Combinatorica (2026) 46:31
https://doi.org/10.1007/s00493-026-00225-y

ORIGINAL PAPER

Multisets Meeting Lines in 0 Modulo p Points and an Improvement of the Bagchi-Inamdar Bound

Bence Csajbók[1] · Giovanni Longobardi[2] · Giuseppe Marino[2] · Rocco Trombetti[2]

Received: 26 October 2025 / Revised: 14 July 2026 / Accepted: 17 August 2026
© The Author(s) 2026

Abstract
The p-ary code associated with the incidence structure of points and t-spaces in a projective space $\mathrm{PG}(m, q)$, 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. The minimum weight of this dual code has been studied since the 1970s; the currently best known lower bound is from 2002 by Bagchi and Inamdar. In this paper we provide a substantial improvement of this bound in the case when $h > 1$ and $m, p > 2$. The main ingredient of the proof is a lower bound on the size of multisets of $\mathrm{AG}(m, q)$ meeting each line in 0 mod p points. We prove this, by generalising the polynomial argument in [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] from (ordinary) planar point sets to multisets in higher dimensional spaces. While the sharpness of the planar result for point sets is in general not known, we can show that our result for multisets is sharp for every $h, m, p \geq 2$.

Keywords Linear codes · Minimum weight · Polynomial method · Multisets

Mathematics Subject Classification 51E20 · 51E22 · 94B65

✉ Bence Csajbók
bence.csajbok@ttk.elte.hu

Giovanni Longobardi
giovanni.longobardi@unina.it

Giuseppe Marino
giuseppe.marino@unina.it

Rocco Trombetti
rtrombet@unina.it

[1] Department of Computer Science, ELTE Eötvös Loránd University, Pázmány P. stny. 1/C, Budapest 1117, Hungary

[2] Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli Federico II, via Cintia, Monte S. Angelo, 80126 Napoli, Italy

Published online: 10 September 2026

1 Introduction

Let Σ be either the projective space $\mathrm{PG}(m,q)$, or the affine space $\mathrm{AG}(m,q)$, 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

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

or

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

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 $\mathbf{v}\in\mathbb{F}_p^v$ is the number of its non-zero coordinates w.r.t. the canonical basis of $\mathbb{F}_p^v$. The *minimum weight* of a code is the minimum of the weights of its non-zero elements. By Assmus and Key [3, Theorem 5.7.9], Calkin, Key and De Resmini [10, Proposition 1] and Delsarte [12], the lower bound

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

was known for the minimum weight of both $\mathcal{C}_{\mathrm{AG}}(m,q)^\perp$ and $\mathcal{C}_{\mathrm{PG}}(m,q)^\perp$. This bound was improved in 2002 by Bagchi and Inamdar, see [4, Theorem 3], to

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

By [13, Theorems 10 and 11], the minimum weight codewords of the dual of the code arising from incidences between points and t-spaces of $\mathrm{PG}(m,q)$ are essentially the same as the minimum weight codewords of $\mathcal{C}_{\mathrm{PG}}(m-t+1,q)^\perp$. In [11, Corollary 1.5] De Boeck and Van de Voorde increased the lower bound on the minimum weight of $\mathcal{C}_{\mathrm{PG}}(2,p^2)^\perp$, $p\geq 5$ prime, from $2q-2p+2$ to $2q-2p+5$.

If q is even, the lower bound in (1) is sharp; see [10, 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 $\mathcal{S}$ of Σ such that each line meets $\mathcal{S}$ 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 [4, Proposition 3], for $q\in\{4,8\}$ in [1]. Finally, in [2], Adriaensen proved for every even q and every integer $m>2$ that the smallest sets of even type in $\mathrm{PG}(m,q)$ are cones with a hyperoval as base and with the vertex deleted. 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) $\mu\colon\mathcal{S}\to\mathbb{Z}^+$ a function that assigns a positive multiplicity to each element of $\mathcal{S}$.

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

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

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 $\mathbf{s}$. We will refer to $\mathcal{S}$ as the support of $\mathcal{M}$.

Let $\mathcal{S}$ denote a non-empty proper subset of the points of $\mathrm{PG}(2, q)$ meeting each line 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 $\mathcal{C}_{\mathrm{PG}}(2, q)^{\perp}$. In [6, 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* $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}(2, q)^{\perp}$ *and* $q > p$. *If* $\mathbf{s}$ *has only coordinates* 0 *and* 1, *then*

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

This bound is sharp when $q = p^2$, or when $p = 2$, see [6, Example 4.4]. Result 1.1 was obtained by first proving it for $\mathbf{s} \in \mathcal{C}_{\mathrm{AG}}(2, q)^{\perp}$. If $\mathcal{S}$ is an ordinary point set of $\mathrm{PG}(2, q)$ 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 $\mathrm{PG}(2, q)$ to $\mathrm{AG}(2, q)$. We point out that for a multiset $\mathcal{M}$ of $\mathrm{PG}(m, q)$, $m \geq 3$, 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 $\mathbf{s} = (s_1, s_2, \ldots, s_v)$ belongs to $\mathcal{C}_{\Sigma}^{\perp}(m, q)$. In Sect. 2, following the main ideas from [6, Theorem 2.1] we prove the following result.

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

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

Clearly, if no coordinate of $\mathbf{s}$ equals 1 and $\mathbf{s} \neq \mathbf{0}$ then by (1) it follows that

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

Although Result 1.1 for the minimum size of planar 0 mod p sets is in general not sharp, in Sect. 3, we prove that the lower bound stated in Theorem 1.2 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 [10, Section 3] starting from a translation hyperoval of $\mathrm{PG}(2, 2^h)$. Finally, using Theorem 1.2, in Sect. 4 we prove a significant improvement of the Bagchi–Inamdar bound in the case $h > 1$ and $m, p > 2$. More precisely, we prove the following result:

Theorem 1.3 *If* $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}(m, q)^{\perp}$ *and* $q > p$, *then*

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

The bound obtained by Bagchi and Inamdar and the one stated in the theorem above both contain the term $2q^{m-1}(1 - 1/p)$. However, the latter also includes the term $2q^{m-2}$, whereas the Bagchi–Inamdar bound contains $2q^{m-2}\left(1 - \frac{1}{p}\right)$. This yields an asymptotic improvement of order $\Theta\left(\frac{q^{m-2}}{p}\right)$. We conclude the article with the investigation of $\sigma(\mathbf{s})$, with $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}(m, q)^{\perp}$, in characteristics 3, 5 and 7.

2 On the Size of an Affine (0 mod 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 mod 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 at most $|\mathcal{M}|$, and if $\mathcal{M}$ meets each line of Σ in 0 mod p points, then the same holds for $\mathcal{M}^*$. 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

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

Now assume $\Sigma = \mathrm{AG}(m, q)$, then the points of Σ can be identified with the elements of $\mathbb{F}_{q^m}$ in a suitable way, so that every point set can also be regarded as a subset of this field. This type of representation is used for $\mathrm{AG}(2, q)$ in [6, Sect. 2].

Note that in this correspondence, three pairwise distinct points $a, b, c \in \mathbb{F}_{q^m}$ are collinear precisely when there is a nonzero scalar $\lambda \in \mathbb{F}_q$ such that $(a - b) = \lambda(a - c)$, equivalently $(a - b)^{q-1} = (a - c)^{q-1}$. It is straightforward to see that the directions of the lines in Σ are in a one-to-one correspondence with the $\frac{q^m-1}{q-1}$-th roots of unity in $\mathbb{F}_{q^m}$, see [5, Sect. 2].

In terms of multisets, Theorem 1.2 from Sect. 1 can be formulated as Theorem 2.1. In the proof we will need the following well-known result. Let $f(Y) \in \mathbb{F}_q[Y]$, where $q = p^h$, let $x \in \mathbb{F}_q$, and $0 \leq k < p$. Then

$$(Y - x)^{k+1} \mid f(Y) \Longleftrightarrow f(x) = f'(x) = \cdots = f^{(k)}(x) = 0. \tag{7}$$

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

$$|\mathcal{M}| \geq (p-1)(q^{m-1} + q^{m-2}) + q^{m-2}. \tag{8}$$

Proof Firstly, note that for $m = 2$, the lower bound in the statement coincides with that in (6). Hence, let us suppose $m \geq 3$. By counting points of $\mathcal{M}$ on lines incident with a fixed point not in $\mathcal{M}$, we obtain $p \mid |\mathcal{M}|$. Let us identify $\mathcal{M}$ with a multiset of $\mathbb{F}_{q^m}$ and define the polynomial

$$R(X, Y) = \prod_{b \in \mathcal{M}} \left(X - (Y - b)^{q-1}\right) = \sum_{j=0}^{|\mathcal{M}|} \sigma_j(Y) X^{|\mathcal{M}|-j}. \tag{9}$$

For $j < 0$ and $j > |\mathcal{M}|$, we set $\sigma_j(Y)$ to be the zero polynomial. Note that for $y \in \mathcal{S}$ with $\mu(y) = t$, it holds that

$$R(X, y) = X^t \left(X^{\frac{q^m-1}{q-1}} - 1\right)^{p-t} g_y(X)^p, \tag{10}$$

where the leading coefficient of $g_y(X)$ is 1. This follows from the fact that any line incident with the point y contains $kp - t$ points of $\mathcal{M}$ (counted with multiplicity) for some positive integer k. The factor X occurs exactly t times in $R(X, y)$ because of the multiplicity of y. The second factor is obtained by multiplying together factors of $R(X, y)$ corresponding to $(p - t)$ points of $\mathcal{M}$ on each line incident with y. Finally, the third factor is just the product of the remaining factors in $R(X, y)$. On the other hand, if $y \notin \mathcal{S}$, then

$$R(X, y) = h_y(X)^p, \tag{11}$$

for some $h_y(X) \in \mathbb{F}_{q^m}[X]$. Indeed, any line incident with the point y contains kp points of $\mathcal{M}$ (counted with multiplicity) for some positive integer k. Consequently, as b ranges in $\mathcal{M}$, the factor $(X - (y - b))^{q-1}$ appears kp times in $R(X, y)$. By (10), if $0 < j < \frac{q^m-1}{q-1}$, $p \nmid j$ and $y \in \mathcal{S}$, then $\sigma_j(y) = 0$. By (11), if $p \nmid j$ and $y \notin \mathcal{S}$, then $\sigma_j(y) = 0$. It follows that for every $y \in \mathbb{F}_{q^m}$ and every $0 < j < \frac{q^m-q}{q-1}$, $p \nmid j$, it holds that $\sigma_j(y) = 0$.

Hence, 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 $0 < j < \frac{q^m-q}{q-1}$ and $p \nmid j$. Then, we may write

$$\begin{aligned} R(X, Y) =& X^{|\mathcal{M}|} + \sigma_p(Y) X^{|\mathcal{M}|-p} + \sigma_{2p}(Y) X^{|\mathcal{M}|-2p} \\ & + \cdots + \sigma_{q^{m-1}+\ldots+q}(Y) X^{|\mathcal{M}|-(q^{m-1}+\ldots+q)} + \\ & \sum_{j=\frac{q^m-1}{q-1}}^{|\mathcal{M}|} \sigma_j(Y) X^{|\mathcal{M}|-j}. \end{aligned}$$

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 $X^{\frac{q^m-1}{q-1}} - 1$, we obtain

$$R(X, y) G_y(X) = (X^{\frac{q^m-1}{q-1}} - 1) \frac{\partial R}{\partial Y}(X, y) \tag{12}$$

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 (12) the highest degree, which is not 1 mod p, is at most $|\mathcal{M}|$. Assume $y \notin \mathcal{S}$, 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 (12) of degree larger than $|\mathcal{M}|$ and of degree not 1 mod p (cf. (11)). This would be a contradiction, which proves that

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

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 (12). 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 $y \notin \mathcal{S}$, on the left-hand side of (12) 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 (12) the coefficient of $X^{|\mathcal{M}|-i}$ is

$$-\sigma'_i(y) + \sigma'_{i+(q^m-1)/(q-1)}(y). \tag{13}$$

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 $kp < q^{m-2}$. Since $m \geq 3$, we have

$$(p-1)\frac{q^m-1}{q-1} + kp > |\mathcal{M}|, \tag{14}$$

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 (12) the coefficient of $X^{|\mathcal{M}|-((p-2)\frac{q^m-1}{q-1}+kp)}$ is equal to 0 and hence by (13):

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

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 $-\sigma'_{kp}(y)$ is the coefficient of $X^{|\mathcal{M}|-kp}$ on the right-hand side of (12). 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

$$\sigma_{kp}(y)\sigma'_{\frac{q^m-1}{q-1}}(y) = -\sigma'_{kp}(y) \tag{15}$$

for each $y \notin \mathcal{S}$. Now, we examine $\sigma_{\frac{q^m-1}{q-1}}(Y)$: if $y \in \mathcal{S}$ with multiplicity $1 \le t \le p-1$, then $\sigma_{\frac{q^m-1}{q-1}}(y) = -(p-t) = t$ (cf. (10)), 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:

$$f(Y)\sigma_{\frac{q^m-1}{q-1}}(Y) = (Y^{q^m} - Y)T(Y). \tag{16}$$

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 $y \in \mathcal{S}$, if $\mu(y) = t$, then, after the derivation of (16)

$$tf'(y) = -T(y).$$

Hence, if $t = 1$, then y is a root of $(f' + T)(Y)$. We generalise this observation and prove that if $1 < t < p$, then y is a t-fold root of $(f' + T)(Y)$. According to (7), it is enough to prove:

$$(f' + T)(y) = (f^{(2)} + T')(y) = \ldots = (f^{(t)} + T^{(t-1)})(y) = 0.$$

From the definition of f and T it is clear that y is a t-fold root of f and a $(t-1)$-fold root of T, and hence

$$(f' + T)(y) = (f^{(2)} + T')(y) = \ldots = (f^{(t-1)} + T^{(t-2)})(y) = 0.$$

The t-th derivative of (16) is

$$\sum_{i=0}^{t}\binom{t}{i} f^{(i)}(Y)\,\sigma^{(t-i)}_{\frac{q^m-1}{q-1}}(Y) = \sum_{i=0}^{t}\binom{t}{i}(Y^{q^m}-Y)^{(i)}\,T^{(t-i)}(Y).$$

At the right hand side the first derivative of $(Y^{q^m}-Y)$ is -1, and all the higher order derivatives are 0, so we have

$$\sum_{i=0}^{t}\binom{t}{i} f^{(i)}(Y)\,\sigma^{(t-i)}_{\frac{q^m-1}{q-1}}(Y) = (Y^{q^m}-Y)\,T^{(t)}(Y) - t\,T^{(t-1)}(Y).$$

After substituting $y \in \mathcal{S}$ with $\mu(y) = t$, and using that y is a t-fold root of $f(Y)$, we obtain

$$f^{(t)}(y)\sigma_{\frac{q^m-1}{q-1}}(y) = -tT^{(t-1)}(y).$$

Substituting $\sigma_{\frac{q^m-1}{q-1}}(y) = t$ and rearranging yields the desired

$$(f^{(t)} + T^{(t-1)})(y) = 0$$

equation. Since $\sum_{y\in\mathcal{S}}\mu(y) = |\mathcal{M}|$, we proved that $f' + T$ has $|\mathcal{M}|$ roots (counted with multiplicities). This is larger than $\deg(f' + T)$ and hence $f' + T$ is the zero polynomial, i.e. $f'(Y) = -T(Y)$, and hence $f'(y) = -T(y)$ holds for each $y \in \mathbb{F}_{q^m}$.

Again, after differentiating (16), substituting $y \notin \mathcal{S}$ and applying $\sigma_{\frac{q^m-1}{q-1}}(y) = 0$, we obtain

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

Then, combined with (15), we obtain

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

and hence $(f\sigma_{kp})'(y) = 0$, for each $y \notin \mathcal{S}$. 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 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 $q^m - |\mathcal{S}|$. Equivalently, we need

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

Because of $|\mathcal{S}| \le |\mathcal{M}| = (p-1)(q^{m-1} + q^{m-2}) + kp$ and $kp < q^{m-2}$, this certainly holds when

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

which is equivalent to $q^{m-2}(q^2 - (2p-1)(q+1)) > -(q+3)$. This inequality clearly holds and hence $(f\sigma_{kp})'$ is the zero polynomial. This means that $(f\sigma_{kp})(Y)$

is a p-th power of a polynomial in $\mathbb{F}_{q^m}[Y]$. We prove that $f(Y)$ divides $\sigma_{kp}(Y)^{p-1}$. Recall that f is a 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, $f(Y) \mid \sigma_{kp}(Y)^{p-1}$. It follows that either $\deg f \leq (p-1)\deg \sigma_{kp}$, and hence $|\mathcal{M}| \leq (p-1)kp(q-1)$, or σ_{kp} is the zero polynomial.

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

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

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 $(-1)^{kp}\binom{|\mathcal{M}|}{kp}$. 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. □

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 $\mathrm{AG}(m,q)$ such that lines meet $\mathcal{S}$ in 0 mod p points. The sharp lower bound for the size of such point sets is given in (1), and it coincides with the value that (8) yields when $p = 2$.

We conclude this section by noting that if $\mathbf{s} \in \mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$, 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 $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$. Clearly, $w(\bar{\mathbf{s}}) = w(\mathbf{s})$ and $\sigma(\bar{\mathbf{s}}) = \sigma(\mathbf{s})$; hence, the minimum weight of $\mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$ is at least the minimum weight of $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$. Similarly, we can conclude that the minimum size of a (0 mod p)-multiset in $\mathrm{AG}(m,q)$ is at least the minimum size of a (0 mod p)-multiset in $\mathrm{PG}(m,q)$.

3 Examples Attaining the Lower Bound

In this section, we construct a family of multisets in $\mathrm{AG}(m,q)$ that attain the bound given in (8), contain at least one point of multiplicity 1, and intersect every affine line in a number of points divisible by p.

Let V denote the $(m+1)$-dimensional $\mathbb{F}_q$-vector space underlying $\Sigma = \mathrm{PG}(m,q)$. 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 [9] and [17, Proposition 2.2].

The subsequent results are crucial for achieving our goal. We state the next proposition in its general form, however, in our applications the $\mathbb{F}_p$-linear set W of rank $h(m-1)+1$ will always be just a hyperplane of $\mathrm{PG}(m,q)$. (It is again an easy consequence of Grassmann's Identity that the point set of a hyperplane can be defined by non-zero vectors of an $(h(m-1)+1)$-dimensional $\mathbb{F}_p$-subspace.)

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

$$\mu(x)=\begin{cases} t & \text{if } x \in L_U \setminus L_W \\ p-t & \text{if } x \in L_W \setminus L_U, \end{cases} \tag{17}$$

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

Proof Let ℓ be any line of $\mathrm{PG}(m,q)$ 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 a $(u,v)_p$-*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 [7]. We will need the following result on $(m-1,(m-2)h)_p$-evasive subspaces:

Result 3.2 ([7, 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 $\mathbb{F}_p$-subspace of dimension at most $(m-2)h$. Then* $\dim_p(U)\le (m-1)h-1$.

Proposition 3.3 *Let $f\colon \mathbb{F}_q^{m-1}\to\mathbb{F}_q$ be an $\mathbb{F}_p$-linear map, $m\ge 2$. In $V=\mathbb{F}_q^{m+1}$ put*

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

and let $\mathcal{H}$ denote the hyperplane of equation $X_m=0$. Define $\mathcal{M}=(L_U\triangle\mathcal{H},\mu)$, a multiset of $\mathrm{PG}(m,q)$, *where μ is defined as in Proposition 3.1 with the choice $t=1$.*

(1) *There is a hyperplane disjoint from $\mathcal{M}$.*
(2) *$\mathcal{M}$ is of size at least*
$$(p-1)(q^{m-1}+q^{m-2})+q^{m-2}$$
and as $|L_U\cap\mathcal{H}|$ increases, $|\mathcal{M}|$ decreases. Equality is reached if and only if
$$|L_U\cap\mathcal{H}|=q^{m-2}\frac{q-1}{p-1}+\frac{q^{m-2}-1}{q-1}.$$

Proof (1) Put $H = \{(x_0, x_1, \ldots, x_{m-1}, 0) : x_0, x_1, \ldots, x_{m-1} \in \mathbb{F}_q\}$, i.e. H is the m-dimensional $\mathbb{F}_q$-subspace of V corresponding to $\mathcal{H}$. Note that $L_U \cap \mathcal{H} = L_{U \cap H}$ is an $\mathbb{F}_p$-linear set of rank $(m-1)h$. By Grassmann's Identity, $L_{U\cap H}$ meets the hyperplanes of $\mathcal{H}$ 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 $\mathcal{H}$ in an $\mathbb{F}_p$-linear set of rank exactly $(m-2)h$.

Hence, $L_{U\cap H}$ meets at least one hyperplane, say Π of $\mathcal{H}$, 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 $\mathrm{PG}(m, q)$ through Π which does not meet $\mathcal{M}$. Assume, to the contrary, that each hyperplane $\mathcal{H}'$ of $\mathrm{PG}(m, q)$ through Π and distinct from $\mathcal{H}$ meets $\mathcal{M}$. Since $\mathcal{M} \cap \mathcal{H}'$ is a multiset of $\mathcal{H}' \setminus \Pi \cong \mathrm{AG}(m-1, q)$ meeting every line in 0 mod p points and having only points of multiplicity 1, by applying Theorem 2.1, for $m \geq 3$ we have that

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

a contradiction. For $m = 2$, $|\mathcal{M} \cap \mathcal{H}'| \geq p$ for each line $\mathcal{H}'$ incident with the point Π and distinct from the line $\mathcal{H}$, thus $|L_U \setminus \mathcal{H}| \geq qp$, which again yields a contradiction.

Then the lower bound of part (2) follows from Theorem 2.1. The remainder of the statement follows from

$$|\mathcal{M}| = (p-1)|\mathcal{H}\backslash(L_U \cap \mathcal{H})| + |L_U\backslash\mathcal{H}|,$$

where $|L_U \setminus \mathcal{H}| = q^{m-1}$.

□

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

Theorem 3.4 *Let L be an $\mathbb{F}_p$-linear set of rank hm in* $\mathrm{PG}(m, q)$*, $q = p^h$. 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 $\mathrm{PG}(m, q)$ we may assume that $(0 : 0 : \ldots : 0 : 1) \notin L$ and hence L can be written as $L = L_U$, where

$$U = \{(x_0, x_1, \ldots, x_{m-1}, f(x_0, \ldots, x_{m-1})) : x_i \in \mathbb{F}_q\}$$

is an $\mathbb{F}_p$-subspace of dimension hm, and hence $f : \mathbb{F}_q^m \to \mathbb{F}_q$ is additive. The hyperplane $\bar{\mathcal{H}}$ of $\mathrm{PG}(m+1, q)$ with equation $X_{m+1} = 0$ is an $\mathbb{F}_p$-linear set of rank $hm + 1$.

Now, consider the $\mathbb{F}_p$-linear set $L_{\overline{U}}$ of rank $hm + 1$, where

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

Then, by Proposition 3.1 with $t = 1$, the multiset $\bar{\mathcal{M}} = (L_{\overline{U}} \triangle \overline{\mathcal{H}}, \mu)$ with μ as in (17) meets any line of $\mathrm{PG}(m+1, q)$ in 0 mod p points. By Proposition 3.3 (2),

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

hence the result follows. □

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

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

which is positive for $h > 1$.

In the remainder, we apply Propositions 3.1 and 3.3 to construct (0 mod p)-multisets in $\mathrm{AG}(m, q)$ of size $(p-1)(q^{m-1}+q^{m-2}) + q^{m-2}$ that contain at least one point of multiplicity 1.

To this aim we first recall that an $\mathbb{F}_p$-linearized polynomial $f(x) = \sum_{i=0}^{h-1} a_i x^{p^i} \in \mathbb{F}_q[x]$ 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 [15].

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

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

where f is any scattered $\mathbb{F}_p$-linearized polynomial. Also, consider the hyperplane $\mathcal{H}$ of $\mathrm{PG}(m, q)$ with equation $X_m = 0$.

It is easy to see that $L_U \cap \mathcal{H}$ is an $\mathbb{F}_p$-linear set, and it is a cone with basis a maximum scattered $\mathbb{F}_p$-linear set on the line with equations $X_1 = X_2 = \ldots = X_{m-2} = X_m = 0$ and vertex an $(m-3)$-dimensional subspace with equations $X_0 = X_{m-1} = X_m = 0$. Then,

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

and $\mathcal{M} = (L_U \triangle \mathcal{H}, \mu)$ defined as in (17) with $t = 1$ is a multiset of $\mathrm{AG}(m, q)$ whose size attains the bound in (8). The fact that this construction can be embedded in $\mathrm{AG}(m, q)$ 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 [14, Theorem 4.14]. In particular, if $f(X) = X^p$, then our construction has the same support as the one in [14, Theorem 4.14]. Moreover, if $p = 2$ the example falls into the family exhibited by Calkin, Key and De Resmini in [10]. Indeed, in such a case L_U is equivalent to a cone with base the $\mathbb{F}_2$-linear set $\{\langle (x, x^{2^s})\rangle_{\mathbb{F}_{2^h}} : x \in \mathbb{F}^*_{2^h}\} \subseteq \mathrm{PG}(1, 2^h)$, with $\gcd(s, h) = 1$, which is the set of directions determined by the points of a translation hyperoval of $\mathrm{PG}(2, 2^h)$ (see [16]). In such a case, our construction provides a set which is equivalent to the one constructed by induction in [10, Note 1].

4 A Lower Bound on the Minimum Weight of $\mathcal{C}_{\mathrm{PG}}(m, q)^\perp$

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

In the remainder of this article, we will use $w_m(q)$ and $\sigma_m(q)$ to denote, respectively, the minimum weight of the code $\mathcal{C}^\perp_{\mathrm{PG}}(m, q)$ and the minimum size of a non-empty $(0 \bmod p)$-multiset in $\mathrm{PG}(m, q)$.

First, we extend [10, Proposition 1] to multisets.

Lemma 4.1 *If $\mathcal{M} = (\mathcal{S}, \mu)$ is a $(0 \bmod p)$-multiset of $\mathrm{PG}(m, q)$, $q = p^h$, and $\mathcal{M}$ meets every hyperplane, then*

$$|\mathcal{S}| > q\, w_{m-1}(q) \quad \text{and} \quad |\mathcal{M}| > q\, \sigma_{m-1}(q).$$

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

$$z_1 + z_2 + \cdots + z_\ell = \frac{q^{m+1} - 1}{q - 1}. \tag{18}$$

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

$$n_1 z_1 + n_2 z_2 + \cdots + n_\ell z_\ell = |\mathcal{S}| \frac{q^m - 1}{q - 1}. \tag{19}$$

Multiplying (18) by n_1 and subtracting (19) we get

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

Since n_1 is at least $w_{m-1}(q)$, the first part of the statement is proved. To prove the second part, assume that the $(m-1)$-dimensional subspaces of $\mathrm{PG}(m, q)$ meet $\mathcal{M}$ in $0 < n_1 < \ldots < n_\ell$ points (counting the points with their multiplicities) and that there are z_i of those meeting $\mathcal{M}$ in n_i points. Clearly (18) holds and by double counting the $(x, \mathcal{H})$ pairs (counting each of them $\mu(x)$ times), we obtain (19) with $|\mathcal{M}|$ on its right side (instead of $|\mathcal{S}|$). Similarly to the arguments above, now we obtain $|\mathcal{M}| > n_1 q$ and the result follows noting that $n_1 \geq \sigma_{m-1}(q)$. $\square$

In [4, Lemma 6] the authors proved that $w_m(q) \leq q\, w_{m-1}(q)$. Combining this with Lemma 4.1, we see that the minimum weight of $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$ is at least that of $\mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$. Indeed, if $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$ has weight $w(\mathbf{s}) = w_m(q)$ and the point set $\mathcal{S}$, consisting of points corresponding to the support of $\mathbf{s}$, meets every hyperplane of $\mathrm{PG}(m,q)$, then

$$q\, w_{m-1}(q) < w_m(q) \leq q\, w_{m-1}(q),$$

a contradiction. It follows that there is a hyperplane disjoint from $\mathcal{S}$, hence the minimum weight of a codeword in $\mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$ is at most the minimum weight of $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$. This observation together with the last paragraph of Sect. 2 yields the following.

Proposition 4.2 *For any minimum weight codeword of $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$, one can find a hyperplane of* $\mathrm{PG}(m,q)$*, which is disjoint from the corresponding multiset. As a consequence, the codes $\mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$ and $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$ have the same minimum weight.* □

Using the same techniques as in [4, Lemma 6], we shall prove a similar inequality relating $\sigma_m(q)$ and $\sigma_{m-1}(q)$.

Proposition 4.3 *For any $m \geq 2$ and $q = p^h$ it holds that*

$$\sigma_m(q) \leq q\, \sigma_{m-1}(q).$$

Proof Let $\mathcal{M} = (\mathcal{S}, \mu)$ be a $(0 \bmod p)$-multiset of $\mathrm{PG}(m-1,q)$ embedded into a hyperplane $\mathcal{H}$ of $\mathrm{PG}(m,q)$. Take a point $P \notin \mathcal{H}$ and consider the cone C with vertex P and base $\mathcal{S}$. Define the multiset $\mathcal{M}' = (\mathcal{S}', \mu')$, where $\mathcal{S}' = C \setminus \{P\}$ and μ' is defined as follows: If $Q \in \mathcal{S}'$ and Q' is the projection of Q from P onto $\mathcal{H}$, then $\mu'(Q) := \mu(Q')$. Clearly, $|\mathcal{M}'| = q|\mathcal{M}|$.

If ℓ is a line incident with P, then it is either exterior to $\mathcal{M}'$, or $|\ell \cap \mathcal{M}'|$ equals q times $\mu(\ell \cap \mathcal{H})$, which is divisible by p.

If ℓ is not incident with P, then let ℓ' denote the projection of ℓ from P onto $\mathcal{H}$. Then $|\ell \cap \mathcal{M}'| = |\ell' \cap \mathcal{M}|$, which is divisible by p because of the choice of $\mathcal{M}$.

If we choose $\mathcal{M}$ to be a $(0 \bmod p)$-multiset of size $\sigma_{m-1}(q)$ in $\mathrm{PG}(m-1,q)$, then $\mathcal{M}'$ is a $(0 \bmod p)$-multiset of $\mathrm{PG}(m,q)$ of size $q\sigma_{m-1}(q)$, which proves the claim. □

As for the minimum weight of $\mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$, by Lemma 4.1 and Proposition 4.3, we obtain the following result.

Proposition 4.4 *There is a hyperplane disjoint from any* $(0 \bmod p)$*-multiset of size $\sigma_m(q)$ in* $\mathrm{PG}(m,q)$*. As a consequence, the minimum size of a non-empty* $(0 \bmod p)$*-multiset is the same in* $\mathrm{AG}(m,q)$ *as in* $\mathrm{PG}(m,q)$. □

In the next proof we will need the following definition.

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

Theorem 4.5 *If $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}(m,q)^{\perp}$ and $q > p$, then*

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

Proof For $p = 2$, the assertion follows from (1). Hence,assume $p > 2$. First, take a codeword $\mathbf{s} \in \mathcal{C}_{\mathrm{AG}}(m, q)^{\perp}$ 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 of $\mathcal{M}$ with multiplicity 1. If there are no points with multiplicity $p-1$, then counting the points on lines through x gives

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

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

$$2((p-1)q^{m-1} + pq^{m-2}) \leq |\mathcal{M}| + |(p-1)\mathcal{M}| = p\, w(\mathbf{s}), \tag{20}$$

from which the result follows. For the origin of the trick applied in (20) see [1, Result 3.2 and Remark 3.4]. By Proposition 4.2, the result follows. □

Let $\mathcal{C}_{\mathrm{PG}}^{(k)}(m, q)$ be the p-ary code associated with the design $\mathcal{D}_{\mathrm{PG}}^{(k)}(m, q)$ of points and k-spaces of $\mathrm{PG}(m, q)$, 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 $\mathcal{C}_{\mathrm{PG}}^{(k)}(m, q)^{\perp}$ is equal to the minimum weight of $\mathcal{C}_{\mathrm{PG}}(m-k+1, q)^{\perp}$, see [13, Theorem 10]. Then, as a corollary of Theorem 4.5, we get the following result.

Corollary 4.6 *If* $\mathbf{s} \in \mathcal{C}_{\mathrm{PG}}^{(k)}(m, q)^{\perp}$ *and* $q > p$, *then*

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

We remark that Corollary 4.6 improves the bounds proved in [13, Theorems 14 and 15].

At last, for small characteristics we are able to extend Theorem 2.1 to multisets of projective spaces, and without the assumption of the existence of at least one point of multiplicity one.

With a slight abuse of notation, we identify the integers $0, 1, \ldots, p-1$ with their residue classes in $\mathbb{F}_p$ and we prove the following elementary scaling lemma.

Lemma 4.7 *Let* $\mathbf{s} \in \mathbb{F}_p^v$ *be non-zero. Assume that at least one of the following conditions holds:*

(1) *there exists an integer* $t \in \{1, 2, \ldots, p-1\}$, *such that every non-zero coordinate of* $\mathbf{s}$ *is equal to either* t *or* $p-t$,
(2) *the prime* p *is in* $\{3, 5, 7\}$.

Then there exists $\lambda \in \mathbb{F}_p^*$ *such that* $\lambda\mathbf{s}$ *has a coordinate equal to* 1 *and*

$$\sigma(\lambda\mathbf{s}) \leq \sigma(\mathbf{s}).$$

Proof Let x_i denote the number of coordinates of $\mathbf{s}$ equal to i, for $i \in \{1, \ldots, p-1\}$. If $x_1 > 0$, then we can take $\lambda = 1$, so assume $x_1 = 0$. For $i \in \{2, \ldots, p-1\}$, put

$$D_i = \sigma(i^{-1}\mathbf{s}) - \sigma(\mathbf{s}),$$

where i^{-1} is taken in $\mathbb{F}_p^*$. It is enough to prove that $D_i \leq 0$ for some i with $x_i > 0$. Clearly, if $x_i > 0$ and $D_i \leq 0$, then $i^{-1}\mathbf{s}$ has a coordinate equal to 1 and

$$\sigma(i^{-1}\mathbf{s}) \leq \sigma(\mathbf{s}).$$

(1) We may assume that $x_t\, x_{p-t} \neq 0$ since otherwise all non-zero coordinates are equal and the assertion follows by taking λ to be the inverse of that non-zero element. In particular, because of $x_1 = 0$, we may also assume $t \notin \{1, p-1\}$. Note that

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

and hence,

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

Therefore,

$$D_t = \sigma(t^{-1}\mathbf{s}) - \sigma(\mathbf{s}) = (t-1)(x_{p-t} - x_t). \tag{21}$$

Similarly, we have that

$$D_{p-t} = \sigma((p-t)^{-1}\mathbf{s}) - \sigma(\mathbf{s}) = (p-1-t)(x_t - x_{p-t}). \tag{22}$$

Suppose by contradiction that both $D_t > 0$ and $D_{p-t} > 0$. Then $x_{p-t} > x_t$ and $x_t > x_{p-t}$, a contradiction.
(2) For $p = 3$ the claim follows from part (1).
For $p = 5$, we have

$$\begin{aligned} D_2 &= -x_2 + x_3 - 2x_4, \\ D_4 &= x_2 - x_3 - 3x_4. \end{aligned}$$

Suppose, to the contrary, that $D_i > 0$ for every i with $x_i > 0$. If $x_4 > 0$, then $D_4 > 0$ and hence $x_2 > 0$, so $D_2 + D_4 = -5x_4 > 0$, which is a contradiction. It follows that $x_4 = 0$ and hence the claim follows from (1).
It remains to consider $p = 7$. In this case

$$\begin{aligned} D_2 &= -x_2 + 2x_3 - 2x_4 + x_5 - 3x_6, \\ D_3 &= x_2 - 2x_3 + 2x_4 - x_5 - 4x_6, \\ D_4 &= 2x_2 + 3x_3 - 3x_4 - 2x_5 - x_6, \\ D_5 &= 4x_2 - x_3 + x_4 - 4x_5 - 2x_6, \\ D_6 &= 3x_2 + x_3 - x_4 - 3x_5 - 5x_6. \end{aligned}$$

Again, suppose that $D_i > 0$ for every i with $x_i > 0$. First, x_2 and x_3 cannot both be positive, since otherwise

$$D_2 + D_3 = -7x_6 \leq 0.$$

Thus $x_2x_3 = 0$. Also $x_2x_5 = 0$, since if $x_2x_5 > 0$, then

$$4D_2 + D_5 = 7x_3 - 7x_4 - 14x_6 > 0,$$

so $x_3 > 0$, contradicting $x_2x_3 = 0$. Similarly $x_3x_4 = 0$, since if $x_3x_4 > 0$, then

$$3D_3 + 2D_4 = 7x_2 - 7x_5 - 14x_6 > 0,$$

so $x_2 > 0$, contradicting $x_2x_3 = 0$ again. If $x_2 > 0$, then $x_3 = x_5 = 0$, and hence

$$D_2 = -x_2 - 2x_4 - 3x_6 \leq 0,$$

a contradiction. Hence $x_2 = 0$. If $x_3 > 0$, then $x_4 = 0$, and hence

$$D_3 = -2x_3 - x_5 - 4x_6 \leq 0,$$

getting a contradiction. Hence $x_3 = 0$. If $x_6 > 0$, then

$$D_6 = -x_4 - 3x_5 - 5x_6 \leq 0,$$

a contradiction again. This implies $x_6 = 0$. Finally, if $x_4 > 0$, then

$$D_4 = -3x_4 - 2x_5 \leq 0,$$

and if $x_5 > 0$, then

$$D_5 = -4x_5 \leq 0.$$

Both are contradictions. Therefore, all x_i are zero, which is impossible and this concludes the proof. □

Proposition 4.8 *Let p be a prime, and $q = p^h$ with $h > 1$. Let $\mathbf{s} \in C^{\perp}_{\mathrm{PG}(m,q)}$ be non-zero. Assume that at least one of the following conditions holds:*

(1) *there exists an integer $t \in \{1, 2, \dots, p-1\}$, such that every non-zero coordinate of $\mathbf{s}$ is equal to either t or $p - t$,*
(2) *the prime p is in $\{3, 5, 7\}$.*

Then

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

Proof For $p = 2$, we have $\sigma(\mathbf{s}) = w(\mathbf{s})$,and the assertion follows from (1). Hence, assume that $p > 2$. By Proposition 4.4, it is enough to prove the result for affine spaces. Let $\mathbf{s} \in \mathcal{C}_{\mathrm{AG}}(m,q)^{\perp}$ be non-zero. By Lemma 4.7, there exists $\lambda \in \mathbb{F}_p^*$ such that $\lambda\mathbf{s}$ has a coordinate equal to 1 and

$$\sigma(\lambda\mathbf{s}) \leq \sigma(\mathbf{s}).$$

Since $\lambda\mathbf{s} \in \mathcal{C}_{\mathrm{AG}}(m, q)^{\perp}$, Theorem 1.2 gives

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

Therefore

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

as required. $\square$

Remark 4.9 The restriction $p \in \{3, 5, 7\}$ in Lemma 4.7 part (2) is essential, moreover, part (1) does not extend to two arbitrary nonzero coordinate values. For every prime $p > 7$, the vector $\mathbf{s} = (2, 3) \in \mathbb{F}_p^2$ is a minimal counterexample. Indeed, $\sigma(\mathbf{s}) = 5$, and the only scalars which produce a coordinate equal to 1 are 2^{-1} and 3^{-1}. We have

$$\sigma(2^{-1}\mathbf{s}) = 1 + \frac{p+3}{2} > 5,$$

while

$$\sigma(3^{-1}\mathbf{s}) = 1 + \begin{cases} \frac{p+2}{3}, & p \equiv 1 \pmod 3, \\ \frac{2p+2}{3}, & p \equiv 2 \pmod 3, \end{cases} > 5.$$

Acknowledgements 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. The authors sincerely thank the referees for their thoughtful comments and useful suggestions, which led to a clearer presentation of the results. They would also like to thank the participants of the Finite Geometry Seminar at Eötvös Loránd University for helpful discussions on the proof of Theorem 2.1.

Funding Open access funding provided by Eötvös Loránd University. This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The research was also supported in part by the ELTE TKP2021-NKTA-62 funding scheme. Project nos. 153080, 151504 and 152582 have been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the ADVANCED_25, EXCELLENCE_24 and SNN_25 funding schemes, respectively.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Adriaensen, S.: A note on small weight codewords of projective geometric codes and on the smallest sets of even type. SIAM J. Discrete Math. **37**(3), 2072–2087 (2023)
2. Adriaensen, S.: Even sets and dual projective geometric codes: a tale of cylinders. Preprint at http://arxiv.org/abs/2601.12451

3. Assmus, E.F. Jr., Key, J.D.: Designs and their Codes. Cambridge Tracts in Mathematics, vol. 103. Cambridge University Press (1992). (**Second printing with corrections, 1993**)
4. Bagchi, B., Inamdar, S.P.: Projective geometric codes. J. Combin. Theory Ser. A **99**(1), 128–142 (2002)
5. Ball, S.: Polynomials in finite geometries. In Lamb, J. D., & Preece, D. A., (Eds.:), Surveys in Combinatorics (London Mathematical Society Lecture Note Series 267) Cambridge University Press pp. 17–35 (1999)
6. Ball, S., Blokhuis, A., Gács, A., Sziklai, P., Weiner, Z.S.: On linear codes whose weights and length have a common divisor. Adv. Math. **211**, 94–104 (2007)
7. Bartoli, D., Csajbók, B., Marino, G., Trombetti, R.: Evasive subspaces. J. Comb. Des. **29**(8), 533–551 (2021)
8. Blokhuis, A., Lavrauw, M.: Scattered Spaces with Respect to a Spread in PG(n, q). Geom. Dedicata. **81**, 231–243 (2000)
9. Bonoli, G., Polverino, O.: $\mathbb{F}_q$-linear blocking sets in PG$(2, q^4)$. Innov. Incidence Geom. **2**, 35–56 (2005)
10. Calkin, N.J., Key, J.D., De Resmini, M.J.: Minimum Weight and Dimension Formulas for Some Geometric Codes. Des. Codes Cryptogr. **17**, 105–120 (1999)
11. De Boeck, M., Van de Voorde, G.: 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. 91, 895–920 (2023)
12. Delsarte, P.: BCH bounds for a class of cyclic codes. SIAM J. Appl. Math. **19**, 420–429 (1970)
13. Lavrauw, M., Storme, L., Van de Voorde, G.: On the code generated by the incidence matrix of points and k-spaces in PG(n, q) and its dual. Finite Fields Appl. **14**(4), 1020–1038 (2008)
14. Lavrauw, M., Storme, L., Van de Voorde, G.: Linear codes from projective spaces. In: Bruen, A.A., Wehlau, D.L. (eds.) Error-Correcting Codes, Finite Geometries and Cryptography, vol. 523. American Mathematical Soc (2010)
15. Longobardi, G.: Scattered polynomials: an overview on their properties, connections and applications. Art Discrete Appl. Math (2025). https://doi.org/10.26493/2590-9770.1842.2f0
16. Payne, S.E.: A complete determination of translation ovoids in finite Desarguian planes. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat **51**, 328–331 (1971)
17. Polverino, O.: Linear sets in finite projective spaces. Discrete Math. **310**, 3096–3107 (2010)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.