemma 9 to both q-binomial coefficients:

$$\lim_{l\to\infty} \frac{q^{(v_0+ls-k)k}}{\begin{bmatrix} (v_0+ls-k)+k \\ k \end{bmatrix}_q} = (1/q; 1/q)_k \quad \text{and} \quad \lim_{l\to\infty} \frac{q^{(v_0+ls-k)(d/2-1)}}{\begin{bmatrix} (v_0+ls-k)+(d/2-1) \\ d/2-1 \end{bmatrix}_q} = (1/q; 1/q)_{d/2-1}.$$

With

$$Z = q^{(v_0-k)(k-d/2+1)} = \frac{q^{(v_0+ls-k)k} q^{-ls(k-d/2+1)}}{q^{(v_0+ls-k)(d/2-1)}} = \frac{q^{(v_0+ls-k)k} b^{-l}}{q^{(v_0+ls-k)(d/2-1)}},$$

which is in particular independent of l, we can finally put all components together

$$\begin{aligned} &\lim_{l\to\infty} \frac{\left(X + Y\frac{1-b^{-l}}{b-1}\right) b^l}{b^l} \frac{q^{(v_0+ls-k)k}}{\begin{bmatrix} v_0+ls \\ k \end{bmatrix}_q} \frac{\begin{bmatrix} v_0+ls-k+d/2-1 \\ d/2-1 \end{bmatrix}_q}{q^{(v_0+ls-k)(d/2-1)}} Z^{-1} \\ &= (X + Y/(b - 1))(1/q; 1/q)_k (1/q; 1/q)_{d/2-1}^{-1} Z^{-1}, \end{aligned}$$

concluding the proof. □

For Example 146 with $d = 4$ and $k = 3$, we obtain a ratio of

$$\left(1\,597\,245 + \frac{\mathrm{A}_2(7, 4; 3)}{4095}\right) \cdot 21/2^{25} \in [0.99963386, 0.99963388]$$

for $v = 13 + 6l$ with $l \to \infty$ using $333 \le \mathrm{A}_2(7, 4; 3) \le 381$, i.e., the Anticode bound of Theorem 107 is almost met by the arithmetic progression of the improved linkage construction.

9.1 Codes better than the LMRD bound

Although CDCs larger than the LMRD bound are very rare, we use the improved linkage construction, cf. Theorem 136, to provide an infinite series of such CDCs with $d = 4$ and $k = 3$.

Proposition 99 yields a bound for CDCs that contain an LMRD. This bound is superseded by two infinite series of CDCs with $q = 2$, $d = 4$, and $k = 3$, cf. [AHL16]. Besides $d = 4$, $k = 3$, the only other case where the MRD bound was superseded is $\mathrm{A}_2(8, 4; 4) \ge 4801 > 4797$, cf. [BÖW16] and [Hei+16]. The improved linkage construction allows to improve on the MRD bound for all field sizes q, if v is large enough.

156 Proposition (cf. [HK17b, Proposition 10])
For $q \geq 2$ prime power and integral $v \geq 12$ we have

$$\frac{\mathrm{A}_q(v,4;3)}{q^{2v-6}+\left[{v-3 \atop 2}\right]_q} \geq \frac{q^{-4}\,\mathrm{A}_q(7,4;3)}{q^4+(1/q;1/q)_2^{-1}} > 1+\frac{1}{2q^3}.$$

Proof
Let $v_0 \in \{12,13,14\}$ and $v = v_0+3l \geq 12$ for $0 \leq l$.
Corollary 140 with $m=7$ shows

$$\mathrm{A}_q(v_0,4;3) \geq \mathrm{A}_q(7,4;3)q^{2v_0-14}+\mathrm{A}_q(v_0-6,4;3) \geq q^{2v_0-14}\,\mathrm{A}_q(7,4;3).$$

Applying Proposition 145 with $s=3$ gives

$$\mathrm{A}_q(v_0+3l,4;3) \geq q^{6l}\,\mathrm{A}_q(v_0,4;3)+\mathrm{A}_q(4,4;3)[l]_{q^6} \geq q^{6l}\,\mathrm{A}_q(v_0,4;3).$$

Hence, we have for all $2 \leq q$ and $12 \leq v$

$$\mathrm{A}_q(v,4;3)=\mathrm{A}_q(v_0{+}3l,4;3) \geq q^{6l}\,\mathrm{A}_q(v_0,4;3) \geq q^{2(v_0+3l)-14}\,\mathrm{A}_q(7,4;3)=q^{2v-14}\,\mathrm{A}_q(7,4;3).$$

From Lemma 9 we conclude the strictly monotonically decreasing convergence

$$\lim_{v\to\infty} q^{2(v-5)}/\left[{(v-5)+2 \atop 2}\right]_q=(1/q;1/q)_2=(q-1)(q^2-1)q^{-3}.$$

Hence, we get

$$\lim_{v\to\infty}\frac{\mathrm{A}_q(v,4;3)}{q^{2v-6}+\left[{v-3 \atop 2}\right]_q} \geq \lim_{v\to\infty}\frac{q^{2v-14}\,\mathrm{A}_q(7,4;3)}{q^{2v-6}+\left[{v-3 \atop 2}\right]_q}=\lim_{v\to\infty}\frac{q^{-4}\,\mathrm{A}_q(7,4;3)}{q^4+\frac{\left[{v-3 \atop 2}\right]_q}{q^{2v-10}}}=\frac{q^{-4}\,\mathrm{A}_q(7,4;3)}{q^4+(1/q;1/q)_2^{-1}}$$

and this convergence is also strictly monotonically decreasing.
Now we have to distinguish $q=2$, $q=3$, and $4 \leq q$ in this proof.
Although $\mathrm{A}_q(7,4;3) \geq q^8+q^5+q^4+q^2-q \geq q^8+q^5+q^4$ for $q \geq 2$ by [HK16, Theorem 4], in the special case of $q=2$ the better bound of $\mathrm{A}_2(7,4;3) \geq 333$ is known. Moreover, we use $(1/q;1/q)_2 \geq (1/2;1/2)_2 = 3/8$ and $(1/3;1/3)_2 = 16/27$ where Lemma 9 shows this inequality.
For $q=2$ we have $\frac{2^{-4}333}{2^4+8/3} > 1.1149 > 1.0625 = 1+1/(2\cdot 2^3)$, for $q=3$ we have $\frac{3^4+3+1}{3^4+27/16} > 1.0279 > 1.0186 > 1+1/(2\cdot 3^3)$, and for $4 \leq q$ a small computation shows $\frac{q^4+q+1}{q^4+8/3} > 1+1/(2q^3)$. □

Many estimations in the proof of Proposition 156 are very coarse for $q=2$ considering that many good codes and hence lower bounds on $\mathrm{A}_2(v,d;k)$ are available, usually found by extensive computer searches involving prescribed automorphisms, see e.g. [KK08a].

157 **Proposition ([HK17b, Proposition 11])**
For $v \geq 19$ we have $\frac{\mathrm{A}_2(v,4;3)}{2^{2v-6}+\left[{v-3 \atop 2}\right]_2} > 1.3056$.

Proof
We will use $\mathrm{A}_2(7,4;3) \geq 333$ [Hei+16], $\mathrm{A}_2(8,4;3) \geq 1326$ [BÖW16], $\mathrm{A}_2(9,4;3) \geq 5986$ [BÖW16], and $\mathrm{A}_2(13,4;3) = 1\,597\,245$ [Bra+16].

Let $v_0 \in \{19, 20, 21\}$. We apply Corollary 140 with $m = 13$ to obtain $\mathrm{A}_2(v_0,4;3) \geq 2^{2v_0-26}\,\mathrm{A}_2(13,4;3) + \mathrm{A}_2(v_0-12,4;3)$, i.e., $\mathrm{A}_2(19,4;3) \geq 6\,542\,315\,853$, $\mathrm{A}_2(20,4;3) \geq 26\,169\,263\,406$, and $\mathrm{A}_2(21,4;3) \geq 104\,677\,054\,306$.

Applying Proposition 145 with $s = 3$ to $v = v_0 + 3l \geq 19$ gives $\mathrm{A}_2(v_0+3l,4;3) \geq 2^{6l}\,\mathrm{A}_2(v_0,4;3) + [l]_{2^6} \geq 2^{6l}\,\mathrm{A}_2(v_0,4;3)$ and with Lemma 9 and $(1/2;1/2)_2 = 3/8$ we obtain

$$
\begin{aligned}
&\lim_{v\to\infty} \frac{\mathrm{A}_2(v,4;3)}{2^{2v-6}+\left[{v-3 \atop 2}\right]_2} \geq \lim_{l\to\infty} \frac{2^{6l}\,\mathrm{A}_2(v_0,4;3)}{2^{2(v_0+3l)-6}+\left[{v_0+3l-3 \atop 2}\right]_2}\\
&= \lim_{l\to\infty} \frac{\mathrm{A}_2(v_0,4;3)}{2^{2v_0-6}+\left[{(v_0+3l-5)+2 \atop 2}\right]_2 / 2^{2(v_0+3l-5)} \cdot 2^{2(v_0-5)}}\\
&= \frac{\mathrm{A}_2(v_0,4;3)}{2^{2v_0-6}+(1/2;1/2)_2^{-1} 2^{2v_0-10}} = \frac{\mathrm{A}_2(v_0,4;3)}{2^{2v_0-6}+8/3\cdot 2^{2v_0-10}} = \frac{\mathrm{A}_2(v_0,4;3)}{7/3\cdot 2^{2v_0-7}}.
\end{aligned}
$$

This convergence is strictly monotonically decreasing.

The right hand side is ≈ 1.3056442380 for $v_0 = 19$, ≈ 1.3056442377 for $v_0 = 20$, and ≈ 1.3056442462 for $v_0 = 21$. Hence, its minimum is attained with $v_0 = 20$. □

In Proposition 156 and Proposition 157, we applied Proposition 145 without the second summand on the right hand side, which is equivalent to directly applying [ST15, Theorem 37]. In that case, only one instead of three starting values for the recursion in Proposition 156 would have sufficed. The usage of Corollary 140 in the last proof was fundamental to derive large CDCs for medium sized ambient spaces by considering $\mathrm{A}_2(13,4;3) = 1\,597\,245$ and good lower bounds for small dimensions.

We compare the sizes of different constructions with the size of an LMRD, the best known lower bound `bklb`, and the best known upper bound `bkub` in Tables 7, 8, and 9. The values of Proposition 99 are given in column `mrdb`. Applying Theorem 135 and Theorem 136 to the best known codes give the columns `lold` and `lnew`, respectively. The results obtained in [AHL16] are stated in column `ea`. The ratio between the mentioned constructions and the MRD bound can be found in Table 9. Since differences are partially beyond the given accuracy, we give absolute numbers in Table 7. Note that the values in column `bklb` of Table 9 show that Proposition 157 is also valid for $v \geq 16$, while we have a smaller ratio for $v < 16$. The relative advantage over LMRD codes is displayed in Table 8.

v	bklb	mrdb	bkub	lold	lnew	ea
6	77	71	77	65	65	
7	333	291	381	257	265	301
8	1326	1179	1493	1033	1101	1117
9	5986	4747	6205	4929	4929	4852
10	23870	19051	24698	21313	21313	18924
11	97526	76331	99718	85249	85257	79306
12	385515	305579	398385	383105	383105	309667
13	1597245	1222827	1597245	1532417	1532425	1287958
14	6241665	4892331	6387029	6241665	6241665	4970117
15	24966665	19571371	25562941	24966657	24966665	20560924
16	102223681	78289579	102243962	102223681	102223681	79608330
17	408894729	313166507	409035142	408894721	408894729	
18	1635578957	1252682411	1636109361	1635578889	1635578957	
19	6542315853	5010762411	6544674621	6542315597	6542315853	5200895489

Table 7: Lower and upper bounds for $\mathrm{A}_2(v, 4; 3)$.

v	bklb	mrdb	bkub	lold	lnew	ea
6	1.203125	1.109375	1.203125	1.015625	1.015625	
7	1.300781	1.136719	1.488281	1.003906	1.035156	1.175781
8	1.294922	1.151367	1.458008	1.008789	1.075195	1.090820
9	1.461426	1.158936	1.514893	1.203369	1.203369	1.184570
10	1.456909	1.162781	1.507446	1.300842	1.300842	1.155029
11	1.488129	1.164719	1.521576	1.300797	1.300919	1.210114
12	1.470623	1.165691	1.519718	1.461430	1.461430	1.181286
13	1.523252	1.166179	1.523252	1.461427	1.461434	1.228292
14	1.488129	1.166423	1.522786	1.488129	1.488129	1.184968
15	1.488129	1.166545	1.52367	1.488129	1.488129	1.225527
16	1.523252	1.166606	1.523554	1.523252	1.523252	1.186257
17	1.523252	1.166636	1.523775	1.523252	1.523252	
18	1.523252	1.166651	1.523746	1.523252	1.523252	
19	1.523252	1.166659	1.523801	1.523252	1.523252	1.210928

Table 8: Lower and upper bounds for $\mathrm{A}_2(v, 4; 3)$ divided by the size of a corresponding LMRD code.

v	bklb	mrdb	bkub	lold	lnew	ea
6	1.084507	1.0	1.084507	0.915493	0.915493	
7	1.144330	1.0	1.309278	0.883162	0.910653	1.034364
8	1.124682	1.0	1.266327	0.876166	0.933842	0.947413
9	1.261007	1.0	1.307141	1.038340	1.038340	1.022119
10	1.252953	1.0	1.296415	1.118734	1.118734	0.993334
11	1.277672	1.0	1.306389	1.116833	1.116938	1.038975
12	1.261589	1.0	1.303705	1.253702	1.253702	1.013378
13	1.306190	1.0	1.306190	1.253176	1.253182	1.053263
14	1.275806	1.0	1.305519	1.275806	1.275806	1.015900
15	1.275673	1.0	1.306140	1.275672	1.275673	1.050561
16	1.305712	1.0	1.305972	1.305712	1.305712	1.016845
17	1.305678	1.0	1.306127	1.305678	1.305678	
18	1.305661	1.0	1.306085	1.305661	1.305661	
19	1.305653	1.0	1.306124	1.305653	1.305653	1.037945

Table 9: Lower and upper bounds for $\mathrm{A}_2(v, 4; 3)$ divided by the corresponding LMRD bound.

10 Theoretic arguments for the exclusion of automorphisms

Prescribing some subgroups of the $\mathrm{P\Gamma L}(\mathbb{F}_q^v)$ as automorphism subgroup of CDCs restricts possible code sizes. In this chapter, we provide theoretic arguments which show that some groups yield only *small* codes, in some cases even smaller than a corresponding LMRD code. Hence, these groups are not automorphism groups of maximum cardinality codes.

First, we need to count b-spaces which are fixed but not point-wise fixed.

158 **Lemma**

Let $q \geq 2$ be a prime power, $0 \leq b \leq v$ be integers and $G \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ be a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-1)$-dimensional subspace if q is even and the disjoint union of a $(v-1)$-dimensional subspace with a point if q is odd. Then

$$\#\left\{U \in \begin{bmatrix}\mathbb{F}_q^v\\ b\end{bmatrix} \,\middle|\, \#(U\cdot G)=1 \wedge \exists P \in \begin{bmatrix}U\\ 1\end{bmatrix} : \#(P\cdot G)=2\right\} = \begin{cases} 0 & \text{if } b \leq 1,\\ \begin{bmatrix}v-2\\ b-2\end{bmatrix}_q q^{v-b} & \text{if } 2 \leq b \wedge 2 \mid q,\\ \begin{bmatrix}v-1\\ b-1\end{bmatrix}_q & \text{if } 2 \leq b \wedge 2 \nmid q.\end{cases}$$

Proof

If $b \leq 1$ then the set is empty and hence we assume wlog. $2 \leq b$. Let $\mathcal{F} = F$ if q is even and $\mathcal{F} = F \dot\cup f$ if q is odd for a hyperplane $F \leq \mathbb{F}_q^v$ and a point $f \leq \mathbb{F}_q^v$ with $f \not\leq F$ the set of fixed points under the operation of G. Let $\langle M \rangle = G$.

If q is even: For any $U \in \begin{bmatrix}\mathbb{F}_q^v\\ b\end{bmatrix}$ that is fixed such that there is a point P in U which is not fixed, there are $\#\left(\begin{bmatrix}\mathbb{F}_q^v\\ 1\end{bmatrix} \setminus \begin{bmatrix}F\\ 1\end{bmatrix}\right) = \begin{bmatrix}v\\ 1\end{bmatrix}_q - \begin{bmatrix}v-1\\ 1\end{bmatrix}_q = q^{v-1}$ possibilities for P. After choosing P, the line $\langle P, P\cdot M\rangle$ contains exactly one fixed point P_F since any line contains $q+1$ points, which is odd, and at least two fixed points on this line would imply that the line is contained in F. Next, there are $\begin{bmatrix}\dim(F)-1\\ \dim(U\cap F)-1\end{bmatrix}_q = \begin{bmatrix}v-2\\ b-2\end{bmatrix}_q$ possibilities to extend P_F to a $(b-1)$-dimensional vector space U_F contained in F. U is then determined via $U = \langle P, U_F\rangle$. Since U contains $\#\left(\begin{bmatrix}U\\ 1\end{bmatrix} \setminus \begin{bmatrix}U\cap F\\ 1\end{bmatrix}\right) = \begin{bmatrix}b\\ 1\end{bmatrix}_q - \begin{bmatrix}b-1\\ 1\end{bmatrix}_q = q^{b-1}$ points which are not fixed, any of them determines the same U. Hence, the total number of possibilities is $q^{v-1} \cdot \begin{bmatrix}v-2\\ b-2\end{bmatrix}_q / q^{b-1} = \begin{bmatrix}v-2\\ b-2\end{bmatrix}_q q^{v-b}$.

If q is odd: Any $U \in \begin{bmatrix}\mathbb{F}_q^v\\ b\end{bmatrix}$ that is fixed such that there is a point P in U which is not fixed contains a $(b-1)$-dimensional fixed subspace $U \cap F$ and $\#\left(\begin{bmatrix}U\\ 1\end{bmatrix} \setminus \begin{bmatrix}U\cap F\\ 1\end{bmatrix}\right) =$

$\begin{bmatrix} b \\ 1 \end{bmatrix}_q - \begin{bmatrix} b-1 \\ 1 \end{bmatrix}_q = q^{b-1}$ points that are not in F, which is an odd number, and hence $f \le U$. Therefore, after fixing one of the $\begin{bmatrix} v-1 \\ b-1 \end{bmatrix}_q$ possible $(b-1)$-dimensional subspaces S in F, U is uniquely determined via $U = f \oplus S$. □

By examining LP-certificates, i.e., multipliers of constraints in an optimal solution of the LP-relaxation of DefaultCDCBLP(q, v, d, k), cf. Definition 47, with a prescribed group, we get the following lemma.

159 Lemma
Let $q \ge 2$ be a prime power, $2 \le d/2 < k \le v-k$ integers and $G \le \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-1)$-dimensional subspace, if q is even and the disjoint union of a $(v-1)$-dimensional subspace with a point, if q is odd. Let C be a $(v, \#C, d; k)_q$ CDC with $G \le \mathrm{Aut}(C)$. Then

$$\begin{bmatrix} k \\ d/2-1 \end{bmatrix}_q \#C \le \begin{bmatrix} v-1 \\ k-d/2+1 \end{bmatrix}_q + \begin{cases} \begin{bmatrix} v-2 \\ k-d/2-1 \end{bmatrix}_q q^{v-k+d/2-1} \frac{[k-1]_q}{[k-d/2]_q} & \text{if } 2 \mid q, \\ \begin{bmatrix} v-1 \\ k-d/2 \end{bmatrix}_q q^{d/2-1} & \text{if } 2 \nmid q. \end{cases}$$

Proof
We abbreviate $b = k - d/2 + 1 \ge 2$ and use the term fixed with respect to G operating on the set of subspaces without further notice and partition $C = C_P \dot\cup C_F \dot\cup C_N$, such that C_P contains all point-wise fixed codewords, C_F contains all codewords that are fixed but not point-wise fixed, and C_N contains all codewords which are not fixed. With B_P, B_F, and B_N we also abbreviate the set of b-spaces which are point-wise fixed, fixed but not point-wise fixed, and non-fixed, respectively. Let $\mathcal{F} = F$ if q is even and $\mathcal{F} = F \dot\cup f$ if q is odd for a hyperplane $F \le \mathbb{F}_q^v$ and a point $f \le \mathbb{F}_q^v$ with $f \not\le F$ the set of fixed points under the operation of $G = \langle M \rangle$.

First, $C_N = \emptyset$, since for any $U \in C_N$ we have $S = U \cap F = (U \cdot M) \cap F = U \cap (U \cdot M)$ with $\dim(S) = k-1$ and hence $\dim(U) + \dim(U \cdot M) - 2\dim(S) = 2 < d$ violating the minimum distance.

Second, any $U \in C_P$ contains exactly $\begin{bmatrix} k \\ b \end{bmatrix}_q$ point-wise fixed b-spaces and no other b-spaces.

Third, any $U \in C_F$ contains exactly $\begin{bmatrix} k-1 \\ b \end{bmatrix}_q$ point-wise fixed b-spaces,

$$\alpha = \begin{cases} \begin{bmatrix} k-2 \\ b-2 \end{bmatrix}_q q^{k-b} & \text{if } 2 \mid q \\ \begin{bmatrix} k-1 \\ b-1 \end{bmatrix}_q & \text{if } 2 \nmid q \end{cases}$$

fixed b-spaces which are not point-wise fixed by Lemma 158, and $\beta = \begin{bmatrix} k \\ b \end{bmatrix}_q - \begin{bmatrix} k-1 \\ b \end{bmatrix}_q - \alpha$ b-spaces which are not fixed.

Fourth, $\#B_P = \left[{v-1 \atop b} \right]_q$ and

$$\#B_F = \begin{cases} \left[{v-2 \atop b-2} \right]_q q^{v-b} & \text{if } 2 \mid q \\ \left[{v-1 \atop b-1} \right]_q & \text{if } 2 \nmid q \end{cases}$$

by Lemma 158.

Fifth, by double counting of $\left\{ (U, W) \in C_P \times \left[{\mathbb{F}_q^v \atop b} \right] \;\middle|\; W \le U \right\}$ and "Second", we have

$$\left[{k \atop b} \right]_q \#C_P = \sum_{W \in B_P} \#\mathcal{I}\left(C_P, W\right).$$

Sixth, by double counting of $\left\{ (U, W) \in C_F \times \left[{\mathbb{F}_q^v \atop b} \right] \;\middle|\; W \le U \right\}$ and "Third", we have

$$\left[{k \atop b} \right]_q \#C_F = \sum_{W \in B_P} \#\mathcal{I}\left(C_F, W\right) + \sum_{W \in B_F} \#\mathcal{I}\left(C_F, W\right) + \sum_{W \in B_N} \#\mathcal{I}\left(C_F, W\right)$$

and by double counting $\{(U, W_F, W_N) \in C_F \times B_F \times B_N \mid W_F \le U \wedge W_N \le U\}$,

$$\beta \sum_{W \in B_F} \#\mathcal{I}\left(C_F, W\right) = \alpha \sum_{W \in B_N} \#\mathcal{I}\left(C_F, W\right).$$

Seventh, combining "Fifth" and "Sixth" as well as the estimation of Lemma 41 and the counting of "Fourth", we conclude

$$\begin{aligned} \left[{k \atop b} \right]_q \#C &= \sum_{W \in B_P} \#\mathcal{I}\left(C, W\right) + (\beta/\alpha + 1) \sum_{W \in B_F} \#\mathcal{I}\left(C, W\right) \\ &\le \#B_P + (\beta/\alpha + 1)\#B_F = \left[{v-1 \atop b} \right]_q + (\beta/\alpha + 1)\#B_F \end{aligned}$$

Eighth, using the q-Pascal identities of Lemma 3 and the representation of q-binomial coefficients of Lemma 2, we compute

$$\begin{aligned} \frac{\beta}{\alpha} + 1 &= \frac{\beta + \alpha}{\alpha} = \frac{\left[{k \atop b} \right]_q - \left[{k-1 \atop b} \right]_q}{\alpha} = \frac{\left[{k-1 \atop b-1} \right]_q q^{k-b}}{\alpha} \\ &= \begin{cases} \dfrac{\left[{k-1 \atop b-1} \right]_q q^{k-b}}{\left[{k-2 \atop b-2} \right]_q q^{k-b}} = \frac{[k-1]_q![b-2]_q![k-b]_q!}{[b-1]_q![k-b]_q![k-2]_q!} = \frac{[k-1]_q}{[b-1]_q} & \text{if } 2 \mid q, \\ \dfrac{\left[{k-1 \atop b-1} \right]_q q^{k-b}}{\left[{k-1 \atop b-1} \right]_q} = q^{k-b} & \text{if } 2 \nmid q, \end{cases} \end{aligned}$$

which concludes the proof. □

160 **Example**
The group $G' = \left(\begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & \\ & I_{v-2} \end{pmatrix} \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_q^v)), \mathrm{id}\right) \le \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ fixes for $2 \le v$ and all $q \ge 2$ prime power the points in

$$\langle (1,1,0,\ldots,0),(0,0,1,\ldots,0),\ldots,(0,0,0,\ldots,1)\rangle \cup \langle (1,-1,0,\ldots,0)\rangle \subseteq \mathbb{F}_q^v$$

and the union is point-wise disjoint iff q is odd.

Let $q=2$, $v=7$, $d=4$, $k=3$, and $G \le \mathrm{GL}(\mathbb{F}_2^7)$ any subgroup with order 2 such that the set of fixed points form a 6-dimensional subspace, e.g., a conjugate to G'. Then, by the last lemma, any $(7,N,4;3;G)_2$ CDC fulfills $7N \le 651 + 1 \cdot 32 \cdot 3$, i.e., $N \le 106.72$. In particular, there is no CDC with these parameters of size at least 107 such that there is a conjugate to the matrix depicted above in its automorphism group.

Ignoring the parity of q, we can prove that the bound for even q in Lemma 159 is always tighter than the bound for odd q. By comparing the bound for odd q with the cardinality of corresponding LMRD codes, we see that latter strictly surpasses the bounds and hence no maximum code for fitting parameters has any group fulfilling the conditions of Lemma 159 as automorphism subgroup.

161 **Corollary**
Let $q \ge 2$ be a prime power and $2 \le d/2 < k \le v-k$ integers. Then

$$\begin{bmatrix} v-2 \\ k-d/2-1 \end{bmatrix}_q q^{v-k+d/2-1} \frac{[k-1]_q}{[k-d/2]_q} < \begin{bmatrix} v-1 \\ k-d/2 \end{bmatrix}_q q^{d/2-1}$$

and in particular the odd bound of Lemma 159 has at least the size of the even bound for the same q.

Next, we also have

$$\begin{bmatrix} v-1 \\ k-d/2+1 \end{bmatrix}_q + \begin{bmatrix} v-1 \\ k-d/2 \end{bmatrix}_q q^{d/2-1} < \begin{bmatrix} k \\ d/2-1 \end{bmatrix}_q q^{(v-k)(k-d/2+1)}$$

which proves that both bounds in Lemma 159 are smaller than an LMRD code with the same parameters of size $q^{(v-k)(k-d/2+1)}$, i.e., no code of size at least $q^{(v-k)(k-d/2+1)}$ has G of Lemma 159 as automorphism group.

Proof
Applying Lemma 2 and the estimation of Lemma 5 yields

$$\begin{aligned}
&\frac{\begin{bmatrix} v-2 \\ k-d/2-1 \end{bmatrix}_q q^{v-k+d/2-1}[k-1]_q}{\begin{bmatrix} v-1 \\ k-d/2 \end{bmatrix}_q q^{d/2-1}[k-d/2]_q} \\
&= \frac{[v-2]_q![k-d/2]_q![v-k+d/2-1]_q!q^{v-k}[k-1]_q}{[k-d/2-1]_q![v-k+d/2-1]_q![v-1]_q![k-d/2]_q} \\
&= \frac{q^{v-k}[k-1]_q}{[v-1]_q} < q^{v-k}q^{k-v} = 1.
\end{aligned}$$

For the next part, we abbreviate $a = v-k$ and $b = k-d/2+1$, i.e., $2 \le b \le a-1$ and $1 \le a-b \le a-2$. Since $0 \le \mu(q)^{-1}q^b - 1$ we conclude

$$\begin{aligned}
&\begin{bmatrix} v-1 \\ b \end{bmatrix}_q + \begin{bmatrix} v-1 \\ b-1 \end{bmatrix}_q q^{k-b} < \begin{bmatrix} k \\ b \end{bmatrix}_q q^{ab} \\
&\Leftarrow \mu(q)q^{b(v-b-1)} + \mu(q)q^{(b-1)(v-b)}q^{k-b} \le q^{b(k-b)}q^{ab} \Leftrightarrow \mu(q)q^{a-b} + \mu(q) \le q^a \\
&\Leftrightarrow 1 \le (\mu(q)^{-1}q^b - 1)q^{a-b} \Leftarrow 1 \le (\mu(q)^{-1}q^b - 1)q \Leftrightarrow (q^{-1}+1)\mu(q) \le q^b.
\end{aligned}$$

This proves the claim for $3 \le q$ or $3 \le b$ because $\mu(q) \le q^2$ for $2 \le q$, $\mu(q) \le q$ for $3 \le q$, and $1+q \le q^2$ for $2 \le q$. Hence, only the case $q = b = 2$ remains.

Using $(1/2;1/2)_1 = 1/2$ and $(1/2;1/2)_2 = 3/8$ we get by applying Lemma 8 the inequalities $\begin{bmatrix} v-1 \\ 2 \end{bmatrix}_2 < \frac{8}{3}2^{2(v-3)}$, $\begin{bmatrix} v-1 \\ 1 \end{bmatrix}_2 < 2 \cdot 2^{v-2}$, and $2^{2(k-2)} < \begin{bmatrix} k \\ 2 \end{bmatrix}_2$ and in turn

$$\begin{aligned}
&\begin{bmatrix} v-1 \\ 2 \end{bmatrix}_2 + \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_2 2^{k-2} < \begin{bmatrix} k \\ 2 \end{bmatrix}_2 2^{2a} \Leftarrow \tfrac{1}{3}2^{2v-3} + 2^{v+k-3} \le 2^{2v-4} \\
&\Leftrightarrow 2 \cdot 2^v + 6 \cdot 2^k \le 3 \cdot 2^v \Leftrightarrow 6 \le 2^{v-k},
\end{aligned}$$

which is true for all $3 \le a$. □

Before we can state Lemma 159 for partial spreads, we first need two auxiliary lemmata to prove that, under the operation of a fitting group, there is a point such that any fixed line which is not point-wise fixed contains this point.

162 Lemma
Let $q \ge 2$ be a prime power and $A, B, C, D \le \mathbb{F}_q^3$ four different points such that they form a quadrangle, i.e., no three points of them are collinear. Then, $((A+B) \cap (C+D)) + ((A+C) \cap (B+D)) + ((A+D) \cap (B+C))$ is a line iff q is even.

Proof
Let $A = \langle a \rangle$, $B = \langle b \rangle$, $C = \langle c \rangle$, and $D = \langle d \rangle$, then $\{a, b, c\}$ span $\mathbb{F}_q^3$ and hence there is a matrix $M' \in \mathrm{GL}(\mathbb{F}_q^3)$ with $aM' = (1,0,0)$, $bM' = (0,1,0)$, and $cM' = (0,0,1)$. Since no three are collinear, $dM' = (x,y,z)$ with $x, y, z \in \mathbb{F}_q^*$ and using $M'' = \begin{pmatrix} x^{-1} & 0 & 0 \\ 0 & y^{-1} & 0 \\ 0 & 0 & z^{-1} \end{pmatrix} \in \mathrm{GL}(\mathbb{F}_q^3)$

with $M := M'M''$, we get $AMZ(\mathrm{GL}(\mathbb{F}_q^3)) = \langle(1,0,0)\rangle$, $BMZ(\mathrm{GL}(\mathbb{F}_q^3)) = \langle(0,1,0)\rangle$, $CMZ(\mathrm{GL}(\mathbb{F}_q^3)) = \langle(0,0,1)\rangle$, and $DMZ(\mathrm{GL}(\mathbb{F}_q^3)) = \langle(1,1,1)\rangle$, which in turn allows to use wlog. $A = \langle(1,0,0)\rangle$, $B = \langle(0,1,0)\rangle$, $C = \langle(0,0,1)\rangle$, and $D = \langle(1,1,1)\rangle$.

Hence we have the six lines $A+B = \tau^{-1}\left(\begin{smallmatrix}1&0&0\\0&1&0\end{smallmatrix}\right)$, $A+C = \tau^{-1}\left(\begin{smallmatrix}1&0&0\\0&0&1\end{smallmatrix}\right)$, $A+D = \tau^{-1}\left(\begin{smallmatrix}1&0&0\\0&1&1\end{smallmatrix}\right)$, $B+C = \tau^{-1}\left(\begin{smallmatrix}0&1&0\\0&0&1\end{smallmatrix}\right)$, $B+D = \tau^{-1}\left(\begin{smallmatrix}1&0&1\\0&1&0\end{smallmatrix}\right)$, and $C+D = \tau^{-1}\left(\begin{smallmatrix}1&1&0\\0&0&1\end{smallmatrix}\right)$, as well as the three intersection points $(A+B)\cap(C+D) = \tau^{-1}(1,1,0)$, $(A+C)\cap(B+D) = \tau^{-1}(1,0,1)$, $(A+D)\cap(B+C) = \tau^{-1}(0,1,1)$.

Then $((A+B)\cap(C+D)) + ((A+C)\cap(B+D)) + ((A+D)\cap(B+C)) = \tau^{-1}\left(\mathrm{RREF}\left(\begin{smallmatrix}1&1&0\\1&0&1\\0&1&1\end{smallmatrix}\right)\right) = \tau^{-1}\left(\mathrm{RREF}\left(\begin{smallmatrix}1&0&1\\0&1&1\\0&0&2\end{smallmatrix}\right)\right)$, which is a line iff q is even. $\square$

163 Lemma

Let $q \geq 2$ be a prime power, v a positive integer and $G \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-1)$-dimensional subspace if q is even and the disjoint union of a $(v-1)$-dimensional subspace with a point if q is odd. Then any fixed line which is not point-wise fixed contains the same point $Q \leq \mathbb{F}_q^v$.

Proof

Let $\mathcal{F} = F$, if q is even and $\mathcal{F} = F \dot\cup f$, if q is odd for a hyperplane $F \leq \mathbb{F}_q^v$ and a point $f \leq \mathbb{F}_q^v$ with $f \not\leq F$ the set of fixed points under the operation of G. Moreover let $g \in G$ be the non-trivial element.

Let q be even and A, B non-fixed points in $\mathbb{F}_q^v$ such that $A + Ag \neq B + Bg$ are two different lines which then are fixed, but not point-wise fixed. We will show that $A + Ag$ and $B + Bg$ contain a common fixed point Q, which then is in all fixed lines which are not point-wise fixed, since any fixed line which is not point-wise fixed contains exactly one fixed point.

Let $P = (A+B)\cap F$, then P is fixed and in particular $P = (Ag+Bg)\cap F = ((A+B)g)\cap F$ and $(A+B)\cap(Ag+Bg) = P$ (if the intersection would be larger, then A, B, Ag, Bg would be on the same line), i.e., $E = A+B+Ag+Bg$ is a plane. Hence $A+Ag$ and $B+Bg$ intersect in exactly a point Q, we have to show that Q is fixed.

Let $P' = (A+Bg)\cap F$, then, like before, $P' = (Ag+B)\cap F = (A+Bg)\cap(Ag+B)$.

Since $E \cong \mathbb{F}_q^3$ and with A, B, $C = Ag$, and $D = Bg$ no three points of $\{A, B, C, D\}$ are collinear, otherwise both lines would be equal, we apply Lemma 162 and see that

$$L = \underbrace{((A+B)\cap(Ag+Bg))}_{P} + \underbrace{((A+Ag)\cap(B+Bg))}_{Q} + \underbrace{((A+Bg)\cap(B+Ag))}_{P'}$$

is a line, which is in particular point-wise fixed, since it contains two different fixed points P and P' and hence Q is fixed.

Let q be odd and L be a line that is fixed, but not point-wise fixed. Since L contains $q+1$ points, which is an even number, and intersects F in exactly one point, it also contains f. Hence, setting $Q = f$ completes the proof. $\square$

The next lemma states Lemma 159 for partial spreads.

164 Lemma
Let $q \geq 2$ be a prime power, $2 \leq k \leq v-k$ integers and $G \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-1)$-dimensional subspace if q is even and the disjoint union of a $(v-1)$-dimensional subspace with a point if q is odd. Let C be a $(v, \#C, 2k; k)_q$ CDC with $G \leq \mathrm{Aut}(C)$. Then

$$[k]_q \#C \leq [v-1]_q + q^{k-1}$$

and in particular

$$\mathrm{A}_q(v, 2k; k; G) \leq \frac{[v-1]_q + q^{k-1}}{[k]_q} = q^{k-1}\frac{q^{v-k}-1}{q^k-1} + 1.$$

Proof
We use the term fixed with respect to G operating on the set of subspaces without further notice and partition $C = C_P \dot\cup C_F \dot\cup C_N$, such that C_P contains all point-wise fixed codewords, C_F contains all codewords that are fixed but not point-wise fixed, and C_N contains all codewords which are not fixed.

Let $\mathcal{F} = F$ if q is even and $\mathcal{F} = F \dot\cup f$ if q is odd for a hyperplane $F \leq \mathbb{F}_q^v$ and a point $f \leq \mathbb{F}_q^v$ with $f \not\leq F$ the set of fixed points under the operation of G.

Let Q be the fixed point that any line which is fixed but not point-wise fixed contains by Lemma 163.

$C_N = \emptyset$ by the minimum distance and $\#C_F \leq 1$, since any two codewords in C_F contain Q.

The inequality

$$\begin{bmatrix} k \\ 1 \end{bmatrix}_q \#C \leq (q^{k-1} + \mathbb{1}_{2|q})\#\mathcal{I}(C, Q) + \sum_{P \in \begin{bmatrix} F \\ 1 \end{bmatrix} \setminus \{Q\}} \#\mathcal{I}(C, P)$$

is valid, since any codeword contributes $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ to the left hand side and

- for an even q, any $U \in C_P$ which contains Q also contains $\begin{bmatrix} k \\ 1 \end{bmatrix}_q - 1$ other fixed points and hence contributes $q^{k-1} + \begin{bmatrix} k \\ 1 \end{bmatrix}_q \geq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$ to the right hand side,
- for an even q, any $U \in C_P$ which does not contain Q contains $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ fixed points, contributing $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ to the right hand side,
- for an even q, any $U \in C_F$ contains Q and also $\begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q - 1$ fixed points, contributing $q^{k-1} + \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q = \begin{bmatrix} k \\ 1 \end{bmatrix}_q$, which is implied by the q-Pascal identities from Lemma 3, to the right hand side,

- for an odd q, any $U \in C_P$ contains $\left[{k \atop 1}\right]_q$ fixed points and hence contributes $\left[{k \atop 1}\right]_q$ to the right hand side, and
- for an odd q, any $U \in C_F$ contains Q and also $\left[{k-1 \atop 1}\right]_q$ fixed points, contributing $q^{k-1} + \left[{k-1 \atop 1}\right]_q = \left[{k \atop 1}\right]_q$, which is implied by the q-Pascal identities from Lemma 3, to the right hand side.

This inequality may be estimated further by Lemma 41 to

$$\begin{aligned}\left[{k \atop 1}\right]_q \#C &\leq (q^{k-1} + \mathbb{1}_{2|q})\#\mathcal{I}(C,Q) + \sum_{P \in \left[{F \atop 1}\right] \setminus \{Q\}} \#\mathcal{I}(C,P) \\ &\leq q^{k-1} + \mathbb{1}_{2|q} + \#(\left[{F \atop 1}\right] \setminus \{Q\}) = q^{k-1} + \mathbb{1}_{2|q} + \left[{v-1 \atop 1}\right]_q - \mathbb{1}_{2|q}\end{aligned}$$

which concludes the proof. □

Analogously to Corollary 161, the size of an LMRD surpasses the bound in the last lemma.

165 Lemma
Let $q \geq 2$ be a prime power, $2 \leq k \leq v-k$ integers and $G \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-1)$-dimensional subspace if q is even and the disjoint union of a $(v-1)$-dimensional subspace with a point if q is odd. Let C be a $(v, \#C, 2k; k)_q$ CDC with $\#C \geq q^{v-k}$. Then $G \not\leq \mathrm{Aut}(C)$, which is particularly true for codes of maximum size.

Proof
We prove that any code with G as automorphism group is smaller than the corresponding LMRD of size q^{v-k}, i.e.,

$$\mathrm{A}_q(v, 2k; k; G) \leq q^{k-1}\frac{q^{v-k}-1}{q^k-1} + 1 < q^{v-k} \leq \mathrm{A}_q(v, 2k; k).$$

Since $1 < 2 \leq q^{k-1}(q-1)$ we have $q^{k-1} < q^k - 1$ and hence $q^{k-1}\frac{q^{v-k}-1}{q^k-1} + 1 < q^{k-1}\frac{q^{v-k}-1}{q^{k-1}} + 1 = q^{v-k}$ the bound of Lemma 164 yields the inequality. □

We can also argue a more tailored upper bound for additional subgroups if q is even.

166 Lemma
Let $q \geq 2$ be an even prime power, $6 \leq v$ integers, and $G \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$ a subgroup with $\#G = 2$ such that the set of fixed points in $\mathbb{F}_q^v$ under the operation of G is a $(v-2)$-dimensional subspace. Let C be a $(v, \#C, 4; 3)_q$ CDC with $G \leq \mathrm{Aut}(C)$. Then

$$\#C \leq \frac{\left[{v-2 \atop 2}\right]_q}{q^2+q+1} + \frac{(q+1)^2 q^{v-3}}{q^2+q+1} + \frac{\left[{v \atop 2}\right]_q - \left[{v-2 \atop 2}\right]_q - [v-2]_q \cdot q^{v-3}(q+1)}{q^2}.$$

Proof
Let F be the $(v-2)$-dimensional subspace consisting of fixed points, $B_P, B_F, B_4 \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ 2 \end{bmatrix}$, such that all lines in B_P are point-wise fixed, all lines in B_F are fixed but not point-wise fixed, and all lines L in B_4 have the property that $\dim(\langle L \cdot G \rangle) = 4$, i.e., L contains no fixed point.

Then, the following equality is valid

$$\#C = \frac{1}{q^2+q+1} \sum_{L \in B_P} \#\mathcal{I}(C, L) + \frac{q+1}{q^2+q+1} \sum_{L \in B_F} \#\mathcal{I}(C, L) + \frac{1}{q^2} \sum_{L \in B_4} \#\mathcal{I}(C, L)$$

by distinguishing three cases of codewords. Let $U \in C$ be a codeword, then U contributes one to the left hand side and

- if U is point-wise fixed, it contains $\begin{bmatrix} 3 \\ 2 \end{bmatrix}_q = q^2+q+1$ lines in B_P and no other lines, contributing exactly one to the right hand side,
- if U is fixed but not point-wise fixed, it intersects F in a line (since $\begin{bmatrix} 3 \\ 2 \end{bmatrix}_q = q^2+q+1$ is odd), hence this line is in B_P and by Lemma 158 it contains q lines of B_F. Since it contains no line of B_4 (otherwise $\dim(U) \geq 4$), it contributes $\frac{1}{q^2+q+1} + q\frac{q+1}{q^2+q+1} = 1$ to the right hand side, and
- if U is not fixed, then $\dim(U \cap F) = 1$, since $\dim(U \cap F) = 2$ violates the minimum distance, and contains in particular no fixed line. Since $\begin{bmatrix} 3-1 \\ 2-1 \end{bmatrix}_q = q+1$ lines in U contain $U \cap F$, all other $\begin{bmatrix} 3 \\ 2 \end{bmatrix}_q - (q+1) = q^2$ lines are in B_4 and consequently U contributes $q^2/q^2 = 1$ to the right hand side.

Using the inequality of Lemma 41 we can estimate the right hand side to

$$\leq \frac{1}{q^2+q+1}\#B_P + \frac{q+1}{q^2+q+1}\#B_F + \frac{1}{q^2}\#B_4.$$

Clearly $\#B_P = \begin{bmatrix} v-2 \\ 2 \end{bmatrix}_q$.

Next, any $L \in B_F$ contains $q+1$ points, which is an odd number, and hence exactly one fixed point. The other q points fall in $q/2$ orbits under G of which each orbit spans L. The total number of orbits of points is $(\begin{bmatrix} v \\ 1 \end{bmatrix}_q - \begin{bmatrix} v-2 \\ 1 \end{bmatrix}_q)/2 = q^{v-2}(q+1)/2$ and hence $\#B_F = \frac{q^{v-2}(q+1)/2}{q/2} = q^{v-3}(q+1)$.

Subtracting the number of point-wise fixed lines and the number of lines that contain exactly one fixed point (any line containing exactly one fixed point contains q points that are not in F) from the number of lines in total, we obtain $\#B_4 = \begin{bmatrix} v \\ 2 \end{bmatrix}_q - \#B_P - \begin{bmatrix} v-2 \\ 1 \end{bmatrix}_q \cdot ([v]_q - [v-2]_q)/q = \begin{bmatrix} v \\ 2 \end{bmatrix}_q - \#B_P - \begin{bmatrix} v-2 \\ 1 \end{bmatrix}_q \cdot \#B_F$. □

For example the group

$$G = \left\langle \left(\begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & \\ & \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & \\ & & I_{v-4} \end{pmatrix} \cdot \mathrm{Z}(\mathrm{GL}(\mathbb{F}_q^v)), \mathrm{id} \right) \right\rangle$$

fulfills the requirements of the lemma and applied to $q = 2$ and $v = 7$ it yields $\mathrm{A}_2(7,4;3;G) \le 298 + \frac{5}{7} \approx 298.7$.

The next lemma considers a specific conjugacy class of subgroups in the $\mathrm{GL}(\mathbb{F}_2^7)$, in which each group has order 3 and each non-trivial element of each group has a 5-dimensional eigenspace for the eigenvalue 1. The reasoning involves computations with `GAP`, cf. [GAP18].

167 Lemma
Let $G = \left\langle \begin{pmatrix} \begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix} & \\ & I_5 \end{pmatrix} \right\rangle \le \mathrm{GL}(\mathbb{F}_2^7) \cong \mathrm{P\Gamma L}(\mathbb{F}_2^7)$. Then $\mathrm{A}_2(7,4;3;G) \le 255$.

Proof
Denote $g = \begin{pmatrix} \begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix} & \\ & I_5 \end{pmatrix} \in \mathrm{GL}(\mathbb{F}_2^7)$. Since points and non-zero vectors correspond in $\mathbb{F}_2$, the set of fixed points F is the set of points in the eigenspace of g for the eigenvalue 1, i.e.,

$$F = \tau^{-1}\begin{pmatrix} 0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}.$$

Let C be a $(7,\#C,4;3;G)_2$ CDC and $B_P, B_F, B_4 \subseteq \begin{bmatrix} \mathbb{F}_2^7 \\ 2 \end{bmatrix}$ such that all lines in B_P are point-wise fixed, all lines in B_F are fixed but not point-wise fixed, and $B_4 = \left\{ L \in \begin{bmatrix} \mathbb{F}_q^v \\ 2 \end{bmatrix} \;\middle|\; \dim(\langle L, Lg, Lg^2\rangle) = 4 \wedge \dim(L \cap Lg \cap Lg^2) = 0 \right\}$.

Note that $B_P = \begin{bmatrix} F \\ 2 \end{bmatrix}$, $B_F = \{\tau^{-1}(\begin{smallmatrix} 1&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0 \end{smallmatrix})\}$ ($L \in B_F \Leftrightarrow \exists l \in \mathbb{F}_2^7 : L = \{\mathbf{0}, l, l \cdot g, l \cdot g^2\} \Leftrightarrow l + l \cdot g = l \cdot g^2 \Leftrightarrow l \in \ker(I_7 + g + g^2)$), and $\#B_4 = 930$, by a computation with `GAP`. Each $U \in \begin{bmatrix} \mathbb{F}_2^7 \\ 3 \end{bmatrix}$ which is not fixed but fulfills $\dim(U \cap (U \cdot g)) \le 1$ and $\dim(U \cap (U \cdot g^2)) \le 1$ (otherwise $U \notin C$ by the minimum distance) contains exactly 4 lines in B_4, by a computation with `GAP`.

Then the following inequality holds

$$\#C \le \frac{1}{7} \sum_{L \in B_P} \#\mathcal{I}(C, L) + \sum_{L \in B_F} \#\mathcal{I}(C, L) + \frac{1}{4} \sum_{L \in B_4} \#\mathcal{I}(C, L)$$

by distinguishing three cases for $U \in C$, which contributes one to the left hand side,

- if U is point-wise fixed, then it contains 7 lines in B_P and no other lines and hence it contributes one to the right hand side,
- if U is fixed but not point-wise fixed, then $\dim(U \cap F) \in \{1, 2\}$. If the intersection would be 2, then the remaining 4 points would have at least a fixed point but all fixed points are contained in F, which is a contradiction. Hence, this intersection is 1-dimensional and U contains no line in B_P and at least one of the seven lines in U is fixed which then cannot be in F, i.e., this line is in B_F. Since it contains no line in B_4 (if it did, then $\dim(U) \ge 4$), U contributes exactly one to the right hand side, and

- if U is not fixed then it does not contain a fixed line by the minimum distance and by the preceding discussion it contains exactly 4 lines of B_4, contributing also exactly one to the right hand side.

With Lemma 41 we can estimate the right hand side further to

$$\leq \#B_P/7 + \#B_F + \#B_4/4 = 155/7 + 1 + 930/4 = 255 + 9/14$$

which then can be rounded down since $\#C$ is an integer. □

Another reasoning is able to provide an upper bound for CDCs having prescribed symmetry.

168 Lemma
Let $q \geq 2$ be a prime power, $2 \leq d/2 \leq k \leq v-k$, $f < m \leq M$, u, o, λ be integers, $U \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$, f be the number of fixed subspaces in $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ under the operation of U, $o = \mathrm{ord}(U)$, u be the smallest positive not-one divisor of o, and $m \leq \mathrm{A}_q(v,d;k) \leq M$.

1. If $M < u$, then $\mathrm{A}_q(v,d;k;U) \leq f$.
2. If o is a prime, $\lambda o + f < m$, and $M < (\lambda+1)o$, then $\mathrm{A}_q(v,d;k;U) \leq \lambda o + f$.

In both cases, no maximum $(v,N,d;k)_q$ CDC has the automorphism subgroup U.

Proof
Since $\mathrm{A}_q(v,d;k) < u$, any $(v,N,d;k;U)_q$ CDC consists of fixed subspaces in the first case and since $\mathrm{A}_q(v,d;k;U) < (\lambda+1)o$, any $(v,N,d;k;U)_q$ CDC contains at most λ orbits of size o and at most f fixed k-spaces. The primality of o completes the second case. □

169 Corollary
$\mathrm{A}_2(4,4;2;U_1) = 0$, $\mathrm{A}_2(5,4;2;U_2) \leq 8$, and $\mathrm{A}_2(5,4;2;U_3) = 0$ for any $U_1 \leq \mathrm{GL}(\mathbb{F}_2^4)$ of order 7, $U_2 \leq \mathrm{GL}(\mathbb{F}_2^5)$ of order 7, and $U_3 \leq \mathrm{GL}(\mathbb{F}_2^5)$ of order 31.

Proof
We will use $\mathrm{A}_2(4,4;2) = 5$ and $\mathrm{A}_2(5,4;2) = 9$ as well as $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$ and $x^{31} - 1 = (x+1)(x^5+x^2+1)(x^5+x^3+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$ over $\mathbb{F}_2$.

Since a line consists of 3 points over $\mathbb{F}_2$ and the order of the three groups are at least 7 and prime, any fixed line is point-wise fixed in all three cases. Moreover, a point $\langle p \rangle$ with $p \in \mathbb{F}_2^v$, $2 \leq v$ is fixed by $\langle M \rangle \leq \mathrm{GL}(\mathbb{F}_2^v) \cong \mathrm{P\Gamma L}(\mathbb{F}_2^v)$ iff $pM = p$, i.e., p is non-zero and in the eigenspace of M for the eigenvalue 1.

Next, in all three cases the minimal polynomial $m(x)$ of an arbitrary generating matrix is monic and not 1 or $x+1$ due to the order of at least 7.

In the first two cases, $m(x)$ divides x^7-1 and has hence at least degree 3 and therefore $x+1$ divides the characteristic polynomial at most once in the first case and at most twice in the second case, i.e., the algebraic multiplicity of 1 is at most 1 in the first case and at most 2 in the second case. Since the geometric multiplicity of 1, i.e., the dimension of the eigenspace of 1, is upper bounded by the algebraic multiplicity of 1, we have at most one fixed point in the first case and at most one point-wise fixed line in the second case. Then Lemma 168 with $m = M = 5$, $\lambda = 0$ and $m = M = 9$, $\lambda = 1$ completes the proof in the first and second case, respectively.

In the third case, $m(x)$ divides $x^{31}-1$ and hence has degree 5 and is therefore equal to the characteristic polynomial and in particular the algebraic multiplicity of 1 is zero. Then Lemma 168 with $m = M = 9$, $\lambda = 0$ completes this case. $\square$

Unfortunately, this technique and especially Lemma 168 may not be applied to upper bound $\mathrm{A}_2(7,4;3;U)$ with an $U \le \mathrm{GL}(\mathbb{F}_2^7)$ of order 127. Although $x^{127}-1 = (x+1)(x^7+x+1)(x^7+x^3+1)(x^7+x^3+x^2+x+1)(x^7+x^4+1)(x^7+x^4+x^3+x^2+1)(x^7+x^5+x^2+x+1)(x^7+x^5+x^3+x+1)(x^7+x^5+x^4+x^3+1)(x^7+x^5+x^4+x^3+x^2+x+1)(x^7+x^6+1)(x^7+x^6+x^3+x+1)(x^7+x^6+x^4+x+1)(x^7+x^6+x^4+x^2+1)(x^7+x^6+x^5+x^2+1)(x^7+x^6+x^5+x^3+x^2+x+1)(x^7+x^6+x^5+x^4+1)(x^7+x^6+x^5+x^4+x^2+x+1)(x^7+x^6+x^5+x^4+x^3+x^2+1)$ proves exactly in the same way as in the last lemma that the minimal polynomial has degree 7 and equals the characteristic polynomial and that there is no fixed point, the tightest known bounds are $333 \le \mathrm{A}_2(7,4;3) \le 381$ and we are forced to choose $m = 333$ and $M = 381$, which renders the application of Lemma 168 infeasible since there is no λ with the needed properties.

11 Algorithmic arguments for the exclusion of automorphisms

In this chapter, we describe a method to compute candidates for automorphism groups of large codes, previously presented in [Hei+17c]. Although it is an exhaustive search of all subgroups of a given finite group, which is, despite of being finite, often simply not possible due to time restrictions, it is nevertheless applicable for large finite ambient groups, since not the subgroups but rather the conjugacy classes of subgroups are enumerated and not even all of them. If, for fixed q, v, d, and k, there is no U-invariant $(v, \#C, d; k)_q$ CDC of the desired size, then by Lemma 29 there is especially no supergroup of any conjugate of U such that there is a $(v, \#C, d; k)_q$ CDC having at least the desired size.

We want to emphasize that this method is a very general technique which can be applied in various situations. We only take advantage that the ambient group is $\mathrm{P\Gamma L}(\mathbb{F}_2^v) = \mathrm{GL}(\mathbb{F}_2^v)$.

Applied to $(7, \#C, 4; 3)_2$ CDCs C we can derive the following facts. The ambient symmetry group is $\mathrm{GL}(\mathbb{F}_2^7)$, which has $163\,849\,992\,929\,280 \approx 1.6 \cdot 10^{14}$ elements and many subgroups.

170 **Theorem ([Hei+17c, Theorem 1])**
Let C be a set of planes in $\mathrm{PG}(6, 2)$ which are mutually intersecting in at most one point. If $|C| \geq 329$, then the automorphism group of C is conjugate to one of the 33 subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$ given in Appendix 14.1.1. The orders of these groups are $1^1 2^1 3^2 4^7 5^1 6^3 7^2 8^{11} 9^2 12^1 14^1 16^1$. Moreover, if $|C| \geq 330$ then $|\mathrm{Aut}(C)| \leq 14$ and if $|C| \geq 334$ then $|\mathrm{Aut}(C)| \leq 12$.

171 **Theorem ([Hei+17c, Theorem 2])**
In $\mathrm{PG}(6, 2)$, there exists a set C of 333 planes which are mutually intersecting in at most one point. Hence,

$$\mathrm{A}_2(7, 4; 3) \geq 333.$$

The set C is given explicitly in Appendix 14.1.2. Its automorphism group $\mathrm{Aut}(C)$ is isomorphic to the Klein four-group. It is the group $G_{4,6}$ in Appendix 14.1.1.

In the language of projective geometry, see e.g. [ES16] for a contemporary survey, a $(7, 333, 4; 3)_2$ CDC corresponds to collections of planes in $\mathrm{PG}(6, 2)$ which mutually intersect in at most one point. Prior to [Hei+17c] the best known bounds were $329 \leq \mathrm{A}_2(7,4;3) \leq 381$, see [BR14] and Theorem 107. Moreover, the q-Steiner system $S(2,3,7)_2$ would be a $(7,381,4;3)_2$ CDC of maximum size, if it exists, and vice versa, cf. Chapter 2. This upper bound of 381 may only be attained if any line is contained in exactly one codeword.

Many articles focus on the existence question for $S(2,3,7)_2$ q-Steiner system respective $(7,381,4;3)_2$ CDCs, e.g. [Etz15a; Etz15b; EV11b; HK16; HS16; KP15; Met99; MMY95; Tho87; Tho96], and in [BKN16; KKW17] all but one conjugacy class of non-trivial automorphism groups ($G_{2,1}$ in Appendix 14.1.1) were eliminated and in particular the automorphism group of any putative $(7,381,4;3)_2$ CDC has at most order two.

11.1 Ascending in the subgroup lattice

The key technique, which renders this method feasible, is to construct only *necessary* groups.

172 **Lemma (cf. [Hei+17c, Lemma 4])**
Let G be a finite group and $\{A \leq G\}$ the set of its subgroups, n, u be positive integers such that $n \mid u \mid \#G$ and any subgroup of G of order u contains at least one normal subgroup of order n, and $f : \{A \leq G\} \to \{0,1\}$ be a map that is monotonically decreasing, i.e., $f(A) \geq f(B)$ for all $A \leq B$.

1. Suppose $T = \{N \leq G \mid \#N = n \text{ and } f(N) = 1\}$ and $L = \{U \leq G \mid \#U = u \text{ and } N \leq U \leq N_G(N) \text{ for an } N \in T\}$. Then $f(U) = 0$ for all $U \leq G$ with $\#U = u$ and $U \notin L$.

2. Let furthermore f be invariant under conjugation, i.e., $f(A^g) = f(A)$ for all $g \in G$ and u/n is prime. Suppose T is a transversal of $\{N^G \mid N \leq G, \#N = n \text{ and } f(N) = 1\}$, P_N is a transversal of $\{g^{N_G(N)} \mid g \in N_G(N)\}$, and $L = \{\langle N, g\rangle^G \mid N \in T, g \in P_N, \#\langle N, g\rangle = u\}$. Then $f(U) = 0$ for all $U \leq G$ with $\#U = u$ and $U^G \notin L$.

Proof

1. Let $\bar{U} \leq G$ with $\#\bar{U} = u$ and $\bar{U} \notin L$. Then $\bar{U}$ contains a normal subgroup $\bar{N}$ of order n and in particular the relation $\bar{N} \leq \bar{U} \leq N_G(\bar{N})$ holds. Since $\bar{U} \notin L$ we have $\bar{N} \notin T$. This implies $f(\bar{N}) = 0$ and by monotonicity $f(\bar{U}) = 0$.

2. First, since u/n is a prime, $U \leq G$ of order u is $\langle N, g\rangle$ for an $N \leq G$ with $\#N = n$ and a $g \in N_G(N)$ with $g \notin N$.

   Second, let $\bar{U} \leq G$ with $\#\bar{U} = u$ and $\bar{U}^G \notin L$. Then $\bar{U}$ contains a normal subgroup $\bar{N}$ of order n. Assume there is a $g \in G$ such that $\bar{N}^g = M \in T$. Note that $\bar{N}^g \leq \bar{U}^g$. Let $l \in \bar{U}^g \setminus M$, then there is a $h \in N_G(M)$ such that $l^h = k \in P_M$ and

$\bar{U}^{gh} = \langle M, k\rangle$. Then $\langle M, k\rangle^G \in L$ is a contradiction. Hence, there is no such g and therefore $f(\bar{N}) = 0$, which in turn implies $f(\bar{U}) = 0$. □

The requirements on n and u may be fulfilled in many cases as the next lemma shows. The Small Groups Library (Page 30) may provide additional constellations of u and n such that Lemma 172 is applicable.

173 Lemma
Let U be a finite group, $p, q_1, \ldots, q_s$ different primes with $p \leq q_i$ for $i \in [s]$ for an integral $s \geq 1$, and $x, x_1, \ldots, x_s$ positive integers. If

1. $\#U = p^x$,
2. $\#U = pq_1^{x_1}$ or
3. $\#U = pq_1^{x_1} \ldots q_s^{x_s}$ and $\#U$ is a solvable number,

then U contains a normal subgroup of index p.

Proof
1. Theorem 16 guarantees a subgroup of order p^{x-1} and Corollary 26 shows its normality.
2. Theorem 16 guarantees a subgroup of order $q_1^{x_1}$ and Corollary 26 shows its normality.
3. By setting $\pi = \{q_1, \ldots, q_s\}$, Theorem 21 guarantees a subgroup of order $q_1^{x_1} \ldots q_s^{x_s}$ and Corollary 26 shows again its normality. □

11.2 Exhaustive search in the subgroup lattice

Throughout this section, let G be a finite group and $\{A \leq G\}$ the set of its subgroups, $\mathcal{P} : \{A \leq G\} \to \{0, 1\}$ be a map that is monotonically decreasing, i.e., $\mathcal{P}(A) \geq \mathcal{P}(B)$ for all $A \leq B$, and invariant under conjugation, i.e., $\mathcal{P}(A^g) = \mathcal{P}(A)$ for all $g \in G$.

We will now describe a technique to compute a superset of $\{A \leq G \mid \mathcal{P}(A) = 1\}$. The full implementation in `Magma`, cf. [BCP97], can be found in the appendix, Chapter 14.3.

11.2.1 The algorithm in pseudo code

The algorithm consists of two steps.

First, we compute a superset of $\{A \leq G \mid \mathcal{P}(A) = 1$ and $\#A$ is a prime power$\}$. Second, we compute a superset of $\{A \leq G \mid \mathcal{P}(A) = 1$ and $\#A$ is a no prime power$\}$.

Let $\mathcal{A}(H)$ be the abstract type of the group H and $\mathcal{G}(A)$ be an arbitrary group having the abstract type A, i.e., $\mathcal{A}(\mathcal{G}(A)) = A$ for all abstract types A.

Algorithm 5 Step 1

```
function GetConClassesSG(G, n, R)
Require: G a finite group, n ∈ ℤ, and R is a superset of a transversal of {A ≤ G : #A |
    n ∧ #A < n ∧ 𝒫(A) = 1} under the conjugation of G
Ensure: T is a transversal of S under conjugation in G with {A ≤ G | #A = n ∧ 𝒫(A) =
    1} ⊆ S ⊆ {A ≤ G | #A = n}. The computation of T does not evaluate 𝒫 but uses it
    implicitly via R as described in Lemma 172 and Lemma 173.
    return T
end function
function Step1(G, 𝒫)
Require: G a finite group, 𝒫 : {A ≤ G} → {0, 1} (monotonically decreasing and
    invariant under conjugation)
    if 𝒫(⟨⟩) = 0 then
        return ∅
    end if
    R ← {⟨⟩}                                        ▷ subgroups with 𝒫(·) = 1
    F ← ∅                                           ▷ subgroups with 𝒫(·) = 0
    Z ← 1  ▷ largest order for Step 2, any larger order contains an excluded p-group
    for p prime that divides #G do                  ▷ in any order, even in parallel
        TakeSylowGroup ← true
        M ← max{l : p^l | #G}
        for e ← 1 to M do                           ▷ in ascending order
            if e = M and TakeSylowGroup = false then
                Z ← Z · p^(M−1)
                continue
            end if
            C ← getConClassesSG(G, p^e, R)
            OneTaken ← false
            for c ∈ C do                            ▷ in any order, even in parallel
                if c contains an f ∈ F up to conjugacy in G or 𝒫(c) = 0 then
                    F ← F ∪ {c}
                    TakeSylowGroup ← false
                else
                    R ← R ∪ {c}
                    OneTaken ← true
                end if
            end for
            if OneTaken = false then
                Z ← Z · p^(e−1)
                break e
            end if
        end for
    end for
    return R, F, Z
end function
```

Algorithm 6 Step 2

function HALLDIVISORS(n)
Require: n is a positive integer
  return $\{a \in \mathbb{Z} \mid \exists b \in \mathbb{Z}, a \cdot b = n, a, b \geq 1, \mathrm{GCD}(a, b) = 1\}$
end function
function STEP2($G, \mathcal{P}, R, F, Z$)
Require: G a finite group, $\mathcal{P} : \{A \leq G\} \to \{0, 1\}$ (monotonically decreasing and invariant under conjugation), R, F, and Z from STEP1
  $F_O \leftarrow \{d | \#G : 1 \leq d, d$ is a prime power $, d \notin \{\#r \mid r \in R\}\}$
  $F_A \leftarrow \{\mathcal{A}(H) \mid H$ is an arbitrary group whose order is a prime power and divides $\#G, \mathcal{A}(H) \notin \{\mathcal{A}(r) \mid r \in R\}\}$
  for $n \in \{d | Z : 1 \leq d, d$ is no prime power$\}$ **do** ▷ in ascending order
    $A \leftarrow \{\mathcal{A}(H) \mid H$ is an arbitrary group of order $n\}$
    $h \leftarrow$ HALLDIVISORS(n)
    if n is a solvable order and $(h \cap F_O) \neq \emptyset$ **then** ▷ any group of order n contains an excluded subgroup
      $F_A \leftarrow F_A \cup A$
      $F_O \leftarrow F_O \cup \{n\}$
      continue
    end if
    for $a \in A$ **do** ▷ in any order, even in parallel
      if ($\mathcal{G}(a)$ is solvable and $(h \cap F_O) \neq \emptyset$) or $(F_O \cap \{\#b \mid b \leq \mathcal{G}(a)\} \neq \emptyset)$ or $(F_A \cap \{\mathcal{A}(b) \mid b \leq \mathcal{G}(a)\} \neq \emptyset)$ **then**
        $F_A \leftarrow F_A \cup \{a\}$
      end if
    end for
    if $A \subseteq F_A$ **then** ▷ all abstract types of order n could be excluded
      $F_O \leftarrow F_O \cup \{n\}$
      continue
    end if
    $C \leftarrow$ GETCONCLASSESSG(G, n, R)
    $OneTaken \leftarrow$ `false`
    for $c \in C$ **do** ▷ in any order, even in parallel
      if $\mathcal{A}(c) \in F_A$ or $\exists f \in F, g \in G : f^g \leq c$ **then**
        continue
      end if
      if $\mathcal{P}(c) = 1$ **then**
        $R \leftarrow R \cup \{c\}$
        $A \leftarrow A \setminus \mathcal{A}(c)$
        $OneTaken \leftarrow$ `true`
      else
        $F \leftarrow F \cup \{c\}$
      end if
    end for
    $F_A \leftarrow F_A \cup A$
    if $OneTaken =$ `false` **then**
      $F_O \leftarrow F_O \cup \{n\}$
    end if
  end for
  return R
end function

11.3 The evaluation function $\mathcal{P}$ for CDCs and shortcuts in the GL

In this section we describe a possibility to choose $\mathcal{P}$ such that $\{A \le G \mid \mathcal{P}(A) = 1\} \supseteq \{A \le G \mid \exists (v, N, d; k)_q$ CDC with $N \ge \kappa$ and $A \le \operatorname{Aut}(C)\}$ for a previously chosen $\kappa \in \mathbb{Z}_{\ge 0}$. Since the evaluation of $\mathcal{P}$ may take a long time, we will abort the computation after it exceeds a time limit of t seconds. If this time limit is set to ∞, then both sets are equal, i.e., $\{A \le G \mid \mathcal{P}(A) = 1\} = \{A \le G \mid \exists (v, N, d; k)_q$ CDC with $N \ge \kappa$ and $A \le \operatorname{Aut}(C)\}$.

Kohnert and Kurz presented in [KK08a, Theorem 2] a Kramer-Mesner approach for constructing constant dimension codes having a prescribed group of automorphisms:

174 **Theorem ([KK08a, Theorem 2])**
Let $H \le \operatorname{GL}(\mathbb{F}_q^v)$. There is a $(v, N, d'; k)_q$ CDC C with $H \le \operatorname{Aut}(C)$ and $d' \ge d$ iff there is a solution $x \in \{0,1\}^{\#\omega}$ for the equations $\sum_{i=1}^{\#\omega} (\#\omega_i) x_i = N$ and $M^H x \le \mathbf{1}$. Here, ω are the orbits of $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ under H, Ω are the orbits of $\begin{bmatrix} \mathbb{F}_q^v \\ k-d/2+1 \end{bmatrix}$ under H, $\mathbf{1} = (1, \ldots, 1)^T$ of length $\#\Omega$, and $M^H \in \mathbb{Z}_{\ge 0}^{\#\Omega \times \#\omega}$ such that $M^H_{\Omega_i, \omega_j} = \#\{U \in \omega_j \mid W \le U\}$ for an arbitrary $W \in \Omega_i$. Then $C = \cup_{i=1 : x_i = 1}^{\#\omega} \omega_i$.

This can be reformulated as BLP:

175 **Corollary**
Using the notation of the last theorem, there is a $(v, N, d'; k)_q$ CDC C with $H \le \operatorname{Aut}(C)$ and $d' \ge d$ of maximum cardinality iff

$$\begin{aligned} N = \max \sum_{i=1}^{\#\omega} (\#\omega_i) x_i & \\ \text{st } M^H x \le \mathbf{1} & \\ x \in \{0,1\}^{\#\omega} & \end{aligned}$$

The BLP in Corollary 175 can be tightened by adding constraints for more dimensions. This is equivalent to DefaultCDCBLP(q, v, d, k) of Definition 47 with a prescribed symmetry group H.

176 **Lemma**
Let $H \le \mathrm{P\Gamma L}(\mathbb{F}_q^v)$. There is a $(v, N, d'; k)_q$ CDC C with $H \le \mathrm{Aut}(C)$ and $d' \ge d$ of maximum cardinality iff

$$\begin{aligned}
N = \max & \sum_{U \in T_k(H)} \#(UH) x_U \\
\text{st} & \sum_{U \in T_k(H)} \#\mathcal{I}(UH, W) x_U \le \mathrm{A}_q(v-l, d; k-l) && \forall W \in T_l(H),\ 1 \le l \le k - d/2 + 1 \\
& \sum_{U \in T_k(H)} \#\mathcal{I}(UH, W) x_U \le \mathrm{A}_q(l, d; k) && \forall W \in T_l(H),\ k + d/2 - 1 \le l \le v - 1 \\
& x \in \{0,1\}^{T_k(H)}
\end{aligned}$$

using $T_i(H)$ as a transversal of $\begin{bmatrix} \mathbb{F}_q^v \\ i \end{bmatrix}$ under the operation of H for $i \in \{0, 1, \ldots, v\}$.

Let $z_{\mathrm{ILP}}(H; q, v, d, k)$ be the optimal value of the integer linear program of Lemma 176 and $z_{\mathrm{LP}}(H; q, v, d, k)$ its linear programming relaxation, i.e., the same program but with

$$x \in [0,1]^{T_k(H)} \quad \text{instead of} \quad x \in \{0,1\}^{T_k(H)}.$$

For each $U \in T_k(H)$ the constraint $x_U \le 1$ is redundant since $\mathrm{A}_q(v-l, d; k-l) = 1$ for $l = k - d/2 + 1$ and for any $U \in T_k(H)$ there is an l-dimensional $W' \le U$ and therefore a $W \in T_l(H)$ with $W' \in WH$. Hence

$$x \in [0, \infty[^{T_k(H)}$$

suffices.

In addition to $\mathrm{A}_q(v-l, d; k-l) = 1$ for $l = k - d/2 + 1$, we also have $\mathrm{A}_q(l, d; k) = 1$ for $l = k + d/2 - 1$. Hence, any x_U $(U \in T_k(H))$ may be trivially fixed to 0 if $\#\mathcal{I}(UH, W) \ge 2$ for a $W \in T_l(H)$ with $l = k - d/2 + 1$ or $l = k + d/2 - 1$.

Algorithm 7 $\mathcal{P}$ for CDCs

```
function P_CDC(H; q, v, d, k; t; κ)
Require: H ≤ PΓL(F_q^v) a subgroup, q, v, d, k the parameters of a CDC, t a time limit in seconds, κ ∈ Z_{≥0} a threshold for the code size
    if z_LP(H; q, v, d, k) < κ then
        return 0
    end if
    z ← the smallest upper bound of z_ILP(H; q, v, d, k) which is computed for t seconds
    if z < κ then
        return 0
    end if
    return 1
end function
```

The computation of the optimal value of the linear programming relaxation is much easier than the computation of the corresponding integer linear program. In fact, the branch & bound solving method for integer linear programs, cf. [Dak65], incorporates the computation of linear programs of subproblems multiple times. In particular, before the actual branch & bound may be started, it determines a global upper bound via the linear programming relaxation of the whole problem, i.e., the computation of z_{ILP} involves the computation of z_{LP} implicitly. Also the computation of z_{ILP} may be aborted, if a feasible solution with objective value at least κ is found. This can be achieved by adding the additional constraint

$$\sum_{U \in T_k(H)} \#(UH)x_U \geq \kappa$$

and setting the objective function to 0.

11.3.1 Using the remaining symmetry

We will use Lemma 24, which guarantees that we still have some symmetry to exploit in order to decrease the solving time of z_{ILP}:

The variables of $z_{\mathrm{ILP}}(H; q, v, d, k)$ are indicator variables of $X = \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} / H$ for $H \leq \mathrm{P\Gamma L}(\mathbb{F}_q^v)$. Using Lemma 24 the group $N = N_{\mathrm{P\Gamma L}(\mathbb{F}_q^v)}(H)$ is an automorphism group of X. Let now $T^N = \{T_1^N, \ldots, T_{\#T^N}^N\}$ be a transversal of N operating on X and define the BLP $z_{\mathrm{ILP}}(H; q, v, d, k; T_i^N)$ for $T_i^N \in T^N$ as the maximization problem $z_{\mathrm{ILP}}(H; q, v, d, k)$ with the additional constraint $x_U = 1$ for $\{U\} = T_k(H) \cap T_i^N$.

The correspondence is: $C = \bigcup D$ with $D \subseteq X$ is a non-empty feasible solution in $z_{\mathrm{ILP}}(H; q, v, d, k)$ iff there is an $n \in N$ and i such that $C \circ n$ is a non-empty feasible solution in $z_{\mathrm{ILP}}(H; q, v, d, k; T_i^N)$ of the same cardinality.

Assume $z_{\mathrm{ILP}}(H; q, v, d, k; T_i^N) < \kappa$ then no orbit in $T_i^N \circ N$ is subset of a $(v, \#C, d; k)_q$ CDC C with $H \leq \mathrm{Aut}(C)$ and $\#C \geq \kappa$. Hence we can fix more variables in all subproblems $z_{\mathrm{ILP}}(H; q, v, d, k; T_i^N)$ and even in $z_{\mathrm{ILP}}(H; q, v, d, k)$, i.e., $x_U = 0$ for all $U \in T_k(H) \cap (T_i^N \circ N)$ in these problems.

This implies that later solved subproblems contain less variables and hence the ordering of the computation of the subproblems is of interest. A heuristical idea is to sort the set T^N in decreasing order of orbit length of the $T_i^N \circ N$. Then, the first subproblems correspond to orbits of large size, i.e., small stabilizer due to the orbit-stabilizer theorem, cf. Lemma 22, and the latter subproblems have even more fixed variables.

To decrease the total computation time of all subproblems even further, we start all of them in parallel while we assume for $z_{\text{ILP}}(H; q, v, d, k; T_i^N)$ that all $z_{\text{ILP}}(H; q, v, d, k; T_j^N) < \kappa$ for all $1 \le j < i \le \#T_N$ integers.

11.3.2 Conjugacy classes of cyclic groups

We focus on $G = \text{GL}(\mathbb{F}_q^v)$ instead of $\text{P}\Gamma\text{L}(\mathbb{F}_q^v)$.

Any group of order p for p prime is cyclic and in particular isomorphic to C_p. The conjugacy classes of elements in G provide a starting point, but different conjugacy classes of elements may yield the same conjugacy class as subgroups.

177 Lemma
Let G be a finite group and $g, h \in G$ of the same order $o \ge 2$. Then $\langle g \rangle$ and $\langle h \rangle$ are conjugate in G iff there is an $l \in G$ with $g^i = h^l$ for an $i \in [o-1]$ such that $\text{GCD}(i, o) = 1$. If g and h are not conjugate in G, then $i \ne 1$ and in particular, if $o = 2$ then g and h are conjugate in G iff $\langle g \rangle$ and $\langle h \rangle$ are conjugate in G.

Proof
On the one hand, if $\langle g \rangle$ and $\langle h \rangle$ are conjugate in G, i.e., there is an $l \in G$ with $\langle g \rangle = \langle h \rangle^l$, we use $\langle h \rangle^l = \langle h^l \rangle$ and $\langle g \rangle = \langle h^l \rangle$ iff $g^i = h^l$ for any g^i which generates $\langle g \rangle$, i.e. $i \in [o-1]$ with $\text{GCD}(i, o) = 1$. On the other hand, if $g^i = h^l$ for an $i \in [o-1]$ such that $\text{GCD}(i, o) = 1$ then $\langle g \rangle = \langle g^i \rangle = \langle h^l \rangle = \langle h \rangle^l$. $\square$

178 Example
$g = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \text{GL}(\mathbb{F}_2^3)$ has order 7 and the characteristic polynomial $x^3 + x + 1$. Note that conjugate matrices, which are sometimes called *similar* in the context of the GL, have the same characteristic polynomial. Although g is not conjugate to $g^3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, which has order 7 and the characteristic polynomial $x^3 + x^2 + 1$, both are trivially conjugate as subgroups, i.e., $\langle g \rangle = \langle g^3 \rangle^{I_3}$.

The conjugacy classes of elements in the $\text{GL}(\mathbb{F}_q^v)$ may be computed with the Frobenius normal form [BKN16].

11.3.3 Conjugation test with the dimension of eigenspaces

The expensive test, whether a group contains a cyclic subgroup or an element up to conjugation, may be replaced by the following, rather easy, criterion in the $\mathrm{GL}(\mathbb{F}_q^v)$.

For a square matrix $M \in \mathbb{F}_q^{v \times v}$ and $\lambda \in \mathbb{F}_q$, we define the subspace $\mathrm{Eig}(M, \lambda) = \ker(M - \lambda I_v) = \{x \in \mathbb{F}_q^v \mid xM = \lambda x\}$, which is exactly the eigenspace of λ if λ is an eigenvector and else it is the subspace $\{0\} \leq \mathbb{F}_q^v$.

179 **Lemma**
Let $M \in \mathrm{GL}(\mathbb{F}_q^v)$ and $\lambda \in \mathbb{F}_q$. Then:

1. $\mathrm{Eig}(M, \lambda) \leq \mathrm{Eig}(M^i, \lambda^i)$ for all $i \in \mathbb{Z}_{\geq 1}$.
2. $\mathrm{Eig}(M^i, \lambda^i) \leq \mathrm{Eig}(M, \lambda^{si})$ for all $i \in \mathbb{Z}_{\geq 1}$ such that there are $s, t \in \mathbb{Z}$ with $s \cdot i + t \cdot \mathrm{ord}(M) = 1$.
3. $\mathrm{Eig}(M, \lambda) \cdot N = \mathrm{Eig}(M^N, \lambda)$ for any $N \in \mathrm{GL}(\mathbb{F}_q^v)$.

Proof

1. If $x \in \mathrm{Eig}(M, \lambda)$ then $xM = \lambda x \Rightarrow xM^i = \lambda^i x$ and in turn $x \in \mathrm{Eig}(M^i, \lambda^i)$.
2. By Lemma 33 there are $s, t \in \mathbb{Z}$ with $s \cdot i + t \cdot \mathrm{ord}(M) = 1$ iff $\mathrm{GCD}(i, \mathrm{ord}(M)) = 1$. If $x \in \mathrm{Eig}(M^i, \lambda^i)$ then $xM^i = \lambda^i x \Rightarrow xM^{si} = \lambda^{si} x$. Since $I_v = M^{t \cdot \mathrm{ord}(M)}$ this implies $xM^{si + t \cdot \mathrm{ord}(M)} = \lambda^{si} x \Leftrightarrow xM = \lambda^{si} x$.
3. $$\begin{aligned} \mathrm{Eig}(M^N, \lambda) &= \{x \in \mathbb{F}_q^v \mid xN^{-1}MN = \lambda x\} \\ &= \{(xN^{-1})N \in \mathbb{F}_q^v \mid (xN^{-1})M = \lambda(xN^{-1})\} \\ &= \{y \in \mathbb{F}_q^v \mid yM = \lambda y\}N = \mathrm{Eig}(M, \lambda) \cdot N \end{aligned}$$ □

In particular for $M \in \mathrm{GL}(\mathbb{F}_q^v)$ the property $\mathrm{Eig}(M, 1)$ is equal for all generators of $\langle M \rangle$, which allows to define $\mathrm{Eig}(\langle M \rangle, 1) = \mathrm{Eig}(M, 1)$. Using this definition with an $N \in \mathrm{GL}(\mathbb{F}_q^v)$, we have $\mathrm{Eig}(\langle M \rangle^N, 1) = \mathrm{Eig}(\langle M^N \rangle, 1) = \mathrm{Eig}(M^N, 1) = \mathrm{Eig}(M, 1) \cdot N$ and although these subspaces may differ, their dimension is invariant. This in turn allows the definition $\dim(\mathrm{Eig}(\langle M \rangle^G, 1)) = \dim(\mathrm{Eig}(M, 1))$.

The criterion to determine whether a group $U \leq \mathrm{GL}(\mathbb{F}_q^v)$ contains a specific cyclic subgroup up to conjugacy is now as follows. Assume, we have a transversal $\{T_1, \ldots, T_n\}$ of conjugacy classes of cyclic groups of order o such that $t_i = \dim(\mathrm{Eig}(T_i, 1))$ for all $i \in [n]$ and there is a $j \in [n]$ such that $t_i \neq t_j$ for all $i \in [n] \setminus \{j\}$. Then U contains a conjugate of T_j iff U contains a matrix M with $\mathrm{ord}(M) = o$ and $\dim(\mathrm{Eig}(M, 1)) = t_j$.

11.4 Application for $(7, N, 4; 3)_2$ CDCs

The described method is applied to $(7, N, 4; 3)_2$ CDCs with $\kappa = 329$, but the technique also yielded results for $\kappa = 330$ and $\kappa = 334$. $G = \mathrm{GL}(\mathbb{F}_2^7)$ is of size $163\,849\,992\,929\,280 = 2^{21} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31 \cdot 127$. Previously, [BKN16] applied similar ideas to the q-Steiner system case $S(2, 3, 7)_2$ and lists some subgroups up to conjugacy that we use also here.

In this context, we write that a subgroup U or conjugacy class of subgroups W of the $\mathrm{GL}(\mathbb{F}_2^7)$ is *excluded*, if the prescription of U or a representative R of W has $\mathrm{A}_2(7, 4; 3; U) < \kappa$ or $\mathrm{A}_2(7, 4; 3; R) < \kappa$, respectively.

It does not matter how we order the prime factors 2, 3, 5, 7, 31, and 127.

$p \in \{5, 31, 127\}$

The primes 5, 31, and 127 have in common that the largest prime power dividing $\#G$ is 5^1, 31^1, and 127^1. Sylow's theorem (Theorem 16) states that the Sylow p-subgroup is unique up to conjugation for $p \in \{5, 31, 127\}$.

The Sylow 127-subgroup in G yields codes of maximum size $N \leq 254$ [KK08a; Tho87]. The Sylow 31-subgroup S_{31} in G yields $z_{\mathrm{ILP}}(S_{31}; 2, 7, 4, 3) = 279$. Both computations took merely seconds.

The Sylow 5-subgroup S_5 in G has one fixed plane and 7 fixed lines. Unfortunately, the solving process of z_{ILP} does not admit an upper bound which is better than 381 in 18 hours and was aborted. Hence, S_5 remains in the final list, cf. $G_{5,1}$ in the appendix.

$p \in \{3, 7\}$

Groups of order 7 Since 7 is prime, all groups of order 7 have to be cyclic.

There are three conjugacy classes of subgroups of G of order 7. One of them, H_7^G, has $z_{\mathrm{ILP}}(H_7; 2, 7, 4, 3) \leq 296$ after 60 seconds and the other two groups do not admit an upper bound of z_{ILP} which is better than 381 in 18 hours and were aborted.

Hence, two conjugacy classes of order 7 remain. Representatives are depicted as $G_{7,1}$ and $G_{7,2}$ in the appendix.

Groups of order 49 Since the up to conjugacy unique Sylow 7-group S_{49} in G has order 7^2 and contains a conjugate of H_7, the monotonicity implies $z_{\mathrm{ILP}}(S_{49}; 2, 7, 4, 3) \leq z_{\mathrm{ILP}}(H_7; 2, 7, 4, 3) \leq 296$.

Groups of order 3 There are three conjugacy classes of groups of order three in G. One of them, H_3^G, has $z_{\mathrm{ILP}}(H_3; 2, 7, 4, 3) \leq 255$ with the argument in Lemma 167 or by a computation after 60 seconds. We have $\dim(\mathrm{Eig}(H_3^G, 1)) = 5$. The other two groups do not admit an upper bound of z_{ILP} which is better than 381 in 18 hours and were aborted. They have $\dim(\mathrm{Eig}(\cdot, 1)) \in \{1, 3\}$.

Groups of order 9 There are four conjugacy classes of groups of order 9 in G, which can e.g. be computed with `SubgroupClasses(GL(7,2):OrderEqual:=9);` in `Magma` [BCP97]. Two of them contain a conjugate of H_3 and hence cannot be automorphism group of $(7, N, 4; 3)_2$ CDCs with $N > 255$ and the other two groups do not admit an upper bound of z_{ILP} which is better than 381 in 18 hours and were aborted. They have abstract type C_9 and $C_3 \times C_3$.

Groups of order 27 Analogously, there are three conjugacy classes of groups of order 27 in G. One of them contains a conjugate to H_3, the other two have an upper bound of z_{ILP} of at most 309. These two computations took merely minutes.

Groups of order 81 The Sylow 3-subgroup S_{81} of G has order 81 and since it contains a conjugate of H_3 we have by monotonicity $z_{\text{ILP}}(S_{81}; 2, 7, 4, 3) \le z_{\text{ILP}}(H_3; 2, 7, 4, 3) \le 255$.

Hence, two conjugacy classes of order 3 and two conjugacy classes of order 9 remain. Representatives for them are depicted as $G_{3,1}$, $G_{3,2}$, $G_{9,1}$, and $G_{9,2}$ in the appendix.

$p = 2$

Groups of order 2 There are three conjugacy classes of groups in G of order 2, H_2^G, $H_2'^G$, and $H_2''^G$. Two of them can be excluded straight forward in merely seconds of computation time or by theoretical arguments via Lemma 159, cf. Example 160, and Lemma 166: $z_{\text{ILP}}(H_2; 2, 7, 4, 3) \le 106$ with $\dim(\text{Eig}(H_2, 1)) = 6$ and $z_{\text{ILP}}(H_2'; 2, 7, 4, 3) \le 298$ with $\dim(\text{Eig}(H_2', 1)) = 5$. Although the computation of $z_{\text{ILP}}(H_2''; 2, 7, 4, 3)$ does not admit an upper bound of z_{ILP} which is better than 381 in 18 hours and was aborted, we have $\dim(\text{Eig}(H_2'', 1)) = 4$.

Hence, the test whether a group contains H_2 or H_2' up to conjugacy can be replaced by the consideration of the dimension of eigenspaces, as described in Section 11.3.3.

Groups of order 4 There are 42 conjugacy classes of order 4 in G. 34 of them contain conjugates of H_2 or H_2'. One additional conjugacy class H_4^G can be excluded, since $z_{\text{ILP}}(H_4; 2, 7, 4, 3) \le 327$ in 18 hours of computation time. Prescribing the remaining seven conjugacy classes, the upper bound of z_{ILP} could not be improved to at most 328 in 18 hours.

Groups of order 8 There are 867 conjugacy classes of subgroups of G of order 8. All but 38 contain a conjugate of H_2 or H_2'. 27 of these 38 conjugacy classes are then excluded via a computation of z_{ILP} in at most 14 hours. The remaining 11 conjugacy classes of groups of order 8 could not be excluded in 14 hours.

Groups of order 16 The conjugacy classes of order 16 in G cannot be computed any more directly with built-in commands in `Magma` due to time and space restrictions, which makes the application of Lemma 172 necessary. Any group of order 16 contains a subgroup of order 8 by Sylow's theorem (Theorem 16) and any subgroup of index two is a normal subgroup (Corollary 26). Hence we can apply Lemma 172 with $n = 8$ and $u = 16$ and extend the remaining 11 subgroups of the last paragraph. This yields 50 conjugacy classes of subgroups of G of order 16 that do not contain a conjugate of H_2 or H_2'. Solving z_{ILP} for these 50 cases shows that the maximum value of 329 is attained exactly once in mostly minutes and at most 8 hours each.

This group is of abstract type $(C_4 \times C_2) \rtimes C_2$, cf. $G_{16,1}$ in the appendix, and a slight modification of a maximum code having $G_{16,1}$ as automorphism group yields the up to now largest code with the parameters $(7, 333, 4; 3)_2$.

There are 12 CDCs up to isomorphism under the $N_G(G_{16,1})$ of type $(7, 329, 4; 3; G_{16,1})_2$. They all have the same orbit structure $1^1 2^2 4^9 8^8 16^{14}$ and each of these isomorphism classes of codes contain 16 CDCs. Hence, the BLP in Lemma 176 has $16 \cdot 12 = 192$ maximum solutions.

Groups of order 2^i with $i \geq 5$ Applying Lemma 172 to $G_{16,1}$, we found the group H_{32} of order 32 and a code of type $(7, 327, 4; 3; H_{32})_2$. Applying again Lemma 172 to H_{32} yields the group H_{64} of order 64 and a code of type $(7, 317, 4; 3; H_{64})_2$.

In particular, any subgroup H of G of order 2^i with $i \geq 5$ contains by Sylow's theorem (Theorem 16) at least one subgroup of order 32 and hence any $(7, N, 4; 3; H)_2$ CDC has $N \leq 327$.

Therefore the 20 remaining representatives of subgroups of order 2^j $(j \geq 1)$ of G are $G_{2,1}$, $G_{4,1}$, ..., $G_{4,7}$, $G_{8,1}$, ..., $G_{8,11}$, and $G_{16,1}$ in the appendix.

Composite order

Any subgroup of G, whose order does not divide $2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040$ contains by Theorem 16 at least one subgroup of prime power order which cannot be automorphism group of a $(7, N, 4; 3)_2$ CDC with $N \geq 329$, as worked out in the last paragraphs. Therefore, we only have to consider subgroups of $G = \mathrm{GL}(\mathbb{F}_2^7)$, whose order divides 5040 and is neither 1 nor a prime power.

Hence, only the 51 orders in $O = \{6, 10, 12, 14, 15, 18, 20, 21, 24, 28, 30, 35, 36, 40, 42, 45, 48, 56, 60, 63, 70, 72, 80, 84, 90, 105, 112, 120, 126, 140, 144, 168, 180, 210, 240, 252, 280, 315, 336, 360, 420, 504, 560, 630, 720, 840, 1008, 1260, 1680, 2520, 5040\}$ remain.

Hall's theorem, cf. Theorem 21 and the Small Groups Library, see Page 30 will be applied. The non-solvable numbers in O are $\{60, 120, 168, 180, 240, 336, 360, 420, 504, 720, 840, 1008, 1260, 1680, 2520, 5040\}$ and the Small Groups Library contains no data for the orders $\{2520, 5040\}$.

The implication of Hall's theorem in this application may be represented by a directed graph, cf. Figure 10a, whose vertices are the solvable numbers in O and there is an arc from a to b iff $a \mid b$, $\mathrm{GCD}(a, b/a) = 1$, and there is no c such that (a, c) and (c, b) are arcs, i.e., we deliberately remove the transitive arcs.

Similarly, the implication of the Small Groups Library in this application may also be represented by a directed graph, cf. Figure 10b, whose vertices are orders in O, for which the Small Groups Library contains all abstract types of groups, and there is an arc from a to b iff any group of order b contains at least one subgroup of order a and there is no c such that (a, c) and (c, b) are arcs, i.e., we remove again the transitive arcs. After inserting the transitive arcs, the graph in Figure 10b contains the graph in Figure 10a as subgraph.

Let o be the label of a vertex in this graph. Then the exclusion of all subgroups of order o in G implies that all subgroups of an order which is the label of an outgoing vertex of the vertex o are excluded as well and this may cascade, since we omitted the transitive arcs.

First, we consider the conjugacy classes of subgroups of G with an order in $\{6, 10, 12, 14, 15, 21, 35, 56, 80, 2520, 5040\}$, since they are vertices in the graph without an ingoing arc in Figure 10, i.e., neither Hall's theorem nor the Small Groups Library is able to provide the information to exclude them on the level of only considering orders.

6 There are 12 subgroups of order 6 up to conjugacy in G. 9 of them contain a conjugate of H_2, H_2' or H_3. The 3 remaining groups cannot be excluded in 18 hours of computation time.

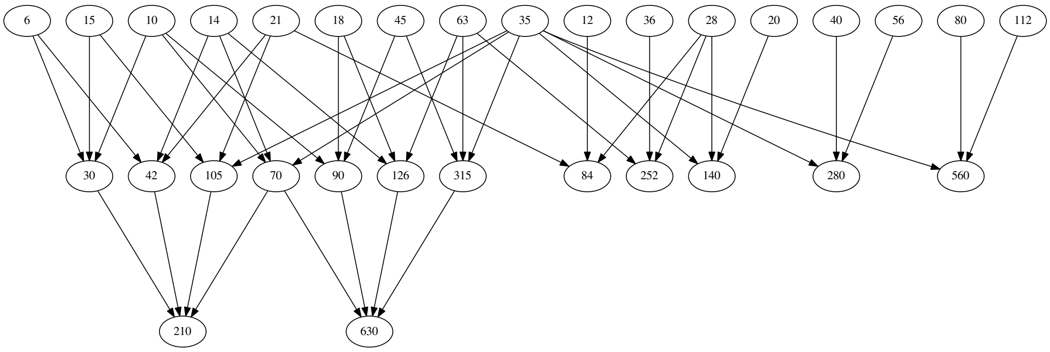
10 There are 3 subgroups of order 10 up to conjugacy in G. 2 of them contain a conjugate of H_2 or H_2'. The remaining group has its z_{ILP} value upper bounded by 306 in about 6 hours. By applying Hall's theorem and the Small Groups Library, e.g. via the graph in Figure 10, the exclusion of order 10 also excludes the orders in $\{20, 30, 40, 60, 70, 90, 120, 140, 180, 210, 280, 360, 420, 630, 840, 1260\}$ by monotonicity.

12 There are 96 subgroups of order 12 up to conjugacy in G. 80 of them contain a conjugate of H_2, H_2' or H_3. All but one group could be excluded computationally in days, this remaining group is of abstract type $C_3 \rtimes C_4$. The solving process of z_{ILP} for this remaining group was aborted after 9 days.

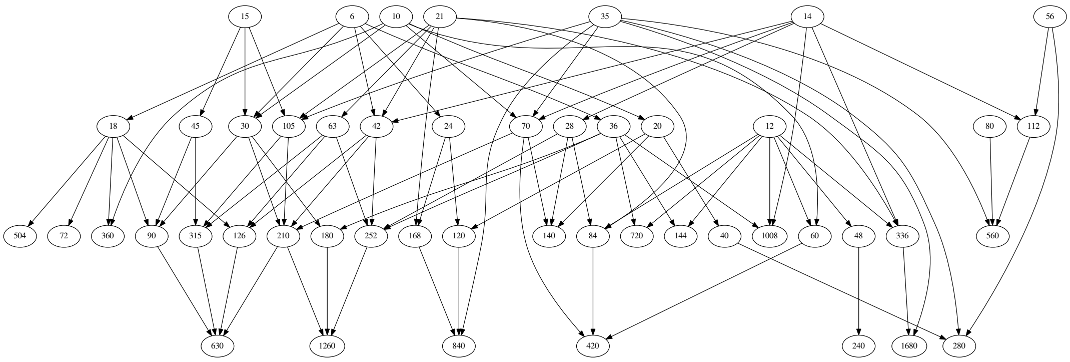
14 There are 4 subgroups of order 14 up to conjugacy in G. 2 of them contain a conjugate of H_2, H_2' or H_7. One, H_{14}, has its z_{ILP} upper bounded by 301 after 60 seconds and the other, H_{14}' is of abstract type C_{14} and its z_{ILP} is at most 332. The computation of the upper bound of $z_{\mathrm{ILP}}(H_{14}'; 2, 7, 4, 3)$ was difficult and the technique described in Section 11.3.1 was applied. The orbit type is $1^1 2^4 7^{30} 14^{828}$ and after removing the trivially forbidden orbits $1^1 2^4 7^{28} 14^{632}$. The normalizer $N_G(H_{14}')$ has order 168 and the normalizer-orbit type is $1^4 4^{13} 6^2 12^{50}$, making a total of 66 subproblems. All subproblems could be solved in about 1 day.

15 There are 3 subgroups of order 15 up to conjugacy in G. One of them contains a conjugate of H_3. The remaining groups could be excluded computationally in days. By considering Figure 10, the exclusion of order 15 implies the exclusion for all orders in $\{30, 45, 90, 105, 180, 210, 315, 630, 1260\}$.

21 There are 8 subgroups of order 21 up to conjugacy in G. 5 of them contain a conjugate of H_3 or H_7. The remaining groups could be excluded computationally in at most 2 hours each. By considering again Figure 10, the exclusion of order



(a) A directed graph which shows the implication of Hall's theorem.



(b) A directed graph which shows the implication of the Small Groups Library. After inserting all transitive arcs, it contains the graph in Figure 10a as subgraph.

Figure 10: Directed graphs which shows the implication of Hall's theorem and the Small Groups Library. The exclusion of any subgroup of order o excludes any subgroup whose orders are the labels for the outgoing arcs of vertex labeled o.

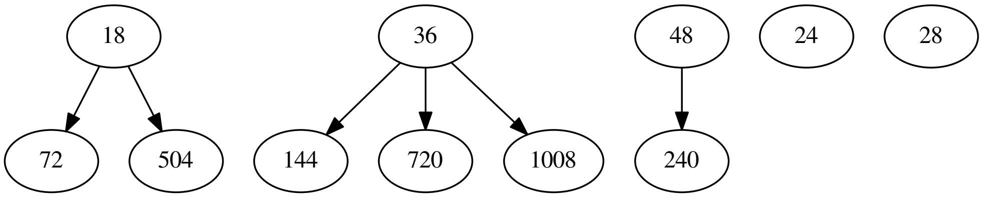


Figure 11: The subgraph of the graph in Figure 10b with vertices with labels in $\{18, 24, 28, 36, 48, 72, 144, 240, 504, 720, 1008\}$.

21 implies the exclusion for all orders in $\{42, 63, 84, 105, 126, 168, 210, 252, 315, 336, 420, 630, 840, 1260, 1680\}$.

35 There is one subgroup of order 35 up to conjugacy in G and it contains a conjugate of H_7. This implies the exclusion for all orders in $\{70, 105, 140, 210, 280, 315, 420, 560, 630, 840, 1260, 1680\}$.

56 There are 38 subgroups of order 56 up to conjugacy in G. 26 of them contain a conjugate of H_2, H_2' or H_7. The remaining 12 groups could be excluded computationally in a few seconds. This implies the exclusion of the orders in $\{112, 280, 560\}$.

80 Referring to the Small Groups Library each group of order 80 contains a subgroup of order 10 or a subgroup of abstract type $C_2 \times C_2 \times C_2 \times C_2$, i.e., order 16, and each subgroup of G of this abstract type cannot be automorphism group of $(7, N, 4; 3)_2$ CDCs with $N \geq 329$. This additionally excludes the order 560.

2520 There are 7 subgroups of order 2520 up to conjugacy in G. All contain a conjugate of H_2, H_2', H_3 or H_7.

5040 There are 4 subgroups of order 5040 up to conjugacy in G. All contain a conjugate of H_2, H_2', H_3 or H_7. None of them is solvable.

The remaining groups are denoted $G_{6,1}$, $G_{6,2}$, $G_{6,3}$, $G_{12,1}$, and $G_{14,1}$ in the appendix.

All these orders, except for 80, may be processed in parallel since no information is shared in between. Only order 80 depends on the previously performed exclusion of order 10 and the excluded abstract types of order 16.

After this iteration, only the 11 orders in $\{18, 24, 28, 36, 48, 72, 144, 240, 504, 720, 1008\}$ remain to be taken into consideration, since the orders 6, 12, and 14 could not be excluded completely.

Note that the exclusion of order 18 implies the exclusion of the orders 72 and 504, and similarly, the exclusion of order 36 implies the exclusion of the orders 144, 720, and 1008, while the exclusion of order 48 implies the exclusion of order 240 by monotonicity, cf. Figure 11.

18 There are 16 subgroups of order 18 up to conjugacy in G. 13 of them contain a conjugate of H_2, H_2' or H_3. The remaining groups could be excluded computationally in at most 5 minutes each.

24 There are 525 subgroups of order 24 up to conjugacy in G. 488 of them contain a conjugate of H_2, H_2' or H_3. The abstract types of these remaining groups are: 14 times S_4, 19 times $C_2 \times A_4$, 2 times $\mathrm{SL}(\mathbb{F}_3^2)$, and 2 times $(C_6 \times C_2) \rtimes C_2$. All but the two groups of abstract type $\mathrm{SL}(\mathbb{F}_3^2)$ contain an excluded C_{12}, $C_6 \times C_2$, or A_4. The remaining two groups of abstract type $\mathrm{SL}(\mathbb{F}_3^2)$ could be excluded computationally in at most 2 minutes.

28 There are 9 subgroups of order 28 up to conjugacy in G. 8 of them contain a conjugate of H_2, H_2' or H_7. The remaining group is of abstract type $C_{14} \times C_2$ and could be excluded computationally in less than 1 minute.

36 There are 61 subgroups of order 36 up to conjugacy in G. 59 of them contain a conjugate of H_2, H_2' or H_3. The remaining groups are both of abstract type $C_3 \times A_4$ and in particular, they contain an excluded A_4.

48 Referring to the Small Groups Library, each group of order 48 contains a subgroup of order 24 or a subgroup of abstract type A_4.

Since all of these conjugacy classes of subgroups could be excluded, the whole subspace lattice of $\mathrm{GL}(\mathbb{F}_2^7)$ was exhaustively searched for subgroups that may be automorphism groups for a $(7, N, 4; 3)_2$ CDC with $N \geq 329$.

11.5 Local search with BLP techniques

An advantage of the automorphism search strategy in Section 11.4 is that we get large codes with large automorphism groups as a byproduct. In this case, we found a $(7, 329, 4; 3; G_{16,1})_2$ CDC C_{329}, cf. $G_{16,1}$ in the appendix, Chapter 14.1.1 and the paragraph "Groups of order 16" on Page 172, which we will modify in this section to get larger codes.

For the sake of a general explanation, let C_{start} be a $(v, N, d; k; G)_q$ CDC and $\eta \in \{0, 1, \ldots, N\}$. Equipping the BLP in Lemma 176 for $H \leq G$ with the additional constraint

$$\sum_{U \in T_k(H) \cap C_{\text{start}}} \#(UH) x_U \geq \eta$$

allows to use BLP solvers to search for large codes in the neighborhood of C_{start}. The parameter η controls how "near" our starting code C_{start} and the computed code C are, i.e., $\#(C \cap C_{\text{start}}) \geq \eta$. Any feasible solution of this modified BLP corresponds to a $(v, N', d'; k; H')_q$ CDC C' with $\eta \leq N'$, $d \leq d'$, and $H \leq H'$.

Applying this local search strategy to $G = G_{16,1}$, a $(7, 329, 4; 3; G_{16,1})_2$ CDC C_{start}, and $H = \langle I_7 \rangle$ with $\eta = 300$ yields a $(7, 333, 4; 3)_2$ CDC C' of whom further investigation shows that $\operatorname{Aut}(C')$ is conjugate to $G_{4,6}$ in the $\mathrm{GL}(\mathbb{F}_2^7)$, cf. Appendix 14.1.1. Hence, choosing $H \le G_{16,1}$ as a conjugate of $G_{4,6}$ in $\mathrm{GL}(\mathbb{F}_2^7)$ suffices to find this code by removing two fixed planes, i.e., creating a temporary CDC of cardinality 325, and extending it by two other fixed planes and two orbits of size two. The code C'' depicted in Section 14.1.2 has $\operatorname{Aut}(C'') = G_{4,6}$, it is in the same orbit as C'.

Moreover, this $(7, 333, 4; 3)_2$ CDC contains 35 planes which are incident to the same hyperplane. By removing these planes and hyperplane, we get a set of 298 planes in the affine geometry $\mathrm{AG}(6, 2)$ which mutually intersect in at most a point, cf. [Zum16].

11.6 An implementation in `Magma` and examples

Here, we discuss some applications of the source code in Section 14.3 in the appendix. Essentially, we implement the pseudo code of Section 11.2.1, which uses an arbitrary finite group G and a function $\mathcal{P} : \{A \le G\} \to \{0, 1\}$ which is monotonically decreasing, i.e., $\mathcal{P}(A) \ge \mathcal{P}(B)$ for all $A \le B$, and invariant under conjugation, i.e., $\mathcal{P}(A^g) = \mathcal{P}(A)$ for all $g \in G$. If G is some subgroup of a general linear group, we add specific details described in Section 11.3.3.

Moreover, Section 14.3 in the appendix lists additional code that implements functionality in the context of subspace coding and CDCs and in particular DefaultCDCBLP, cf. Definition 47.

It also provides functionality that solves a BLP automatically from `Magma` [BCP97] using `Gurobi` [Gur16] via an adapter in `Python` [Ros95]. This is used in a prototype of an evaluation function $\mathcal{P}'$ which can be specialized to $\mathcal{P}$ depending on different settings.

Automorphisms of $(4, 5, 4; 2)_2$ CDCs

There is only one isomorphism class of $(4, 5, 4; 2)_2$ CDCs and we denote a representative as C. The automorphism group of C is isomorphic to $\mathrm{GL}(\mathbb{F}_{2^2}^{4/2}) \times \operatorname{Aut}(\mathbb{F}_{2^2}/\mathbb{F}_2)$ of order $(4^2 - 1) \cdot (4^2 - 4) \cdot 2 = 360$, cf. [Tra13c, Theorem 11 and Corollary 12] and [Tra13b, Theorem 4.16 and Theorem 4.17].

The following call of the algorithm searches all subgroups of $G = \mathrm{GL}(\mathbb{F}_2^4)$ for conjugacy classes U^G such that there is a $(4, 5, 4; 2; U)_2$ CDC. Its result is shown in Figure 12. The overall computations took a few seconds.

```
DefaultCDCBLP("defcdc_2442.lp", 2,4,4,2 : rhs:=[1,1,1], lb:=5,
    replaceme:="replaceme");
write_python_helper("adapter.py", "defcdc_2442.lp", "add_", "
    replaceme");
myeval := func<U_idx | eval_DefaultCDCBLP(2,4,4,2,U_idx[1],100,"
    sg" cat IntegerToString(U_idx[2]),"add_",U_idx[2],"adapter.
    py") >;
sgc := SearchSubgroupLattice(GL(4,2), myeval);
```

```
L := PostProcess_PossibleConjugayClassesSubgroupsLattice(GL(4,2)
    ,sgc);
PrintSubgroupLatticeAsDigraph(sgc,L);
```

Listing 1: Using the algorithm for $(4, 5, 4; 2)_2$ CDCs

Although the $\mathrm{GL}(\mathbb{F}_{2^2}^{4/2}) \times \mathrm{Aut}(\mathbb{F}_{2^2}/\mathbb{F}_2) \cong C_3 \times S_5$ has 44 subgroups up to conjugacy, the algorithm and Figure 12 list only 37, since multiple groups are conjugate under G.

Automorphisms of $(5, 9, 4; 2)_2$ CDCs

There are four isomorphism classes of $(5, 9, 4; 2)_2$ CDCs and their automorphism groups are isomorphic to $A_4 \times C_2$, C_6, or S_3, cf. [GSS00, Theorem 5.1].

The following call of the algorithm searches all subgroups of $G = \mathrm{GL}(\mathbb{F}_2^5)$ for conjugacy classes U^G such that there is a $(5, 9, 4; 2; U)_2$ CDC. Its result is shown in Figure 13. The overall computations took a few seconds.

```
DefaultCDCBLP("defcdc_2542.lp", 2,5,4,2 : rhs:=[1,1,1,5], lb:=9,
     replaceme:="replaceme");
write_python_helper("adapter.py", "defcdc_2542.lp", "add_", "
    replaceme");
myeval := func<U_idx | eval_DefaultCDCBLP(2,5,4,2,U_idx[1],100,"
    sg" cat IntegerToString(U_idx[2]),"add_",U_idx[2],"adapter.
    py") >;
sgc := SearchSubgroupLattice(GL(5,2), myeval);
L := PostProcess_PossibleConjugayClassesSubgroupsLattice(GL(5,2)
    ,sgc);
PrintSubgroupLatticeAsDigraph(sgc,L);
```

Listing 2: Using the algorithm for $(5, 9, 4; 2)_2$ CDCs

Automorphisms of $(7, N, 4; 3)_2$ CDCs with $329 \le N$

We can also apply our algorithm to the same setting as in Section 11.4 to get automatically a superset of cardinality 47 of the manually reasoned subgroup classes. Here, we choose the timeout for the evaluation function to be 600 seconds. The first part of the algorithm involving groups of prime power took about 11 hours wall-time and the second part involving composite group orders took additionally 3 hours wall-time. About 6 hours were used for the ascending step from groups of order 4 to groups of order 8. To be specific, the test if two subgroups of order 8 are conjugate is the expensive operation. The evaluation function was executed 147 times and took 45 times 600 seconds and one time 7 seconds if its value is 1 and in the remaining 101 cases it took less than 1 hour combined. Note that the evaluation function was not called for $\langle\rangle \le \mathrm{GL}(\mathbb{F}_2^7)$.

Obviously, the groups that the algorithm returned may be used as a starting point for more elaborate exclusion methods to retrieve the same result as Theorem 170.

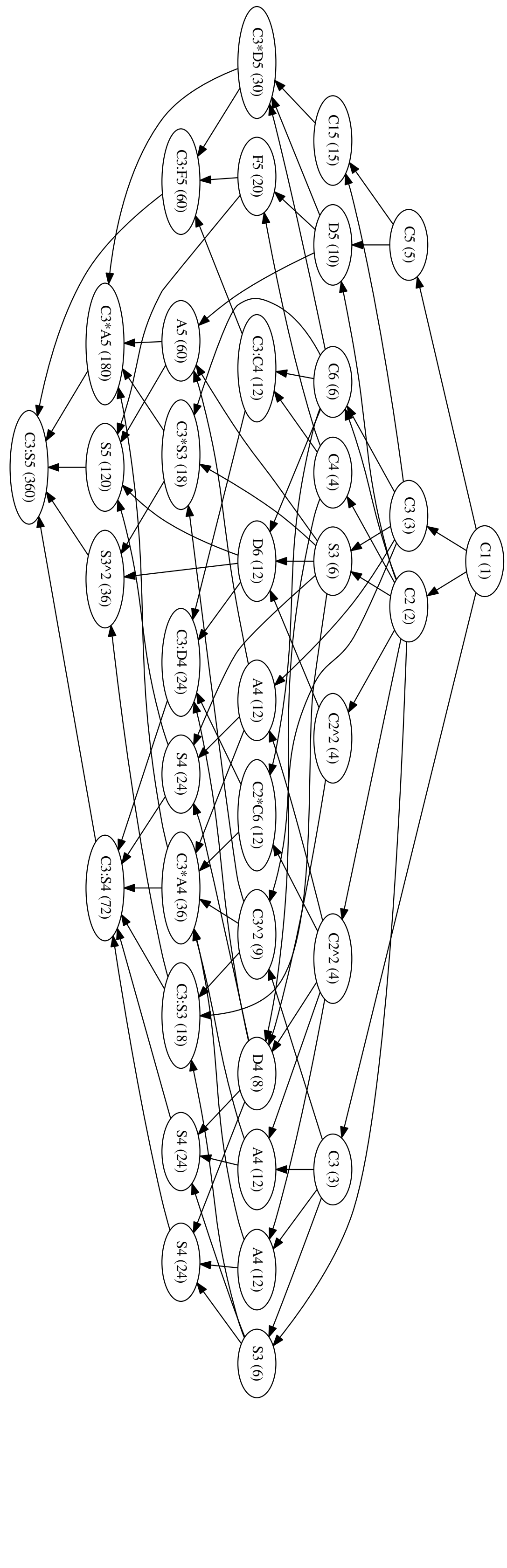


Figure 12: Output of the code of Listing 1. Any label shows the abstract type and the order in brackets. An arrow means that a group is subgroup up to conjugacy.

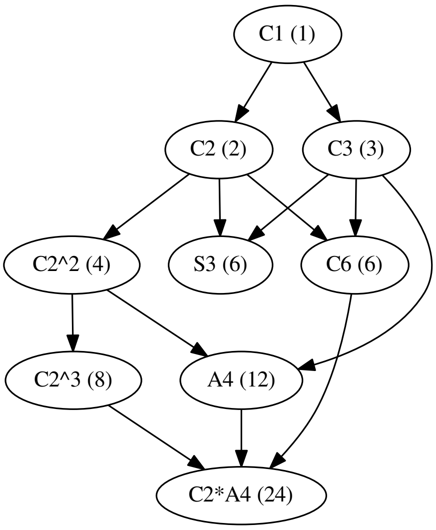


Figure 13: Output of the code of Listing 2. Any label shows the abstract type and the order in brackets. An arrow means that a group is subgroup up to conjugacy.

```
DefaultCDCBLP("defcdc_2743.lp", 2,7,4,3 : lb:=329, replaceme:="
    replaceme");
write_python_helper("adapter.py", "defcdc_2743.lp", "add_", "
    replaceme");
myeval := func<U_idx | eval_DefaultCDCBLP(2,7,4,3,U_idx[1],600,"
    sg" cat IntegerToString(U_idx[2]),"add_",U_idx[2],"adapter.
    py") >;
sgc := SearchSubgroupLattice(GL(7,2), myeval);
L := PostProcess_PossibleConjugayClassesSubgroupsLattice(GL(7,2)
    ,sgc);
PrintSubgroupLatticeAsDigraph(sgc,L);
```

Listing 3: Using the algorithm for $(7, N, 4; 3)_2$ CDCs with $329 \leq N$

$2-(7,3,2)_2$ subspace packing and covering designs

The BLP in the evaluation function for CDCs of Lemma 176 may slightly be changed to only use constraints with $l = t$ and right hand side $\leq \lambda$ to allow the exclusion of automorphisms of simple $t-(v,k,\lambda)_q$ subspace packing designs. As a byproduct, feasible solutions of the BLP which is solved in the evaluation function are subspace packing designs.

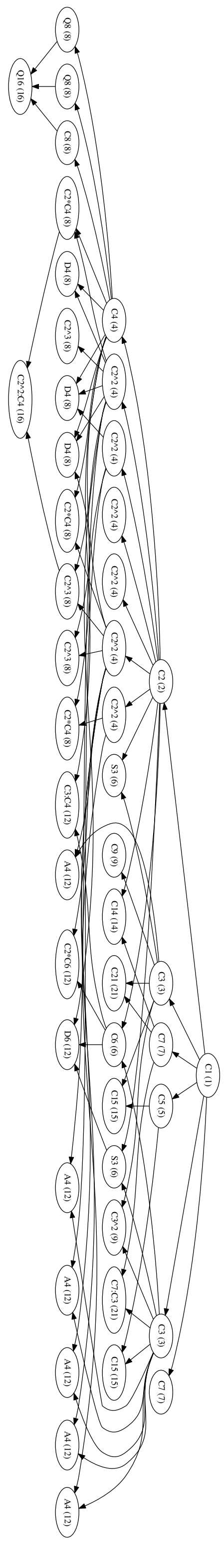


Figure 14: Output of the code of Listing 3. Any label shows the abstract type and the order in brackets. An arrow means that a group is subgroup up to conjugacy.

```
DefaultCDCBLP("defpackingdesign_2743.lp", 2,7,4,3 : rhs
    :=[0,2,0,0,0,0], lb:=741, replaceme:="replaceme");
write_python_helper("adapter.py", "defpackingdesign_2743.lp", "
    add_", "replaceme");
myeval := func<U_idx | eval_DefaultCDCBLP(2,7,4,3,U_idx[1],100,"
    sg" cat IntegerToString(U_idx[2]),"add_",U_idx[2],"adapter.
    py") >;
sgc := SearchSubgroupLattice(GL(7,2), myeval);
```

Listing 4: Using the algorithm to find large simple $2-(7,3,2)_2$ subspace packing designs

We did not perform a complete search of the subgroup lattice with the code in Listing 4, since too many groups of order 8 could not be excluded and hence it was computationally infeasible to ascend to all necessary subgroups of order 16. As an intermediate result of the solving proceess, we found a group of order 27, i.e.,

$$U = \left\langle \begin{pmatrix} 1&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&1&1&0&0 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&0&1&1&0 \\ 0&0&0&1&0&1&1 \\ 0&0&1&0&0&0&0 \\ 1&1&0&0&1&0&1 \\ 1&0&0&1&0&1&0 \\ 1&0&0&0&1&0&1 \\ 0&1&0&1&0&1&0 \end{pmatrix} \right\rangle,$$

which yields a simple $2-(7,3,2)_2$ subspace packing designs of cardinality 741. This attains the maximum cardinality for all simple $2-(7,3,2)_2$ packing designs with prescribed automorphism group U and the computation took about 30 seconds. The upper bound without prescribed automorphisms is $381 \cdot 2 = 762$. U is a Heisenberg group and the orbits of the subspace packing designs have the orders $3^4 9^9 27^{24}$.

Since this simple $2-(7,3,2)_2$ subspace packing design of size 741 is close to the upper bound of 762 we used U also in the search for good simple $2-(7,3,2)_2$ subspace covering designs. Modifying the BLP to a minimization problem, such that all inequalities are "≥ 2" instead of "≤ 2" and prescribing U yields a simple $2-(7,3,2)_2$ subspace covering design of size 783 and orbits under U of sizes $9^{12}27^{25}$. This also attains the minimum cardinality for all simple $2-(7,3,2)_2$ covering designs with prescribed automorphism group U and the computation took about 5 minutes. Any simple $2-(7,3,2)_2$ subspace covering design has size at least $2 \cdot 381 = 762$ and hence, this is again optimal up to 21 elements.

Applied to simple $2-(7,3,2)_2$ subspace designs, the algorithm computes a list L of 75 subgroups of $\mathrm{GL}(\mathbb{F}_2^7)$ such that all conjugacy classes of subgroups which do not have a representative in this list cannot be automorphism group of such a subspace design. The orders of the groups in L are in $\{1,2,4,7,8,14,16\}$.

Starting with the subspace packing design of size 741, the strategy of Section 11.5 with $H = \langle\rangle$ and $\eta = 730$ was not capable of increasing its cardinality.

12 $(2k, N, 2k-2; k)_q$ CDCs with $q^{2k}+1 \le N$

The only three cases in which the values of $\mathrm{A}_q(v, d; k)$ are determined are $\mathrm{A}_2(6, 4; 3) = 77$, $\mathrm{A}_2(8, 6; 4) = 257$, and $\mathrm{A}_2(13, 4; 3) = 1597245$. In the first two cases, the exact number of non-isomorphic maximum codes in the PΓL, i.e., without orthogonality, is known: 5 and 2. For general $(2k, N, 2k-2; k)_q$ CDCs with $k \ge 3$ integer and $q \ge 2$ prime power, the best lower bound is given by the Echelon-Ferrers construction and the best upper bound is given by the Johnson bound, involving the maximum size of partial spreads in Theorem 126, as $q^{2k}+1 \le N \le (q^k+1)^2$. For $4 \le k$ the lower bound also achieves the LMRD bound in Proposition 99. For $k = 3$, the LMRD bound is $q^{2k}+q^2+q+1$. Any improvements on these lower and upper bounds then have direct consequences for mixed dimension subspace codes via Theorem 30. In the paper [Hei+17a; HK17a], we focused on the case $257 \le \mathrm{A}_2(8, 6; 4) \le 289$ and by theoretical and computer aided arguments, we could decrease this upper bound to attain the lower bound. By a further investigation of the involved substructures, we could determine the non-isomorphic codes.

Here, we develop the theory depicted in the paper [Hei+17a; HK17a] in a more general perspective for $(2k, N, 2k-2; k)_q$ CDCs, where $k \ge 3$ is an integer and $q \ge 2$ is a prime power. In the paper [Hei+17a; HK17a], we used similar arguments, which were very specific for $(8, N, 6; 4)_2$ CDCs. For these parameters, the Echelon-Ferrers construction can only increase the size of a corresponding LMRD by one additional codeword, which intersects the special subspace of the LMRD $S_k = \tau^{-1}(\mathbf{0}_{k\times k} \mid I_k)$ in at least a $(k-1)$-space. Hence, we immediately get at least two non-isomorphic $(2k, q^{2k}+1, 2k-2; k)_q$ CDCs. One that contains S_k and several that contain k-spaces U_i with $\dim(S_k \cap U_i) = k-1$.

Since we want to study the number of hyperplanes that contain a specific number i of codewords for all reasonable i of all $(2k, q^{2k}+1, 2k-2; k)_q$ extended LMRD codes, we need the number of codewords of a $(2k, q^{2k}, 2k-2; k)_q$ LMRD which are incident to a fixed point.

180 **Lemma**
Let $k \ge 3$ be an integer and $q \ge 2$ a prime power. Any point in $\mathbb{F}_q^{2k}$ which is not in $S_k = \tau^{-1}(\mathbf{0}_{k\times k} \mid I_k)$ is contained in exactly q^k codewords of any $(2k, q^{2k}, 2k-2; k)_q$ LMRD L.

Proof
Since $\#\mathcal{I}(C, P) \le \mathrm{A}_q(2k-1, 2k-2; k-1) = q^k+1$ for any $(2k, \#C, 2k-2; k)_q$ CDC C and any point P in $\mathbb{F}_q^{2k}$ and the mean value of codewords in L that contain a fixed point P which is not in S_k is $q^{2k} \cdot \left[\begin{smallmatrix} k \\ 1 \end{smallmatrix}\right]_q / (\left[\begin{smallmatrix} 2k \\ 1 \end{smallmatrix}\right]_q - \left[\begin{smallmatrix} k \\ 1 \end{smallmatrix}\right]_q) = q^k$, we only have to show that there is no point $P' \not\le S_k$ with $\#\mathcal{I}(L, P') = q^k+1$.

Assume that there is a point $P' = \langle (p_1 \mid p_2) \rangle$ $(p_1, p_2 \in \mathbb{F}_q^k)$ with $\#\mathcal{I}(L, P') = q^k + 1$. Then a basis change with $M \in \mathrm{GL}(\mathbb{F}_q^{2k})$ such that $\langle (p_1 \mid p_2) \rangle M\, \mathrm{Z}(\mathrm{GL}(\mathbb{F}_q^{2k})) = \langle (u_k \mid \mathbf{0}_{1\times k}) \rangle$, where u_i is the i-th unit vector, yields an isomorphic LMRD L' with

$$\#\mathcal{I}\left(L', \tau^{-1}((u_k \mid \mathbf{0}_{1\times k}))\right) = q^k + 1.$$

Denote these q^k+1 codewords with U_i for $1 \le i \le q^k+1$. Then

$$\tau(U_i) = \begin{pmatrix} I_{k-1} & \mathbf{0}_{(k-1)\times 1} & M_i \\ \mathbf{0}_{1\times(k-1)} & 1 & \mathbf{0}_{1\times k} \end{pmatrix}$$

for $1 \le i \le q^k+1$, and particularly, the MRD code corresponding to L' contains $\begin{pmatrix} M_i \\ \mathbf{0}_{1\times k} \end{pmatrix}$ for $1 \le i \le q^k+1$. Omitting the last row of each matrix in $\left\{ \begin{pmatrix} M_i \\ \mathbf{0}_{1\times k} \end{pmatrix} \mid 1 \le i \le q^k+1 \right\}$ yields a $((k-1)\times k, q^k+1, k-1)_q$ rank-distance code, which cannot exist, since the maximum cardinality for these parameters is $q^{k((k-1)-(k-1)+1)} = q^k$. □

We are now prepared to state the hyperplane spectrum of $(2k, q^{2k}, 2k-2; k)_q$ LMRDs and $(2k, q^{2k}+1, 2k-2; k)_q$ extended LMRDs.

181 **Lemma**
Let $k \ge 3$ be an integer and $q \ge 2$ a prime power.

For any $(2k, q^{2k}, 2k-2; k)_q$ LMRD L there are $[k]_q$ hyperplanes containing no codewords and each of the $[2k]_q - [k]_q$ remaining hyperplanes contains q^k codewords.

For any $(2k, q^{2k}+1, 2k-2; k)_q$ CDC $L \cup \{S_k\}$, using $S_k = \tau^{-1}(\mathbf{0}_{k\times k} \mid I_k)$, there are $[k]_q$ hyperplanes containing one codeword and each of the $[2k]_q - [k]_q$ remaining hyperplanes contains q^k codewords.

For any $(2k, q^{2k}+1, 2k-2; k)_q$ CDC $L \cup \{U\}$, such that U has dimension k and $\dim(U \cap S_k) = k-1$, there are $[k-1]_q$ hyperplanes containing one codeword, $[k]_q - [k-1]_q$ hyperplanes containing no codewords, $[k]_q - [k-1]_q$ hyperplanes containing q^k+1 codewords, and each of the $[2k]_q - 2[k]_q + [k-1]_q$ remaining hyperplanes contains q^k codewords.

Proof
Let, on the one hand, H be a hyperplane containing S_k. Then it contains no LMRD codeword since any LMRD codeword intersects S_k trivially and consequently their sum span $\mathbb{F}_q^{2k}$. On the other hand, let H be a hyperplane that does not contain S_k. Then applying the fact $\#\mathcal{I}(L, H) = \#\mathcal{I}\left(L^\perp, H^\perp\right)$ and Lemma 180, since $H^\perp$ is a point non-incident to $S_k^\perp$, i.e., the special subspace of the LMRD $L^\perp$, shows $\#\mathcal{I}\left(L^\perp, H^\perp\right) = q^k$. There is a total of $\begin{bmatrix} 2k-k \\ 2k-1-k \end{bmatrix}_q$ hyperplanes containing S_k and all remaining $\begin{bmatrix} 2k \\ 2k-1 \end{bmatrix}_q - \begin{bmatrix} 2k-k \\ 2k-1-k \end{bmatrix}_q$ hyperplanes do not contain S_k.

In the second case, i.e., $L \cup \{S_k\}$, any hyperplane containing S_k contains the codeword S_k. The remainder of the argumentation is the same as in the previous case.

In the third case, there are $\left[{2k-k \atop 2k-1-k}\right]_q$ hyperplanes containing S_k, $\left[{2k-k \atop 2k-1-k}\right]_q$ hyperplanes containing U, and $\left[{2k-k-1 \atop 2k-1-k-1}\right]_q$ hyperplanes containing $\langle S_k, U\rangle$. Therefore, all hyperplanes containing S_k and not U contain no codewords, all hyperplanes containing S_k and U contain one codeword, i.e., U, all hyperplanes which do not contain S_k but U contain in addition to the q^k codewords from L also U, and all remaining hyperplanes contain q^k LMRD-codewords like in the first argument. □

In particular, there are $(2k, q^{2k}+1, 2k-2; k)_q$ CDCs C_1 and C_2 and hyperplanes H_1 and H_2 with $\#\mathcal{I}(C_1, H_1) = q^k + 1$, $\#\mathcal{I}(C_2, H_2) = q^k$, and $\#\mathcal{I}(C_2, H) \le q^k$ for all hyperplanes H. This implies that both cases of the following lemma are in fact attained.

182 Lemma ([Hei+17a, Lemma 2])
For an integral $k \ge 3$ and prime power $q \ge 2$, let $\widetilde{P}$ be a point and $\widetilde{H}$ be a hyperplane, both in $\mathbb{F}_q^{2k}$ with $\widetilde{P} \not\le \widetilde{H}$. Let further C be a $(2k, N, 2k-2; k)_q$ CDC with $N \ge q^{2k}+1$. Then there is a $g \in \langle \mathrm{P\Gamma L}(\mathbb{F}_q^{2k}), \pi\rangle$ such that for all points P and hyperplanes H in $\mathbb{F}_q^{2k}$ one of the two following cases is true for $D = g \circ C$:

	$\#\mathcal{I}\left(D, \widetilde{H}\right) =$	$\#\mathcal{I}(D, H) \le$	$\#\mathcal{I}(D, P) \le$	$\#\mathcal{I}\left(D, \widetilde{P}\right) \ge$
case 1	q^k+1	q^k+1	q^k+1	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)(q^k+1)}{q^{2k-1}(q-1)} \right\rceil$
case 2	q^k	q^k	q^k	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)q^k}{q^{2k-1}(q-1)} \right\rceil$

Proof
First, by Lemma 41 $\#\mathcal{I}(C, H) \le \mathrm{A}_q(2k-1, 2k-2; k) = q^k + 1$ for all hyperplanes H and $\#\mathcal{I}(C, P) \le \mathrm{A}_q(2k-1, 2k-2; k-1) = q^k + 1$ for all points P.

Second, if $\#\mathcal{I}(C, H) \le l - 1$ for all hyperplanes H, then double-counting of

$$\left\{(U, H) \in C \times \left[{\mathbb{F}_q^{2k} \atop 2k-1}\right] \;\middle|\; U \le H\right\}$$

yields $N \cdot \left[{k \atop 1}\right]_q = \sum_H \#\mathcal{I}(C, H) \le \left[{2k \atop 1}\right]_q (l-1)$, i.e, $N \le (q^k+1)(l-1)$. Since $N \ge q^{2k} + 1 = (q^k+1)(q^k-1) + 2$, there is a hyperplane H' that is incident to $l \ge q^k$ codewords.

Third, fix an arbitrary hyperplane H'' and assume $\#\mathcal{I}(C, P) \le \alpha$ for all $P \le H''$. Then there is a point P'' not incident to H'' with $\#\mathcal{I}(C, P) \ge \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)\alpha}{q^{2k-1}(q-1)} = \beta$. Assuming that $\#\mathcal{I}(C, P) < \beta$ for all points $P \not\le H''$ and double counting the set $\left\{(U, P) \in C \times \left[{\mathbb{F}_q^{2k} \atop 1}\right] \;\middle|\; P \le U\right\}$ yields $(q^{2k}+1) \cdot \left[{k \atop 1}\right]_q \le N \cdot \left[{k \atop 1}\right]_q = \sum_{P \le H''} \#\mathcal{I}(C, P) + \sum_{P \not\le H''} \#\mathcal{I}(C, P) < \left[{2k-1 \atop 1}\right]_q \alpha + (\left[{2k \atop 1}\right]_q - \left[{2k-1 \atop 1}\right]_q)\beta$, i.e., $\beta > \frac{(q^{2k}+1)\cdot\left[{k \atop 1}\right]_q - \left[{2k-1 \atop 1}\right]_q \alpha}{\left[{2k \atop 1}\right]_q - \left[{2k-1 \atop 1}\right]_q} = \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)\alpha}{q^{2k-1}(q-1)}$, which is a contradiction.

Fourth, we distinguish three cases.

1. There is a hyperplane H' that is incident to exactly q^k+1 codewords. Then we use $g_1 \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ with $g_1 \circ H' = \widetilde{H}$, which exists via basis extension. Then, using “Third”, there is a point P' which is not contained in $\widetilde{H}$ and incident to at least $\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)(q^k+1)}{q^{2k-1}(q-1)} \right\rceil$ codewords. Since the stabilizer of $\widetilde{H}$ in $\mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ is transitive on the set of points non-incident to $\widetilde{H}$, there is a $g_2 \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ with $g_2 \circ \widetilde{H} = \widetilde{H}$ and $g_2 \circ P' = \widetilde{P}$.
2. Any hyperplane is incident to at most q^k codewords, but there is a point P' that is incident to q^k+1 codewords. Then we use $g_1' \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ with $g_1' \circ (\pi(P')) = \widetilde{H}$ and using $g_1 = g_1' \cdot \pi$ we are in the first case.
3. Any hyperplane and any point is incident to at most q^k codewords. Then the argument in “Second” guarantees the existence of a hyperplane H' that is incident to exactly q^k codewords. Again, we use $g_1 \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ with $g_1 \circ H' = \widetilde{H}$. Then, again using “Third”, there is a point P' which is not contained in $\widetilde{H}$ and incident to at least $\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)q^k}{q^{2k-1}(q-1)} \right\rceil$ codewords. Since the stabilizer of $\widetilde{H}$ in $\mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ operates again transitive on the set of points non-incident to $\widetilde{H}$, there is a $g_2 \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ with $g_2 \circ \widetilde{H} = \widetilde{H}$ and $g_2 \circ P' = \widetilde{P}$.

The map g is $g_2 \cdot g_1$ and $g \circ C$ has the stated properties in all three cases. □

The first three cases for k and $q = 2$ are:

183 Corollary
Any $(6, N, 4; 3)_2$ CDC C with $65 \le N$ is isomorphic to a CDC D, such that for a fixed point $\widetilde{P}$ and a hyperplane $\widetilde{H}$ which are non-incident, one of two cases is attained:

	$\#\mathcal{I}\left(D, \widetilde{H}\right) =$	$\#\mathcal{I}(D, H) \le$	$\#\mathcal{I}(D, P) \le$	$\#\mathcal{I}\left(D, \widetilde{P}\right) \ge$
case 1	9	9	9	$\lceil 5.5 \rceil$
case 2	8	8	8	$\lceil 6.47 \rceil$

Any $(8, N, 6; 4)_2$ CDC C with $257 \le N$ is isomorphic to a CDC D, such that for a fixed point $\widetilde{P}$ and a hyperplane $\widetilde{H}$ which are non-incident, one of two cases is attained:

	$\#\mathcal{I}\left(D, \widetilde{H}\right) =$	$\#\mathcal{I}(D, H) \le$	$\#\mathcal{I}(D, P) \le$	$\#\mathcal{I}\left(D, \widetilde{P}\right) \ge$
case 1	17	17	17	$\lceil 13.25 \rceil$
case 2	16	16	16	$\lceil 14.24 \rceil$

Any $(10, N, 8; 5)_2$ CDC C with $1025 \le N$ is isomorphic to a CDC D, such that for a fixed point $\widetilde{P}$ and a hyperplane $\widetilde{H}$ which are non-incident, one of two cases is attained:

	$\#\mathcal{I}\left(D,\widetilde{H}\right) =$	$\#\mathcal{I}\left(D,H\right) \le$	$\#\mathcal{I}\left(D,P\right) \le$	$\#\mathcal{I}\left(D,\widetilde{P}\right) \ge$
case 1	33	33	33	$\lceil 29.13 \rceil$
case 2	32	32	32	$\lceil 30.12 \rceil$

P is an arbitrary point and H is an arbitrary hyperplane in the respective vector space in all three cases.

The set of codewords incident to the hyperplane $\widetilde{H}$ is called *hyperplane configuration* and can be investigated even further using the bijection $\iota : \mathbb{F}_q^{2k-1} \to \widetilde{H}$ for subspaces and sets of subspaces. The next lemma shows that all possible hyperplane configurations are determined by the non-isomorphic $(2k-1, N, 2k-2, k)_q$ CDCs with $q^k \le N \le q^k+1$, which are the orthogonal codes of $(2k-1, N, 2k-2, k-1)_q$ partial spreads with $q^k \le N \le q^k+1$.

184 Lemma
Let $\widetilde{P}$ and $\widetilde{H}$ be a point and a hyperplane in $\mathbb{F}_q^{2k}$ which are not incident and $\mathcal{A}_i$ be a superset of the transversal of $(2k-1, i, 2k-2, k)_q$ CDCs for $q^k \le i \le q^k+1$, where $3 \le k$. Let C be a $(2k, \#C, 2k-2; k)_q$ CDC with $\#C \ge q^{2k}+1$. Then there is a $g \in \langle \mathrm{P\Gamma L}(\mathbb{F}_q^{2k}), \pi \rangle$ such that for all points P and hyperplanes H in $\mathbb{F}_q^{2k}$ one of the two following cases is true for $D = g \circ C$:

	$\iota^{-1}\left(\mathcal{I}\left(D,\widetilde{H}\right)\right) \in$	$\#\mathcal{I}\left(D,H\right) \le$	$\#\mathcal{I}\left(D,P\right) \le$	$\#\mathcal{I}\left(D,\widetilde{P}\right) \ge$
case 1	$\mathcal{A}_{q^k+1}$	q^k+1	q^k+1	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)(q^k+1)}{q^{2k-1}(q-1)} \right\rceil$
case 2	$\mathcal{A}_{q^k}$	q^k	q^k	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)q^k}{q^{2k-1}(q-1)} \right\rceil$

Proof
Applying Lemma 182, we only have to show that there is a $g \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$ such that $g \circ \widetilde{P} = \widetilde{P}$, $g \circ \widetilde{H} = \widetilde{H}$, and $\iota^{-1}\left(\mathcal{I}\left(g \circ C, \widetilde{H}\right)\right) \in \mathcal{A}_{q^k} \cup \mathcal{A}_{q^k+1}$ for a C with

	$\#\mathcal{I}\left(C,\widetilde{H}\right) =$	$\#\mathcal{I}\left(C,H\right) \le$	$\#\mathcal{I}\left(C,P\right) \le$	$\#\mathcal{I}\left(C,\widetilde{P}\right) \ge$
case 1	q^k+1	q^k+1	q^k+1	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)(q^k+1)}{q^{2k-1}(q-1)} \right\rceil$
case 2	q^k	q^k	q^k	$\left\lceil \frac{(q^{2k}+1)\cdot(q^k-1)-(q^{2k-1}-1)q^k}{q^{2k-1}(q-1)} \right\rceil$

Moreover we assume wlog. $\widetilde{P} = \langle u_{2k} \rangle$ and $\widetilde{H} = \langle u_1, \ldots, u_{2k-1} \rangle$ since we can map any non-incident pair of point and hyperplane to $\langle u_{2k} \rangle$ and $\langle u_1, \ldots, u_{2k-1} \rangle$ in the $\mathrm{PGL}(\mathbb{F}_q^{2k})$, using the canonical basis $\langle u_1, \ldots, u_{2k} \rangle$ of $\mathbb{F}_q^{2k}$.

Since $\mathcal{A}_{q^k}$ and $\mathcal{A}_{q^k+1}$ are supersets of transversals, there is a $g' = (M \cdot Z(\mathrm{GL}(\mathbb{F}_q^{2k-1})), \alpha) \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k-1})$ with $g' \circ \iota^{-1}\left(\mathcal{I}\left(C, \widetilde{H}\right)\right) \in \mathcal{A}_{q^k} \cup \mathcal{A}_{q^k+1}$, where $M \in \mathrm{GL}(\mathbb{F}_q^{2k-1})$, $Z(G)$ is the center of the group G, and α is a field automorphism.

Now we define $g = \left(\begin{pmatrix} M & \mathbf{0}_{(2k-1)\times 1} \\ \mathbf{0}_{1\times(2k-1)} & 1 \end{pmatrix} \cdot Z(\mathrm{GL}(\mathbb{F}_q^{2k})), \alpha\right) \in \mathrm{P\Gamma L}(\mathbb{F}_q^{2k})$. Then this g has the stated properties: $g \circ \widetilde{P} = \alpha\left(\langle u_{2k}\rangle \cdot \begin{pmatrix} M & \mathbf{0}_{(2k-1)\times 1} \\ \mathbf{0}_{1\times(2k-1)} & 1 \end{pmatrix} \cdot Z(\mathrm{GL}(\mathbb{F}_q^{2k}))\right) = \widetilde{P}$ and similarly $g \circ \widetilde{H} = \alpha\left(\langle u_1, \ldots, u_{2k-1}\rangle \cdot \begin{pmatrix} M & \mathbf{0}_{(2k-1)\times 1} \\ \mathbf{0}_{1\times(2k-1)} & 1 \end{pmatrix} \cdot Z(\mathrm{GL}(\mathbb{F}_q^{2k}))\right) = \widetilde{H}$ since $\alpha(0) = 0$, $\alpha(1) = 1$, and $\mathrm{rk}(M) = 2k-1$. $\square$

The main difference of $(6, N_3, 4; 3)_2$ CDCs and $(8, N_4, 6; 4)_2$ CDCs, i.e., $q = 2$ and $3 \le k \le 4$, to other combinations of q and k is that the classification of $(2k-1, N, 2k-2, k-1)_q$ for $q^k \le N \le q^k + 1$ is known:

185 **Theorem ([GSS00, Theorem 5.1])**
$\mathrm{A}_2(5, 4; 2) = 9$ and there are 4 isomorphism types of $(5, 9, 4; 2)_2$ CDCs. Their automorphism groups have the orders: $6^3 24^1$.

186 **Theorem ([GSS00, Theorem 5.3])**
There are 9 isomorphism types of $(5, 8, 4; 2)_2$ CDCs. Their automorphism groups have the orders: $1^1 2^4 3^2 6^1 168^1$.

187 **Theorem ([HKK16a, Theorem 1])**
$\mathrm{A}_2(7, 6; 3) = 17$ and there are 715 isomorphism types of $(7, 17, 6; 3)_2$ CDCs. Their automorphism groups have the orders: $1^{551} 2^{70} 3^{27} 4^{19} 6^6 7^1 8^8 12^2 16^7 24^6 32^5 42^1 48^5 64^2 96^1$ $112^1 128^1 192^1 2688^1$.

188 **Theorem ([HKK16a, Theorem 2])**
There are 14445 isomorphism types of $(7, 16, 6; 3)_2$ CDCs. Their automorphism groups have the orders: $1^{13587} 2^{511} 3^{143} 4^{107} 6^{20} 7^4 8^{19} 9^3 12^{24} 16^1 18^1 20^1 21^1 24^9 36^1 42^1 48^3 64^1 96^1 112^1$ $168^2 288^1 384^1 960^1 2688^1$.

Suppose we know that a $(2k, N, 2k-2; k)_q$ CDC contains a subset $F \subseteq \begin{bmatrix} \mathbb{F}_q^{2k} \\ k \end{bmatrix}$, then we can state two BLP upper bounds for N and additionally, we get a third upper bound as an LP-relaxation of one of these two BLPs.

These bounds are similar to DefaultBLP but respect the distinction of Lemma 182 in the two cases.

189 Lemma
Let $k \geq 3$ be an integer and $q \geq 2$ a prime power. Let $F \subseteq \begin{bmatrix} \mathbb{F}_q^{2k} \\ k \end{bmatrix}$ and $f \in \{q^k, q^k+1\}$, then any $(2k, \#C, 2k-2; k)_q$ CDC C with $F \subseteq C$ such that each point and hyperplane is incident to at most f codewords has $\#C \leq z_{2k}^{\mathrm{BLP}}(F,f) \leq z_{2k}^{\mathrm{LP}}(F,f)$, where $\mathrm{Var}_{2k} = \begin{bmatrix} \mathbb{F}_q^{2k} \\ k \end{bmatrix}$, z_{2k}^{LP} is the LP-relaxation of z_{2k}^{BLP}, and

$$\begin{aligned} z_{2k}^{\mathrm{BLP}}(F,f) = \max \sum_{U \in \mathrm{Var}_{2k}} x_U & & & \\ \text{st} \sum_{U \in \mathcal{I}(\mathrm{Var}_{2k}, W)} x_U &\leq f & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k} \\ w \end{bmatrix} & \quad \forall w \in \{1, 2k-1\} \\ \sum_{U \in \mathcal{I}(\mathrm{Var}_{2k}, W)} x_U &\leq 1 & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k} \\ w \end{bmatrix} & \quad \forall w \in \{2, 2k-2\} \\ x_U &= 1 & \forall U \in F & \\ x_U &\in \{0,1\} & \forall U \in \mathrm{Var}_{2k}\,. & \end{aligned}$$

Proof
Interpreting $(x_U)_{U \in \mathrm{Var}_{2k}}$ as incidence vector of C, the objective function is equal to $\#C$. The first set of constraints is feasible by the choice of f and the second set of constraints is feasible by Lemma 41: $\#\mathcal{I}(C,W) \leq \mathrm{A}_q(2k-2, 2k-2; k-2) = 1$ for any 2-dimensional W and $\#\mathcal{I}(C,W) \leq \mathrm{A}_q(2k-2, 2k-2; k) = \mathrm{A}_q(2k-2, 2k-2; k-2) = 1$ for any $2k-2$-dimensional W. The third set of constraints is feasible since $F \subseteq C$. $\square$

Note that in z_{2k}^{LP} the constraints $x_U \leq 1$ may be omitted, since for any $U \in \mathrm{Var}_{2k}$, there is a line W in U and hence implicitly a constraint $x_U \leq \sum_{U \in \mathcal{I}(\mathrm{Var}_{2k}, W)} x_U \leq 1$.

In addition to the two upper bounds of the last lemma, we consider an integer linear programming formulation of $\widetilde{C} = \{U \cap \widetilde{H} \mid U \in C\}$ for a $(2k, \#C, 2k-2; k)_q$ CDC C. Any codeword that is contained in $\widetilde{H}$ has dimension k in $\widetilde{C}$ and any other codeword has dimension $k-1$ in $\widetilde{C}$.

190 Lemma
For a prime power $q \geq 2$ and an integer $3 \leq k$ and $F \subseteq \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ k \end{bmatrix}$ let $\mathrm{Var}_{2k-1}(F) := \left\{ U \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ k-1 \end{bmatrix} \,\middle|\, \dim(U \cap S) \leq 1 \, \forall S \in F \right\}$ and $\omega(F,W) = \max\{\#\Omega \mid \Omega \subseteq \mathcal{I}(\mathrm{Var}_{2k-1}(F), W) \wedge \dim(U_1 \cap U_2) \leq 1 \, \forall U_1 \neq U_2 \in \Omega\}$. If $\#F \in \{q^k, q^k+1\}$, then any $(2k, \#C, 2k-2; k)_q$ CDC C with $\#C \geq l$ and $\iota(F) \subseteq C$ such that each point and

hyperplane is incident to at most $\#F$ codewords satisfies $\#C \le z_{2k-1}^{\mathrm{BLP}}(F)$, where

$$
\begin{array}{lll}
 & z_{2k-1}^{\mathrm{BLP}}(F) = \max \displaystyle\sum_{U \in \mathrm{Var}_{2k-1}(F)} x_U + \#F \quad \text{st} & \\
\displaystyle\sum_{U \in \mathcal{I}(\mathrm{Var}_{2k-1}(F), W)} & x_U \le \#F - \#\mathcal{I}(F, W) & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ 1 \end{bmatrix} \\
\displaystyle\sum_{U \in \mathcal{I}(\mathrm{Var}_{2k-1}(F), W)} & x_U \le 1 & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ 2 \end{bmatrix} \setminus \left(\cup_{S \in F} \begin{bmatrix} S \\ 2 \end{bmatrix}\right) \\
\displaystyle\sum_{U \in \mathcal{I}(\mathrm{Var}_{2k-1}(F), W)} & x_U \le 1 & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ 2k-4 \end{bmatrix} : S \not\le W \, \forall S \in F \\
\displaystyle\sum_{U \in \mathcal{I}(\mathrm{Var}_{2k-1}(F), W)} & x_U \le \min\{\omega(F, W), q^2+q+1\} & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ 2k-3 \end{bmatrix} : S \not\le W \, \forall S \in F \\
\displaystyle\sum_{U \in \mathcal{I}(\mathrm{Var}_{2k-1}(F), W)} & x_U \le q(\#F - \#\mathcal{I}(F, W)) & \forall W \in \begin{bmatrix} \mathbb{F}_q^{2k-1} \\ 2k-2 \end{bmatrix} \\
\displaystyle\sum_{U \in \mathrm{Var}_{2k-1}(F)} & x_U \ge l - \#F & \\
 & x_U \in \{0, 1\} & \forall U \in \mathrm{Var}_{2k-1}(F)
\end{array}
$$

Proof

Interpreting $(x_U)_{U \in \mathrm{Var}_{2k-1}(F)}$ as incidence vector of $\{U \cap \widetilde{H} \mid U \in C \wedge U \not\le \widetilde{H}\}$, one can check the objective function and the last two lines. Since two k-spaces in C intersect in at most a point, any two elements in $\{U \cap \widetilde{H} \mid U \in C\}$ also intersect in at most a point, which proves the constraints with $\dim(W) \in \{2, 2k-4\}$.

Any $(2k-3)$-space W contains at most $\omega(F, W)$ planes by the definition of ω, also $\iota(W)$ is incident to $\begin{bmatrix} (2k)-(2k-3) \\ (2k-2)-(2k-3) \end{bmatrix}_q = q^2+q+1$ $(2k-2)$-spaces, which in turn contain at most one codeword of C. If W contains a k-space of F, then any $(k-1)$-space in W meets this k-space in at least a line. This proves the constraints with $\dim(W) = 2k-3$.

For any point W its embedding $\iota(W)$ is incident to at most $\#F$ codewords of C proving the constraints with $\dim(W) = 1$.

For any $(2k-2)$-subspace W its embedded $\iota(W)$ is contained in $\begin{bmatrix} (2k)-(2k-2) \\ (2k-1)-(2k-2) \end{bmatrix}_q = q+1$ hyperplanes in $\mathbb{F}_q^{2k}$ of which one of them is $\widetilde{H}$. Since each hyperplane of $\mathbb{F}_q^{2k}$ is incident to at most $\#F$ codewords and $\widetilde{H}$ is incident to exactly $\#F$ codewords, i.e., $\iota(F)$, the other q hyperplanes are each incident to either $\#F$ codewords if W contains no element of F or $\#F-1$ codewords if W contains one element of F. Obviously two k-spaces in a $(2k-2)$-space intersect in at least a line and hence W contains at most one element of F. This proves the constraints with $\dim(W) = 2k-2$. □

The single last inequality allows the BLP solver to cut the branch & bound tree early since we are only interested in solutions of cardinality at least l, cf. [Dak65]. $\omega(F, W)$ is in fact the clique number of the subgraph incident to W of the graph having vertex set $\operatorname{Var}_{2k-1}(F)$ and two vertices $U_1 \neq U_2$ have an edge iff $\dim(U_1 \cap U_2) \leq 1$. Although the upper bound $\min\{\omega(F, W), \#F - \#\mathcal{I}(F, W)\}$ is feasible for $\dim(W) = 1$ and $\min\{\omega(F, W), q(\#F - \#\mathcal{I}(F, W))\}$ is feasible for $\dim(W) = 2k - 2$ the computation of $\omega(F, W)$ is difficult, since these subgraphs have many vertices.

Some of the involved problems are also too difficult to be tackled directly and it is often easier to split a large problem into subproblems while utilizing symmetry to reduce the number of constructed subproblems via e.g. Lemma 32.

12.1 The application for $(8, N, 6; 4)_2$ CDCs with $257 \leq N$

The main result of this whole chapter is

191 **Theorem ([Hei+17a, Theorem 1])**
$\mathrm{A}_2(8, 6; 4) = 257$ and up to isomorphism there are two maximum codes. Both are extended LMRD codes.

This surprising theorem has then additional implications for MDCs via Theorem 30.

192 **Corollary ([Hei+17a, Corollary 3])**
$\mathrm{A}_2(8, 6) = 257$.

Theorem 191 has two very interesting aspects. First, the simple construction for CDCs using an LMRD and extending it, which is here also a special case of the Echelon-Ferrers construction, is capable of providing maximum codes for these parameters. Second, any maximum code contains 256 evenly distributed codewords, i.e., all points are covered by exactly 16 codewords of the LMRD, and one additional codeword that intersects the special subspace $S_4 = \tau^{-1}(\mathbf{0}_{4\times 4} \mid I_4)$ in at least a plane. This irregular structure is a necessity to get maximum codes.

As special subspaces we explicitly label a point $\widetilde{P} = \langle(0, 0, 0, 0, 0, 0, 0, 1)\rangle$ and a hyperplane $\widetilde{H} = \{x \in \mathbb{F}_2^8 \mid x_8 = 0\}$. Note that $\widetilde{P}$ and $\widetilde{H}$ are not incident.

The remaining section uses four phases to prove Theorem 191. Since Lemma 184 determines substructures of $(8, N, 6; 4)_2$ CDCs with $257 \leq N$, these phases resemble the strategy to exclude possible hyperplane configurations in Phase 1, then extend the remaining possible hyperplane configurations to 31-*point-hyperplane configurations* in Phase 2, i.e., sets of 31 codewords such that 16 respective 17 are incident to $\widetilde{H}$ and 15 respective 14 are incident to $\widetilde{P}$, which have to be contained in any CDC of size at least 257 by Lemma 184. These 31-point-hyperplane configurations fix 31 out of at least 257 codewords which reduces the search space significantly. Therefore, it is possible to compute $\mathrm{A}_2(8,6;4) \le 257$ in Phase 3. In the last phase, i.e., Phase 4, we reuse the 31-point-hyperplane configurations which are subset of $(8,257,6;4)_2$ CDCs to argue that any code with these parameters is necessarily an extended LMRD. Using an independent reasoning, we show that the LMRD is unique up to isomorphism, cf. Theorem 193, hence proving Theorem 191.

Let $\mathcal{A}_{17}$ be a transversal of the 715 $(7,17,6;3)_2$ CDCs of Theorem 187 and $\mathcal{A}_{16}$ be a transversal of the 14445 $(7,16,6;3)_2$ CDCs of Theorem 188.

12.1.1 Excluding hyperplane configurations (Phase 1)

For all $A \in \mathcal{A}_{16} \cup \mathcal{A}_{17}$ we computed $z_8^{\mathrm{LP}}(\iota(A^\perp), \#A)$ of Lemma 189 and found that all but 33 elements in $\mathcal{A}_{16}$ (37 251 hours wall-time with `CPLEX` [IBM10])[1] and 5 elements in $\mathcal{A}_{17}$ (1021 hours wall-time with `CPLEX` [IBM10]) have an optimal value smaller than 256.9, i.e., we have implemented a safety threshold of $\varepsilon = 0.1$, and cannot be extended to $(8,257,6;4)_2$ CDCs. These 38 remaining elements are listed in Table 12 and their LP values are stated in Table 11. By F_i we denote the corresponding sets of solids in $\mathbb{F}_2^8$ for $1 \le i \le 38$.

For indices $1 \le i \le 38$ we computed $z_7^{\mathrm{BLP}}(\iota(F_i))$ of Lemma 190 and obtained 27 elements in $\mathcal{A}_{16}$ and 3 elements in $\mathcal{A}_{17}$ that have $z_7^{\mathrm{BLP}}(\iota(F_i)) < 256.9 \le z_8^{\mathrm{LP}}(\iota(F_i), \#F_i)$, cf. Table 11 for details. This computation was aborted after 100 hours of wall-time with `CPLEX` [IBM10] for each of these 38 subproblems.

Since $z_7^{\mathrm{BLP}}(\iota(F_8)) \le 257.2408$ was close to 256.9, we split the BLP into subproblems with Lemma 32. $\mathrm{Var}_7(\iota(F_8))$ has exactly 948 planes which form 56 orbits $(4^3 8^{13} 16^{28} 32^{12})$ under the action of its automorphism group of order 32. Hence, Lemma 32 generated 56 subproblems. After 15 hours, the first subproblem was solved optimally with an upper bound of 256. The objective values of the other 55 subproblems could be upper bounded by 254 in less than 15 minutes.

The computation performed up to this point shows $\mathrm{A}_2(8,6;4) \le 271$ in a total of 42 087 hours wall-time.

12.1.2 Extending hyperplane configurations to 31-point-hyperplane configurations (Phase 2)

Next we want to enlarge the remaining seven hyperplane configurations, cf. indices $1 \le i \le 7$ in Table 12, to 31-point-hyperplane configurations.

We build up a graph $G_i = (V_i, E_i)$, whose vertex set V_i consists of all solids in $\begin{bmatrix} \mathbb{F}_2^8 \\ 4 \end{bmatrix}$ that contain $\widetilde{P}$ and intersect the elements from F_i in at most a point. For $U, W \in V_i$, we have $\{U, W\} \in E_i$ iff $U \cap W = \widetilde{P}$. Using `Cliquer` [NÖ03], we enumerate all cliques of size $31 - \#F_i$ of G_i and compute a transversal $T(F_i)$ of the action of the stabilizer of F_i, see

[1] Most computations were performed on the Cluster of the University of Bayreuth using mostly CPUs of type Intel E5-2630 v4 @ 2.20GHz, which we assume if nothing else is further specified.

the sixth column of Table 11 for the corresponding orbit lengths. The clique computations for $1 \leq i \leq 7$, $i \neq 5$ took between 27 and 589 hours wall-time with `Cliquer` [NÖ03] on an AMD Opteron 6348 @ 1.4GHz, see Table 10 for details about the running times and $\#V_i$, while the computation time for the transversal was negligible. Altogether, the clique computation wall-time for $1 \leq i \leq 7$, $i \neq 5$, was 1464 hours. The clique computation for G_5 was aborted after 600 hours wall-time and then performed in parallel using Lemma 32.

With X as the vertex set of G_5, Γ the automorphism group of F_5, and $f(S)$ equals 1 iff S is a clique in G_5. The 1258 vertices of G_5 are partitioned into 24 orbits of size 1 and 617 orbits of size 2 by Γ, which leaves us 641 graphs where we have to enumerate all cliques of size $31 - \#F_5 - 1 = 14$. Since some of these graphs still consist of *many* vertices, we iteratively apply Lemma 32 with the identity group as Γ for at most two further times: After the first round, we split the 68 subproblems, which lead to graphs with at least 700 vertices. Then, we split the 81 subproblems, which lead to graphs with at least 600 vertices. Finally, we end up with 104 029 graphs, where we have to enumerate all cliques of size 14, 13 or 12. All of these instances have been solved in parallel with `Cliquer` [NÖ03] to get a superset of the transversal of all cliques of size 15 of G_5. Applying the action of the automorphism group of order 2 then allowed to get a transversal as well as all cliques, simply as union of the orbits. This took about 750 hours in CPU-time with 16 processes on two Intel Xeon E5-2690 @ 2.90GHz, where the smaller problems were preprocessed on a single computer and the remaining 55 420 larger subproblems were processed in parallel with 16 cores.

The complete extension step took about 2 214 hours wall-time.

12.1.3 Excluding 31-point-hyperplane configurations (Phase 3)

For the 73 234 31-point-hyperplane configurations resulting from the last step, we computed $z_8^{\mathrm{LP}}(\cdot)$ in 953 hours. The maximum value aggregated by the contained hyperplane configuration with index i is stated in the seventh column of Table 11 and Table 10. For the configuration with index 1 there are 195, for the configuration with index 3 there are 98, and for the configuration with index 7 there are 240 31-point-hyperplane configurations with $z_8^{\mathrm{LP}} \geq 256.9$.

Next, we computed z_8^{BLP} for these remaining $195 + 98 + 240$ cases in 851 hours, see the eighth column of Table 11 and Table 10. The counts for value at least 257 are $2 + 0 + 240$ and all of them have exactly 257 as optimum value, i.e., we have $\mathrm{A}_2(8, 6; 4) = 257$ and any maximum CDC with these parameters contains one of these 242 31-point-hyperplane configurations up to isomorphism.

In total, the computations needed for the exclusion of the 31-point-hyperplane configurations took 1 804 hours wall-time.

12.1.4 Classification of $(8, 257, 6; 4)_2$ CDCs (Phase 4)

Now we will verify indirectly that there exists a codeword U such that $C \setminus \{U\}$ is an LMRD code in all those extensions.

The hyperplane configuration of C in $\widetilde{H}$ is either $F_1 \in \mathcal{A}_{16}$ or $F_7 \in \mathcal{A}_{17}$ with 2 and 240 possible 31-point-hyperplane configurations, respectively.

For F_1 there exists a unique solid S in $\mathbb{F}_2^8$ which is disjoint from the 31 prescribed solids in both cases. Adding the constraint $x_S = 0$ to the BLP of Lemma 189 yields an upper bound of 256, i.e., S has to be a codeword in C, in about 2 hours of wall-time with `CPLEX` [IBM10] in each of the two cases. The codeword S covers its 15 contained points. Via $x_S = 1$ and

$$\sum_{P \in \begin{bmatrix} S \\ 1 \end{bmatrix}} \sum_{U \in \mathcal{I}(\mathrm{Var}_8, P)} x_U \ge 16,$$

we can ensure that another codeword of C meets S in a point. This modification of the BLP of Lemma 189 again yields an upper bound of 256 in about two hours of wall-time with `CPLEX` [IBM10] in both cases. Thus, $C \setminus \{S\}$ has to be an LMRD code.

For F_7 there exists a unique solid S in $\mathbb{F}_2^8$ which is disjoint from 30 of the prescribed solids and meets the other prescribed solid S' in a plane, in all 240 cases. By adding

$$\sum_{P \in \begin{bmatrix} S \\ 1 \end{bmatrix}} \sum_{U \in \mathcal{I}(\mathrm{Var}_8, P)} x_U \ge 8,$$

we can ensure that S is met by another codeword, besides S', from C in a point. The augmented BLP of Lemma 189 needs 9 hours wall-time with `CPLEX` [IBM10] and end up with $z_8^{\mathrm{BLP}} \le 256$ for each of the 240 cases. Thus, $C \setminus \{S'\}$ has to be an LMRD code.

This sums up to 2 168 hours wall-time for this indirect classification.

Moreover, the contained LMRD code is then unique up to isomorphism:

193 Theorem ([Hei+17a; Hei+on, Theorem 10])
The Gabidulin construction gives the unique isomorphism type of not necessarily linear 4×4 MRD codes with minimum rank distance 3.

Proof
Let C be a 4×4 MRD code of minimum rank distance 3. Then $\#C = 256$. For each vector $u \in \mathbb{F}_2^4$, there are exactly 16 matrices in C having u as their last row, cf. Lemma 180. After removing this common row, those 16 matrices form a binary 3×4 MRD code of minimum rank distance 3. These MRD codes have been classified in [HKK16a] into 37 isomorphism classes.

Let C' be one of these codes, extended to size 4×4 by appending the zero vector as a last row to all the matrices in C'. Up to isomorphism, C is the extension of one of these 37 codes C' by $256 - 16 = 240$ matrices. In particular, for each $u \in \mathbb{F}_2^4 \setminus \{\mathbf{0}\}$, it must be possible to add 16 matrices of size 4×4 with last row u without violating the rank distance. For fixed u, this question can be formulated as a clique problem: We define a graph G_u, whose vertex set is given by all 4×4 matrices with last row u having rank distance ≥ 3 to all matrices in C'. Two vertices are connected by an edge if the corresponding matrices have their rank distance ≥ 3. Now the question is whether the graph G_u admits a clique of size 16 for all $u \in \mathbb{F}_2^4 \setminus \{\mathbf{0}\}$. Using `Cliquer` [NÖ03], we compute that this is only possible for a single type of the 37 codes C'.

For this remaining type, the full extension problem to a 4×4 MRD code is again formulated as a clique problem. The graph is defined in a similar way, but without the restriction on the last row of the matrices in the vertex set. This yields a graph with 1920 vertices. The maximum clique problem is solved within seconds for this graph. The result are 8 cliques of maximum possible size 240, such that we get 8 extensions to a rank distance code of size $16 + 240 = 256$, which are MRD codes. Those 8 codes turn out to be isomorphic to the Gabidulin MRD code. □

By the last theorem, in our setting there is only a single type of an LMRD code, which is the lifted Gabidulin MRD code. It is iso-dual (isomorphic to its orthogonal code).

194 **Corollary**

Let C be an $(8, 257, 6; 4)_2$ CDC, then C is isomorphic to either $\{\langle(I_4 \mid B)\rangle \mid B \in M\} \cup \{\langle(\mathbf{0}_{4\times4} \mid I_4)\rangle\}$ or $\{\langle(I_4 \mid B)\rangle \mid B \in M\} \cup \{\langle(\mathbf{0}_{4\times3} \mid I_4 \mid \mathbf{0}_{4\times1})\rangle\}$, where M is the 4×4 Gabidulin MRD code with minimum rank distance 3.

Proof

From Theorem 193 we conclude that the contained LMRD code $C' \subseteq C$ is isomorphic to the lifted version of the Gabidulin MRD code M. It has a stabilizer of cardinality 230 400, which partitions the 451 solids intersecting each codeword of C' in at most a point in two orbits: the special solid of C', which intersects all codewords of C' trivially, and an orbit consisting of 450 solids, which all intersect the special solid of C' in a plane. □

12.2 Another approach for $\mathrm{A}_2(8,6;4) \le 272$

In [HK17a] we show another approach to get $\mathrm{A}_2(8,6;4) \le 272$ computationally by involving $(7, 34, 5; \{3, 4\})_2$ and $(7, 33, 5; \{3, 4\})_2$ subspace codes and produce the classification of the latter as byproduct.

These substructures can be found at `http://subspacecodes.uni-bayreuth.de` associated with [Hei+16].

For any $(8, \#C, 6; 4)_2$ CDC C with $281 \le \#C$ $(273 \le \#C)$ Corollary 46 guarantees a non-incident point-hyperplane-pair $(\widetilde{P}, \widetilde{H})$ such that the *shortened code* of C via Lemma 44, using $\widetilde{P}$ and $\widetilde{H}$, has the parameters $(7, N, 5; \{3, 4\})_2$ with $34 \le N$ $(33 \le N)$, respectively.

195 **Theorem ([HKK16b, Theorem 3.3.ii], [HKK16a, Theorem 6])**

$\mathrm{A}_2(7, 5) = 34$ and there are exactly 20 isomorphism types of codes having these parameters. All of them have dimension distribution $3^{17}4^{17}$. In 11 cases the automorphism group is trivial and in the remaining 9 cases the automorphism group is a unique group of order 7, which partitions $\mathbb{F}_2^7$ into 2 fixed vectors and 18 orbits of size 7.

These 20 isomorphism types contain just 9 of the 715 isomorphism types of $(7,17,6;3)_2$ and $(7,17,6;4)_2$ CDCs. Denoting these nine cases by $a_1,\ldots,a_9$, the 20 isomorphism types of $(7,34,5;\{3,4\})_2$ subspace codes can be categorized as $\{\{a_1,a_6\},\{a_2,a_6\},\{a_3,a_7\},$ $\{a_3,a_8\},\{a_4,a_4\},\{a_4,a_9\},\{a_5,a_6\},\{a_6,a_6\}\}$.

In particular, these pairings can be covered by just the three cases $\{a_3,a_4,a_6\}$, i.e., any of these eight sets contain at least one of these three elements. Prescribing the corresponding 17 codewords and computing the LP-relaxation of DefaultCDCBLP$(2,8,6,4)$ gives:

type	# Aut	LP bound
a_4	32	221.00
a_6	7	230.63
a_3	32	268.04

This excludes any possible $(7,34,5;\{3,4\})_2$ embedded subcode.

Thus, by computing only three linear programs, we can conclude $\mathrm{A}_2(8,6;4) \le 280$. We remark that the classification results of Theorem 187 and Theorem 195 were obtained using the clique search software `Cliquer` [NÖ03], which is not based on floating point numbers.

The next step is to consider codes of size at least 273 and hence their shortened codes have a cardinality of at least 33.

196 **Theorem ([HK17a, Theorem 3])**
There are 563 isomorphism types of $(7,33,5;\{3,4\})_2$ codes. Their automorphism groups have the orders: $1^{481}2^{19}4^{4}7^{56}8^{1}14^{2}$ and the possible dimension distributions are $3^{16}4^{17}$ and $3^{17}4^{16}$.

Proof
Any $(7,33,5;\{3,4\})_2$ subspace code contains a $(7,17,6;3)_2$ CDC up to orthogonality. For each of the 715 isomorphism types of $(7,17,6;3)_2$ CDCs C in $\mathbb{F}_2^7$, we first compute $A(C) = \left\{W \in \begin{bmatrix}\mathbb{F}_2^7\\4\end{bmatrix} \;\middle|\; \mathrm{d_s}(W,U) \ge 5\,\forall U \in C\right\}$. Then, we build up a graph $G(C)$ with vertex set $A(C)$ in which two different vertices $U, W \in A(C)$ are joined by an edge iff $\mathrm{d_s}(U,W) \ge 6$. These 715 graphs have between 832 and 1056 vertices and between 213 760 and 353 088 edges. Applying the software `Cliquer` [NÖ03] on the computing cluster of the University of Bayreuth gives 23 740 cliques of cardinality 16 – after 11 200 hours of CPU time. Via the group action of the automorphism group of the corresponding $(7,17,6;3)_2$ CDC C, they form 563 orbits. □

Only 76 out of the 715 isomorphism types of $(7,17,6;3)_2$ CDCs can be extended to $(7,33,5;\{3,4\})_2$ codes. These 76 codes have automorphism groups of orders $1^{51}2^{7}3^{3}4^{2}6^{1}$ $7^{1}12^{1}16^{2}32^{2}42^{1}64^{1}112^{1}128^{1}192^{1}2688^{1}$ and together can be extended to $1^{56}2^{7}3^{1}4^{1}5^{2}6^{1}10^{1}$ $11^{1}44^{1}49^{1}67^{1}77^{1}104^{1}108^{1}$ codes of size 33, whereas i^{n_i} means there are n_i CDCs of size 17 that give rise to i codes of size 33.

In 75 of these 76 cases the LP relaxation of DefaultCDCBLP$(2,8,6,4)$ with 17 forced codewords gives an objective value strictly smaller than 272, so that only one case with LP relaxation 282.96 and $\#\,\mathrm{Aut} = 64$ remains, which is in only five $(7,33,5,\{3,4\})_2$ codes. This automorphism group of order 64 partitions the 127 non-zero vectors of $\mathbb{F}_2^7$ into 8 orbits of types: $1^1 2^1 4^3 16^1 32^1 64^1$. Thus, besides exact arithmetic clique computations, 75 LP computations and 40 BLP computation of DefaultCDCBLP$(2,8,6,4)$ with 33 forced codewords, one for each of the 8 orbit representatives and 5 extensions to $(7,33,5,\{3,4\})_2$ codes, suffices to deduce $\mathrm{A}_2(8,6;4) \le 272$.

Instead of decomposing the 563 isomorphism types of $(7,33,5;\{3,4\})_2$ codes into their components, we may also utilize the following BLP formulation.

197 Lemma
If C is a $(2k,\#C,2k-2;k)_q$ CDC containing the $(2k-1,q^k+1,2k-2;k-1)_q$ CDC F_{k-1} and $(2k-1,q^k,2k-2;k)_q$ CDC F_k in the hyperplane $\mathrm{im}(\iota)$ then $\#C \le z(F_{k-1},F_k)$, where $\iota : \mathbb{F}_q^{2k-1} \to \mathbb{F}_q^{2k}, v \mapsto (v \mid 0)$, $G := \begin{bmatrix}\mathbb{F}_q^{2k}\\ k\end{bmatrix}$, $Q := \begin{bmatrix}\mathbb{F}_q^{2k}\\ 1\end{bmatrix} \setminus \mathcal{I}\left(\begin{bmatrix}\mathbb{F}_q^{2k}\\ 1\end{bmatrix}, \mathrm{im}(\iota)\right)$, and

$$
\begin{aligned}
z(F_{k-1},F_k) = \max & \sum_{U\in G} x_U \\
\text{st} \quad & \sum_{U\in\mathcal{I}(G,A)} x_U \le 1 && \forall\, A \in \begin{bmatrix}\mathbb{F}_q^{2k}\\ a\end{bmatrix} \forall\, a \in \{2,2k-2\} \\
& \sum_{U\in\mathcal{I}(G,A)} x_U \le q^k+1 && \forall\, A \in \begin{bmatrix}\mathbb{F}_q^{2k}\\ a\end{bmatrix} \forall\, a \in \{1,2k-1\} \\
& \sum_{U'\in\iota(F_{k-1})} x_{\langle U',P\rangle} = y_P && \forall\, P \in Q \\
& \sum_{P\in Q} y_P = 1 \\
& x_U = 1 && \forall\, U \in \iota(F_k) \\
& x_U \in \{0,1\} && \forall\, U \in G \\
& y_P \in \{0,1\} && \forall\, P \in Q
\end{aligned}
$$

In fact Q may even be restricted to a transversal of points of the embedded stabilizer of F_k. Of course, we also obtain $z(F_3,F_4) \le 272$ in all 563 cases.

Given the bounds $\mathrm{A}_2(6,4;3) = 77 < 81$ and $\mathrm{A}_2(8,6;4) = 257 < 289$, one might conjecture that $\mathrm{A}_2(2k,2k-2;k)$ is much smaller than $\left(2^k+1\right)^2$, which is implied by the Johnson bound (Theorem 113) and Beutelspacher's result for partial spreads (Theorem 126), for

$k \ge 3$, i.e.,

$$\mathrm{A}_q(2k, 2k-2; k) \le \left\lfloor \frac{q^{2k}-1}{q^k-1} \mathrm{A}_2(2k-1, 2k-2; k-1) \right\rfloor$$
$$= (q^k+1)\left(\frac{q^{2k}-q^{k+1}}{q^k-1}+1\right) = (q^k+1)^2.$$

Unfortunately, those potential results cannot yield improvements when combined with the Johnson bound for $\mathrm{A}_q(2k+1, 2k-2; k)$.

198 Lemma

No improvement on the upper bound of $\mathrm{A}_q(2k, 2k-2; k)$ for $k \ge 3$ yields a stronger bound on $\mathrm{A}_q(2k+1, 2k-2; k)$ involving an application of Johnson IIa Theorem 113.

Proof

Due to the Johnson bound, $\mathrm{A}_q(2k, 2k-2; k-1) \le \frac{q^{2k}-1}{q^{k-1}-1}$, and $\mathrm{A}_q(2k, 2k-2; k) \ge q^{2k}+1$, i.e., a LMRD extended by one additional codeword, we have

$$\mathrm{A}_q(2k+1, 2k-2; k) \le \left\lfloor \frac{q^{2k+1}-1}{q^k-1} \mathrm{A}_q(2k, 2k-2; k-1) \right\rfloor \le \frac{q^{2k+1}-1}{q^k-1} \cdot \frac{q^{2k}-1}{q^{k-1}-1}$$
$$< \frac{q^{2k+1}-1}{q^{k+1}-1} \cdot q^{2k} \le \left\lfloor \frac{q^{2k+1}-1}{q^{k+1}-1} \cdot (q^{2k}+1) \right\rfloor \le \left\lfloor \frac{q^{2k+1}-1}{q^{k+1}-1} \mathrm{A}_q(2k, 2k-2; k) \right\rfloor. \quad \square$$

The main obstacle to use the same approach for the next parameters, i.e., the bound $1025 \le \mathrm{A}_2(10, 8; 5) \le 1089$, is that, up to our knowledge, the $(9, 33, 8; 4)_2$ CDCs have not been classified and not even $65 \le \mathrm{A}_2(9, 7; \{4, 5\}) \le 66$ could be determined.

13 Conclusion

In this thesis, we applied mainly techniques of integer linear programming to constant dimension codes to tighten bounds of maximum CDCs and to classify them.

We improve many lower bounds on this maximum size of CDCs with the coset construction, the improved linkage construction and additional sporadic cases. One of our constructions in the Echelon-Ferrers scheme is provably able to raise the ratio between lower bound and upper bound to approximately 61.6% for all parameters.

By proving new relations between known upper bounds, we compare them and in particular list all state-of-the-art upper bounds.

We also generalize bounds for CDCs containing lifted maximum rank distance codes.

By theoretical arguments and a computer search in the subgroup lattice of a finite group, we identified a comprehensive list of candidates for the automorphism group of CDCs in the setting of the binary q-Fano plane and get as byproduct a $(7, 333, 4; 3)_2$ CDC, which is the largest currently known CDC for these parameters.

We also classify maximum $(8, N, 6; 4)_2$ CDCs by a very involved computer search.

Despite or because of these achievements, there are open problems that seem to be reachable.

Although Proposition 99 settles many cases, there is still no LMRD bound for $q \geq 2$ prime power, $2 \leq d/2 \leq k \leq v - k$ integers, and $3d/2 \leq k$, cf. Figure 7. The ratio of LMRD bound and best known upper bound is still an open question. The methods of Section 6.4 are far from being exhausted and that may even be a hint for infinite series of large or even LMRD bound achieving codes.

In this thesis, we applied integer linear programming methods to CDCs. They may also be applied to subspace codes in a BLP similar to DefaultCDCBLP in Definition 47. A relaxation of binary linear programming is semidefinite programming and the techniques in this area may be applied instead or in addition to solve e.g. the subproblems arising of the evaluation function of our algorithm.

This leads to applications of this algorithm. Since it only needs a finite group G and a monotone and conjugation-invariant map on the set of subgroups of G to the co-domain $\{0, 1\}$, it is a very general tool to get a superset of interesting subgroups which then may be handled intensively in a post-processing step. Hence, there are countless application areas of which subspace code sizes are only the tip of the iceberg. One open issue is the time which is needed for the conjugation test of subgroups. Additionally, an implementation in `GAP` [GAP18] would be useful for easy usage and broad availability. Further automorphism groups may be excluded in theory.

The question of the size of the coset construction is still open, just like Ferrers diagram rank metric codes and the question of optimal skeleton codes. Solving these questions would imply many improved code sizes for a wide variety of parameters.

Being recursive in nature, the improved linkage construction would then profit of these advances and boost the code sizes even more. This construction depends, next to q, v, d, and k, on one additional parameter and maybe one can prove the optimal choice of this parameter. A first step in this direction is done by Lemma 141. This would be in particular useful since this allows then an explicit formula, which in turn could be compared to the upper bounds in terms of limit behaviour as demonstrated in Proposition 151.

14 Appendix

We use a special format when writing subspaces for a compact overview. Let p be a prime and $1 \le k \le v$ and $U \in \left[{v \atop k}\right]_p$ be the subspace in question. First, we use the RREF $M = \tau(U) \in \mathbb{F}_p^{k \times v}$, in which we represent each entry in the matrix with the canonical representative of $\mathbb{F}_p \cong \mathbb{Z}/(p \cdot \mathbb{Z})$ in $\{0, 1, \ldots, p-1\}$. Each column of M is then replaced by an integer which is the p-adic number with coefficients in this column, i.e., $M_{*,j}$ is replaced by $N_j = \sum_{i=1}^{k} M_{i,j} \cdot p^{i-1}$ for $j \in \{1, \ldots, v\}$. Finally, even the brackets and occasionally leading zeros, if v is obvious from the context, are omitted and usually, if each $N_j \le 9$, additionally the separating commata are omitted.

For example, the subspace

$$U = \tau^{-1} \begin{pmatrix} 0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \in \left[{7 \atop 3}\right]_2$$

is hence replaced by 0102004 or even 102004, if $v = 7$ is fixed.

Since we are encoding matrices in RREF, the k pivot columns are the first numbers $p^0, p^1, \ldots, p^{k-1}$ appearing in this order and no digit is larger than $\sum_{i=1}^{k} p^{i-1} = [k]_p$.

14.1 Appendix for $\mathrm{A}_2(7, 4; 3) \ge 333$

14.1.1 The *surviving* groups

By $G_{n,m}$ we denote the groups corresponding to Theorem 170. Here n denotes the order of $G_{n,m}$ and m is a consecutive index. To the right or bottom of each group $G_{n,m}$, we list the abstract type of $G_{n,m}$.

$$G_{1,1} = \langle I_7 \rangle$$

C_1

$$G_{2,1} = \left\langle \begin{pmatrix} 1&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&1&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle$$

C_2

$$G_{3,1} = \left\langle \begin{pmatrix} 1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle$$

C_3

$$G_{3,2} = \left\langle \begin{pmatrix} 1&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle$$

C_3

$$G_{4,1} = \left\langle \begin{pmatrix} 0&0&1&0&1&0&0 \\ 0&1&1&0&0&1&0 \\ 0&0&1&1&0&0&0 \\ 0&0&0&1&0&0&0 \\ 1&0&1&1&0&0&0 \\ 0&0&0&1&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&1&0&1&0 \\ 1&0&0&1&1&0&1 \\ 0&0&0&1&0&0&0 \\ 0&0&1&0&1&1&0 \\ 1&0&1&1&1&1&1 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle$$

$C_2 \times C_2$

$$G_{4,2} = \left\langle \begin{pmatrix} 1&0&0&1&0&1&0 \\ 1&0&0&1&1&1&1 \\ 0&0&1&1&0&1&0 \\ 1&0&1&1&0&0&0 \\ 1&0&1&0&1&0&0 \\ 1&0&1&0&0&1&0 \\ 0&1&1&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&1&1 \\ 1&1&1&1&0&1&0 \\ 1&1&1&0&0&1&1 \\ 1&0&1&1&1&1&0 \\ 1&0&1&0&0&1&0 \\ 1&0&1&0&1&0&0 \\ 1&1&0&1&1&1&0 \end{pmatrix} \right\rangle$$

$C_2 \times C_2$

$$G_{4,3} = \left\langle \begin{pmatrix} 1&1&0&0&0&1&0 \\ 1&1&1&1&1&0&0 \\ 0&1&1&0&0&1&0 \\ 1&0&1&0&1&0&0 \\ 1&0&1&1&0&0&0 \\ 1&0&1&1&1&1&0 \\ 0&1&0&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1&1&0&0 \\ 1&0&1&1&1&1&0 \\ 1&0&0&1&1&0&0 \\ 1&1&1&1&0&1&0 \\ 1&1&1&0&1&1&0 \\ 1&1&1&1&1&0&0 \\ 1&0&1&1&1&0&1 \end{pmatrix} \right\rangle$$

$C_2 \times C_2$

$$G_{4,4} = \left\langle \begin{pmatrix} 1&1&1&0&0&1&1 \\ 1&1&1&1&0&1&0 \\ 0&1&0&1&1&1&1 \\ 1&1&0&1&1&0&1 \\ 1&1&0&0&0&0&1 \\ 1&1&0&1&0&1&1 \\ 0&0&0&1&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1&1&0 \\ 0&0&1&0&0&1&1 \\ 1&0&0&1&0&1&0 \\ 0&1&1&1&0&1&1 \\ 0&1&1&0&1&1&1 \\ 0&1&1&1&1&0&1 \\ 1&0&1&0&1&1&1 \end{pmatrix} \right\rangle$$

$C_2 \times C_2$

$$G_{4,5} = \left\langle \begin{pmatrix} 1&1&1&0&1&0&1\\ 0&0&1&0&0&1&1\\ 0&1&0&1&0&0&1\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&1&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1&1&0\\ 0&0&1&0&0&1&1\\ 1&0&0&1&0&1&0\\ 0&1&1&1&0&1&1\\ 0&1&1&0&1&1&1\\ 0&1&1&1&1&0&1\\ 1&0&1&0&1&1&1 \end{pmatrix} \right\rangle \qquad C_2 \times C_2$$

$$G_{4,6} = \left\langle \begin{pmatrix} 0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0\\ 0&1&0&1&1&0&0\\ 0&1&0&0&0&0&0\\ 0&1&0&0&1&1&0\\ 1&0&1&1&1&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&0&0&1&0\\ 1&1&0&1&1&0&1\\ 0&1&1&0&0&1&0\\ 1&0&0&1&0&0&1\\ 1&0&0&0&1&0&1\\ 1&0&0&1&1&1&1\\ 0&1&0&0&0&1&1 \end{pmatrix} \right\rangle \qquad C_2 \times C_2$$

$$G_{4,7} = \left\langle \begin{pmatrix} 1&1&0&0&0&0&0\\ 0&1&1&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&1&1&0\\ 0&0&0&0&0&1&1\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_4$$

$$G_{5,1} = \left\langle \begin{pmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 1&1&1&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_5$$

$$G_{6,1} = \left\langle \begin{pmatrix} 0&1&0&0&1&1&0\\ 1&1&0&0&0&1&0\\ 0&1&1&1&1&0&0\\ 0&0&0&1&0&0&0\\ 1&0&0&0&1&1&0\\ 1&1&0&0&1&0&0\\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&1&1&0&0\\ 1&1&1&1&0&0&0\\ 0&1&0&0&1&1&0\\ 0&1&1&1&0&1&0\\ 0&0&1&1&0&0&0\\ 1&0&1&0&1&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad S_3$$

$$G_{6,2} = \left\langle \begin{pmatrix} 1&1&0&1&0&1&0\\ 1&1&0&1&1&0&0\\ 0&0&0&1&1&1&0\\ 1&1&1&0&0&0&0\\ 1&0&1&0&1&1&0\\ 0&1&1&0&1&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&0&1&0\\ 1&0&1&0&1&0&0\\ 0&0&0&0&1&1&0\\ 1&1&0&0&1&1&0\\ 1&0&0&0&0&0&0\\ 0&1&1&1&1&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad S_3$$

$$G_{6,3} = \left\langle \begin{pmatrix} 1&0&0&0&1&0&0\\ 1&0&0&1&1&1&0\\ 1&1&1&0&1&0&0\\ 1&0&1&1&1&0&0\\ 1&1&1&0&0&0&0\\ 0&1&1&0&1&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_6$$

$$G_{7,1} = \left\langle \begin{pmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 1&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_7$$

$$G_{7,2} = \left\langle \begin{pmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 1&0&1&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&1&0&1&0\\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_7$$

$$G_{8,1} = \left\langle \begin{pmatrix} 1&1&1&0&1&0&0\\ 1&0&0&0&0&1&0\\ 0&0&0&1&0&0&0\\ 0&0&1&0&0&0&0\\ 1&1&1&1&1&1&0\\ 1&0&1&0&1&0&0\\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1&1&1\\ 1&0&0&1&0&0&0\\ 1&1&0&0&0&0&1\\ 0&1&1&0&1&1&1\\ 0&0&1&1&1&0&1\\ 1&1&1&0&0&1&1\\ 1&0&0&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&1&1\\ 1&1&1&0&0&1&1\\ 1&0&0&0&0&1&1\\ 0&1&0&0&0&0&1\\ 0&0&0&0&1&0&0\\ 1&0&0&1&0&0&0\\ 1&1&1&1&0&1&1 \end{pmatrix} \right\rangle \qquad C_2 \times C_2 \times C_2$$

$$G_{8,2} = \left\langle \begin{pmatrix} 1&0&0&1&1&1&1\\ 0&0&1&1&0&1&1\\ 0&0&0&0&1&1&0\\ 0&1&1&1&1&0&0\\ 0&1&0&1&0&0&1\\ 0&1&1&1&0&0&1\\ 0&1&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&0&1&1&0\\ 0&0&1&0&1&0&0\\ 0&0&0&1&0&0&1\\ 0&0&0&0&1&1&1\\ 0&1&0&1&0&0&1\\ 0&1&1&0&1&1&0\\ 0&0&1&0&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&1&0&1\\ 1&0&0&0&0&1&1\\ 1&1&1&0&0&1&1\\ 1&0&1&1&0&1&1\\ 0&0&0&0&1&0&0\\ 1&0&0&1&1&0&0\\ 0&1&1&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_2 \times C_2 \times C_2$$

$$G_{8,3} = \left\langle \begin{pmatrix} 1&0&1&1&0&0&0\\ 1&0&0&0&1&1&1\\ 1&0&0&0&0&1&1\\ 0&0&0&1&1&0&0\\ 0&1&1&0&0&0&0\\ 0&0&0&0&1&1&1\\ 1&0&1&0&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&0&0&1\\ 1&0&0&0&0&1&1\\ 1&0&1&1&1&1&0\\ 1&0&0&0&1&1&0\\ 0&1&0&1&0&0&1\\ 1&1&1&1&0&0&0\\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&1&1&1\\ 0&1&1&1&0&0&1\\ 0&0&0&1&0&0&1\\ 0&1&1&1&1&0&0\\ 0&0&0&0&1&0&0\\ 1&1&0&0&0&0&1\\ 0&1&0&1&1&0&0 \end{pmatrix} \right\rangle \qquad C_4 \times C_2$$

$$G_{8,4} = \left\langle \begin{pmatrix} 1&0&0&1&1&1&1\\ 1&1&0&1&0&1&0\\ 1&1&1&0&0&1&1\\ 1&1&0&0&0&0&0\\ 1&0&1&0&0&1&1\\ 0&0&1&1&0&1&1\\ 0&1&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&1&1&0\\ 1&1&0&0&0&0&1\\ 0&0&0&0&0&1&0\\ 0&1&0&1&1&1&0\\ 0&0&0&0&1&0&0\\ 1&1&0&1&1&1&0\\ 0&1&1&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&0&0\\ 1&0&1&1&1&1&0\\ 1&1&0&1&1&1&0\\ 0&1&0&0&1&0&1\\ 0&0&0&0&1&0&0\\ 0&1&0&1&0&1&1\\ 1&0&1&0&0&1&0 \end{pmatrix} \right\rangle \qquad Q_8$$

$$G_{8,5} = \left\langle \begin{pmatrix} 0&0&1&0&0&1&1\\ 1&1&0&0&0&0&0\\ 0&0&0&0&1&1&1\\ 1&0&1&0&1&0&1\\ 1&1&1&1&1&1&0\\ 1&0&1&1&0&1&1\\ 1&1&0&0&1&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&1&1&0\\ 0&1&1&1&1&0&0\\ 0&1&0&0&0&0&1\\ 0&1&1&1&1&0&1\\ 1&0&1&0&0&1&1\\ 1&0&1&0&1&0&0\\ 1&1&1&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&1&0&1&0\\ 1&1&1&0&0&1&1\\ 1&0&0&0&0&1&1\\ 0&0&0&1&1&0&0\\ 0&0&0&0&1&0&0\\ 1&1&1&1&1&0&0\\ 1&0&1&0&1&1&0 \end{pmatrix} \right\rangle \qquad Q_8$$

$$G_{8,6} = \left\langle \begin{pmatrix} 1&1&0&1&1&0&1\\ 1&1&1&1&1&0&1\\ 1&1&0&0&0&0&0\\ 0&1&0&1&0&1&1\\ 0&1&0&1&0&0&1\\ 0&0&0&1&1&0&0\\ 1&0&1&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&1&1&0\\ 0&1&0&1&1&1&1\\ 0&0&0&0&1&1&0\\ 1&0&1&0&0&0&0\\ 0&0&1&1&1&0&1\\ 0&0&0&1&1&0&1\\ 1&0&0&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 1&1&0&1&1&0&1\\ 0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&0&1&1&0&0\\ 0&0&0&0&1&0&0\\ 0&1&0&1&0&1&1\\ 0&1&1&0&1&0&1 \end{pmatrix} \right\rangle \qquad D_8$$

$$G_{8,7} = \left\langle \begin{pmatrix} 0&0&1&0&0&1&1\\ 1&1&0&0&0&0&0\\ 1&1&0&0&1&0&0\\ 1&0&0&1&1&0&0\\ 0&1&1&0&0&0&0\\ 0&0&0&1&1&0&0\\ 0&1&1&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&1&1\\ 1&1&0&0&0&0&1\\ 1&1&1&1&1&0&0\\ 0&0&0&0&1&1&1\\ 0&1&0&1&0&0&1\\ 1&0&0&0&0&1&1\\ 1&1&0&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&1&1&0&0&1\\ 1&1&1&0&0&1&1\\ 1&0&0&0&0&1&1\\ 1&1&0&1&1&1&1\\ 0&0&0&0&1&0&0\\ 1&1&1&1&1&0&0\\ 0&1&1&0&1&0&1 \end{pmatrix} \right\rangle \qquad C_4 \times C_2$$

$$G_{8,8} = \left\langle \begin{pmatrix} 1&0&0&1&1&1&1\\ 1&1&0&1&0&1&0\\ 1&1&1&0&0&1&1\\ 1&1&0&0&0&0&0\\ 1&0&1&0&0&1&1\\ 0&0&1&1&0&1&1\\ 0&1&0&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0&1&0\\ 0&1&0&1&1&1&1\\ 1&0&0&1&1&0&0\\ 1&1&0&0&0&0&0\\ 0&0&0&0&1&0&0\\ 0&1&0&0&1&0&0\\ 0&1&1&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&0&0\\ 1&0&1&1&1&1&0\\ 1&1&0&1&1&1&0\\ 0&1&0&0&1&0&1\\ 0&0&0&0&1&0&0\\ 0&1&0&1&0&1&1\\ 1&0&1&0&0&1&0 \end{pmatrix} \right\rangle \qquad C_4 \times C_2$$

$$G_{8,9} = \left\langle \begin{pmatrix} 0&0&1&0&0&1&1\\ 1&1&1&0&0&1&1\\ 1&1&0&1&1&1&0\\ 1&0&0&0&0&1&0\\ 0&1&0&1&0&0&1\\ 0&0&1&1&0&1&1\\ 0&1&1&0&1&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&1&0&0&0&1\\ 0&1&0&1&0&1&1\\ 0&0&0&0&0&1&0\\ 1&1&1&0&0&1&0\\ 0&0&1&1&1&0&1\\ 0&0&1&0&0&0&0\\ 1&1&0&1&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0&1&0\\ 1&0&0&0&1&1&1\\ 1&1&1&0&1&1&1\\ 0&1&1&1&1&0&0\\ 0&0&0&0&1&0&0\\ 1&1&1&1&1&0&0\\ 1&0&1&0&0&1&0 \end{pmatrix} \right\rangle \qquad D_8$$

$$G_{8,10} = \left\langle \begin{pmatrix} 1&0&0&0&0&0&0\\ 0&0&1&0&1&0&0\\ 0&0&0&1&0&0&1\\ 1&0&0&0&0&1&0\\ 0&1&0&1&0&0&1\\ 1&0&0&1&0&0&0\\ 1&0&1&0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&0&1&1\\ 1&1&0&0&1&0&1\\ 1&0&0&1&1&0&0\\ 1&0&0&0&1&1&0\\ 0&0&1&1&1&0&1\\ 1&0&1&1&1&1&0\\ 0&0&1&0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1&0&1&0\\ 1&0&0&0&1&1&1\\ 1&1&1&0&1&1&1\\ 0&1&1&1&1&0&0\\ 0&0&0&0&1&0&0\\ 1&1&1&1&1&0&0\\ 1&0&1&0&0&1&0 \end{pmatrix} \right\rangle \qquad D_8$$

$$G_{8,11} = \left\langle \begin{pmatrix} 0&0&1&1&1&0&0 \\ 0&1&0&0&0&0&1 \\ 0&0&1&0&1&0&1 \\ 1&1&0&0&1&0&1 \\ 0&1&0&1&0&0&1 \\ 1&1&1&1&1&0&1 \\ 0&1&0&0&0&1&1 \end{pmatrix} \right\rangle \qquad C_8$$

$$G_{12,1} = \left\langle \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&0&0&1&1&0&1 \\ 1&1&1&1&1&0&0 \\ 1&1&0&0&1&1&0 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&1&1&1 \\ 0&0&0&0&1&0&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&0&0 \\ 1&1&0&0&0&1&1 \\ 1&0&1&0&1&0&1 \\ 1&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&1&1&1&1 \\ 1&0&1&1&1&0&0 \\ 1&1&0&0&0&1&1 \\ 1&0&0&0&1&0&0 \\ 1&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0 \end{pmatrix} \right\rangle \qquad C_3 \rtimes C_4$$

$$G_{9,1} = \left\langle \begin{pmatrix} 1&0&1&1&0&1&0 \\ 1&0&1&1&1&0&0 \\ 0&0&1&1&1&0&0 \\ 1&1&0&0&1&1&0 \\ 1&1&0&1&1&0&0 \\ 0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_9$$

$$G_{14,1} = \left\langle \begin{pmatrix} 0&1&1&1&1&0&0 \\ 0&1&1&0&0&0&0 \\ 0&1&1&0&1&0&0 \\ 0&1&0&0&0&0&0 \\ 0&0&1&0&1&1&0 \\ 1&0&1&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_{14}$$

$$G_{9,2} = \left\langle \begin{pmatrix} 0&1&0&0&0&1&0 \\ 1&0&0&0&0&1&0 \\ 0&1&1&0&0&1&0 \\ 1&1&0&0&1&0&0 \\ 1&1&0&1&1&0&0 \\ 0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&0&1&0 \\ 1&0&1&0&0&0&0 \\ 1&0&1&0&0&1&0 \\ 0&1&1&1&1&0&0 \\ 0&0&0&1&0&1&0 \\ 0&1&1&0&0&1&0 \\ 0&0&0&0&0&0&1 \end{pmatrix} \right\rangle \qquad C_3 \times C_3$$

$$G_{16,1} = \left\langle \begin{pmatrix} 0&0&1&0&1&0&0 \\ 1&0&0&0&1&0&0 \\ 0&0&0&1&0&1&0 \\ 0&1&0&0&0&0&1 \\ 1&0&1&0&1&1&1 \\ 1&0&1&0&0&1&0 \\ 0&0&1&1&1&1&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&1&0&1&1 \\ 1&0&1&1&1&0&1 \\ 0&1&1&1&1&1&0 \\ 0&0&1&1&0&1&0 \\ 1&1&1&1&0&1&0 \\ 1&0&0&1&0&1&1 \\ 0&0&1&0&0&0&0 \end{pmatrix} \right\rangle \qquad (C_4 \times C_2) \rtimes C_2$$

14.1.2 The code of size 333 in the binary Fano setting

The code of size 333 is printed below. Since the group $G_{4,6}$ of Appendix 14.1.1 is its automorphism group we print only one representative in each orbit. The orbit type is $1^9 2^{26} 4^{68}$.

9 fixed subspaces:

0124412
1012460
1124633
1204601
1213457
1214425
1224713
1240020
1242770

26 representatives of orbits of length 2:

0102140
1024453
1112434
1122124
1123346
1204571
1210410
1211460
1212473
1214336
1230426
1241116
1242375
1242415
1242577
1243345
1243422
1243774
1244105
1244164
1244225
1245130
1245346
1245505
1245775
1246357

68 representatives of orbits of length 4:

0102004
0102467
0110224
0111240
0112034
0120240
0121457
0122241
0122344
0124161
0124435
0124473
1002146
1002342
1002427
1012413
1020467
1021034
1021247
1024355
1024446
1102204
1102452
1121430
1122405
1124210
1124231
1200314
1202246
1202422
1203413
1210324
1210475
1211415
1212142
1214026
1214507
1220433
1224217
1224605
1231465
1234241
1234413
1234610
1240266
1240416
1241157
1241265
1241533
1242430
1242672
1243544
1243727
1244067
1244343
1244401
1244606
1245122
1245311
1245663
1246050
1246073
1246134
1246240
1246517
1247007
1247404
1247754

14.2 Appendix for $\mathrm{A}_2(8,6;4) = 257$

In Table 12, we list the 38 $(7,16,6;3)_2$ and $(7,17,6;3)_2$ CDCs with $z_8^{\mathrm{LP}}(.) \geq 256.9$. Table 11 lists for these CDCs whether it is in $\mathcal{A}_{16}$ or $\mathcal{A}_{17}$, the size of their automorphism group, the relaxations $z_8^{\mathrm{LP}}(.)$ and $z_7^{\mathrm{BLP}}(.)$, which are applied to the hyperplane configurations, then the orbits of the extension to point-hyperplane configurations of each hyperplane configuration and finally the maximum of $z_8^{\mathrm{LP}}(.)$ with prescribed point-hyperplane configuration grouped by the contained hyperplane configuration and, if needed, the maximum $z_8^{\mathrm{LP}}(.)$, again for prescribed point-hyperplane configuration grouped by the contained hyperplane configuration. Details for the extension of one of the first seven hyperplane configurations to all point-hyperplane configurations is depicted in Table 10.

			Wall-time in hours for	
i	$\#V_i$	Phase 2	LP in Phase 3	BLP in Phase 3
1	1231	144	51	328
2	1303	589	78	
3	1194	217	21	519
4	1243	278	22	
5	1258	750	419	
6	1251	209	13	
7	864	27	349	4

Table 10: Details for the computation of all 31-point-hyperplane configurations in Phase 2 and Phase 3.

14.3 The `Magma` implementation corresponding to Section 11.6

An implementation of the pseudo code of Section 11.2.1 in `Magma`

```
////////////////////
// functions for saving intermediate results to files for a reentrant
   algorithm
////////////////////

function FileHelper(fname,func,args : mode:="associativearray")
 assert mode in ["associativearray","array"];

 // try to get storage from file
 try
  storage := eval(Read(fname));
 catch e // storage does not exist
  if mode eq "associativearray" then
   storage := AssociativeArray(Parent(args));
```

Index	Type	Aut	$z_8^{\mathrm{LP}}(.)$	$z_7^{\mathrm{BLP}}(.)$	Orbits of Phase 2	$\max z_8^{\mathrm{LP}}(\text{“31”})$	$\max z_8^{\mathrm{BLP}}(\text{“31”})$
1	16	960	272	271.1856	$16^2, 240^6, 480^{47}, 960^{242}$	263.0287799	257
2	16	384	266.26086957	267.4646	$96^6, 192^{91}, 384^{711}$	206.04279728	
3	16	4	270.83786676	265.3281	$1^{13}, 2^{29}, 4^{2638}$	257.20717665	254
4	16	48	271.43451032	262.082	$4^3, 12^{11}, 24^{59}, 48^{1104}$	200.5850228	
5	16	2	263.8132689	259.8044	$1^5, 2^{59966}$	206.39304042	
6	16	20	267.53272206	259.394	$5, 10^9, 20^{1843}$	199.98690666	
7	17	64	282.96047431	259.1063	$16^{10}, 32^{145}, 64^{6293}$	259.45364626	257
8	17	32	268.0388109	257.2408			
9	16	1	263.82742528	256.392			
10	16	1	263.36961743	255.8305			
11	16	1	264.25957151	≤ 254			
12	16	1	263.85869815	≤ 254			
13	16	2	263.07052878	≤ 254			
14	16	12	261.91860556	≤ 254			
15	16	4	261.62648174	≤ 254			
16	16	12	261.31512837	≤ 254			
17	17	4	261.11518721	≤ 254			
18	16	1	260.96388752	≤ 254			
19	16	1	260.82432878	≤ 254			
20	16	2	260.65762276	≤ 254			
21	16	4	260.43036283	≤ 254			
22	16	2	260.19475349	≤ 254			
23	16	1	260.08583792	≤ 254			
24	16	1	260.04857193	≤ 254			
25	16	1	259.75041996	≤ 254			
26	16	2	259.55230081	≤ 254			
27	16	2	259.46335297	≤ 254			
28	16	12	259.11945025	≤ 254			
29	16	1	258.89395938	≤ 254			
30	17	24	258.75142045	≤ 254			
31	16	8	258.35689437	≤ 254			
32	16	1	257.81420526	≤ 254			
33	16	2	257.75126819	≤ 254			
34	16	4	257.63965018	≤ 254			
35	16	1	257.57663803	≤ 254			
36	16	1	257.2820438	≤ 254			
37	16	4	257.01931801	≤ 254			
38	17	128	257	≤ 254			

Table 11: Details for the 38 $(7,16,6;3)_2$ and $(7,17,6;3)_2$ CDCs with $z_8^{\mathrm{LP}}(.) \geq 256.9$.

Index	16 or 17 planes in $\mathbb{F}_2^7$
1	1240000,1240124,1241062,1241146,1242463,1242547,1243401,1243525,1244635,1244711,1245657,1245773,1246256,1246372,1247234,1247310
2	1240000,1240124,1241062,1241146,1242647,1242763,1243625,1243701,1244234,1244310,1245256,1245372,1246473,1246557,1247411,1247535
3	124,1240000,1240124,1241447,1241563,1242631,1242715,1243276,1243352,1244230,1244314,1245753,1246401,1246525,1247046,1247162
4	1240000,1240524,1241042,1241566,1242237,1242403,1243165,1243751,1244270,1244354,1245632,1245716,1246127,1246313,1247441,1247675
5	124,1240124,1241046,1241162,1242637,1242713,1243671,1243755,1244230,1244314,1245276,1245352,1246407,1246523,1247441,1247565
6	1240000,1240124,1241370,1241757,1242605,1242721,1243276,1243451,1244017,1244133,1245263,1245345,1246534,1246612,1247446,1247562
7	124,124000,124124,1024062,1024146,1214452,1214746,1224403,1224727,1241572,1241633,1242557,1242615,1245461,1245724,1246476,1246730
8	124,124000,124124,1024062,1024146,1214546,1214652,1224503,1224627,1241471,1241730,1242416,1242754,1245527,1245662,1246575,1246633
9	124,1240000,1240124,1241157,1242634,1242756,1243673,1243710,1244211,1244335,1245262,1245347,1246463,1246501,1247425,1247546
10	124,1240000,1240124,1241072,1241157,1242634,1242756,1243673,1243710,1244211,1244335,1245347,1246463,1246501,1247425,1247546
11	124,1240000,1241072,1241157,1242634,1242756,1243673,1243710,1244211,1244335,1245262,1245347,1246463,1246501,1247425,1247546
12	124,1240000,1240124,1241072,1241157,1242634,1242756,1243673,1243710,1244211,1245262,1245347,1246463,1246501,1247425,1247546
13	124,1240000,1240124,1241241,1241630,1242415,1242561,1243166,1244023,1244452,1245613,1245737,1246354,1246775,1247206,1247372
14	124,1240000,1240124,1241241,1241630,1242415,1242561,1243166,1243547,1244023,1244452,1245737,1246354,1246775,1247206,1247372
15	124,1240000,1241437,1241513,1242661,1242745,1243252,1243376,1244230,1244314,1245647,1245763,1246051,1246175,1247422,1247506
16	124,1240000,1241241,1241630,1242415,1242561,1243166,1243547,1244023,1244452,1245613,1245737,1246354,1246775,1247206,1247372
17	124,124000,124124,1024466,1024553,1204267,1204342,1234506,1234713,1240570,1240721,1243437,1243565,1245042,1245126,1246453,1246634
18	124,1240000,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
19	124,1240000,1240124,1241367,1241446,1242521,1243243,1243562,1244076,1244757,1245311,1245734,1246150,1246673,1247235,1247412
20	124,1240000,1240124,1241367,1241446,1242521,1242605,1243243,1243562,1244757,1245311,1245734,1246150,1246673,1247235,1247412
21	124,1240000,1240124,1241367,1241446,1242521,1242605,1243243,1243562,1244076,1244757,1245311,1245734,1246150,1247235,1247412
22	124,1240000,1240124,1241664,1241740,1242427,1242503,1243165,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
23	124,1240000,1240124,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247311
24	124,1240000,1240124,1241367,1241446,1242521,1242605,1243243,1244076,1244757,1245311,1245734,1246150,1246673,1247235,1247412
25	124,1240000,1240124,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1247235,1247311
26	124,1240000,1240124,1241664,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
27	124,1240000,1240124,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
28	124,1240000,1240124,1241437,1241513,1242661,1242745,1243376,1244230,1244314,1245647,1245763,1246051,1246175,1247422,1247506
29	124,1240124,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
30	124,124000,124124,1024341,1024630,1204526,1204653,1234367,1234644,1240046,1240135,1243474,1243726,1245237,1245664,1246512,1246605
31	124,1240000,1240124,1241057,1241173,1242655,1242771,1243602,1243726,1244230,1244314,1245267,1245343,1246465,1246541,1247516
32	124,1240000,1240124,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1245516,1245632,1246372,1246451,1247235,1247311
33	124,1240000,1240124,1241664,1241740,1242427,1242503,1243243,1244076,1244757,1245516,1245632,1246372,1246451,1247235,1247311
34	124,1240000,1240124,1241367,1241446,1242521,1242605,1243243,1243562,1244076,1244757,1245311,1245734,1246673,1247235,1247412
35	124,1240000,1240124,1241367,1241446,1242521,1242605,1243243,1243562,1244076,1244757,1245311,1245734,1246150,1246673,1247235
36	124,1240000,1240124,1241664,1241740,1242427,1242503,1243165,1243243,1244076,1244757,1245632,1246372,1246451,1247235,1247311
37	10024,1202436,1211471,1221433,1232464,1240776,1243450,1243712,1244143,1244522,1245307,1245660,1246021,1246615,1247267,1247546
38	124,124000,124124,1024062,1024146,1214466,1214772,1224437,1224713,1241561,1241620,1242574,1242636,1245407,1245742,1246423,1246765

Table 12: The 38 $(7,16,6;3)_2$ and $(7,17,6;3)_2$ CDCs with $z_8^{\mathrm{LP}}(.) \geq 256.9$.

```
  else
   storage := [];
  end if;
 end try;

 // look up for args
 if mode eq "associativearray" then
  if IsDefined(storage, args) then
   return storage[args];
  end if;
 else
  findme := [i[2] : i in storage | i[1] eq args];
  if #findme ge 1 then
   return findme[1];
  end if;
 end if;

 // args not processed previously
 ret := func(args);

 if mode eq "associativearray" then
  storage[args]:=ret;
 else
  Append(~storage,<args,ret>);
 end if;

 Write(fname, storage, "Magma" : Overwrite:=true);
 return ret;
end function;

////////////////////
// (non) solvable numbers
////////////////////

// https://oeis.org/A056866:
// A positive integer n is a non-solvable number if and only if it is a
   multiple of any of the following numbers:
// a) 2^p(2^2p-1), p any prime.
// b) 3^p(3^2p-1)/2, p odd prime.
// c) p(p^2-1)/2, p prime greater than 3 such that p^2+1 = 0 (mod 5).
// d) 2^4*3^3*13.
// e) 2^2p(2^2p+1)(2^p-1), p odd prime.

function IsNonSolvableNumber_helper_a(n)
 p := 2;
 while true do
  t := 2^p*(2^(2*p)-1);
  if (n mod t) eq 0 then
   return true;
  end if;
  if t gt n then
   return false;
  end if;
  p := NextPrime(p);
```

```
 end while;
end function;

function IsNonSolvableNumber_helper_b(n)
 p := 3;
 while true do
  t := Integers() ! (3^p*(3^(2*p)-1)/2);
  if (n mod t) eq 0 then
   return true;
  end if;
  if t gt n then
   return false;
  end if;
  p := NextPrime(p);
 end while;
end function;

function IsNonSolvableNumber_helper_c(n)
 p := 7;
 while true do
  t := Integers() ! (p*(p^2-1)/2);
  if ((p^2+1) mod 5 eq 0) and ((n mod t) eq 0) then
   return true;
  end if;
  if t gt n then
   return false;
  end if;
  p := NextPrime(p);
 end while;
end function;

function IsNonSolvableNumber_helper_d(n)
 return (n mod 5616) eq 0;
end function;

function IsNonSolvableNumber_helper_e(n)
 p := 3;
 while true do
  t := 2^(2*p)*(2^(2*p)+1)*(2^p-1);
  if (n mod t) eq 0 then
   return true;
  end if;
  if t gt n then
   return false;
  end if;
  p := NextPrime(p);
 end while;
end function;

function IsNonSolvableNumber(n)
 if ((n mod 20) ne 0) and ((n mod 12) ne 0) then
  return false;
 end if;
 return IsNonSolvableNumber_helper_a(n)
```

```
     or IsNonSolvableNumber_helper_b(n)
     or IsNonSolvableNumber_helper_c(n)
     or IsNonSolvableNumber_helper_d(n)
     or IsNonSolvableNumber_helper_e(n);
end function;

function IsSolvableNumber(n)
 return not IsNonSolvableNumber(n);
end function;

// Tests
// non_solvable_orders := [60, 120, 168, 180, 240, 300, 336, 360, 420, 480,
     504, 540, 600, 660, 672, 720, 780, 840, 900, 960, 1008, 1020, 1080,
    1092, 1140, 1176, 1200, 1260, 1320, 1344, 1380, 1440, 1500];
// t := Cputime();
// for i in [1..1500] do
//   if (i in non_solvable_orders and (not IsNonSolvableNumber(i))) or ((not
     i in non_solvable_orders) and IsNonSolvableNumber(i)) then
//    i;
//   end if;
//   if (i mod 300) eq 0 then
//    "->",i;
//   end if;
// end for;
// Cputime(t);

////////////////////
// utility functions
////////////////////

function CyclicGroupGenerator(U)
 assert IsCyclic(U);
 return [ i : i in U | Order(i) eq Order(U) ][1];
end function;

function IsConjugateHelperGroups(G,A,B)
 assert A subset G;
 assert B subset G;

 if Order(A) ne Order(B) then
  return false;
 end if;

 if CanIdentifyGroup(Order(A)) then // also B identifyable
  if IdentifyGroup(A) ne IdentifyGroup(B) then
   return false;
  end if;
 end if;

 if IsCyclic(A) then // also B cyclic
  if Type(A.1) eq GrpMatElt then // also B.1 GrpMatElt
   if Dimension(Eigenspace(CyclicGroupGenerator(A),1)) ne Dimension(
       Eigenspace(CyclicGroupGenerator(B),1)) then
    return  false;
```

```
   end if;
  end if;
 end if;

 return IsConjugate(G,A,B);
end function;

function IsConjugateHelperElements(G,a,b)
 assert a in G;
 assert b in G;

 if Order(a) ne Order(b) then
  return false;
 end if;

 if Type(a) eq GrpMatElt then // also b GrpMatElt
  if Dimension(Eigenspace(a,1)) ne Dimension(Eigenspace(b,1)) then
   return  false;
  end if;
 end if;

 return IsConjugate(G,a,b);
end function;

function IsConjugateHelperSubgroupsConjugate(G,A,B)
 assert A subset G;
 assert B subset G;
 assert Order(B) le Order(A);

 if Order(A) eq Order(B) then
  return IsConjugateHelperGroups(G,A,B);
 end if;

 SGC := { i`subgroup : i in SubgroupClasses( A : OrderEqual:=Order(B) ) };

 for i in SGC do
  if IsConjugateHelperGroups(G,i,B) then
   return true;
  end if;
 end for;

 return false;
end function;

function FilterListOfGroupsForConjugates(G,L)
 R:=[];
 for i in [1..#L] do
  for j in [i+1..#L] do
   if IsConjugateHelperGroups(G,L[i],L[j]) then
    // continue can be used since the conjugation is transitive
    continue i;
   end if;
  end for;
  Append(~R,L[i]);
```

```
 end for;
 return R;
end function;

procedure FilterListOfCyclicGroupsNotNecessarySameOrderForConjugates(G,~L :
     AssumeNoElementWiseConjugation:=false)
 start := 1;
 if AssumeNoElementWiseConjugation then
  start := 2;
 end if;

 i:=0;
 while true do
  i +:= 1;
  if i gt #L then
   return;
  end if;
  j := i+1;
  while true do
   if j gt #L then
    break;
   end if;
   if Order(L[i]) eq Order(L[j]) then
    for z in [start..Order(L[i])] do
     if GCD(z,Order(L[i])) ne 1 then
      continue;
     end if;
     if IsConjugateHelperElements(G, CyclicGroupGenerator(L[i])^z,
         CyclicGroupGenerator(L[j])) then
      Remove(~L,j);
      break;
     end if;
    end for;
   end if;
   j +:= 1;
  end while;
 end while;
end procedure;

// G ambient group
// A subgroup to use for ascension
// p prime, i.e., we generate groups U of size #A * p with A <= U
function AscendSubgroupLattice_NoCheck(G,A,p)
 assert IsPrime(p);
 assert (Order(G) mod p) eq 0;
 assert A subset G;
 // assert p le Minimum(Factorization(Order(A)))[1]; // normality criterion
      of Strong Cayley theorem

 N  := Normalizer(G,A);
 CN := SetToSequence({ sub<G|i[3]> : i in ConjugacyClasses(N) | ((Order(A)*
     p mod i[1]) eq 0) and (not i[3] in A) and (Order(sub<G|Generators(A)
     join {i[3]}>) eq Order(A)*p)});
 L  := {@ sub<G|Generators(A) join {CyclicGroupGenerator(i)}> : i in CN @};
```

```
 return L;
end function;

// G ambient group
// A subgroup to use for ascension
// p prime, i.e., we generate groups U of size #A * p with A <= U
function AscendSubgroupLattice(G,A,p)
 assert p le Minimum(Factorization(Order(A)))[1]; // normality criterion of
      Strong Cayley theorem
 return AscendSubgroupLattice_NoCheck(G,A,p);
end function;

// we assume that if a cyclic group of order o is in possiblesgc of
    excludedsgc,
// then all representatives of conjugacy classes of cyclic groups of order
    o are either in possiblesgc of excludedsgc
function FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc,
     excludedsgc, collectionsgtotest)
 if Type(G) ne GrpMat then
  return collectionsgtotest;
 end if;
 all_cyclic_group_orders := {Order(i) : i in possiblesgc | IsCyclic(i)}
                        join {Order(i) : i in excludedsgc | IsCyclic(i)};
 filter := AssociativeArray(Integers());
 for o in all_cyclic_group_orders do
  pos_o      := { i : i in possiblesgc | Order(i) eq o and IsCyclic(i)};
  forb_o     := { i : i in excludedsgc | Order(i) eq o and IsCyclic(i)};
  eig_pos_o  := { Dimension(Eigenspace(CyclicGroupGenerator(i),1)) : i in
      pos_o };
  eig_forb_o := { Dimension(Eigenspace(CyclicGroupGenerator(i),1)) : i in
      forb_o };
  filter[o]  := eig_forb_o diff eig_pos_o;
 end for;
 R := [];
 for U in collectionsgtotest do
  for o in all_cyclic_group_orders do
   if (Order(U) mod o) ne 0 then
    continue;
   end if;
   all_conclasses_o     := { i[3] : i in ConjugacyClasses(U) | i[1] eq o };
   eig_all_conclasses_o := { Dimension(Eigenspace(i,1)) : i in
       all_conclasses_o };
   if (# (eig_all_conclasses_o meet filter[o])) ge 1 then
    continue U;
   end if;
  end for;
  Append(~R,U);
 end for;
 return R;
end function;

// e.g.:
// ComputeListOfCandidateSubgroups(GL(5,2),2^1,[],[]);
// ComputeListOfCandidateSubgroups(GL(5,2),31^1,[],[]);
```

```
// a:=ComputeListOfCandidateSubgroups(GL(5,2),2^1,[],[]);
// ComputeListOfCandidateSubgroups(GL(5,2),2^2,[a[1]],[]);
// ComputeListOfCandidateSubgroups(SymmetricGroup(4), 12, [PermutationGroup
    <4|[4,3,2,1],[3,4,1,2]:Order:=4>,PermutationGroup
    <4|[1,2,4,3],[1,3,4,2]:Order:=6>], []);
function ComputeListOfCandidateSubgroups(G, targetorder, possiblesgc,
   excludedsgc : use_expensive_conjugation_tests:=true)
 if targetorder eq 1 then
  return [sub<G|Id(G)>];
 end if;

  // Sylow group
 b,p,e := IsPrimePower(targetorder);
 if b and (Order(G) mod (p^(e+1))) ne 0 then
  SC := [SylowSubgroup(G,p)];
  SC := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc,
      excludedsgc, SC);
  return SC;
 end if;

 // fast way to get groups of prime order
 if IsPrime(targetorder) then
  CC := SetToSequence({ sub<G|i[3]> : i in ConjugacyClasses(G) | i[1] eq
      targetorder });
  if use_expensive_conjugation_tests then
   FilterListOfCyclicGroupsNotNecessarySameOrderForConjugates(G,~CC :
       AssumeNoElementWiseConjugation:=true);
  end if;
  return CC;
 end if;

 FactTargetorder := Factorization(targetorder);
 // targetorder = p^y or p^1 N such that N is not divisible by p and all
    prime factors of N are larger than p and targetorder is a solvable
    number
 if (#FactTargetorder eq 1) or (FactTargetorder[1][2] eq 1 and (#
    FactTargetorder le 2 or IsSolvableNumber(targetorder))) then
  p  := FactTargetorder[1][1];
  SC := &join[AscendSubgroupLattice(G,i,p) : i in possiblesgc | Order(i) eq
       (targetorder / p) ];
  SC := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc,
      excludedsgc, SC);
  if use_expensive_conjugation_tests then
   SC := FilterListOfGroupsForConjugates(G,SC);
  end if;
  return SC;
 end if;

 if IsInSmallGroupDatabase(targetorder) then
  AllTargetOrderAbstractGroups := SmallGroups(targetorder);
  try
   // ": IsNormal:=true" does sometimes raise an exception: Parameter '
       IsNormal' is not defined for this function
```

```
   AllTargetOrderAbstractGroups_NormalSubgroups_Orders := [ [j`order : j in
        SubgroupClasses( i : IsNormal:=true )] : i in
       AllTargetOrderAbstractGroups ];
  catch e
   AllTargetOrderAbstractGroups_NormalSubgroups_Orders := [ [j`order : j in
        SubgroupClasses(i) | IsNormal(i,j`subgroup)] : i in
       AllTargetOrderAbstractGroups ];
  end try;
  AllTargetOrderAbstractGroups_NormalSubgroups_Orders_IndexPrime :=
   { { j : j in i | IsPrime( Integers() ! (targetorder/j) ) } : i in
       AllTargetOrderAbstractGroups_NormalSubgroups_Orders };

  if &and[ #i ge 1 : i in
      AllTargetOrderAbstractGroups_NormalSubgroups_Orders_IndexPrime ] then
   // use the largest normal subgroup with prime index for ascension (
       prime index does not have to be _smallest_ prime divisor of
       targetorder )
   OrdersToUseForAscension := { Maximum(i) : i in
       AllTargetOrderAbstractGroups_NormalSubgroups_Orders_IndexPrime };
   SC := &join[AscendSubgroupLattice_NoCheck(G,i,Integers() ! (targetorder/
       Order(i))) : i in possiblesgc | Order(i) in OrdersToUseForAscension
       ];
   SC := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc,
        excludedsgc, SC);
   if use_expensive_conjugation_tests then
    SC := FilterListOfGroupsForConjugates(G,SC);
   end if;
   return SC;
  end if;
 end if;

 //fallback
 SC := [ i`subgroup : i in Subgroups(G : OrderEqual:=targetorder) ];
  SC := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc,
      excludedsgc, SC);
  return SC;
end function;

function ComputeListOfCandidateSubgroups_Caller(
    G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests)
 return ComputeListOfCandidateSubgroups(
  G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests[1],
  G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests[2],
  G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests[3],
  G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests[4]
  : use_expensive_conjugation_tests:=
  G_targetorder_possiblesgc_excludedsgc_use_expensive_conjugation_tests[5])
      ;
end function;

function HallDivisors(ord)
 return { &*i : i in Subsets( { i[1]^i[2] : i in Factorization(ord) } ) };
end function;
```

```
function ContainsExcludedSubgroupUpToConjugacy(G, excludedsgc, U)
 toconsider := { i : i in excludedsgc | (Order(U) mod Order(i) eq 0) and (
     Order(i) ne Order(U)) };
 if &or[ i subset U : i in toconsider ] then
  return true;
 end if;
 for i in toconsider do
  if IsConjugateHelperGroups(G,U,i) then
   return true;
  end if;
 end for;
 return false;
end function;

////////////////////
// main functions
////////////////////

function SearchSubgroupLattice_PGroups(G, evalfunc :
    use_expensive_conjugation_tests:=true, fname_saved_SC:="saved_SC.txt",
    fname_saved_evals:="saved_evals.txt", verbose:=true,
    SubgroupClassesInfusion:=[])
 MaximumPrimePowers := [];
 excludedsgc        := [];
 possiblesgc        := [sub<G|Id(G)>];
 name_counter       := 1;
 indices            := [];
 FactOrderG         := Factorization(Order(G));
 if verbose then
  globaltime      := Realtime();
  "II: Factorization of group order =", FactOrderG;
 end if;

 // from large to small primes, this order is arbitrary
 for pcounter := #FactOrderG to 1 by -1 do
  p                               := FactOrderG[pcounter][1];
  IsSylowPGroupPossible           := true;
  LargestPrimePowerDividingOrderG := FactOrderG[pcounter][2];
  for ecounter in [1..LargestPrimePowerDividingOrderG] do
   if verbose then
    "################";
    "# processing all subgroups of order =", p^ecounter;
    "################";
   end if;
   MaximumNotCompleteExcludedPrimePowerThisPrime := ecounter;
   if ecounter eq LargestPrimePowerDividingOrderG and IsSylowPGroupPossible
       eq false then
    if verbose then
     "II: at least one subgroup was excluded which implies by monotonicity
         that the Sylow p-group is excluded";
    end if;
    MaximumNotCompleteExcludedPrimePowerThisPrime :=
        MaximumNotCompleteExcludedPrimePowerThisPrime-1;
    break;
```

```
end if;

if verbose then
 "II: compute subgroup conjugacy classes";
 t  := Cputime();
end if;
if p^ecounter in [Order(i[1]) : i in SubgroupClassesInfusion] then
 if verbose then
  "II: using subgroup classes from infusion";
 end if;
 idx := Index([Order(i[1]) : i in SubgroupClassesInfusion], p^ecounter);
 SC  := SubgroupClassesInfusion[idx];
 SC  := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G,
     possiblesgc, excludedsgc, SC);
elif fname_saved_SC eq "" then
 SC  := ComputeListOfCandidateSubgroups_Caller(<G, p^ecounter,
     possiblesgc, excludedsgc, use_expensive_conjugation_tests>);
else
 SC  := FileHelper(fname_saved_SC,
     ComputeListOfCandidateSubgroups_Caller, <G, p^ecounter, possiblesgc
     , excludedsgc, use_expensive_conjugation_tests>);
end if;
if verbose then
 "II: computed subgroup conjugacy classes in ", Cputime(t);
 "II: # subgroup conjugacy classes =", #SC;
end if;

AtLeastOneSubgroupClassIncluded := false;
for sccounter in [1..#SC] do
 if verbose then
  "II: progress", sccounter, "of", #SC;
 end if;
 U := SC[sccounter];

 if use_expensive_conjugation_tests then
  if ContainsExcludedSubgroupUpToConjugacy(G,excludedsgc,U) then
   if verbose then
    "II: contains an excluded subgroup up to conjugacy";
   end if;
   continue;
  end if;
 end if;

 if verbose then
  t   := Realtime();
 end if;
 if fname_saved_evals eq "" then
  ret := evalfunc(<U, name_counter>);
 else
  ret := FileHelper(fname_saved_evals, evalfunc, <U, name_counter>);
 end if;
 if verbose then
  "II: eval took (real time)", Realtime(t), "and was", ret;
 end if;
```

```
    name_counter +:= 1;

    if ret then
     AtLeastOneSubgroupClassIncluded := true;
     Append(~possiblesgc, U);
     Append(~indices,name_counter-1);
    else
     IsSylowPGroupPossible := false;
     Append(~excludedsgc, U);
    end if;
   end for;

   if AtLeastOneSubgroupClassIncluded eq false then
    if verbose then
     "II: all subgroup conjugacy classes are excluded, hence skip larger p-
         groups";
    end if;
    MaximumNotCompleteExcludedPrimePowerThisPrime :=
        MaximumNotCompleteExcludedPrimePowerThisPrime-1;
    break;
   end if;

  end for;

  Append(~MaximumPrimePowers, <p,
      MaximumNotCompleteExcludedPrimePowerThisPrime>);
 end for;

 // Write("save_SearchSubgroupLattice_PGroups.txt",<MaximumPrimePowers,
     excludedsgc,possiblesgc,name_counter,indices>,"Magma" : Overwrite:=
     true);

 if verbose then
  "II: SearchSubgroupLattice_PGroups total real time", Realtime(globaltime)
      ;
 end if;
 return MaximumPrimePowers,excludedsgc,possiblesgc,name_counter,indices;
end function;

function SearchSubgroupLattice_NonPGroups(G, evalfunc, MaximumPrimePowers,
    excludedsgc, possiblesgc, name_counter, indices :
    use_expensive_conjugation_tests:=true, fname_saved_SC:="saved_SC.txt",
    fname_saved_evals:="saved_evals.txt", verbose:=true,
    SubgroupClassesInfusion:=[])
 CompletelyExcludedOrders        := {};
 CompletelyExcludedAbstractTypes := {};
 if verbose then
  globaltime                     := Realtime();
 end if;

 // initialize CompletelyExcludedAbstractTypes using groups og prime power
     order
 for o in {Order(i) : i in possiblesgc} do
  if IsInSmallGroupDatabase(o) then
```

```
  CompletelyExcludedAbstractTypesOfPrimePowerOrder := { <o,i> : i in [1..
      NumberOfSmallGroups(o)] };
  for g in [ i : i in possiblesgc | Order(i) eq o ] do
   Exclude(~CompletelyExcludedAbstractTypesOfPrimePowerOrder,
       IdentifyGroup(g));
  end for;
  CompletelyExcludedAbstractTypes join:=
      CompletelyExcludedAbstractTypesOfPrimePowerOrder;
 end if;
end for;
if verbose then
 "II: CompletelyExcludedAbstractTypes after initializaion =",
     CompletelyExcludedAbstractTypes;
end if;

remainingorders := [ i : i in Divisors( &*[i[1]^i[2] : i in
    MaximumPrimePowers] ) | i gt 1 and not IsPrimePower(i) ];
if verbose then
 "II: remaining orders =", remainingorders;
end if;

for ord in remainingorders do
 if verbose then
  "################";
  "# processing all subgroups of order =", ord;
  "################";
 end if;

 // "#####status#####";
 // "# CompletelyExcludedOrders =", CompletelyExcludedOrders;
 // "# CompletelyExcludedAbstractTypes =", CompletelyExcludedAbstractTypes
     ;
 // "# halldivisors =", HallDivisors(ord);
 // "# not IsNonSolvableNumber(ord) =", not IsNonSolvableNumber(ord);
 // "# NumberOfSmallGroups(ord) =", NumberOfSmallGroups(ord);
 // "################";

 // does the Hall theorem suffice to exclude all conjugacy classes of
     groups of order ord?
 halldivisors      := HallDivisors(ord);
 issolvablenumber := IsSolvableNumber(ord);
 IsExcludedByHall := #( halldivisors meet CompletelyExcludedOrders ) ge 1;
 if issolvablenumber and IsExcludedByHall then
  if verbose then
   "II: Hall theorem implies excluded subgroup of orders:", halldivisors
       meet CompletelyExcludedOrders;
  end if;
  Include(~CompletelyExcludedOrders,ord);
  continue;
 end if;

 SetOfAbstractTypesToExcludeForThisOrder := {};
 if IsInSmallGroupDatabase(ord) then
```

```
 SetOfAbstractTypesToExcludeForThisOrder := {<ord,i> : i in [1..
     NumberOfSmallGroups(ord)] };
end if;

// can we exclude all abstract types of representatives of conjugacy
    classes?
AbstractTypesWhichAreExcluded := {};
if IsInSmallGroupDatabase(ord) then
 CanExcludeAllAbstractTypes := true;
 for i in [1..NumberOfSmallGroups(ord)] do
  if IsExcludedByHall and SmallGroupIsSolvable(ord,i) then
   // abstract type contains by Hall's theorem an excluded subgroup
   Include(~AbstractTypesWhichAreExcluded, <ord,i>);
   continue;
  end if;
  AT  := SmallGroup(ord,i);
  SAT := SubgroupClasses(AT);
  if #( { i`order : i in SAT } meet CompletelyExcludedOrders) ge 1 then
   // AT contains a subgroup with excluded order
   Include(~AbstractTypesWhichAreExcluded, <ord,i>);
   continue;
  end if;
  if #( { IdentifyGroup(i`subgroup) : i in SAT } meet
      CompletelyExcludedAbstractTypes) ge 1 then
   // AT contains a subgroup with excluded abstract type
   Include(~AbstractTypesWhichAreExcluded, <ord,i>);
   continue;
  end if;
  CanExcludeAllAbstractTypes := false;
 end for;
 if CanExcludeAllAbstractTypes then
  if verbose then
   "II: the Smallgroups Library excludes all abstract types of
       representatives of this order";
  end if;
  Include(~CompletelyExcludedOrders,ord);
  continue;
 end if;
end if;

if verbose then
 "II: compute subgroup conjugacy classes";
 t  := Cputime();
end if;
if ord in [Order(i[1]) : i in SubgroupClassesInfusion] then
 if verbose then
  "II: using subgroup classes from infusion";
 end if;
 idx := Index([Order(i[1]) : i in SubgroupClassesInfusion], ord);
 SC  := SubgroupClassesInfusion[idx];
 SC  := FilterMatrixGroupCyclicGroupDimensionEigenspaceOne(G, possiblesgc
      , excludedsgc, SC);
elif fname_saved_SC eq "" then
```

```
  SC  := ComputeListOfCandidateSubgroups_Caller(<G, ord, possiblesgc,
      excludedsgc, use_expensive_conjugation_tests>);
 else
  SC  := FileHelper(fname_saved_SC, ComputeListOfCandidateSubgroups_Caller
      , <G, ord, possiblesgc, excludedsgc, use_expensive_conjugation_tests
      >);
 end if;
 if verbose then
  "II: computed subgroup conjugacy classes in ", Cputime(t);
  "II: # subgroup conjugacy classes =", #SC;
 end if;

 IsThisOrderCompletelyExcluded := true;

 for sccounter in [1..#SC] do
  if verbose then
   "II: progress", sccounter, "of", #SC;
  end if;
  U := SC[sccounter];

  if IsInSmallGroupDatabase(ord) and IdentifyGroup(U) in
      AbstractTypesWhichAreExcluded then
   if verbose then
    "II: skip this group due to AbstractTypesWhichAreExcluded";
   end if;
   continue;
  end if;

  if use_expensive_conjugation_tests then
   if ContainsExcludedSubgroupUpToConjugacy(G,excludedsgc,U) then
    if verbose then
     "II: contains an excluded subgroup up to conjugacy";
    end if;
    continue;
   end if;
  end if;

  if verbose then
   t   := Realtime();
  end if;
  if fname_saved_evals eq "" then
   ret := evalfunc(<U, name_counter>);
  else
   ret := FileHelper(fname_saved_evals, evalfunc, <U, name_counter>);
  end if;
  if verbose then
   "II: eval took (real time)", Realtime(t), "and was", ret;
  end if;
  name_counter +:= 1;

  if ret then
   IsThisOrderCompletelyExcluded := false;
   if IsInSmallGroupDatabase(ord) then
    Exclude(~SetOfAbstractTypesToExcludeForThisOrder, IdentifyGroup(U));
```

```
     end if;
     Append(~possiblesgc, U);
     Append(~indices,name_counter-1);
    else
     Append(~excludedsgc, U);
    end if;
   end for;
   if IsThisOrderCompletelyExcluded then
    Include(~CompletelyExcludedOrders,ord);
   else
    CompletelyExcludedAbstractTypes join:=
        SetOfAbstractTypesToExcludeForThisOrder;
   end if;
  end for;

  // Write("save_SearchSubgroupLattice_NonPGroups.txt",<excludedsgc,
      possiblesgc,name_counter,indices>,"Magma" : Overwrite:=true);

  if verbose then
   "II: SearchSubgroupLattice_NonPGroups total real time", Realtime(
       globaltime);
  end if;
  return excludedsgc,possiblesgc,name_counter,indices;
end function;

function SearchSubgroupLattice(G, evalfunc :
    use_expensive_conjugation_tests:=true, fname_saved_SC:="saved_SC.txt",
    fname_saved_evals:="saved_evals.txt", verbose:=true,
    SubgroupClassesInfusion:=[])
 MaximumPrimePowers,excludedsgc,possiblesgc,name_counter,indices :=
     SearchSubgroupLattice_PGroups( G, evalfunc
   : use_expensive_conjugation_tests:=use_expensive_conjugation_tests,
      fname_saved_SC:=fname_saved_SC, fname_saved_evals:=fname_saved_evals,
       verbose:=verbose, SubgroupClassesInfusion:=SubgroupClassesInfusion);
 excludedsgc,possiblesgc,name_counter,indices :=
     SearchSubgroupLattice_NonPGroups( G, evalfunc, MaximumPrimePowers,
     excludedsgc, possiblesgc, name_counter, indices
   : use_expensive_conjugation_tests:=use_expensive_conjugation_tests,
      fname_saved_SC:=fname_saved_SC, fname_saved_evals:=fname_saved_evals,
       verbose:=verbose, SubgroupClassesInfusion:=SubgroupClassesInfusion);
 possiblesgc_sorted := Sort(possiblesgc,func<x,y | Order(x)-Order(y)>);
 return possiblesgc_sorted;
end function;

////////////////////
// post processing functions
////////////////////

function
    PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Initialize(
    possiblesgc)
 SGCLattice := [];
 for i in [1..#possiblesgc-1] do
  for j in [i+1..#possiblesgc] do
```

```
   if Order(possiblesgc[i]) lt Order(possiblesgc[j]) and (Order(possiblesgc
       [j]) mod Order(possiblesgc[i])) eq 0 then
    Append(~SGCLattice,<i,j,"?">);
   end if;
   if Order(possiblesgc[i]) gt Order(possiblesgc[j]) and (Order(possiblesgc
       [i]) mod Order(possiblesgc[j])) eq 0 then
    Append(~SGCLattice,<j,i,"?">);
   end if;
  end for;
 end for;
 for i in SGCLattice do
  x := i[1];
  y := i[2];
  z := i[3];
  if z eq "?" and possiblesgc[x] subset possiblesgc[y] then
   Exclude(~SGCLattice, i);
   Append(~SGCLattice,<x,y,"S">);
  end if;
 end for;
 return SGCLattice;
end function;

function
    PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Expensive(G,
    possiblesgc, SGCLattice)
 for i in SGCLattice do
  x := i[1];
  y := i[2];
  z := i[3];
  if z eq "?" then
   if IsConjugateHelperSubgroupsConjugate(G, possiblesgc[y], possiblesgc[x])
       then
    Append(~SGCLattice,<x,y,"C">);
   end if;
   Exclude(~SGCLattice, i);
  end if;
 end for;
 return SGCLattice;
end function;

// remove utility data, transitive edges, and sort
function PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Cleanup
    (SGCLattice)
 assert #{ i : i in SGCLattice | i[3] eq "?" } eq 0;
 SGCLattice := {@ <i[1],i[2]> : i in SGCLattice @};
 R := [ i : i in SGCLattice ];
 for a in [1..#SGCLattice] do
  for b in [a+1..#SGCLattice] do
   for c in [b+1..#SGCLattice] do
    if [<a,b>, <b,c>, <a,c>] subset SGCLattice then
     if Index(R,<a,c>) ne 0 then
      Remove(~R, Index(R,<a,c>));
     end if;
    end if;
```

```
    end for;
   end for;
  end for;
  Sort(~R);
  return R;
end function;

// e.g. PostProcess_PossibleConjugayClassesSubgroupsLattice(GL(5,2),
    possiblesgc);
function PostProcess_PossibleConjugayClassesSubgroupsLattice(G, possiblesgc)
  SGCLattice :=
      PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Initialize(
      possiblesgc);
  SGCLattice :=
      PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Expensive(G
      ,possiblesgc,SGCLattice);
  SGCLattice :=
      PostProcess_PossibleConjugayClassesSubgroupsLattice_helper_Cleanup(
      SGCLattice);
  return SGCLattice;
end function;

function GroupNameCollection(CollectionOfGroups)
  return [ GroupName(i) : i in CollectionOfGroups ];
end function;

function PrintSubgroupLatticeAsDigraph(possiblesgc, Lattice)
  names := GroupNameCollection(possiblesgc);
  ret := "digraph{";
  for i in [1..#names] do
    ret cat:= "a" cat IntegerToString(i) cat "[label=\"" cat names[i] cat "
        (" cat IntegerToString(Order(possiblesgc[i])) cat ")\"];";
  end for;
  for i in Lattice do
    ret cat:= "a" cat IntegerToString(i[1]) cat "->a" cat IntegerToString(i
        [2]) cat ";";
  end for;
  ret cat:= "}";
  return ret;
end function;

////////////////////////////////////////
// automatic test:
// -> S7,       all subgroups of order at most 5
// -> GL(3,2),  all subgroups of order at most 10
////////////////////////////////////////

for i in <
   <SymmetricGroup(7), func< o | o le 5> >,
   <GL(3,2),           func< o | o le 5> >
   > do
  G       := i[1];
  f       := i[2];
```

```
 actual   := SearchSubgroupLattice(G, func<U_idx | f(Order(U_idx[1])) > :
    fname_saved_SC:="", fname_saved_evals:="", verbose:=false);
 expected := Sort([i`subgroup:i in SubgroupClasses(G) | f(i`order) ],func<x
    ,y | Order(x)-Order(y)>);
 assert SequenceToSet(GroupNameCollection(actual)) eq SequenceToSet(
    GroupNameCollection(expected));
 assert IsIsomorphic(
  Digraph<#actual   | [ [i[1],i[2]] : i in
      PostProcess_PossibleConjugayClassesSubgroupsLattice(G,actual)]>,
  Digraph<#expected | [ [i[1],i[2]] : i in
      PostProcess_PossibleConjugayClassesSubgroupsLattice(G,expected)]>);
end for;
```

Some Magma implementations for subspace codes

```
////////////////////
// functions for subspaces and subspace / injection distance
////////////////////

function Grassmannian(q,v,k)
 return {@ x[2] : x in OrbitsOfSpaces(sub<GL(v,q) | Id(GL(v,q))>, k) @};
end function;

// Subspaces(q,v,k) = Grassmannian(q,v,k) for Grassmannian
// Subspaces(q,v) for all subspaces
function Subspaces(q,vk,...)
 assert #vk le 2;
 if #vk eq 2 then
  return Grassmannian(q,vk[1],vk[2]);
 else
  return SetToIndexedSet(&join {@ Grassmannian(q,vk[1],k) : k in [0..vk[1]]
      @});
 end if;
end function;

// get all t-subspaces of U
function IncidencesSmaller(U,t)
    G := GL(Dimension(U),BaseRing(U));
    O := OrbitsOfSpaces(sub<G|Identity(G)>,t);
    T := [ BasisMatrix(i[2]) : i in O ];
    M := BasisMatrix(U);
    return {@ VectorSpaceWithBasis(i*M) : i in T @};
end function;

// get all t-subspaces of A which contain U
function IncidencesBigger(A, U, t)
        return {@ U+i : i in IncidencesSmaller(Complement(A,U),t-Dimension(
           U)) @};
end function;

// get all t-subspaces of A which are incident with U
function Incidences(A, U, t)
 if Dimension(U) eq t then
```

```
   return U;
  elif Dimension(U) gt t then
   return IncidencesSmaller(U,t);
  else
   return IncidencesBigger(A,U,t);
 end if;
end function;

function SubspaceDistance(U,W)
 return Dimension(U+W) - Dimension(U meet W);
end function;

function InjectionDistance(U,W)
 return Maximum(Dimension(U), Dimension(W)) - Dimension(U meet W);
end function;

function SubspaceCodeParameters(code)
 // convert to list with unique entries
    C := [j : j in {i:i in code}];
    v := Degree(C[1]);
    assert &and[Degree(i) eq v : i in C];
    return <v, #C, Minimum([SubspaceDistance(C[i],C[j]) : i,j in [1..#C] |
        i lt j]), {Dimension(i) : i in C}>;
end function;

// rhs is either a list with v-1 non-negative integers or false
// if rhs is a list, then the entries should be: A_q(v-w,d;k-w) (w=1,...,k-
   d/2), 1 (w=k-d/2+1,...,k+d/2-1), A_q(w,d;k) (w=k+d/2,...,v-1)
// depending on the situation these entries may differ (e.g., <=2 for
   Packing Designs)
// if rhs_i=0 then no inequalities of dimension i are generated
// never constraints will be generated for the dimensions in k-delta+2,
   ..., k+delta-2
// if rhs == false, then only constraints with w=k-d/2+1 are generated
// lb = lower bound on the objective, defaults to zero
// replaceme generates a placeholder with the contents of placeholder (e.g.
    for additional constraints)
// e.g. DefaultCDCBLP("defcdc_2542.lp", 2,5,4,2 : rhs:=[1,1,1,5], lb:=9,
   replaceme:="replaceme");
// e.g. DefaultCDCBLP("defcdc_2743.lp", 2,7,4,3 : rhs:=[21,1,1,1,9,77], lb
   :=329, replaceme:="replaceme");
procedure DefaultCDCBLP(fname, q,v,d,k : rhs:=false, lb:=0, replaceme:=
   false)
 delta := Integers()!(d/2);
 G := Grassmannian(q,v,k);

 // objective function
 out := "max\n";
 for i in [1..#G] do out cat:= " +x" cat IntegerToString(i); end for; out
    cat:= "\n";
 out cat:= "st\n";

 // optimal lower bound for the objective function
 if lb ne 0 then
```

```
  for i in [1..#G] do out cat:= " +x" cat IntegerToString(i); end for; out
      cat:= " >= " cat IntegerToString(lb) cat "\n";
 end if;

 // constraints
 if Type(rhs) eq BoolElt then
  rhs            := [ 0 : i in [1..v-1] ];
  rhs[k-delta+1] := 1;
 end if;
 for w in [1..v-1] do
  if w in [k-delta+2..k+delta-2] then
   continue;
  end if;
  if rhs[w] eq 0 then
   continue;
  end if;

  for W in Grassmannian(q,v,w) do
   Gsub := Incidences(VectorSpace(GF(q),v),W,k);
   for U in Gsub do
    out cat:= " +x" cat IntegerToString(Index(G,U));
   end for;
   out cat:= " <= " cat IntegerToString(rhs[w]) cat "\n";
  end for;
 end for;

 // optional placeholder
 if Type(replaceme) ne BoolElt then
  out cat:= replaceme cat "\n";
 end if;

 // footer of the lp file: declaration of variables as binaries
 out cat:= "binary\n";
 for i in [1..#G] do
  out cat:= " x" cat IntegerToString(i);
 end for;
 out cat:= "\n";
 out cat:= "end";

 Write(fname, out : Overwrite:=true);
end procedure;

function CollectionOfSubspacesToListOfRREFMatrices(c)
 return [EchelonForm(BasisMatrix(i)) : i in c];
end function;

// a x b matrices over F_q with rank distance d
function MRDGeneralizedGabidulin(a, b, d, q : s:=1)
 if a lt b then
  m          := a;
  M          := b;
  transpose := true;
 else
  m          := b;
```

```
  M          := a;
  transpose := false;
 end if;
 // M x m matrices, m <= M
 assert GCD(s,M) eq 1;

 // k is dimension of subspace, i.e., number of rows of G
 k := m-d+1;
 if k le 0 then
  return {@ ZeroMatrix(GF(q), a, b) @};
 end if;
 F       := GF(q^M);
 g       := NormalElement(F, GF(q)); // g^(q^0), ..., g^(q^(M-1)) are basis
     of F over F_q
 G       := Matrix(F, k, m, [ [(g^(q^col))^(q^((row*s) mod M)) : col in [0..
     m-1]] : row in [0..k-1]]);
 MRDvec := [ a*G : a in VectorSpace(F,k) ];
 x,y     := VectorSpace(F, GF(q)); // y: F -> GF(q)^M
 myMRD   := {@ HorizontalJoin([ Matrix(M,1,ElementToSequence(y(i))) : i in
     ElementToSequence(j) ]) : j in  MRDvec @};

 if transpose then
  myMRD := {@ Transpose(i) : i in myMRD @};
 end if;

 assert &and[ Nrows(i) eq a : i in myMRD ];
 assert &and[ Ncols(i) eq b : i in myMRD ];
 assert &and[ Parent(i[1][1]) eq GF(q) : i in myMRD ];
 assert &and[ Rank(i) ge d : i in myMRD | i ne 0 ];
 assert #myMRD eq q^(M*(m-d+1));

 return myMRD;
end function;

// s controls generalization in MRDGeneralizedGabidulin
function LMRD(q, v, d, k : s:=1)
 myMRD    := MRDGeneralizedGabidulin(k, v-k, Integers()!(d/2), q : s:=s);
 LMRDmat := [ HorizontalJoin(IdentityMatrix(GF(q),k),i) : i in myMRD ];
 myLMRD   := {@ sub<VectorSpace(GF(q),v) | Rows(i)> : i in LMRDmat @};

 assert #myLMRD eq Ceiling(q^((Maximum(v-k,k))*(Minimum(v-k,k)-d/2+1)));
 assert &and[ Dimension(i) eq k : i in myLMRD ];
 assert &and[ i subset VectorSpace(GF(q),v) : i in myLMRD ];

 return myLMRD;
end function;

////////////////////////////////////////
// additional constraints for DefaultCDCBLP and the solving process
////////////////////////////////////////

// e.g. eval_DefaultCDCBLP(2,5,4,2,SylowSubgroup(GL(5,2),2),100,"sg1","add_
    ",1,"adapter.py");
```

```
function eval_DefaultCDCBLP(q,v,d,k,U,timelimit,subgroupname,
    addendum_prefix,addendum_number,adaptername)
 addendum := "";
 G        := Subspaces(q,v,k);
 orbits   := { x[2]^U : x in OrbitsOfSpaces(U,k) };

 for orbit in orbits do
  orep    := Representative(orbit);
  orepidx := Index(G,orep);
  for j in orbit do
   if j ne orep then
    jidx        := Index(G,j);
    addendum cat:= "+x" cat IntegerToString(orepidx) cat " -x" cat
        IntegerToString(jidx) cat " = 0\n";
   end if;
  end for;
 end for;

 Write(subgroupname, U, "Magma" : Overwrite:=true);
 Write(addendum_prefix cat IntegerToString(addendum_number) cat ".txt",
    addendum : Overwrite:=true);

 returnvalue := System("gurobi.sh " cat adaptername cat " " cat
    IntegerToString(addendum_number) cat " " cat IntegerToString(timelimit
    ));
 returnvalue := returnvalue / 256;
 assert returnvalue in [0,1];
 if returnvalue eq 0 then
  return true; // true means there is a solution or the time limit was
      reached
 else
  return false; // false means the problem is infeasible
 end if;
end function;

////////////////////////////////////////
// adapter between Magma and Gurobi
////////////////////////////////////////

// creates a Python file called fname_helper, which can be executed with
// gurobi.sh fname_helper <number of addendum file> <timelimit>
// It then replaces replaceme in fname_DefaultCDCBLP with the contents in
    addendum_prefix<number of addendum file>.txt
// and executes Gurobi for at most the specified amount of time.
// It returns 0 iff a solution is found or the timelimit is reached, 1 iff
    the problem is infeasible, or 99 in any other case
// e.g. write_python_helper("adapter.py", "defcdc_2542.lp", "add_", "
    replaceme");
procedure write_python_helper(fname_helper, fname_DefaultCDCBLP,
    addendum_prefix, replaceme)
 a := "
import gurobipy, sys, datetime, os\n\
\n\
default = open('" cat fname_DefaultCDCBLP cat "').read()\n\
```

```
addendum = open('" cat addendum_prefix cat "%s.txt'%sys.argv[1]).read()\n\
outfile = open('" cat addendum_prefix cat "ilp_%s.lp'%sys.argv[1],'w')\n\
outfile.write(default.replace('" cat replaceme cat "',addendum))\n\
outfile.close()\n\
os.system('gzip -f " cat addendum_prefix cat "ilp_%s.lp'%sys.argv[1])\n\
\n\
try:\n\
 time = int(sys.argv[2])\n\
except:\n\
 time = 10\n\
\n\
m = gurobipy.read('" cat addendum_prefix cat "ilp_%s.lp.gz'%sys.argv[1])\n\
m.params.LogToConsole = 0\n\
m.params.LogFile = '" cat addendum_prefix cat "ilp_%s.lp.log'%sys.argv[1]\n
   \
m.params.TimeLimit = time\n\
m.optimize()\n\
\n\
if m.Status == gurobipy.GRB.TIME_LIMIT:\n\
 try:\n\
  m.write('" cat addendum_prefix cat "ilp_%s.lp.sol'%sys.argv[1])\n\
   print datetime.datetime.now(), 'time', m.ObjVal\n\
 except gurobipy.GurobiError:\n\
   print datetime.datetime.now(), 'time'\n\
 sys.exit(0)\n\
elif m.Status == gurobipy.GRB.OPTIMAL:\n\
 m.write('" cat addendum_prefix cat "ilp_%s.lp.sol'%sys.argv[1])\n\
 print datetime.datetime.now(), 'opt', m.ObjVal, m.ObjBound\n\
 sys.exit(0)\n\
elif m.Status == gurobipy.GRB.INFEASIBLE:\n\
 print datetime.datetime.now(), 'infeasible'\n\
 sys.exit(1)\n\
else:\n\
 print datetime.datetime.now(), 'EE: Gurobi status is:', m.Status\n\
 sys.exit(99)\n\
";
 Write(fname_helper, a : Overwrite:=true);
end procedure;
```

List of Figures

List of Tables

List of Algorithms

Listings

Glossary

$\mathrm{d_h}(u, w) = \#\{i \in \{1, 2, \ldots, v\} \mid u_i \neq w_i\}$, Hamming distance.

$\mathrm{wt}(u) = \mathrm{d_h}(u, \mathbf{0})$, weight.

$\mathrm{d_i}(U, W) = \max\{\dim(U), \dim(W)\} - \dim(U \cap W)$, injection distence.

$\mathrm{D_i}(C) = \min\{\mathrm{d_i}(U, W) \mid U \neq W \in C\}$, minimum injection distance.

$\mathrm{d_r}(M, N) = \mathrm{rk}(M - N)$, rank distance.

$\mathrm{D_r}(M, N) = \min\{\mathrm{d_r}(U, W) \mid U \neq W \in C\}$, minimum rank distance.

$\mathrm{d_s}(U, W) = \dim(U + W) - \dim(U \cap W)$, subspace distance.

$\mathrm{D_s}(C) = \min\{\mathrm{d_s}(U, W) \mid U \neq W \in C\}$, minimum subspace distance.

$\mathbb{F}_q$ the up to isomorphism unique finite field with q elements, $2 \leq q$ prime power.

$\mathbb{F}_q^v$ the up to isomorphism unique vector space of dimension $1 \leq v$ over $\mathbb{F}_q$, usually row vectors $\mathbb{F}_q^{1\times v}$.

$\mathbb{F}_q^{m\times n}$ the up to isomorphism unique vector space of $m \times n$ matrices over $\mathbb{F}_q$.

$\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ set of all k-dimensional subspaces of $\mathbb{F}_q^v$, Grassmannian.

$\begin{bmatrix} v \\ k \end{bmatrix}_q = \# \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} = \prod_{i=0}^{k-1} \frac{q^v - q^i}{q^k - q^i}$, q-binomial coefficient.

$\begin{bmatrix} W \backslash U \\ c \end{bmatrix}$ set of c-subspaces of W which have trivial intersection with U.

$\begin{bmatrix} w \backslash u \\ c \end{bmatrix}_q = \# \begin{bmatrix} W \backslash U \\ c \end{bmatrix} = q^{uc} \begin{bmatrix} w-u \\ c \end{bmatrix}_q$.

$[n]_q = (q^n - 1)/(q - 1)$, q-number.

$[n]_q! = \prod_{i=1}^{n} [i]_q$, q-factorial.

$\mathrm{GL}(V)$ general linear group of V.

$\mathrm{Z}(\mathrm{GL}(V)) = \{\lambda I_v \mid \lambda \in \mathbb{F}_q^*\}$, center of $\mathrm{GL}(V)$.

$\mathrm{PGL}(V) = \mathrm{GL}(V)/\mathrm{Z}(\mathrm{GL}(V))$, projective general linear group.

$\mathrm{P\Gamma L}(\mathbb{F}_q^v)$ $= \mathrm{PGL}(\mathbb{F}_q^v) \rtimes \mathrm{Aut}(\mathbb{F}_q)$, projective semilinear group.

I_v $v \times v$ identity matrix, I if the dimension is obvious.

$\mathbf{0}_{m\times n}$ $m \times n$ zero matrix, $\mathbf{0}$ if the dimension is obvious.

$J_{m\times n}$ $m \times n$ all-one matrix, J if the dimension is obvious.

$M_{i,*}$ i-th row of the matrix M.

$M_{*,j}$ j-th column of the matrix M.

$M_{i,j}$ element of the matrix M in row i and column j.

Ug $= \{ug \mid u \in U\}$, right coset.

$U\backslash G$ $= \{Ug \mid g \in G\}$.

gU $= \{gu \mid u \in U\}$, left coset.

G/U $= \{gU \mid g \in G\}$.

$(G : U)$ $= \#G/\#U$, index.

h^g $= g^{-1}hg$, conjugation.

h^G $= \{h^g \mid g \in G\}$.

U^g $= \{u^g \mid u \in U\}$.

U^G $= \{U^g \mid g \in G\}$.

C_n cyclic group of order n, used as abstract type.

D_n dihedral group of order n, used as abstract type.

Q_n quaternion group of order n, used as abstract type.

A_n alternating group on n elements, used as abstract type.

S_n symmetric group on n elements, used as abstract type.

$\rtimes$ semidirect product.

$\times$ direct product, cartesian product.

$N_B(A)$ $= \{b \in B \mid A^b = A\}$, normalizer.

$\trianglelefteq$ normal subgroup.

$\circ$ group action, sometimes without symbol, concatenation of maps.

xG $= \{xg \mid g \in G\}$, orbit.

X/G $= \{xG \mid x \in X\}$, orbit space.

$\mathrm{Stab}_G(x)$ $= \{g \in G \mid xg = x\}$, stabilizer.

$\mathrm{Aut}(L/K)$ $= \{g \in \mathrm{Aut}(L) \mid g(k) = k \,\forall k \in K\}$.

$U^\perp$ $= \pi(U)$, orthogonal space. , *see* $\pi(U)$

$\tau_{q,k,v}$: $\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \to \left\{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k, A \text{ is in RREF}\right\}$, bijection, τ if parameters are obvious.

$\mathrm{p}_{q,v,k}(U)$ $\in \mathbb{F}_2^v$, $\mathrm{p}(U)_i = 1$ iff column i in the RREF matrix of U is a pivot column, for $U \in \mathbb{F}_q^{k\times v}$ in RREF or $U \in \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$, p if the parameters are known.

$\pi(U)$ $= \{v \in V \mid \beta(v,u) = 0 \,\forall u \in U\}$ for some non-degenerate symmetric bilinear form β.

$\mathrm{RREF}_{q,k,v}$: $\{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k\} \to \{A \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(A) = k, A \text{ is in RREF}\}$, RREF if parameters are obvious.

$\Lambda_{q,m,n}$: $\mathbb{F}_q^{m\times n} \to \begin{bmatrix} \mathbb{F}_q^{m+n} \\ m \end{bmatrix}, M \mapsto \tau^{-1}((I_m \mid M))$, Λ if parameters are obvious.

$(a;q)_n$ $= \prod_{i=0}^{n-1}(1 - aq^i)$, q-Pochhammer symbol.

$\mu(q)$ $= (1/q; 1/q)_\infty^{-1}$.

$(m \times n, N, d)_q$ rank metric code $C \subseteq \mathbb{F}_q^{m\times n}$, $\#C = N$, and $\mathrm{D_r}(C) \geq d$.

$[m \times n, k, d]_q$ linear $(m \times n, q^k, d)_q$ rank metric code.

$t - (v, k, \lambda)_q$ subspace design.

$S(t, k, v)_q$ q-Steiner system.

$\mathrm{A}_q^{\mathrm{x}}(v, d; K; U)$ maximum size M of a $(v, M, d; K; U)_q^{\mathrm{x}}$ subspace code.

$\mathrm{Aut}(C)$ $\leq \langle \mathrm{P\Gamma L}(V), \pi\rangle$ with $g \in \mathrm{Aut}(C)$ iff $Cg = C$.

$\delta(C)$ $= (\delta_0, \delta_1, \ldots, \delta_v)$ such that δ_i is the number of i-subspaces in C.

$K(C)$ $= \{\dim(U) \mid U \in C\}$.

$\mathcal{L}(V)$ $= \{U \mid U \leq V\}$.

$(v, M, d; K; U)_q^{\mathrm{x}}$ subspace code $C \subseteq \mathcal{L}(\mathbb{F}_q^v)$ with $\#C = M$, $\mathrm{D_x}(C) \geq d$ ($\mathrm{x} \in \{\mathrm{i}, \mathrm{s}\}$), $K(C) \subseteq K$, and $U \leq \mathrm{Aut}(C)$, U defaults to $\langle\rangle$, K defaults to $\{0, \ldots, v\}$ (MDC) or k (CDC).

$\leq$ smaller or equal, subgroup, subspace.

$\langle\rangle$ trivial group, trivial subspace.

1_l $1\dots1$ of length l.

0_l $0\dots0$ of length l.

$\mathrm{GCD}(a,b)$ greatest common divisor of a and b.

$v-K$ $=\{v-k \mid k\in K\}$.

$[n]$ $=\{1, 2, \dots, \mathrm{n}\}$.

$\mathcal{S}_X$ symmetric group of the set X.

$\mathcal{S}_n$ $=\mathcal{S}_{[n]}$.

$\mathcal{H}_k(U)$ arbitrary k-subspace in U.

$\mid$ horizontal concatenation of matrices.

$Ax\leq b$ $A_{i,*}x\leq b_i$ for all i.

$\binom{X}{2}$ $=\{\{x,y\}\in X\times X \mid x\neq y\}$.

$\mathbb{1}_\varphi$ $\in\{0,1\}$, 1 iff φ is true, indicator function.

$\mathbb{1}_S(x)$ $\in\{0,1\}$, 1 iff $x\in S$ is true, characteristic function.

st subject to.

$\oplus$ direct sum of subspaces.

$\#$ cardinality of a set.

rk rank of a matrix.

$a\neq b\in c$ synonym of $\{a,b\}\in\binom{c}{2}$.

u_i i-th unit vector in $\mathbb{F}_q^v$ for $i\in[v]$.

$:=$ the term on the left hand side is defined to be the term on the right hand side.

$\ker(M)$ $=\{x \mid xM=0\}$, kernel of M.

$\min S$ smallest element in S, minimum.

$\operatorname{argmin}\{f(x) \mid x\in S\}$ $y\in S$ with $f(y)=\min\{f(x) \mid x\in S\}$.

$\mathrm{SL}(V)$ $=\{M\in\mathrm{GL}(V) \mid \det(M)=1\}$, special linear group.

Index

Bibliography

[AA09] Rudolf Ahlswede and Harout K. Aydinian. “On error control codes for random network coding”. In: *Network Coding, Theory, and Applications, 2009. NetCod’09. Workshop on*. IEEE. 2009, pp. 68–73 (cit. on pp. 92, 109–111).

[AAK01] Rudolf Ahlswede, Harout K. Aydinian, and Levon H. Khachatrian. “On perfect codes and related concepts”. In: *Des. Codes Cryptogr.* 22.3 (2001), pp. 221–237. ISSN: 0925-1022. URL: `https://doi.org/10.1023/A:1008394205999` (cit. on pp. 109, 110).

[AAR99] George E. Andrews, Richard Askey, and Ranjan Roy. *Special functions*. Vol. 71. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1999, pp. xvi+664. ISBN: 0-521-62321-9; 0-521-78988-5. DOI: `10.1017/CBO9781107325937`. URL: `https://doi.org/10.1017/CBO9781107325937` (cit. on p. 17).

[AHL16] Jingmei Ai, Thomas Honold, and Haiteng Liu. “The Expurgation-Augmentation Method for Constructing Good Plane Subspace Codes”. In: *arXiv preprint 1601.01502* (2016) (cit. on pp. 89, 144, 146).

[And76] George E. Andrews. *The theory of partitions*. Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976, pp. xiv+255 (cit. on pp. 17, 59).

[AVZ00] Erik Agrell, Alexander Vardy, and Kenneth Zeger. “Upper bounds for constant-weight codes”. In: *IEEE Trans. Inform. Theory* 46.7 (2000), pp. 2373–2395. ISSN: 0018-9448. URL: `https://doi.org/10.1109/18.887851` (cit. on p. 116).

[BB52] Raj C. Bose and Katherine A. Bush. “Orthogonal arrays of strength two and three”. In: *Ann. Math. Statistics* 23 (1952), pp. 508–524. ISSN: 0003-4851 (cit. on p. 121).

[BCN89] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-regular graphs*. Vol. 18. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1989, pp. xviii+495. ISBN: 3-540-50619-5. URL: `https://doi.org/10.1007/978-3-642-74341-2` (cit. on pp. 24, 44, 45).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. URL: `https://doi.org/10.1006/jsco.1996.0125` (cit. on pp. 15, 30, 163, 172, 178).

[BE12] Simon R. Blackburn and Tuvi Etzion. “The asymptotic behavior of Grassmannian codes”. In: *IEEE Trans. Inform. Theory* 58.10 (2012), pp. 6605–6609. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2012.2207370` (cit. on p. 137).

[BEO] Hans Ulrich Besche, Bettina Eick, and Eamonn O’Brien. *Small Groups library*. visited on Dec. 12, 2016. URL: `http://www.icm.tu-bs.de/ag_algebra/software/small/` (cit. on p. 30).

[Ber10] Bruce C. Berndt. "What is a q-series?" In: *Ramanujan rediscovered.* Vol. 14. Ramanujan Math. Soc. Lect. Notes Ser. Ramanujan Math. Soc., Mysore, 2010, pp. 31–51 (cit. on p. 17).

[Beu75] Albrecht Beutelspacher. "Partial spreads in finite projective spaces and partial designs". In: *Math. Z.* 145.3 (1975), pp. 211–229. ISSN: 0025-5874. URL: `https://doi.org/10.1007/BF01215286` (cit. on p. 120).

[BK92] Achim Bachem and Walter Kern. *Linear programming duality.* Springer, 1992, p. 215 (cit. on p. 38).

[BKN16] Michael Braun, Michael Kiermaier, and Anamari Nakić. "On the automorphism group of a binary q-analog of the Fano plane". In: *European J. Combin.* 51 (2016), pp. 443–457. ISSN: 0195-6698. URL: `https://doi.org/10.1016/j.ejc.2015.07.014` (cit. on pp. 162, 169, 171).

[BKW18a] Michael Braun, Michael Kiermaier, and Alfred Wassermann. "Computational Methods in Subspace Designs". In: *Network Coding and Subspace Designs.* Springer, 2018, pp. 213–244 (cit. on p. 39).

[BKW18b] Michael Braun, Michael Kiermaier, and Alfred Wassermann. "q-Analogs of Designs: Subspace Designs". In: *Network Coding and Subspace Designs.* Springer, 2018, pp. 171–211 (cit. on pp. 17, 22, 39).

[BÖW16] Michael Braun, Patric R. J. Östergård, and Alfred Wassermann. "New Lower Bounds for Binary Constant-Dimension Subspace Codes". In: *Experimental Mathematics* (2016), pp. 1–5. DOI: `10.1080/10586458.2016.1239145`. eprint: `http://dx.doi.org/10.1080/10586458.2016.1239145`. URL: `http://dx.doi.org/10.1080/10586458.2016.1239145` (cit. on pp. 103, 144, 146).

[BPV13] Christine Bachoc, Alberto Passuello, and Frank Vallentin. "Bounds for projective codes from semidefinite programming". In: *Adv. Math. Commun.* 7.2 (2013), pp. 127–145. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2013.7.127` (cit. on pp. 46, 107).

[BR14] Michael Braun and Jan Reichelt. "q-q-Analogs of Packing Designs". In: *J. Combin. Des.* 22.7 (2014), pp. 306–321. ISSN: 1063-8539. URL: `https://doi.org/10.1002/jcd.21376` (cit. on p. 162).

[Bra+16] Michael Braun, Tuvi Etzion, Patric R. J. Östergård, Alexander Vardy, and Alfred Wassermann. "Existence of q-analogs of Steiner Systems". In: *Forum Math. Pi* 4 (2016), e7, 14. ISSN: 2050-5086. URL: `https://doi.org/10.1017/fmp.2016.5` (cit. on pp. 39, 132, 146).

[Cay54] Arthur Cayley. "On the Theory of Groups as Depending on the Symbolic Equation $\theta^n = 1$". In: *Philosophical Magazine* 7.4 (1854), pp. 40–47 (cit. on p. 32).

[Cox74] Harold S. M. Coxeter. *Projective geometry.* Second. University of Toronto Press, Toronto, Ont., 1974, pp. xii+163 (cit. on p. 38).

[CP17] Antonio Cossidente and Francesco Pavese. "Subspace codes in $\mathrm{PG}(2n-1, q)$". In: *Combinatorica* 37.6 (2017), pp. 1073–1095. ISSN: 1439-6912. DOI: `10.1007/s00493-016-3354-5`. URL: `http://dx.doi.org/10.1007/s00493-016-3354-5` (cit. on p. 85).

[CPS18] Antonio Cossidente, Francesco Pavese, and Leo Storme. "Geometrical Aspects of Subspace Codes". In: *Network Coding and Subspace Designs.* Springer, 2018, pp. 107–129 (cit. on pp. 24, 85).

[Dak65] R. J. Dakin. "A tree-search algorithm for mixed integer programming problems". In: *Comput. J.* 8 (1965), pp. 250–255. ISSN: 0010-4620. URL: `https://doi.org/10.1093/comjnl/8.3.250` (cit. on pp. 52, 105, 168, 193).

[Del76a] Philippe Delsarte. "Association schemes and t-designs in regular semilattices". In: *J. Combinatorial Theory Ser. A* 20.2 (1976), pp. 230–243 (cit. on p. 46).

[Del76b] Philippe Delsarte. "Properties and applications of the recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) - q^k F(i,k,n)$". In: *SIAM J. Appl. Math.* 31.2 (1976), pp. 262–270. ISSN: 0036-1399. URL: `https://doi.org/10.1137/0131021` (cit. on p. 46).

[Del78a] Philippe Delsarte. "Bilinear forms over a finite field, with applications to coding theory". In: *J. Combin. Theory Ser. A* 25.3 (1978), pp. 226–241. ISSN: 0097-3165. URL: `https://doi.org/10.1016/0097-3165(78)90015-8` (cit. on p. 37).

[Del78b] Philippe Delsarte. "Hahn polynomials, discrete harmonics, and t-designs". In: *SIAM J. Appl. Math.* 34.1 (1978), pp. 157–166. ISSN: 0036-1399. URL: `https://doi.org/10.1137/0134012` (cit. on p. 46).

[DF79] David A. Drake and J. W. Freeman. "Partial t-spreads and group constructible (s, r, μ)-nets". In: *J. Geom.* 13.2 (1979), pp. 210–216. ISSN: 0047-2468. URL: `https://doi.org/10.1007/BF01919756` (cit. on p. 121).

[DT03] George B. Dantzig and Mukund N. Thapa. *Linear programming. 2.* Springer Series in Operations Research. Theory and extensions. Springer-Verlag, New York, 2003, pp. xxvi+448. ISBN: 0-387-98613-8 (cit. on p. 38).

[DT97] George B. Dantzig and Mukund N. Thapa. *Linear programming. 1.* Springer Series in Operations Research. Introduction, With 1 CD-ROM for Windows. Springer-Verlag, New York, 1997, pp. xxxviii+435. ISBN: 0-387-94833-3 (cit. on p. 38).

[ElZ+10] Saad El-Zanati, Heather Jordon, George F. Seelinger, Papa A. Sissokho, and Lawrence Spence. "The maximum size of a partial 3-spread in a finite vector space over GF(2)". In: *Des. Codes Cryptogr.* 54.2 (2010), pp. 101–107. ISSN: 0925-1022. URL: `https://doi.org/10.1007/s10623-009-9311-1` (cit. on p. 121).

[ES09] Tuvi Etzion and Natalia Silberstein. "Error-Correcting Codes in Projective Spaces via Rank-Metric Codes and Ferrers Diagrams". In: *IEEE Trans. Inform. Theory* 55.7 (2009), pp. 2909–2919. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2009.2021376` (cit. on pp. 59, 60, 64, 74, 77, 99, 103).

[ES13] Tuvi Etzion and Natalia Silberstein. "Codes and Designs Related to Lifted MRD Codes". In: *IEEE Trans. Inform. Theory* 59.2 (2013), pp. 1004–1017. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2012.2220119` (cit. on pp. 61, 67, 79, 85, 89, 90, 92–95, 99, 137, 139, 141).

[ES16] Tuvi Etzion and Leo Storme. "Galois geometries and coding theory". In: *Des. Codes Cryptogr.* 78.1 (2016), pp. 311–350. ISSN: 0925-1022. URL: `https://doi.org/10.1007/s10623-015-0156-5` (cit. on pp. 24, 41, 89, 161).

[Etz+16] Tuvi Etzion, Elisa Gorla, Alberto Ravagnani, and Antonia Wachter-Zeh. "Optimal Ferrers diagram rank-metric codes". In: *IEEE Trans. Inform. Theory* 62.4 (2016), pp. 1616–1630. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2016.2522971` (cit. on pp. 59–61, 65, 77).

[Etz13] Tuvi Etzion. "Problems on q-Analogs in Coding Theory". In: *arXiv preprint 1305.6126* (2013), p. 37 (cit. on p. 89).

[Etz15a] Tuvi Etzion. “A New Approach to Examine q-Steiner Systems”. In: *arXiv preprint 1507.08503* (2015) (cit. on p. 162).

[Etz15b] Tuvi Etzion. “On the Structure of the q-Fano Plane”. In: *arXiv preprint 1508.01839* (2015) (cit. on p. 162).

[EV11a] Tuvi Etzion and Alexander Vardy. “Error-Correcting Codes in Projective Space”. In: *IEEE Trans. Inform. Theory* 57.2 (2011), pp. 1165–1173. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2010.2095232` (cit. on pp. 107, 110, 114–117, 125).

[EV11b] Tuvi Etzion and Alexander Vardy. “On q-analogs of Steiner systems and covering designs”. In: *Adv. Math. Commun.* 5.2 (2011), pp. 161–176. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2011.5.161` (cit. on p. 162).

[Ext83] Harold Exton. *q-hypergeometric functions and applications*. Ellis Horwood Series: Mathematics and its Applications. With a foreword by L. J. Slater. Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York, 1983, p. 347. ISBN: 0-85312-491-4 (cit. on p. 17).

[FR85] Péter Frankl and Vojtěch Rödl. “Near perfect coverings in graphs and hypergraphs”. In: *European J. Combin.* 6.4 (1985), pp. 317–326. ISSN: 0195-6698. URL: `https://doi.org/10.1016/S0195-6698(85)80045-7` (cit. on p. 137).

[FW86] Péter Frankl and Richard M. Wilson. “The Erdős-Ko-Rado theorem for vector spaces”. In: *J. Combin. Theory Ser. A* 43.2 (1986), pp. 228–236. ISSN: 0097-3165. URL: `https://doi.org/10.1016/0097-3165(86)90063-4` (cit. on pp. 53, 110).

[Gab85] Ernst M. Gabidulin. “Theory of codes with maximum rank distance”. In: *Problemy Peredachi Informatsii* 21.1 (1985), pp. 3–16. ISSN: 0555-2923 (cit. on pp. 36, 37).

[Gan59] Felix R. Gantmacher. *Applications of the theory of matrices*. Translated by J. L. Brenner, with the assistance of D. W. Bushaw and S. Evanusa. Interscience Publishers, Inc., New York; Interscience Publishers Ltd., London, 1959, pp. ix+317 (cit. on p. 45).

[GAP18] GAP. *GAP – Groups, Algorithms, and Programming, Version 4.8.10*. The GAP Group. 2018. URL: `https://www.gap-system.org` (cit. on pp. 30, 158, 201).

[GMT15] Heide Gluesing-Luerssen, Katherine Morrison, and Carolyn Troha. “Cyclic orbit codes and stabilizer subfields”. In: *Adv. Math. Commun.* 9.2 (2015), pp. 177–197. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2015.9.177` (cit. on p. 125).

[Gor16] Alexey L. Gorodentsev. *Algebra. I. Textbook for students of mathematics*. Translated from the 2013 Russian orginal. Springer, Cham, 2016, pp. xx+564. ISBN: 978-3-319-45284-5; 978-3-319-45285-2 (cit. on p. 23).

[GR18] Elisa Gorla and Alberto Ravagnani. “Codes Endowed with the Rank Metric”. In: *Network Coding and Subspace Designs*. Springer, 2018, pp. 3–23 (cit. on p. 37).

[GSS00] Neil A. Gordon, Ron Shaw, and Leonard H. Soicher. “Classification of partial spreads in PG$(4, 2)$”. In: *Mathematics Research Reports (University of Hull)* XIII.1 (2000), pp. 1–63 (cit. on pp. 179, 190).

[GT16] Heide Gluesing-Luerssen and Carolyn Troha. “Construction of subspace codes through linkage”. In: *Adv. Math. Commun.* 10.3 (2016), pp. 525–540. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2016023` (cit. on pp. 125, 133, 134).

[Gur16] Inc. Gurobi Optimization. *Gurobi Optimizer Reference Manual.* 2016. URL: `http://www.gurobi.com` (cit. on pp. 105, 178).

[Hed12] Olof Heden. “A survey of the different types of vector space partitions”. In: *Discrete Math. Algorithms Appl.* 4.1 (2012), pp. 1250001, 14. ISSN: 1793-8309. URL: `https://doi.org/10.1142/S1793830912500012` (cit. on p. 40).

[Hei+16] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. “Tables of subspace codes”. In: *arXiv preprint 1601.02864* (2016) (cit. on pp. 14, 36, 89, 90, 101, 103, 107, 113, 125, 127, 132, 144, 146, 197).

[Hei+17a] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. “Classifying optimal binary subspace codes of length 8, constant dimension 4 and minimum distance 6”. In: *arXiv preprint 1711.06624* (2017). Accepted in Designs, Codes and Cryptography. (cit. on pp. 15, 118, 185, 187, 193, 196).

[Hei+17b] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. “Projective divisible binary codes”. In: The Tenth International Workshop on Coding and Cryptography. 2017 (cit. on p. 121).

[Hei+17c] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. “A subspace code of size 333 in the setting of a binary q-analog of the Fano plane”. In: *arXiv preprint 1708.06224* (2017). Submitted to IEEE Transactions on Information Theory (cit. on pp. 15, 161, 162).

[Hei+on] Daniel Heinlein, Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Classification of binary MRD codes”. In: (in preparation) (cit. on p. 196).

[Hei18] Daniel Heinlein. “New LMRD bounds for constant dimension codes and improved constructions”. In: *arXiv preprint 1801.04803* (2018). Submitted to IEEE Transactions on Information Theory (cit. on pp. 14, 61, 89, 99).

[HK16] Thomas Honold and Michael Kiermaier. “On putative q-Analogues of the Fano Plane and Related Combinatorial Structures”. In: *Dynamical systems, number theory and applications.* World Sci. Publ., Hackensack, NJ, 2016, pp. 141–175 (cit. on pp. 145, 162).

[HK17a] Daniel Heinlein and Sascha Kurz. “An upper bound for binary subspace codes of length 8, constant dimension 4 and minimum distance 6”. In: The Tenth International Workshop on Coding and Cryptography. 2017 (cit. on pp. 15, 89, 119, 185, 197, 198).

[HK17b] Daniel Heinlein and Sascha Kurz. “Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound”. In: *Coding theory and applications.* Vol. 10495. Lecture Notes in Computer Science. Springer, 2017, pp. 163–191 (cit. on pp. 15, 21, 89, 107, 108, 111, 114–116, 125–129, 131–134, 137, 138, 141, 143, 145, 146).

[HK17c] Daniel Heinlein and Sascha Kurz. “Coset Construction for Subspace Codes”. In: *IEEE Transactions on Information Theory* 63.12 (2017), pp. 7651–7660 (cit. on pp. 14, 67, 68, 70, 71, 74, 75, 77, 80, 81, 84–87, 89, 235).

[HK18] Daniel Heinlein and Sascha Kurz. “Binary Subspace Codes in Small Ambient Spaces”. In: *Advances in Mathematics of Communications* 13.4 (2018), pp. 817–839 (cit. on p. 35).

[HKK15] Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Minimum Distance 4”. In: *Topics in finite fields*. Vol. 632. Contemp. Math. Amer. Math. Soc., Providence, RI, 2015, pp. 157–176. URL: https://doi.org/10.1090/conm/632/12627 (cit. on pp. 57, 86, 88–90, 107, 119).

[HKK16a] Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Classification of large partial plane spreads in PG(6, 2) and related combinatorial objects”. In: *arXiv preprint 1606.07655* (2016) (cit. on pp. 190, 196, 197).

[HKK16b] Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Constructions and Bounds for Mixed-Dimension Subspace Codes”. In: *Adv. Math. Commun.* 10.3 (2016), pp. 649–682. ISSN: 1930-5346. URL: https://doi.org/10.3934/amc.2016033 (cit. on pp. 20, 33–36, 48, 197).

[HKK18a] Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Partial spreads and vector space partitions”. In: *Network Coding and Subspace Designs*. Ed. by M. Greferath, M.O. Pavčević, N. Silberstein, and A. Vazquez-Castro. arXiv preprint 1611.06328. Springer, 2018 (cit. on pp. 121, 122).

[HKK18b] Thomas Honold, Michael Kiermaier, and Sascha Kurz. “Partial spreads and vector space partitions”. In: *Network Coding and Subspace Designs*. Springer, 2018, pp. 131–170 (cit. on p. 121).

[HM17] Anna-Lena Horlemann-Trautmann and Kyle Marshall. “New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions”. In: *Adv. Math. Commun.* 11.3 (2017), pp. 533–548. ISSN: 1930-5346. URL: https://doi.org/10.3934/amc.2017042 (cit. on p. 37).

[Ho+03] Tracey Ho, Ralf Kötter, Muriel Medard, David R. Karger, and Michelle Effros. “The benefits of coding over routing in a randomized setting”. In: (2003) (cit. on p. 13).

[HR18] Anna-Lena Horlemann-Trautmann and Joachim Rosenthal. “Constructions of Constant Dimension Codes”. In: *Network Coding and Subspace Designs*. Springer, 2018, pp. 25–42 (cit. on p. 60).

[HS16] Olof Heden and Papa A. Sissokho. “On the existence of a $(2,3)$-spread in $V(7,2)$”. In: *Ars Combin.* 124 (2016), pp. 161–164. ISSN: 0381-7032 (cit. on p. 162).

[IBM10] IBM. *IBM ILOG CPLEX Optimizer*. 2010. URL: http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/ (cit. on pp. 194, 196).

[JJ98] Gareth A. Jones and J. Mary Jones. *Elementary number theory*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998, pp. xiv+301. ISBN: 3-540-76197-7. URL: https://doi.org/10.1007/978-1-4471-0613-5 (cit. on p. 38).

[Joh62] Selmer M. Johnson. “A new upper bound for error-correcting codes”. In: *IRE Trans.* IT-8 (1962), pp. 203–207 (cit. on pp. 113, 114).

[KK08a] Axel Kohnert and Sascha Kurz. “Construction of large constant dimension codes with a prescribed minimum distance”. In: *Mathematical methods in computer science*. Vol. 5393. Lecture Notes in Comput. Sci. Springer, Berlin, 2008, pp. 31–42. URL: https://doi.org/10.1007/978-3-540-89994-5_4 (cit. on pp. 145, 166, 171).

[KK08b] Ralf Kötter and Frank R. Kschischang. "Coding for Errors and Erasures in Random Network Coding". In: *IEEE Trans. Inform. Theory* 54.8 (2008), pp. 3579–3591. ISSN: 0018-9448. URL: https://doi.org/10.1109/TIT.2008.926449 (cit. on pp. 13, 20, 24, 27, 108, 110, 112, 113, 137).

[KK17] Michael Kiermaier and Sascha Kurz. "An improvement of the Johnson bound for subspace codes". In: *arXiv preprint 1707.00650* (2017) (cit. on pp. 118, 142).

[KKW17] Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. "The order of the automorphism group of a binary q-analog of the Fano plane is at most two". In: *Designs, Codes and Cryptography* (2017), pp. 1–12. ISSN: 1573-7586. DOI: 10.1007/s10623-017-0360-6. URL: http://dx.doi.org/10.1007/s10623-017-0360-6 (cit. on p. 162).

[KM79] Mikhail I. Kargapolov and Jurij I. Merzljakov. *Fundamentals of the theory of groups*. Vol. 62. Graduate Texts in Mathematics. Translated from the second Russian edition by Robert G. Burns. Springer-Verlag, New York-Berlin, 1979, pp. xvii+203. ISBN: 0-387-90396-8 (cit. on pp. 28–30).

[Knu71] Donald E. Knuth. "Subspaces, subsets, and partitions". In: *J. Combinatorial Theory Ser. A* 10 (1971), pp. 178–180 (cit. on p. 24).

[Koc70] Rudolf Kochendörffer. *Group theory*. McGraw-Hill, 1970 (cit. on pp. 29, 30).

[KP15] Michael Kiermaier and Mario Osvin Pavčević. "Intersection numbers for subspace designs". In: *J. Combin. Des.* 23.11 (2015), pp. 463–480. ISSN: 1063-8539. URL: https://doi.org/10.1002/jcd.21403 (cit. on p. 162).

[KS04] Hans Kurzweil and Bernd Stellmacher. *The theory of finite groups*. Universitext. An introduction, Translated from the 1998 German original. Springer-Verlag, New York, 2004, pp. xii+387. ISBN: 0-387-40510-0. URL: https://doi.org/10.1007/b97433 (cit. on pp. 28, 30, 31).

[KSK09] Azadeh Khaleghi, Danilo Silva, and Frank R. Kschischang. "Subspace Codes". In: *Cryptography and coding*. Vol. 5921. Lecture Notes in Comput. Sci. Springer, Berlin, 2009, pp. 1–21. URL: https://doi.org/10.1007/978-3-642-10868-6_1 (cit. on pp. 107, 111, 112, 116, 117).

[Kur17a] Sascha Kurz. "Improved upper bounds for partial spreads". In: *Des. Codes Cryptogr.* 85.1 (2017), pp. 97–106. ISSN: 0925-1022. URL: https://doi.org/10.1007/s10623-016-0290-8 (cit. on p. 121).

[Kur17b] Sascha Kurz. "Packing vector spaces into vector spaces". In: *Australas. J. Combin.* 68.1 (2017), pp. 122–130. ISSN: 1034-4942 (cit. on pp. 121, 122).

[Lan90] Serge Lang. *Undergraduate algebra. 2nd ed.* English. 2nd ed. New York etc.: Springer-Verlag, 1990, pp. xi + 367. ISBN: 0-387-97279-X (cit. on p. 33).

[LH14] Haiteng Liu and Thomas Honold. "A New Approach to the Main Problem of Subspace Coding". In: *arXiv preprint 1408.1181* (2014) (cit. on p. 89).

[LYC03] Shuo-Yen Robert Li, Raymond W. Yeung, and Ning Cai. "Linear network coding". In: *IEEE Trans. Inform. Theory* 49.2 (2003), pp. 371–381. ISSN: 0018-9448. URL: https://doi.org/10.1109/TIT.2002.807285 (cit. on p. 11).

[Met99] Klaus Metsch. "Bose-Burton type theorems for finite projective, affine and polar spaces". In: *Surveys in combinatorics, 1999 (Canterbury)*. Vol. 267. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1999, pp. 137–166 (cit. on p. 162).

[MMY95] Masashi Miyakawa, Akihiro Munemasa, and Satoshi Yoshiara. “On a class of small 2-designs over GF(q)”. In: *J. Combin. Des.* 3.1 (1995), pp. 61–77. ISSN: 1063-8539. URL: `https://doi.org/10.1002/jcd.3180030108` (cit. on p. 162).

[MS77a] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–xv and 1–369. ISBN: 0-444-85009-0 (cit. on p. 34).

[MS77b] Florence J. MacWilliams and Neil J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, i–ix and 370–762. ISBN: 0-444-85010-4 (cit. on pp. 44, 45, 115).

[NÖ03] Sampo Niskanen and Patric R. J. Östergård. *Cliquer User's Guide, Version 1.0.* Tech. rep. T48. Espoo, Finland: Communications Laboratory, Helsinki University of Technology, 2003 (cit. on pp. 85, 194, 195, 197, 198).

[NS17] Esmeralda L. Năstase and Papa A. Sissokho. “The maximum size of a partial spread in a finite projective space”. In: *J. Combin. Theory Ser. A* 152 (2017), pp. 353–362. ISSN: 0097-3165. URL: `https://doi.org/10.1016/j.jcta.2017.06.012` (cit. on p. 122).

[OÖ18] Kamil Otal and Ferruh Özbudak. “Constructions of Cyclic Subspace Codes and Maximum Rank Distance Codes”. In: *Network Coding and Subspace Designs.* Springer, 2018, pp. 43–66 (cit. on p. 37).

[Pit14] Leonidas S. Pitsoulis. *Topics in matroid theory.* SpringerBriefs in Optimization. Springer, New York, 2014, pp. xiv+127. ISBN: 978-1-4614-8956-6; 978-1-4614-8957-3. URL: `https://doi.org/10.1007/978-1-4614-8957-3` (cit. on pp. 43, 235).

[PS00] Jonathan Pakianathan and Krishnan Shankar. “Nilpotent numbers”. In: *Amer. Math. Monthly* 107.7 (2000), pp. 631–634. ISSN: 0002-9890. URL: `https://doi.org/10.2307/2589118` (cit. on p. 29).

[PS93] William R Pulleyblank and Bruce Shepherd. “Formulations for the stable set polytope”. In: *Proceedings Third IPCO Conference.* 1993, pp. 267–279 (cit. on p. 39).

[Rom12] Steven Roman. *Fundamentals of group theory. An advanced approach.* English. Boston, MA: Birkhäuser, 2012, pp. xii + 380. ISBN: 978-0-8176-8300-9/hbk; 978-0-8176-8301-6/ebook. DOI: `10.1007/978-0-8176-8301-6` (cit. on pp. 31, 32).

[Ros95] Guido Rossum. *Python Reference Manual.* Tech. rep. Amsterdam, The Netherlands, The Netherlands, 1995 (cit. on p. 178).

[Rot91] Ron M. Roth. “Maximum-rank array codes and their application to crisscross error correction”. In: *IEEE Trans. Inform. Theory* 37.2 (1991), pp. 328–336. ISSN: 0018-9448. URL: `https://doi.org/10.1109/18.75248` (cit. on p. 37).

[SE11] Natalia Silberstein and Tuvi Etzion. “Large constant dimension codes and lexicodes”. In: *Adv. Math. Commun.* 5.2 (2011), pp. 177–189. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2011.5.177` (cit. on pp. 59, 103).

[Seg64] Beniamino Segre. “Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane”. In: *Ann. Mat. Pura Appl. (4)* 64.1 (1964), pp. 1–76. ISSN: 0003-4622. URL: `https://doi.org/10.1007/BF02410047` (cit. on p. 120).

[SK09] Danilo Silva and Frank R. Kschischang. "On metrics for error correction in network coding". In: *IEEE Trans. Inform. Theory* 55.12 (2009), pp. 5479–5490. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2009.2032817` (cit. on pp. 27, 32).

[Ska10] Vitaly Skachek. "Recursive code construction for random networks". In: *IEEE Trans. Inform. Theory* 56.3 (2010), pp. 1378–1382. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2009.2039163` (cit. on p. 61).

[SKK08] Danilo Silva, Frank R. Kschischang, and Ralf Kötter. "A rank-metric approach to error control in random network coding". In: *IEEE Trans. Inform. Theory* 54.9 (2008), pp. 3951–3967. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2008.928291` (cit. on pp. 13, 61).

[Soh14] Houshang H. Sohrab. *Basic real analysis. 2nd extended ed.* English. 2nd extended ed. New York, NY: Birkhäuser/Springer, 2014, pp. xi + 683. ISBN: 978-1-4939-1840-9/hbk; 978-1-4939-1841-6/ebook. DOI: `10.1007/978-1-4939-1841-6` (cit. on p. 143).

[ST13] Natalia Silberstein and Anna-Lena Trautmann. "New lower bounds for constant dimension codes". In: *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on.* IEEE. 2013, pp. 514–518 (cit. on p. 89).

[ST15] Natalia Silberstein and Anna-Lena Trautmann. "Subspace Codes based on Graph Matchings, Ferrers Diagrams and Pending Blocks". In: *IEEE Trans. Inform. Theory* 61.7 (2015), pp. 3937–3953. ISSN: 0018-9448. URL: `https://doi.org/10.1109/TIT.2015.2435743` (cit. on pp. 61, 89, 103, 125, 146).

[Tho68] John G. Thompson. "Nonsolvable finite groups all of whose local subgroups are solvable". In: *Bull. Amer. Math. Soc.* 74 (1968), pp. 383–437. ISSN: 0002-9904. URL: `https://doi.org/10.1090/S0002-9904-1968-11953-6` (cit. on p. 29).

[Tho87] Simon Thomas. "Designs over finite fields". In: *Geom. Dedicata* 24.2 (1987), pp. 237–242. ISSN: 0046-5755. URL: `https://doi.org/10.1007/BF00150939` (cit. on pp. 162, 171).

[Tho96] Simon Thomas. "Designs and partial geometries over finite fields". In: *Geom. Dedicata* 63.3 (1996), pp. 247–253. ISSN: 0046-5755. URL: `https://doi.org/10.1007/BF00181415` (cit. on p. 162).

[Ton98] Vladimir D. Tonchev. "Codes and designs". In: *Handbook of coding theory, Vol. I, II.* North-Holland, Amsterdam, 1998, pp. 1229–1267 (cit. on p. 113).

[TR10] Anna-Lena Trautmann and Joachim Rosenthal. "New Improvements on the Echelon-Ferrers Construction". In: *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems–MTNS.* Vol. 5. 9. 2010 (cit. on p. 77).

[Tra13a] Anna-Lena Trautmann. "A lower bound for constant dimension codes from multi-component lifted MRD codes". In: *arXiv preprint: 1301.1918, 4 pages* (2013) (cit. on pp. 62, 63).

[Tra13b] Anna-Lena Trautmann. "Constructions, decoding and automorphisms of subspace codes". In: *PhD, University of Zürich* (2013), p. 112 (cit. on p. 178).

[Tra13c] Anna-Lena Trautmann. "Isometry and automorphisms of constant dimension codes". In: *Adv. Math. Commun.* 7.2 (2013), pp. 147–160. ISSN: 1930-5346. URL: `https://doi.org/10.3934/amc.2013.7.147` (cit. on pp. 33, 40, 178).

[WXS03] Huaxiong Wang, Chaoping Xing, and Rei Safavi-Naini. “Linear authentication codes: bounds and constructions”. In: *IEEE Trans. Inform. Theory* 49.4 (2003), pp. 866–872. ISSN: 0018-9448. URL: https://doi.org/10.1109/TIT.2003.809567 (cit. on p. 110).

[XF09] Shu-Tao Xia and Fang-Wei Fu. “Johnson type bounds on constant dimension codes”. In: *Des. Codes Cryptogr.* 50.2 (2009), pp. 163–172. ISSN: 0925-1022. URL: https://doi.org/10.1007/s10623-008-9221-7 (cit. on pp. 112–115, 117).

[ZJX11] Zong-Ying Zhang, Yong Jiang, and Shu-Tao Xia. “On the Linear Programming Bounds for Constant Dimension Codes”. In: *Network Coding (NetCod), 2011 International Symposium on*. IEEE. 2011, pp. 1–4 (cit. on pp. 46, 117, 119).

[Zum16] Jens Zumbrägel. “Designs and codes in affine geometry”. In: *arXiv preprint 1605.03789* (2016) (cit. on p. 178).

Publications of the author

[Hei+16] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. "Tables of subspace codes". In: *arXiv preprint 1601.02864* (2016).

[Hei+17a] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. "Classifying optimal binary subspace codes of length 8, constant dimension 4 and minimum distance 6". In: *arXiv preprint 1711.06624* (2017). Accepted in Designs, Codes and Cryptography.

[Hei+17b] Daniel Heinlein, Thomas Honold, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. "Projective divisible binary codes". In: The Tenth International Workshop on Coding and Cryptography. 2017.

[Hei+17c] Daniel Heinlein, Michael Kiermaier, Sascha Kurz, and Alfred Wassermann. "A subspace code of size 333 in the setting of a binary q-analog of the Fano plane". In: *arXiv preprint 1708.06224* (2017). Submitted to IEEE Transactions on Information Theory.

[Hei+18] Daniel Heinlein, Thomas Honold, Michael Kiermaier, and Sascha Kurz. "Generalized vector space partitions". In: *arXiv preprint 1803.10180* (2018). Accepted in Australasian Journal of Combinatorics.

[Hei18] Daniel Heinlein. "New LMRD bounds for constant dimension codes and improved constructions". In: *arXiv preprint 1801.04803* (2018). Submitted to IEEE Transactions on Information Theory.

[HK17a] Daniel Heinlein and Sascha Kurz. "An upper bound for binary subspace codes of length 8, constant dimension 4 and minimum distance 6". In: The Tenth International Workshop on Coding and Cryptography. 2017.

[HK17b] Daniel Heinlein and Sascha Kurz. "Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound". In: *Coding theory and applications*. Vol. 10495. Lecture Notes in Computer Science. Springer, 2017, pp. 163–191.

[HK17c] Daniel Heinlein and Sascha Kurz. "Coset Construction for Subspace Codes". In: *IEEE Transactions on Information Theory* 63.12 (2017), pp. 7651–7660.

[HK18] Daniel Heinlein and Sascha Kurz. "Binary Subspace Codes in Small Ambient Spaces". In: *Advances in Mathematics of Communications* 13.4 (2018), pp. 817–839.

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die von mir angegebenen Quellen und Hilfsmittel verwendet habe. Weiterhin erkläre ich, dass ich die Hilfe von gewerblichen Promotionsberatern bzw. -vermittlern oder ähnlichen Dienstleistern weder bisher in Anspruch genommen habe, noch künftig in Anspruch nehmen werde.
Zusätzlich erkläre ich hiermit, dass ich keinerlei frühere Promotionsversuche unternommen habe.

Erklärung

gemäß §4 PromO

Hiermit erkläre ich, dass ich nicht diese oder eine andere gleichartige Doktorprüfung nicht bestanden habe.
Des Weiteren erkläre ich, dass ich nicht bereits an einer anderen Hochschule oder einer anderen promovierenden Einrichtung der Universität Bayreuth im gleichen Fach zur Promotion angenommen bin.

Einverständniserklärung

gemäß §8 (7) und (8) PromO

Hiermit erkläre ich mich einverstanden, dass die elektronische Fassung meiner Dissertation unter Wahrung meiner Urheberrechte und des Datenschutzes einer gesonderten Überprüfung unterzogen werden kann.
Des Weiteren erkläre ich mich einverstanden, dass bei Verdacht wissenschaftlichen Fehlverhaltens Ermittlungen durch universitätsinterne Organe der wissenschaftlichen Selbstkontrolle stattfinden können.

Bayreuth, den