

# Divisible minimal codes

Sascha Kurz

Mathematisches Institut, Universität Bayreuth, D-95440 Bayreuth, Germany,  
sascha.kurz@uni-bayreuth.de

## Abstract

Minimal codes are linear codes where all non-zero codewords are minimal, i.e., whose support is not properly contained in the support of another codeword. The minimum possible length of such a  $k$ -dimensional linear code over  $\mathbb{F}_q$  is denoted by  $m(k, q)$ . Here we determine  $m(7, 2)$ ,  $m(8, 2)$ , and  $m(9, 2)$ , as well as full classifications of all codes attaining  $m(k, 2)$  for  $k \leq 7$  and those attaining  $m(9, 2)$ . For  $m(11, 2)$  and  $m(12, 2)$  we give improved upper bounds. It turns out that in many cases attaining extremal codes have the property that the weights of all codewords are divisible by some constant  $\Delta > 1$ . So, here we study the minimum lengths of minimal codes where we additionally assume that the weights of the codewords are divisible by  $\Delta$ .

## 1 Introduction

Let  $\mathbb{F}_q$  be a finite field of cardinality  $q$  and  $C \subseteq \mathbb{F}_q^n$  be a linear code. If  $C$  has cardinality  $q^k$ , then we speak of an  $[n, k]_q$ -code. A non-zero codeword  $c \in C$  is called *minimal* if the *support*  $\text{supp}(c) := \{i \mid c_i \neq 0\}$  of  $c$  is minimal with respect to inclusion in the set  $\{\text{supp}(u) \mid u \in C \setminus \mathbf{0}\}$ . The code  $C$  is a *minimal code* if all of its non-zero codewords are minimal. One of the many applications of minimal codes is secret sharing, see e.g. [AB98]. An important line of research is the determination of the minimum possible length  $n$  of a minimal  $[n, k]_q$ -code, which we denote by  $m(k, q)$ . In e.g. [ABNR22, Theorem 2.14] the lower bound  $m(k, q) \geq (q + 1)(k - 1)$  was shown. Here we determine  $m(7, 2)$ ,  $m(8, 2)$ , and  $m(9, 2)$ , as well as full classifications of all codes attaining  $m(k, 2)$  for  $k \leq 7$  and those attaining  $m(9, 2)$ . For  $m(11, 2)$  and  $m(12, 2)$  we give improved upper bounds.

A linear  $[n, k]_q$ -code is called  $\Delta$ -divisible if all of its weights are divisible by  $\Delta$ . For some background we refer e.g. to the recent survey [Kur21]. Minimal codes constructed by concatenation with simplex codes, see e.g. [ABN23, BB23], naturally come with a non-trivial divisibility constant  $\Delta > 1$ . The unique example attaining  $m(2, q) = q$ , which geometrically corresponds to the points of a line, is  $q$ -divisible. For  $k' \leq 3$  all minimal binary codes of length  $m(2k', 2)$  are 2-divisible and for dimension  $k = 8$  there are minimal binary codes of length  $m(8, 2) = 24$  that are 2-divisible while not all examples are of this type. In [Kur23] it was shown that the unique minimal code attaining  $m(5, 3) = 19$  is 3-divisible. So, at least for the small parameters we have considered here there exist  $q$ -divisible examples of minimum possible size  $m(k, q)$  whenever the lower bound  $(q - 1)(k - 1) + 1$  on the minimum distance, see Theorem 2.(b), is divisible by  $q$ .<sup>1</sup> We remark that also some constructions for minimal codes are based on few-weight codes, which often have a non-trivial divisibility constant, see e.g. [MS19, SF20, SL21]. Due to the mentioned possible relations between minimal and divisible codes we introduce the minimum possible length  $n = m(k, q; \Delta)$  of a  $\Delta$ -divisible minimal  $[n, k]_q$ -code. Here we initiate the study of  $m(k, q; \Delta)$  and give bounds and exact values, both computationally and theoretically.

The remaining part of this paper is structured as follows. In Section 2 we state the necessary preliminaries before we study bounds and exact values for  $m(k, q; \Delta)$  in Section 3. For the special case of binary minimal codes with trivial divisibility  $\Delta = 1$  we study the minimum possible length  $m(k, 2; 1) = m(k, 2)$  in Section 4.

<sup>1</sup>The second case where this condition is met, after the first  $k = 2$ , is at dimension  $k = q + 2$ .

## 2 Preliminaries

First we consider the well-known correspondence between (non-degenerated)  $[n, k]_q$ -codes and multisets of points in the projective space  $\text{PG}(k-1, q)$  of cardinality  $n$ , i.e., the columns of a generator matrix each generate a point, see e.g. [DS98]. We represent each multiset of points in  $\text{PG}(v-1, q)$  by a mapping  $M: \mathcal{P} \rightarrow \mathbb{N}_{\geq 0}$  from the set of points  $\mathcal{P}$  in  $\text{PG}(v-1, q)$  to the non-negative integers, i.e., to each point  $P$  we assign a multiplicity  $M(P)$ . We extend this notion to arbitrary subspaces  $S$  by defining  $M(S)$  as the sum over all point multiplicities  $M(P)$  for all points  $P$  in  $S$ . The cardinality of  $M$ , i.e., the sum of the multiplicities of all points, is denoted by  $\#M$ . We say that a multiset  $M$  of points is *spanning* if the points with positive multiplicity span the entire ambient space.

**Definition 1.** *A multiset  $M$  of points in a projective space is called a strong blocking multiset if for every hyperplane  $H$ , we have  $\langle S \cap H \rangle = H$ .*

If  $M$  is the multiset of points associated to a linear code  $C$ , then  $C$  is minimal iff  $M$  is a strong blocking multiset, see e.g. [ABN22, TQLZ21]. Directly from the definition of a strong blocking multiset we can read off that a multiset of points in  $\text{PG}(1, q)$  is a strong blocking multiset iff it contains every point of the entire projective space. Clearly adding points to a multiset does not destroy the property of being a strong blocking multiset, so that we consider *minimal strong blocking sets* in the following, i.e., set of points that are a strong blocking multiset but such that every proper subset is not a strong blocking multiset. So, in  $\text{PG}(1, q)$  the unique minimal strong blocking set is a line, so that

$$m(2, q) = q. \tag{1}$$

Since each linear code associated to the point set of a  $k$ -dimensional subspace over  $\mathbb{F}_q$  is  $q$ -divisible, see e.g. [KK20, Lemma 2.a], we have

$$m(2, q; q) = q \tag{2}$$

for each positive integer  $\Delta$ . For dimension  $k = 1$  we clearly have  $m(1, q) = 1$  and  $m(1, q; \Delta) = \Delta$  for all  $\Delta \in \mathbb{N}_{\geq 1}$ .

The representation of a linear code  $C$  by a multiset of points  $M$  is pretty useful. If we multiply the multiplicity  $M(P)$  of every point  $P$  by some positive integer  $t$ , the cardinality as well as the divisibility is increased by a factor of  $t$ . So, we have

$$m(k, q) \leq m(k, q; \Delta) \leq \Delta \cdot m(k, q) \tag{3}$$

for all  $\Delta \in \mathbb{N}_{\geq 1}$ . Our examples for dimensions 1 and 2 show that both bounds can be attained with equality. Similarly, we have

$$m(k, q; \Delta) \leq m(k, q; t \cdot \Delta) \leq t \cdot m(k, q; \Delta) \tag{4}$$

for all  $\Delta, t \in \mathbb{N}_{\geq 1}$ . If  $t$  is coprime to  $q$ , then a  $t$ -divisible linear code over  $\mathbb{F}_q$  is a  $t$ -fold repetition of a smaller code, see e.g. [War81, Theorem 1]. So, we have

$$m(k, q; t \cdot \Delta) = t \cdot m(k, q; \Delta) \tag{5}$$

for all  $t \in \mathbb{N}_{\geq 1}$  with  $\gcd(q, t) = 1$ . For binary codes we can consider extension by a parity bit to conclude

$$m(k, 2; 2) \leq m(k, 2; 1) + 1. \tag{6}$$

Given a linear code  $C$  the *weight*  $\text{wt}(c)$  of a codeword  $c \in C$  is the number of non-zero entries. With this, the minimum Hamming distance  $d$  of  $C$  is the minimum weight over all non-zero codewords of  $C$ . If an  $[n, k]_q$ -code has minimum Hamming distance  $d$  then we also speak of an  $[n, k, d]_q$ -code. We summarize the current knowledge on general bounds for the length  $n$ , the minimum (non-zero) weight  $w_{\min}$ , and the maximum (non-zero) weight  $w_{\max}$  of a minimal linear code as follows:

**Theorem 2.** For each minimal  $[n, k]_q$ -code we have

- (a)  $n \geq (q + 1)(k - 1)$ ;
- (b)  $d = w_{\min} \geq (k - 1)(q - 1) + 1$ ; and
- (c)  $w_{\max} \leq n - k + 1$ .

*Proof.* For (a) see e.g. [ABNR22, Theorem 2.14], for (b) see e.g. [HN21, Theorem 23] or [ABNR22, Theorem 2.8], and for (c) see [ABNR22, Proposition 1.5].  $\square$

### 3 Minimum lengths of divisible minimal codes

In this section we consider the determination of the smallest possible length  $n = m(k, q; \Delta)$  of a minimal  $\Delta$ -divisible  $[n, k]_q$ -code. For dimensions  $k \leq 2$  the results are stated easily using the geometric reformulation of linear codes as multisets of points. Clearly, we have  $m(1, q; \Delta) = \Delta$  attained by a  $\Delta$ -fold point. For dimension  $k = 2$  each point has multiplicity at least 1 since the code has to be minimal. From  $\Delta$ -divisibility we conclude that the point multiplicities are pairwise congruent modulo  $\Delta$ , so that the minimum possible length is attained if all point multiplicities are equal. Thus, we have  $m(2, q; \Delta) = \frac{(q+1)\Delta}{q}$  if  $\Delta$  is divisible by  $q$  (attained by a  $\Delta/q$ -fold line) and  $m(2, q; \Delta) = (q + 1)\Delta$  (attained by a  $\Delta$ -fold line). Due to Equation (5) it suffices to consider the cases where  $\Delta$  does not contain a non-trivial factor  $t$  that is coprime to the field size  $q$ .

If the divisibility constant is large enough, when considering power of the characteristic only, we can give a precise answer:

**Proposition 3.** For  $r \geq k - 1$  we have  $m(k, q; q^r) = q^{r-k+1} \cdot \frac{q^k - 1}{q - 1}$ .

*Proof.* Since the code is  $q^r$ -divisible we have  $d \geq q^r$ , so that we can apply the Griesmer bound for the lower bound. An attaining example is given by the  $q^{r-k+1}$ -fold full  $k$ -space.  $\square$

**Proposition 4.** For  $k \geq 2$  we have  $m(k, 2; 2^{k-2}) = 2^k - 1$ .

*Proof.* Since the  $k$ -dimensional simplex code is  $2^{k-1}$ -divisible and minimal, we have  $m(k, 2; 2^{k-2}) \leq 2^k - 1$ , so that we assume  $n \leq 2^k - 1$  for the length of an attaining code  $C$ . Note that the possible non-zero weights of  $C$  are given by  $i \cdot 2^{k-2}$  for  $1 \leq i \leq 3$ .

If  $c \in C$  is a codeword of weight  $3 \cdot 2^{k-2}$ , then the corresponding residual code  $C_c$  has length at most  $2^{k-2} - 1$  and dimension  $k - 1$  (since  $C$  is minimal). Thus, we have  $k \geq 3$  and  $C_c$  is  $2^{k-3}$ -divisible with  $2^{k-3}$  as the unique non-zero weight. Since one-weight codes are repetitions of simplex codes, see e.g. [Bon84],  $C_c$  can have dimension of at most  $k - 2$  — contradiction.

So, let  $a_1$  be the number of codewords of weight  $2^{k-2}$  and  $a_2$  be the number of codewords of weight  $2^{k-1}$ . From the first two MacWilliams equations we compute  $a_1 + a_2 = 2^k - 1$  and  $2n = a_1 + 2a_2$ , so that  $a_1 = 2^{k+1} - 2 - 2n$ , i.e.,  $a_1$  is even. Since the code is minimal, the sum of any two different codewords of weight  $2^{k-2}$  has again weight  $2^{k-2}$ , i.e. the codewords of the smallest weight form subcode and we have  $a_1 = 2^t - 1$  for some integer  $t$ .<sup>2</sup> Thus, we have  $t = 0$  and  $a_1 = 0$ , i.e., we have  $d \geq 2^{k-1}$  for the minimum distance and can apply the Griesmer bound for the lower bound  $n \geq 2^k - 1$ .  $\square$

For parameters not covered by these two propositions and dimension  $k \geq 3$  we have applied the software `LinCode` for the enumeration of linear codes [BBK21] using the bounds for the minimum and maximum possible weight in Theorem 2 and also using the weight restrictions implied by the divisibility constant  $\Delta$ . For field sizes  $q = 2$  and  $q = 3$  we summarize our numerical results in Table 1. With this,  $m(k, q; \Delta)$  is completely determined for  $k \leq 9$  if  $q = 2$  and for  $k \leq 5$  if  $q = 3$ .

<sup>2</sup>We remark that  $\Delta$ -divisible linear codes spanned by codewords of weight  $\Delta$  have been completely classified in [KK23a]. Note that there exists a  $2^{k-2}$ -divisible linear code of length  $2^{k-1}$  and dimension  $k$  satisfying  $a_1 = 2^k - 2$ ,  $a_2 = 1$ . However, this code, corresponding to an affine subspace, is not minimal.

|                   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |
|-------------------|---|---|----|----|----|----|----|----|----|----|----|----|----|----|
| $k$               | 4 | 4 | 5  | 5  | 5  | 6  | 6  | 6  | 6  | 7  | 7  | 7  | 7  | 7  |
| $q$               | 2 | 2 | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  | 2  |
| $\Delta$          | 1 | 2 | 1  | 2  | 4  | 1  | 2  | 4  | 8  | 1  | 2  | 4  | 8  | 16 |
| $m(k, q; \Delta)$ | 9 | 9 | 13 | 14 | 17 | 15 | 15 | 18 | 36 | 20 | 21 | 26 | 42 | 84 |

  

|                   |    |    |    |    |    |     |    |    |    |    |    |     |     |    |
|-------------------|----|----|----|----|----|-----|----|----|----|----|----|-----|-----|----|
| $k$               | 8  | 8  | 8  | 8  | 8  | 8   | 9  | 9  | 9  | 9  | 9  | 9   | 9   | 10 |
| $q$               | 2  | 2  | 2  | 2  | 2  | 2   | 2  | 2  | 2  | 2  | 2  | 2   | 2   | 2  |
| $\Delta$          | 1  | 2  | 4  | 8  | 16 | 32  | 1  | 2  | 4  | 8  | 16 | 32  | 64  | 4  |
| $m(k, q; \Delta)$ | 24 | 24 | 29 | 45 | 90 | 174 | 26 | 27 | 30 | 58 | 96 | 192 | 384 | 31 |

  

|                   |    |    |     |     |   |    |    |    |    |    |    |    |     |
|-------------------|----|----|-----|-----|---|----|----|----|----|----|----|----|-----|
| $k$               | 10 | 10 | 10  | 10  | 3 | 3  | 4  | 4  | 4  | 5  | 5  | 5  | 5   |
| $q$               | 2  | 2  | 2   | 2   | 3 | 3  | 3  | 3  | 3  | 3  | 3  | 3  | 3   |
| $\Delta$          | 8  | 16 | 32  | 64  | 1 | 3  | 1  | 3  | 9  | 1  | 3  | 9  | 27  |
| $m(k, q; \Delta)$ | 60 | 93 | 186 | 366 | 9 | 12 | 14 | 15 | 38 | 19 | 19 | 48 | 116 |

Table 1: Exact values of  $m(k, q; \Delta)$  for small parameters where  $q \in \{2, 3\}$ .

**Lemma 5.** For each integer  $t \geq 2$  we have  $m(2t, 2; 2^{t-1}) \leq 3 \cdot (2^t - 1)$ .

*Proof.* Consider the linear code  $C$  corresponding to three pairwise disjoint  $t$ -dimensional subspaces of  $\text{PG}(2t-1, 2)$ . With this,  $C$  is an  $[3 \cdot (2^t - 1), 2t]_2$ -code with non-zero weights  $2 \cdot 2^{t-1}$  and  $3 \cdot 2^{t-1}$ , which is minimal due to the Ashikhmin-Barg condition [AB98].  $\square$

We remark that the constructed projective two-weight code contains to the family  $\text{SU}_2$  in [CK86]. While equality is attained in Lemma 5 for  $t \in \{2, 4, 5\}$ , we have  $m(6, 2; 4) = 18 < 21$ .

The interesting codes, i.e. those that cannot be obtained by repetitions of smaller codes, are given by

$$\begin{pmatrix} 1111111111010000 \\ 0000011111101000 \\ 00111000111100100 \\ 01011011001100010 \\ 11100001011100001 \end{pmatrix}$$

attaining  $m(5, 2; 4) = 17$  with weight enumerator  $1 + 25x^8 + 6x^{12}$  and an automorphism group of order 720, as well as

$$\begin{pmatrix} 11111111110100000 \\ 00000111111010000 \\ 001110001111001000 \\ 010110110011000100 \\ 111000010111000010 \\ 011011100101000001 \end{pmatrix}$$

attaining  $m(6, 2; 4) = 18$  with weight enumerator  $1 + 45x^8 + 18x^{12}$  and an automorphism group of order 2160, see [BE97]. For the first code we remark that the automorphism group is isomorphic to the symmetric group  $S_6$  and has point orbits in  $\text{PG}(4, 2)$  of sizes 1, 15 and 15. The unique point has multiplicity 2 in the attaining construction and the points in one of the other classes have multiplicity 1. The unique code









$m(5, 2) = 13$  is attained by exactly two non-equivalent codes given e.g. by generator matrices

$$\begin{pmatrix} 1111110010000 \\ 0001111101000 \\ 1110010100100 \\ 0010101100010 \\ 0101010100001 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1111111010000 \\ 0001111101000 \\ 0110011100100 \\ 1010101100010 \\ 0101110000001 \end{pmatrix}.$$

The corresponding weight enumerators and orders of the automorphism groups are given by  $1 + 8x^5 + 8x^6 + 4x^7 + 7x^8 + 4x^9$ ,  $1 + 6x^5 + 12x^6 + 4x^7 + 3x^8 + 6x^9$  and 8, 48, respectively. For  $m(6, 2) = 15$  there is again a unique example given e.g. by the generator matrix

$$\begin{pmatrix} 111111100100000 \\ 000111110010000 \\ 011001101001000 \\ 100011101000100 \\ 001110101000010 \\ 011010110000001 \end{pmatrix}$$

of a BCH code, see [CL85]. This code has weight enumerator  $1 + 30x^6 + 15x^8 + 18x^{10}$  and an automorphism group of order 360. For a description of this code as the concatenation of two codes we refer to [BB23].

We remark that all above extremal codes meet the bounds for the minimum weight  $w_{\min} \geq (k-1)(q-1) + 1 = k$  (see Theorem 2.(b)) and the maximum weight  $w_{\max} \leq n - k + 1$  (see Theorem 2.(c)). Using these bounds we have applied the software `LinCode` for the enumeration of linear codes [BBK21] to determine  $m(7, 2) = 20$  and  $m(8, 2) = 24$ . For  $k = 7$  there are 33 non-equivalent extremal codes (all with  $w_{\min} = 7$  and  $w_{\max} = 14$ ). Generator matrices for those with more than eight automorphisms are given by

$$\begin{pmatrix} 1111111100001000000 \\ 00001111111100100000 \\ 00110011101110010000 \\ 01010101110110001000 \\ 11011000110100000100 \\ 10001000111010000010 \\ 111100100100100000001 \end{pmatrix}, \begin{pmatrix} 11111111100001000000 \\ 00001111111100100000 \\ 00110011101110010000 \\ 01010100111110001000 \\ 10111001110100000100 \\ 11100101110010000010 \\ 110001101001100000001 \end{pmatrix}, \begin{pmatrix} 11111111100001000000 \\ 00001111111100100000 \\ 00110011101110010000 \\ 01010100111110001000 \\ 10111001110110000100 \\ 11101010001100000010 \\ 110010010110100000001 \end{pmatrix}, \begin{pmatrix} 11111111100001000000 \\ 00001111111100100000 \\ 00110011101110010000 \\ 01011101100110001000 \\ 11111100111010000100 \\ 10110100100110000010 \\ 010011010110100000001 \end{pmatrix}.$$

We remark that there are 88010 minimal  $[22, 7, 8]_2$ -codes. None of them can be extended to a minimal  $[23, 8, 8]_2$ -code. There are e.g. 2778120 minimal  $[22, 6, 8]_2$ -codes. Due to the large number of subcodes we have not enumerated all extensions. So far we have enumerated 2459606 minimal  $[23, 7, 8]_2$  and 31994 minimal  $[24, 8, 8]_2$  non-isomorphic codes. One example is given by the generator matrix

$$\begin{pmatrix} 11111111111100010000000 \\ 00000001111111101000000 \\ 000111100011101100100000 \\ 011000100100111100010000 \\ 001001101101110000001000 \\ 000010111000011100000100 \\ 110111100001110000000010 \\ 0100010000111101000000001 \end{pmatrix}$$

with weight enumerator  $1 + 18x^8 + 30x^9 + 30x^{10} + 30x^{11} + 22x^{12} + 42x^{13} + 42x^{14} + 26x^{15} + 15x^{16}$  and an automorphism group of order 6. (There is also one example with an automorphism group of order 18.) We remark that most of the examples satisfy  $w_{\min} = 8$ ,  $w_{\max} = 17$ , and all intermediate weights occur. Another

example, that is 2-divisible, is given by the generator matrix

$$\begin{pmatrix} 11111111111100010000000 \\ 00000001111111101000000 \\ 000111100011101100100000 \\ 001011100101110100010000 \\ 011101100110110000001000 \\ 001110111101011100000100 \\ 001001101100001100000010 \\ 101100011100100000000001 \end{pmatrix}$$

and has weight enumerator  $1 + 28x^8 + 60x^{10} + 72x^{12} + 68x^{14} + 27x^{16}$ . So far, we found 258 such non-isomorphic examples.

For dimension  $k = 9$  we have slightly changed our algorithmic approach. Using the fact that adding a parity bit to a binary code yields a 2-divisible (also called even) code, we have enumerated all 2-divisible minimal  $[n, 9]_2$ -codes with  $n \leq 27$ . It turns out that there are exactly 5 such non-isomorphic codes with length  $n = 27$  and none with a strictly smaller length. If  $C$  is a minimal  $[n, 9]_2$ -code that is not even, that adding a parity bit yields an even minimal  $[n + 1, 9]_2$ -code. Inverting this operation, we have deleted a column of the above five codes in all possible ways and obtained 34 non-isomorphic  $[26, 9, 9]_2$ -codes of which exactly 4 are minimal, i.e., we have  $m(9, 2) = 26$ . One example is given by

$$\begin{pmatrix} 111111111000000010000000 \\ 000011111111110001000000 \\ 0111000111001111100100000 \\ 0011001001010110100010000 \\ 11010010101100111000010000 \\ 01110110000010110000001000 \\ 01101010110110001000000100 \\ 10011100101001011000000010 \\ 11001101001100010000000001 \end{pmatrix}$$

with weight enumerator  $1 + 32x^9 + 62x^{10} + 64x^{11} + 84x^{12} + 64x^{13} + 44x^{14} + 64x^{15} + 43x^{16} + 32x^{17} + 22x^{18}$  and an automorphism group of order 16.

For dimension  $k = 10$  we remark that [CZ94, Section II.A] reports an example verifying  $m(10, 2) \leq 30$ . The idea was to puncture a 4-divisible (cyclic) minimal  $[31, 10, 12]_2$  code. In Section 3 we have determined all 4-divisible minimal  $[31, 10, 12]_2$  codes. There are exactly two such non-isomorphic codes and also two non-isomorphic puncturings with generator matrices

$$\begin{pmatrix} 111111111111000000100000000 \\ 0000001111111111000010000000 \\ 00111100001111000111001000000 \\ 01011100110011011001000100000 \\ 11101101010001100011000010000 \\ 010101100000011011110000010000 \\ 111010101101011111010000001000 \\ 011100000101111100100000000100 \\ 111101011001000011010000000010 \\ 110110000111000010110000000001 \end{pmatrix} \text{ and } \begin{pmatrix} 111111111111000000100000000 \\ 0000001111111111000010000000 \\ 00111100001111000111001000000 \\ 01011100110011011001000100000 \\ 11101101010001100011000010000 \\ 010101100000011011110000010000 \\ 100110100001101111010000001000 \\ 110100001110011100100000000100 \\ 001010001001011110110000000010 \\ 011100111010100011010000000001 \end{pmatrix}.$$

The codes both have an automorphism group of order five and weight enumerator  $1 + 120x^{11} + 190x^{12} + 272x^{15} + 255x^{16} + 120x^{19} + 66x^{20}$ .

In order to construct small minimal codes in dimensions 11 and 12 we consider a geometric construction. If  $M$  is a multiset of points and  $Q$  is a point in  $\text{PG}(v-1, q)$ , where  $v \geq 2$ , then we can construct a multiset  $M_Q$  by projection through  $Q$ , that is the multiset image under the map  $P \mapsto \langle P, Q \rangle / Q$  setting  $M_Q(L/Q) = M(L) - M(Q)$  for every line  $L \geq P$  in  $\text{PG}(v-1, q)$ . We directly verify the following properties:

**Lemma 7.** *Let  $M$  be a strong blocking multiset  $\text{PG}(k-1, q)$ , where  $k \geq 2$ , and let  $M_Q$  arise from  $M$  by projection through a point  $Q$ . Then we have  $\#M_Q = \#M - M(Q)$ , the span of  $M_Q$  has dimension  $k-1$ , and  $M_Q$  is a strong blocking multiset.*

By  $M'$  we denote the set of points that have positive multiplicity in  $M_Q$ , so that also  $M'$  is a strong blocking (multi-)set in  $\text{PG}(k-1, q)/Q \cong \text{PG}(k-2, q)$ , i.e., we can reduce points with multiplicity larger than one to multiplicity one. So, starting from a minimal  $[n, k]_q$ -code  $C$  we consider the corresponding multiset of points  $M$ , apply projection through a point  $Q$ , reduce point multiplicities to obtain  $M'$ , and then consider the corresponding minimal  $[\#M', k]_q$ -code  $C'$ .

As an example we consider the binary code

$$\begin{pmatrix} 1111110010000 \\ 0001111101000 \\ 1110010100100 \\ 0010101100010 \\ 0101010100001 \end{pmatrix}$$

attaining  $m(5, 2) = 13$ . Choosing  $Q$  as the first column of the generator matrix gives the code  $C'$  with generator matrix

$$\begin{pmatrix} 001111101 \\ 001100110 \\ 010101100 \\ 101010100 \end{pmatrix},$$

which is a representation of the unique code attaining  $m(4, 2) = 9$ , i.e., the union of three disjoint lines. In our examples the lines through column 1 that contain at least three points (which is the maximum for  $q = 2$  and projective codes) are given by the triples of column indices  $(1, 2, 13)$ ,  $(1, 3, 12)$ , and  $(1, 9, 11)$ . Also choosing the point  $Q$  as the second column yields a minimal  $[9, 4]_2$ -code, while all other columns yield (minimal) codes of larger lengths. For projective binary codes or point sets  $M$  in  $\text{PG}(k-1, 2)$  the geometric description of the cardinality of  $M'$  equals  $\#M - 1$  minus the number of full lines through  $Q$ . I.e., if  $Q$  equals the first or the second column, then there are exactly three full lines through  $Q$ , which is the maximum since  $m(4, 2) \geq 9$ . If  $Q$  equals the last column then there is unique full line through  $Q$  and there are exactly two full lines through  $Q$  in all other cases.

Applying projection to the second non-isomorphic code attaining  $m(5, 2) = 13$  yields minimal  $[10, 4]_2$ - and a minimal  $[12, 4]_2$ -code. Applying projection to the unique minimal  $[9, 4]_2$ -code yields the unique minimal  $[6, 3]_2$ -code in all cases. This continues for dimension three and two, as can be easily seen from the geometric description of the extremal point sets. Applying projection to the unique minimal  $[15, 6]_2$ -code yields minimal  $[13, 5]_2$ -codes in all cases (which all have automorphism groups of order 48, i.e. are equivalent to second non-isomorphic  $[13, 5]_2$ -code). We remark that in [Slo93, Table I] the example for a minimal  $[13, 5]_2$ -code was described as “omit coordinates 1,6 from” the (unique) minimal  $[15, 6]_2$ -code. In the same vein a minimal  $[29, 9]_2$ -code was constructed from a minimal  $[31, 10]_2$ -code. We remark that applying projection to the

minimal  $[26, 9]_2$ -code

$$\begin{pmatrix} 111111111100000010000000 \\ 0000011111111110001000000 \\ 0011100011100111100100000 \\ 0101100100101010100010000 \\ 1110001111010001100001000 \\ 0010111101000111000000100 \\ 10001100111011001000000100 \\ 10110101110111111000000010 \\ 11001001110110100000000001 \end{pmatrix}$$

gives minimal  $[n, 8]_2$ -codes for  $n \in \{24, 25\}$ . This phenomenon also occurs for field sizes larger than 2.

The inversion of the projection transformation gives rise to an integer linear programming formulation to search for minimal codes of small length. Starting with the first minimal  $[30, 10]_2$  code let us find the following minimal  $[35, 11]_2$  code with generator matrix

$$\begin{pmatrix} 11011110101100100010110010010101000 \\ 0100000000011000110110110000011100 \\ 00110000000101000110111101011100100 \\ 00001000000010011000011100000010111 \\ 00000100000101011110111010101110101 \\ 00000010000111010110010101100000001 \\ 00000001100011010000111011010010001 \\ 0000000010001001110010111001110011 \\ 000000000111100000001111000001111 \\ 0000000000000011111000000111111111 \\ 0000000000000000001111111111111111 \end{pmatrix},$$

weight enumerator  $1 + 19x^{11} + 83x^{12} + 142x^{13} + 118x^{14} + 125x^{15} + 194x^{16} + 296x^{17} + 356x^{18} + 237x^{19} + 141x^{20} + 134x^{21} + 102x^{22} + 67x^{23} + 29x^{24} + 4x^{25}$  and a trivial automorphism group. Applying the approach again yields the following minimal  $[40, 12]_2$  code with generator matrix

$$\begin{pmatrix} 1001110000000101010110100110011101010111 \\ 0100011001011100100110000000011000111101 \\ 0000011111001000110010100000011000110010 \\ 0000001001010111001110010000000100111000 \\ 0011001101011000111100000000001000001011 \\ 0000100011010111101000001000010000001101 \\ 0000010011010011011100000100000100000011 \\ 0000010111001100111010000010001100001111 \\ 0000001111000111100110000001000000000001 \\ 0000000000111100011110000000111100000111 \\ 00000000000000011111110000000000011111111 \\ 0000000000000000000000001111111111111111 \end{pmatrix},$$

weight enumerator  $1 + 21x^{12} + 70x^{13} + 120x^{14} + 173x^{15} + 183x^{16} + 261x^{17} + 408x^{18} + 493x^{19} + 560x^{20} + 521x^{21} + 408x^{22} + 319x^{23} + 240x^{24} + 167x^{25} + 88x^{26} + 39x^{27} + 19x^{28} + 5x^{29}$  and a trivial automorphism group. We remark that both ILP computations were aborted before finishing.

## Acknowledgments

The author thanks Gianira Alfarano, Anurag Bishnoi, Jozefien D'haeseleer, Dion Gijswijt, Alessandro Neri, Sven Polak, and Martin Scotti for many helpful remarks on an earlier version of this paper, which originally started to investigate so-called triferent codes, see [Kur23].

## References

- [AB98] Alexei Ashikhmin and Alexander Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.
- [ABN22] Gianira N. Alfarano, Martino Borello, and Alessandro Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, 16(1):115–133, 2022.
- [ABN23] Gianira N. Alfarano, Martino Borello, and Alessandro Neri. Outer strong blocking sets. *arXiv preprint 2301.09590*, 2023.
- [ABNR22] Gianira N. Alfarano, Martino Borello, Alessandro Neri, and Alberto Ravagnani. Three combinatorial perspectives on minimal codes. *SIAM Journal on Discrete Mathematics*, 36(1):461–489, 2022.
- [BB23] Daniele Bartoli and Martino Borello. Small strong blocking sets by concatenation. *SIAM Journal on Discrete Mathematics*, 37(1):65–82, 2023.
- [BBK21] Iliya Bouyukliev, Stefka Bouyuklieva, and Sascha Kurz. Computer classification of linear codes. *IEEE Transactions on Information Theory*, 67(12):7807–7814, 2021.
- [BDGP23] Anurag Bishnoi, Jozefien D’haeseleer, Dion Gijswijt, and Aditya Potukuchi. Blocking sets, minimal codes and trifferent codes. *arXiv preprint 2301.09457*, 2023.
- [BE97] Jürgen Bierbrauer and Yves Edel. A family of 2-weight codes related to bch-codes. *Journal of Combinatorial Designs*, 5(5):391–396, 1997.
- [Bon84] Arrigo Bonisoli. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combinatoria*, 18:181–186, 1984.
- [CK86] Robert Calderbank and William M Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18(2):97–122, 1986.
- [CL85] Gérard Cohen and Abraham Lempel. Linear intersecting codes. *Discrete Mathematics*, 56(1):35–43, 1985.
- [CZ94] Gerard D Cohen and Gilles Zémor. Intersecting codes and independent families. *IEEE Transactions on Information Theory*, 40(6):1872–1881, 1994.
- [dCK21] Romar dela Cruz and Sascha Kurz. On the maximum number of minimal codewords. *Discrete Mathematics*, 344(9):112510, 2021.
- [DS98] Stefan Dodunekov and Juriaan Simonis. Codes and projective multisets. *The Electronic Journal of Combinatorics*, 5:1–23, 1998.
- [HN21] Tamás Héger and Zoltán Lóránt Nagy. Short minimal codes and covering codes via strong blocking sets in projective spaces. *IEEE Transactions on Information Theory*, 68(2):881–890, 2021.
- [KK20] Michael Kiermaier and Sascha Kurz. On the lengths of divisible codes. *IEEE Transactions on Information Theory*, 66(7):4051–4060, 2020.
- [KK23a] Michael Kiermaier and Sascha Kurz. Classification of  $\delta$ -divisible linear codes spanned by codewords of weight  $\delta$ . *IEEE Transactions on Information Theory*, 69(6):3544–3551, 2023.
- [KK23b] Theresa Körner and Sascha Kurz. Lengths of divisible codes with restricted column multiplicities. *arXiv preprint 2303.17172*, 2023.

- [Kur21] Sascha Kurz. Divisible codes. *arXiv preprint 2112.11763*, page 101 pp., 2021.
- [Kur23] Sascha Kurz. Trifferent codes with small lengths. *arXiv preprint ???*, 2023.
- [MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*, volume 16. Elsevier, 1977.
- [MS19] Sihem Mesnager and Ahmet Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transactions on Information Theory*, 66(4):2296–2310, 2019.
- [Sco23] Martin Scotti. On the lower bound for the length of minimal codes. *arXiv preprint 2302.05350*, 2023.
- [SF20] Zexia Shi and Fang-Wei Fu. Several families of  $q$ -ary minimal linear codes with  $w_{\min}/w_{\max} \leq (q-1)/q$ . *Discrete Mathematics*, 343(6):111840, 2020.
- [SL21] Minjia Shi and Xiaoxiao Li. Two classes of optimal  $p$ -ary few-weight codes from down-sets. *Discrete Applied Mathematics*, 290:60–67, 2021.
- [Slo93] N.J.A. Sloane. Covering arrays and intersecting codes. *Journal of Combinatorial Designs*, 1(1):51–63, 1993.
- [Sma23] Valentino Smaldore. All minimal  $[9, 4]_2$ -codes are hyperbolic quadrics. *Examples and Counterexamples*, 3:100097, 2023.
- [TQLZ21] Chunming Tang, Yan Qiu, Qunying Liao, and Zhengchun Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Transactions on Information Theory*, 67(6):3690–3700, 2021.
- [War81] Harold N Ward. Divisible codes. *Archiv der Mathematik*, 36(1):485–494, 1981.