

A lower bound on the minimum weight of some geometric codes

Bence Csajbók*, Giovanni Longobardi, Giuseppe Marino, Rocco Trombetti

Abstract

The p -ary code associated with the incidence structure of points and t -spaces in a projective space $\text{PG}(m, q)$, where $q = p^h$, is the $\mathbb{F}_p$ -subspace generated by the incidence vectors of the blocks of this design. The dual of this code consists of all vectors orthogonal to every codeword of the original code. In contrast to the codes derived from point–subspace incidences, the minimum weight of the corresponding dual codes is generally unknown, which makes the problem more challenging.

In 2008 Lavrauw, Storme and Van de Voorde proved the following reduction: the minimum weight of the dual of the code derived from point and t -space incidences in $\text{PG}(m, q)$ is the same as the minimum weight of the dual of the code derived from point and line incidences in $\text{PG}(m - t + 1, q)$. After a series of works by Delsarte (1970), Assmus and Key (1992), Calkin, Key and De Resmini (1999), the best known lower bound for the case of point-line incidences was established in [B. Bagchi and P. Inamdar: Projective geometric codes, J. Combin. Theory Ser. A, 99(1) (2002), 128–142].

The problem of determining the minimum weight of these codes admits a natural geometric interpretation in terms of multisets of points in a projective space which meet each line in 0 modulo p points. In this paper, by adopting this geometrical perspective and exploiting certain polynomial techniques from [S. Ball, A. Blokhuis, A. Gács, P. Sziklai, Zs. Weiner: On linear codes whose weights and length have a common divisor, Adv. Math., 211 (2007), 94–104], we prove a substantial improvement of the Bagchi–Inamdar bound in the case where $h > 1$ and $m, p > 2$.

1 Introduction

Let Σ be either the projective space $\text{PG}(m, q)$, or the affine space $\text{AG}(m, q)$, where $q = p^h$ for some prime p and integer $h \geq 1$. Let $\mathcal{D}_\Sigma(m, q)$ be the design of points and lines of Σ , i.e. the $2 - (v, k, 1)$ design with

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = q + 1,$$

or

$$v = q^m, \quad k = q,$$

respectively. The p -ary code $\mathcal{C}_\Sigma(m, q)$ associated with $\mathcal{D}_\Sigma(m, q)$ is the $\mathbb{F}_p$ -subspace generated by the incidence vectors of the blocks of the corresponding design. The *dual* $\mathcal{C}^\perp$ of a code $\mathcal{C}$ is the $\mathbb{F}_p$ -subspace of vectors orthogonal to all vectors of $\mathcal{C}$ (under the standard inner product). The *weight* $w(\mathbf{v})$ of a vector $\mathbf{v} \in \mathbb{F}_q^v$ is the number of its non-zero coordinates w.r.t. the canonical basis of $\mathbb{F}_q^v$. The *minimum weight* of a code is the minimum of the weights of its non-zero elements. By Assmus

*This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and partially by the ELTE TKP 2021-NKTA-62 funding scheme.

and Key [2, Theorem 5.7.9], Calkin, Key and De Resmini [8, Proposition 1] and Delsarte [10], the lower bound

$$(q + p)q^{m-2} \quad (1)$$

was known for the minimum weight of both $\mathcal{C}_{\text{AG}}(m, q)^\perp$ and $\mathcal{C}_{\text{PG}}(m, q)^\perp$. This bound was improved in 2002 by Bagchi and Inamdar, see [3, Theorem 3], to

$$2 \left(\frac{q^m - 1}{q - 1} \left(1 - \frac{1}{p} \right) + \frac{1}{p} \right).$$

By [11, Theorems 10 and 11], the minimum weight codewords of the dual of the code arising from incidences between points and k -spaces of $\text{PG}(m, q)$ are the same as the minimum weight codewords of $\mathcal{C}_{\text{PG}}(m - k + 1, q)^\perp$. In [9, Corollary 1.5] De Boeck and Van de Voorde increased the lower bound on the minimum weight of $\mathcal{C}_{\text{PG}}(2, p^2)^\perp$, $p \geq 5$ prime, from $2q - 2p + 2$ to $2q - 2p + 5$.

If q is even, the lower bound in (1) is sharp; see [8, Corollary 1] by Calkin, Key and De Resmini. In fact, if q is even, then investigating the minimum weight of $\mathcal{C}_\Sigma(m, q)^\perp$ is equivalent to finding the minimum size of a non-empty point set S of Σ such that each line meets S in an even number of points. These are the so called sets of *even type*. The smallest sets of even type were characterised for $q = 2$ in [3, Proposition 3] and for $q \in \{4, 8\}$ in [1].

In the following, we recall the geometrical link between the codewords of $\mathcal{C}_\Sigma(m, q)^\perp$ and certain multisets of Σ . A *multiset* $\mathcal{M}$ of Σ is a pair $(\mathcal{S}, \mu)$ where

- (1) $\mathcal{S}$ a non empty set of points of Σ , and
- (2) $\mu: \mathcal{S} \rightarrow \mathbb{Z}^+$ a function that assigns a positive multiplicity to each element of $\mathcal{S}$.

If T is a subset of Σ , then $|T \cap \mathcal{M}| = \sum_{x \in T \cap \mathcal{S}} \mu(x)$. In particular, $|\mathcal{M}| = \sum_{x \in \mathcal{S}} \mu(x)$.

Let $\mathcal{P} = \{x_1, x_2, \dots, x_v\}$ be the point set of Σ , and consider $\mathcal{M} = (\mathcal{S}, \mu)$, a multiset of Σ . The vector $\mathbf{s} = (s_1, \dots, s_v)$, such that

$$s_i = \begin{cases} \mu(x_i) & \text{if } x_i \in \mathcal{S}, \\ 0 & \text{otherwise,} \end{cases} \quad i = 1, 2, \dots, v, \quad (2)$$

is called the *characteristic vector* of $\mathcal{M}$. Let $\sigma(\mathbf{s})$ be the sum of the coordinates of the characteristic vector $\mathbf{s}$, then $\sigma(\mathbf{s}) = |\mathcal{M}|$ and if $\mu(x) = 1$ for all $x \in \mathcal{S}$, then $\mathcal{M}$ is an ordinary set. Moreover, for an ordinary set, the weight $w(\mathbf{s})$ of its characteristic vector $\mathbf{s}$ is the same as the sum $\sigma(\mathbf{s})$ of the coordinates of $\mathbf{s}$.

Let $\mathcal{S}$ denote a non-empty point set of $\text{PG}(2, q)$ meeting each line of the plane in $0 \bmod r$ points. It follows from easy counting arguments that r has to be a power of p and hence lines meet $\mathcal{S}$ in $0 \bmod p$ points. It follows that the characteristic vector $\mathbf{s}$ of $\mathcal{S}$ is an element of $\mathcal{C}_{\text{PG}}(2, q)^\perp$. In [4, Theorem 2.1], Ball *et al.* proved a lower bound on the size of such point sets. In fact, they proved something more general: a lower bound for the size of non-empty point sets meeting each line in $0 \bmod p^s$ points. What we will cite here is their result in the $s = 1$ case, in terms of characteristic vectors.

Result 1.1. Suppose $\mathbf{s} \in \mathcal{C}_{\text{PG}}(2, q)^\perp$ and $q > p$. If $\mathbf{s}$ has only coordinates 0 and 1, then

$$w(\mathbf{s}) \geq (p - 1)(q + p). \quad (3)$$

This bound is sharp when $q = p^2$, or when $p = 2$, see [4, Example 4.4]. Result 1.1 was obtained by first proving it for $\mathbf{s} \in \mathcal{C}_{\text{AG}}(2, q)^\perp$. If $\mathcal{S}$ is an ordinary point set of $\text{PG}(2, q)$ of size less than $p(q + 1)$ and meeting each line in $0 \bmod p$ points, then there always exists a line disjoint from $\mathcal{S}$. The existence of such a line allows to transfer the problem from $\text{PG}(2, q)$ to $\text{AG}(2, q)$. We point out that

for a multiset $\mathcal{M}$ of $\text{PG}(m, q)$, $m \geq 3$, we cannot see how a similar restriction on $|\mathcal{M}|$ could ensure the existence of a hyperplane disjoint from $\mathcal{M}$.

From now on, a multiset of Σ intersecting each line in $0 \bmod p$ points will be called a $(0 \bmod p)$ -multiset. Note that $\mathcal{M}$ is a $(0 \bmod p)$ -multiset if and only if its characteristic vector $\mathbf{s} = (s_1, s_2, \dots, s_v)$ belongs to $\mathcal{C}_\Sigma^\perp(m, q)$. In Section 2, following the main ideas from [4, Theorem 2.1] we prove the following result.

Theorem 1.2. *Suppose $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$ and $q > p > 2$ with $m \geq 2$. If $\mathbf{s}$ has a coordinate equal to 1, then*

$$\sigma(\mathbf{s}) \geq (p-1)q^{m-1} + pq^{m-2}. \quad (4)$$

Clearly, if no coordinates in $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$ equals 1 and $\mathbf{s} \neq \mathbf{0}$ then by (1) it follows that

$$\sigma(\mathbf{s}) \geq 2q^{m-1} + 2pq^{m-2}. \quad (5)$$

In Section 3, we show that the lower bound stated in (4) is sharp for any $q > p$ and $m \geq 2$, by showing a family of examples attaining it. When $p = 2$, then our construction is the same as the recursive one presented by Calkin *et al.* in [8, Section 3] starting from a translation hyperoval of $\text{PG}(2, 2^h)$. Finally, using Theorem 1.2, in Section 4 we prove a significant improvement of the Bagchi–Inamdar bound in the case $h > 1$ and $m, p > 2$, obtaining:

$$2 \left(q^{m-1} \left(1 - \frac{1}{p} \right) + q^{m-2} \right).$$

We conclude the article with the investigation of $\sigma(\mathbf{s})$, with $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$, in characteristics 3 and 5.

2 On the size of an affine $(0 \bmod p)$ -multiset

Let $\mathcal{M} = (\mathcal{S}, \mu)$ be a multiset of Σ . Since we are interested in a lower bound on the size of multisets meeting lines in $0 \bmod p$ points, from now on we assume that the multiplicities of the points of $\mathcal{S}$ are between 1 and $p-1$. In fact, for each point $z \in \mathcal{S}$, put $\mu^*(z) = \mu(z) \bmod p$ (the residue of $\mu(z)$ modulo p), and let $\mathcal{S}^*$ denote the points of $\mathcal{S}$ with multiplicity not divisible by p . Then $\mathcal{M}^* = (\mathcal{S}^*, \mu^*)$ is a multiset of size (possibly) smaller than $\mathcal{M}$ and intersecting each line of Σ in $0 \bmod p$ points. Let us suppose that there exists at least one point $x \in \mathcal{S}$ such that $\mu(x) = 1$, then by counting the lines of Σ through x , we have

$$|\mathcal{M}| \geq 1 + (p-1) \frac{q^m - 1}{q - 1}. \quad (6)$$

In terms of multisets, Theorem 1.2 from Section 1 can be formulated as follows.

Theorem 2.1. *Let $\mathcal{M} = (\mathcal{S}, \mu)$ be a non-empty $(0 \bmod p)$ -type multiset of points in $\text{AG}(m, q)$, $m \geq 2$, $q = p^h$ with $p > 2$ and $h > 1$. If there is at least one point $x \in \mathcal{S}$ with $\mu(x) = 1$, then*

$$|\mathcal{M}| \geq (p-1)(q^{m-1} + q^{m-2}) + q^{m-2}. \quad (7)$$

Proof. Firstly, note that for $m = 2$, the lower bound in the statement coincides with that in (6). Hence, let us suppose $m > 3$. By counting points of $\mathcal{M}$ on lines incident with a fixed point not in $\mathcal{M}$, we obtain $p \mid |\mathcal{M}|$. We will use the same type of representation for $\text{AG}(m, q)$ as the one used in [4, Section 2] for $\text{AG}(2, q)$. In this way we can identify $\mathcal{M}$ with a multiset of $\mathbb{F}_{q^m}$. Define the polynomial

$$R(X, Y) = \prod_{b \in \mathcal{M}} (X + (Y - b)^{q-1}) = \sum_{j=0}^{|\mathcal{M}|} \sigma_j(Y) X^{|\mathcal{M}|-j}.$$

For $j < 0$ and $j > |\mathcal{M}|$ we define $\sigma_j(Y)$ to be the zero polynomial.

For $y \in \mathcal{M}$ with $\mu(y) = t$, it holds that

$$R(X, y) = X^t \left(X^{\frac{q^m-1}{q-1}} + (-1)^{m-1} \right)^{p-t} g_y(X)^p, \quad (8)$$

where the leading coefficient of $g_y(X)$ is 1. Whereas, if $y \notin \mathcal{M}$, then

$$R(X, y) = h_y(X)^p, \quad (9)$$

for some $h_y(X) \in \mathbb{F}_{q^m}[X]$. It means that for each $y \in \mathbb{F}_{q^m}$, if $0 < j < \frac{q^m-1}{q-1}$ and $p \nmid j$, then $\sigma_j(y) = 0$. Then for these j 's the polynomial $Y^{q^m} - Y$ divides $\sigma_j(Y)$, which is of degree at most $j(q-1) < q^m$, and hence $\sigma_j(Y)$ is the zero polynomial when $0 < j < \frac{q^m-1}{q-1}$ and $p \nmid j$. Then we may write

$$R(X, Y) = X^{|\mathcal{M}|} + \sigma_p(Y)X^{|\mathcal{M}|-p} + \sigma_{2p}(Y)X^{|\mathcal{M}|-2p} + \cdots + \sigma_{q^{m-1}+\dots+q}(Y)X^{|\mathcal{M}|-(q^{m-1}+\dots+q)} + \sum_{j=\frac{q^m-1}{q-1}}^{|\mathcal{M}|} \sigma_j(Y)X^{|\mathcal{M}|-j}. \quad (10)$$

The partial derivative of $R(X, Y)$ with respect to Y , evaluated in $y \in \mathbb{F}_{q^m}$, is

$$\frac{\partial R}{\partial Y}(X, y) = \left(\sum_{b \in \mathcal{M}} \frac{-(y-b)^{q-2}}{X + (y-b)^{q-1}} \right) R(X, y).$$

Since the above denominators are all divisors of $X^{\frac{q^m-1}{q-1}} + (-1)^{m-1}$, we obtain

$$R(X, y)G_y(X) = (X^{\frac{q^m-1}{q-1}} + (-1)^{m-1}) \frac{\partial R}{\partial Y}(X, y) \quad (11)$$

for some polynomial $G_y(X) \in \mathbb{F}_{q^m}[X]$, depending on y , whose degree is at most $\frac{q^m-1}{q-1} - p$.

Next, we prove some properties of the polynomial $G_y(X)$.

Note that at the right-hand side of (11) the highest degree, which is not 1 mod p , is at most $|\mathcal{M}|$. Assume $y \notin \mathcal{M}$, if there was a non-constant term in $G_y(X)$ of degree not 1 mod p then there would be a term on the left-hand side of (11) of degree larger than $|\mathcal{M}|$ and of degree not 1 mod p (cf. (9)). This would be a contradiction, which proves that

$$G_y(X) = c_y + XH_y(X)^p$$

for some polynomial $H_y(X) \in \mathbb{F}_{q^m}[X]$. To find the constant $c_y \in \mathbb{F}_{q^m}$, we compare the coefficients of $X^{|\mathcal{M}|}$ with (11). It follows that

$$c_y = \sigma'_{\frac{q^m-1}{q-1}}(y).$$

Next, we prove some properties of the σ_j 's. For each i such that $|\mathcal{M}| - i$ is not congruent to 0 or 1 modulo p (i.e., i is not congruent to 0 or -1 modulo p) and $y \notin \mathcal{M}$, on the left-hand side of (11) the coefficients of terms of degree $|\mathcal{M}| - i$ are equal to zero.

For each $y \in \mathbb{F}_{q^m}$, on the right-hand side of (11) the coefficient of $X^{|\mathcal{M}|-i}$ is

$$(-1)^{m-1} \sigma'_i(y) + \sigma'_{i+(q^m-1)/(q-1)}(y). \quad (12)$$

We can put

$$|\mathcal{M}| = (p-1)(q^{m-1} + q^{m-2}) + kp \geq 1 + (p-1)\frac{q^m-1}{q-1}.$$

Clearly, $kp > 0$. To obtain a contradiction, from now on we assume $kp < q^{m-2}$. Then

$$(p-1)\frac{q^m-1}{q-1} + kp > |\mathcal{M}|, \quad (13)$$

and hence $\sigma_{(p-1)\frac{q^m-1}{q-1}+kp}(Y)$ is the zero polynomial by definition. Since $(p-2)\frac{q^m-1}{q-1} + kp$ is not congruent to 0 or -1 modulo p , on the left-hand side of (11) the coefficient of $X^{|\mathcal{M}|-(p-2)\frac{q^m-1}{q-1}+kp}$ is equal to 0 and hence by (12):

$$\sigma'_{(p-2)\frac{q^m-1}{q-1}+kp}(y) = (-1)^m \sigma'_{(p-1)\frac{q^m-1}{q-1}+kp}(y).$$

Here, the right-hand side – and hence also the left-hand side – are equal to zero. Iterating the same argument, we obtain $\sigma'_{(p-\ell)\frac{q^m-1}{q-1}+kp}(y) = 0$, for any $\ell \in \{1, \dots, p-1\}$, in particular

$$\sigma'_{\frac{q^m-1}{q-1}+kp}(y) = 0.$$

It follows that $(-1)^{m-1}\sigma'_{kp}(y)$ is the coefficient of $X^{|\mathcal{M}|-kp}$ on the right-hand side of (11). At the left-hand side, this coefficient is $\sigma_{kp}(y)c_y = \sigma_{kp}(y)\sigma'_{(q^m-1)/(q-1)}(y)$ and hence

$$\sigma_{kp}(y)\sigma'_{\frac{q^m-1}{q-1}}(y) = (-1)^{m-1}\sigma'_{kp}(y) \quad (14)$$

for each $y \notin \mathcal{M}$. Now we examine $\sigma_{\frac{q^m-1}{q-1}}(Y)$. If $y \notin \mathcal{M}$ then $\sigma_{\frac{q^m-1}{q-1}}(y) = 0$ (cf. (9)) and hence the degree of $\sigma_{\frac{q^m-1}{q-1}}(Y)$ is at least $q^m - |\mathcal{M}|$, or it is the zero polynomial. If $y \in \mathcal{M}$ with multiplicity $1 \leq t \leq p-1$, then $\sigma_{\frac{q^m-1}{q-1}}(y) = (p-t)(-1)^{m-1} = (-1)^mt$ (cf. (8)), in particular $\sigma_{\frac{q^m-1}{q-1}}(Y)$ is not the zero polynomial.

Put $f(Y) = \prod_{y \in \mathcal{M}}(Y - y)$. Then $f(Y)\sigma_{\frac{q^m-1}{q-1}}(Y)$ is zero for each $y \in \mathbb{F}_{q^m}$, hence, we may put it in the following form:

$$f(Y)\sigma_{\frac{q^m-1}{q-1}}(Y) = (Y^{q^m} - Y)T(Y). \quad (15)$$

Moreover, the degree of $f(Y)\sigma_{\frac{q^m-1}{q-1}}(Y)$ is at most $|\mathcal{M}| + q^m - 1$. This implies that $T(Y)$ has degree at most $|\mathcal{M}| - 1$. For each $y \in \mathcal{M}$, if $\mu(y) = t$, then, after the derivation of (15)

$$(-1)^{m-1}tf'(y) = T(y).$$

If $t = 1$, then $(-1)^{m-1}f'(y) = T(y)$, while if $t > 1$, y is a multiple root of $f(Y)$ and hence $f'(y) = 0$, thus $T(y) = (-1)^{m-1}tf'(y) = 0$. Therefore,

$$(-1)^{m-1}f'(y) = T(y)$$

holds for each $y \in \mathcal{M}$ and since $|\mathcal{M}|$ is larger than the degree of $((-1)^{m-1}f' - T)(Y)$, it follows that $(-1)^{m-1}f'(Y) = T(Y)$.

Again, after derivating (15), substituting $y \notin \mathcal{M}$ and applying $\sigma_{\frac{q^m-1}{q-1}}(y) = 0$, we obtain

$$f(y)\sigma'_{\frac{q^m-1}{q-1}}(y) = -T(y) = (-1)^mf'(y).$$

Then, combined with (14), we obtain

$$\sigma_{kp}(y)f'(y) = -\sigma'_{kp}(y)f(y)$$

and hence $(f\sigma_{kp})'(y) = 0$, for each $y \notin \mathcal{M}$. Since the degree of $(f\sigma_{kp})(Y)$ is at most $kp(q-1) + |\mathcal{M}|$, which is divisible by p , the polynomial $(f\sigma_{kp})'$ has the degree at most $kp(q-1) + |\mathcal{M}| - 2$. In order

for $(f\sigma_{kp})'$ to be the zero polynomial, we need this degree to be less than $q^m - |\mathcal{M}|$. Equivalently, we need

$$kp(q-1) + 2|\mathcal{M}| - 2 < q^m,$$

which certainly holds when

$$kp(q-1) + 2\left((p-1)\frac{q^m-1}{q-1} + kp - 1\right) - 2 < q^m.$$

This in turn certainly holds when $kp \leq q^{m-2}(q-2p)$. In summary, if $|\mathcal{M}| < (p-1)\frac{q^m-1}{q-1} + q^{m-2}(q-2p)$, then $(f\sigma_{kp})'$ is the zero polynomial. Since the lower bound in the statement for $|\mathcal{M}|$ is smaller than this number, we may indeed assume for the rest of the proof that $(f\sigma_{kp})'$ is the zero polynomial. This means that $(f\sigma_{kp})(Y)$ is a p -th power of a polynomial in $\mathbb{F}_{q^m}[Y]$, and hence $f(Y)$ divides $\sigma_{kp}(Y)^{p-1}$. Indeed, f is product of linear factors, each of them with multiplicity at most $p-1$. Assume $(Y-c) \mid f(Y)$ for some c . Then c is at least p -fold root of $f\sigma_{kp}$, so it is also a root of σ_{kp} . Hence, $(Y-c)^{p-1} \mid \sigma_{kp}(Y)^{p-1}$. Since this holds for each root c of f , $f(Y) \mid \sigma_{kp}(Y)^{p-1}$.

Moreover, by definition, f is a product of linear factors over $\mathbb{F}_{q^m}$, each of them with multiplicity at most $p-1$. It follows that either $\deg f \leq (p-1)\deg \sigma_{kp}$, and hence $|\mathcal{M}| \leq kp(p-1)(q-1)$, or σ_{kp} is the zero polynomial.

Recall $kp < q^{m-2}$, and hence

$$|\mathcal{M}| = (p-1)(q^{m-1} + q^{m-2}) + kp > kp(p-1)(q-1),$$

i.e. $\deg f > (p-1)\deg \sigma_{kp}$ and hence σ_{kp} is the zero polynomial. Note that the coefficient of the term $X^{(p-1)(q^{m-1}+q^{m-2})}Y^{kp(q-1)}$ in $R(X, Y)$ is $\binom{|\mathcal{M}|}{kp}$. According to Lucas' theorem, recall $kp < q^{m-2}$, $\binom{|\mathcal{M}|}{kp} = 1$ and hence it is a non-zero term which appears also in σ_{kp} , a contradiction.

Since the assumption $kp < q^{m-2}$ led to a contradiction, the assertion follows. $\square$

Theorem 2.1 assumes $p > 2$, while the analogous question for $p = 2$ asks for the minimum size of a non-empty (ordinary) point set $\mathcal{S}$ in $\text{AG}(m, q)$ such that lines meet $\mathcal{S}$ in $0 \pmod p$ points. The sharp lower bound for the size of such point sets is given in (1), and it coincides with the value that (7) yields when $p = 2$.

We conclude this section by noting that if $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$, then we can extend $\mathbf{s}$ with $(q^m-1)/(q-1)$ zeroes (corresponding to points of the hyperplane at infinity) to obtain a codeword $\bar{\mathbf{s}}$ in $\mathcal{C}_{\text{PG}}(m, q)^\perp$. Clearly, $w(\bar{\mathbf{s}}) = w(\mathbf{s})$ and $\sigma(\bar{\mathbf{s}}) = \sigma(\mathbf{s})$; hence, the minimum weight of $\mathcal{C}_{\text{AG}}(m, q)^\perp$ is at least the minimum weight of $\mathcal{C}_{\text{PG}}(m, q)^\perp$.

3 Examples attaining the lower bound

This subsection is devoted to the construction of a family of multisets in $\text{AG}(m, q)$ that contains at least one point of multiplicity 1, such that every affine line intersects the multiset in a number of points divisible by p , and whose size attains the bound given in (7).

Let V denote the $(m+1)$ -dimensional $\mathbb{F}_q$ -vector space underlying $\Sigma = \text{PG}(m, q)$. If $q = p^h$, then we can view V as an $h(m+1)$ -dimensional $\mathbb{F}_p$ -vector space. If W is an r -dimensional $\mathbb{F}_p$ -subspace of V , then the set of points L_W of Σ defined by non zero vectors of W is called an $\mathbb{F}_p$ -linear set of rank r . It is straightforward to see that $|L_W| \leq \frac{p^r-1}{p-1}$. Lines of Σ correspond to sets of points defined by non-zero vectors of 2-dimensional $\mathbb{F}_q$ -subspaces of V , which can be viewed as $2h$ -dimensional $\mathbb{F}_p$ -subspaces. By Grassmann's Identity, if U is an $(h(m-1)+1)$ -dimensional $\mathbb{F}_p$ -subspace of V , then it meets every 2-dimensional $\mathbb{F}_q$ -subspace non-trivially. If T is any 2-dimensional $\mathbb{F}_q$ -subspace and ℓ is the line of Σ defined by non zero vectors of T , then it follows that $\ell \cap L_U \neq \emptyset$. Moreover, it can be seen that $|\ell \cap L_U| \equiv 1 \pmod p$, see [7] and [15, Proposition 2.2].

The subsequent results are crucial for achieving our goal.

Proposition 3.1. Let L_U and L_W be any two $\mathbb{F}_p$ -linear sets of rank $h(m-1)+1$ in $\text{PG}(m, q)$, $q = p^h$, $h > 1$. Put $\mathcal{S} = L_U \triangle L_W$ (the symmetric difference of L_U and L_W) and define μ as follows:

$$\mu(x) = \begin{cases} t & \text{if } x \in L_U \setminus L_W \\ p-t & \text{if } x \in L_W \setminus L_U, \end{cases} \quad (16)$$

where $1 \leq t \leq p-1$ is fixed. Then $\mathcal{M} = (\mathcal{S}, \mu)$ is a multiset meeting each line of $\text{PG}(m, q)$ in $0 \pmod p$ points.

Proof. Let ℓ be any line of $\text{PG}(m, q)$ and put $a = |\ell \cap (L_U \setminus L_W)|$, $b = |\ell \cap (L_U \cap L_W)|$ and $c = |\ell \cap (L_W \setminus L_U)|$. From above it holds that $a + b \equiv 1 \equiv b + c \pmod p$. Moreover, we also have the following:

$$|\mathcal{M} \cap \ell| = ta + (p-t)c \equiv 0 \pmod p.$$

□

An $\mathbb{F}_p$ -subspace U of $H \cong \mathbb{F}_q^m$ is said to be an $(u, v)_p$ -evasive subspace if the $\mathbb{F}_q$ -subspace $\langle U \rangle_{\mathbb{F}_q}$ has dimension at least u over $\mathbb{F}_q$ and the u -dimensional $\mathbb{F}_q$ -subspaces of H meet U in $\mathbb{F}_p$ -subspaces of dimension at most v . For more details see [5]. We will need the following result on $(m-1, (m-2)h)_p$ -evasive subspaces:

Result 3.2 ([5, Special case of Corollary 4.4]). Let U be an $\mathbb{F}_p$ -subspace of $H \cong \mathbb{F}_q^m$, $q = p^h$, and assume that U meets every $(m-1)$ -dimensional $\mathbb{F}_q$ -subspace of H in an $\mathbb{F}_p$ -subspaces of dimension at most $(m-2)h$. Then $\dim_p(U) \leq (m-1)h-1$.

Proposition 3.3. Let $f: \mathbb{F}_q^{m-1} \rightarrow \mathbb{F}_q$ be an $\mathbb{F}_p$ -multilinear map, $m \geq 2$. In $V = \mathbb{F}_q^{m+1}$ put

$$U = \{(x_0, x_1, \dots, x_{m-2}, f(x_0, x_1, \dots, x_{m-2}), y) : x_0, x_1, \dots, x_{m-2} \in \mathbb{F}_q, y \in \mathbb{F}_p\}, \quad (17)$$

$$W = \{(x_0, x_1, \dots, x_{m-2}, y, 0) : x_0, x_1, \dots, x_{m-2} \in \mathbb{F}_q, y \in \mathbb{F}_p\}. \quad (18)$$

Define $\mathcal{M} = (L_U \triangle L_W, \mu)$, a multiset of $\text{PG}(m, q)$, with μ as in Proposition 3.1 with $t = 1$.

(1) There is a hyperplane disjoint from $\mathcal{M}$.

(2) $\mathcal{M}$ is of size

$$(p-1)(q^{m-1} + q^{m-2}) + q^{m-2}$$

if and only if

$$|L_U \cap L_W| = q^{m-2} \frac{q-1}{p-1} + \frac{q^{m-2}-1}{q-1}.$$

Proof. (1) First, observe that $L_W = \text{PG}(H, \mathbb{F}_q)$ where H is an m -dimensional $\mathbb{F}_q$ -vector space. Hence, $L_U \cap L_W = L_{U \cap H}$ is an $\mathbb{F}_p$ -linear set of rank $(m-1)h$. By Grassmann's Identity, $L_{U \cap H}$ meets hyperplanes of L_W in linear sets of rank at least $(m-2)h$. By Result 3.2, it follows that $L_{U \cap H}$ cannot meet every hyperplane of L_W in an $\mathbb{F}_p$ -linear set of rank exactly $(m-2)h$. Hence, $L_{U \cap H}$ meets at least a hyperplane, say Π of L_W , in an $\mathbb{F}_p$ -linear set of rank at least $(m-2)h+1$. Then, again by Grassmann's Identity, Π must be fully contained in $L_{U \cap H}$. To prove (1), it is enough to find a hyperplane of $\text{PG}(m, q)$ through Π which does not meet $\mathcal{M}$. Assume for the contrary, that each hyperplane $\mathcal{H}$ of $\text{PG}(m, q)$ through Π and distinct from $L_W: X_m = 0$ meets $\mathcal{M}$. Since $\mathcal{M} \cap \mathcal{H}$ is a multiset of $\mathcal{H} \setminus \Pi \cong \text{AG}(m-1, q)$ meeting every line in $0 \pmod p$ points and having only points of multiplicity 1, by applying Theorem 2.1, we have that

$$q^{m-1} = |L_U \setminus L_W| = \sum_{\substack{\Pi \subset \mathcal{H} \\ \mathcal{H} \neq L_W}} |\mathcal{M} \cap \mathcal{H}| \geq q((p-1)(q^{m-2} + q^{m-3}) + q^{m-3}),$$

a contradiction.

To prove (2), it is enough to note that, by construction,

$$|\mathcal{M}| = (p-1)|L_W \setminus (L_U \cap L_W)| + |L_U \setminus L_W|$$

and $|L_U \setminus L_W| = q^{m-1}$. □

By Proposition 3.3, we can get an upper bound on the size of an $\mathbb{F}_p$ -linear set of rank hm in $\text{PG}(m, q)$, $m \geq 2$, $q = p^h$, and $h > 1$. Indeed, the following holds.

Theorem 3.4. *Let L be a $\mathbb{F}_p$ -linear set of rank hm in $\text{PG}(m, q)$, $q = p^h$. Then,*

$$|L| \leq q^{m-1} \frac{q-1}{p-1} + \frac{q^{m-1}-1}{q-1}.$$

Proof. After a suitable collineation, for any $\mathbb{F}_p$ -linear set L of rank hm in $\text{PG}(m, q)$ we may assume that $(0 : 0 : \dots : 0 : 1) \notin L$ and hence L can be written as $L = L_U$, where

$$U = \{(x_0, x_1, \dots, x_{m-1}, f(x_0, \dots, x_{m-1})) : x_i \in \mathbb{F}_{q^m}\}$$

U is an $\mathbb{F}_p$ -subspace of dimension hm , and hence $f : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$ is additive. Let us consider the $\mathbb{F}_p$ -linear sets $L_{\overline{U}}$ and $L_{\overline{W}}$ of $\text{PG}(m+1, q)$, where

$$\overline{U} = \{(x_0, x_1, \dots, x_{m-1}, f(x_0, \dots, x_{m-1}), y) : x_0, \dots, x_{m-1} \in \mathbb{F}_q, y \in \mathbb{F}_p\},$$

$$\overline{W} = \{(x_0, x_1, \dots, x_{m-1}, y, 0) : x_0, \dots, x_{m-1} \in \mathbb{F}_q, y \in \mathbb{F}_p\}.$$

Then, by Proposition 3.1 with $t = 1$, the multiset $\overline{\mathcal{M}} = (L_{\overline{U}} \triangle L_{\overline{W}}, \mu)$ with μ as in (16) meets any line of $\text{PG}(m+1, q)$ in $0 \pmod p$ points. By Proposition 3.3 (2),

$$|L_U| = |L_{\overline{U}} \cap L_{\overline{W}}| \leq q^{m-1} \frac{q-1}{p-1} + \frac{q^{m-1}-1}{q-1},$$

hence the result follows. □

The trivial upper bound for the size of an $\mathbb{F}_p$ -linear set of rank hm in $\text{PG}(m, q)$, $q = p^h$, is $\frac{p^{hm}-1}{p-1} = \frac{q^m-1}{p-1}$. It is easy to see that our bound is stronger, indeed $\frac{q^m-1}{p-1} > q^{m-1} \frac{q-1}{p-1} + \frac{q^{m-1}-1}{q-1}$ follows from

$$(q-1)(q^m-1) - (q^{m-1}(q-1)^2 + (q^{m-1}-1)(p-1)) = (q-p)(q^{m-1}-1) > 0.$$

In the remainder, we apply Propositions 3.1 and 3.3 to show that in $\text{AG}(m, q)$ there exist $(0 \pmod p)$ -multisets having at least one point with multiplicity 1, with size $(p-1)(q^{m-1} + q^{m-2}) + q^{m-2}$.

To this aim we first recall that an $\mathbb{F}_p$ -linearized polynomial $f(x) = \sum_{i=0}^{r-1} a_i x^{p^i} \in \mathbb{F}_q[x]$ is called *scattered* if

$$\left| \left\{ \frac{f(x)}{x} : x \in \mathbb{F}_q^* \right\} \right| = \frac{q-1}{p-1},$$

for a survey on scattered polynomials, see [13].

Now, assume $L_U \subset \text{PG}(m, q)$ to be an $\mathbb{F}_p$ -linear set whose underlying $\mathbb{F}_p$ -vector space is

$$U = \{(x_0, x_1, \dots, x_{m-2}, f(x_0), y) : x_0, x_1, \dots, x_{m-2} \in \mathbb{F}_q, y \in \mathbb{F}_p\},$$

where f is any scattered $\mathbb{F}_p$ -linearized polynomial. Also, consider the $\mathbb{F}_p$ -subspace W of $\mathbb{F}_q^{m+1}$ as in (18). It is easy to see that $L_U \cap L_W$ is an $\mathbb{F}_p$ -linear set contained in the hyperplane of $\text{PG}(m, q)$ with equation $X_m = 0$ and it is a cone with basis a maximum scattered $\mathbb{F}_p$ -linear set on the line

with equations $X_1 = X_2 = \dots = X_{m-2} = X_m = 0$ and vertex an $(m-3)$ -dimensional subspace with equations $X_0 = X_{m-1} = X_m = 0$. Then,

$$|L_U \cap L_W| = q^{m-2} \frac{q-1}{p-1} + \frac{q^{m-2}-1}{q-1},$$

and $\mathcal{M} = (L_U \triangle L_W, \mu)$ as defined in (16) is a multiset of $\text{AG}(m, q)$ whose size attains the bound in (7). The fact that this construction can be embedded in $\text{AG}(m, q)$ follows from Proposition 3.3 (1).

We note that the characteristic vector of the construction above has the same weight as the one associated with the point set constructed by Lavrauw, Storme and Van de Voorde in [12, Theorem 4.14]. In particular, if $f(X) = X^p$, then our construction has the same support as the one in [12, Theorem 4.14]. Moreover, if $p = 2$ the example falls into the family exhibited by Calkin, Key and De Resmini in [8]. Indeed, in such a case L_U is equivalent to a cone with base the $\mathbb{F}_2$ -linear set $\{\langle (x, x^{2^s}) \rangle_{\mathbb{F}_{2^h}} : x \in \mathbb{F}_{2^h}^*\} \subseteq \text{PG}(1, 2^h)$, with $\gcd(s, h) = 1$, which is the set of directions determined by the points of a translation hyperoval of $\text{PG}(2, 2^h)$ (see [14]). In such a case, our construction provides a set which is equivalent to the one constructed by induction in [8, Note 1].

4 A lower bound on the minimum weight of $\mathcal{C}_{\text{PG}}(m, q)^\perp$

In this section, we will show a new lower bound for the minimum weight of a codeword $\mathbf{s}$ of $\mathcal{C}_{\text{PG}}(m, q)^\perp$ and for the minimum size of $(0 \bmod p)$ -multisets of $\text{PG}(m, q)$. Firstly, we extend of [8, Proposition 1] to multisets.

Lemma 4.1. *Let w_{m-1} denote the minimum weight of the code $\mathcal{C}_{\text{PG}}^\perp(m-1, q)$ and let σ_{m-1} denote the minimum size of a non-empty $(0 \bmod p)$ -multiset in $\text{PG}(m-1, q)$, $q = p^h$. If $\mathcal{M} = (\mathcal{S}, \mu)$ is a $(0 \bmod p)$ -multiset of $\text{PG}(m, q)$ which meets every hyperplane, then*

$$|\mathcal{S}| \geq qw_{m-1} \quad \text{and} \quad |\mathcal{M}| \geq q\sigma_{m-1}.$$

Proof. Let $\mathcal{M} = (\mathcal{S}, \mu)$ be a $(0 \bmod p)$ -multiset of $\text{PG}(m, q)$ such that the hyperplanes of $\text{PG}(m, q)$ meet $\mathcal{S}$ in $0 < n_1 < n_2 < \dots < n_k$ points, and there are z_i hyperplanes meeting $\mathcal{S}$ in n_i points. Clearly

$$z_1 + z_2 + \dots + z_k = \frac{q^{m+1} - 1}{q - 1}. \quad (19)$$

By double counting the pairs $(x, \mathcal{H})$ where $x \in \mathcal{S}$ and $\mathcal{H}$ is a hyperplane incident with x , we obtain:

$$n_1 z_1 + n_2 z_2 + \dots + n_k z_k = |\mathcal{S}| \frac{q^m - 1}{q - 1}. \quad (20)$$

Multiplying (19) by n_1 and subtracting (20) we get

$$|\mathcal{S}| \geq n_1 \frac{q^{m+1} - 1}{q^m - 1} \geq n_1 q.$$

Since n_1 is at least w_{m-1} the first part of the statement is proved. To prove the second part, assume that hyperplanes meet $\mathcal{M}$ in $0 < n_1 < \dots < n_k$ points (counting the points with their multiplicities) and that there are z_i hyperplanes meeting $\mathcal{M}$ in n_i points. Clearly (19) holds and by double counting the $(x, \mathcal{H})$ pairs (counting each of them $\mu(x)$ times), we obtain (20) with $|\mathcal{M}|$ on its right side (instead of $|\mathcal{S}|$). Similarly to the arguments from above, now we obtain $|\mathcal{M}| \geq n_1 q$ and the result follows noting that $n_1 \geq \sigma_{m-1}$. $\square$

We will need the following triviality.

Proposition 4.2. *The minimum weight w_1 of $\mathcal{C}_{\text{PG}}(1, q)^\perp$, $q = p^h$, is 2 and*

$$\sigma_1 = \min \{ \sigma(\mathbf{s}) : \mathbf{s} \in \mathcal{C}_{\text{PG}}(1, q)^\perp \setminus \{\mathbf{0}\} \} = p.$$

In the next proof we will need the following definition.

Definition 4.3. *For a multiset $\mathcal{M} = (\mathcal{S}, \mu)$ of Σ we define $(p-1)\mathcal{M}$ as the multiset $(\mathcal{S}, \bar{\mu})$ of Σ , where for each $x \in \mathcal{S}$, $\bar{\mu}(x) \in \{1, 2, \dots, p-1\}$ such that $\bar{\mu}(x) \equiv (p-1)\mu(x) \pmod{p}$.*

Theorem 4.4. *If $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ and $q > p$, then*

$$w(\mathbf{s}) \geq 2(q^{m-1}(p-1)/p + q^{m-2}).$$

Proof. First, take a codeword $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$ and let $\mathcal{M}$ be the multiset associated with $\mathbf{s}$. Scaling the codeword $\mathbf{s}$ does not alter its weight. Thus we may assume the existence of a point $x \in \mathcal{M}$ with multiplicity 1. If there are no points with multiplicity $p-1$, then counting the points on lines through x gives

$$w(\mathbf{s}) \geq 1 + 2(q^{m-1} + q^{m-2} + \dots + q + 1),$$

and hence the assertion follows. If there is a point with multiplicity $p-1$, the multiset $(p-1)\mathcal{M}$ has a point of multiplicity 1. Since $|\mathcal{M}| + |(p-1)\mathcal{M}|$ is p times the weight of $\mathbf{s}$, by (4) (applied twice) we obtain

$$2((p-1)q^{m-1} + pq^{m-2}) \leq |\mathcal{M}| + |(p-1)\mathcal{M}| = pw(\mathbf{s}), \quad (21)$$

from which the result follows. For the origin of the trick applied in (21) see [1, Result 3.2 and Remark 3.4].

Now, let us assume $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ and let $\mathcal{M} = (\mathcal{S}, \mu)$ be the multiset associated with it. If there is a hyperplane of $\text{PG}(m, q)$ disjoint from $\mathcal{M}$, the result follows from the first part of the proof. Now, suppose that each hyperplane of $\text{PG}(m, q)$ meets $\mathcal{M}$ and hence $\mathcal{S}$. Take first $m = 2$. Then, by Lemma 4.1 and Proposition 4.2,

$$w(\mathbf{s}) = |\mathcal{S}| \geq 2q \geq 2(q(p-1)/p + 1),$$

as required. Now suppose that $m > 2$ and, by the induction hypothesis, assume that the weight w_{m-1} of each non-zero codeword of $\mathcal{C}_{\text{PG}}^\perp(m-1, q)$ is at least $2(q^{m-2}(p-1)/p + q^{m-3})$. Thus, by Lemma 4.1

$$w(\mathbf{s}) = |\mathcal{S}| \geq qw_{m-1} \geq 2(q^{m-1}(p-1)/p + q^{m-2}),$$

which completes the proof. $\square$

Let $\mathcal{C}_{\text{PG}}^{(k)}(m, q)$ be the p -ary code associated with the design $\mathcal{D}_{\text{PG}}^{(k)}(m, q)$ of points and k -spaces of $\text{PG}(m, q)$, i.e. the $\mathbb{F}_p$ -subspace generated by the incidence vectors of the blocks of the corresponding design. As said before, the minimum weight of $\mathcal{C}_{\text{PG}}^{(k)}(m, q)^\perp$ is equal to the minimum weight of $\mathcal{C}_{\text{PG}}(m-k+1)^\perp$, see [11, Theorem 10]. Then, as a corollary of Theorem 4.4, we get the following result.

Corollary 4.5. *If $\mathbf{s} \in \mathcal{C}_{\text{PG}}^{(k)}(m, q)$ and $q > p$, then*

$$w(\mathbf{s}) \geq 2(q^{m-k}(p-1)/p + q^{m-k-1}).$$

We remark that Corollary 4.5 improves the bounds proved in [11, Theorems 14 and 15].

In the next propositions we will frequently use $\lambda\mathbf{s}$, where $\mathbf{s} = (s_1, \dots, s_n)$ is a vector with coordinates in $\mathbb{F}_p$ and λ is an integer. Of course, the i -th coordinate of $\lambda\mathbf{s}$ is defined to be the unique element of $\{0, 1, \dots, p-1\}$ congruent to λs_i modulo p .

Proposition 4.6. *Let $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ with $q = p^h$, $h > 1$ and p an odd prime power. Let $1 \leq t \leq \frac{p-1}{2}$. If the non-zero coordinates of $\mathbf{s}$ are equal to t or $p-t$, then*

$$\sigma(\mathbf{s}) \geq (p-1)(q^{m-1} + q^{m-2}) + q^{m-2}.$$

Proof. Firstly, we prove the result for a codeword in $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$. Let us suppose that $\mathbf{s}$ has all non-zero coordinates equal to $t > 1$. Let λ be an integer such that $\lambda t \equiv 1 \pmod{p}$, then $\sigma(\mathbf{s}) \geq \sigma(\lambda \mathbf{s}) \geq (p-1)(q^{m-1} + q^{m-2}) + q^{m-2}$ (by Theorem 1.2). A similar argument applies if all the non-zero coordinates of $\mathbf{s}$ are equal to $p-t$. If $\mathbf{s}$ has a coordinate equal to 1, then the result follows again from Theorem 1.2. If this is not the case, then denote by x_i the number of coordinates in $\mathbf{s}$ equal to i , with $i \in \{t, p-t\}$. Then $\sigma(\mathbf{s}) = tx_t + (p-t)x_{p-t}$. Let λ, μ be integers such that $\lambda t \equiv 1 \pmod{p}$ and $\mu t \equiv p-1 \pmod{p}$, respectively. Then we get

$$\sigma(\lambda \mathbf{s}) = x_t + (p-1)x_{p-t},$$

$$\sigma(\mu \mathbf{s}) = (p-1)x_t + x_{p-t}.$$

If $\sigma(\mathbf{s}) \geq \sigma(\lambda \mathbf{s})$ or $\sigma(\mathbf{s}) \geq \sigma(\mu \mathbf{s})$, the result directly follows from Theorem 1.2. This will always occurs: indeed, if otherwise $\sigma(\mathbf{s}) < \sigma(\lambda \mathbf{s})$ and $\sigma(\mathbf{s}) < \sigma(\mu \mathbf{s})$, we have

$$\sigma(\mathbf{s}) = tx_t + (p-t)x_{p-t} < x_t + (p-1)x_{p-t},$$

$$\sigma(\mathbf{s}) = tx_t + (p-t)x_{p-t} < (p-1)x_t + x_{p-t},$$

which leads to $x_t < x_{p-t} < x_t$, a contradiction.

Now, let us assume $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ and let $\mathcal{M}$ be the multiset associated with it. If there is a hyperplane of $\text{PG}(m, q)$ disjoint from $\mathcal{M}$, the result follows from the first part of the proof. Now, suppose that each hyperplane of $\text{PG}(m, q)$ meet $\mathcal{M}$. Take first $m = 2$, then by Lemma 4.1 and Proposition 4.2,

$$\sigma(\mathbf{s}) = |\mathcal{M}| \geq pq \geq (p-1)(q+1) + 1,$$

as required. Now suppose that $m > 2$ and, by induction hypothesis, we may assume that for any non-zero codeword in $\mathcal{C}_{\text{PG}}^\perp(m-1, q)$ the sum of its coordinates is at least $(p-1)(q^{m-2} + q^{m-3}) + q^{m-3}$. Thus, by Lemma 4.1

$$\sigma(\mathbf{s}) = |\mathcal{M}| \geq q\sigma_{m-1} \geq (p-1)(q^{m-1} + q^{m-2}) + q^{m-2},$$

which completes the proof. □

As a direct consequence of this result, we get the following.

Corollary 4.7. *If $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ with $q = 3^h$ and $h > 1$, then*

$$\sigma(\mathbf{s}) \geq 2q^{m-1} + 3q^{m-2}. \tag{22}$$

We conclude the section by showing the following achievement in which we slightly relax the hypothesis of Proposition 4.6, providing $p = 5$.

Proposition 4.8. *If $\mathbf{s} \in \mathcal{C}_{\text{PG}}(m, q)^\perp$ with $q = 5^h$ and $h > 1$, then*

$$\sigma(\mathbf{s}) \geq 4q^{m-1} + 5q^{m-2}.$$

Proof. First consider the case $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$ and assume that $\mathbf{s}$ has a non-zero coordinate which is equal to 1 or 4. If $\mathbf{s}$ has a coordinate equal to 1, then the result follows from Theorem 1.2. If this is not the case, then denote by x_i the number of i coordinates in $\mathbf{s}$ for $i = 2, 3, 4$. Then

$$\sigma(\mathbf{s}) = 2x_2 + 3x_3 + 4x_4,$$

$$\begin{aligned}\sigma(2\mathbf{s}) &= 4x_2 + x_3 + 3x_4, \\ \sigma(3\mathbf{s}) &= x_2 + 4x_3 + 2x_4, \\ \sigma(4\mathbf{s}) &= 3x_2 + 2x_3 + x_4.\end{aligned}$$

If $x_3 \neq 0$ and $\sigma(2\mathbf{s})$ is less than or equal to $\sigma(\mathbf{s})$, then the assertion follows from Theorem 1.2. The same holds when $x_2 \neq 0$ and $\sigma(3\mathbf{s})$ is less than or equal to $\sigma(\mathbf{s})$. Since $x_4 \neq 0$, if $\sigma(4\mathbf{s})$ is less than or equal to $\sigma(\mathbf{s})$, then we are done by Theorem 1.2. From now on, we assume the contrary.

If $x_2 = x_3 = 0$, then $\sigma(\mathbf{s}) \geq \sigma(4\mathbf{s})$, contradicting $\sigma(4\mathbf{s}) > \sigma(\mathbf{s})$. If $x_2 \neq 0$ and $\sigma(3\mathbf{s}) > \sigma(\mathbf{s})$, then

$$\begin{aligned}\sigma(3\mathbf{s}) &= x_2 + 4x_3 + 2x_4 > 2x_2 + 3x_3 + 4x_4, \\ \sigma(4\mathbf{s}) &= 3x_2 + 2x_3 + x_4 > 2x_2 + 3x_3 + 4x_4,\end{aligned}$$

and summing these two inequalities yields a contradiction. It follows that $x_2 = 0$.

If $x_2 = 0$, $x_3 \neq 0$, then we may assume

$$\begin{aligned}\sigma(2\mathbf{s}) &= x_3 + 3x_4 > 3x_3 + 4x_4, \\ \sigma(4\mathbf{s}) &= 2x_3 + x_4 > 3x_3 + 4x_4.\end{aligned}$$

Similarly, summing up these two inequalities gives a contradiction. Then, for any $\mathbf{s} \in \mathcal{C}_{\text{AG}}(m, q)^\perp$ with a non-zero coordinate equal to 1 or 4, $\sigma(\mathbf{s}) \geq 4q^{m-1} + 5q^{m-2}$.

By applying induction as in Proposition 4.6, we obtain that the result holds for codewords in $\mathcal{C}_{\text{PG}}(m, q)^\perp$ with a non-zero coordinate equal to 1 or 4. Now, let us suppose that the non-zero coordinates of $\mathbf{s}$ are equal to 2 or 3. Then the result follows directly from Proposition 4.6. $\square$

5 Acknowledgment

This work was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INDAM). The first author gratefully acknowledges the hospitality of the University of Naples Federico II. The second author would like to express his gratitude for the hospitality received at Eötvös Loránd University (ELTE), Budapest.

References

- [1] S. ADRIAENSEN: A note on small weight codewords of projective geometric codes and on the smallest stes of even type, SIAM J. Discrete Math. 37(3) (2023), 2072–2087.
- [2] E. F. ASSMUS, JR., J. D. KEY: Designs and their Codes, Cambridge Tracts in Mathematics, Cambridge University Press, 103 (1992) (Second printing with corrections, 1993).
- [3] B. BAGCHI, S. P. INAMDAR: Projective geometric codes, J. Combin. Theory Ser. A, 99(1) (2002), 128–142.
- [4] S. BALL, A. BLOKHUIS, A. GÁCS, P. SZIKLAI, ZS. WEINER: On linear codes whose weights and length have a common divisor, Adv. Math. 211 (2007), 94–104.
- [5] D. BARTOLI, B. CSAJBÓK, G. MARINO, R. TROMBETTI: Evasive subspaces, J. Comb. Des. 29(8) (2021), 533–551.
- [6] A. BLOKHUIS, M. LAVRAUW: Scattered Spaces with Respect to a Spread in $\text{PG}(n, q)$, Geom. Dedicata 81 (2000), 231–243.

- [7] G. BONOLI, O. POLVERINO: $\mathbb{F}_q$ -linear blocking sets in $\text{PG}(2, q^4)$, *Innov. Incidence Geom.* 2 (2005), 35–56.
- [8] N.J. CALKIN, J. D. KEY, M.J. DE RESMINI: Minimum Weight and Dimension Formulas for Some Geometric Codes, *Des. Codes Cryptogr.* 17 (1999), 105–120.
- [9] M. DE BOECK, G. VAN DE VOORDE: Embedded antipodal planes and the minimum weight of the dual code of points and lines in projective planes of order p^2 , *Des. Codes Cryptogr.* (2022), 1–26.
- [10] P. DELSARTE: BCH bounds for a class of cyclic codes, *SIAM J. Appl. Math.* 19 (1970), 420–429.
- [11] M. LAVRAUW, L. STORME, G. VAN DE VOORDE: On the code generated by the incidence matrix of points and k -spaces in $\text{PG}(n, q)$ and its dual, *Finite Fields Appl.* 14(4) (2008), 1020–1038.
- [12] M. LAVRAUW, L. STORME, G. VAN DE VOORDE: Linear codes from projective spaces, *Error-Correcting Codes, Finite Geometries and Cryptography* Edited by: Aiden A. Bruen and David L. Wehlau, *Contemporary Mathematics* 523 (2010).
- [13] G. LONGOBARDI: Scattered polynomials: an overview on their properties, connections and applications, *Art Discrete Appl. Math.* (2025) DOI: <https://doi.org/10.26493/2590-9770.1842.2f0>
- [14] S. E. PAYNE: A complete determination of translation ovoids in finite Desarguian planes, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* 51 (1971), 328–331.
- [15] O. POLVERINO: Linear sets in finite projective spaces, *Discrete Math.* 310 (2010), 3096–3107.

Giovanni Longobardi, Giuseppe Marino, Rocco Trombetti,
 Dipartimento di Matematica e Applicazioni “Renato Caccioppoli”
 Università degli Studi di Napoli Federico II,
 via Cintia, Monte S. Angelo I-80126 Napoli, Italy.
 email:
`{giovanni.longobardi, giuseppe.marino rtrombet}@unina.it`

Bence Csajbók,
 Department of Computer Science
 ELTE Eötvös Loránd University
 H-1117 Budapest, Pázmány P. stny. 1/C, Hungary.
 E-mail: `bence.csajbok@ttk.elte.hu`