Lengths of divisible codes – the missing cases

Sascha Kurz

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

Abstract

A linear code C over \mathbb{F}_q is called Δ -divisible if the Hamming weights wt(c) of all codewords $c \in C$ are divisible by Δ . The possible effective lengths of q^r -divisible codes have been completely characterized for each prime power q and each non-negative integer r in [KK20]. The study of Δ -divisible codes was initiated by Harold Ward [War81]. If t divides Δ but is coprime to q, then each Δ -divisible code C over \mathbb{F}_q is the t-fold repetition of a Δ/t -divisible code. Here we determine the possible effective lengths of p^r -divisible codes over finite fields of characteristic p, where $r \in \mathbb{N}$ but p^r is not a power of the field size, i.e., the missing cases.

Keywords: Divisible codes, linear codes, Galois geometry Mathematics Subject Classification: 51E23 (05B40)

1 Introduction

A linear code C over \mathbb{F}_q is called Δ -divisible if the Hamming weights wt(c) of all codewords $c \in C$ are divisible by Δ . The study of divisible codes was initiated by Harold Ward [War81]. Linear codes meeting the Griesmer bound in many cases have to admit a relatively large divisibility constant Δ , see [War98]. In order to state a connection between divisible codes and Galois geometries we associate each subspace $U \in \mathrm{PG}(v-1,q)$ with its characteristic function χ_U mapping each point $\mathrm{PG}(v-1,q)$ to a non-negative integer multiplicity, i.e., $\chi_U(P) = 1$ iff $P \leq U$ and $\chi_U(P) = 0$ otherwise. We say that a mapping \mathcal{M} from the point set of $\mathrm{PG}(v-1,q)$ to \mathbb{N} is Δ -divisible if the corresponding linear code $C_{\mathcal{M}}$ associated with the multiset of points characterized by \mathcal{M} is Δ -divisible. We call $\mathcal{M}(P)$ the multiplicity of a point P and extend this notion additively to arbitrary subspaces S by letting $\mathcal{M}(S)$ be the sum over all point multiplicities $\mathcal{M}(P)$ where P is contained in S. If S is the entire ambient space then we speak of the cardinality $\#\mathcal{M}$. Using this notion, we can more directly state that a multiset of points \mathcal{M} in $\mathrm{PG}(v-1,q)$ is Δ -divisible iff we have $\#\mathcal{M} \equiv \mathcal{M}(H) \pmod{\Delta}$ for every hyperplane H. The effective length of $C_{\mathcal{M}}$ equals the cardinality $\#\mathcal{M}$. We say that a multiset M of points is spanning if the points with positive multiplicity span the entire ambient space. Using the geometric language we will call 1-, 2-, 3-, and (v-1)-dimensional subspaces points, lines, planes, and hyperplanes, respectively.

In e.g. [KK20, Lemma 11] it was shown that for each multiset of subspaces \mathcal{U} in $\mathrm{PG}(v-1,q)$ that have dimensions at least k the multiset of points $\chi_{\mathcal{U}} := \sum_{U \in \mathcal{U}} \chi_U$ is q^{k-1} -divisible. Since also the complementary multiset of points is q^{k-1} -divisible, non-existence results for q^{k-1} -divisible codes imply upper bounds on the maximum size of k-spreads, see e.g. [HKK18] for more details. Similarly, non-existence results for so-called vector space partitions, i.e., set of subspaces partitioning the point set of $\mathrm{PG}(v-1,q)$, can be deduced from certain non-existence results for q^r -divisible codes, see e.g. [Kur22]. Also in the situation where some points can be contained in several subspaces non-existence results for q^{k-1} -divisible codes can be applied to deduce results for problems in Galois geometry. For constant-dimension codes, i.e., sets of k-dimensional subspaces of $\mathrm{PG}(v-1,q)$ such that the dimensions of the pairwise intersections are upper bounded by some integer, they can be utilized for upper bounds on the cardinality, see e.g. [KK20, Theorem 12]. For similar bounds for mixed-dimension subspace codes, where the codewords can have different dimensions, we refer to [HKK19]. Two surveys on applications of divisible codes are given by [Kur21, War01].

The possible (effective) lengths of q^r -divisible codes have been completely characterized for each prime power q and each non-negative integer r in [KK20, Theorem 1]. An important structure result for Δ -divisible codes C over \mathbb{F}_q was shown in [War81]: If $t \in \mathbb{N}$ divides Δ and is coprime to Δ then there exists a Δ/t divisible code C' over \mathbb{F}_q such that C is the t-fold repetition of C'. So, it suffices to study the possible (effective) lengths of p^e -divisible codes over \mathbb{F}_q , where p is the characteristic of the field and e an integer. When q is not a prime the characterization result from [KK20] does not give an answer for the cases when the divisibility constant Δ is not a power of the field size (but only its characteristic). Here we close this gap and state a corresponding characterization of the possible (effective) lengths in Theorem 2.

A few general (and easy) constructions for Δ -divisible multisets of points \mathcal{M} in PG(v - 1, q) are known, see e.g. [KK20] for proofs:

- (1) if a multiset of points \mathcal{M} in $\operatorname{PG}(v-1,q)$ is Δ -divisible, then there exists an embedding \mathcal{M}' of \mathcal{M} in $\operatorname{PG}(v'-1,q)$ for each $v' \geq v$ that is also Δ -divisible;
- (2) if multisets of points $\mathcal{M}, \mathcal{M}'$ in $\mathrm{PG}(v-1,q)$ are Δ -divisible with cardinalities n, n', then $\mathcal{M} + \mathcal{M}'$ is Δ -divisible with cardinality n + n' in $\mathrm{PG}(v-1,q)$;
- (3) if a multiset of points \mathcal{M} in PG(v-1,q) is Δ -divisible with cardinalities n, then $c \cdot \mathcal{M}$ is $c \cdot \Delta$ -divisible with cardinality cn for each positive integer c;
- (4) for each integer $u \ge 1$ and each *u*-dimensional subspace U in PG(v-1,q) the corresponding characteristic function χ_U is q^{u-1} -divisible with cardinality $\frac{q^u-1}{q-1}$.

Due to (1) we are only interested in the possible cardinalities of Δ -divisible multisets of points and not in their dimensions (while they may play a role in some applications). Assume $q = p^e$ for a prime p and an integer e. With this we will use the parameterization $\Delta = p^{ae-b}$ where $a, b \in \mathbb{N}$ with $a \ge 1$ and $b \le e-1$. By (4) an (a + 1)-dimensional subspace is q^a -divisible. Since $ae \ge ae - b$ it is also p^{ae-b} -divisible. For $1 \le i \le a$ we can consider an p^{ie-b} -fold (a - i + 1)-dimensional subspace which is p^{ae-b} -divisible using (3). Let us denote the corresponding cardinalities by $s_q(a, b, i)$, where $1 \le i \le a$, and write $s_q(a, b, 0)$ for the cardinality of an (a + 1)-dimensional subspace. Using (2) we conclude that for each $c_0, \ldots, c_a \in \mathbb{N}$ there exists a p^{ae-b} -divisible multiset of points of cardinality

$$n = \sum_{i=0}^{a} c_i \cdot s_q(a, b, i)$$

in PG(v-1,q) for sufficiently large dimension v of the ambient space. Our main theorem, see Theorem 2, will state that for other cardinalities there is no p^{ae-b} -divisible multiset of points and we will give a direct characterization of the attainable cardinalities, i.e., we solve the so-called Frobenius coin problem for the "coin values" $s_q(a, b, 0), \ldots, s_q(a, b, a)$. For a solution of the Frobenius coin problem for geometric sequences we refer to [OP08].

The remaining part of this paper is structured as follows. In Section 2 we prove our main theorem and in Section 3 we consider the possible cardinalities of Δ -divisible sets of points. In the latter section we can only state a few numerical results and leave the general problem widely open. We especially study 2-divisible sets of points and obtain a few preliminary results. Related results can be found in the literature under the terms of sets of odd and of even type, see e.g. [Adr23, HH80, KdR98, Lim10, She83, TM13, WS14].

2 The generalized theorem

For each integer $i \ge 1$ we define $[i]_q := \frac{q^i - 1}{q - 1}$, i.e., the number of points of an *i*-dimensional subspace. For each prime power q we write $q = p^e$, where p is the characteristic of \mathbb{F}_q . When we consider Δ -divisible codes

over \mathbb{F}_q we assume that Δ is a power of p. More concretely, we will use the parameterization $\Delta = p^{ae-b}$ where $a, b \in \mathbb{N}$ with $a \geq 1$ and $b \leq e-1$. Sometimes we will also use f := ae - b, i.e., the exponent in $\Delta = p^f$. For a fixed prime power $q = p^e$, non-negative integers a, b with $a \geq 1$, $b \leq e-1$, and $i \in \{0, \ldots, a\}$ we define

$$s_q(a,b,i) := [a+1]_q$$
 (1)

if i = 0 and

$$s_q(a,b,i) := q^i \cdot [a-i+1]_q / p^b = p^{ie-b} \cdot [a-i+1]_q = p^{e-b} \cdot \left(q^{i-1} + q^i + \dots + q^{a-1}\right)$$
(2)

for $1 \leq i \leq a$. Note that for $i \geq 1$ the number $s_q(a, b, i)$ is divisible by p^{ie-b} but not by p^{ie-b+1} , where $ie-b \geq 1$, and $s_q(a, b, 0)$ is coprime to p. This property allows us to create kind of a positional system upon the sequence of base numbers

$$S_q(a,b) := (s_q(a,b,0), s_q(a,b,1), \dots, s_q(a,b,a)).$$

As it can be easily shown, each integer n has a unique $S_q(a, b)$ -adic expansion

$$n = \sum_{i=0}^{a} c_i \cdot s_q(a, b, i) \tag{3}$$

with $c_0 \in \{0, \ldots, p^{e-b} - 1\}$, $c_1, \ldots, c_a - 1 \in \{0, \ldots, q - 1\}$ and *leading coefficient* $c_a \in \mathbb{Z}$. The sum $p^b c_0 + c_1 + c_2 + \cdots + c_a$ will be called the *cross sum* of the $S_q(a, b)$ -adic expansion of n.

Example 1. For q = 8 and $\Delta = 32$ we have p = 2, e = 3, a = 2, b = 1, and

$$S_8(2,1) = (s_8(2,1,0), s_8(2,1,1), s_8(2,1,2)) = (73,36,32).$$

The characteristic function χ_E of a plane in $\operatorname{PG}(v-1,8)$ is 64-divisible with cardinality $s_8(2,1,0) = 73$. Since the characteristic function χ_L of a line over \mathbb{F}_8 is 8-divisible $4 \cdot \chi_L$ is 32-divisible with cardinality $s_8(2,1,1) = 36$. A 32-fold point corresponds to a 32-divisible multiset of points in $\operatorname{PG}(v-1,8)$ with cardinality $s_8(2,1,2) = 32$. As an example, the $S_8(2,1)$ -adic expansion of 1049 is given by

$$1049 = 1 \cdot 73 + 4 \cdot 36 + 26 \cdot 32$$

and the $S_8(2,1)$ -adic expansion of 195 is given by

$$195 = 3 \cdot 73 + 2 \cdot 36 - 3 \cdot 32.$$

In the first case the leading coefficient is 26 and a 32-divisible multiset of points of cardinality 1049 is given e.g. by $\chi_{E_1} + \sum_{i=1}^{4} 4 \cdot \chi_{L_i} + \sum_{i=1}^{26} 32 \cdot \chi_{P_i}$ or by $\sum_{i=1}^{5} \chi_{E_i} + \sum_{i=1}^{11} 4 \cdot \chi_{L_i} + \sum_{i=1}^{9} 32 \cdot \chi_{P_i}$, where the E_i are arbitrary planes, the L_i are arbitrary lines, and the P_i are arbitrary points. In the second case the leading coefficient is -3 and the subsequent theorem tells us that no 32-divisible multiset of points of cardinality 195 exists in PG(v - 1, 8), which also implies that $195 = 73c_0 + 36c_1 + 32c_2$ does not have a solution $(c_0, c_1, c_2) \in \mathbb{N}^3$.

Based on the $S_q(a, b)$ -adic expansion we can state our main theorem.

Theorem 2. Let $q = p^e$, $n \in \mathbb{Z}$, and $a, b \in \mathbb{N}$ with $a \ge 1$, $b \le e - 1$. The following statements are equivalent:

- (i) There exists a p^{ae-b} -divisible linear code of effective length n over \mathbb{F}_q .
- (ii) The leading coefficient c_a of the $S_q(a,b)$ -adic expansion of n is non-negative.

First we will show the implication (ii) \Rightarrow (i):

Lemma 3. Let $q = p^e$, $n \in \mathbb{Z}$, and $a, b \in \mathbb{N}$ with $a \ge 1$, $b \le e - 1$. If the leading coefficient c_a of the $S_q(a,b)$ -adic expansion of n is non-negative, then there exists a p^{ae-b} -divisible linear code of effective length n over \mathbb{F}_q .

Proof. Let $n = \sum_{i=0}^{a} c_i \cdot s_q(a, b, i)$ be the $S_q(a, b)$ -adic expansion of n and $\Delta := p^{ae-b}$. By assumption on the non-negativity of the leading coefficient c_a and the definition of the $S_q(a, b)$ -adic expansion of n we have $c_i \in \mathbb{N}$ for all $0 \leq i \leq a$. Next we will construct a Δ -divisible multiset \mathcal{M} of points in $\mathrm{PG}(v-1,q)$ of cardinality n. To this end, let U_i be *i*-dimensional subspaces for $1 \leq i \leq a+1$ (assuming that the ambient dimension v is sufficiently large). With this $\mathcal{M}_0 := \chi_{U_{a+1}}$ is a q^a -divisible multiset of points with cardinality $s_q(a, b, 0) = [a+1]_q$. Since Δ divides q^a , \mathcal{M}_0 is also Δ -divisible. For $1 \leq i \leq a$ we set $\mathcal{M}_i := p^{ie-b} \cdot \chi_{U_{a-i+1}}$, so that \mathcal{M}_i is Δ -divisible with cardinality $s_q(a, b, i)$. With this, we set $\mathcal{M} := \sum_{i=0}^{a} c_i \cdot \mathcal{M}_i$, so that \mathcal{M} is Δ -divisible with cardinality n. The corresponding linear code $C_{\mathcal{M}}$ over \mathbb{F}_q has effective length n and is Δ -divisible.

Lemma 4. ([Syl82]) Let a_1, a_2 be two positive coprime integers. The largest integer that cannot be written as a non-negative integer linear combination $c_1a_1+c_2a_2$, where $c_1, c_2 \in \mathbb{N}$, is given by $g(a_1, a_2) := a_1a_2-a_1-a_2$.

Lemma 5. Let $q = p^e$ and $0 \le b \le e - 1$ be an integer. If \mathcal{M} is a p^{e-b} -divisible multiset of points in $\operatorname{PG}(v-1,q)$ of cardinality n, then there exist non-negative integers s, t such that $n = s \cdot (q+1) + t \cdot \Delta$, where $\Delta := p^{e-b}$.

Proof. W.l.o.g. we assume $n \ge 1$. Let k be the dimension of the span of \mathcal{M} , i.e. the span of the points with positive multiplicity, and w.l.o.g. we assume v = k. If k = 1, then we have $\mathcal{M}(P) \equiv 0 \pmod{\Delta}$ for the unique point in $\mathrm{PG}(0,q)$ and there exists a non-negative integer t such that $n = t \cdot \Delta$. If k = 2, then $\mathrm{PG}(1,q)$ consists of q+1 pairwise different points P_0, \ldots, P_q and we have $\mathcal{M}(P_i) \equiv n \pmod{\Delta}$ for all $0 \le i \le q$. Now let \mathcal{M}' arise from \mathcal{M} by decreasing the points multiplicities by Δ till we have $\mathcal{M}(P_i) = s$ for all $0 \le i \le q$ for some integer $0 \le s < \Delta$. Here t is given by $(n - s \cdot (q + 1))/\Delta$.

Since q + 1 and Δ are coprime, the largest integer that cannot be written as $s = s(q + 1) + t\Delta$ for non-negative integers s, t is given by

$$(q+1)\Delta - (q+1) - \Delta \le q^2 + q - (q+1) - \Delta < q^2,$$

see Lemma 4. So, we can assume $n < q^2$ and $k \ge 3$ in the following. Since $k \ge 3$ there are at least $[3]_q = q^2 + q + 1 > q^2$ points and there exists a point P with multiplicity zero. Let S be a subspace attaining the maximum possible dimension l satisfying $\mathcal{M}(S) = 0$. Clearly we have $l \ge 1$. If l < k - 2 then consider the $[k-l]_q \ge [3]_q = q^2 + q + 1 > q^2$ (l+1) dimensional subspaces $S' \ge S$. Since $\mathcal{M}(S') > 0$ and these spaces pairwise intersect in S we have $n = \#\mathcal{M} \ge q^2 + q + 1 > q^2$ – contradiction. So, let S be a (k-2)-dimensional subspace with $\mathcal{M}(S) = 0$ and consider the q + 1 hyperplanes H_0, \ldots, H_q that contain S. Since $\mathcal{M}(H_i) \equiv n$ (mod Δ) for all $0 \le i \le q$, there exists an integer $0 \le s < \Delta$ such that $\mathcal{M}(H_i) \equiv s \pmod{\Delta}$. Since the hyperplanes H_i pairwise intersect in S and $\mathcal{M}(S) = 0$, we have $n = \sum_{i=0}^q \mathcal{M}(H_i)$, so that $n \ge s \cdot (q+1)$ and $n \equiv s \pmod{\Delta}$ (using the fact that Δ divides q). Thus, we can set $t = (n - (q+1)s)/\Delta$.

Lemma 6. Theorem 2 is true for a = 1.

Proof. Due to Lemma 3, it suffices to show the implication (i) \Rightarrow (ii). From Lemma 5 we conclude the existence of $s', t' \in \mathbb{N}$ with $n = s'(q+1) + t'\Delta$. Write $s' = s + x\Delta$ for $s, x \in \mathbb{N}$ with $s < \Delta$ and set $t := t' + x(q+1) \ge 0$.

Lemma 7. (E,g, [KK20, Lemma 5]) Let \mathcal{M} be a non-empty multiset of points in PG(v-1,q), then there exists a hyperplane H with $\mathcal{M}(H) < \frac{\#\mathcal{M}}{q}$.

Lemma 8. ([KK20, Lemma 4]) Let \mathcal{M} be a Δ -divisible multiset of points in PG(v-1,q) and H be an arbitrary hyperplane. If q divides Δ , then the restriction $\mathcal{M}|_H$ of \mathcal{M} to H is Δ/q -divisible.

Proof of Theorem 2. Due to Lemma 3, it suffices to show the implication (i) \Rightarrow (ii). Using Lemma 6 we can assume a > 1 and prove by induction on a.

So, let $n = \sum_{i=0}^{a} c_i s_q(a, b, i)$ be the $S_q(a, b)$ -adic expansion of n and $\sigma = p^b c_0 + \sum_{i=1}^{a} c_i$ be its cross sum. Let H be a hyperplane and set $m := \mathcal{M}(H)$. Since \mathcal{M} is Δ -divisible for $\Delta := p^{ae-b}$ there exists a non-negative integer τ with $n - m = \tau \Delta$. We compute

$$m = n - \tau \Delta = c_0 s_q(a, b, 0) + \sum_{i=1}^{a-1} c_i s_q(a, b, i) + c_a s_q(a, b, a) - \tau \Delta$$

$$= c_0 s_q(a - 1, b, 0) + c_0 \cdot q^a + \sum_{i=1}^{a-1} c_i \left(s_q(a - 1, b, i) + \Delta \right) + c_a \Delta - \tau \Delta$$

$$= \sum_{\substack{i=0\\a-1}}^{a-1} c_i s_q(a - 1, b, i) + (\sigma - \tau) \Delta$$
(4)

$$= \sum_{i=0}^{a-1} c_i s_q (a-1,b,i) + (c_{a-1} + q(\sigma - \tau)) \Delta/q$$
(5)

By construction, $\mathcal{M}|_H$ is Δ/q -divisible, see Lemma 8, with cardinality m and Equation (5) gives the $S_q(a-1,b)$ -adic expansion of m. Hence, by induction we get $c_{a-1} + q(\sigma - \tau) \ge 0$. So $q(\sigma - \tau) \ge -c_{a-1} > -q$, implying $\sigma - \tau > -1$ and thus $\sigma \ge \tau$.

By Lemma 7 we may choose H such that $m < \frac{n}{q}$. Thus using the expression in Equation (4) for m we compute

$$0 < n - qm = \sum_{i=0}^{a} c_i s_q(a, b, i) - \sum_{i=0}^{a-1} c_i s_q(a - 1, b, i)q - (\sigma - \tau)\Delta q$$

$$= c_0 + \sum_{i=1}^{a-1} p^{e-b} q^{i-1} c_i + c_a \Delta - (\sigma - \tau)\Delta q$$

$$\leq p^{e-b} - 1 + p^{e-b} (q - 1) \sum_{i=0}^{a-2} q^i + c_a \Delta$$

$$< p^{e-b} + p^{e-b} (q^{a-1} - 1) + c_a \Delta$$

$$= (1 + c_a)\Delta,$$

which implies $c_a \ge 0$.

Example 9. For each positive integer n that is either even or at least 5 a 2-divisible code of effective length n exists over \mathbb{F}_4 . For the constructive part we can consider a 2-fold point, a line, and combinations thereof. For the other direction we can easily check that the leading coefficient of the $S_4(1,1)$ -adic expansion of 1 as well as of 3 is negative, so that we can apply Theorem 2.

Example 10. For each positive integer n that is not contained in

 $\{2, 4, 6, 12, 14, 22\} \cup \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 33, 35, 43\}$

an 8-divisible linear code of effective length n exists over \mathbb{F}_4 . Note that an 8-fold point, a 2-fold line and a plane are 8-divisible of cardinalities 8, 10, and 21. The mentioned positive integers are the only ones that cannot be expressed as non-negative integer linear combinations of 8, 10, and 21.

Example 11. For each positive integer n that is either even or at least 9 a 2-divisible code of effective length n exists over \mathbb{F}_8 . For the constructive part we can consider a 2-fold point, a line, and combinations thereof. For the other direction we can easily check that the leading coefficient of the $S_8(1,2)$ -adic expansion of $n \in \{1,3,5,7\}$ is negative, so that we can apply Theorem 2.

We can also consider the dimension k of the span of a Δ -divisible multiset of points \mathcal{M} . If k = 1, then \mathcal{M} clearly is a λ -fold point where Δ divides λ . Also the case k = 2 can be easily classified.

Lemma 12. Let \mathcal{M} be a Δ -divisible multiset of points in $\mathrm{PG}(1,q)$. Then, there exist l, possibly equal, points P_1, \ldots, P_l such that $\mathcal{M} = \sum_{i=1}^l \Delta \chi_{P_i} + s \chi_L$, where L is the line forming the ambient space and $s = (\#\mathcal{M} - l\Delta)/(q+1) \in \mathbb{N}$. Moreover, Δ divides qs.

Proof. Let \mathcal{M}' arise from \mathcal{M} by recursively removing points of multiplicity Δ and let l be the number of removed points. So, we have $\#\mathcal{M}' = \#\mathcal{M} - l\Delta$, the maximum point multiplicity of \mathcal{M}' is at most $\Delta - 1$, and \mathcal{M}' is also Δ -divisible. From Δ -divisibility we conclude $\mathcal{M}'(P) \equiv \#\mathcal{M}' \pmod{\Delta}$ for every point $P \leq L$. Since the maximum point multiplicity of \mathcal{M}' is at most $\Delta - 1$ there exists a non-negative integer s with $\mathcal{M}'(P) = s$ for all points P, i.e., $\mathcal{M}' = s\chi_L$. Counting points gives $s = \#\mathcal{M}'/(q+1) = (\#\mathcal{M} - l\Delta)/(q+1)$. Since \mathcal{M}' is Δ -divisible and χ_L is q-divisible we conclude that Δ divides qs (including the case s = 0). \Box

As we have mentioned the Frobenius coin problem the formulate the result for the largest possible effective length n such that no p^{ae-b} -divisible linear code over \mathbb{F}_{p^e} exists in this vein:

Proposition 13. Let $q = p^e$ and $a, b \in \mathbb{N}$ with $a \ge 1$, $b \le e - 1$. The largest integer that cannot be written as a non-negative integer linear combination $\sum_{i=0}^{a} c_i s_q(a, b, i)$, where $c_0, c_1, \ldots, c_a \in \mathbb{N}$, is given by

$$g(s_q(a,b,0),\ldots,s_q(a,b,0)) := a \cdot p^{(a+1)e-b} - \frac{q^{a+1}-1}{q-1}$$

Proof. Given the definition of the $S_q(a, b)$ -adic expansion of an integer n we conclude that the largest integer with a negative leading coefficient is given by

$$\begin{split} & \left(p^{e-b}-1\right) \cdot s_q(a,b,0) \,+\, \sum_{i=1}^{a-1} (q-1) \cdot s_q(a,b,i) \,+\, (-1) \cdot s_q(a,b,a) \\ & = \quad \left(p^{e-b}-1\right) \cdot \frac{q^{a+1}-1}{q-1} \,+\, \sum_{1=1}^{a-1} p^{ie-b} \cdot \left(q^{a-i+1}-1\right) \,-\, p^{ae-b} \\ & = \quad \left(p^{e-b}-1\right) \cdot \frac{q^{a+1}-1}{q-1} \,+\, (a-1) \cdot p^{(a+1)e-b} \,-\, p^{e-b} \cdot \sum_{i=0}^{a-2} q^i \,-\, p^{ae-b} \\ & = \quad \left(p^{e-b}-1\right) \cdot \frac{q^{a+1}-1}{q-1} \,-\, p^{e-b} \cdot \frac{q^{a-1}-1}{q-1} \,+\, (a-1) \cdot p^{(a+1)e-b} \,-\, p^{ae-b} \\ & = \quad p^{e-b} \cdot q^{a-1} \cdot (q+1) \,-\, \frac{q^{a+1}-1}{q-1} \,+\, (a-1) \cdot p^{(a+1)e-b} \,-\, p^{ae-b} \\ & = \quad a \cdot p^{(a+1)e-b} \,-\, \frac{q^{a+1}-1}{q-1} \,. \end{split}$$

With this, the stated result is implied by Theorem 2.

In Examples (9)-(11) the corresponding numbers $g(s_q(a, b, 0), \ldots, s_q(a, b, 0))$ are given by 3, 43, and 7.

3 Projective divisible codes

In some applications, e.g. for upper bounds for partial spreads, see e.g. [HKK18], the maximum point multiplicity of the multisets of points has to be 1, i.e., we indeed have sets of points and the corresponding linear codes have to be projective. The possible effective lengths of q^r -divisible projective codes are very far from being characterized and only partial results are known. Here there a papers treating just one length, see [Kur20]. The characterization problem is again finite since for every (u + 1)-dimensional space U and

every (u + 2)-dimensional space $U' \ge U$ we have that χ_U is a q^u -divisible set of cardinality $[u + 1]_q$ and $\chi_{U'} - \chi_U$ (i.e., the characteristic function of an affine subspace) is a q^u -divisible set of cardinality q^u , so that we can apply Lemma 4 since $gcd([u + 1]_q, q^u) = 1$. For a recent survey on the possible lengths of q^r -divisible projective codes for integers r we refer to [Kur21, Section 7]. First few preliminary results for the case of restricted column multiplicities larger than 1 can be found in [KK23].

For non-prime field sizes q Baer subspaces and the like give another construction of Δ -divisible point sets:

Lemma 14. Let $q = p^e$ and $1 \le f < e$. Then the set of points of an u-space U over $GF(p^e)$ that is also contained in the subfield $GF(p^f)$ is p^{uf-e} divisible with cardinality $\frac{p^{fu}-1}{p^f-1}$ for all $u \in \mathbb{N}_{\ge 3}$.

Note that the assumption $u \ge 3$ is necessary since the hyperplanes of Baer lines are points and there is nothing like a "Baer point", i.e., multiplicities 1 and 0 both occur. Hyperplanes of Baer planes are of course Baer lines and so on.

Example 15. Over \mathbb{F}_4 a line gives a 2-divisible projective code of effective length 5 and a Baer plane gives a 2-divisible projective code of effective length 7. The largest integer that cannot be written as a sum of 5s and 7s is $5 \cdot 7 - 5 - 7 = 23$, see Lemma 4. The linear code corresponding to an affine plane is 4-divisible and has effective length 25.

In order to get the full picture of the possible effective lengths of 2-divisible projective codes over \mathbb{F}_4 we may simply enumerate all such codes using a computer program. To this end we have used LinCode [BBK21]. For field sizes $q = p^e$ we represent the field elements by polynomials over \mathbb{F}_p modulo an irreducible polynomial f of degree e. Here we use the Conway polynomials $f(\alpha) = \alpha^2 + \alpha + 1$, $f(\alpha) = \alpha^3 + \alpha + 1$, and $f(\alpha) = \alpha^2 + 2\alpha + 2$ for q = 4, q = 8, and q = 27, respectively. For an even more compact representation we replace $\sum_{i=0}^{e-1} c_i \alpha^i$ by the integer $\sum_{i=0}^{e-1} c_i p^i$.

Proposition 16. A 2-divisible projective code of effective lengths $n \ge 1$ over \mathbb{F}_4 exists iff $n \ge 5$.

Proof. As mentioned in Example 15 n = 5 and n = 7 can be attained. Further examples are given by

• length n = 6, weight enumerator $1z^0 + 45z^4 + 18z^6$, |Aut| = 2160, generator matrix

1	1	1	1	1	0	$0\rangle$	
	1	2	3	0	1	0	;
1	$\langle 2$	1	3	0	0	1/	

• length n = 8, weight enumerator $1z^0 + 6z^4 + 48z^6 + 9z^8$, |Aut| = 1728, generator matrix

/1	1	1	1	1	1	0	$0 \rangle$
0	0	1	2	3	0	1	0
$\backslash 1$	2	3	3	3	0	0	1/

• length n = 9, weight enumerator $1z^0 + 36z^6 + 27z^8$, |Aut| = 1296, generator matrix

(1)	1	1	1	1	0	1	0	0)
0	1	1	3	3	1	0	1	0.
$\setminus 3$	2	3	0	2	2	0	0	1/

It can be easily checked that all $n \ge 5$ can be written as a non-negative integer linear combination of the numbers 5, 6, 7, 8, and 9. The non-existence for $n \in \{1, 2, 3, 4\}$ can e.g. be checked by exhaustive enumeration (since the maximum possible dimension is 4 for these lengths).

We remark that it is also not too hard to give purely theoretical non-existence proofs for $n \in \{1, 2, 3, 4\}$. As observed in Example 9 we can use Theorem 2 to exclude $n \in \{1, 3\}$. The non-existence for n = 2 follows e.g. from the classification result in Lemma 12. Profitable sources for projective divisible codes are projective two-weight codes, i.e. linear codes with just two non-zero weights, that very often come with relatively large divisibility constants. E.g. the codes of lengths 6 and 9 mentioned in the proof of Proposition 16 contain to the families TF1 and RT3, respectively, see [CK86]. Family TF1 from [CK86] spelled out in geometrical terms:

Lemma 17. For each integer $e \ge 1$ let $q := 2^e$ and \mathcal{M} by a hyperoval in PG(3-1,q). Then, we have $\#\mathcal{M} = q+2$, \mathcal{M} is 2-divisible, and all points have multiplicity at most 1.

Also our example for n = 8 generalizes to an infinite family by taking lines through a common point without the intersection point:

Lemma 18. Let $q = p^f$ and 1 < e < f be an integer. With this let P be a point and L_1, \ldots, L_{p^e} be pairwise different lines through P in PG(2,q). The point set \mathcal{M} is defined by $\mathcal{M}(Q) = 1$ iff $Q \neq P$ and there exists an index $1 \leq i \leq p^e$ with $Q \leq L_i$ and $\mathcal{M}(Q) = 0$ otherwise. Then, we have $\#\mathcal{M} = p^e q$ and \mathcal{M} is p^e -divisible.

n	9	10	12	13	14	15	16	17	18	19	20
#	1	1	1	1	1	3	7	8	20	35	91

Table 1: Number of non-isomorphic 2-divisible projective $[n, 3]_8$ -codes.

Whenever we have a construction for a Δ -divisible projective code over \mathbb{F}_q of length n such that we do not know such codes with smaller lengths n_1, n_2 satisfying $n = n_1 + n_2$, we speak of a "base example". So, for $\Delta = 2$ and q = 4 we have stated base examples for $n \in \{5, 6, 7, 8, 9\}$. For $\Delta = 2$ and q = 8 base examples are given by a line for n = 9, a hyperoval for n = 10, and one example for n = 16 constructed via Lemma 18. Besides that we have computationally found the following base examples:

• <i>n</i> = 12:	$\begin{pmatrix} 111111111100\\ 001234567010\\ 136547277001 \end{pmatrix}$
• <i>n</i> = 13:	$\begin{pmatrix} 1111111110100\\0225555661010\\3370237236001 \end{pmatrix}$
• <i>n</i> = 14:	$\begin{pmatrix} 1111111111100\\00111234567010\\26124752344001 \end{pmatrix}$
• <i>n</i> = 15:	$\begin{pmatrix} 111111111110100\\011223366771010\\656675667061001 \end{pmatrix}$
• <i>n</i> = 17:	$\begin{pmatrix} 11111111111110100\\00022335566771010\\23737032634461001 \end{pmatrix}$

The number of non-isomorphic 3-dimensional 2-divisible projective codes over \mathbb{F}_8 of length n are given in Table 1 for $n \leq 20$. For the underlying exhaustive enumeration we have again used LinCode [BBK21]. We also found 4-dimensional 2-divisible points over \mathbb{F}_8 of cardinalities 14, 16, 17, and 18. In principle we may computationally determine the possible lengths of 2-divisible projective codes over \mathbb{F}_8 by exhaustive enumeration. However, we will state a purely theoretical argument in Proposition 24 anyway, so that we refrain from stating the details.

In the following we state partial results for further divisibility constants Δ and field sizes q. "Base examples" for 4-divisible projective codes over \mathbb{F}_8 :

- n = 9: line
- n = 28: TF2 [CK86]
- n = 32: Lemma 18

"Base examples" for 2-divisible projective codes over \mathbb{F}_{16} :

- n = 17: line
- n = 18: hyperoval
- n = 32: Lemma 18
- n = 65: [ACG23, Section 4]

"Base examples" for 4-divisible projective codes over \mathbb{F}_{16} :

- n = 17: line
- n = 21: RT1 [CK86]
- n = 52: TF2 [CK86]
- n = 64: Lemma 18
- n = 65: RT3 [CK86]
- n = 221: TF2d [CK86]

"base examples" for 8-divisible projective codes over \mathbb{F}_{16} :

- n = 17: line
- n = 120: TF2 [CK86]
- n = 128: Lemma 18
- n = 153: TF2d [CK86]
- n = 257: TF3, RT2, CY1 [CK86]

"base examples" for 3-divisible projective codes over \mathbb{F}_9 :

- n = 10: line
- n = 13: Baer plane
- n = 24: $\begin{pmatrix} 111111111111111111111110100\\000011223344556677881010\\467801122523265824372001 \end{pmatrix}$

	(1111111111111111111111111110100)
• $n = 27$:	0000112233445566666677881010
	125628242438071345624474001

• n = 28: RT3 [CK86]; quasicyclic degree 4 linear code over \mathbb{F}_9 attaining the Griesmer bound

	(1111111111111111111111111111100100)
• $n = 31$:	0000011122233344455577788811010
	2467802514724612605827812514001

Note that there are no 3-divisible multisets of points over \mathbb{F}_9 with a cardinality in $\{1, 2, 4, 5, 7, 8, 11\}$.

In the remaining part of this section we consider 2-divisible (multi-)sets of points over \mathbb{F}_q .

Lemma 19. Let \mathcal{M} be a 2-divisible multiset of points in PG(v-1,q). If $q \equiv 1 \pmod{2}$, then there exists a multiset of points \mathcal{M}' in PG(v-1,q) such that $\mathcal{M} = 2\mathcal{M}'$, so that especially $\#\mathcal{M} \equiv 0 \pmod{2}$.

Proof. Since 2 does not divide q for $q \equiv 1 \pmod{2}$ the stated result is implied by [War81].

Lemma 20. Let \mathcal{M} be a 2-divisible multiset of points in PG(v-1,q). Then there exist s points P_1, \ldots, P_s and t 2-divisible sets of points B_1, \ldots, B_t such that $\mathcal{M} = \sum_{i=1}^s 2 \cdot \chi_{P_i} + \sum_{i=1}^t \chi_{B_i}$.

Proof. If Q is a point with multiplicity $\mathcal{M}(Q) \geq 2$, then $\mathcal{M} - 2 \cdot \chi_Q$ is also 2-divisible, so that we can assume that \mathcal{M} is a 2-divisible set of points after some points with multiplicity 2 have been removed.

A direct specialization of Lemma 12 is:

Lemma 21. Let \mathcal{M} be a 2-divisible multiset of points in PG(1,q) where q is even, then we have $\mathcal{M} = \sum_{i=1}^{s} 2 \cdot \chi_{P_i} + t \cdot \chi_L$ for some points P_1, \ldots, P_s (which may coincide) and the line L forming the ambient space.

We call a multiset \mathcal{M} in $\mathrm{PG}(v-1,q)$ spanning if the points with strictly positive multiplicity span the entire ambient space $\mathrm{PG}(v-1,q)$. For a multiset \mathcal{M} in V and a point Q in V the projection \mathcal{M}_Q is the multiset of points in V/Q with $\mathcal{M}_Q(L/Q) = \mathcal{M}(L) - \mathcal{M}(Q)$ for each line $L \geq Q$ in V. It can be easily verified that if \mathcal{M} is Δ -divisible, then \mathcal{M}_Q is Δ -divisible with cardinality $\#\mathcal{M} - \mathcal{M}(Q)$. The maximum point multiplicity may increase up to a factor of q. If \mathcal{M} is spanning, so is \mathcal{M}_Q .

Proposition 22. Let S be a 2-divisible set of points in PG(v - 1, q) for even field size q. Then we have $\#S \ge q + 1$. Moreover, if #S = q + 1, then S is the characteristic function of a line and if #S = q + 2, then S is the characteristic function of a hyperoval.

Proof. First we consider the case $\#S \equiv 1 \pmod{2}$ and denote by Q an arbitrary point with multiplicity 0. (If there is no point of multiplicity zero then we have $\#S = (q^v - 1)/(q - 1) \ge q + 1$ and in the case of equality S is the characteristic function of a line.) Since $\chi(Q) \not\equiv 1 \equiv \#S$ we have $v \ge 3$. If v = 3 then each of the q + 1 lines through Q has multiplicity at least 1, so that $\#S \ge q + 1$. In the case of equality each line L' that contains a point of multiplicity zero satisfies $\mathcal{M}(L') = 1$, so that the line L spanned by $2 \le q + 1$ points of multiplicity 1 contains q + 1 points of multiplicity 1, i.e., $S = \chi_L$. In the following we assume that S is spanning, $v \ge 4$, and $\#S \le q + 1$. Let L be a line with at least two points of multiplicity one and a point Q with multiplicity 0. Then, S_Q is a 2-divisible multiset with cardinality q + 1 and at least one point P of multiplicity at least two. By iteratively projecting through points of multiplicity zero we can assume that the ambient space of S_Q is three-dimensional. Setting $\mathcal{M} = S_Q - 2 \cdot \chi_P$ gives a 2-divisible multiset of points with cardinality $\le q - 1$ in PG(2, q). Iteratively removing double points yields a 2-divisible set S' of points with $\#S' \le q - 1$ and $\#S' \equiv 1 \pmod{2}$, which is impossible as we have seen before.

Next we consider the case $\#S \equiv 0 \pmod{2}$. Since v = 2 would imply $S(P) \equiv \#S \equiv 0 \pmod{2}$ and #S = 0, we can assume $v \ge 3$. If v = 3, then let P be a point of multiplicity 1. 2-divisibility implies that the q + 1 points through P have multiplicity at least 2, so that $\#S \ge q + 2$. In the case of equality each line

through P has multiplicity 2, i.e., the line multiplicities are contained in $\{0, 2\}$ and S is the characteristic function of a hyperoval. If $v \ge 4$ and S is spanning, then we consider a point Q of multiplicity 1, so that the projection S_Q through Q is a 2-divisible multiset of odd cardinality #S - 1. Thus, the previous part implies $\#S \ge q + 2$. In the case of equality we have $\#S_Q = q + 1$ and S_Q has to be the characteristic function of a line, which contradicts $v \ge 4$ for S spanning.

The 2-divisible sets over \mathbb{F}_2 with cardinality at most 14 have been computationally classified in [HHK⁺17]. A purely theoretical argumentation for cardinalities up to seven can e.g. be found in [KK23]. For q = 4 a 2-divisible set of q + 3 = 7 points exists in PG(2, 4), see family RT1 in [CK86]. With a little bit of effort one can show that this is the unique possibility of a 2-divisible set with cardinality 7.

Proposition 23. For even q > 4 no 2-divisible set S in PG(v-1,q) of cardinality q+3 exists.

Proof. Clearly we have $v \ge 3$. First we assume the case v = 3, so that all lines have odd multiplicity. If the support of S contains a line L, then $S - \chi_L$ would be a 2-divisible set of cardinality 2, which is impossible. If there is a line L with multiplicity at least 5, then L contains a point Q with multiplicity S(Q) = 0 and the projection S_Q would be 2-divisible and contains a point of multiplicity at least 4. Iteratively removing double points would yield a 2-divisible set of cardinality at most q - 1 which is impossible. Thus, all lines have multiplicity 1 or 3, so that the standard equations yield a contradiction if $q \neq 4$.

Proposition 22, Proposition 23, Lemma 20, and our stated base examples yield:

Proposition 24. A 2-divisible set $S \neq \emptyset$ of cardinality n over \mathbb{F}_8 exists iff and only if $n \in \{9, 10\} \cup \mathbb{N}_{>12}$.

A (q+t,t)-arc of type (0,2,t) in PG(2,q), also called KM-arc, see [KM90], is a set S of q+t points such that every line meets S in either 0, 2 or t points.

Proposition 25. Let S be a 2-divisible set in PG(v-1,q) of cardinality q+4. If q > 4 is even, then S is a KM-arc of type (0,2,4).

Proof. W.l.o.g. we assume that S is spanning. For an arbitrary point Q of multiplicity S(Q) = 1 consider the projection S_Q through Q, which is a 2-divisible multiset \mathcal{M} of cardinality q + 3. From Lemma 20, Proposition 22, and Proposition 23 we conclude $\mathcal{M} = \chi_L + 2 \cdot \chi_P$ for some line L and some point P. If $P \leq L$, then we have v = 3, so that we are in this situation for all points Q with multiplicity S(Q) = 1. Moreover the line multiplicities are contained in $\{0, 2, 4\}$, so that the statement holds.

Otherwise we have $P \not\leq L$ and this is the case for all points Q with multiplicity S(Q) = 1. Thus, we have v = 4 and the line multiplicities are contained in $\{0, 1, 2, 3\}$. Moreover, the preimage of L is a hyperplane H of cardinality q + 2 and the other two points outside of H form a line L meeting Q. (Actually, L is the unique 3-line for Q.) Now choose a 2-line L' in H that does not contain Q and a point $P' \neq Q$ on L with multiplicity S(P') = 1. Then, the hyperplane $H' := \langle P', L' \rangle$ has multiplicity 3, since all points with positive multiplicity are contained in either H or L – contradiction.

References

- [ACG23] Angela Aguglia, Bence Csajbók, and Luca Giuzzi. On regular sets of affine type in finite Desarguesian planes and related codes. *arXiv preprint 2305.17103*, 2023.
- [Adr23] Sam Adriaensen. A note on small weight codewords of projective geometric codes and on the smallest sets of even type. *arXiv preprint 2302.04718*, 2023.
- [BBK21] Iliya Bouyukliev, Stefka Bouyuklieva, and Sascha Kurz. Computer classification of linear codes. *IEEE Transactions on Information Theory*, 67(12):7807–7814, 2021.
- [CK86] Robert Calderbank and William M. Kantor. The geometry of two-weight codes. Bulletin of the London Mathematical Society, 18(2):97–122, 1986.

- [HH80] J.W.P. Hirschfeld and Xavier Hubaut. Sets of even type in PG(3, 4), alias the binary (85, 24) projective geometry code. *Journal of Combinatorial Theory, Series A*, 29(1):101–112, 1980.
- [HHK⁺17] 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: WCC Proceedings. IEEE Information Theory Society, Saint-Petersburg, September 2017. URL: https://eref.uni-bayreuth.de/40887/.
- [HKK18] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Partial spreads and vector space partitions. In *Network Coding and Subspace Designs*, pages 131–170. Springer, 2018.
- [HKK19] Thomas Honold, Michael Kiermaier, and Sascha Kurz. Johnson type bounds for mixed dimension subspace codes. *The Electronic Journal of Combinatorics*, 26(3), 2019.
- [KdR98] Jennifer D. Key and Marialuisa J. de Resmini. Small sets of even type and codewords. *Journal of Geometry*, 61:83–104, 1998.
- [KK20] Michael Kiermaier and Sascha Kurz. On the lengths of divisible codes. IEEE Transactions on Information Theory, 66(7):4051–4060, 2020.
- [KK23] Theresa Körner and Sascha Kurz. Lengths of divisible codes with restricted column multiplicities. arXiv preprint 2303.17172, 2023.
- [KM90] Gábor Korchmáros and Francesco Mazzocca. On (q + t)-arcs of type (0, 2, t) in a Desarguesian plane of order q. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 108, pages 445–459. Cambridge University Press, 1990.
- [Kur20] Sascha Kurz. No projective 16-divisible binary linear code of length 131 exists. *IEEE Commu*nications Letters, 25(1):38–40, 2020.
- [Kur21] Sascha Kurz. Divisible codes. arXiv preprint 2112.11763, 2021.
- [Kur22] Sascha Kurz. Vector space partitions of GF(2)⁸. Serdica Journal of Computing, 16(2):71–100, 2022.
- [Lim10] Jirapha Limbupasiriporn. Small sets of even type in finite projective planes of even order. Journal of Geometry, 98:139–149, 2010.
- [OP08] Darren C. Ong and Vadim Ponomarenko. The Frobenius number of geometric sequences. *Integers:* Electronic Journal of Combinatorial Number Theory, 8(1):A33, 2008.
- [She83] Brian Sherman. On sets with only odd secants in geometries over GF(4). Journal of the London Mathematical Society, 2(3):539–551, 1983.
- [Syl82] James J. Sylvester. On subvariants, ie semi-invariants to binary quantics of an unlimited order. American Journal of Mathematics, 5(1):79–136, 1882.
- [TM13] Taichiro Tanaka and Tatsuya Maruta. Classification of the odd sets in PG(4, 4) and its application to coding theory. Applicable Algebra in Engineering, Communication and Computing, 24(3-4):179–196, 2013.
- [War81] Harold N. Ward. Divisible codes. Archiv der Mathematik, 36(1):485–494, 1981.
- [War98] Harold N. Ward. Divisibility of codes meeting the Griesmer bound. Journal of Combinatorial Theory, Series A, 83(1):79–93, 1998.
- [War01] Harold Ward. Divisible codes a survey. Serdica Mathematical Journal, 27(4):263–278, 2001.
- [WS14] Zsuzsa Weiner and Tamás Szőnyi. On the stability of sets of even type. Advances in Mathematics, 267:381–394, 2014.