PROJECTIVE DIVISIBLE BINARY CODES

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

ABSTRACT. For which positive integers n, k, r does there exist a linear $[n, k]$ code C over $\mathbb{F}_q$ with all codeword weights divisible by q^r and such that the columns of a generating matrix of C are projectively distinct? The motivation for studying this problem comes from the theory of partial spreads, or subspace codes with the highest possible minimum distance, since the set of holes of a partial spread of r-flats in $\mathrm{PG}(v-1, \mathbb{F}_q)$ corresponds to a q^r-divisible code with $k \le v$. In this paper we provide an introduction to this problem and report on new results for $q = 2$.

1. Introduction

Let $q = p^e > 1$ be a prime power and $\Delta > 1$ an integer. A linear code C over $\mathbb{F}_q$ is said to be Δ-*divisible* if the Hamming weight $\mathrm{w}(\mathbf{c})$ of every codeword $\mathbf{c} \in C$ is divisible by Δ. The classical examples are self-dual codes over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$, which have $\Delta \in \{2, 4\}$, $\Delta = 3$ and $\Delta = 2$, respectively. While self-dual codes or, slightly more general, $[n, n/2]$ codes cannot have other divisors by the Gleason-Pierce-Ward Theorem [13, Ch. 9.1], there exist interesting examples in (necessarily) smaller dimension for every pair q, Δ in which $\Delta = p^f$ is a power of the characteristic of $\mathbb{F}_q$. The most well-known example is the family of q-ary $\left[\frac{q^k-1}{q-1}, k, q^{k-1}\right]$ simplex codes (dual Hamming codes), which have constant weight $\Delta = q^{k-1} = p^{e(k-1)}$. In the remaining case $\Delta = mp^f$ with $m > 1$ and $\gcd(m, p) = 1$, a Δ-*divisible* code is necessarily an m-fold replicated code [20, Th. 1], reducing this case to the former.

Our motivation for studying divisible codes comes from Finite Geometry and the recently established field of Subspace Coding. A *partial* r-*spread* in the projective geometry $\mathrm{PG}(v-1, \mathbb{F}_q) = \mathrm{PG}(\mathbb{F}_q^v/\mathbb{F}_q)$ is a set of pairwise disjoint r-subspaces of $\mathbb{F}_q^v/\mathbb{F}_q$.[1] To avoid trivialities, we assume $r \ge 2$.

In the case $r \mid v$ the existence of r-*spreads*, i.e., partial r-spreads partitioning the point set of $\mathrm{PG}(v-1, \mathbb{F}_q)$ is well-known, but in the case $r \nmid v$ (in which spreads cannot exist) the maximum size of a partial r-spread in $\mathrm{PG}(v-1, \mathbb{F}_q)$ is generally unknown. The problem of determining this maximum size forms a special case of the so-called *Main Problem of Subspace Coding*, which arose from the elegant Koetter-Kschischang-Silva model for Random Linear Network Coding [14, 16, 17] and is akin to the Main Problem of classical Coding Theory. It asks for the maximum number of subspaces of $\mathbb{F}_q^v/\mathbb{F}_q$ at mutual distance $\ge d$ in the subspace metric defined by $\mathrm{d_S}(X, Y) = \dim(X + Y) - \dim(X \cap Y)$. If attention is restricted to subspaces of constant dimension r and $d = 2r$ is the maximum possible distance under this restriction, we recover the original geometric problem.

1991 *Mathematics Subject Classification.* Primary 94B05; Secondary 51E23.
Key words and phrases. divisible codes, projective codes, partial spreads.

[1] Here r refers to the vector space dimension of the subspace (the geometric dimension as a flat of $\mathrm{PG}(v-1, \mathbb{F}_q)$ being $r-1$), but "disjoint" means disjoint as point sets in $\mathrm{PG}(v-1, \mathbb{F}_q)$ (the corresponding vector space intersection being $\{\mathbf{0}\}$).

We will not discuss the known results about maximal partial spreads in this paper, for which we refer interested readers to the recent exhaustive survey [11]. Instead we will describe the link between partial spreads and divisible codes (Section 2), formulate a "Main Problem" for projective divisible codes (Section 3), discuss some general divisible code constructions (Section 4), and report on new results for the particular case $q = 2$, $\Delta = 2^r$ (Section 5).

2. Linking Partial Spreads and Divisible Codes

The link between partial spreads and divisible codes is provided by the concept of a "hole" of a family $\mathcal{S}$ of subspaces of $\mathrm{PG}(v-1, \mathbb{F}_q)$. A point of $\mathrm{PG}(v-1, \mathbb{F}_q)$ (i.e., a 1-dimensional subspace of $\mathbb{F}_q^v/\mathbb{F}_q$) is said to be a *hole* of $\mathcal{S}$ if it is not covered by (i.e., not incident with) a member of $\mathcal{S}$. Further, we recall from [9, 19] that associating with a linear $[n, k]$-code C the multiset $\mathfrak{K}_C$ of points generated by the columns of any generating matrix $\mathbf{G}$ of C yields a one-to-one correspondence between monomial equivalence classes of linear $[n, k]$-codes over $\mathbb{F}_q$ without universal zero coordinate and isomorphism classes of n-element spanning multisets of points in $\mathrm{PG}(k-1, \mathbb{F}_q)$. The relation $C \mapsto \mathfrak{K}_C$ preserves the metric in the sense that the weight $\mathrm{w}(\mathbf{c})$ of a nonzero codeword $\mathbf{c} = \mathbf{aG}$ and the multiplicity $\mathfrak{K}_C(H) = \sum_{P \in H} \mathfrak{K}_C(P)$ of the corresponding hyperplane $H = \mathbf{a}^\perp = \{\mathbf{x} \in \mathbb{F}_q^k; a_1x_1 + \cdots + a_kx_k = 0\}$ are related by $\mathrm{w}(\mathbf{aG}) = n - \mathfrak{K}_C(\mathbf{a}^\perp) = \mathfrak{K}_C(\mathcal{P} \setminus \mathbf{a}^\perp)$, where $\mathcal{P}$ denotes the point set of $\mathrm{PG}(k-1, \mathbb{F}_q)$. The code C is Δ-divisible iff the multiset $\mathfrak{K}_C$ is Δ-*divisible* in the sense that the multiplicity $\mathfrak{K}_C(A)$ of any $(k-1)$-dimensional affine subspace A of $\mathrm{PG}(k-1, \mathbb{F}_q)$ is divisible by Δ.

The code C is said to be *projective* if $\mathfrak{K}_C$ is a set or, equivalently, the n columns of $\mathbf{G}$ are projectively distinct. In terms of the minimum distance of the dual code this can also be expressed as $\mathrm{d}(C^\perp) \geq 3$.

Proposition 1 (compare [11, Th. 8])**.** *Let $\mathcal{S}$ be a partial r-spread in $\mathrm{PG}(v-1, \mathbb{F}_q)$, $\mathfrak{H}$ its set of holes, and $C_\mathfrak{H}$ any linear $[n, k]$ code over $\mathbb{F}_q$ associated with $\mathfrak{H}$ as defined above. Then*

(i) $C_\mathfrak{H}$ is projective and q^{r-1}-divisible;
(ii) the parameters of $C_\mathfrak{H}$ satisfy $n = \frac{q^v-1}{q-1} - \#\mathcal{S} \cdot \frac{q^r-1}{q-1}$ and $k \leq v$.

Proof. All assertions except the q^{r-1}-divisibility of $C_\mathfrak{H}$ are straightforward. For the proof of the latter let $\mathcal{S} = \{S_1, \ldots, S_M\}$, $M = \#\mathcal{S}$, and consider a generating matrix

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{G}_2 & \ldots & \mathbf{G}_M & \mathbf{H} \end{pmatrix}$$

of the q-ary $\left[\frac{q^v-1}{q-1}, v, q^{v-1}\right]$ simplex code, partitioned in such a way that the columns of $\mathbf{G}_j$ account for all points in S_j and those of $\mathbf{H}$ for all points in $\mathfrak{H}$. For a nonzero codeword $\mathbf{c} = \mathbf{xG}$ of the simplex code we have

$$q^{v-1} = \mathrm{w}(\mathbf{xG}) = \sum_{j=1}^{M} \mathrm{w}(\mathbf{xG}_j) + \mathrm{w}(\mathbf{xH}).$$

Since each matrix $\mathbf{G}_j$ generates an r-dimensional simplex code (in the broader sense, i.e., the rows of $\mathbf{G}_j$ need not be linearly independent), we have $\mathrm{w}(\mathbf{xG}_j) \in \{0, q^{r-1}\}$. Since $v - 1 \geq r - 1$, it follows that $\mathrm{w}(\mathbf{xH})$ is divisible by q^{r-1} as well. But $\mathbf{H}$ generates $C_\mathfrak{H}$ and the result follows. $\square$

Proposition 1 looks rather innocent at the first glance, but in fact it provides a powerful tool for bounding the size of partial spreads. This is already illustrated by the following

Corollary 1. *If $v \geq 2r+1$ and $v \bmod r = 1$, the maximum size of a partial r-spread in $\mathrm{PG}(v-1,\mathbb{F}_q)$ is*

$$\left\lfloor \frac{q^v-1}{q^r-1} \right\rfloor - (q-1) = q^{v-r} + q^{v-2r} + \cdots + q^{r+1} + 1,$$

with corresponding number of holes equal to q^r.

Proof. It is readily shown by induction that there exists a partial r-spread with the required property, the induction step being provided by generating matrices in $\mathbb{F}_q^{v\times r}$ of the form $\binom{\mathbf{I}_r}{\mathbf{A}}$, where $\mathbf{A} \in \mathbb{F}_q^{(v-r)\times r}$ runs through a matrix representation of $\mathbb{F}_{q^{v-r}}$ with the last $v-2r$ columns stripped off. The subspaces of the partial spread are the column spaces of the matrices $\binom{\mathbf{I}_r}{\mathbf{A}}$, and the anchor of the induction is provided by adding the column space of $\binom{\mathbf{0}}{\mathbf{I}_r} \in \mathbb{F}_q^{(2r+1)\times r}$ to the q^{r+1} subspaces obtained for $v = 2r+1$ in the same way as in the inductive step.

Conversely, let $\mathcal{S}$ by a partial r-spread in $\mathrm{PG}(v-1,\mathbb{F}_q)$ and $\mathfrak{H}$ its set of holes. By Proposition 1, the $[n,k]$ code $C_{\mathfrak{H}}$ is q^{r-1}-divisible satisfying $n = \#\mathfrak{H} = 1 + h\cdot\frac{q^r-1}{q-1}$ for some integer h. We must show $h \geq q-1$.

Assuming $h < q-1$, we have $n = 1 + h(1+q+\cdots+q^{r-1}) = n_1 + hq^{r-1}$ with $n_1 = 1 + h(1+q+\cdots+q^{r-2}) < q^{r-1}$. This implies that the maximum weight of $C_{\mathfrak{H}}$ cannot exceed hq^{r-1}. But on the other hand, $C_{\mathfrak{H}}$ has average weight $n(1-1/q) = \frac{q-1-h}{q} + hq^{r-1} > hq^{r-1}$ and hence also a codeword of weight $> hq^{r-1}$. Contradiction. □

Corollary 1 settles the determination of the maximum size of partial line spreads ($r = 2$) in $\mathrm{PG}(v-1,\mathbb{F}_q)$ completely. For $q = 2$ also the maximum size of partial plane spreads ($r = 3$) in $\mathrm{PG}(v-1,\mathbb{F}_2)$ is known for all v. The key ingredient to this theorem is a computer construction of a partial plane spread of size 34 in $\mathrm{PG}(7,\mathbb{F}_2)$. The corresponding number of holes is $2^8-1 = 34\cdot 7 = 17$, and a partial plane spread of size 35 is readily excluded with the aid of Proposition 1: The associated projective binary $[10,k]$ code $C_{\mathfrak{H}}$ would be doubly-even by Proposition 1, but such a code does not exist. For more details on this case and for the best currently available general upper bounds we refer to [11].

3. The Main Problem for Projective Divisible Codes

In this section we formulate the general existence problem for projective divisible codes with given parameters. In order to be as general as possible, we note that a divisor $\Delta = p^f$ of a p^e-ary code can be expressed in terms of the alphabet size $q = p^e$ as $\Delta = q^{f/e}$. Hence, by allowing exponents $r \in \frac{1}{e}\mathbb{Z}^+$ we can subsume all interesting code divisors under the notion of "q^r-divisibility".[2]

Let $\mathrm{PD}(q,r)$ be the set of all pairs of positive integers (n,k), for which a projective q^r-divisible linear $[n,k]$ code over $\mathbb{F}_q$ exists and

$$\mathrm{LPD}(q,r) = \left\{n \in \mathbb{Z}^+; \exists k \text{ such that } (n,k) \in \mathrm{PD}(q,r)\right\};$$

i.e., $\mathrm{LPD}(q,r)$ is the set of (realizable) lengths of such codes without restricting the code dimension. The general existence problem for projective divisible codes amounts to the determination of the sets $\mathrm{PD}(q,r)$ for all prime powers $q > 1$ and all $r \in \mathbb{Z}^+$. Since this is a formidable problem even when q and r are fixed to some small numbers, we try to determine the sets $\mathrm{LPD}(q,r)$ first.

It turns out that each set $\mathrm{LPD}(q,r)$ contains all but finitely many integers. Thus there is a well-defined function $\mathrm{F}(q,r)$, assigning to q,r the largest integer n that is not equal to the length of a projective q^r-divisible linear code over $\mathbb{F}_q$. Determining $\mathrm{F}(q,r)$ is in some sense analogous to the well-known *Frobenius Coin*

[2]For example, the divisor $\Delta = 2$ of a quaternary code corresponds to $r = \frac{1}{2}$.

Problem (see, e.g., [4]), which in its simplest form asks for the largest integer not representable as $a_1n_1 + a_2n_2$ with $a_1, a_2 \geq 0$, where n_1 and n_2 are given relatively prime positive integers. The solution is $(n_1 - 1)(n_2 - 1) - 1$, as is easily shown, and this observation together with the juxtaposition construction for divisible codes yields an upper bound for $\mathrm{F}(q, r)$ (and shows that $\mathrm{F}(q, r)$ is well-defined). Details are contained in the next section. The determination of $\mathrm{F}(q, r)$ may be seen as the first important step en route to the solution of the main problem for projective divisible codes.

4. Constructions

Suppose C_i $(i = 1, 2)$ are linear $[n_i, k_i]$ codes over $\mathbb{F}_q$ with generating matrices $\mathbf{G}_i$ (in the broader sense), chosen as follows: $\mathbf{G}_1$ and $\mathbf{G}_2$ have the same number k of rows, and their left kernels intersect only in $\{\mathbf{0}\}$. Then $\mathbf{G} = (\mathbf{G}_1|\mathbf{G}_2)$ generates a linear $[n_1 + n_2, k]$ code C, called a *juxtaposition* of C_1 and C_2. It is clear that C is q^r-divisible if C_1 and C_2 are. If C_1 and C_2 are projective, we can force C to be projective as well by choosing $\mathbf{G}_i$ appropriately, e.g., $\mathbf{G}_1 = \begin{pmatrix} \mathbf{G}'_1 \\ \mathbf{0} \end{pmatrix}$, $\mathbf{G}_2 = \begin{pmatrix} \mathbf{0} \\ \mathbf{G}'_2 \end{pmatrix}$, in which case C is just the direct sum of C_1 and C_2. This implies that the sets $\mathrm{LPD}(q, r)$ are additively closed. Of course juxtaposition can be iterated, and hence we see that in the case $\gcd(n_1, n_2) = 1$ we can obtain projective q^r-divisible codes of all lengths $n = a_1n_1 + a_2n_2$ with $a_1, a_2 \geq 0$. Hence, choosing for C_1 a $\left[\frac{q^{r+1}-1}{q-1}, r+1, q^r\right]$ simplex code and for C_2 a $\left[q^{r+1}, r+2, q^r\right]$ first-order (generalized) Reed-Muller code gives the bound

$$\begin{aligned} \mathrm{F}(q, r) &\leq \frac{q^{r+1}-1}{q-1} \cdot q^{r+1} - \frac{q^{r+1}-1}{q-1} - q^{r+1} \\ &= q^{2r+1} + q^{2r} + \cdots + q^{r+2} - q^r - q^{r-1} - \cdots - 1, \end{aligned} \tag{1}$$

as indicated in the previous section.

The implications of the juxtaposition construction for the sets $\mathrm{PD}(q, r)$ are less clear, but we note the following. If $\mathfrak{K}_i$ denotes a set of points in $\mathrm{PG}(k_i - 1, \mathbb{F}_q)$ associated with C_i, m_i the maximum dimension of a subspace X_i with $\mathfrak{K}_i(X_i) = 0$ ("empty subspace") and $m = \max\{m_1, m_2\}$, then precisely all dimensions $k_1 + k_2 - m \leq k \leq k_1 + k_2$ can be realized by a disjoint embedding of $\mathfrak{K}_1$ and $\mathfrak{K}_2$ into a common ambient space, and hence by a projective juxtaposition of C_1 and C_2. An example for this can be found in [10, Th. 2], where a plane $\mathrm{PG}(2, \mathbb{F}_2)$ and an affine solid $\mathrm{AG}(3, \mathbb{F}_2)$ are combined in 4 possible ways to yield all except 1 isomorphism type of hole sets of partial plane spreads of size 16 in $\mathrm{PG}(6, \mathbb{F}_2)$. Indeed, since the affine solid in its embedding into $\mathrm{PG}(3, \mathbb{F}_2)$ has a free 3-subspace, the possible dimensions are $4 \leq k \leq 7$.

Viewed geometrically, the juxtaposition construction is based on the trivial fact that the sum $\mathfrak{K}_1 + \mathfrak{K}_2$ of two Δ-divisible multisets $\mathfrak{K}_1$, $\mathfrak{K}_2$ is again Δ-divisible. This observation generalizes, of course, to integral linear combinations, shows that $(r{+}1)$-dimensional affine subspaces of $\mathrm{PG}(v - 1, \mathbb{F}_q)$ are, q^r-divisible (since t-subspaces with $t \geq r + 1$ are) and provides the basis for the *sunflower construction* [11]. If q distinct subspaces $S_1, \ldots, S_q$ of dimension at least $r{+}1$ $\mathrm{PG}(v{-}1, \mathbb{F}_q)$ pass through a common r-subspace T but are otherwise disjoint, $S = (S_1 \cup \cdots \cup S_q) \setminus T$ is q^r-divisible. For the proof note that $S = S_1 + \cdots + S_q - qT$ as a multiset, and that qT has the divisor $q \cdot q^{r-1} = q^r$. The construction is especially useful for $q = 2$, in which case it allows "switching" an r subspace $T \subset S_1$ into an $(r + 1)$-dimensional affine subspace $S_2 \setminus T$.[3] This increases the code length only by one and can usually be repeated, see:

Example 1. *According to R. L. Miller's database of binary doubly-even codes at* `http://www.rlmiller.org/de\_codes` *there exist precisely* 192 *non-equivalent binary doubly-even codes of length* 19*, with all dimensions* $3 \leq k \leq 8$ *realizable. However, only* 3 *of these codes, with parameters* $[19, 8, 4]$*,* $[19, 7, 4]$ *and* $[19, 7, 8]$*, are projective. They correspond to the following geometric construction.*

Chose a solid S in $\mathrm{PG}(7, \mathbb{F}_2)$ *and* 4 *planar quadrangles ("affine planes") A_1, A_2, A_3, A_4 meeting the solid in* 4 *disjoint lines L_i. Let L be complement of $L_1 \cup L_2 \cup L_3 \cup L_4$ in S (which is also a line). Viewed as points of the quotient geometry* $\mathrm{PG}(\mathbb{F}_2^8/S)$*, the planes A_i can be arranged in* 3 *distinct ways—(i) a planar quadrangle, (ii) a line plus a plane, and (iii)* 4 *points in general position. This gives* 3 *inequivalent* 19*-sets $A_1 \cup A_2 \cup A_3 \cup A_4 \cup L$ in* $\mathrm{PG}(7, \mathbb{F}_2)$ *and hence* 3 *inequivalent codes with parameters* $[19, 7]$*,* $[19, 7]$ *and* $[19, 8]$*. The point sets/codes are doubly-even, since they arise from S by switching L_i into A_i. The code with minimum distance $d = 8$ corresponds to Case (i). It can also be obtained by shortening the* $[24, 12, 8]$ *Golay code $\mathcal{G}_{24}$ in* 5 *(arbitrary) positions, since $d^\perp(\mathcal{G}_{24}) = d(\mathcal{G}_{24}) = 8$ implies $d^\perp \geq 3$ for the shortened code.*

Another important geometric construction of divisible codes introduced in [11] is the *cone construction*, which increases the divisor from q^r to q^{r+1} (or, in its most general form using an s-dimensional vertex, to q^{r+s}). Let H be a hyperplane of $\mathrm{PG}(v-1, \mathbb{F}_q)$. A cone K with vertex $P \notin H$ and base $B \subseteq H$ is defined as the union of the lines PQ with $Q \in B$. If B is q^r-divisible then the number of points of K outside any hyperplane through P is clearly a multiple of q^{r+1}, and we may adjust the multiplicity of P in K without affecting this property. Since the number of points of $K \setminus \{P\}$ outside every other hyperplane is $(q-1)\#B$, it follows that $K \setminus \{P\}$ is q^{r+1}-divisible if $\#B \equiv 0 \pmod{q^{r+1}}$, and K is q^{r+1}-divisible if $\#B(q-1) \equiv -1 \pmod{q^{r+1}}$.

Example 2. *A projective basis of* $\mathrm{PG}(k-1, \mathbb{F}_2)$ *corresponds to the binary* $[k+1, k, 2]$ *even-weight code and gives via the cone construction a self-dual doubly-even* $[2k+2, k+1, 4]$ *code if* $k \equiv 3 \pmod 4$ *and a doubly-even* $[2k+3, k+1, 4]$ *code if* $k \equiv 2 \pmod 4$*. Generating matrices for $k = 6, 7$ are as follows:*

$$\left(\begin{array}{cccccccccccccc|c}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&1&1&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&1&1&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&1&1&0\\
\hline
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1
\end{array}\right), \quad
\left(\begin{array}{cccccccccccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
\hline
1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0
\end{array}\right).$$

Here $v = k+1$, H is the hyperplane with equation $x_{k+1} = 0$, and $P = (0:0:\cdots:1)$. The reader should recognize the second matrix as one of the basic self-dual code constructions for $q = 2$. The first matrix corresponds to the 5*th isomorphism type of hole sets of partial plane spreads of size* 16 *in* $\mathrm{PG}(6, \mathbb{F}_2)$*; cf.* [10, Th. 2].

Several other constructions are known—for example concatenating a q-divisible code over $\mathbb{F}_{q^r}$ with an r-dimensional simplex code over $\mathbb{F}_q$ obviously yields a q^r-divisible code—and a wealth of further examples: Higher-order (generalized) Reed-Muller codes are divisible by Ax's Theorem [1], semisimple abelian group algebra codes under certain conditions by Delsarte-McEliece [8] (for these two theorems see

[3]For this $S_2 \supset T$ is chosen as an $(r+1)$-subspace, but can otherwise be arbitrary.

also [20]), and projective two-weight codes if the weights satisfy $w_2 > w_1 + 1$ [6].[4] For the latter the survey [5] is a particularly useful source.

5. Results for $q = 2$

First we determine the length-dimension pairs realizable by a binary projective 2-divisible code. The case $r = 1$ is the only case, where we can determine the set $\mathrm{PD}(2, r)$ completely.

Theorem 1. *The set* $\mathrm{PD}(2, 1)$ *consists of all pairs* (n, k) *of positive integers satisfying* $k + 1 \le n \le 2^k - 1$ *and* $n \notin \{2^k - 3, 2^k - 2\}$.

Proof. It is clear that the stated conditions are necessary for the existence of a projective 2-divisible $[n, k]$ code.

For the converse we consider k as fixed and use induction on n in the range $k+1 \le n \le 2^{k-1}$. The $[k+1, k]$ even-weight code, which corresponds to a projective basis of $\mathrm{PG}(k - 1, \mathbb{F}_2)$, provides the base for the induction. Now assume that $\mathfrak{K}$ is a 2-divisible spanning point set in $\mathrm{PG}(k - 1, \mathbb{F}_2)$ with $k + 1 \le n = \#\mathfrak{K} < 2^{k-1}$. If $\mathfrak{K}$ has a tangent L, we can switch the point of tangency into the other two points on L and increase n by one.[5] If $\mathfrak{K}$ has no tangent then the complementary point set $\mathcal{P} \setminus \mathfrak{K}$ must be a subspace (since it is closed with respect to taking the join of any two of its points). This can only occur for $n \ge 2^{k-1}$.

Since the complement of a 2-divisible point set in $\mathrm{PG}(k - 1, \mathbb{F}_2)$ is 2-divisible, we get $(n, k) \in \mathrm{PD}(2, 1)$ also for $2^{k-1} < n \le 2^k - k - 2$. The proof is concluded by removing from $\mathcal{P}$ a projective basis in an l-subspace, $2 \le l \le k - 1$, which is 2-divisible. This covers the range $2^k - k - 1 \le n \le 2^k - 4$ and completes the proof. □

Now we assume $r \ge 2$ and restrict attention to the sets $\mathrm{LPD}(2, r)$. First we sharpen the simple upper bound (1), which for $q = 2$ is $\mathrm{F}(2, r) \le 2^{2r+2} - 3 \cdot 2^{r+1} + 1$.

Theorem 2. *For* $k \ge 2$ *we have* $\mathrm{F}(2, r) \le 2^{2r} - 2^{r-1} - 1$.

The proof uses a combination of the switching and concatenation constructions described in Section 4 together with the observation that $n \in \mathrm{LPD}(2, r)$ implies $n + (2^{r+1} - 1)\mathbb{Z} \subseteq \mathrm{LPD}(2, r)$ (juxtaposition with $(r+1)$-dimensional simplex codes).

Theorem 2 is sharp for $r = 2$, i.e., $\mathrm{F}(2, 2) = 13$. In fact it is not difficult to see that a projective doubly-even binary code of length n does not exist for $n \le 6$ and $9 \le n \le 13$, and hence $\mathrm{LPD}(2, 2) = \{7, 8\} \cup \mathbb{Z}_{\ge 14}$.

The case $r = 3$ ("triply-even" codes) was settled in [11] with one exception: $\mathrm{F}(2, 3) \in \{58, 59\}$, and $\mathrm{LPD}(2, 3)$ contains $\{15, 16, 30, 31, 32, 45, 46, 47, 48, 49, 50, 51\} \cup \mathbb{Z}_{\ge 60}$ and possibly 59. The non-existence proof in the remaining cases uses the methods developed in [15] and adhoc linear programming bounds derived from the first four MacWilliams identities.

The existence of a projective triply-even binary code of length 59 remains an open question. If such a code exists it must be constructible from two projective doubly-even codes of lengths 27 and 32 using the juxtaposition construction in [2, Prop. 19].[6]

Now we are going to give a classification of short projective 2^r-divisible binary codes for $r \le 3$. The case $r = 1$ is special as the set of all even-weight words forms a linear subspace of $\mathbb{F}_2^n$, the $[n, n - 1]$ *even-weight code*. Thus, we can produce all types of projective 2-divisible $[n, k]$ codes by starting with the even-weight code and

[4] This condition is always satisfied if $k \ge 3$ and the code is not a punctured simplex code [3, Prop. 2].

[5] The new point set will of course be spanning as well.

[6] The putative code contains a codeword of weight 32; hence [2, Prop. 22] applies.

recursively enumerating the codes C of codimension 1, as long as C is projective and not isomorphic to some previously produced code. While this somewhat simplistic approach could certainly be improved in various ways, it is good enough to produce the results shown in Table 1.

Table 1. Classification of projective 2-divisible binary codes

n	Σ	$k=$ 2	3	4	5	6	7	8	9	10	11	12	13
3	1	1											
4	1		1										
5	1			1									
6	2			1	1								
7	4		1	1	1	1							
8	7			2	2	2	1						
9	12			1	4	4	2	1					
10	26			1	6	9	6	3	1				
11	61			1	8	21	18	9	3	1			
12	169			1	11	45	59	35	13	4	1		
13	505				12	91	182	141	57	17	4	1	
14	1944				12	191	633	668	318	94	22	5	1

The projective binary doubly-even $[n,k]$ codes with lengths $n \le 26$ ($n = 26$, $k = 12$ not yet finished) have been classified by using the command

```
sage.coding.databases.self_orthogonal_binary_codes()
```

in SageMath [18]. The result is shown in Table 2.

Table 2. Classification of projective 4-divisible binary codes

n	Σ	$k=$ 3	4	5	6	7	8	9	10	11	12
7	1	1									
8	1		1								
14	1				1						
15	4		1	1	1	2					
16	9			2	2	3	2				
17	3				1	1	1				
18	3				1	1	1				
19	3					2	1				
20	7					2	4	1			
21	24				2	7	9	6			
22	101				3	24	41	24	9		
23	503			1	11	83	201	146	50	11	
24	1856			1	15	181	679	663	250	58	9
25	4972				6	234	1688	2162	748	121	13
26	$\ge$ *21843*				3	376	6021	11010	3920	478	$\ge$ *35*

We note that self-dual doubly-even codes are necessarily projective, and hence the classification of such codes for a particular n yields the classification of projective doubly-even $[n, n/2]$ codes. For example, from [7] we know that there are exactly 85 types of such codes for $n = 32$.

In [2], the binary 8-divisible codes of length 48 have been classified. On the first author's web page `http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/`, all 7647 types of *self-complementary* (i.e., containing the all-one word) binary 8-divisible codes are given explicitly. From this data, we have derived the classification of all projective binary 8-divisible codes of length up to 48. First, the self-complementary ones of length exactly 48 are produced by simply going through the list of all 7647 codes and checking them for projectivity, which leads to 291 types of codes.

For all other codes, we note that lengthening to $n = 48$ (padding codewords with zeros) and then augmenting by the all-one word of length 48, a binary self-complementary (not necessarily projective) 8-divisible code is produced. Therefore we can produce all codes by going through the list of 7647 codes C, enumerating all codimension 1 subcodes C' of C not containing the all-one word (their number is $2^{\dim(C)-1}$), removing all-zero coordinates, and checking the resulting code for projectivity. No code is lost in this way, but it may happen that the same isomorphism type of a code is produced several times. Filtering the list of codes for isomorphic copies produced the result shown in Table 3.

TABLE 3. Classification of projective 8-divisible binary codes

n	Σ	$k=$	4	5	6	7	8	9	10	11	12	13	14	15
15	1		1											
16	1			1										
30	1						1							
31	6			1	1	1	2	1						
32	11				2	2	3	3	1					
45	6						2	1	1	1	1			
46	51						6	18	14	8	4	1		
47	856				1	11	100	299	274	122	40	8	1	
48	2973				1	15	211	921	1071	529	173	44	7	1

We have the following constructions for projective 2^r-divisible binary $[n, k]$ codes. The codes are described in terms of their associated point sets in $\mathrm{PG}(k-1, \mathbb{F}_2)$.

- $n = 2^{r+1} - 1$: A projective r-flat ($[2^{r+1} - 1, r + 1]$ simplex code)
- $n = 2^{r+1}$: An affine $(r + 1)$-flat ($[2^{r+1}, r + 2]$ 1st-order RM code)
- $n = 2^{r+2} - 2$: The (unique) disjoint union of two projective r-flats, of ambient space dimension $k = 2r + 2$
- $n = 2^{r+2} - 1$: The disjoint union of a projective r-flat F and an affine $(r + 1)$-flat A. We get one type of code for each intersection dimension $s \in \{0, \ldots, r + 1\}$ of F with the hyperplane at infinity of A. The ambient dimension is $k = 2r+3-s$. In the case $s = r+1$, we simply get a projective $(r + 1)$-flat, which is even 2^{r+1}-divisible.

  A further code is given by the set of 7 projective $(r - 1)$-flats passing through a common $(r - 2)$-flat V such that the image modulo V is a projective basis. The ambient dimension is $k = r + 5$.
- $n = 2^{r+2}$: The disjoint union of two affine $(r + 1)$-flats A_1 and A_2. There are two types of such unions for each $k \in \{r + 3, \ldots, 2r + 3\}$ and a single type for $k = 2r + 4$. One of the types for $k = r + 3$ actually is an affine $(r + 2)$-flat, which is even 2^{r+1}-divisible.

  There are two more types: Let $\{S_1, \ldots, S_8\}$ be a set of 8 projective $(r - 1)$-flats passing through a common $(r - 2)$-flat V, such that the image modulo V is a projective basis. Then $(S_1 \cup \ldots \cup S_8) \setminus V$ yields a suitable code with $k = r + 6$.

  Furthermore, let X be the disjoint union of maximum possible dimension of $\mathrm{PG}(1, \mathbb{F}_2)$ and a projective basis of $\mathrm{PG}(3, \mathbb{F}_2)$. Then $\#X = 8$ and

$\dim\langle X\rangle = 6$. Now let V be a projective $(r-2)$-flat disjoint from $\langle X\rangle$. Then $(\bigcup_{P\in X}\langle P,V\rangle)\setminus V$ yields a suitable code with $k = r+5$.

Note that the three constructions involving an $(r-1)$-subspace V ("vertex") are examples of the generalized cone construction (with a vertex of dimension $s = r-1$) mentioned in Section 4.

For $r \in \{1,2,3\}$, the above constructions cover all types of codes of the corresponding lengths, with the exception of $r = 1$, $n = 6$, where additionally the even-weight code shows up.

For $n = 3(2^{r+1}-1) = 2^{r+2}+2^{r+1}-3$, suitable codes can be produced as the disjoint union of three projective r-flats. This yields a unique type of code for each ambient space dimension $k \in \{2r+2,\ldots,3r+3\}$. In the case $k = 2r+2$, the resulting code is a two-weight code with weights 2^{r+1} and $2^{r+1}+2^r$. However, for all $r \in \{1,2,3\}$, there are projective 2^r-divisible codes different from this construction. The most interesting case is $r = 3$, $n = 45$, where only a single further code shows up. It is another $[45,8]$ two-weight code with weights 16 and 24; see [12, Th. 4.1]. The associated point set $\mathfrak{K}$ in $\mathrm{PG}(7,\mathbb{F}_2)$ consists of a projective basis $P_1,\ldots,P_9$ and the $\binom{9}{2} = 36$ remaining points on the lines P_iP_j. Furthermore, it is worth mentioning that also in the case $r = 2$, $n = 21$ there is a second $[21,6]$ two-weight with weights 8 and 12, see [3].

For further information on $r = 2$, $n = 15$ see [10] and on $r = 2$, $n = 17$ see [11, Sect. 1.6.1]. A further settled case worth mentioning is $r = 3$, $n = 51$, see [11, Lem. 24]. In that case, there is a unique code, which can be constructed as the concatenation of an ovoid in $\mathrm{PG}(3,\mathbb{F}_4)$ with the binary $[3,2]$ simplex code.

Acknowledgement

The authors are grateful to Robert L. Miller for explaining how to use his database of doubly-even codes in SageMath, and to Koichi Betsumiya and Akihiro Munemasa for additional information on the classification of triply-even codes. Thomas Honold was supported by the National Natural Science Foundation of China under Grant 61571006. The authors would like to acknowledge the financial support provided by COST – *European Cooperation in Science and Technology*. The first, fourth, and fifth author were supported in part by the grant KU 2430/3-1 and WA 1666/9-1 – Integer Linear Programming Models for Subspace Codes and Finite Geometry – from the German Research Foundation.

References

[1] Ax, J.: Zeroes of polynomials over finite fields. Amer. J. Math. 86, 255–261 (1964)

[2] Betsumiya, K., Munemasa, A.: On triply even binary codes. J. Lond. Math. Soc. (2) 86(1), 1–16 (2012)

[3] Bouyukliev, I., Fack, V., Willems, W., Winne, J.: Projective two-weight codes with small parameters and their corresponding graphs. Des. Codes Cryptogr. 41(1), 59–78 (2006)

[4] Brauer, A.: On a problem of partitions. Amer. J. Math. 64(1), 299–312 (1942)

[5] Calderbank, R., Kantor, W.: The geometry of two-weight codes. Bull. London Math. Soc. 18(2), 97–122 (1986)

[6] Delsarte, P.: An algebraic approach to the association schemes of coding theory. Philips research reports supplements (10), 103 (1973)

[7] Conway, J.H., Pless, V., Sloane, N.J.A.: The binary self-dual codes of length up to 32: A revised enumeration. J. Combin. Theory Ser. A 60, 183–195 (1992)

[8] Delsarte, P., McEliece, R.J.: Zeroes of functions in finite abelian group algebras. Amer. J. Math. 98, 197–224 (1976)

[9] Dodunekov, S., Simonis, J.: Codes and projective multisets. Electron. J. Combin. 5(R37), 1–23 (1998)

[10] Honold, T., Kiermaier, M., Kurz, S.: Classification of large partial plane spreads in $\mathrm{PG}(6,\mathbb{F}_2)$ and related combinatorial objects (Apr 2016), submitted for publication. Preprint arXiv:1606.07655

[11] Honold, T., Kiermaier, M., Kurz, S.: Partial spreads and vector space partitions (Nov 2016), preprint arXiv:1611.06328
[12] Haemers, W.H., Peeters, R., van Rijckevorsel, J.M.: Binary codes of strongly regular graphs. Des. Codes Cryptogr. 17, 187–209 (1999)
[13] Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press (2003)
[14] Koetter, R., Kschischang, F.: Coding for errors and erasures in random network coding. IEEE Trans. Inform. Theory 54(8), 3579–3591 (Aug 2008)
[15] Kurz, S.: Packing vector spaces into vector spaces. Australas. J. Combin. 68(1) (2017), to appear
[16] Silva, D., Kschischang, F., Koetter, R.: A rank-metric approach to error control in random network coding. IEEE Trans. Inform. Theory 54(9), 3951–3967 (Sep 2008)
[17] Silva, D., Kschischang, F., Koetter, R.: Communication over finite-field matrix channels. IEEE Trans. Inform. Theory 56(3), 1296–1306 (Mar 2010)
[18] Stein, W.A., et al.: Sage Mathematics Software (Version 7.1), The Sage Development Team, 2016, `http://www.sagemath.org`
[19] Tsfasman, M.A., Vlăduţ, S.G.: Geometric approach to higher weights. IEEE Trans. Inform. Theory 41, 1564–1588 (1995)
[20] Ward, H.: Divisible codes—a survey. Serdica Math. J. 27(4), 263–278 (2001)

Daniel Heinlein, University of Bayreuth, 95440 Bayreuth, Germany, daniel.heinlein@uni-bayreuth.de

Thomas Honold, Zhejiang University, 310027 Hangzhou, China, honold@zju.edu.cn

Michael Kiermaier, University of Bayreuth, 95440 Bayreuth, Germany, michael.kiermaier@uni-bayreuth.de

Sascha Kurz, University of Bayreuth, 95440 Bayreuth, Germany, sascha.kurz@uni-bayreuth.de

Alfred Wassermann, University of Bayreuth, 95440 Bayreuth, Germany, alfred.wassermann@uni-bayreuth.de