Small weight codewords of the code generated by the lines of PG$(2, q)$

Tamás Szőnyi and Zsuzsa Weiner *

July 27, 2018

Abstract

In this paper, we prove a stability result on t mod p multisets of points in PG$(2, q)$, $q = p^h$. The particular case $t = 0$ is used to describe small weight codewords of the code generated by the lines of PG$(2, q)$, as linear combination of few lines. Our result is sharp when $27 < q$ square and $h \geq 4$. When q is a prime, De Boeck and Vandendriessche (see [2]) constructed a codeword of weight $3p - 3$ that is not the linear combination of three lines. We characterise their example.

1 Introduction

In a previous paper ([11]), we proved a stability result on point sets of even type in PG$(2, q)$. A *set of even type* S is a point set intersecting each line in an even number of points. It is easy to see that sets of even type can only exist when q is even. A stability theorem says that when a structure is "close" to being extremal, then it can be obtained from an extremal one by changing it a little bit. More precisely, we proved that if the number of odd secants, δ, of a point set is less than $(\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$, then we can add and delete, altogether $\lceil\frac{\delta}{q+1}\rceil$ points, so that we obtain a point set of even type. As a consequence, we described small weight codewords of $C_1(2, 2^h)$.

*In the earlier phase of this research, both authors were partially supported by OTKA Grant K 81310. In the final phase, the first author was partially supported by the Slovenian-Hungarian OTKA Grant NN 114614.

$C_1(2, 2^h)$ is the binary code generated by the characteristic vectors of lines in $\mathrm{PG}(2, 2^h)$. As the complement of an (almost) even set is an (almost) odd set, the same results hold for odd sets.

The aim of this paper is to generalise the above results to odd q. A possible generalisation of sets of even type are sets intersecting every line in t mod p points, briefly *t mod p sets*. We expect the union of a t_1 mod p and a t_2 mod p set be a $t_1 + t_2$ mod p set. This is only true if we consider multisets, that is the points of the set have weights. We call a multiset a *t mod p multiset* if it intersects every line in t mod p points counted with weights (multiplicities). Hence our aim is to generalise the stability results of sets of even type to t mod p multisets where $q = p^h$, p prime. More precisely, the following theorems will be proved.

Theorem 1.1 *Let $\mathcal{M}$ be a multiset in $\mathrm{PG}(2, q)$, $17 < q$, $q = p^h$, where p is prime. Assume that the number of lines intersecting $\mathcal{M}$ in not k mod p points is δ, where $\delta < \sqrt{\frac{q}{2}}(q+1)$. Then there exists a set S of points with size $\lceil \frac{\delta}{q+1} \rceil$, which blocks all the not k mod p lines.*

Theorem 1.2 *Let $\mathcal{M}$ be a multiset in $\mathrm{PG}(2, q)$, $27 < q$, $q = p^h$, where p is prime and $h > 1$ (that is q not a prime). Assume that the number of lines intersecting $\mathcal{M}$ in not k mod p points is δ, where*

(1) $\delta < (\lfloor \sqrt{q} \rfloor + 1)(q + 1 - \lfloor \sqrt{q} \rfloor)$, when $2 < h$.

(2) $\delta < \frac{(p-1)(p-4)(p^2+1)}{2p-1}$, when $h = 2$.

Then there exists a multiset $\mathcal{M}'$ with the property that it intersects every line in k mod p points and the number of different points in $(\mathcal{M} \cup \mathcal{M}') \setminus (\mathcal{M} \cap \mathcal{M}')$ is exactly $\lceil \frac{\delta}{q+1} \rceil$.

Remark 1.3 Observe that the conclusion in Theorem 1.2 is much stronger than in Theorem 1.1, but Theorem 1.2 does not say anything when $h = 1$ or $h = 2$ and $\delta \geq \frac{(p-1)(p-4)(p^2+1)}{2p-1}$. Nevertheless, the conclusion in Theorem 1.2 does not apply in case $h = 1$ as Example 4.6 and Example 4.7 show it in Section 3.

Remark 1.4 Note that a complete arc of size $q - \sqrt{q} + 1$ has $(\sqrt{q} + 1)(q + 1 - \sqrt{q})$ odd-secants, which shows that Theorem 1.2 is sharp, when q is an even square. (Since the smallest sets of even type are hyperovals.) For the existence of such arcs, see [3], [5], [7] and [9], [12].

Let $C_1(2,q)$ be the p-ary linear code generated by the characteristic vectors of the lines of PG$(2,q)$ $q=p^h$, p prime. Hence a codeword c is a linear combination of lines, that is $c=\sum_i \lambda_i l_i$. The vectors l_i corresponds to a point in the dual plane of PG$(2,q)$. If we consider the point corresponding to l_i with weight λ_i, then c corresponds to a multiset in the dual plane of PG$(2,q)$. A codeword c with weight $w(c)$ (the number of non-zero coordinates) corresponds to a multiset intersecting all but $w(c)$ lines in 0 mod p points. The coordinates of c that are zero correspond to lines intersecting the multiset in the dual plane in 0 mod p points. Hence we can translate our stability results on multisets (Theorem 1.1 and 1.2) to results on small weight codewords, see Theorem 4.2, 4.3 and 4.4. The prime case is a bit more difficult, because of some examples of weight $3p$ constructed by De Boeck and Vandendriessche, see [2] and Example 4.6. A slight generalisation that gives also codewords of weight $3p+1$ is given in Example 4.7. In this case, we prove the following results.

Theorem 4.8 *Let c be a codeword of $C(2,p)$, $p>17$ prime. If $2p+1<w(c)\leq 3p+1$, then c is either the linear combination of three lines or Example 4.7.*

Corollary 4.9 *For any integer $0<k+1<\sqrt{\frac{q}{2}}$, there is no codeword whose weight lies in the interval $(kq+1,((k+1)q-\frac{3}{2}k^2-\frac{5}{2}k-1)$.*

Note that, when $k=3$, the above results give that codewords of weight less than $4p-22$ can be obtained via Example 4.7 or it is the linear combination of three lines.

2 The algebraic background

Result 2.1 ([12], [11]) *Suppose that the nonzero polynomials $u(X,Y)=\sum_{i=0}^{n} u_i(Y)X^{n-i}$ and $v(X,Y)=\sum_{i=0}^{n-m} v_i(Y)X^{n-m-i}$, $m>0$, satisfy $\deg u_i(Y)\leq i$ and $\deg v_i(Y)\leq i$ and $u_0\neq 0$.*

Furthermore, assume that there exists a value y, so that the degree of the greatest common divisor of $u(X,y)$ and $v(X,y)$ is $n-s$. Denote by n_h, the number of values y' for which $\deg(\gcd(u(X,y'),v(X,y')))=n-(s-h)$. Then

$$\sum_{h=1}^{s} hn_h \leq s(s-m). \blacksquare$$

Remark 2.2 In our earlier paper [11], unfortunately the index h in Result 2.1 ran until $s-1$ only, but the proof used s. However, the original Lemma 3.4 in [12] contains the right bound. Note that $h = s$ corresponds to $v = 0$.

Let ℓ_∞ be the line at infinity intersecting the multiset $\mathcal{M}$ in k mod p points. Furthermore, let $\mathcal{M} \setminus \ell_\infty = \{(a_v, b_v)\}_v$ and $\mathcal{M} \cap \ell_\infty = \{(y_i)\}_i$, $(y_i) \neq (\infty)$. Consider the following polynomial:

$$g(X,Y) = \sum_{v=1}^{|\mathcal{M}\setminus\ell_\infty|} (X+a_vY-b_v)^{q-1} + \sum_{y_i\in\mathcal{M}\cap\ell_\infty} (Y-y_i)^{q-1} - |\mathcal{M}| + k = \sum_{i=0}^{q-1} r_i(Y)X^{q-1-i}, \tag{1}$$

Note that $\deg r_i \leq i$.

Lemma 2.3 *Through a point (y) there pass s non-k mod p affine secants of $\mathcal{M}$ if and only if the degree of the greatest common divisor of $g(X,y)$ and $X^q - X$ is $q-s$.*

Proof. To prove this lemma, we only have to show that x is a root of $g(X,y)$ if and only if the line $Y = yX + x$ intersects $\mathcal{M}$ in k mod p points.

Since $a^{q-1} = 1$, if $a \neq 0$ and $0^{q-1} = 0$, for the pair (x,y) the number of zero terms in the first sum is exactly the number of affine points of $\mathcal{M}$ on the line $Y = yX + x$, the rest of the terms are 1. So assume that the ideal point (y) of the line $\ell : Y = yX + x$ is in $\mathcal{M}$ with multiplicity s $(0 \leq s \leq p-1)$. Hence the first sum is $|\mathcal{M}| - k - (|\ell \cap \mathcal{M}| - s)$ (note that $|\mathcal{M} \cap l_\infty| = k$). The second sum is $k - s$. Hence in total we get $|\mathcal{M}| - k - (|\ell \cap \mathcal{M}| - s) + (k - s) - |\mathcal{M}| + k = k - |\ell \cap \mathcal{M}|$ and so the lemma follows. ■

Remark 2.4 Assume that the line at infinity intersects $\mathcal{M}$ in k mod p points and suppose also that there is an ideal point, different from (∞), with s non-k mod p secants through it. Let n_h denote the number of ideal points different from (∞), through which there pass $s-h$ non-k mod p secants of the multiset $\mathcal{M}$. Then Lemma 2.3 and Result 2.1 imply that $\sum_{h=1}^{s} hn_h \leq s(s-1)$.

Lemma 2.5 *Let $\mathcal{M}$ be a multiset in* PG$(2,q)$, $17 < q$, *so that the number of lines intersecting it in non-k mod p points is δ, where $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$. Then the number of non-k mod p secants through any point is at most* $\min(\frac{\delta}{q+1} + 2, \lfloor\sqrt{q}\rfloor + 1)$ *or at least* $\max(q + 1 - (\frac{\delta}{q+1} + 2), q - \lfloor\sqrt{q}\rfloor)$.

PROOF. Pick a point P with s non-k mod p secants through it and let ℓ_∞ be a k mod p secant of $\mathcal{M}$ through P. (If there was no such secant, then the lemma follows immediately.) By Remark 2.4, counting the number of non-k mod p secants through the points of $\ell_\infty \setminus (\infty)$, we get:

$$qs - s(s-1) \leq \delta.$$

Solving the inequality we estimate the discriminant by $1 - \frac{x}{2} - \frac{x^2}{4} \leq \sqrt{1-x}$, which is certainly true when $x < \frac{4}{5}$. In our case $x = \frac{4\delta}{(q+1)^2}$, giving the condition $q > 17$. Hence $s < \frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3} (< \frac{\delta}{q+1} + 2)$ or $s > q+1-(\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3}) (> q - 1 - \frac{\delta}{q+1})$. On the other hand, as the discriminant is larger than $q + 1 - 2(\lfloor\sqrt{q}\rfloor + 2)$ (since $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$), $s < \lfloor\sqrt{q}\rfloor + 2$ or $s > q + 1 - (\lfloor\sqrt{q}\rfloor + 2)$; whence the lemma follows. ■

The next proposition is a generalisation of Lemma 2.5 and follows immediately.

Proposition 2.6 *Let $\mathcal{M}$ be a multiset in* PG$(2, q)$, $17 < q$, *so that the number of lines intersecting it in non-k mod p points is δ, where $\delta < \frac{3}{16}(q + 1)^2$. Then the number of non-k mod p secants through any point is at most $\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3}$ or at least $q + 1 - (\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3})$.* ■

3 Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1: First we show that every line intersecting $\mathcal{M}$ in non-k mod p points contains a point through that there are at least $q + 1 - (\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3})$ lines intersecting $\mathcal{M}$ in non-k mod p points. On the contrary, assume that ℓ is a line intersecting $\mathcal{M}$ in non-k mod p points but containing no such point. Then by Proposition 2.6, through each point of ℓ there pass at most $\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3}$ non-k mod p secants. Hence δ is at most $(q + 1)(\frac{\delta}{q+1} + \frac{2\delta^2}{(q+1)^3} - 1) + 1$. But this is less than δ as $\delta < \sqrt{\frac{q}{2}}(q + 1)$; a contradiction.

It is obvoiuos that to cover every line intersecting $\mathcal{M}$ in non-k mod p points we need at least $\lceil\frac{\delta}{q+1}\rceil$ points. We only need to show that there are less than $\frac{\delta}{q+1} + 1$ such points. Through every such point there are at least

$q+1-(\frac{\delta}{q+1}+\frac{2\delta^2}{(q+1)^3})$ non-k mod p secants, hence if there were at least $\frac{\delta}{q+1}+1$ of them, then

$$\delta \geq (\frac{\delta}{q+1}+1)(q+1-(\frac{\delta}{q+1}+\frac{2\delta^2}{(q+1)^3})) - \binom{\frac{\delta}{q+1}+1}{2}.$$

This is a contradiction since $\delta < \sqrt{\frac{q}{2}}(q+1)$.■

Remark 3.1 It follows from the beginning of the above proof that through each point of S in Theorem 1.1, there pass at least $q+1-(\frac{\delta}{q+1}+\frac{2\delta^2}{(q+1)^3})$ lines intersecting $\mathcal{M}$ in non-k mod p points.

Proposition 3.2 *Let $\mathcal{M}$ be a multiset in* $\mathrm{PG}(2,q)$, $17<q$, *having less than $(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$ non-k mod p secants. Assume that through each point there pass less than $(q-\lfloor\sqrt{q}\rfloor)$ non-k mod p secants. Then the total number δ of lines intersecting $\mathcal{M}$ in non-k mod p points is at most $\lfloor\sqrt{q}\rfloor q-q+2\lfloor\sqrt{q}\rfloor+1$.*

Proof. Assume to the contrary that $\delta > \lfloor\sqrt{q}\rfloor q - q + 2\lfloor\sqrt{q}\rfloor + 1$. Pick a point P and let ℓ_∞ be a k mod p secant of $\mathcal{M}$ through P. Assume that there are s non-k mod p secants through P. If there is a point Q on ℓ_∞ through which there pass at least s non-k mod p secants, then choose the coordinate system so that Q is (∞). Then, by Remark 2.4, counting the number of non-k mod p secants through ℓ, we get a lower bound on δ:

$$(q+1)s - s(s-1) \leq \delta.$$

Since $\delta < (\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$, from the above inequality we get that $s < \lfloor\sqrt{q}\rfloor + 1$ (hence $s \leq \lfloor\sqrt{q}\rfloor$) or $s > q+1-\lfloor\sqrt{q}\rfloor$, but by the assumption of the proposition the latter case cannot occur.

Now we show that through each point there are at most $\lfloor\sqrt{q}\rfloor$ non-k mod p secants. The argument above and Lemma 2.5 show that on each k mod p secant there is at most one point through which there pass $\lfloor\sqrt{q}\rfloor+1$ non-k mod p secants and through the rest of the points there are at most $\lfloor\sqrt{q}\rfloor$ of them. Assume that there is a point R with $\lfloor\sqrt{q}\rfloor+1$ non-k mod p secants. Since $\delta > \lfloor\sqrt{q}\rfloor+1$, we can find a non-$k$ mod p secant ℓ not through R. From above, the number of non-k mod p secants through the intersection point of a k mod p secant on R and ℓ is at most $\lfloor\sqrt{q}\rfloor$. So counting the non-k mod p secants through the points of ℓ, we get at most

$(q - \lfloor\sqrt{q}\rfloor)(\lfloor\sqrt{q}\rfloor - 1) + (\lfloor\sqrt{q}\rfloor + 1)\lfloor\sqrt{q}\rfloor + 1$, which is a contradiction. So there was no point with $\lfloor\sqrt{q}\rfloor + 1$ non-k mod p secants through it.

This means that the non-k mod p secants form a dual $\lfloor\sqrt{q}\rfloor$-arc, hence $\delta \leq (\lfloor\sqrt{q}\rfloor - 1)(q+1) + 1$, which is a contradiction again; whence the proof follows. ■

Property 3.3 *Let $\mathcal{M}$ be a multiset in* PG$(2,q)$, *$q = p^h$, where p is prime. Assume that there are δ lines that intersect $\mathcal{M}$ in non-k mod p points. If through a point there are more than $q/2$ lines intersecting $\mathcal{M}$ in non-k mod p points, then there exists a value r such that the intersection multiplicity of more than $2\frac{\delta}{q+1} + 5$ of these lines is r.*

In Section 3, we are going to show that there are cases when the above property holds automatically.

Theorem 3.4 *Let $\mathcal{M}$ be a multiset in* PG$(2,q)$, *$17 < q$, $q = p^h$, where p is prime. Assume that the number of lines intersecting $\mathcal{M}$ in not k mod p points is δ, where $\delta < (\lfloor\sqrt{q}\rfloor + 1)(q + 1 - \lfloor\sqrt{q}\rfloor)$. Assume furthermore, that Property 3.3 holds. Then there exists a multiset $\mathcal{M}'$ with the property that it intersects every line in k mod p points and the number of different points in $(\mathcal{M} \cup \mathcal{M}') \setminus (\mathcal{M} \cap \mathcal{M}')$ is exactly $\lceil\frac{\delta}{q+1}\rceil$.*

Note that Theorem 3.4 is also valid for $h = 1$ and $h = 2$ (not like Theorem 1.2). Hence, for example, in case $h = 1$ or $h = 2$, if for a given set we know that Property 3.3 holds, then Theorem 3.4 yields a stronger result than Theorem 1.2.

Proof. By Lemma 2.5, through each point there pass either at most $\frac{\delta}{q+1} + 2$ or at least $q - 1 - \frac{\delta}{q+1}$ lines intersecting the multiset $\mathcal{M}$ in non-k mod p points. Let $\mathcal{P}$ be the set containing the points P_i through which there pass at least $q - 1 - \frac{\delta}{q+1}$ non-k mod p points. By Property 3.3, to each point P_i, there is a value k_i, so that more than $\frac{\delta}{q+1} + 2$ lines through P_i intersect $\mathcal{M}$ in k_i mod p points. Add the point $P_1 \in \mathcal{P}$ to the multiset $\mathcal{M}$ with multiplicity $p - k_1$ and denote this new multiset by $\mathcal{M}^{(1)}$. As there were only less than $\frac{\delta}{q+1} + 2$ lines through P_1 which intersect $\mathcal{M}$ in k mod p points and now by Property 3.3, we "repaired" more than $\frac{\delta}{q+1} + 2$ lines, the total number of non-k mod p secants of $\mathcal{M}^{(1)}$ is less than δ. Hence again by Lemma 2.5, through each

point there pass either at most $\frac{\delta}{q+1}+2$ or at least $q-1-\frac{\delta}{q+1}$ lines intersecting the multiset $\mathcal{M}^{(1)}$ in non-k mod p points. So, it follows that there are at most $\frac{\delta}{q+1}+2$ non-k mod p secants of $\mathcal{M}^{(1)}$ through P_1. It is also easy to see that the number of non-k mod p secants of $\mathcal{M}^{(1)}$ is at least $q+1-2(\frac{\delta}{q+1}+2)$ less than that of $\mathcal{M}$. Note also that from the argument above and from Lemma 2.5, it also follows immediately that the set containing the points through which there pass at least $q-1-\frac{\delta}{q+1}$ non-k mod p secants of $\mathcal{M}^{(1)}$ is exactly $\mathcal{P}\setminus P_1$. We add the points of $\mathcal{P}$ one by one to $\mathcal{M}$ as above. At the rth step we want to add the point $P_r\in\mathcal{P}$ to $\mathcal{M}^{(r-1)}$. By Property 3.3 and because of our algorithm, there are at least $2\frac{\delta}{q+1}+5-(r-1)$ lines through P_r intersecting $\mathcal{M}^{(r-1)}$ in k_r mod p points. If $2\frac{\delta}{q+1}+5-(r-1)>\frac{\delta}{q+1}+2$, then we can repeat the argument above and obtain the multiset $\mathcal{M}^{(r)}$. Note that at each step we "repair" at least $q+1-2(\frac{\delta}{q+1}+2)$ lines, hence there can be at most $\frac{\delta}{q+1-2(\frac{\delta}{q+1}+2)}$ steps in our algorithm, so our argument is valid at each step.

Let $\mathcal{M}'$ be the set which we obtain when $\mathcal{P}$ is empty and let δ' be the number of lines intersecting it in non-k mod p points. Proposition 3.2 applies and so $\delta'\le\lfloor\sqrt{q}\rfloor q-q+2\lfloor\sqrt{q}\rfloor+1$. *Our first aim is to show that $\mathcal{M}'$ is a multiset intersecting each line in k mod p points.*

Let P be an arbitrary point with s secants intersecting $\mathcal{M}'$ in not k mod p points, and let ℓ_∞ be a k mod p secant through P. Assume that there is a point on ℓ_∞ with at least s secants intersecting $\mathcal{M}'$ in non-k mod p points. Then as in Proposition 3.2, counting the number of non-k mod p secants through ℓ, we get a lower bound on δ':

$$(q+1)s-s(s-1)\le\delta'.$$

This is a quadratic inequality for s, where the discriminant is larger than $(q+2-2\frac{\delta'+q}{q+1})$. Hence $s<\frac{\delta'+q}{q+1}$ or $s>q+2-\frac{\delta'+q}{q+1}$, but by the construction of $\mathcal{M}'$, the latter case cannot occur.

Now we show that there is no point through which there pass at least $\frac{\delta'+q}{q+1}$ non-k mod p secants. On the contrary, assume that T is a point with $\frac{\delta'+q}{q+1}\le s$ non-k mod p secants. We choose our coordinate system so that the ideal line is a k mod p secant through T and $T\neq(\infty)$. Then from the argument above, through each ideal point, there pass less than $s(\ge\frac{\delta'+q}{q+1})$ non-k mod p secants. First we show that there exists an ideal point through which there pass exactly $(s-1)$ non-k mod p secants. Otherwise, by Remark 2.4, $2(q-1)\le s(s-1)$; but this is a contradiction since $s\le\lfloor\sqrt{q}\rfloor+1$ by

Lemma 2.5. Let (∞) be a point with $(s-1)$ non-k mod p secants. Then as before, we can give a lower bound on the total number of non-k mod p secants of $\mathcal{M}'$:

$$(s-1)+qs-s(s-1)\leq\delta'$$

Bounding the discriminant (from below) by $(q+2-2\frac{\delta'+q}{q+1})$, it follows that $s<\frac{\delta'+q}{q+1}$ or $s>q+2-\frac{\delta'+q}{q+1}$. This is a contradiction, since by assumption, the latter case cannot occur and the first case contradicts our choice for T.

Hence through each point there pass less than $\frac{\delta'+q}{q+1}$ non-k mod p secants. Assume that ℓ is a secant intersecting $\mathcal{M}'$ in non-k mod p points. Then summing up the non-k mod p secants through the points of ℓ we get that $\delta'<(q+1)\frac{\delta'-1}{q+1}+1$, which is a contradiction. So $\mathcal{M}'$ is a multiset intersecting each line in k mod p points.

To finish our proof we only have to show that the number of different points in $(\mathcal{M}\cup\mathcal{M}')\setminus(\mathcal{M}\cap\mathcal{M}')$ is $\lceil\frac{\delta}{q+1}\rceil$. As we saw in the beginning of this proof, the number ε of modified points is smaller than $2\lfloor\sqrt{q}\rfloor$. On the one hand, if we construct $\mathcal{M}$ from the set $\mathcal{M}'$ of k mod p type, then we see that $\delta\geq\varepsilon(q+1-(\varepsilon-1))$. Solving the quadratic inequality we get that $\varepsilon<\lfloor\sqrt{q}\rfloor+1$ or $\varepsilon>q+1-\lfloor\sqrt{q}\rfloor$, but from the argument above this latter case cannot happen. On the other hand, $\delta\leq\varepsilon(q+1)$. From this and the previous inequality (and from $\varepsilon\leq\lfloor\sqrt{q}\rfloor$), we get that $\frac{\delta}{q+1}\leq\varepsilon\leq\frac{\delta}{q+1}+\frac{\lfloor\sqrt{q}\rfloor(\lfloor\sqrt{q}\rfloor-1)}{q+1}$. Hence the theorem follows. ■

Proof of Theorem 1.2 The previous proposition shows that to prove Theorem 1.2, we only have to show that Property 3.3 holds. By the pigeonhole principle, there is a value r, so that the intersection multiplicity of at least $(q-1-\frac{\delta}{q+1})/(p-1)$ of the (non-k mod p) lines with $\mathcal{M}$ is r. When $h>2$ and $q>27$, then this is clearly greater than $2\frac{\delta}{q+1}+5$; hence Property 3.3 holds. In case $h=2$, assumption (2) in the theorem ensures exactly that $(p^2-1-\frac{\delta}{p^2+1})/(p-1)>2\frac{\delta}{p^2+1}+5$ holds, so again the property holds. ■

4 Codewords of $\mathbf{PG}(2,q)$

Definition 4.1 *Let $C_1(2,q)$ be the p-ary linear code generated by the incidence vectors of the lines of* $\mathrm{PG}(2,q)$ *$q=p^h$, p prime. The weight $w(c)$ of a codeword $c \in C_1(2,q)$ is the number of non-zero coordinates. The set of coordinates, where c is non-zero is denoted by supp(c).*

The next theorem is a straightforward corollary of the dual of Theorem 1.1.

Theorem 4.2 *Let c be a codeword of $C_1(2,q)$, with $17<q$, $q=p^h$, p prime. If $w(c)<\sqrt{\frac{q}{2}}(q+1)$, then the points of* $\mathrm{supp}(c)$ *can be covered by $\lceil \frac{w(c)}{q+1} \rceil$ lines.*

Proof. By definition, c is the linear combination of lines l_i of $\mathrm{PG}(2,q)$, that is $c=\sum_i \lambda_i l_i$. For each point P, add the multiplicities λ_i of the lines l_i which pass through P. By definition of the weight, there are exactly $w(c)$ points in $\mathrm{PG}(2,q)$ through which this sum is not 0 mod p. Hence the theorem follows from the dual of Theorem 1.1. ■

Similary, from the dual of Theorem 1.2, we get the following theorem.

Theorem 4.3 *Let c be a codeword of $C_1(2,q)$, with $27<q$, $q=p^h$, p prime. If*

- $w(c)<(\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$, $2<h$, *or*
- $w(c)<\frac{(p-1)(p-4)(p^2+1)}{2p-1}$, *when $h=2$,*

then c is a linear combination of exactly $\lceil \frac{w(c)}{q+1} \rceil$ different lines.

Proof. By definition, c is a linear combination of lines l_i of $\mathrm{PG}(2,q)$, that is $c=\sum_i \lambda_i l_i$. Let $\mathcal{C}$ be the multiset of lines where each line l_i has multiplicity λ_i. The dual of Theorem 1.2 yields that there are exactly $\lceil \frac{w(c)}{q+1} \rceil$ lines m_j with some multiplicity μ_j, such that if we add the lines m_j with multiplicity μ_j to $\mathcal{C}$ then through any point of $\mathrm{PG}(2,q)$, we see 0 mod p lines (counted with multiplicity).

In other words, we get that $c+\sum_{j=1}^{\lceil \frac{w(c)}{q+1} \rceil} \mu_j m_j$ is the $\underline{0}$ codeword. Hence $c=\sum_{j=1}^{\lceil \frac{w(c)}{q+1} \rceil}(p-\mu_j)m_j$. ■

Note that if we investigate proper point sets as codewords, then Property 3.3 holds automatically. More precisely, let B be a proper point set (each point has multiplicity 1), which is a codeword of $C_1(2,q)$. Hence B corresponds to a codeword $c = \sum_i \lambda_i l_i$, where l_i are lines of PG$(2,q)$. Again consider the dual of the multiset of lines where each line l_i has multiplicity λ_i. Then, clearly, there are $w(c)$ lines intersecting this dual set in not 0 mod p point. Furthermore each of these lines has intersection multiplicity 1 mod p (as B is a proper point set) and so Property 3.3 holds; hence we can apply Theorem 3.4.

Theorem 4.4 *Let B be a proper point set in $PG(2,q)$, $17 < q$. Suppose that B is a codeword of the lines of $PG(2,q)$. Assume also that $|B| < (\lfloor\sqrt{q}\rfloor + 1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then B is the linear combination of at most $\lceil\frac{|B|}{q+1}\rceil$ lines.*
■

The following result summarises what was known about small weight codewords.

Result 4.5 *Let c be a non-zero codeword of $C_1(2,q)$, $q = p^h$, p prime. Then*

(1) (Assmus, Key [1]) *$w(c) \geq q+1$. The weight of a codeword is $(q+1)$ if and only if the points corresponding to non-zero coordinates are the $q+1$ points of a line.*

(2) (Chouinard [4]) *There are no codewords with weight in the closed interval $[q+2, 2q-1]$, for $h = 1$.*

(3) (Fack, Fancsali, Storme, Van de Voorde, Winne [6]) *For $h = 1$, the only codewords with weight at most $2p+(p-1)/2$, are the linear combinations of at most two lines; so they have weight $p+1$, $2p$ or $2p+1$. When $h > 1$, the authors exclude some values in the interval $[q+2, 2q-1]$. In particular, they exclude all weights in the interval $[3q/2, 2q-1]$, when $h \geq 4$.*

■

Example 4.6 (Maarten De Boeck, Peter Vandendriessche [2], Example 10.3.4) *Let c be a vector of the vector space $GF(p)^{p^2+p+1}$, $p \neq 2$ a prime, whose positions correspond to the points of* $\mathrm{PG}(2,p)$*, such that*

$$c_P = \begin{cases} a & if\ P = (0,1,a), \\ b & if\ P = (1,0,b), \\ c & if\ P = (1,1,c), \\ 0 & otherwise, \end{cases}$$

where c_P is the value of c at the position corresponding to the point P. Note that the points corresponding to positions with non-zero coordinates belong to the line $m : X_0 = 0$, the line $m' : X_1 = 0$ or the line $m'' : X_0 = X_1$. These three lines are concurrent at the point $(0,0,1)$. Observe $w(c) = 3p - 3$.

Next we generalise the example above. Note that, a collineation of the underlying plane $\mathrm{PG}(2,q)$ induces a permutation on the coordinates of $C_1(2,p)$, which maps codewords to codewords.

Example 4.7 *Let c be the codeword in Example 4.6. Let v_m be the incidence vector of the line m, $v_{m'}$ the incidence vector of the line m' and $v_{m''}$ of the line m'' in Example 4.6. Let $d := \gamma c + \lambda v_m + \lambda' v'_m + \lambda'' v''_m$. Note that $w(d) \leq 3p + 1$ as the points corresponding to non-zero coordinates are on the three lines m, m', m''. Finally, let π be a permutation on the coordinates induced by a projective transformation of the underlying plane $PG(2,p)$. Our general example for codewords with weight at most $3p + 1$ are the codewords d with a permutation π applied on its coordinate positions.*

Theorem 4.8 *Let c be a codeword of $C_1(2,p)$, $p > 17$ prime. If $2p + 1 < w(c) \leq 3p + 1$, then c is either the linear combination of three lines or given by Example 4.7.*

Proof. By Theorem 4.2 (and since two lines can contain at most $2p + 1$ points), $\mathrm{supp}(c)$ can be covered by three lines l_1, l_2, l_3.

Assume that c is in $C^\perp$ and the $l_i s$ pass through the common point P. Note that as c is in $C^\perp$, P is not in $\mathrm{supp}(c)$. First we show that either each multiplicity of the points in $\mathrm{supp}(c)$ are different on each l_i, or the multiplicities of points of $\mathrm{supp}(c)$ on a line l_i are the same. Let S be the set of the points of l_1 that have multiplicity m. Choose a point Q from $l_2 \setminus \{P\}$, with multiplicity m_Q. As c is in $C^\perp$, the multiplicities of the intersection

points of any line with the l_is should add up to 0; hence the projection of S from Q onto l_3 is a set S' of points with multiplicity $-(m_Q + m)$. Note that every point of l_3 outside S' must have multiplicity different from $-(m_Q+m)$. Otherwise, projecting such a point back to l_1 from Q, the projection would have multiplicity m (as c is in the dual code); so it would be in S. Now pick a point R of $l_3 \setminus \{P\}$ with multiplicity n and choose a point Q_R, so that Q_R projects to R in S. From above, we see that there are exactly $|S|$ points on l_3 with multiplicity n (which is the projection of S from Q_R onto l_3). This implies that $l_3 \setminus \{P\}$ is partitioned in sets of size $|S|$. As the number of points of $l_3 \setminus \{P\}$ is a prime, we get that $|S| = 1$ or p. If the multiplicities of points of $\mathrm{supp}(c)$ on a line l_i are the same, then clearly c is a linear combination of the lines l_i.

We show that it is Example 4.7, when each multiplicity of the points in $\mathrm{supp}(c)$ are different on each l_i. As each point on l_i has different multiplicity, let us choose our coordinate system, so that P is the point $(0, 0, 1)$. The point of l_1 with multiplicity 0 is the point $(0, 1, 0)$, the point of l_3 with multiplicity 0 is the point $(1, 0, 0)$ and the point of l_2 with multiplicity -1 is the point $(1, 1, 1)$. Now we use the fact again that c is in the dual code. Hence from the line $[1, 0, 0]$ we get that the point $(0, 1, 1)$ has multiplicity 1. Examining line $[0, 1, 0]$ we get that the point $(1, 0, 1)$ has multiplicity 1. Similarly if the point $(a, a, 1)$ has multiplicity $-m$, we see that the points $(0, a, 1)$ and $(a, 0, 1)$ have the same multiplicity, namely m. Considering the line $< (0, 1, 1), (1, 0, 1) >$ we see that $(1/2, 1/2, 1)$ has multiplicity -2. So from above, the multiplicity of $(1/2, 0, 1)$ and $(0, 1/2, 1)$ are 2. Now considering the line $< (0, 1/2, 1), (1, 0, 1) >$ we see that $(1/3, 1/3, 1)$ has multiplicity -3 and so $(1/3, 0, 1)$ and $(0, 1/3, 1)$ have multiplicity 3. Similarly, considering the line $< (0, 1/n, 1), (1, 0, 1) >$ we see that $(1/(n + 1), 1/(n + 1), 1)$ has multiplicity $-(n + 1)$ and so $(1/(n + 1), 0, 1)$ and $(0, 1/(n + 1), 1)$ have multiplicity $(n + 1)$; which shows that in this case c is of Example 4.7.

Now assume that c is in $C^{\perp}$, but the lines l_i are not concurrent. Assume that the intersection point Q of $l_1 \cap l_2$ has multiplicity m. Considering the lines through Q, we see that at least $(p - 1)$ point on l_3 have multiplicity $-m$. Similarly, we see at least $(p - 1)$ points on l_2 and $(p - 1)$ points on l_3 that have the same multiplicity. Hence taking the linear combination of l_is with the right multiplicity, we get a codeword that only differs from c in at most 3 positions (at the three intersection points of the lines l_i). There are no codewords with weight larger than 0 but at most 3, which means that c must be the linear combination of the l_is.

Now assume that c is not in the dual code. As the dimension of the code is one larger than the dimension of the dual code (see [8] and [10]), and l_1 is not in the dual code, there exists a multiplicity λ, so that $c+\lambda l_1$ is in the dual code. It is clear that the weight of $c+\lambda l_1$ is $\leq 3p$, and clearly $\mathrm{supp}(c+\lambda l_1)$ can be covered by the three lines l_1, l_2, l_3. Now the result follows from the argument above when the weight of $c+\lambda l_1$ is greater than $2p$, and from Result 4.5 otherwise. ■

Corollary 4.9 *For any integer $0 < k+1 < \sqrt{\frac{q}{2}}$, there is no codeword whose weight lies in the interval $(kq+1, ((k+1)q - \frac{3}{2}k^2 - \frac{5}{2}k - 1)$, for $q > 17$.*

Proof. Suppose to the contrary that c is a codeword whose weight lies in the interval $(kq+1, ((k+1)q - \frac{3}{2}k^2 - \frac{5}{2}k - 1)$. Then by Theorem 4.2, $\mathrm{supp}(c)$ can be covered by the set $k+1$ lines l_i. It follows from Remark 3.1, that the number of points of $\mathrm{supp}(c)$ on a line l_i is at least $q-k-1$. Hence $w(c)$ is at least $(k+1)(q-k-1) - \binom{k+1}{2}$.

Corollary 4.10 *Let c be a codeword of $C(2,p)$, $p > 17$ prime. If $w(c) \leq 4p - 22$, then c is either the linear combination of at most three lines or Example 4.7.*

Proof. It follows from Corollary 4.9, Theorem 4.8 and Result 4.5. ■

Acknowledgment. The results on small weight codewords were inspired by conversation with András Gács. We gratefully dedicate this paper to his memory.

References

[1] E.F. Assmus, J.D. Key, *Designs and their Codes*, Cambridge University Press, 1992.

[2] M. De Boeck, *Intersection problems in finite geometries*, Ph.D. Thesis, Universiteit Gent 2014.

[3] E. Boros, T. Szőnyi, On the sharpness of the theorem of B. Segre, *Combinatorica* **6** (1986), 261–268.

[4] K.L. Chouinard, *Weight distributions of codes from planes*, Ph.D Thesis, University of Virginia 2000.

[5] G. Ebert, Partitioning projective geometries into caps, *Canad. J. Math.* **37** (1985), 1163–1175.

[6] V. Fack, Sz.L. Fancsali, L. Storme, G. Van de Voorde, J. Winne, Small weight codewords in the codes arising from Desarguesian projective planes, *Des. Codes Cryptogr.*, **46** (2008), pp. 2543.

[7] J.C. Fisher, J.W.P. Hirschfeld, J.A. Thas, Complete arcs on planes of square order, *Ann. Discrete Math.* **30** (1986), 243–250.

[8] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes, *Hiroshima Math. J.* **3** (1973), 153–226.

[9] B.C. Kestenband, A family of complete arcs in finite projective planes, *Colloq. Math.* **57** (1987), 59–67.

[10] F.J. MacWilliams, H.B. Mann, On the p-rank of the design matrix of a difference set, *Information and Control* **12** (1968)474–488.

[11] T. Szőnyi, Zs. Weiner, On the stability of the sets of even type, *Adv. Math.* **267** (2014), 381–394.

[12] Zs. Weiner, On (k, p^e)-arcs in Galois planes of order p^h, *Finite Fields and Appl.*, **10**, (2004), no. 3, 390–404.

Authors address:
Tamás Szőnyi
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY
e-mail: szonyi@cs.elte.hu

Tamás Szőnyi, Zsuzsa Weiner
MTA-ELTE Geometric and Algebraic Combinatorics Research Group,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY
e-mail: zsuzsa.weiner@gmail.com

Zsuzsa Weiner
Prezi.com
H-1065 Budapest, Nagymező utca 54-56, HUNGARY