

THE LENGTHS OF PROJECTIVE TRIPLY-EVEN BINARY CODES

THOMAS HONOLD, MICHAEL KIERMAIER, SASCHA KURZ, AND ALFRED WASSERMANN

ABSTRACT. It is shown that there does not exist a projective triply-even binary code of length 59. This settles the last open length for projective triply-even binary codes, which therefore exist precisely for the lengths 15, 16, 30, 31, 32, 45–51, and ≥ 60 .

Dedicated to Ivan Landjev on the occasion of his 59. birthday.

Keywords: divisible codes, projective codes, partial spreads

MSC: Primary 94B05; Secondary 51E23.

1. INTRODUCTION

Doubly-even binary codes have been the subject of extensive research for decades. For recent applications and enumeration results we refer, e.g., to [1]. A substantial study has also been done for triply-even binary codes; see [2]. These two classes are special cases of so-called Δ -divisible codes, i.e., q -ary linear codes C with all (Hamming) weights divisible by an integer $\Delta > 1$; see, e.g., [3].

Assuming that C has length n , dimension k and no all-zero coordinate, the columns of a $k \times n$ generator matrix of C span n (not necessarily distinct) one-dimensional subspaces of \mathbb{F}_q^k that can be viewed as *points* in the associated projective geometry, see e.g. [4] or [5, Chapter 17]. The codewords correspond to the hyperplanes of the geometry, and the weight of a codeword is the number of points outside of the corresponding hyperplane. This geometric setting provides a basis-free approach to linear codes (for details see the end of Section 2). The Δ -divisibility of the linear code C translates into the following property of the associated multiset \mathcal{P} of points in \mathbb{F}_q^k . For each hyperplane H of \mathbb{F}_q^k we have $\#(\mathcal{P} \cap H) \equiv \#\mathcal{P} \pmod{\Delta}$. In this case, we will say that the multiset \mathcal{P} is Δ -divisible, too.

For a general linear code C , the number of non-zero columns of a generator matrix of C is called the *effective length* of C . If the effective length equals the length, C is said to be of *full length*. The code C is called *projective* if it is full-length and any pair of columns of a generator matrix is linearly independent, i.e., if the associated multiset \mathcal{P} of points is actually a set.

Recently, Δ -divisible codes have been applied for obtaining upper bounds on the size of partial t -spreads in \mathbb{F}_q^k , i.e., sets of t -dimensional subspaces in \mathbb{F}_q^k with pairwise trivial intersection, see e.g. [6, 7]. Due to the intersection property, every point of \mathbb{F}_q^k is covered by at most one element of a given partial t -spread. Calling every non-covered point a *hole*, the set of holes of a partial t -spread is q^{t-1} -divisible; see, e.g., [6, Theorem 8], where also a generalization to so-called vector space partitions is considered.¹ So, from the non-existence of q^{t-1} -divisible sets of suitable size n (or equivalently, projective q^{t-1} -divisible codes of effective length n), one can conclude the non-existence of partial t -spreads in \mathbb{F}_q^k of a certain cardinality. Indeed, all currently known upper bounds on the size of a partial t -spread can be obtained from such non-existence results for divisible codes; see, e.g., [6, 7].

Thus from an application point of view q^r -divisible codes over \mathbb{F}_q , where r is a positive integer (or, more generally, a positive rational number such that q^r is an integer²) are of considerable interest. If G_1 is a generator matrix of a Δ -divisible $[n_1, k_1]_q$ code and G_2 is a generator matrix of another Δ -divisible

¹In a special case, the divisibility of the set of holes was already used in [8] to determine an upper bound for the maximum cardinality of a partial t -spread.

²cf. the beginning of Section 2

$[n_2, k_2]_q$ code, then $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ is the generator matrix of a Δ -divisible $[n_1 + n_2, k_1 + k_2]_q$ code. Since the set of all points of a k -dimensional subspace of \mathbb{F}_q^v is a q^{k-1} -divisible point set in \mathbb{F}_q^v (where $v \geq k$ can be any integer) and $\gcd((q^k - 1)/(q - 1), (q^{k+1} - 1)/(q - 1)) = 1$, for each prime power q and each $r \in \mathbb{Q}_{>0}$ such that $q^r \in \mathbb{N}$, the set $\mathcal{F}_q(r)$ of positive integers that do not occur as the cardinality of a q^r -divisible (multi-)set or effective length of a (projective) q^r -divisible code is actually a finite set (using a Frobenius Coin problem type argument for the proof). For multisets of points, i.e., not necessarily projective linear codes, the question is completely resolved: In [9, Theorem 4] for all integers r and all prime powers q the set $\mathcal{F}_q(r)$ has been determined. For sets of points or projective q^r -divisible codes the question is more complicated. A partial answer is given in [6, Theorem 13]:

Fact 1.

- (i) 2^1 -divisible sets over \mathbb{F}_2 of cardinality n exist for all $n \geq 3$ and do not exist for $n \in \{1, 2\}$.
- (ii) 2^2 -divisible sets over \mathbb{F}_2 of cardinality n exist for $n \in \{7, 8\}$ and all $n \geq 14$, and do not exist in all other cases.
- (iii) 2^3 -divisible sets over \mathbb{F}_2 of cardinality n exist for

$$n \in \{15, 16, 30, 31, 32, 45, 46, 47, 48, 49, 50, 51\},$$

for all $n \geq 60$, and possibly for $n = 59$; in all other cases they do not exist.

In Part (iii) the existence question for a binary projective 2^3 -divisible code of length 59 remains undecided. The aim of this paper is to complete the characterization with the following theorem:

Theorem 2. *There is no projective triply-even binary linear code of length 59.*

Let us remark that the distinction between the existence of a projective/non-projective q^r -divisible code of a certain length matters indeed, e.g., for the determination of upper bounds on the maximum possible cardinality of partial t -spreads. As an example, in [6, Theorem 13] (cf. also [7]) it is shown that no projective 2^3 -divisible code of length 52 exists, while there are non-projective examples with these parameters. From this non-existence result for projective q^r -divisible codes we can conclude that there can be at most 132 solids in \mathbb{F}_2^{11} with pairwise trivial intersection, which is the sharpest currently known upper bound. With a corresponding lower bound of 129, this is the smallest open case for the maximum cardinality of partial t -spreads over \mathbb{F}_2 .

The remaining part of the paper is structured as follows. In Section 2 we state the necessary preliminaries from coding theory, before proving the non-existence of a binary projective 2^3 -divisible code of length $n = 59$ in Section 3. In Section 4 we derive a corollary which excludes the existence of vector space partitions of certain types. We close the paper with a discussion of some open problems in Section 5.

2. PRELIMINARIES

A linear code C over \mathbb{F}_q is called q^r -divisible for some $r \in \mathbb{Q}_{>0}$ such that $q^r \in \mathbb{N}^3$, if the weight of each codeword is divisible by q^r . Given our assumption that C is projective, the length equals the effective length, i.e., there are no zero-columns in the generator matrix of C , and C corresponds to a set of n points spanning \mathbb{F}_q^k . We denote the number of codewords of weight i in C by a_i and the number of codewords of weight i in the dual code C^\perp by a_i^\perp . The well-known MacWilliams identities, see e.g. [11], relate the numbers a_i and a_i^\perp as follows. For all $i \in \{0, \dots, n\}$ we have

$$\sum_{j=0}^n K_i(j) a_j = (\#C) a_i^\perp \quad \text{for } i \in \{0, \dots, n\},$$

³More precisely, this conditions says that q^r should be an integral power of the field characteristic p . In [10, Theorem 1] it has been shown that Δ -divisible codes with Δ relatively prime to p correspond to repetitions of smaller codes. Thus, it suffices to consider the so-called modular case $\Delta = p^l$ for integers $l > 0$.

where

$$K_i(j) = K_i^{n,q}(j) = \sum_{s=0}^n (-1)^s (q-1)^{i-s} \binom{n-j}{i-s} \binom{j}{s}$$

is the i -th Krawtchouk polynomial of order n . Obviously, we have $\sum_{i=0}^n a_i = \#C$, which is in fact the first ($i=0$) MacWilliams equation. The polynomial $w(C) = \sum_{i=0}^n a_i x^i$ is called the weight enumerator of C .

For a given $[n, k]_q$ code C and a codeword $\mathbf{c} \in C$ of weight w the *residual code* $C_{\mathbf{c}}$ arises from C by restricting all codewords to those coordinates where \mathbf{c} has a zero entry. Thus, $C_{\mathbf{c}}$ is an $[n-w, \leq k-1]_q$ code. If C is projective, then obviously also $C_{\mathbf{c}}$ is projective. Moreover, if C is q^r -divisible, then $C_{\mathbf{c}}$ is q^{r-1} -divisible; see, e.g., [6, Lemma 7].

It is well-known (see, e.g., [4]) that the relation $C \rightarrow C$, associating with a full-length linear $[n, k]$ code C over \mathbb{F}_q the n -multiset \mathcal{C} of points in the projective geometry $\text{PG}(\mathbb{F}_q^k)$ defined by the columns of any generator matrix, induces a one-to-one correspondence between classes of (semi-)linearly equivalent full-length linear codes and classes of (semi-)linearly equivalent spanning multisets of points. The importance of the correspondence lies in the fact that it relates coding-theoretic properties of C to geometric or combinatorial properties of \mathcal{C} via

$$w(\mathbf{a}G) = n - \#\{1 \leq j \leq n; \mathbf{a} \cdot \mathbf{g}_j = 0\} = n - \#(\mathcal{C} \cap \mathbf{a}^\perp), \quad (1)$$

where w denotes the Hamming weight, $G = (\mathbf{g}_1 | \dots | \mathbf{g}_n) \in \mathbb{F}_q^{k \times n}$ a generating matrix of C , $\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \dots + a_k b_k$, and \mathbf{a}^\perp is the hyperplane in $\text{PG}(\mathbb{F}_q^k)$ with equation $a_1 x_1 + \dots + a_k x_k = 0$.⁴ In the usual coding theory setting, the Hamming weight depends on the chosen basis, as the standard basis vectors are exactly the vectors of Hamming weight 1. In contrast to that, the geometric setting provides a basis-free approach to linear codes.

3. PROOF OF THE MAIN THEOREM

In this section, we prove Theorem 2. For this purpose, let C be a projective 8-divisible binary code of length 59 and minimum possible dimension k . We are going to restrict the weight frequencies a_i in a series of lemmas, until we finally get a contradiction.

Lemma 3. $a_{48} = a_{56} = 0$.

Proof. The residual code of C with respect to a codeword of weight w is a projective 4-divisible code of length $59-w$. By Fact 1(ii), there is no such code of lengths 3 or 11. So the weights $w = 48$ and $w = 56$ are not possible. \square

Hence the only possible weights are 0, 8, 16, 24, 32 and 40. The first four MacWilliams identities give

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 59 & 43 & 27 & 11 & -5 & -21 \\ 1711 & 895 & 335 & 31 & -17 & 191 \\ 32509 & 11997 & 2493 & -99 & 125 & -931 \end{pmatrix} \begin{pmatrix} a_0 \\ a_8 \\ a_{16} \\ a_{24} \\ a_{32} \\ a_{40} \end{pmatrix} = \#C \cdot \begin{pmatrix} a_0^\perp \\ a_1^\perp \\ a_2^\perp \\ a_3^\perp \end{pmatrix}.$$

⁴In the non-projective case, $\mathcal{C} \cap \mathbf{a}^\perp$ must be interpreted as the multiset containing the points of \mathbf{a}^\perp with their \mathcal{C} -multiplicities.

Of course, $a_0 = a_0^\perp = 1$. Since C is projective, we have $a_1^\perp = a_2^\perp = 0$.

Multiplying the matrix of coefficients with the inverse of the rightmost 4×4 submatrix yields

$$\begin{aligned} a_{16} &= -10 - 4a_8 - \frac{45}{2^{12}}\#C + \frac{1}{2^{12}}a_3^\perp\#C, \\ a_{24} &= 20 + 6a_8 + \frac{1447}{2^{12}}\#C - \frac{3}{2^{12}}a_3^\perp\#C, \\ a_{32} &= -15 - 4a_8 + \frac{2617}{2^{12}}\#C + \frac{3}{2^{12}}a_3^\perp\#C, \\ a_{40} &= 4 + a_8 + \frac{77}{2^{12}}\#C - \frac{1}{2^{12}}a_3^\perp\#C. \end{aligned}$$

Lemma 4. $k \geq 10$.

Proof. $0 \leq a_{16} + a_{40} = -6 - 3a_8 + \frac{1}{128}\#C \leq -6 + \frac{1}{128}\#C$. Thus $2^k = \#C \geq 6 \cdot 128 = 768$. Therefore $k \geq 10$. \square

Lemma 5. $k = 10$.

Proof. Let $V = \mathbb{F}_2^k$ and \mathcal{C} the set of 59 points in $\text{PG}(V)$ corresponding to the linear code C .

Let Q be a point in $\text{PG}(V)$ not contained in \mathcal{C} . We consider the projection of \mathcal{C} modulo Q , that is the multiset image of \mathcal{C} under the map $V \rightarrow V/Q, \mathbf{v} \mapsto (\mathbf{v} + Q)/Q$. The resulting multiset \mathcal{C}' consists of 59 points in $\text{PG}(V/Q) \cong \text{PG}(\mathbb{F}_2^{k-1})$ and arises by identifying points of \mathcal{C} on the same line through Q . The corresponding linear code C' is a subcode of C of effective length 59 and dimension $k - 1$. Therefore, C' is 2^3 -divisible, and the assumed minimality of k implies that C' is not projective. Equivalently, there is a secant through Q , that is a line whose remaining two points are contained in \mathcal{C} .

So each of the $2^k - 60$ points of $\text{PG}(V)$ not contained in \mathcal{C} lies on a secant. Since \mathcal{C} admits at most $\binom{\#C}{2} = \binom{59}{2} = 1711$ secants, covering at most 1711 different points not in \mathcal{C} , we get $2^k - 60 \leq 1711$ and therefore $k \leq 10$. Hence $k = 10$ by Lemma 4. \square

Lemma 6. $a_8 = 0$ and $a_{16} + a_{40} = 2$.

Proof. Plugging $\#C = 2^{10}$ from Lemma 5 into $a_{16} + a_{40} = -6 - 3a_8 + \frac{1}{128}\#C$ (proof of Lemma 4) yields $a_{16} + a_{40} = 2 - 3a_8$. As this expression cannot be negative, $a_8 = 0$ and $a_{16} + a_{40} = 2$. \square

Lemma 7. $a_{16} = 0$.

Proof. Assume that $a_{16} \neq 0$. Then by Lemma 6, either $(a_{16}, a_{40}) = (1, 1)$ or $(a_{16}, a_{40}) = (2, 0)$. Let \mathbf{c} be a codeword of weight 16 and $\pi : C \rightarrow \mathbb{F}_2^{16}$ the restriction of C to $\text{supp}(\mathbf{c})$, i.e., to the 16 non-zero positions of \mathbf{c} . Then $C' = \pi(C)$ is a binary linear code of effective length 16. By the 2^3 -divisibility of C and the fact that C' contains the all-1-word, we see that C' is 2^2 -divisible. Therefore, C' is self-orthogonal of length 16, implying that $\dim(C') \leq \frac{16}{2} = 8$.

Assume that there exists a codeword $\mathbf{x} \in \ker(\pi) \setminus \{\mathbf{0}\}$. Then the supports of \mathbf{x} and \mathbf{c} are disjoint, so $w(\mathbf{x} + \mathbf{c}) = w(\mathbf{x}) + 16$. In the case $(a_{16}, a_{40}) = (2, 0)$ we have $w(\mathbf{x} + \mathbf{c}) \leq 32$, so $w(\mathbf{x}) \leq 16$ and hence \mathbf{x} is uniquely determined as the other word of weight 16. In the case $(a_{16}, a_{40}) = (1, 1)$, $w(\mathbf{x}) \geq 24$ (since the only word of weight 16 is \mathbf{c}). Hence $w(\mathbf{x}) = 24$ and $w(\mathbf{x} + \mathbf{c}) = 40$. So $\mathbf{x} + \mathbf{c}$ is the unique codeword of weight 40, and \mathbf{x} is uniquely determined as $(\mathbf{x} + \mathbf{c}) + \mathbf{c}$.

Therefore in both cases $\dim \ker(\pi) \leq 1$. The application of the rank-nullity theorem to π then gives $\dim C = \dim \ker(\pi) + \dim \text{im}(\pi) \leq 1 + 8 = 9$, a contradiction. \square

Lemma 8. *The code C does not exist.*

Proof. By Lemma 6 and 7, $a_{40} = 2$.⁵ Let \mathbf{c} be a codeword of weight 40. We consider the restriction $\pi : C \rightarrow \mathbb{F}_2^{19}$ to the 0-coordinates of \mathbf{c} . The image $D = \pi(C)$ is the residual code $C_{\mathbf{c}}$, which is a binary

⁵In fact, at this point the weight enumerator of C is uniquely determined: $a_8 = a_{16} = 0$ yields $a_3^\perp = 85$ and $w(C) = 1 + 318x^{24} + 703x^{32} + 2x^{40}$; cf. the proof of Lemma 4.

projective 2^2 -divisible code of length 19. The kernel $D' = \ker \pi$ consists of all codewords of C whose support is contained in $\text{supp}(\mathbf{c})$.

The first 5 MacWilliams equations for the residual code D are

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 19 & 11 & 3 & -5 & -13 \\ 171 & 51 & -5 & 3 & 75 \\ 969 & 121 & -23 & 25 & -247 \\ 3876 & 116 & 4 & -44 & 484 \end{pmatrix} \begin{pmatrix} b_0 \\ b_4 \\ b_8 \\ b_{12} \\ b_{16} \end{pmatrix} = \#D \cdot \begin{pmatrix} b_0^\perp \\ b_4^\perp \\ b_8^\perp \\ b_{12}^\perp \\ b_{16}^\perp \end{pmatrix}.$$

Using $b_0 = b_0^\perp = 1$ and $b_1^\perp = b_2^\perp = 0$, the first 4 equations lead to

$$\begin{pmatrix} b_4 \\ b_8 \\ b_{12} \\ b_{16} \end{pmatrix} = \frac{\#D}{2^9} \begin{pmatrix} 15 + b_3^\perp \\ 291 - 3b_3^\perp \\ 205 + 3b_3^\perp \\ 1 - b_3^\perp \end{pmatrix} + \begin{pmatrix} -4 \\ 6 \\ -4 \\ 1 \end{pmatrix}.$$

Plugging these expressions into the fifth MacWilliams identity leads to

$$b_4^\perp = -11 - b_3^\perp + \frac{2^{12}}{\#D}.$$

Hence $0 \leq b_4^\perp \leq -11 + \frac{2^{12}}{\#D}$, i.e., $\#D \leq \frac{2^{12}}{11} < 2^9$. Therefore, $\dim(D) \leq 8$.

The code D' contains \mathbf{c} . For $\mathbf{x} \in D'$, $w(\mathbf{c} + \mathbf{x}) = 40 - w(\mathbf{x})$. So D' cannot contain codewords of weights 8 or 16 (as $a_8 = a_{16} = 0$), nor of weight 24 or 32 (as $\mathbf{c} + \mathbf{x}$ would then have weight 16, resp., 8). Therefore, $D' = \{\mathbf{0}, \mathbf{c}\}$ and $\dim(D') = 1$. Application of the rank-nullity theorem to π then yields $\dim(C) = \dim(D') + \dim(D) \leq 1 + 8 = 9$, the final contradiction. \square

4. APPLICATION TO VECTOR SPACE PARTITIONS

Let V be a finite vector space over \mathbb{F}_q . A set P of non-zero subspaces of V is called a *vector space partition* of V if every non-zero vector of V is contained in exactly one element of P . In other words, the elements of P form a partition of the point set of $\text{PG}(V)$. Denoting the number of elements of dimension i in P by d_i , the *type* of P is given by the sequence (d_1, d_2, d_3, \dots) , or “multiplicatively” as $(1^{d_1} 2^{d_2} 3^{d_3} \dots)$ with factors having $d_i = 0$ omitted.

Corollary 9. *Let V be a finite vector space over \mathbb{F}_2 . There is no vector space partition of V of type (d_i) with $d_1 = 59$ and $d_2 = d_3 = 0$.*

Proof. Assume that P is a vector space partition of the given type. By [6, Theorem 8], the 59 subspaces of dimension 1 form an 8-divisible set of points in $\text{PG}(V)$. This set corresponds to a projective 8-divisible binary code of length 59, which does not exist by Theorem 2. \square

Example 10. The smallest nontrivial cases excluded by Corollary 9 are vector space partitions of \mathbb{F}_2^{10} of type $(1^{59} 4^{56} 5^4)$ and of type $(1^{59} 4^{25} 5^{19})$.

5. CONCLUSION AND OPEN PROBLEMS

Using purely theoretical methods we were able to exclude the existence of a projective 2^3 -divisible binary code of length 59. This completes the characterization of the possible lengths of projective 2^3 -divisible binary codes, which play some role in applications.

It would be desirable to have generalizations of the completed characterization in Fact 1 to other parameters. To this end, we state the list of lengths of projective 2^4 -divisible binary codes for which the

existence question is undecided, at least according to our knowledge:

$$\{130, 163, 164, 165, 185, 215, 216, 232, 233, \\ 244, 245, 246, 247, 274, 275, 277, 278, 306, 309\}.$$

For $q = 3$ the smallest open case is that of a projective 3^2 -divisible ternary code of length 70. The complete list of undecided lengths is

$$\{70, 77, 99, 100, 101, 102, 113, 114, 115, 128\}.$$

REFERENCES

- [1] C. F. Doran, M. G. Faux, S. J. Gates, T. Hübsch, K. M. Iga, G. D. Landweber, and R. L. Miller, “Codes and supersymmetry in one dimension,” *Advances in Theoretical and Mathematical Physics*, vol. 15, no. 6, pp. 1909–1970, 2011.
- [2] K. Betsumiya and A. Munemasa, “On triply even binary codes,” *Journal of the London Mathematical Society*, vol. 86, no. 1, pp. 1–16, 2012.
- [3] H. N. Ward, “An introduction to divisible codes,” *Designs, Codes and Cryptography*, vol. 17, no. 1, pp. 73–79, 1999.
- [4] S. Dodunekov and J. Simonis, “Codes and projective multisets,” *The Electronic Journal of Combinatorics*, vol. 5, no. 1, p. 37, 1998.
- [5] J. Bierbrauer, *Introduction to coding theory*. Chapman and Hall/CRC, 2004.
- [6] T. Honold, M. Kiermaier, and S. Kurz, “Partial spreads and vector space partitions,” in *Network Coding and Subspace Designs*, M. Greferath, M. O. Pavčević, N. Silberstein, and M. Á. Vázquez-Castro, Eds. Springer, 2018, pp. 131–170.
- [7] S. Kurz, “Packing vector spaces into vector spaces,” *The Australasian Journal of Combinatorics*, vol. 68, no. 1, pp. 122–130, 2017.
- [8] A. Beutelspacher, “Partial spreads in finite projective spaces and partial designs,” *Mathematische Zeitschrift*, vol. 145, no. 3, pp. 211–229, 1975.
- [9] M. Kiermaier and S. Kurz, “An improvement of the Johnson bound for subspace codes,” *arXiv preprint 1707.00650*, 2017.
- [10] H. N. Ward, “Divisible codes,” *Archiv der Mathematik*, vol. 36, no. 1, pp. 485–494, 1981.
- [11] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977.

THOMAS HONOLD, ZJU-UIUC INSTITUTE, ZHEJIANG UNIVERSITY, 314400 HAINING, CHINA.
Email address: honold@zju.edu.cn

MICHAEL KIERMAIER, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY
Email address: michael.kiermaier@uni-bayreuth.de

SASCHA KURZ, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY
Email address: sascha.kurz@uni-bayreuth.de

ALFRED WASSERMANN, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY
Email address: alfred.wassermann@uni-bayreuth.de