THE GEOMETRY OF TWO-WEIGHT CODES

R. CALDERBANK AND W. M. KANTOR

ABSTRACT

We survey the relationships between two-weight linear $[n, k]$ codes over GF(q), projective (n, k, h_1, h_2) sets in PG($k-1, q$), and certain strongly regular graphs. We also describe and tabulate essentially all the known examples.

1. *Introduction*

This paper surveys relationships between subsets of finite projective spaces, strongly regular graphs, and linear codes. Each subject is interesting in itself and has attracted the attention of finite geometers, combinatorists or coding theorists. What is remarkable is that results from one area can immediately be translated into the other two. We have sought to explain the relationships involved in this translation and to describe and tabulate all the known examples. Our goal is to stimulate further research by making specialists in each area aware of a wider variety of techniques.

Delsarte **[14, 15, 16, 17]** was the first to investigate the relationships between the projective sets, graphs, and linear codes that are considered here. The relationships are a special case of his more general theory of association schemes arising in coding theory. Much of this survey merely describes his results, though we provide different proofs. However, new results have since appeared and additional examples have been noticed, many of them geometric.

Section 2 contains basic definitions arranged by subject. The definitions are intended to make subsequent sections more accessible to specialists in finite projective geometry, combinatorics, or coding theory. The reader need not be familiar with all three subjects in order to understand this survey.

In Section 3 we prove the equivalence of two-weight codes, projective (n, k, h_1, h_2) sets and certain strongly regular graphs. Section 4 describes a theorem of Goethals and van Tilborg that characterizes a two-weight code C in terms of the dual code $C^{\perp}$. In Section 5 we describe the dual of a projective (n, k, h_1, h_2) set, and the projective dual of a two-weight code. Section 6 shows how to construct new two-weight codes from a given two-weight code by changing the underlying field.

In the second half of this survey we describe essentially all the known examples of two-weight codes. The most visible examples of two-weight $[n, k]$ codes arise from subspaces of GF$(q)^k$, and these are described in Section 7. There are examples that occur when the dimension k is 3 or 4 and that do not generalize to higher dimensions. These are discussed in Section 8. In Section 9 we describe the cyclotomic examples. These are two-weight $[n, k]$ codes constructed from subgroups of GF$(q^k)^*$. Section 10 contains examples arising from groups of collineations of PG$(k-1, q)$ with exactly two point orbits. Examples that do not fit into any of the above sections are collected in Section 11.

Received 30 April 1982; revised 27 September 1985.

1980 *Mathematics Subject Classification* 05B25, 51E20, 94B05.

Bull. London Math. Soc. 18 (1986) 97–122

Section 12 contains theorems characterizing projective (n, k, h_1, h_2) sets subject to some additional geometric constraint. Theorem 12.9 is a new result. We conclude this survey by tabulating the parameters of essentially all the known two-weight codes and the corresponding strongly regular graphs.

2. *Definitions*

2A: *Two-weight codes.* Let $q = p^m$, where p is prime. If $u = (u_i)$, $v = (v_i)$ are vectors in $GF(q)^n$ then the dot product $u \cdot v$ is given by $u \cdot v = \sum_{i=1}^{n} u_i v_i$. An $[n, k]$ *code* C over $GF(q)$ is a k-dimensional subspace of $GF(q)^n$. Vectors in C are called *codewords*. The *dual code* $C^{\perp} = \{v \in GF(q)^n \mid v \cdot C = 0\}$; it is an $[n, n-k]$ code. The *weight* $\mathrm{wt}(x)$ of a vector x in $GF(q)^n$ is the number of non-zero entries. The *weight enumerator* $W_C(x, y)$ of C is the polynomial

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where A_i is the number of codewords of weight i. The MacWilliams Identities [**43**, Chapter 5] relate the weight enumerator of C to that of $C^{\perp}$ as follows:

$$W_{C^{\perp}}(x, y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y). \tag{2.1}$$

A *two-weight code* is a code C for which $|\{i \mid i \neq 0 \text{ and } A_i \neq 0\}| = 2$.

The distance $d(x, y)$ between two vectors x and y in $GF(q)^n$ is the number of entries where x and y differ. Thus $d(x, y) = \mathrm{wt}(x-y)$ and the minimum distance between two codewords is the minimum weight among all non-zero codewords. A code C is said to be *an* $[n, k, d]$ *code* if d is the minimum non-zero weight in C. If $e = [\frac{1}{2}(d-1)]$ then C is also said to be *e-error-correcting*.

If C is an $[n, k]$ code over $GF(q)$ then there exist linear functionals

$$f_i : GF(q)^k \longrightarrow GF(q),\ i = 1, \ldots, n$$

such that

$$C = \{(f_1(x), \ldots, f_n(x)) \mid x \in GF(q)^k\}. \tag{2.2}$$

Let $B(x, y)$ be any non-singular bilinear form on $GF(q)^k$. Then there exist $y_1, \ldots, y_n$ in $GF(q)^k$ such that $f_i(x) = B(x, y_i)$ for $i = 1, \ldots, n$. If $B(x, y) = x \cdot y$ is the dot product then

$$C = \{(x \cdot y_1, \ldots, x \cdot y_n) \mid x \in GF(q)^k\}. \tag{2.3}$$

Since $\dim(C) = k$ the vectors $y_1, \ldots, y_n$ span $GF(q)^k$. If no two of the vectors $y_1, \ldots, y_n$ are dependent then the code C is said to be *projective*. Thus C is projective if and only if the minimum weight in the dual code $C^{\perp}$ is at least 3.

An $n \times n$ *monomial matrix* M is a matrix of the form $M = DP$, where D is an $n \times n$ diagonal matrix and P is an $n \times n$ permutation matrix. Two $[n, k]$ codes C and C' over $GF(q)$ are said to be *equivalent* if there exists an $n \times n$ monomial matrix M such that $MC = C'$. Note that monomial transformations are precisely those linear transformations that preserve the metric d on $GF(q)^n$.

2B: *Projective* (n, k, h_1, h_2) *sets. A projective* (n, k, h_1, h_2) *set* $\boldsymbol{O}$ is a proper, non-empty set of n points of the projective space $PG(k-1, q)$ with the property that every hyperplane meets O in h_1 points or in h_2 points. The complement of O in PG$(k-1, q)$ is a projective

$$\left(\left(\frac{q^k-1}{q-1}\right)-n,\, k,\, \left(\frac{q^{k-1}-1}{q-1}\right)-h_1,\, \left(\frac{q^{k-1}-1}{q-1}\right)-h_2\right) \text{ set.}$$

Let $O = \{\langle y_i\rangle \mid i = 1, \ldots, n\}$ and $O' = \{\langle y_i'\rangle \mid i = 1, \ldots, n\}$ be two projective (n, k, h_1, h_2) sets. Then O and O' are said to be *equivalent* if there exists $A \in \mathrm{GL}(n, q)$ such that $A(O) = O'$. If O and O' span PG$(k-1, q)$ then O and O' determine $[n, k]$ codes C and C', respectively, via (2.3). We remark that O and O' are equivalent as projective sets if and only if C and C' are equivalent as codes. (Of course this is true not only for two-weight codes but for any projective codes.) It is possible to generalize the definitions of equivalence of codes and of projective sets by allowing automorphisms of GF(q). This corresponds to the observation that C and C^σ are essentially the same for each $\sigma \in \mathrm{Aut}\ \mathrm{GF}(q)$.

2C: *Strongly regular graphs*. A connected graph on N vertices is said to be *strongly regular* with parameters (N, K, λ, μ) if it is regular with valency K and if the number of vertices joined to two given vertices is λ or μ according as the two given vertices are adjacent or non-adjacent; we shall always exclude the null and complete graphs. We label the vertices $v_1, \ldots, v_N$, and we define an $N \times N$ integral matrix $A = (a_{ij})$ by setting

$$a_{ij} = \begin{cases} 1, & \text{if } v_i \text{ and } v_j \text{ are adjacent} \\ 0, & \text{otherwise.} \end{cases}$$

The matrix A is the *adjacency matrix* of the graph. If I is the $N \times N$ identity matrix and if J is the $N \times N$ matrix with every entry 1 then

$$AJ = JA = KJ \quad \text{and} \quad A^2 - (\lambda-\mu)A - (K-\mu)I = \mu J. \tag{2.4}$$

Multiplying the second equation by J and comparing coefficients gives

$$K(K-\lambda-1) = (N-K-1)\mu. \tag{2.5}$$

The eigenvalues of A are K, ρ_1, and ρ_2 where

$$\rho_1, \rho_2 = \tfrac{1}{2}((\lambda-\mu) \pm \sqrt{d})$$

and

$$d = (\lambda-\mu)^2 + 4(K-\mu).$$

The multiplicities of k, ρ_1 and ρ_2 are 1, e_1, and e_2, respectively, where

$$e_1, e_2 = \frac{1}{2}\left((N-1) \pm \frac{(N-1)(\lambda-\mu)+2K}{\sqrt{d}}\right). \tag{2.7}$$

Equation (2.7) is called the *integrality* or *rationality condition* because e_1 and e_2 must be integers.

2D: *Rank* 3 *groups*. Let G be a permutation group acting transitively on a set X. The group G is a *rank* 3 *group* if it has exactly three orbits on $X \times X$. Suppose $|G|$ is even and let R be an orbit of G on $X \times X$ other than $\{(x, x) \mid x \in X\}$. If $(x, y) \in R$ then $(y, x) \in R$. The orbit R determines a graph on the elements of X in which two elements x, y are joined if and only if $(x, y) \in R$. The group G acts transitively on ordered pairs of adjacent vertices and on ordered pairs of non-adjacent vertices. It follows that the graph is strongly regular.

2E: $\{\lambda_1, \lambda_2\}$ *difference sets*. Let Ω be a proper set of non-zero vectors in a vector space V over GF(q). Then Ω is a $\{\lambda_1, \lambda_2\}$ *difference set* over GF(q) if $\mathrm{GF}(q)^*\Omega = \Omega$ and if, for $v \in V$, $v \neq 0$, we have

$$|\{(x,y) \mid x, y \in \Omega \quad \text{and} \quad x-y=v\}| = \begin{cases} \lambda_1, & \text{if } v \in \Omega \\ \lambda_2, & \text{if } v \notin \Omega,\ v \neq 0. \end{cases}$$

3. *Fundamental correspondences*

In this section we shall describe the equivalence of two-weight codes, projective (n, k, h_1, h_2) sets, $\{\lambda_1, \lambda_2\}$ difference sets and certain strongly regular graphs.

THEOREM 3.1. (1) *If the code C defined by* (2.3) *is a projective two-weight* $[n, k]$ *code then* $\{\langle y_i \rangle \mid i = 1, \ldots, n\}$ *is a projective* $(n, k, n-w_1, n-w_2)$ *set that spans* PG$(k-1, q)$.

(2) *Conversely if* $\{\langle y_i \rangle \mid i = 1, \ldots, n\}$ *is a projective* $(n, k, n-w_1, n-w_2)$ *set that spans* PG$(k-1, q)$ *then the code C defined by* (2.3) *is a projective two-weight* $[n, k]$ *code with weights w_1 and w_2.*

Proof. Let x be any non-zero vector in $\mathrm{GF}(q)^k$. If $x^\perp = \{y \in \mathrm{GF}(q)^k \mid x \cdot y = 0\}$ then $n - |x^\perp \cap \{y_1, \ldots, y_n\}|$ is the weight of the codeword $(x \cdot y_1, \ldots, x \cdot y_n)$.

Note that if $\boldsymbol{O} = \{\langle y_i \rangle \mid i = 1, \ldots, n\}$ does not span PG$(k-1, q)$ then the points of $\boldsymbol{O}$ are in a PG(r, q) subgeometry of PG$(k-1, q)$.

Let $V = \mathrm{GF}(q)^k$. Let $\Omega \subseteq V$ and suppose that $\Omega = -\Omega$ and $0 \notin \Omega$. We define a graph $G(\Omega)$ with vertices the vectors of V and where two vertices are joined if and only if their difference is in Ω.

THEOREM 3.2. *Let* $\boldsymbol{O} = \{\langle y_i \rangle \mid i = 1, \ldots, n\}$ *be a proper non-empty set of points of* PG$(k-1, q)$, *and let* $\Omega = \{v \in V \mid \langle v \rangle \in \boldsymbol{O}\}$. *If* $\boldsymbol{O}$ *spans* PG$(k-1, q)$ *then the following are equivalent:*

(1) Ω *is a* $\{\lambda_1, \lambda_2\}$ *difference set for some* λ_1, λ_2,

(2) $G(\Omega)$ *is a strongly regular graph,*

(3) $\boldsymbol{O}$ *is a projective* $(n, k, n-w_1, n-w_2)$ *set for some* w_1, w_2.

Proof. It follows directly from the definitions that (1) and (2) are equivalent. Delsarte essentially proves that (2) and (3) are equivalent in [15]. We outline the proof because it contains information needed later.

Let $N = q^k$. We order the vectors $v_1, \ldots, v_N$ of V and use this ordering to define the adjacency matrix $A = (a_{ij})$ of $G(\Omega)$. Let $\chi : \mathrm{GF}(q)^+ \to \mathbb{C}^*$ be any non-principal character of the additive group $\mathrm{GF}(q)^+$. If $u \in V$ then the map $\chi_u(v) = \chi(u \cdot v)$ for all $v \in V$ is a character of the abelian group V. We define a vector $e_v \in \mathbb{C}^N$ by setting

$$(e_v)_i = \chi_v(v_i) \quad \text{for } i = 1, \ldots, N. \tag{3.3}$$

LEMMA 3.4. *The vector e_v is an eigenvector of A with eigenvalue* $(q-1)(n-w_v)-w_v$, *where* $(q-1)(n-w_v) = |v^\perp \cap \Omega|$. *The vectors* e_v, $v \in V$, *are a basis of* $\mathbb{C}^N$.

Proof. We have

$$(e_v A)_j = \sum_i \chi_v(v_i)\, a_{ij} = \sum_{v_i - v_j \in \Omega} \chi_v(v_i) = \sum_{u \in \Omega} \chi_v(u+v_j)$$
$$= \chi_v(v_j) \Big(\sum_{u \in \Omega} \chi_v(u) \Big) = (e_v)_j \Big(\sum_{u \in \Omega} \chi_v(u) \Big),$$

where

$$\sum_{u\in\Omega}\chi_v(u)=\sum_{\substack{u\in\Omega\\ u\cdot v=0}}\chi_v(u)+\sum_{\substack{u\in\Omega\\ u\cdot v=1}}\Big(\sum_{\alpha\in GF(q)^*}\chi_v(\alpha u)\Big)$$
$$=(q-1)(n-w_v)-w_v.$$

Finally

$$e_v\cdot e_w=\sum_{i=1}^{N}\chi(v\cdot v_i)\chi(w\cdot v_i)=\sum_{i=1}^{N}\chi((v+w)\cdot v_i)$$
$$=\begin{cases}N, & \text{if } v+w=0,\\ 0, & \text{otherwise.}\end{cases}$$

This completes the proof of the lemma.

If $G(\Omega)$ is strongly regular then A has just 3 eigenvalues and Lemma 3.4 implies that (3) holds. Conversely, if (3) holds then A has 3 distinct eigenvalues and the multiplicity of the valency $n(q-1)$ of $G(\Omega)$ is 1. The adjacency matrix A satisfies an equation of the form $A^2=aI+bA+cJ$ for scalars a, b, and c and this readily yields the strong regularity asserted in Theorem 3.2.

COROLLARY 3.5. *Let $O=\{\langle y_i\rangle \mid i,\ldots,n\}$ be as in Theorem* 3.2, *let C be the code defined by* (2.3), *and suppose that conditions* (1), (2), *and* (3) *of Theorem* 3.2 *hold. Then the eigenvalues of A are $n(q-1)$, $n(q-1)-qw_1$, and $n(q-1)-qw_2$, with multiplicities* 1, *A_{w_1}, and A_{w_2} respectively, where A_{w_i} is the number of codewords of C with weight w_i. If $w_2>w_1$ then*

$$A_{w_1}=\frac{1}{(w_2-w_1)}(w_2(q^k-1)-nq^{k-1}(q-1)). \tag{3.6}$$

Proof. The only part that is not immediate is (3.6), but we shall postpone the proof of (3.6) until (5.6).

COROLLARY 3.7. *If conditions* (1), (2), *and* (3) *of Theorem* 3.2 *hold then the parameters (N,K,λ,μ) of $G(\Omega)$ are given by*

$$N=q^k,$$
$$K=n(q-1),$$
$$\lambda=K^2+3K-q(w_1+w_2)-Kq(w_1+w_2)+q^2w_1w_2,$$

and

$$\mu=\frac{q^2w_1w_2}{q^k}=K^2+K-Kq(w_1+w_2)+q^2w_1w_2.$$

Proof. By Corollary 3.5

$$(A-(n(q-1)-qw_1)I)(A-(n(q-1)-qw_2)I)=cJ \tag{3.8}$$

for some constant c. Premultiplying both sides by J we obtain $c=q^2w_1w_2/q^k$. Now compute λ and μ by comparing (3.8) with (2.4).

COROLLARY 3.9. *If $G(\Omega)$ is strongly regular with parameters (N,K,λ,μ) as in* (3.7) *then*

$$K^2+K-Kq(w_1+w_2)+(q^k-1)\frac{w_1w_2}{q^{k-2}}=0, \tag{3.10}$$

and

$$q(w_2-w_1)=((\lambda-\mu)^2+4(k-\mu))^{\frac{1}{2}}. \tag{3.11}$$

Proof. Equation (3.10) follows immediately from (3.7), but (3.10) and (3.11) also follow from (2.5) and (2.6) respectively. We remark that, given (3.7), conditions (3.10) and (3.11) are equivalent.

COROLLARY 3.12. *Let O be as in Theorem* 3.2. *Then conditions* (1), (2), *and* (3) *of Theorem* 3.2 *hold if and only if there exist constants E and E′ such that*

(1) *if $\langle v\rangle$ is a point of* $\mathrm{PG}(k-1, q)$ *not in O then $\langle v\rangle$ is collinear with E pairs of points of O, and*

(2) *if $\langle v\rangle \in O$ then $\langle v\rangle$ is collinear with E′ pairs of points of $O\backslash\{\langle v\rangle\}$.*

In that case $\mu = 2E$ and $\lambda = 2E' + (q-2)$.

Proof. If $\langle x\rangle$, $\langle y\rangle$, and $\langle z\rangle$ are distinct collinear points of $\mathrm{PG}(k-1, q)$ then there exist unique scalars $s, t \in \mathrm{GF}(q)$ such that $x = sy + tz$. There also exist $q-2$ scalars $u \in \mathrm{GF}(q)\backslash\{0, 1\}$ such that $x = ux + (1-u)x$. It follows that (1) and (2) hold if and only if $G(\Omega)$ is strongly regular, and in that case $\mu = 2E$ and $\lambda = 2E' + (q-2)$.

PROPOSITION 3.13. *There are integers j and t such that, if $w_2 > w_1$, then $w_1 = p^j t$ and $w_2 = p^j(t+1)$.*

The proof is postponed until (5.5). We remark that the characterizations obtained in Section 12 rely heavily on (3.11) and (3.13).

4. *Uniformly packed codes*

In this section we describe how a two-weight code is characterized by metric properties of the dual code.

Given a vector v in $\mathrm{GF}(q)^n$, the sphere $S_r(v)$ of radius r, centered at v, is given by $S_r(v) = \{w \in \mathrm{GF}(q)^n \mid d(v, w) \leqslant r\}$. If $C^\perp$ is an e-error-correcting code then the spheres $S_e(c)$, $c \in C^\perp$, are pairwise disjoint. The code $C^\perp$ is *perfect* if the union of the spheres $S_e(c)$, $c \in C^\perp$, exhausts $\mathrm{GF}(q)^n$. The following characterization of perfect codes is due to MacWilliams ([**41**, **42**]).

THEOREM 4.1. *Let $C^\perp$ be an e-error-correcting code. Then $C^\perp$ is perfect if and only if there are exactly e non-zero weights in the dual code C.*

Perfect codes have been classified by van Lint and Tietäväinen (see [**37**, **52**]). The only perfect 2-error-correcting codes are the ternary [11, 6, 5] Golay code and the binary repetition code $\{(0, 0, 0, 0, 0), (1, 1, 1, 1, 1)\}$.

Uniformly packed codes are a generalization of perfect codes and were introduced by Semakov, Zinovjev, and Zaitzev in [**49**]. Given $v \in \mathrm{GF}(q)^n$, let $B(v, i)$ be the number of codewords at distance i from v.

DEFINITION. Let $C^\perp$ be an e-error-correcting code. Then $C^\perp$ is *uniformly packed* with parameters λ and μ if the following hold for all $x \in \mathrm{GF}(q)^n$:

(1) if $d(x, C^\perp) = e$, then $B(x, e+1) = \lambda$,

(2) if $d(x, C^\perp) \geqslant e+1$, then $B(x, e+1) = \mu$, and

(3) $\lambda < \dfrac{(n-e)(q-1)}{e+1}$.

If d is the minimum distance in $C^{\perp}$ then $d = 2e+2$ if and only if $\lambda = 0$. If $C^{\perp}$ is an arbitrary e-error-correcting code then a counting argument proves that if $d(x, C^{\perp}) = e$ then

$$B(x, e+1) \leqslant \frac{(n-e)(q-1)}{e+1}.$$

Goethals and van Tilborg [29] prove that $C^{\perp}$ is perfect if and only if (1) and (2) hold and $\lambda = (n-e)(q-1)/(e+1)$. They also prove the following analogue of Theorem 4.1.

THEOREM 4.2. *Let $C^{\perp}$ be an e-error-correcting code. Then $C^{\perp}$ is uniformly packed if and only if there are exactly $e+1$ non-zero weights in the dual code C.*

Van Tilborg [53] proved that there are no uniformly packed e-error-correcting codes for $e \geqslant 4$, and that the extended binary Golay code is the only binary 3-error-correcting uniformly packed code. However many examples exist when $e = 1$:

COROLLARY 4.3. *Let $C^{\perp}$ be a 1-error-correcting code. Then $C^{\perp}$ is uniformly packed if and only if C is a two-weight code.*

5. *Duality*

In this section we describe the dual of a projective (n, k, h_1, h_2) set, and the projective dual of a two-weight code.

Given a positive integer l, set

$$b_l = \frac{q^l - 1}{q-1}.$$

Let $\boldsymbol{O}$ be a projective $(n, k, n-w_1, n-w_2)$ set in $PG(k-1, q)$. Recall that the complement $\boldsymbol{O}'$ of $\boldsymbol{O}$ in $PG(k-1, q)$ is a projective $(n', k, n'-w_1', n'-w_2')$ set, where

$$n' = b_k - n \quad \text{and} \quad w_i + w_i' = q^{k-1}, \quad \text{for } i = 1, 2. \tag{5.1}$$

Let $\boldsymbol{H}_i$ be the set of all hyperplanes H of $PG(k-1, q)$ such that $|H \cap \boldsymbol{O}| = n - w_i$. Then $\boldsymbol{O}$ determines a two-weight code C by (2.3) and $\boldsymbol{H}_i$ determines the set of codewords of weight w_i in C. If $B_i = |\boldsymbol{H}_i|$ then $(q-1)B_i = A_{w_i}$, where A_{w_i} is the number of codewords of weight w_i in C.

THEOREM 5.2. *The set $\boldsymbol{H}_i$ is a projective (B_i, k, a_i, a_i') set in the dual of the original projective space, where*

$$(w_j' - w_i')\, a_i = w_j'\, b_{k-1} - n' q^{k-2}, \tag{5.3}$$

and

$$(w_j - w_i)\, a_i' = w_j\, b_{k-1} - n q^{k-2}, \tag{5.4}$$

for $j = 3-i$ and $i = 1, 2$.

Proof. Fix $x \in \boldsymbol{O}'$ and let a_i' be the number of hyperplanes in $\boldsymbol{H}_i$ that contain x. Then $a_1' + a_2' = b_{k-1}$, and counting the pairs (y, H) where $y \in \boldsymbol{O}$ and H is a hyperplane containing x and y we obtain

$$a_1'(n-w_1) + a_2'(n-w_2) = n b_{k-2}.$$

It follows that a_i' does not depend on x and that (5.4) holds. Let $y \in \boldsymbol{O}$ and let a_i be the number of hyperplanes in $\boldsymbol{H}_i$ that contain y. By symmetry it follows that a_i does not depend on y and that (5.3) holds.

COROLLARY 5.5. *There are integers j and t such that, if $w_2 > w_1$, then $w_1 = p^j t$ and $w_2 = p^j(t+1)$.*

Proof. Together (5.1), (5.3), and (5.4) imply $(w_2 - w_1)(a_1 - a_1') = q^{k-2}$ and so $w_2 - w_1 = p^j$ for some integer j. Now (5.4) implies $(w_2 - w_1) \mid w_2$, and the result follows.

We remark that $w_2 - w_1$ need not be a power of q (see Examples TF1, TF1^d, TF2, TF2^d, RT3, and FE3).

COROLLARY 5.6.

$$A_{w_1} = (q-1)|\boldsymbol{H}_1| = \frac{1}{(w_2 - w_1)}(w_2(q^k - 1) - nq^{k-1}(q-1)).$$

Proof. Since $|\boldsymbol{H}_1|(b_{k-1} - (n - w_1)) = n'a_1'$ and since $|\boldsymbol{H}_1|(n - w_1) = na_1$ we have $|\boldsymbol{H}_1| = n'a_1' + na_1$. Now expand this using (5.1), (5.4), and the identity $(w_2 - w_1)(a_1 - a_1') = q^{k-2}$.

We remark that A_{w_1} can be calculated directly from the MacWilliams Identities (2.1) using the fact that the minimum weight in the dual code $C^{\perp}$ is at least 3. Since A_{w_1} is the multiplicity of the eigenvalue $n(q-1) - qw_1$ of the adjacency matrix A of the graph $G(\Omega)$ it can also be calculated via (2.7).

If there exists a correlation Θ of $PG(k-1, q)$ such that $\Theta(\boldsymbol{O}) = \boldsymbol{H}_1$ or $\boldsymbol{H}_2$ then $\boldsymbol{O}$ and the two-weight code determined by $\boldsymbol{O}$ are said to be *projectively self-dual.* Clearly $n = A_{w_1}/(q-1)$ or $A_{w_2}/(q-1)$ is a necessary condition for projective self duality; but it is not sufficient.

THEOREM 5.7. *Let G be the graph with vertices the codewords of C in which two codewords c and d are joined if and only if* $\mathrm{wt}(c-d) = w_1$. *Then* $G \cong G(\Omega')$, *where* $\Omega' = \{x \in V \mid x^{\perp} \in \boldsymbol{H}_1\}$. *In particular, G is strongly regular.*

Proof. The isomorphism follows immediately from the definitions of G and Ω'. Strong regularity is then a consequence of (5.2) and (3.2). (A different proof is given by Delsarte in [**14**].)

A strongly regular graph may be regarded as a symmetric association scheme with two classes (see [**4, 16**]). If (V, R) is the association scheme corresponding to $G(\Omega)$ then $R = \{R_0, R_1, R_2\}$ where $R_0 = \{(v,v) \mid v \in V\}$, $R_1 = \{(v,w) \mid v - w \in \Omega\}$ and $R_2 = (V \times V) \backslash (R_0 \cup R_1)$. If A is the adjacency matrix of $G(\Omega)$ then, by (2.4), I, J, and A span a three-dimensional complex algebra. This algebra is the *Bose–Mesner algebra of* (V, R) ([**3, 16**]). The hermitian matrix $S = (\chi_v(u))_{u, v \in V}$ diagonalizes this algebra. The dual association scheme with respect to $0 \in V$ and to S is defined to have $R' = \{R_0', R_1', R_2'\}$, where $R_0' = R_0$, $R_1' = \{(v,w) \mid v - w \in \Omega'\}$, and

$$R_2' = (V \times V) \backslash (R_0' \cup R_1').$$

(See [15, p. 23].) Alternatively, we may define the dual association scheme in terms of the character group $V^* = \{\chi_v \mid v \in V\}$: it is the pair (V^*, R^*) where $R^* = (R_0^*, R_1^*, R_2^*\}$ and $R_0^* = \{(g,g) \mid g \in V^*]$, $R_1^* = \{(\chi_v, \chi_w) \mid v-w \in \Omega'\}$ and $R_2^* = (V^* \times V^*)\backslash(R_0^* \cup R_1^*)$.

6. *Field changes*

In this section we show how to construct new two-weight codes from a given two-weight code by changing the underlying field.

THEOREM 6.1. *Let C be a projective two-weight* $[n,k]$ *code over* GF(q), *with weights* w_1 *and* w_2. *Let* GF(q_0) *be a subfield of* GF(q) *and let* $q = q_0^r$. *Then C canonically determines a projective two-weight* $[n', kr]$ *code* C' *over* GF(q_0) *with weights* w_1' *and* w_2', *where*

$$n' = \frac{(q-1)n}{q_0-1}, \quad w_1' = \frac{qw_1}{q_0}, \quad \textit{and} \quad w_2' = \frac{qw_2}{q_0}.$$

Proof. Let $V = \mathrm{GF}(q)^k$. By (3.1) there exists a set $\boldsymbol{O} = \{\langle y_i \rangle \mid i = 1, \ldots, n\}$ of n distinct points of PG($k-1$, q) such that $C = \{(x \cdot y_1, \ldots, x \cdot y_n) \mid x \in V\}$. Let $\Omega = \{v \in V \mid \langle v \rangle \in \boldsymbol{O}\}$. Then Ω determines a set $\boldsymbol{O}' = \{\langle z_i \rangle \mid i = 1, \ldots, n'\}$ of $n' = (q-1)n/(q_0-1)$ distinct points of PG($kr-1, q_0$), and $\boldsymbol{O}'$ determines an $[n', kr]$ code over GF(q_0) via (2.3).

Recall that the vertices of the graph $G(\Omega)$ are the vectors of V and two vertices are joined if and only if their difference is in Ω. Observe that this definition does not depend on GF(q) or GF(q_0). By (3.2) the following are equivalent:

(1) $\boldsymbol{O}$ is a projective set in PG($k-1, q$);

(2) $G(\Omega)$ is strongly regular;

(3) $\boldsymbol{O}'$ is a projective set in PG($kr-1, q_0$).

By (3.1), C' is a projective two-weight $[n', kr]$ code over GF(q_0). The eigenvalues of $G(\Omega)$ are $|\Omega|$, ρ_1, and ρ_2, where

$$\rho_i = |\Omega| - qw_i = |\Omega| - q_0 w_i', \quad \text{for } i = 1, 2.$$

Hence $w_i' = qw_i/q_0$.

REMARKS. (1) Since any set of points of PG($1, q$) is a projective set we shall generally disregard examples that arise in this way. However, observe that in Example SU2 of Section 7 there are examples of two-weight $[i(q^l-1)/(q-1), l]$ codes over GF(q), with weights $(i-1)q^{l-1}$, and iq^{l-1}, that arise via (6.1).

(2) The set of all points of PG($r-1, q_0$) determines a projective $[q_0^r - 1/(q_0-1), r]$ code D over GF(q_0) via (2.3). The code D is the r-dimensional simplex code over GF(q_0) and it has just one non-zero weight, namely q_0^{r-1}. The construction described in (6.1) corresponds to substituting codewords of D for elements of GF(q_0^r). Observe that if $\phi: \mathrm{GF}(q_0^r) \to D$ is any bijective GF(q_0)-linear map, and if $\phi': \mathrm{GF}(q_0^r)^n \to \mathrm{GF}(q_0)^{n'}$ is given by $\phi'(a_1, \ldots, a_n) = (\phi(a_1), \ldots, \phi(a_n))$, then $\mathrm{wt}(\phi' v) = q_0^{r-1}\,\mathrm{wt}(v)$.

The next result is (6.1) viewed backwards.

THEOREM 6.2. *Let* $V = \mathrm{GF}(q)^k$, *let* $\mathrm{GF}(q) \subseteq \mathrm{GF}(q^*)$, *and let* ψ *be a linear transformation of V of order* q^*-1 *such that* $\{0\} \cup \langle \psi \rangle$ *is a field of linear transformations isomorphic to* GF(q^*); *this makes V into an s-dimensional* GF(q^*)*-space. Suppose that* $\boldsymbol{O}$ *is a projective* $(n, k, n-w_1, n-w_2)$ *set in* PG($k-1, q$) *and that* ψ *preserves* $\boldsymbol{O}$. *Then*

O canonically determines a projective $(n^*, s, n^*-w_1^*, n^*-w_2^*)$ set O^* in PG$(s-1, q^*)$ *where*

$$n^* = \frac{(q-1)n}{q^*-1}, \quad w_1^* = \frac{qw_1}{q^*}, \quad \textit{and} \quad w_2^* = \frac{qw_2}{q^*}.$$

Proof. If $\Omega = \{v \in V \mid \langle v \rangle \in O\}$ then $\psi\Omega = \Omega$, so Ω determines a set O^* of $n^* = (q-1)n/(q^*-1)$ points of PG$(s-1, q^*)$. By (3.2) the following are equivalent:

(1) O is a projective set in PG$(k-1, q)$;

(2) $G(\Omega)$ is strongly regular;

(3) O^* is a projective set in PG$(s-1, q^*)$.

Compute w_i^* as in (6.1).

7. *Subspace Examples*

The most visible examples of projective $(n, k, n-w_1, n-w_2)$ sets arise from subspaces.

EXAMPLE SU1. Let Ω be the complement of a t-dimensional subspace of GF$(q)^k$ where $1 \leqslant t \leqslant k-1$. If v is a non-zero vector then $|v^\perp \cap \Omega| = q^{k-1}-q^t$ or $q^{k-1}-q^{t-1}$.

EXAMPLE SU2. Let $k = 2l$ and let Σ be a family of l-spaces any two of which span GF$(q)^k$. Then $2 \leqslant |\Sigma| \leqslant q^l+1$. Let Ω be the set of non-zero vectors that are contained in the members of Σ. If v is a non-zero vector and $v^\perp$ contains a member of Σ then

$$|v^\perp \cap \Omega| = (q^l-1)+(|\Sigma|-1)(q^{l-1}-1).$$

Otherwise $|v^\perp \cap \Omega| = |\Sigma|(q^{l-1}-1)$.

Examples of such families Σ abound. The simplest examples are obtained from any family of 1-dimensional GF(q^l)-subspaces of GF$(q^l)^2$, as in Section 6. There are other examples of families of q^l+1 pairwise independent l-spaces in GF$(q)^k$. These families correspond to important types of affine planes, namely translation planes; see Dembowski [**19**, Chapter 5] and Lüneburg [**39**]. We remark that not every family Σ of pairwise independent l-spaces can be extended to a family of size q^l+1 (compare Bruen and Thas [**7**]).

8. *Dimensions* 3 *and* 4

There are important examples that occur when the dimension k is 3 or 4 and that do not necessarily generalize to higher dimensions.

EXAMPLE TF1. Let $k = 3$, let q be even, and let O be a *hyperoval* in PG$(2, q)$. Then O is a set of $n = q+2$ points, no three collinear, with the property that if L is a line then $|L \cap O| = 0$ or 2. There are unique examples when $q = 2$ or $q = 4$ but many projectively different examples for large q (Hirschfeld [**33**, Chapter 8]).

EXAMPLE TF1$^{\mathrm{d}}$. This is the projective dual of Example TF1. If O is as in TF1 then each point outside O lies on exactly $\frac{1}{2}q$ lines that miss O.

EXAMPLE TF2. In this example $k = 3$, q is even, and $n = 1+(q+1)(h-1)$, where $h \mid q$ and $1 < h < q$. The set O has the property that if L is any line then $|L \cap O| = 0$ or h.

EXAMPLE TF2^d. This is the projective dual of Example TF2. If $\boldsymbol{O}$ is as in TF2 then each point outside $\boldsymbol{O}$ lies on exactly q/h lines that miss $\boldsymbol{O}$.

When $h = 2$ we revert to TF1. Large numbers of examples for arbitrary h were found by Denniston [**20**].

EXAMPLE TF3. Let $k = 4$, $n = q^2+1$, and let $\boldsymbol{O}$ be an *ovoid* in PG$(3, q)$: a set of q^2+1 points, no three collinear, with the property that if H is a plane then $|H \cap \boldsymbol{O}| = 1$ or $q+1$.

In the classical case, $\Omega \cup \{0\}$ consists of all vectors (x, y, z, w) in GF$(q)^4$ such that $xy+z^2+azw+w^2 = 0$, where $a \in \text{GF}(q)$ and $z^2+az+1 = 0$ has no root in GF(q). Only one further class of examples is known and these arise when $q = 2^{2e+1} > 2$ (Tits [**54**]).

Note that $\boldsymbol{O}$ together with the planes meeting $\boldsymbol{O}$ in $q+1$ points forms an inversive plane: a $3-(q^2+1, q+1, 1)$ design. We refer the reader to Dembowski [**19**, Chapter 6] for a detailed discussion of ovoids.

REMARKS. Examples TF1, TF2, and TF3 are not the only examples in dimensions 3 and 4. Others are given in SU1, SU2, CY1, CY4, RT1 and RT2, where generalizations to higher dimensions are given. We note that the classical examples in TF3 are special cases of RT2.

9. *Cyclotomic examples*

In this section we construct two-weight $[n, k]$ codes from subgroups of GF$(q^k)^*$. We warn the reader that some examples begin life as cyclic codes that are not projective: after deleting coordinates to obtain a projective code the cyclic property may be lost.

We shall replace GF$(q)^k$ by GF(q^k), and the dot product $x \cdot y$ by the nonsingular bilinear form $T(xy)$, where T:GF$(q^k) \to$ GF(q) is the trace map. (Recall that if $x \in \text{GF}(q^k)$ then $T(x) = \sum_{i=0}^{k-1} x^{q^i}$.) If $\gamma \in \text{GF}(q^k)^*$ then $\gamma^\perp$ denotes the hyperplane $\{x \in \text{GF}(q^k) \mid T(\gamma x) = 0\}$.

THEOREM 9.1. *Let $k = 2l$, let z be a primitive element of* GF(q^k), *and let $R = \langle z^{q+1} \rangle$ be the subgroup of $(q+1)$th powers in* GF$(q^k)^*$. *Define the coset S of R by*

$$S = \begin{cases} R, & \text{if } q \text{ is even,} \\ \omega R, & \text{if } q \text{ is odd,} \end{cases}$$

where $\omega = z^{(q^{2l}-1)/2(q-1)}$. (Thus $S = R$ unless q and l are odd.) Then

$$|S \cap \gamma^\perp| = \begin{cases} \dfrac{(q^l-\varepsilon)(q^{l-1}+\varepsilon)}{q+1}, & \text{if } \gamma \notin S, \\[2ex] \dfrac{q^2((q^{l-1}+\varepsilon)(q^{l-2}-\varepsilon)+1)-1}{q+1}, & \text{if } \gamma \in S, \end{cases}$$

where $\varepsilon = (-1)^l$.

Proof. Given $\gamma \in \text{GF}(q^k)^*$, the map $Q(x) = T(\gamma x^{q+1})$, for all $x \in \text{GF}(q^k)$, defines a quadratic form over GF(q). The corresponding bilinear form is given by $(x, y) = T(\gamma x^q y + \gamma x y^q)$ for all $x, y \in \text{GF}(q^k)$. We shall calculate the rank of this form.

If $y \in \mathrm{GF}(q^k)^*$ then

$$\begin{aligned} T(yxy^q + yx^q y) = 0 \quad &\text{for all } x \in \mathrm{GF}(q^k) \\ \Leftrightarrow T((y^q y^{q^2} + yy)\, x^q) = 0 \quad &\text{for all } x \in \mathrm{GF}(q^k) \\ \Leftrightarrow (yy^{q+1})^{q-1} = -1. & \end{aligned}$$

If q is even then $yy^{q+1} = a$, where $a \in \mathrm{GF}(q)$, and in particular $y \in S$. There are $q^2 - 1$ ways to choose a pair (a, y) with $yy^{q+1} = a$. If q is odd then $yy^{q+1} = a\omega$, where $a \in \mathrm{GF}(q)$. Once again $y \in S$ and there are $q^2 - 1$ ways to choose the pair (a, y). Thus, for any q, we conclude that if $y \notin S$ then the bilinear form is non-degenerate, and that if $y \in S$ then the form has a 2-dimensional radical.

If $y \notin S$ then the number of non-zero singular vectors is $(q^l + \varepsilon_1)(q^{l-1} - \varepsilon_1)$, where $\varepsilon_1 = \pm 1$ depends on the type of the quadratic form $T(yx^{q+1})$. If $y \in S$ then $\mathrm{GF}(q^k) = V_1 + V_2$, where V_1 is the radical of the quadratic form and V_2 is any $(k-2)$-dimensional subspace such that $V_1 \cap V_2 = \{0\}$. The number of non-zero singular vectors is $q^2((q^{l-1} + \varepsilon_2)(q^{l-2} - \varepsilon_2) + 1) - 1$, where $\varepsilon_2 = \pm 1$ depends on the type of the quadratic form.

If $y \in S$ then the number of non-singular vectors is $(q^l + \varepsilon_1) q^{l-1}(q-1)$. If $x \in \mathrm{GF}(q^k)$ and $c \in \mathrm{GF}(q^2)$, then $Q(cx) = c^{q+1} Q(x)$. It follows that $q^2 - 1 \mid (q^l + \varepsilon_1) q^{l-1}(q-1)$ and so $\varepsilon_1 = -\varepsilon$. If $y \notin S$ then a similar argument shows that $\varepsilon_2 = \varepsilon$.

To compute $|S \cap y^\perp|$, observe that the set of singular vectors is closed under multiplication by $(q+1)$th roots of unity and that if $y \in S \cap y^\perp$, then $y = x^{q+1}$, where x is a singular vector.

COROLLARY 9.2. *Let A be a proper subset of $\{0, 1, \ldots, q\}$, let $\Omega = \bigcup_{t \in A} Sz^t$, and let $\Omega^{-1} = \{y \mid y^{-1} \in \Omega\}$. Then*

$$|\Omega \cap y^\perp| = \begin{cases} |A| \dfrac{(q^l - \varepsilon)(q^{l-1} + \varepsilon)}{q+1}, & \text{if } y \notin \Omega^{-1} \\[2ex] \dfrac{q^2((q^{l-1} + \varepsilon)(q^{l-2} - \varepsilon) + 1) - 1 + (|A| - 1)(q^l - \varepsilon)(q^{l-1} + \varepsilon)}{q+1}, & \text{if } y \in \Omega^{-1}. \end{cases}$$

Proof. Since $y^\perp z^{-t} = (yz^t)^\perp$,

$$|y^\perp \cap \Omega| = \sum_{t \in A} |y^\perp \cap Sz^t| = \sum_{t \in A} |S \cap y^\perp z^{-t}| = \sum_{t \in A} |S \cap (yz^t)^\perp|,$$

and $|y^\perp \cap \Omega|$ depends only on whether $y \in Sz^{-t}$ for some $t \in A$.

EXAMPLE CY1. Let $k = 2l$ and define Ω as in (9.2). Let $\mathrm{GF}(q_0) \subseteq \mathrm{GF}(q)$, set $n = |\Omega|/(q_0 - 1)$, and choose any elements $y_1, \ldots, y_n$ of Ω lying in different $\mathrm{GF}(q_0)^*$ cosets. Let $T' : \mathrm{GF}(q^k) \to \mathrm{GF}(q_0)$ be the trace map and let $k' = k \log_{q_0} q$. Then by (6.1) and (9.2),

$$C = \{T'(yy_1), \ldots, T'(yy_n)) \mid y \in \mathrm{GF}(q_0^{k'})\} \tag{9.3}$$

defines a projective two-weight $[n, k']$ code over $\mathrm{GF}(q_0)$. The elements $y_1, \ldots, y_n$ can be chosen to be a subgroup of $\mathrm{GF}(q^k)^*$ if and only if $n \mid q^k - 1$ and $(n, q_0 - 1) = 1$. In this case let y_1 be a generator of the subgroup and set $y_i = y_1^{i-1}$ for $i \geqslant 2$. The code C is then cyclic.

REMARKS. (1) The fact that (9.3) determines a two-weight code when $\Omega = S$ is due to McEliece [45] and Delsarte and Goethals [17] (compare Dodunekov and Iorgov [25]). We observe that the weight of the codeword $(T'(\gamma y_1), \ldots, T'(\gamma y_n))$ is a constant w_1 as γ ranges over Ω^{-1} and a constant w_2 as γ ranges over $GF(q^k)^* \backslash \Omega^{-1}$. This strengthening of the results of [17] and [45] is due to Wolfmann [56]; when $q_0 = 2$, it is also outlined in an exercise on p. 445 of [43]. Our proof of (9.1) is based upon this outline.

(2) If $k = 2l = 4$, then $|S| = (q^2+1)(q-1)$. When viewed projectively S becomes the q^2+1 points of $PG(3, q)$ that lie on a quadric (compare TF3 and RT2).

(3) If $k = 2l = 8$ then $|S| = (q^4+1)(q^2+1)(q-1)$. In this case if q is even then S is the following geometric curiosity. We choose a set P of coset representatives for $GF(q^4)^*$ in $GF(q^8)^*$ with the property that every element of P is a $(q+1)$th power. The set S is obtained by placing a quadric in $GF(q^4)^*$ as in Remark 2 and then multiplying by the elements of P. The result is one quadric per coset for a total of q^4+1 quadrics.

(4) Van Lint and Schrijver [38] discovered special cases of (9.1) and (9.2) by other methods.

EXAMPLE CY2. Let $k = 2l$ and define Ω as in (9.2). Suppose that $\Omega = GF(q')^* \Omega$ for some subfield $GF(q')$ of $GF(q^{2l})$. Then by (6.2), Ω determines a two-weight code over $GF(q')$. Remark 2 at the end of this section describes examples in $PG(2, q^4)$ due to Metz [46].

EXAMPLE CY3. Let $\Omega = GF(q^j)^* \subseteq GF(q^k)^*$. The complement of Ω in $GF(q^k)^*$ is a special case of Example SU1.

EXAMPLE CY4. Let $GF(q') \subset GF(q^{2l})$, and let Ω be any union of at least two cosets of the subgroup $GF(q^l)^* GF(q')^*$ of $GF(q^{2l})^*$. Then by (6.1) Ω yields a 2-weight code over $GF(q) \cap GF(q')$ (compare SU2), and hence over $GF(q')$ as well (by (6.2)).

The strongly regular graph arising from Ω does not depend on q'. Hence the parameters of the code can be found as in Section 6.

Projective $(n, 3, h_1, h_3)$ *sets.* In the geometry literature projective $(n, 3, h_1, h_2)$ sets have received special attention. We shall now list the examples of such sets that rise in this section.

(1) Example CY4 (with $q' = q^2, l = 3$) yields projective $(n, 3, h_1, h_2)$ sets in $PG(2, q^2)$ with $n = (q^2+q+1)t$, $h_1 = (q+1)t$, $h_2 = (q+1)t-q$, where $1 \leqslant t \leqslant q^2-q$ (de Finis [26]).

(2) Example CY2 yields projective $(n, 3, h_1, h_2)$ sets $\boldsymbol{O}$ in $PG(2, q^4)$ with

$$n = \left(\frac{q^{12}-1}{q^3+1}\right)\frac{(q+1)t}{(q^4-1)} = (q^4-q^2+1)(q^2+q+1)t,$$

$h_1 = t(q^2+q+1)$, and $h_2 = q+1+(t-1)(q^2+q+1)$, where $1 \leqslant t \leqslant q^2-q$. These sets were found by Metz [46]. When $t = 1$, $\boldsymbol{O}$ can be partitioned into q^4-q^2+1 subplanes $PG(2, q)$. The lines of $PG(2, q^4)$ which contain a line of one of the subplanes form an orbit of the cyclic group $\boldsymbol{O}$. Every other line of $PG(2, q^4)$ contains q^2+q+1 points of $\boldsymbol{O}$. Thus $\boldsymbol{O}$ determines a 2-design with parameters $v = (q^4-q^2+1)(q^2+q+1)$, $k = q^2+q+1$, $\lambda = 1$: the blocks of the design are the q^4-q^2+1 subplanes together with the lines meeting $\boldsymbol{O}$ in q^2+q+1 points.

(3) Example CY2 yields a projective $(n, 3, h_1, h_2)$ set in $PG(2, q^l)$ with

$$n(q^l-1) = \left(\frac{q^{3l}-1}{q+1}\right)\left(\frac{q+1}{3}\right) = (q^{3l}-1)/3$$

whenever $q \equiv -1 \pmod 3$.

10. *Rank* 3 *groups*

A group of collineations of $PG(k-1, q)$ with exactly 2 point-orbits also has exactly 2 hyperplane-orbits (Dembowski [**19**, p. 78]). If $\boldsymbol{O}$ is one of these point-orbits then $\boldsymbol{O}$ is a projective (n, k, h_1, h_2) set for some n, h_1, and h_2. In this section we describe all the known examples of projective (n, k, h_1, h_2) sets that arise in this way. (We remind the reader that $k > 2$, and that we shall not discuss examples arising from subspaces, or examples obtained by changing the underlying field as in (6.1).)

The aforementioned group of collineations is induced by a group G of semilinear transformations of $V = GF(q)^k$. Thus G consists of certain transformations $v \mapsto A^\sigma v$, where A is an invertible matrix and $\sigma \in \mathrm{Aut}(GF(q))$. Here we assume that G is the largest group inducing the given collineation group. Then $\{v \mapsto gv + c \mid g \in G \text{ and } c \in V\}$ acts as a rank 3 group on V, and $\{v \mapsto v + c \mid c \in V\}$ is a transitive elementary abelian normal subgroup. Conversely, any rank 3 group with a transitive elementary abelian normal subgroup arises from a group of collineations of a projective space having exactly 2 point-orbits. If $\Omega = \{v \in V \mid \langle v \rangle \in \boldsymbol{O}\}$ then the graph $G(\Omega)$ described in Section 3 is just the strongly regular graph associated with G that is described in Section 2D.

EXAMPLE RT1. The set $\boldsymbol{O}$ is a $PG(l-1, q)$ subgeometry of $PG(l-1, q^2)$. Then $\Omega \cup \{0\}$ is the union of $q+1$ l-dimensional subspaces of the $2l$-dimensional $GF(q)$-space $GF(q^2)^l$. Therefore the graph $G(\Omega)$ already arose in SU2.

In order to prove that this is a rank 3 example, fix $\Theta \in GF(q^2) \backslash GF(q)$ and observe that every non-zero vector in $GF(q^2)^l$ can be written in the form $u + \Theta v$, where $u, v \in GF(q)^l$. The orbits of $GF(q^2)^* \cdot GL(l, q)$ on $GF(q^2)^l \backslash \{0\}$ are $\{u + \Theta v \mid u \text{ and } v$ are dependent over $GF(q)\}$ and $\{u + \Theta v \mid u$ and v are independent over $GF(q)\}$. Furthermore

$$\dim_{GF(q)} [GF(q)^l \cap (u + \Theta v)^\perp] = \begin{cases} l-1, & \text{if } u \text{ and } v \text{ are dependent,} \\ l-2, & \text{if } u \text{ and } v \text{ are independent.} \end{cases}$$

EXAMPLE RT2. Let $k = 2l$, let Q be a nonsingular quadratic form on $GF(q)^k$, and let $\Omega = \{v \in GF(q)^k \mid v \neq 0 \text{ and } Q(v) = 0\}$.

We refer the reader to Dickson [**21**], or Dieudonné [**22**], for the definitions and basic geometric properties of quadratic forms and their associated orthogonal geometries. Clearly $GF(q)^* \Omega = \Omega$. The orthogonal group preserving Q acts transitively on $\{v \in GF(q)^k \mid v \neq 0 \text{ and } Q(v) = a\}$ for each $a \in GF(q)$. If G consists of all nonsingular linear transformations g such that $Q(gv) = c_g Q(v)$ for some $c_g \in GF(q)$ and all $v \in GF(q)^k$, then G has only two orbits of non-zero vectors.

We have $|\Omega| = (q^l - \varepsilon)(q^{l-1} + \varepsilon)$ where $\varepsilon = \pm 1$ depends on the type of the quadratic form Q. If we define perpendicularity in terms of the bilinear form $(u,v) = Q(u+v)-Q(u)-Q(v)$, then

$$|v^{\perp}\cap\Omega| = \begin{cases} q-1+q(q^{l-1}-\varepsilon)(q^{l-2}+\varepsilon), & \text{if } v\in\Omega,\\ q^{2l-2}-1, & \text{if } Q(v)\neq 0.\end{cases}$$

When $k = 4$ and $n = q^2+1$, this example appeared in TF3.

If $\varepsilon = 1$ then the parameters of the corresponding code and strongly regular graph are exactly the same as in Example SU2 (when $i = q^{l-1}+1$). However, if l is odd then Ω cannot contain 3 pairwise independent l-spaces. If l is even then the only examples where Ω is known to arise as in SU2 are as follows (compare Kantor [36]): $l = 2$, q is even; $l = 4$ and $q \equiv 0$ or 2 (mod 3).

EXAMPLE RT3. Let (,) be a nonsingular hermitian form on $V = GF(q^2)^l$, and let $\Omega = \{v\in V \mid v\neq 0 \text{ and } (v,v) = 0\}$.

We refer the reader to Dickson [21] or Dieudonné [22] for the definition and elementary properties of such forms. If $G = \{g\in GL(V) \mid (gu,gv) = c_g(u,v)$ for some $c_g\in GF(q)$ and all $v\in V\}$, then G has only two orbits of non-zero vectors.

We have $|\Omega| = (q^l-\varepsilon)(q^{l-1}+\varepsilon)$, where $\varepsilon = (-1)^l$. If we define perpendicularity in terms of the hermitian form then

$$|v^{\perp}\cap\Omega| = \begin{cases} q^2-1+q^2(q^{l-2}-\varepsilon)(q^{l-3}+\varepsilon), & \text{if } v\in\Omega,\\ (q^{l-1}+\varepsilon)(q^{l-2}-\varepsilon), & \text{if } (v,v)\neq 0.\end{cases}$$

The corresponding strongly regular graph already arose in RT2. For if we set $Q(v) = (v,v)$, and if we regard V as a $2l$-dimensional space over GF(q), then Q is a nonsingular quadratic form over GF(q). We see from RT2 that for each possible dimension, only one of the two types of code/geometry in RT2 arises from a hermitian form in this way.

EXAMPLE RT4. Let V be the space of all skew symmetric 5×5 matrices over GF(q) with zero diagonal, and let Ω be the subset of matrices with rank 2. This example is due to Cameron (compare Hubaut [34, p. 377]) and to Delsarte and Goethals [18].

Here dim $V = 10$. If A is a non-zero matrix in V then the rank of A is even and hence is 2 or 4. If M is a 5×5 invertible matrix then M acts on V by $A\mapsto MAM^t$, for all $A\in V$. If $A, B\in V$ and rank A = rank B then there exists $M\in GL(5,q)$ such that $B = MAM^t$.

We remark that skew-symmetric 4×4 matrices also afford a rank 3 example in the above manner (via the Klein correspondence). However this example coincides with RT2 (when $k = 6$ and $\varepsilon = 1$).

The preceding examples are all projectively self-dual. The following examples are not and so they come in pairs. These examples are related to the Golay codes (compare MacWilliams and Sloane [43, Chapter 20] or Conway [12]).

EXAMPLE RT5. Here $q = 2$, $k = 11$, and $n = 759$. The extended binary Golay code C is a [24,12] code invariant under the Mathieu group M_{24}. Regard C as 2^{12} subsets of a 24-set S, namely $\varnothing, S$, 759 octads, their 759 complements, and 2.1288 dodecads coming in complementary pairs. Set $V = C/\{\varnothing, S\}$ and observe that M_{24} has just two orbits on V.

EXAMPLE RT5^d. Here $q = 2$, $k = 11$, and $n = 276$. This example arises as the projective dual of RT5. Let $V = E/C$ where E is the set of all subsets of a 24-set S with even cardinality and C is the extended binary Golay code. Any element of E is congruent mod C to a 2-subset of S or to a sextet (compare Conway [12]).

EXAMPLE RT6. Here $q = 3$, $k = 5$, and $n = 11$. The two-weight code is the dual of the $[11, 6, 5]$ ternary Golay code. The Mathieu group M_{11} has point-orbits on PG(4, 3) of size 11 and 110 (compare Coxeter [13]).

EXAMPLE RT6^d. Here $q = 3$, $k = 5$, and $n = 66$. This example arises as the projective dual of RT6. Consider the point orbit of size 11 of M_{11} on PG(4, 3). Any 4 points of this orbit span a hyperplane of PG(4, 3) containing a fifth point of the orbit. In this way we obtain 66 hyperplanes, one for each block of the Steiner system $S(4, 5, 11)$.

REMARK. Examples RT5^d, RT6 and RT6^d are described in [14]. All solvable, primitive, rank 3 permutation groups have been determined by Foulser [27]. Each group gives rise to a two-weight code and strongly regular graph. These examples have been studied from a point of view similar to ours by van Lint and Schrijver [38]. They have been described earlier, many of them in Section 9.

11. *Further examples*

In this section we describe additional examples that do not fit into the previous sections.

EXAMPLE FE1. Let $k = 2l$, let Q be a nonsingular quadratic form on $GF(q)^{2l}$ with q odd, and let $\Omega = \{v \in GF(q)^{2l} \mid Q(v) \text{ is a non-zero square}\}$.

Then $GF(q)^* \Omega = \Omega$. If G consists of all nonsingular linear transformations g such that $Q(gv) = c_g Q(v)$ for some $c_g \in GF(q)$ and all $v \in GF(q)^{2l}$ then G acts transitively on Ω. However this example differs from Example RT2 in that G has three orbits of non-zero vectors.

We have $|\Omega| = \frac{1}{2}(q^l - \varepsilon) q^{l-1}(q-1)$, where $\varepsilon = \pm 1$ depends on the type of the quadratic form Q. Let $v \in GF(q)^{2l}$ be a non-zero vector. Then

$$|v^\perp \cap \Omega| = \tfrac{1}{2} q (q^{l-1} - \varepsilon) q^{l-2}(q-1) \quad \text{if } Q(v) = 0,$$

and

$$|v^\perp \cap \Omega| = \tfrac{1}{2} q^{l-1}(q^{l-1} \pm 1)(q-1) \quad \text{if } Q(v) \neq 0,$$

where the sign depends on whether $Q(v)$ is a square or a non-square.

EXAMPLE FE2. Here $q = 3$, $k = 6$, and $n = 56$. The corresponding projective set in PG(5, 3) was studied by Segre [48], McLaughlin [40], Hill [30], and Bruen and Hirschfeld [6].

A description is given in [30] in terms of a collineation of order 7 that acts on the set. We shall give a description using the group $\mathbb{Z}_2^5 \rtimes PSL_2(5)$, which appears to be new.

Let $e_\infty, e_0, e_1, e_2, e_3, e_4$ be a basis for a 6-dimensional vector space over GF(3). All vectors will be written in terms of their coordinates with respect to this basis. Our

$\mathbb{Z}_2^5$ consists of all diagonal transformations, $\mathrm{diag}(\pm 1, \pm 1, \pm 1, \pm 1, \pm 1, \pm 1)$, with determinant 1. The group PSL(2, 5) represented by all transformations

$$x \to \frac{ax+b}{cx+d}, \quad ad-bc = 1 \quad (a, b, c, d \in \mathrm{GF}(5)),$$

acts on $\{e_\infty, e_0, e_1, e_2, e_3, e_4\}$ in the obvious way while normalizing our $\mathbb{Z}_2^5$. The resulting group $\mathbb{Z}_2^5 \rtimes \mathrm{PSL}_2(5)$ sends $\langle(111000)\rangle$ to 40 points and $\langle(111111)\rangle$ to 16 points. The required set $\boldsymbol{O}$ is the union of these two sets, and is readily found to have the required properties. Moreover it is easy to check that no 3 points of $\boldsymbol{O}$ are collinear and that $\sum x_i^2 = 0$ whenever $\langle(x_i)\rangle \in \boldsymbol{O}$.

Hill [**30**] showed that there is essentially just one subset $\boldsymbol{O}$ of PG(5, 3) with the desired properties.

EXAMPLE FE3. Here $q = 4$, $k = 6$, and $n = 78$. This example was discovered by Hill [**31**]. We shall give a cyclotomic description.

Let z be a primitive element of $\mathrm{GF}(4^6)$ and let $\langle z^{35}\rangle$ denote the subgroup of 35th powers in $\mathrm{GF}(4^6)^*$. Choose $\beta = 7, 14, 21$, or 28. The required set $\boldsymbol{O}$ consists of the 78 GF(4)-1-spaces in $\{0\} \cup \langle z^{35}\rangle \cup \langle z^{35}\rangle z^\beta$. A computer checked that no three points of $\boldsymbol{O}$ are collinear. It also discovered that any union $\{0\} \cup \langle z^{35}\rangle \cup \langle z^{35}\rangle z^\alpha$ with $1 \leqslant \alpha \leqslant 34$, $\alpha \neq 7, 14, 21$, or 28, contains 3 collinear points. Note that the different choices for β are related by the transformation $x \to x^2$.

EXAMPLE FE3$^{\mathrm{d}}$. Here $q = 3$, $k = 4$, and $n = 936$. This example arises as the projective dual of FE3.

EXAMPLE FE4. Here $q = 3$, $k = 4$, and $n = 15$. This example, due to van Lint and Schrijver [**38**], has several descriptions (Cameron and van Lint [**9**]). We shall give a cyclotomic description.

Let $F = \mathrm{GF}(3^4)$ and let $\gamma \in F^*$ be an element of order 5. Let $L = \{0\} \cup \langle\gamma\rangle$ and let $\Omega = \{x - y \mid x, y \in L, x \neq y\}$. Then $G(\Omega)$ is a strongly regular graph with parameters $N = 3^4$, $K = 30$, $\lambda = 9$, and $\mu = 12$. Therefore it determines a two-weight code. This code is equivalent to its projective dual.

12. *Characterization theorems*

In Section 3 we established numerical constraints on the parameters of any (n, k, h_1, h_2) set. In this section we describe theorems that characterize such projective sets subject to some additional geometric restriction.

The first theorem is due to Calderbank [**8**] and characterizes projective sets $\boldsymbol{O}$ such that no three points of $\boldsymbol{O}$ are collinear. If the parameters of the strongly regular graph $G(\Omega)$ are (N, K, λ, μ) then this geometric hypothesis implies $\lambda = q-2$. The theorem is only proved after a very intricate analysis of (3.11).

THEOREM 12.1. *Let $k \geqslant 3$, let $\boldsymbol{O}$ be a projective $(n, k, n-w_1, n-w_2)$ set in* PG$(k-1, q)$ *and suppose that no three points of $\boldsymbol{O}$ are collinear.*

(A) *If $q = 2$ then either*

(1) *$\boldsymbol{O}$ is the complement of a hyperplane in* PG$(k-1, 2)$, *or*

(2) *$\boldsymbol{O}$ is an ovoid in* PG(3, 2).

(B) *If $q \neq 2$ then either*

(3) *q is even and $\boldsymbol{O}$ is a hyperoval in* PG$(2, q)$,

(4) O *is an ovoid in* PG(3, q),

(5) $n(q-1) = t(q^{\frac{1}{2}k}+1)$, $w_1 = tq^{\frac{1}{2}(k-2)}$, $w_2 = (t+1)q^{\frac{1}{2}(k-2)}$, *where* t *is a positive integer and* $(2t+3)^2 = 4q^{\frac{1}{2}k}+4q+1$, *or*

(6) $2(q-1)n = (2t+1)q^{\frac{1}{2}(k-2)}+q-2(t(t+1)/q)$, $w_1 = tq^{\frac{1}{2}(k-3)}$, $w_2 = (t+1)q^{\frac{1}{2}(k-3)}$, *where* t *is a positive integer and* $(2t+(2q+1))^2 = 4q^{\frac{1}{2}(k+1)}+4q+1$.

A set O satisfying the hypotheses of Theorem 12.1 will be called a *projective* $(n, k, n-w_1, n-w_2)$ *cap*. If (5) or (6) holds then there exists an integer solution (y, a) of the equation

$$y^2 = 4q^{a/2}+4q+1. \tag{12.2}$$

Since $(y, a) = (2q+1, 4)$ is a solution, case 5 of Theorem 12.1 includes case 4. If $q = 3$ or $q = 4$ then there exist projective caps that do not fall under cases 3 and 4. If $q = 3$ then (12.2) becomes

$$y^2 = 4.3^b+13. \tag{12.3}$$

It is shown by Bremner *et al.* [**5**] that the only integer solutions (y, b) of (12.3) are $(y, b) = (5, 1)$ $(7, 2)$ and $(11, 3)$. It is also shown that if O is a projective $(n, k, n-w_1, n-w_2)$ cap in PG$(k-1, 3)$ then $(n, k, n-w_1, n-w_2) = (10, 4, 4, 1)$, $(11, 5, 5, 2)$, or $(56, 6, 20, 11)$. Projective caps with these parameters are described in Examples TF3, RT6, and FE2 respectively. If $q = 4$ then (12.2) becomes

$$y^2-17 = 2^b. \tag{12.4}$$

Beukers [**2**] has shown that the only integer solutions (y, b) of (12.4) are $(y, b) = (5, 3)$, $(7, 5)$, $(9, 6)$, and $(23, 9)$. Theorem 12.1 implies that if O is a projective $(n, k, n-w_1, n-w_2)$ cap in PG$(k-1, 4)$ then $(n, k, n-w_1, n-w_2) = (6, 3, 2, 0)$, $(17, 4, 5, 1)$, $(78, 6, 22, 14)$, or $(430, 7, 110, 78)$. Projective caps with the first three parameters are described in Examples TF1, TF3, and FE3 respectively. The existence of a projective $(430, 7, 110, 78)$ cap is an open problem.

Let r, k, t, be integers with $r \geqslant 2$, $k \geqslant 2$, $t \geqslant 1$. A *partial quadrangle with parameters* (r, k, t) is an incidence structure of points and lines with the following properties:

(1) any point is incident with r lines and any line with k points;

(2) (a) two points are incident with at most one line;

(b) if three points are pairwise collinear then all three are collinear; and

(3) if two points are not collinear, then exactly t points are collinear with both.

Cameron [**9**] regards a projective $(n, k, n-w_1, n-w_2)$ cap O in PG$(k-1, q)$ as a linear representation of a partial quadrangle with parameters (n, q, μ), where $\mu = q^2 w_1 w_2/q^k$: the points of the quadrangle are the vectors of GF$(q)^k$, the lines through 0 are the 1-spaces in O, and the other lines are obtained by translation. Condition 2(b) is satisfied because no three points of O are collinear. Theorem 3.2 implies that (3) holds and μ is given in (3.7). The strongly regular graph $G(\Omega)$ of (3.2) is the point graph of the partial quadrangle.

The next theorem is due to Tallini-Scafati [**50**] and does not appear to involve codes or projective (n, k, h_1, h_2) sets at all. (However, compare the hypotheses of the theorem with (3.12).)

THEOREM 12.5. *Let* $k \geqslant 4$, *and let* O *be a set of points of* PG$(k-1, q)$ *such that neither* O *nor its complement is empty, a point or a hyperplane. Suppose there exist* *constants a and b such that every line of* PG$(k-1, q)$ *contains exactly a or b points of* $\boldsymbol{O}$. *Then q is odd and a square and if* $a \leqslant b$ *then*

$$a = \tfrac{1}{2}(q+1-\sqrt{q}(1-\varepsilon)),$$
$$b = \tfrac{1}{2}(q+1+\sqrt{q}(1+\varepsilon)),$$

and

$$|\boldsymbol{O}| = \frac{1}{2}\left(1+\frac{q^{k-1}-1}{q-1}(q+\varepsilon\sqrt{q})+\delta\sqrt{q^{k-1}}\right),$$

where $\varepsilon = \pm 1$ *and* $\delta = \pm 1$.

We note that no examples of such sets $\boldsymbol{O}$ are known. The complement of $\boldsymbol{O}$ corresponds to replacing δ by $-\delta$, and ε by $-\varepsilon$.

We outline the proof and describe the connection with two-weight codes. A preliminary argument establishes that $0 < a \leqslant b < q+1$. It follows that, if X is any subspace of the projective space, then $\boldsymbol{O} \cap X$ satisfies the hypotheses of the theorem. In particular, if X is a plane then $\boldsymbol{O} \cap X$ is a projective $(|\boldsymbol{O} \cap X|, 3, a, b)$ set in X. Hence $|\boldsymbol{O} \cap X|$ is a root of the quadratic equation (3.10), and, by (3.13), $b-a$ is a power of p. If i_a and i_b are the numbers of lines meeting $\boldsymbol{O}$ in a and b points, respectively, then

$$i_a + i_b = \frac{(q^k-1)(q^{k-1}-1)}{(q-1)(q^2-1)},$$

$$ai_a + bi_b = \frac{|\boldsymbol{O}|(q^{k-1}-1)}{(q-1)},$$

and

$$a(a-1)\,i_a + b(b-1)\,i_b = |\boldsymbol{O}|(|\boldsymbol{O}|-1).$$

Thus $|\boldsymbol{O}|$ satisfies a quadratic equation with coefficients depending on q, k, a, and b. If X is any hyperplane then we can obtain a quadratic equation satisfied by $|\boldsymbol{O} \cap X|$ in the same way. Therefore $\boldsymbol{O}$ is a projective (n, k, h_1, h_2) set. It only remains to find a and b, and hence we may assume that $k = 4$. After some nontrivial manipulation of the quadratic constraints, Tallini-Scafati obtains the desired values of a and b.

The next result is due to Thas **[51]** and is more clearly related to codes: it concerns two-weight $[n, k]$ codes for which $n-1$ is one of the weights. Since it is readily proved using the diophantine conditions of Section 3, we shall include a short proof. We remind the reader that a projective $(n, k, n-w_1, 0)$ set is the complement of a hyperplane.

THEOREM 12.6. *Let* $q = p^m$ *and let* $k \geqslant 4$. *If* $\boldsymbol{O}$ *is a projective* $(n, k, n-w_1, 1)$ *set in* PG$(k-1, q)$ *then* $\boldsymbol{O}$ *is a line of* PG$(k-1, q)$ *or an ovoid in* PG$(3, q)$.

Proof. If $\boldsymbol{O}$ does not span PG$(k-1, q)$ then $\boldsymbol{O}$ is a PG(r, q) subgeometry and hence is a line. If $\boldsymbol{O}$ spans PG$(k-1, q)$, then by (3.1) and (3.13) $\boldsymbol{O}$ determines a two-weight $[n, k]$ code with weights $w_1 = n-1-p^j = p^j t$ and $w_2 = n-1 = p^j(t+1)$. Substituting $n = p^j(t+1)+1$ into (3.10) and simplifying we obtain

$$0 = p^j((t+1)-q)((t+1)p^j-(q-1))+q(q-1)-\frac{t(t+1)p^{2j}}{q^{k-2}}. \tag{12.7}$$

If $j = 0$ then $\boldsymbol{O}$ is a projective $(n, k, 1, 2)$ set and any three points of $\boldsymbol{O}$ span PG$(k-1, q)$. However this contradicts the hypothesis $k \geqslant 4$. If $j \geqslant m$ then $(t+1)p^j-(q-1) > tq$, and (12.7) implies that $t+1 \geqslant q$. If $0 < j < m$ then (12.7) implies that $p^j \mid t(t+1)p^{2j-2m}$; hence $p^{2m-j} \mid t(t+1)$ and $t+1 \geqslant q$. In either case $t+1 \geqslant q$.

If $t+1 > q$ then $t+1-q \geqslant (t+1)/(q+1)$, $t+2-q \geqslant t/(q-1)$, and

$$p^j(t+1-q)((t+1)p^j-(q-1)) > p^{2j}t(t+1)/(q^2-1).$$

However, this implies that the right-hand side of (12.7) is positive.

Therefore $t+1 = q$ and $2j = m(k-2)$ by (12.7). Thus $w_2 = q^{k/2}$, $w_1 = q^{k/2}-q^{(k-2)/2}$ and hence $2E' = q^2-q^{k/2}$ by (3.2) and (3.12). Since E' is non-negative, $k = 4$ and $\boldsymbol{O}$ is a projective $(q^2+1, 4, q+1, 1)$ set in $\mathrm{PG}(3,q)$.

The next result is new and may be regarded as a generalization of Theorem 12.6.

THEOREM 12.8. *Let $q = p^m$ and let i be a fixed positive integer. If $\boldsymbol{O}$ is a projective (n,k,h,i) set that spans* $\mathrm{PG}(k-1,q)$ *then $h \leqslant (q+1)i$. Equality holds if and only if $\boldsymbol{O}$ is an ovoid in* $\mathrm{PG}(3,q)$. *Furthermore, $k \leqslant (q+1)i+1$, and there are only finitely many projective sets for given q and i.*

Proof. If $h \leqslant (q+1)i$ then any $(q+1)i+1$ points of $\boldsymbol{O}$ span $\mathrm{PG}(k-1,q)$ and $k \leqslant (q+1)i+1$. In order to prove that $h \leqslant (q+1)i$ we may assume that $h > i$, and by Theorem 12.6 we may assume $i > 1$.

By (3.1) and (3.13), $\boldsymbol{O}$ determines a two-weight $[n,k]$ code with weights $w_1 = n-1-p^j = p^jt$ and $w_2 = n-i = p^j(t+1)$. Substituting $n = p^j(t+1)+i$ into (3.10) and simplifying we obtain

$$0 = (t+1-q)p^j((t+1)p^j-i(q-1))-(q-1)p^j(i-1)(t+1) + i(q-1)(iq-i+1)-\frac{t(t+1)p^{2m+2j}}{q^k}. \quad (12.9)$$

Suppose by way of contradiction that $0 \leqslant h-(q+1)i = p^j-iq$. Then $(q-1)p^j(i-1)(t+1) > i(q-1)(iq-i+1)$. Hence (12.9) implies that $t+1 > q$, or equivalently, $t+1-q \geqslant (t+1)/(q+1)$.

Let $i(q-1)(iq-i+1) = p^\alpha u$ where $p \nmid u$. If $p \mid i$ then $p^\alpha \leqslant i$, and if $p \mid i-1$ then $p^\alpha < iq$. Therefore $p^\alpha < iq$ in either case. Since $p^j \geqslant iq$, (12.9) implies that $p^{\alpha+1} \nmid t(t+1)p^{2m+2j-km}$. Hence $t(t+1)p^{2m+2j-km} \leqslant p^\alpha t(t+1)$.

Let R be the right-hand side of (12.9). If $p^j = iq$ then $p \mid i$, $p^\alpha \leqslant i$, and

$$R > \frac{t(t+1)p^{2j}}{q+1}-(i-1)(q-1)p^j(t+1)-it(t+1)$$
$$= \frac{iq(t+1)}{q+1}\left(tiq-(i-1)(q^2-1)-\frac{t(q+1)}{q}\right). \quad (12.10)$$

Since $t \geqslant q$, (12.10) implies that $R > 0$, which contradicts (12.9).

Therefore $p^j \geqslant iq+1$, and hence $p^j \geqslant (i+1)q$. This time,

$$R > \frac{t(t+1)p^{2j}}{q+1}-(i-1)(q-1)p^j(t+1)-iqt(t+1)$$
$$\geqslant \frac{(t+1)p^j}{q+1}(t(i+1)q-(i-1)(q^2-1)-t(q+1)). \quad (12.11)$$

Since $t \geqslant q$, (12.11) implies that $R > 0$, which contradicts (12.9).

We conclude this section with a theorem of Mann [44] on (v, K, λ) difference sets in elementary abelian groups (compare with Camion [11, p. 57]). A (v, K, λ) *difference set* in a group G of order v is a set $\Omega = \{g_1, \ldots, g_K\}$ of K elements of G such that for every $g \in G$ with $g \neq 1$, the equation $g_i g_j^{-1} = g$ has exactly λ solutions (we shall exclude $\Omega = G$ and $\Omega = G\backslash\{g\}$ for some $g \in G$). Observe that the complement of a difference set is a difference set.

THEOREM 12.12. *Let p be a prime and let Ω be a (p^k, K, λ) difference set in* $\mathrm{GF}(p)^k$. *If* $\mathrm{GF}(p)^* \Omega = \Omega$ *then* $p = 2$, $k = 2l$, $K = 2^{l-1}(2^l + \varepsilon)$, *and* $\lambda = 2^{l-1}(2^{l-1} + \varepsilon)$, *where* $\varepsilon = \pm 1$.

Proof. After possibly taking complements we may assume that $0 \notin \Omega$. Thus Ω is a $\{\lambda, \mu\}$ difference set with $\lambda = \mu$. By (3.2) and (3.13), Ω determines a two-weight $[n, k]$ code with weights $w_1 = p^j t$ and $w_2 = p^j(t+1)$. Corollary 3.7 gives $\mu = p^{2-k} w_1 w_2$ and $\lambda - \mu = 2n(p-1) - p(w_1 w_2)$. Hence

$$\rho_1 = n(p-1) - pw_1 = -(n(p-1) - pw_2) = -\rho_2.$$

By (3.13), $\rho_1 - \rho_2 = 2\rho_1$ is a power of p and so $p = 2$. Thus $n = (2t+1)2^j$, $\mu = 2^{2j+2-k} t(t+1)$, and (3.11) becomes

$$2^{2j+2} = 4((2t+1)2^j - 2^{2j+2-k} t(t+1)),$$

or

$$t^2 - (2^{k-j-1} - 1)t + 2^{k-j-2}(2^j - 1) = 0. \tag{12.13}$$

If t_0, t_1 are the roots of (12.13) then $t_0, t_1 > 0$ and we may assume $t_0 \equiv 0 \pmod{2^{k-j-2}}$ and $t_1 \equiv -1 \pmod{2^{k-j-2}}$. Since $t_0 + t_1 = 2^{k-j-1} - 1$ we have $t_0 = 2^{k-j-2}$ and $t_1 = 2^{k-j-2} - 1$. Since $t_0 t_1 = 2^{k-j-2}(2^j - 1)$ we have $j + 1 = k/2 = l$ say. Hence $\lambda = 2^{l-1}(2^{l-1} + \varepsilon)$ and $K = n = 2^{l-1}(2^l + \varepsilon)$, where $\varepsilon = \pm 1$ depends on whether $t = t_0$ or $t = t_1$.

We obtain examples of $(2^{2l}, 2^{l-1}(2^l + \varepsilon), 2^{l-1}(2^{l-1} + \varepsilon))$ difference sets from the complement of Example RT2 in $\mathrm{GF}(q)^{2l}\backslash\{0\}$ when $q = 2$. If H is any hyperplane then $|H \Delta \Omega| = 2^{l-1}(2^l \pm 1)$, where Δ denotes symmetric difference. Let B consist of all sets $\Omega, \Omega', H\Delta\Omega, H\Delta\Omega'$, where Ω' is the complement of Ω in $\mathrm{GF}(2)^{2l}$, and H ranges over all hyperplanes. The 2^{2l} subsets in B of size $2^{l-1}(2^l + \varepsilon)$ form a symmetric design having the same parameters as that arising from the difference set Ω (see Kantor [35]). The sets Ω are closely related to bent functions (MacWilliams and Sloane [43, Chapter 14.5], Rothaus [47], and Dillon [23]).

13. *Tables*

In Section 3 we described how a two-weight $[n, k]$ code C with weights w_1 and w_2 determines a projective $(n, k, n - w_1, n - w_2)$ set $\boldsymbol{O}$ and a strongly regular graph $G(\Omega)$ with parameters (N, K, λ, μ).

Figure 1 lists the underlying field and the parameters n, k, w_1 and w_2 of essentially all the known two-weight codes. 'Essentially all' means that we have omitted the following:

(1) two-dimensional codes;
(2) codes obtained from those listed in Figure 1 by changing the underlying field as in Section 6; and
(3) codes obtained from those listed in Figure 1 by taking the complement of the corresponding projective set.

Example	n	k	Field	w_1	w_2
SU1	$\frac{q^l-q^t}{q-1}$ $1 \leqslant t \leqslant l-1$	l	GF(q)	$q^{l-1}-q^{t-1}$	q^{l-1}
SU2	$\frac{(q^l-1)i}{q-1}$ $2 \leqslant i \leqslant q^l$	$2l$	GF(q)	$(i-1)q^{l-1}$	iq^{l-1}
TF1	$q+2$	3	GF(q) q even	q	$q+2$
TF1[d]	$\frac{1}{2}(q+1)(q+2)$	3	GF(q) q even	$\frac{1}{2}q(q+1)$	$\frac{1}{2}q(q+2)$
TF2	$1+(q+1)(h-1)$ where $1<h<q, h\mid q$	3	GF(q) q even	$q(h-1)$	$1+(q+1)(h-1)$
TF2[d]	$\frac{(q+1)(1+(q+1)(h-1))}{h}$ where $1<h<q, h\mid q$	3	GF(q) q even	$\frac{q(q+1)(h-1)}{h}$	$\frac{q(1+(q+1)(h-1))}{h}$
TF3	q^2+1	4	GF(q)	$q(q-1)$	q^2
CY1 ($\varepsilon=(-1)^l$)	$\frac{(q^{2l}-1)i}{(q+1)(q_0-1)}$ where $q=q_0^r$, $1 \leqslant i \leqslant q$	$2lr$	GF(q_0)	$\frac{q}{q_0}\left(\frac{iq^{l-1}(q^l-\varepsilon)}{q+1}\right)$	$\frac{q}{q_0}\left(\varepsilon q^{l-1}+\frac{iq^{l-1}(q^l-\varepsilon)}{q+1}\right)$
CY2 ($\varepsilon=(-1)^l$)	$\frac{(q^{2l}-1)i}{(q+1)(q_1-1)}$ where $q_1^S=q^{2l}$, $2 \leqslant i \leqslant q$	S	GF(q_1)	$\frac{q}{q_1}\left(\frac{iq^{l-1}(q^i-\varepsilon)}{q+1}\right)$	$\frac{q}{q_1}\left(\varepsilon q^{l-1}+\frac{iq^{l-1}(q^l-\varepsilon)}{q+1}\right)$
CY4	$\frac{(q^l-1)i}{q_1-1}$ where $q_1^S=q^{2l}$, $2 \leqslant i \leqslant q^l$	S	GF(q_1)	$\frac{q}{q_1}((i-1)q^{l-1})$	$\frac{q}{q_1}(iq^{l-1})$

FIGURE 1a.

Example	n	k	Field	w_1	w_2
RT1	$\frac{q^l-1}{q-1}$	l	GF(q^2)	q^{l-1}	$q^{l-2}(q+1)$
RT2	$\frac{(q^l-\varepsilon)(q^{l-1}+\varepsilon)}{q-1}$ where $\varepsilon=\pm 1$	$2l$	GF(q)	q^{2l-2}	$q^{2l-2}+\varepsilon q^{l-1}$
RT3	$\frac{(q^l-\varepsilon)(q^{l-1}+\varepsilon)}{q^2-1}$ where $\varepsilon=(-1)^l$	l	GF(q^2)	q^{2l-3}	$q^{2l-3}+\varepsilon q^{l-2}$
RT4	$\frac{(q^5-1)(q^2+1)}{q-1}$	10	GF(q)	q^6	$(q^2+1)q^4$
RT5	759	11	GF(2)	352	384
RT5[d]	276	11	GF(2)	128	144
RT6	11	5	GF(3)	6	9
RT6[d]	66	5	GF(3)	36	45
FE1	$\frac{1}{2}q^{l-1}(q^l+\varepsilon)$ where $\varepsilon=\pm 1$	$2l$	GF(q)	$\frac{1}{2}q^{2l-2}(q-1)$	$\frac{1}{2}q^{2l-2}(q-1)-\varepsilon q^{l-1}$
FE2	56	6	GF(3)	36	45
FE3	78	6	GF(4)	56	64
FE3[d]	936	6	GF(4)	672	704
FE4	15	4	GF(3)	9	12

FIGURE 1b.

Example	N	K	λ	μ	ρ_1	ρ_2	A_{w_1}	A_{w_2}
SU1	q^l	q^l-q^t $1 \leqslant t \leqslant l-1$	q^l-2q^t	q^l-q^t	0	$-q^t$	q^l-q^{l-t}	$q^{l-t}-1$
SU2	q^{2l}	$i(q^l-1)$ $2 \leqslant i \leqslant q^l$	$q^l+i(i-3)$	$i(i-1)$	q^l-i	$-i$	$i(q^l-1)$	$(q^l-1)(q^l+1-i)$
TF1	q^3 q even	$(q+2)(q-1)$	$q-2$	$q+2$	$q-2$	$-(q+2)$	$\frac{1}{2}(q+2)(q^2-1)$	$\frac{1}{2}q(q-1)^2$
TF1^d	q^3 q even	$\frac{1}{2}(q+2)(q^2-1)$	$q-2+$ $\frac{1}{4}q(q-1)(q+6)$	$\frac{1}{4}q(q+1)(q+2)$	$\frac{1}{2}(q+1)(q-2)$	$-\frac{1}{2}(q+2)$	$(q+2)(q-1)$	$(q-1)(q^2-1)$
TF2	q^3 q even	$(q-1)\alpha$ where $\alpha=$ $1+(q+1)(h-1)$ $1<h<q, h\mid q$	$q-h+(h-2)\alpha$	$(h-1)\alpha$	$q-h$	$-\alpha$	$\frac{1}{h}\alpha(q^2-1)$	$\frac{1}{h}q(q+1)(q+1-h)$
TF2^d	q^3 q even	$\frac{1}{h}\alpha(q^2-1)$ where $\alpha=$ $1+(q+1)(h-1)$ $1<h<q, h\mid q$	$K-1-$ $\frac{(h-1)q^2(q+1-h)}{h^2}$	$\frac{(h-1)q(q+1)\alpha}{h^2}$	$\frac{(q+1)(q-h)}{h}$	$-\frac{\alpha}{h}$	$(q-1)\alpha$	$(q-1)\times$ $\{(q^2-h+2)(q+1)$ $-1\}$
TF3	q^4	$(q^2+1)(q-1)$	$q-2$	$q(q-1)$	$q-1$	$-(q^2-q+1)$	$q(q^2+1)(q-1)$	$(q^2+1)(q-1)$
CY1 $(\varepsilon=(-1)^l)$	q^{2l}	$\frac{(q^{2l}-1)i}{q+1}$ $1 \leqslant i \leqslant q$	$\mu-\varepsilon q^l+\frac{2i\varepsilon(q^l-\varepsilon)}{q+1}$	$i(q^l-1)\times$ $(i(q^l-1)+\varepsilon)$	$\frac{i\varepsilon(q^l-\varepsilon)}{q+1}$	$\frac{i\varepsilon(q^l-\varepsilon)}{q+1}-\varepsilon q^l$	$\frac{(q-i+1)(q^{2l}-1)}{q+1}$	$\frac{(q^{2l}-1)i}{q+1}$

FIGURE 2a.

Example	N	K	λ	μ	ρ_1	ρ_2	A_{w_1}	A_{w_2}
CY2 ($\varepsilon = (-1)^l$)	q^{2l}	$\frac{(q^{2l}-1)i}{q+1}$ $1 \leqslant i \leqslant q$	$\mu - \varepsilon q^l + \frac{2i\varepsilon(q^l-\varepsilon)}{q+1}$	$i(q^l-1)(i(q^l-1)+\varepsilon)$	$\frac{i\varepsilon(q^l-\varepsilon)}{q+1}$	$\frac{i\varepsilon(q^l-\varepsilon)}{q+1} - \varepsilon q^l$	$\frac{(q-i+1)(q^{2l}-1)}{q+1}$	$\frac{(q^{2l}-1)i}{q+1}$
CY4	q^{2l}	$i(q^l-1)$ $2 \leqslant i \leqslant q^l$	$q^l+i(i-3)$	$i(i-1)$	q^l-i	$-i$	$i(q^l-1)$	$(q^l-1)(q^l+1-i)$
RT1	q^{2l}	$(q^l-1)(q+1)$	$q(q^l-1)+q^2-2$	$q(q+1)$	q^l-q-1	$-(q+1)$	$(q+1)(q^l-1)$	$(q^l-1)(q^l-q)$
RT2	q^{2l}	$(q^l-\varepsilon)(q^{l-1}+\varepsilon)$ where $\varepsilon = \pm 1$	$q-2+$ $q(q^{l-1}-\varepsilon)(q^{l-2}+\varepsilon)$	$q^{2l-2}+\varepsilon q^{l-1}$	$\varepsilon q^{l-1}(q-1)-1$	$-(\varepsilon q^{l-1}+1)$	$(q^l-\varepsilon)(q^{l-1}+\varepsilon)$	$q^{l-1}(q-1)(q^l-\varepsilon)$
RT3	q^{2l}	$(q^l-\varepsilon)(q^{l-1}+\varepsilon)$ where $\varepsilon = (-1)^l$	$q-2+$ $q(q^{l-1}-\varepsilon)(q^{l-2}+\varepsilon)$	$q^{2l-2}+\varepsilon q^{l-1}$	$\varepsilon q^{l-1}(q-1)-1$	$-(\varepsilon q^{l-1}+1)$	$(q^l-\varepsilon)(q^{l-1}+\varepsilon)$	$q^{l-1}(q-1)(q^l-\varepsilon)$
RT4	q^{10}	$(q^5-1)(q^2+1)$	$q-2+$ $q(q+1)(q^3-1)$	$q^2(q^2+1)$	q^5-q^2-1	$-(q^2+1)$	$(q^5-1)(q^2+1)$	$q^2(q^5-1)(q^3-1)$
RT5	2048	759	310	264	55	−9	276	1771
RT5[d]	2048	276	44	36	20	−12	759	1288
RT6	243	22	1	2	4	−5	132	110
RT6[d]	243	132	81	60	24	−3	22	220
FE1	q^{2l} q odd	$\frac{1}{2}q^{l-1}(q^l-\varepsilon)(q-1)$ where $\varepsilon = \pm 1$	$\frac{5}{4}q^{2l-2}(q-1)^2$ $-\left(\frac{q-3}{2}\right)\varepsilon q^{l-1}$	$\frac{1}{2}(q-1) \times$ $(\frac{1}{2}q^{2l-2}(q-1)-\varepsilon q^{l-1})$.	$-\frac{1}{2}\varepsilon q^{l-1}(q-1)$	$\frac{1}{2}\varepsilon q^{l-1}$	$q^{2l}-1-$ $\frac{1}{2}q^{l-1}(q^l-\varepsilon)(q-1)$	$\frac{1}{2}q^{l-1}(q^l-\varepsilon)(q-1)$
FE2	729	112	1	20	4	−23	616	112
FE3	4096	234	2	14	10	−22	2808	1287
FE3[d]	4096	2808	1960	1848	120	−8	234	3861
FE4	81	30	9	12	3	−6	50	30

FIGURE 2b.

The notation $TF1^d$ denotes the projective dual of Example TF1 (see Section 5). Recall that Example CY3 is subsumed by Example SU1 (see Section 9).

Figure 2 lists the parameters N, K, λ, and μ of the corresponding strongly regular graph. It also lists the eigenvalues ρ_1 and ρ_2 of $G(\Omega)$ other than the valence K, and their multiplicities A_{w_1} and A_{w_2} respectively. Recall from (3.5) that $\rho_i = K - qw_i$, for $i = 1, 2$ and that A_{w_i} is the number of codewords of C with weight w_i.

NOTE ADDED IN PROOF. New results have been obtained since this paper was submitted. A. E. Brouwer has constructed new examples of projective (n, k, h_1, h_2) sets by taking a quadric defined over a small field and cutting out a quadric defined over a larger field (A. E. BROUWER, 'Some new two-weight codes and strongly regular graphs', *Discrete Applied Math.* 10 (1985) 111–114). N. Tzanakis and J. Wolfskill have determined the possible parameters of projective (n, k, h_1, h_2) caps by finding all integer solutions to equation (12.2). There are no parameter sets other than those appearing in Theorem 12.1 and the remarks following that theorem (N. TZANAKIS and J. WOLFSKILL, 'The diophantine equation $x^2 = 4q^{a/2} + 4q + 1$ with an application to coding theory', *J. Number Theory*, to appear). The second author has shown that construction SU2 produces large numbers of pairwise inequivalent two-weight codes having the same parameters (W. M. KANTOR, 'Exponential numbers of two-weight codes, difference sets, and symmetric designs', *Discrete Math.* 46 (1983) 95–98).

References

1. E. R. BERLEKAMP, J. H. VAN LINT and J. J. SEIDEL, 'A strongly regular graph derived from the perfect ternary Golay code', *A survey of combinatorial theory* (ed. J. N. Srivastava, North-Holland, Amsterdam, 1973), pp. 25–30.
2. F. BUEKERS, 'On the generalized Ramanujan–Nagell equation I', *Acta Arith.* 38 (1981) 389–410.
3. R. C. BOSE and D. M. MESNER, 'On linear associative algebras corresponding to association schemes of partially balanced designs', *Ann. Math. Statist.* 30 (1959) 21–38.
4. R. C. BOSE and T. SHIMAMOTO, 'Classification and analysis of partially balanced incomplete block designs with two associate classes', *J. Amer. Statist. Assoc.* 47 (1952) 151–184.
5. A. BREMNER, R. CALDERBANK, P. HANLON, P. MORTON and J. WOLFSKILL, 'Two-weight ternary codes and the equation $y^2 = 4.3^a + 13$', *J. Number Theory* 16 (1983) 212–234.
6. A. A. BRUEN and J. W. P. HIRSCHFELD, 'Applications of line geometry over finite fields II. The hermitian surface', *Geom. Dedicata* 7 (1978) 333–353.
7. A. A. BRUEN and J. A. THAS, 'Partial spreads, packings and hermitian manifolds in PG(3, q)', *Math. Z.* 125 (1972) 122–128.
8. R. CALDERBANK, 'On uniformly packed $[n, n-k, 4]$ codes over GF(q) and a class of caps in PG($k-1, q$)', *J. London Math. Soc.* 26 (1982) 365–384.
9. P. J. CAMERON and J. H. VAN LINT, 'On the partial geometry pg (6, 6, 2)', *J. Comb. Theory* (*A*) 32 (1982) 252–255.
10. P. J. CAMERON, 'Partial quadrangles', *Quart. J. Math.* 26 (1975) 61–73.
11. P. CAMION, *Difference sets in elementary abelian groups* (Les Presses de L'Université de Montréal, 1979).
12. J. H. CONWAY, 'Three lectures on exceptional groups', *Finite simple groups* (ed. M. B. Powell and G. Higman, Academic Press, New York, 1971), pp. 215–247.
13. H. S. M. COXETER, 'Twelve points in PG(5, 3) with 95040 self-transformations', *Proc. Royal Soc.* (*A*) 247 (1958) 279–293.
14. P. DELSARTE, 'Two-weight linear codes and strongly regular graphs', Report R160, MBLE Res. Lab., Brussels, 1971.
15. P. DELSARTE, 'Weights of linear codes and strongly regular normed spaces', *Discrete Math.* 3 (1972) 47–64.
16. P. DELSARTE, 'An algebraic approach to the association schemes of coding theory', *Philips Research Reports Supplements* 10, 1973.
17. P. DELSARTE and J. M. GOETHALS, 'Irreducible binary cyclic codes of even dimension', *Combinatorial mathematics and its applications*, Proc. Second Chapel Hill Conference (Univ. of N. Carolina, Chapel Hill, N.C., 1970), pp. 100–113.
18. P. DELSARTE and J. M. GOETHALS, 'Alternating bilinear forms over GF(q)', *J. Comb. Theory* (*A*) 19 (1975) 26–50.
19. P. DEMBOWSKI, *Finite geometries* (Springer-Verlag, Berlin, 1968).
20. R. H. F. DENNISTON, 'Some maximal arcs in finite projective planes', *J. Comb. Theory* 6 (1969) 317–319.
21. L. E. DICKSON, *Linear groups with an exposition of the Galois field theory* (Dover, New York, 1958).
22. J. DIEUDONNÉ, *La géométrie des groupes classiques* (3-ème édition, Springer, Berlin, 1971).
23. J. F. DILLON, 'Elementary Hadamard difference sets', Ph.D. Thesis, Univ. of Maryland, 1974.

24. J. F. Dillon, 'Elementary Hadamard difference sets', *Proc. 6th S-E Conf. Combinatorics, Graph Theory and Computing* (Utilitas Math., Winnepeg, 1975), pp. 237–249.
25. S. M. Dodunekov and V. I. Iorgov, 'Distribution of weights of irreducible cyclic codes and strongly regular graphs', *Problems Inform. Transmission* 16 (1980) no. 2, 105–110.
26. M. de Finis, 'On k-sets of type (m, n) in projective planes of square order', *Finite geometries and designs*, L.M.S. Lecture Note Series 49 (Cambridge Univ. Press, 1981), pp. 98–103.
27. D. A. Foulser, 'Solvable primitive permutation groups of low rank', *Trans. Amer. Math. Soc.* 143 (1969) 1–54.
28. R. A. Games, 'The packing problem for finite projective geometries', Thesis, The Ohio State University, 1980.
29. J. M. Goethals and H. C. A. van Tilborg, 'Uniformly packed codes', *Philips Research Reports* 30 (1975) 9–36.
30. R. Hill, 'On the largest size cap in $S_{5,3}$', *Rend. Accad. Naz. Lincei* (8) 54 (1973) 378–384.
31. R. Hill, 'Caps and groups', *Atti dei Convegni Lincei, Colloquio Internazionale sulle Teorie Combinatorie (Roma 1973)*, no. 17 (Accad. Naz. Lincei, 1976), pp. 384–394.
32. R. Hill, 'Caps and codes', *Discrete Math.* 22 (1978) 111–137.
33. J. W. P. Hirschfeld, *Projective geometries over finite fields* (Oxford Univ. Press, Oxford, 1979).
34. X. L. Hubaut, 'Strongly regular graphs', *Discrete Math.* 13 (1975) 357–381.
35. W. M. Kantor, 'Symplectic groups, symmetric designs, and line ovals', *J. Algebra* 33 (1975) 43–58.
36. W. M. Kantor, 'Spreads, translation planes, and Kerdock sets I', *SIAM J. Algebraic Discrete Methods* 3 (1982) 151–165.
37. J. H. van Lint, 'A survey of perfect codes', *Rocky Mountain J. Math.* 5 (1975) 199–224.
38. J. H. van Lint and A. Schrijver, 'Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields', *Combinatorica* 1 (1981) 63–75.
39. H. Lüneburg, *Translation planes* (Springer, New York, 1980).
40. J. McLaughlin, 'A simple group of order 898, 128, 000', *Theory of finite groups* (Benjamin, New York, 1969), pp. 109–111.
41. F. J. MacWilliams, 'Combinatorial problems of elementary group theory', Thesis, Department of Math., Harvard University, 1962.
42. F. J. MacWilliams, 'A theorem on the distribution of weights in a systematic code', *Bell System Tech. J.* 42 (1963) 79–94.
43. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes* (North-Holland, Amsterdam, 1977).
44. H. B. Mann, 'Difference sets in elementary abelian groups', *Illinois J. Math.* 9 (1965) 212–219.
45. R. J. McEliece, 'A class of two-weight codes', J. P. L. Space Programs Summary, 37–41, Vol. IV, pp. 264–266.
46. R. Me~z, 'On point sets with two intersection numbers', unpublished report.
47. O. S. Rothaus, 'On "bent" functions', *J. Comb. Theory (A)* 20 (1976) 300–305.
48. B. Segre, 'Forme e geometrie hermitiane, con particolare riguardo al caso finito', *Ann. Mat. Pura Appl.* 70 (1965) 1–202.
49. N. V. Semakov, V. A. Zinovjev and G. V. Zaitzev, 'Uniformly packed codes', *Problems Inform. Transmission* 7 (1971) no. 1, 30–39.
50. M. Tallini-Scafati, '(k, n)-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri. Note I, II', *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Nat.* (8) 40 (1966) 812–818, 1020–1025.
51. J. A. Thas, 'A combinatorial problem', *Geom. Dedicata* 1 (1973) 236–240.
52. A. Tietäväinen, 'A short proof for the non-existence of unknown perfect codes over GF(q), $q > 2$', *Ann. Acad. Sci. Fenn. Ser. A I. Math.* 580 (1974) 1–6.
53. H. C. A. van Tilborg, 'Uniformly packed codes', Thesis, Tech. Univ. Eindhoven, 1976.
54. J. Tits, 'Ovoïdes et groupes de Suzuki', *Arch. Math.* 13 (1962) 187–198.
55. J. Wolfmann, 'Formes quadratiques et codes à deux poids', *C. R. Acad. Sci. Paris* 281 (1975) A533–A535.
56. J. Wolfmann, 'Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie', *Discrete Math.* 14 (1975) 185–211.
57. J. Wolfmann, 'Propriétés combinatoires déduites de l'étude des codes à deux poids', *C. R. Acad. Sci. Paris* 284 (1977) A641–A642.
58. J. Wolfmann, 'Codes projectifs à deux poids, "caps" complets et ensembles de différences', *J. Comb. Theory (A)* 23 (1977) 208–222.

Bell Laboratories
Murray Hill
N.J. 07974, USA

Mathematics Department
University of Oregon
Eugene, OR 97403, USA