Chapter 1

Two-weight Codes

1.1 Generalities

A *linear code* C with *length* n, *dimension* m, and *minimum distance* d over the field $\mathbb{F}_q$ (in short, an $[n, m, d]_q$-code) is an m-dimensional subspace of the vector space $\mathbb{F}_q^n$ such that any two code words (elements of C) differ in at least d coordinates.

The *weight* $\mathrm{wt}(c)$ of the code word c is its number of nonzero coordinates. A weight of C is the weight of some code word in C.

A *two-weight code* is a linear code with exactly two nonzero weights.

A *generator matrix* for C is an $m \times n$ matrix M such that its rows span C.

The *weight enumerator* of C is the polynomial $\sum f_i X^i$ where the coefficient f_i of X^i is the number of words of weight i in C.

The *dual code* $C^\perp$ of C is the $(n-m)$-dimensional code consisting of the vectors orthogonal to all of C for the inner product $(u, v) = \sum u_i v_i$.

1.2 Codes as projective multisets

Let C be a linear code of length n and dimension m over the field $\mathbb{F}_q$. Let the $m \times n$ matrix M be a generator matrix of C.

The columns of M are elements of $V = \mathbb{F}_q^m$, the m-dimensional vector space over $\mathbb{F}_q$, and up to coordinate permutation the code C is uniquely determined by the n-multiset of column vectors consisting of the columns of M.

Let us call a coordinate position where C is identically zero a *zero position*. The code C will have zero positions if and only if the dual code $C^\perp$ has words of weight 1. Usually, zero positions are uninteresting and can be discarded.

Let PV be the projective space of which the points are the 1-spaces in V. If C does not have zero positions, then each column c of M determines a projective point $\langle c \rangle$ in PV, and we find a projective multiset X of size n in PV. Note that PV is spanned by X.

In this way we get a 1-1 correspondence between codes C without zero positions (up to equivalence) and projective multisets X (up to nonsingular linear transformations): If C' is an arbitrary code equivalent to C, and M' a generator matrix for C', then $M' = AMB$, where A is a nonsingular matrix of order m (so that $AC = C$), and B is a monomial matrix of order n (a matrix with a single nonzero entry in each row and column), so that $XB = X$.

The code C is called *projective* when no two coordinate positions are dependent, i.e., when the dual code $C^\perp$ has minimum distance at least 3. This condition says that the multiset does not contain repeated points, i.e., is a set.

1.2.1 Weights

Let Z be the (multi)set of columns of M, so that $V = \langle Z \rangle$. We can extend any code word $u = (u(z))_{z \in Z} \in C$ to a linear functional on V. Let X be the projective (multi)set in PV determined by the columns of M. For $u \neq 0$, let H_u be the hyperplane in PV defined by $u(z) = 0$. The weight of the code word u is its number of nonzero coordinates, which equals $\mathrm{wt}(u) = n - |X \cap H_u|$.

So, searching for codes with a large minimum distance is the same as searching for a projective (multi)set such that all hyperplane intersections are small. Searching for a code with few different weights is the same as searching for a projective (multi)set such that its hyperplane sections only have a few different sizes.

1.2.2 Example

Consider codes with dimension $m = 3$ and minimum distance $d = n - 2$. According to the above, these correspond to subsets X of the projective plane $PG(2, q)$ such that each line meets X in at most 2 points. It follows that X is an arc (or a double point). For odd q the best one can do is to pick a conic (of size $q + 1$) and one finds $[q + 1, 3, q - 1]_q$ codes. For even q one can pick a hyperoval (of size $q + 2$) and one finds $[q + 2, 3, q]_q$ codes. The $[6, 3, 4]_4$ code is the famous hexacode ([16]).

1.3 Graphs

Let Γ be a graph with vertex set S of size s, undirected, without loops or multiple edges. For $x, y \in S$ we write $x = y$ or $x \sim y$ or $x \not\sim y$ when the vertices x and y are equal, adjacent, or nonadjacent, respectively. The *adjacency matrix* of Γ is the matrix A of order s with rows and columns indexed by S, where $A_{xy} = 1$ if $x \sim y$ and $A_{xy} = 0$ otherwise. The *spectrum* of Γ is the spectrum of A, that is, its (multi)set of eigenvalues.

1.3.1 Difference sets

Given an abelian group G and a subset D of G such that $D = -D$ and $0 \notin D$, we can define a graph Γ with vertex set G by letting $x \sim y$ whenever $y - x \in D$. This graph is known as the *Cayley graph* on G with difference set D.

If A is the adjacency matrix of Γ, and χ is a character of G, then $(A\chi)(x) = \sum_{y \sim x} \chi(y) = \sum_{d \in D} \chi(x + d) = (\sum_{d \in D} \chi(d))\chi(x)$. It follows that the eigenvalues of Γ are the numbers $\sum_{d \in D} \chi(d)$, where χ runs through the characters of G. In particular, the trivial character χ_0 yields the eigenvalue $|D|$, the valency of Γ.

1.3.2 Using a projective set as difference set

Let V be a vector space of dimension m over the finite field $\mathbb{F}_q$. Let X be a subset of size n of the point set of the projective space PV. Define a graph Γ with vertex set V by letting $x \sim y$ whenever $\langle y-x\rangle \in X$. This graph has $v = q^m$ vertices, and is regular of valency $k = (q-1)n$.

Let q be a power of the prime p, let $\zeta = e^{2\pi i/p}$ be a primitive p-th root of unity, and let $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace function. Let V^* be the dual vector space to V, that is the space of linear forms on V. Then the characters χ are of the form $\chi_a(x) = \zeta^{\mathrm{tr}(a(x))}$, with $a \in V^*$. Now

$$\sum_{\lambda\in\mathbb{F}_q} \chi_a(\lambda x) = \begin{cases} q & \text{if } a(x) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $\sum_{d\in D} \chi_a(d) = q.|H_a \cap X| - |X|$ where H_a is the hyperplane $\{\langle x\rangle \mid a(x) = 0\}$ in PV.

This can be formulated in terms of coding theory. To the set X corresponds a (projective) linear code C of length n and dimension m. Each $a \in V^*$ gives rise to the vector $(a(x))_{x\in X}$ indexed by X, and the collection of all these vectors is the code C. A code word a of weight w corresponds to a hyperplane H_a that meets X in $n-w$ points, and hence to an eigenvalue $q(n-w)-n = k-qw$. The number of code words of weight w in C equals the multiplicity of the eigenvalue $k-qw$ of Γ.

1.3.3 Strongly regular graphs

A *strongly regular graph* with parameters (v, k, λ, μ) is a graph on v vertices, regular of valency k, where $0 < k < v-1$ (there are both edges and non-edges), such that the number of common neighbours of any two distinct vertices equals λ if they are adjacent, and μ if they are nonadjacent. For the adjacency matrix A of the graph this means that $A^2 = kI + \lambda A + \mu(J-I-A)$, where J is the all-1 matrix. A regular graph is strongly regular precisely when apart from the valency it has precisely two distinct eigenvalues. The eigenvalues of Γ, that is, the eigenvalues of A, are the valency k and the two solutions of $x^2 + (\mu-\lambda)x + \mu - k = 0$.

In the above setting, with a graph Γ on a vector space, with adjacency defined by a projective set X as difference set, the graph Γ will be strongly regular precisely when $|H \cap X|$ takes only two different values for hyperplanes H, that is, when the code corresponding to X is a two-weight code.

This 1-1-1 correspondence between projective two-weight codes, projective sets that meet the hyperplanes in two cardinalities (these are known as *2-character sets*), and strongly regular graphs defined on a vector space by a projective difference set, is due to Delsarte [21].

The more general case of a code C with dual $C^\perp$ of minimum distance at least 2 corresponds to a multiset X. Brouwer & van Eupen [10] gives a 1-1 correspondence between arbitrary projective codes and arbitrary two-weight codes. See §1.9 below.

A survey of two-weight codes was given by Calderbank & Kantor [13]. Additional families and examples are given in [19], [18]. In [7] numerical data (such as the number of nonisomorphic codes and the order of the automorphism group) is given for small cases.

1.3.4 Parameters

Let V ba a vector space of dimension m over $\mathbb{F}_q$. Let X be a subset of size n of the point set of PV, that meets hyperplanes in either m_1 or m_2 points, where $m_1 > m_2$. Let f_1 and f_2 be the numbers of such hyperplanes. Then f_1 and f_2 satisfy

$$f_1 + f_2 = \frac{q^m - 1}{q - 1},$$
$$f_1 m_1 + f_2 m_2 = n\frac{q^{m-1} - 1}{q - 1},$$
$$f_1 m_1(m_1 - 1) + f_2 m_2(m_2 - 1) = n(n-1)\frac{q^{m-2} - 1}{q - 1}$$

and it follows that

$$(q^m - 1)m_1 m_2 - n(q^{m-1} - 1)(m_1 + m_2 - 1) + n(n-1)(q^{m-2} - 1) = 0,$$

so that in particular $n \mid (q^m - 1)m_1 m_2$.

The corresponding two-weight code is a q-ary linear code with dimension m, length n, weights $w_1 = n - m_1$ and $w_2 = n - m_2$, minimum distance w_1, and weight enumerator $1 + (q-1)f_1 X^{w_1} + (q-1)f_2 X^{w_2}$.
Here $(q-1)f_1 = \frac{1}{w_2 - w_1}(w_2(q^m - 1) - nq^{m-1}(q-1))$.

The corresponding strongly regular graph Γ has parameters

$$\begin{aligned}
v &= q^m, \\
k &= (q-1)n, \\
r &= qm_1 - n, \\
s &= qm_2 - n, \\
\lambda &= \mu + r + s, \\
\mu &= rs + k = \frac{w_1 w_2}{q^{m-2}}, \\
f &= (q-1)f_1, \\
g &= (q-1)f_2,
\end{aligned}$$

where r, s are the eigenvalues of Γ other than k (with $r \geq 0 > s$) and f, g their multiplicities.

For example, the hyperoval in $PG(2,4)$ $(m = 3, q = 4, n = 6)$ gives the linear $[6,3,4]_4$ code (with weight enumerator $1+45X^4+18X^6$), but also corresponds to a strongly regular graph with parameters $(v,k,\lambda,\mu) = (64,18,2,6)$ and spectrum $18^1\ 2^{45}\ (-6)^{18}$.

It is not often useful, but one can also check the definition of strong regularity directly. The graph Γ defined by the difference set X will be strongly regular with constants λ,μ if and only if each point outside X is collinear with μ ordered pairs of points of X, while each point p inside X is collinear with $\lambda - (q-2)$ ordered pairs of points of $X \setminus \{p\}$.

1.3.5 Complement

Passing from a 2-character set X to its complement corresponds to passing from the strongly regular graph to its complement. The two-weight codes involved have a more complicated relation and will look very different, with different lengths and minimum distances.

For example, the dual of the ternary Golay code is a $[11,5,6]_3$-code with weights 6 and 9. It corresponds to an 11-set in $PG(4,3)$ such that hyperplanes meet it in 5 or 2 points. Its complement is a 110-set in $PG(4,3)$ such that hyperplanes meet it in 35 or 38 points. It corresponds to a $[110,5,72]_3$-code with weights 72 and 75.

1.3.6 Duality

Suppose X is a subset of the point set of PV that meets hyperplanes in either m_1 or m_2 points. We find a subset Y of the point set of the dual space PV^* consisting of the hyperplanes that meet X in m_1 points. Also Y is a 2-character set. If each point of PV is on n_1 or n_2 hyperplanes in Y, with $n_1 > n_2$, then $n_2 = \frac{n(q^{m-2}-1)-m_2(q^{m-1}-1)}{(q-1)(m_1-m_2)}$ and $(m_1-m_2)(n_1-n_2) = q^{m-2}$. It follows that the difference of the weights in a projective two-weight code is a power of the characteristic. (This is a special case of the duality for translation association schemes. See [22], §2.6, and [9], §2.10B.)

To a pair of complementary sets or graphs belongs a dual pair of complementary sets or graphs. The valencies $k, v-k-1$ of the dual graph are the multiplicities f_1, f_2 of the graph.

Let C be the two-weight code belonging to X. Then the graph belonging to Y has vertex set C, where code words are joined when their difference has weight w_1.

For example, for the above $[11,5,6]_3$-code (with weight enumerator $1 + 132X^6 + 110X^9$) the corresponding strongly regular graph has parameters $(v,k,\lambda,\mu) = (243,22,1,2)$ and spectrum $22^1\ 4^{132}\ (-5)^{110}$. One of the two dual graphs has parameters $(v,k,\lambda,\mu) = (243,110,37,60)$ and spectrum $110^1\ 2^{220}\ (-25)^{22}$. The corresponding two-weight code is a $[55,5,36]_3$-code with weights 36 and 45.

1.3.7 Field change

Our graphs are defined by a difference set in an abelian group, and are independent of a multiplicative field structure we put on that additive group.

Suppose V is a vector space of dimension m over F, where F has a subfield F_0 with $[F : F_0] = e$, say $F = \mathbb{F}_q$, $F_0 = \mathbb{F}_r$, with $q = r^e$. Let V_0 be V, but regarded as a vector space (of dimension me) over F_0. Each projective point in PV corresponds to $\frac{q-1}{r-1}$ projective points in PV_0. If our graph belonged to a projective subset X of size n of PV, it also belongs to a set X_0 of size $n\frac{q-1}{r-1}$ of PV_0. If the intersection numbers were m_i before, they will be $\frac{r^e-1}{r-1}m_i + \frac{r^{e-1}-1}{r-1}(n - m_i)$ now. We see that a q-ary code of dimension m, length n, and weights w_i becomes an r-ary code of dimension me, length $n\frac{q-1}{r-1}$ and weights $w_i\frac{q}{r}$.

1.4 Irreducible cyclic two-weight codes

In the case of a vector space that is a field F, one conjectures that all examples are known of difference sets that are subgroups of the multiplicative group F^* containing the multiplicative group of the base field.

Conjecture 1.4.1 (Schmidt & White [62], Conj. 4.4; cf. [35], Conj. 1.2) *Let F be a finite field of order $q = p^f$. Suppose $1 < e \mid (q-1)/(p-1)$ and let D be the subgroup of F^* of index e. If the Cayley graph on F with difference set D is strongly regular, then one of the following holds:*

(i) (subfield case) D is the multiplicative group of a subfield of F.

(ii) (semiprimitive case) There exists a positive integer l such that $p^l \equiv -1 \pmod{u}$.

(iii) (exceptional case) $|F| = p^f$, and (e, p, f) takes one of the following eleven values: $(11, 3, 5)$, $(19, 5, 9)$, $(35, 3, 12)$, $(37, 7, 9)$, $(43, 11, 7)$, $(67, 17, 33)$, $(107, 3, 53)$, $(133, 5, 18)$, $(163, 41, 81)$, $(323, 3, 144)$, $(499, 5, 249)$.

In each of the mentioned cases the graph is strongly regular. These graphs correspond to two-weight codes over $\mathbb{F}_p$.

Since F^* has a partition into cosets of D, the point set of the projective space PF is partitioned into isomorphic copies of the two-intersection set $X = \{\langle d \rangle \mid d \in D\}$.

See also [60], [28], [65].

1.5 Cyclotomy

More generally, the difference set D can be be a union of cosets of a subgroup of F^*, for some finite field F. Let $F = \mathbb{F}_q$ where $q = p^f$, p is prime, and let $e \mid q-1$, say $q = em+1$. Let $K \subseteq \mathbb{F}_q^*$ be the subgroup of the e-th powers (so that $|K| = m$). Let α be a primitive element of $\mathbb{F}_q$. For $J \subseteq \{0, 1, \ldots, e-1\}$ put $u := |J|$ and $D := D_J := \bigcup\{\alpha^j K \mid j \in J\} = \{\alpha^{ie+j} \mid j \in J,\, 0 \le i < m\}$. Define a graph $\Gamma = \Gamma_J$ with vertex set $\mathbb{F}_q$ and edges (x, y) whenever $y - x \in D$. Note that Γ will be undirected if q is even or $e|(q-1)/2$.

As before, the eigenvalues of Γ are the sums $\sum_{d\in D} \chi(d)$ for the characters χ of F. Their explicit determination requires some theory of Gauss sums. Let us write $A\chi = \theta(\chi)\chi$. Clearly, $\theta(1) = mu$, the valency of Γ. Now assume $\chi \neq 1$. Then $\chi = \chi_g$ for some g, where

$$\chi_g(\alpha^j) = \exp\left(\frac{2\pi i}{p}\mathrm{tr}(\alpha^{j+g})\right)$$

and $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace function. If μ is any multiplicative character of order e (say, $\mu(\alpha^j) = \zeta^j$, where $\zeta = \exp(\frac{2\pi i}{e})$), then

$$\sum_{i=0}^{e-1} \mu^i(x) = \begin{cases} e & \text{if } \mu(x) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\theta(\chi_g) = \sum_{d\in D} \chi_g(d) = \sum_{j\in J}\sum_{y\in K} \chi_{j+g}(y) = \frac{1}{e}\sum_{j\in J}\sum_{x\in\mathbb{F}_q^*} \chi_{j+g}(x)\sum_{i=0}^{e-1}\mu^i(x) =$$

$$= \frac{1}{e}\sum_{j\in J}\left(-1 + \sum_{i=1}^{e-1}\sum_{x\neq 0}\chi_{j+g}(x)\mu^i(x)\right) = \frac{1}{e}\sum_{j\in J}\left(-1 + \sum_{i=1}^{e-1}\mu^{-i}(\alpha^{j+g})G_i\right)$$

where G_i is the Gauss sum $\sum_{x\neq 0} \chi_0(x)\mu^i(x)$.

In a few cases these sums can be evaluated.

Proposition 1.5.1 (Stickelberger and Davenport & Hasse; see [56]) *Suppose $e > 2$ and p is semiprimitive $\bmod e$, i.e., there exists an l such that $p^l \equiv -1 \pmod e$. Choose l minimal and write $f = 2lt$. Then*

$$G_i = (-1)^{t+1}\varepsilon^{it}\sqrt{q},$$

where

$$\varepsilon = \begin{cases} -1 & \text{if } e \text{ is even and } (p^l+1)/e \text{ is odd} \\ +1 & \text{otherwise.} \end{cases}$$

Under the hypotheses of this proposition, we have

$$\sum_{i=1}^{e-1} \mu^{-i}(\alpha^{j+g})G_i = \sum_{i=1}^{e-1} \zeta^{-i(j+g)}(-1)^{t+1}\varepsilon^{it}\sqrt{q} = \begin{cases} (-1)^t\sqrt{q} & \text{if } r \neq 1, \\ (-1)^{t+1}\sqrt{q}(e-1) & \text{if } r = 1, \end{cases}$$

where $r = r_{g,j} = \zeta^{-j-g}\varepsilon^t$ (so that $r^e = \varepsilon^{et} = 1$), and hence

$$\theta(\chi_g) = \frac{u}{e}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q} \,.\, \#\{j \in J \mid r_{g,j} = 1\}.$$

If we abbreviate the cardinality in this formula with # then: If $\varepsilon^t = 1$ then $\# = 1$ if $g \in -J \pmod e$, and $\# = 0$ otherwise. If $\varepsilon^t = -1$ (then e is even and p is odd) then $\# = 1$ if $g \in \frac{1}{2}e - J \pmod e$, and $\# = 0$ otherwise. We proved:

Theorem 1.5.2 ([3], [12]) *Let $q = p^f$, p prime, $f = 2lt$ and $e \mid p^l + 1 \mid q - 1$. Let $u = |J|$, $1 \leq u \leq e - 1$. Then the graphs Γ_J are strongly regular with eigenvalues*

$$\begin{array}{rl} k = \frac{q-1}{e}u & \textit{with multiplicity 1,} \\ \frac{u}{e}(-1 + (-1)^t\sqrt{q}) & \textit{with multiplicity } q-1-k, \\ \frac{u}{e}(-1 + (-1)^t\sqrt{q}) + (-1)^{t+1}\sqrt{q} & \textit{with multiplicity } k. \end{array}$$

The will yield two-weight codes over $\mathbb{F}_r$ in case K is invariant under multiplication by nonzero elements in $\mathbb{F}_r$, i.e., when $e \mid \frac{q-1}{r-1}$. This is always true for $r = p^l$, but also happens, for example, when $q = p^{2lt}$, $r = p^{lt}$, $e \mid p^l + 1$ and t is odd.

1.5.1 The Van Lint-Schrijver construction

Van Lint & Schrijver [53] use the above setup in case e is an odd prime, and p primitive mod e (so that $l = (e-1)/2$ and $f = (e-1)t$), and notice that the group G consisting of the maps $x \mapsto ax^{p^i} + b$, where $a \in K$ and $b \in F$ and $i \geq 0$ acts as a rank 3 group on F.

1.5.2 The De Lange graphs

De Lange [51] found that one gets strongly regular graphs in the following three cases (that are not semiprimitive).

p	f	e	J
3	8	20	$\{0, 1, 4, 8, 11, 12, 16\}$
3	8	16	$\{0, 1, 2, 8, 10, 11, 13\}$
2	12	45	$\{0, 5, 10\}$

One finds two-weight codes over $\mathbb{F}_r$ for $r = 9, 3, 8$, respectively.

This last graph can be viewed as a graph with vertex set $\mathbb{F}_q^3$ for $q = 16$ such that each vertex has a unique neighbour in each of the $q^2 + q + 1 = 273$ directions.

1.5.3 Generalizations

The examples given by De Lange and by Ikuta & Munemasa [45, 46] ($p = 2$, $f = 20$, $e = 75$, $J = \{0, 3, 6, 9, 12\}$ and $p = 2$, $f = 21$, $e = 49$, $J = \{0, 1, 2, 3, 4, 5, 6\}$) and the sporadic cases of the Schmidt-White Conjecture 1.4.1 were generalized by Feng & Xiang [32], Ge, Xiang & Yuan [35], Momihara [57], and Wu [66], who find several further infinite families of strongly regular graphs. See also [58].

1.6 Rank 3 groups

Let Γ be a graph and G a group of automorphisms of Γ. The group G is called *rank 3* when it is transitive on vertices, edges, and non-edges. In this case, the graph Γ is strongly regular (or complete or empty).

All rank 3 groups have been classified in a series of papers by Foulser, Kallaher, Kantor, Liebler, Liebeck, Saxl and others. The affine case that interests us here was finally settled by Liebeck [52]

1.6.1 One-dimensional affine rank 3 groups

Let $q = p^r$ be a prime power, where p is prime. Consider the group $\mathrm{A\Gamma L}(1, q)$ consisting of the semilinear maps $x \mapsto ax^\sigma + b$ on $\mathbb{F}_q$. Let T be the subgroup of size q consisting of the translations $x \mapsto x + b$. We classify the rank 3 subgroups R of $\mathrm{A\Gamma L}(1, q)$ that contain T. They are the groups generated by T and H, where H fixes 0 and has two orbits on the nonzero elements.

Consider the 1-dimensional semilinear group $G = \Gamma L(1, q)$ acting on the nonzero elements of $\mathbb{F}_q$. It consists of the maps $t_{a,i} : x \mapsto ax^\sigma$, where $a \neq 0$ and $\sigma = p^i$. Foulser & Kallaher ([34], §3) determined which subgroups H of G have precisely two orbits.

Lemma 1.6.1 *Let H be a subgroup of $\Gamma L(1, q)$. Then $H = \langle t_{b,0} \rangle$ for suitable b, or $H = \langle t_{b,0}, t_{c,s} \rangle$ for suitable b, c, s, where $s|r$ and $c^{(q-1)/(p^s-1)} \in \langle b \rangle$.*

Proof. The subgroup of all elements $t_{a,0}$ in H is cyclic and has a generator $t_{b,0}$. If this was not all of H, then $H/\langle t_{b,0} \rangle$ is cyclic again, and has a generator $t_{c,s}$ with $s|r$. Since ${t_{c,s}}^i = t_{c^j,is}$ where $j = 1 + p^s + p^{2s} + \cdots + p^{(i-1)s}$, it follows for $i = r/s$ that $c^{(q-1)/(p^s-1)} \in \langle b \rangle$. $\square$

Theorem 1.6.2 *$H = \langle t_{b,0} \rangle$ has two orbits if and only if q is odd and H consists precisely of the elements $t_{a,0}$ with a a square in $\mathbb{F}_q^*$.*

Proof. Let b have multiplicative order m. Then $m|(q-1)$, and $\langle t_{b,0}\rangle$ has d orbits, where $d=(q-1)/m$. $\square$

Let b have order m and put $d=(q-1)/m$. Choose a primitive element $\omega \in \mathbb{F}_q^*$ with $b=\omega^d$. Let $c=\omega^e$.

Theorem 1.6.3 *$H=\langle t_{b,0}, t_{c,s}\rangle$ (where $s|r$ and $d\,|\,e(q-1)/(p^s-1)$) has two orbits of different lengths n_1, n_2, where $n_1<n_2$, $n_1+n_2=q-1$, if and only if (0) $n_1=m_1m$, where (1) the prime divisors of m_1 divide p^s-1, and (2) $v:=(q-1)/n_1$ is an odd prime, and p^{m_1s} is a primitive root mod v, and (3) $gcd(e,m_1)=1$, and (4) $m_1s(v-1)|r$.*

That settled the case of two orbits of different lengths. Next consider that of two orbits of equal length. As before, let b have order m and put $d=(q-1)/m$. Choose a primitive element $\omega\in\mathbb{F}_q^*$ with $b=\omega^d$. Let $c=\omega^e$.

Theorem 1.6.4 *$H=\langle t_{b,0}, t_{c,s}\rangle$ (where $s|r$ and $d\,|\,e(q-1)/(p^s-1)$) has exactly two orbits of the same length $(q-1)/2$ if and only if (0) $(q-1)/2=m_1m$, (1) the prime divisors of $2m_1$ divide p^s-1, (2) no odd prime divisor of m_1 divides e, (3) $m_1s|r$, (4) one of the following cases applies: (i) m_1 is even, $p^s\equiv 3 \pmod 8$, and e is odd, (ii) $m_1\equiv 2 \pmod 4$, $p^s\equiv 7 \pmod 8$, and e is odd, (iii) m_1 is even, $p^s\equiv 1 \pmod 4$, and $e\equiv 2 \pmod 4$, (iv) m_1 is odd and e is even.*

The graphs from Theorem 1.6.2 are the Paley graphs.

The Van Lint-Schrijver construction from §1.5.1 is the special case of Theorem 1.6.3 where $s=1$, $e=0$, $m_1=1$.

1.7 Two-character sets in projective space

Since projective two-weight codes correspond to 2-character sets in projective space, we want to classify the latter. The surrounding space will always be the projective space PV, where V is an m-dimensional vector space over $\mathbb{F}_q$.

1.7.1 Subspaces

(i) Easy examples are subspaces of PV. A subspace with vector space dimension i (projective dimension $i-1$), where $1\le i\le m-1$, has size $n=\frac{q^i-1}{q-1}$ and meets hyperplanes in either $m_1=\frac{q^i-1}{q-1}$ or $m_2=\frac{q^{i-1}-1}{q-1}$ points. Here $m_1-m_2=q^{i-1}$ can take many values.

(ii) If $m=2l$ is even, we can take the union of any family of pairwise disjoint l-subspaces. A hyperplane will contain either 0 or 1 of these, so that $n = \frac{q^l-1}{q-1}u$, $m_1 = \frac{q^{l-1}-1}{q-1}u + q^{l-1}$, $m_2 = \frac{q^{l-1}-1}{q-1}u$ where u is the size of the family, $1 \le u \le q^l$.

Clearly, one has a lot of freedom choosing this family of pairwise disjoint l-subspaces, and one obtains exponentially many nonisomorphic graphs with the same parameters (cf. [49]). There are many further constructions with these parameters, see, e.g., §1.7.2 (ii) below, the alternating forms graphs on $\mathbb{F}_q^5$ (with $u = q^2 + 1$, see [9], Thm. 9.5.6), and [15], [4], [5], [20], [27].

1.7.2 Quadrics

(i) Let $X = Q$ be the point set of a nondegenerate quadric in PV. Intersections $Q \cap H$ are quadrics in H, and in the cases where there is only one type of nondegenerate quadric in H, there are two intersection sizes, dependent on whether H is tangent or not.

More in detail: If m is even, then $n = |Q| = \frac{q^{m-1}-1}{q-1} + \varepsilon q^{m/2-1}$ with $\varepsilon = 1$ for a hyperbolic quadric, and $\varepsilon = -1$ for an elliptic quadric. A nondegenerate hyperplane meets Q in $m_1 = \frac{q^{m-2}-1}{q-1}$ points, and a tangent hyperplane meets Q in $m_2 = \frac{q^{m-2}-1}{q-1} + \varepsilon q^{m/2-1}$ points. (Here we dropped the convention that $m_1 > m_2$.) The corresponding weights are $w_1 = q^{m-2} + \varepsilon q^{m/2-1}$ and $w_2 = q^{m-2}$.

The corresponding graphs are known as the affine polar graphs $VO^{\varepsilon}(m, q)$.

In the special case $m = 4$, $\varepsilon = -1$ one has $n = q^2 + 1$, $m_1 = q + 1$, $m_2 = 1$, and not only the elliptic quadrics but also the Tits ovoids have these parameters.

(ii) The above construction with $\varepsilon = 1$ has the same parameters as the subspaces construction in §1.7.1 (ii) with $u = q^{m/2-1}+1$. Brouwer et al. [11] gave a common generalization of both by taking (for $m = 2l$) the disjoint union of pairwise disjoint l-spaces and nondegenerate hyperbolic quadrics, where possibly a number of pairwise disjoint l-spaces contained in some of the hyperbolic quadrics is removed.

(iii) For odd q and even m, consider a nondegenerate quadric Q of type $\varepsilon = \pm 1$ in V, the m-dimensional vector space over $\mathbb{F}_q$. The nonisotropic points fall into two classes of equal size, depending on whether $Q(x)$ is a square or not. Both sets are (isomorphic) 2-character sets.

Let X be the set of nonisotropic projective points x where $Q(x)$ is a nonzero square (this is well-defined). Then $|X| = \frac{1}{2}(q^{m-1} - \varepsilon q^{m/2-1})$ and $m_1, m_2 = \frac{1}{2}q^{m/2-1}(q^{m/2-1} \pm 1)$ (independent of ε).

The corresponding graphs are known as $VNO^{\varepsilon}(m, q)$.

(iv) In Brouwer [8] a construction for two-weight codes is given by taking a quadric defined over a small field and cutting out a quadric defined over a larger field. Let $F_1 = \mathbb{F}_r$, and $F = \mathbb{F}_q$, where $r = q^e$ for some $e > 1$. Let V_1 be a vector space of dimension d over F_1, where d is even, and write V for V_1 regarded as a vector space of dimension de over F. Let $\mathrm{tr} : F_1 \to F$ be the trace map. Let $Q_1 : V_1 \to F_1$ be a nondegenerate quadratic form on V_1. Then $Q = \mathrm{tr} \circ Q_1$ is a nondegenerate quadratic form on V. Let $X = \{x \in PV \mid Q(x) = 0 \text{ and } Q_1(x) \neq 0\}$. Write $\varepsilon = 1$ ($\varepsilon = -1$) if Q is hyperbolic (elliptic).

Proposition 1.7.1 *In the situation described, the corresponding two-weight code has length* $n = |X| = (q^{e-1} - 1)(q^{de-e} - \varepsilon q^{de/2-e})/(q-1)$, *and weights* $w_1 = (q^{e-1} - 1)q^{de-e-1}$ *and* $w_2 = (q^{e-1} - 1)q^{de-e-1} - \varepsilon q^{de/2-1}$.

For example, this yields a projective binary $[68, 8]$-code with weights 32, 40. This construction was generalized in Hamilton [40].

1.7.3 Maximal arcs and hyperovals

A *maximal arc* in a projective plane $PG(2, q)$ is a 2-character set with intersection numbers $m_1 = a$, $m_2 = 0$, for some constant a $(1 < a < q)$. Clearly, maximal arcs have size $n = qa - q + a$, and necessarily $a \mid q$. For $a = 2$ these objects are called *hyperovals*, and exist for all even q. Denniston [23] constructed maximal arcs for all even q and all divisors a of q. Ball et al. [1] showed that there are no maximal arcs in $PG(2, q)$ when q is odd.

These arcs show that the difference between the intersection numbers need not be a power of q. Also for a unital one has intersection sizes 1 and $\sqrt{q} + 1$.

1.7.4 Baer subspaces

Let $q = r^2$ and let m be odd. Then $PG(m-1, q)$ has a partition into pairwise disjoint Baer subspaces $PG(m-1, r)$. Each hyperplane hits all of these in a $PG(m-3, r)$, except for one which is hit in a $PG(m-2, r)$. Let X be the union of u such Baer subspaces, $1 \leq u < (r^m + 1)/(r + 1)$. Then $n = |X| = u(r^m - 1)/(r - 1)$, $m_2 = u(r^{m-2} - 1)/(r - 1)$, $m_1 = m_2 + r^{m-2}$.

1.7.5 Hermitean quadrics

Let $q = r^2$ and let V be provided with a nondegenerate Hermitean form. Let X be the set of isotropic projective points. Then

$$\begin{aligned} n = |X| &= (r^m - \varepsilon)(r^{m-1} + \varepsilon)/(q-1), \\ w_2 &= r^{2m-3}, \\ w_1 - w_2 &= \varepsilon r^{m-2}, \end{aligned}$$

where $\varepsilon = (-1)^m$. If we view V as a vector space of dimension $2m$ over $\mathbb{F}_r$, the same set X now has $n = (r^m - \varepsilon)(r^{m-1} + \varepsilon)/(r-1)$, $w_2 = r^{2m-2}$, $w_1 - w_2 = \varepsilon r^{m-1}$, as expected, since the form is a nondegenerate quadratic form in $2m$ dimensions over $\mathbb{F}_r$. Thus, the graphs that one gets here are also graphs one gets from quadratic forms, but the codes here are defined over a larger field.

1.7.6 Sporadic examples

We give some small sporadic examples (or series of parameters for which examples are known, some of which are sporadic). Many of these also have a cyclotomic description.

q	m	n	w_1	w_2-w_1	comments
2	9	73	32	8	Fiedler & Klin [33]; [50]
2	9	219	96	16	dual
2	10	198	96	16	Kohnert [50]
2	11	276	128	16	Conway-Smith $2^{11}.M_{24}$ rank 3 graph
2	11	759	352	32	dual; [36]
2	12	$65i$	$32i$	32	Kohnert [50] $(12 \le i \le 31, i \ne 19)$
2	24	98280	47104	2048	Rodrigues [61]
4	5	$11i$	$8i$	8	Dissett [29] $(7 \le i \le 14, i \ne 8)$
4	6	78	56	8	Hill [42]
4	6	429	320	32	dual
4	6	147	96	16	[8]; Cossidente et al [17]
4	6	210	144	16	Cossidente et al [17]
4	6	273	192	16	§1.7.1; De Wispelaere & Van Maldeghem [26]
4	6	315	224	16	[8]; Cossidente et al [17]
8	4	117	96	8	De Lange [51]
16	3	78	72	4	De Resmini & Migliori [25]
3	5	11	6	3	dual of the ternary Golay code
3	5	55	36	9	dual
3	6	56	36	9	Games graph, Hill cap [41]
3	6	84	54	9	Gulliver [37]; [55]
3	6	98	63	9	Gulliver [37]; [55]
3	6	154	99	9	Van Eupen [31]; [38]
3	8	$82i$	$54i$	27	Kohnert [50] $(8 \le i \le 12)$
3	8	$41i$	$27i$	27	Kohnert [50] $(26 \le i \le 39)$
3	8	1435	945	27	De Lange [51]
3	12	32760	21627	243	Liebeck [52] 3^{12}.2.Suz rank 3 graph
9	3	35	30	3	De Resmini [24]
9	3	42	36	3	Penttila & Royle [59]
9	4	287	252	9	De Lange [51]
5	4	39	30	5	Dissett [29]; [7]
5	6	1890	1500	25	Liebeck [52] $5^6.4.J_2$ rank 3 graph
125	3	829	820	5	Batten & Dover [2]
125	3	7461	7400	25	dual
343	3	3189	3178	7	Batten & Dover [2]
343	3	28701	28616	49	dual

Usually, if m is even, then $w_2 - w_1 = q^{m/2-1}$. An exception is the Hill example with $(q, m, n) = (4, 6, 78)$. Also subspaces are exceptions. Are there any further exceptions when $m = 4$?

1.8 Nonprojective codes

When the code C is not projective (which is necessarily the case when $n > \frac{q^m-1}{q-1}$) the set X is a multiset. Still, it allows a geometric description of the code, which is very helpful. For example, see Cheon et al. [14].

Two-weight $[n,m,d]_q$ codes with the two weights d and n were classified in Jungnickel & Tonchev [48]—the corresponding multiset X is either a multiple of a plane maximal arc, or a multiple of the complement of a hyperplane.

Part of the literature is formulated in terms of the complement Z of X in PV (or the multiset containing some fixed number t of copies of each point of PV). The code C will have minimum distance at least d when $|X \cap H| \leq n-d$ for all hyperplanes H. For Z that says $|Z \cap H| \geq t\frac{q^{m-1}-1}{q-1} - n + d$ for all hyperplanes H. Such sets Z are studied under the name *minihypers*, especially when they correspond to codes meeting the *Griesmer bound* $n \geq \sum_{i=0}^{m-1} \lceil \frac{d}{q^i} \rceil$. See, e.g., Hamada & Deza [39], Storme [63], Hill & Ward [44].

For projective two-weight codes we saw that $w_2 - w_1$ is a power of the characteristic. So, whenever this does not hold, the code must be nonprojective. (This settles, e.g., a question in [54].)

1.9 Brouwer - van Eupen duality

Brouwer & van Eupen [10] gives a correspondence between arbitrary projective codes and arbitrary two-weight codes. The correspondence can be said to be 1-1, even though there are choices to be made in both directions.

1.9.1 From projective code to two-weight code

Given a linear code C with length n, let n_C be its *effective length*, that is, the number of coordinate positions where C is not identically zero.

Let C be a projective $[n,m,d]_q$ code with nonzero weights $w_1, \ldots, w_t$. In a subcode D of codimension 1 in C these weights occur with frequencies $f_1, \ldots, f_t$, where $\sum f_i = q^{m-1}-1$ and $\sum (n_D - w_i) f_i = n_D(q^{m-2}-1)$. It follows that for arbitrary choice of α, β the sum $\sum (\alpha w_i + \beta) f_i$ does not depend on D but only on n_D.

Since C is projective, we have $n_D = n-1$ for n subcodes D, and $n_D = n$ for the remaining $\frac{q^m-1}{q-1} - n$ subcodes of codimension 1. Therefore, the above sum takes only two values.

Fix α, β in such a way that all numbers $\alpha w_i + \beta$ are nonnegative integers, and consider the multiset Y in PC consisting of the 1-spaces $\langle c\rangle$ with $c \in C$ taken $\alpha w + \beta$ times, where w is the weight of c. Since an arbitrary hyperplane D meets Y in $\alpha q^{m-2} n_D + \beta \frac{q^m-1}{q-1}$ points, the set Y defines a two-weight code of length $|Y| = \beta \frac{q^m-1}{q-1} + q^{m-1}\alpha n$, dimension m, and weights $w = |Y| - \frac{|Y|-\beta}{q}$ and $w' = w + \alpha q^{m-2}$.

For example, if we start with the unique $[16,5,9]_3$-code, with weight enumerator $0^1\ 9^{116}\ 12^{114}\ 15^{12}$ and take $\alpha = 1/3$, $\beta = -3$, we find a $[69,5,45]_3$-code with weight enumerator $0^1\ 45^{210}\ 54^{32}$. With $\alpha = -1/3$, $\beta = 5$, we find a $[173,5,108]_3$-code with weight enumerator $0^1\ 108^{32}\ 117^{210}$.

1.9.2 From two-weight code to projective code

Let C be a two-weight $[n,m,d]_q$-code with nonzero weights w_1 and w_2. Let X be the corresponding projective multiset. Let Y be the set of hyperplanes meeting X in $|X| - w_2$ points. Then Y defines a projective code of length $|H| = \frac{1}{w_2-w_1}(nq^{m-1} - w_1 \frac{q^m-1}{q-1})$ and dimension m, and with a number of distinct weights equal to the number of distinct multiplicities in X.

1.9.3 Remarks

In both directions there is a choice: pick α, β or pick $w_2 \in \{w_1, w_2\}$. The correspondence is 1-1 in the sense that if C^* is a BvE-dual of C, then C is a BvE-dual of C^*.

If the projective code C one starts with has only two different weights, then one can choose α, β so that Y becomes a set and the BvE-dual coincides with the Delsarte dual.

For another introduction and further examples, see Hill & Kolev [43].

In the above, the degree 1 polynomial $p(w) = \alpha w + \beta$ was used. One can use higher degree polynomials when more information about subcodes is available. See the last section of [10] and Dodunekov & Simonis [30].

See also [47], [64] (Lemma 5.1), and [6].

Bibliography

[1] S. Ball, A. Blokhuis & F. Mazzocca, *Maximal arcs in Desarguesian planes of odd order do not exist*, Combinatorica **17** (1997) 31–41

[2] L. Batten & J. M. Dover, *Some sets of type* (m, n) *in cubic order planes*, Des. Codes Cryptogr. **16** (1999) 211–213.

[3] L. D. Baumert, W. H. Mills & R. L. Ward, *Uniform Cyclotomy*, J. Number Th. **14** (1982) 67–82.

[4] A. Blokhuis & M. Lavrauw, *Scattered spaces with respect to a spread in* $PG(n, q)$, Geom. Dedicata **81** (2000) 231–243.

[5] A. Blokhuis & M. Lavrauw, *On two-intersection sets with respect to hyperplanes in projective spaces*, J. Comb. Th. (A) **99** (2002) 377–382.

[6] Iliya G. Bouyukliev, *Classification of Griesmer codes and dual transform*, Discr. Math. **309** (2009) 4049–4068.

[7] Iliya Bouyukliev, Veerle Fack, Wolfgang Willems & Joost Winne, *Projective two-weight codes with small parameters and their corresponding graphs*, Des. Codes Cryptogr. **41** (2006) 59–78.

[8] A. E. Brouwer, *Some new two-weight codes and strongly regular graphs*, Discrete Appl. Math. **10** (1985) 111–114.

[9] A. E. Brouwer, A. M. Cohen & A. Neumaier, *Distance-regular graphs*, Springer, 1989.

[10] A. E. Brouwer & M. van Eupen, *The correspondence between projective codes and 2-weight codes*, Des. Codes Cryptogr. **11** (1997) 261–266.

[11] A. E. Brouwer, A. V. Ivanov & M. H. Klin, *Some new strongly regular graphs*, Combinatorica **9** (1989) 339–344.

[12] A. E. Brouwer, R. M. Wilson & Qing Xiang, *Cyclotomy and Strongly Regular Graphs*, J. Alg. Combin. **10** (1999) 25–28.

[13] A. R. Calderbank & W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986) 97–122.

[14] Eun Ju Cheon, Yuuki Kageyama, Seon Jeong Kim, Namyong Lee & Tatsuya Maruuta, *A construction of two-weight codes and its applications*, Bull. Korean Math. Soc. **54** (2017) 731–736.

[15] F. De Clerck & M. Delanote, *Two-weight codes, partial geometries and Steiner systems*, Des. Codes Cryptogr. **21** (2000) 87–98.

[16] J. H. Conway & N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer, 1988.

[17] A. Cossidente, N. Durante, G. Marino, T. Penttila & A. Siciliano, *The geometry of some two-character sets*, Des. Codes Cryptogr. **46** (2008) 231–241.

[18] A. Cossidente & Oliver H. King, *Some two-character sets*, Des. Codes Cryptogr. **56** (2010) 105–113.

[19] A. Cossidente & G. Marino, *Veronese embedding and two-character sets*, Des. Codes Cryptogr. **42** (2007) 103–107.

[20] A. Cossidente & H. Van Maldeghem, *The exceptional simple group $G_2(q)$, q even, and two-character sets*, J. Combin. Theory (A) **114** (2007) 964–969.

[21] Ph. Delsarte, *Weights of linear codes and strongly regular normed spaces*, Discrete Math. **3** (1972) 47–64.

[22] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973).

[23] R. H. F. Denniston, *Some maximal arcs in finite projective planes*, J. Comb. Theory **6** (1969) 317–319.

[24] M. J. de Resmini, *A 35-set of type (2,5) in $PG(2,9)$*, J. Combin. Theory (A) **45** (1987) 303–305.

[25] M. J. de Resmini & G. Migliori, *A 78-set of type (2,6) in $PG(2,16)$*, Ars Combinatoria **22** (196) 73–75.

[26] A. De Wispelaere & H. Van Maldeghem, *Codes from generalized hexagons*, Des. Codes Cryptogr. **37** (2005) 435–448.

[27] A. De Wispelaere & H. Van Maldeghem, *Some new two-character sets in $PG(5,q^2)$ and a distance-2 ovoid in the generalized hexagon $H(4)$*, Discrete Math. **308** (2008) 2976–2983.

[28] Cunsheng Ding & Jing Yang, *Hamming weights in irreducible cyclic codes*, Discr. Math. **313** (2013) 434–446.

[29] Luis A. Dissett, *Combinatorial and computational aspects of finite geometries*, Ph.D. Thesis, Toronto, 2000.

[30] S. Dodunekov & J. Simonis, *Codes and projective multisets*, Electr. J. Combin. **5** (1998) R37.

[31] M. van Eupen, *Some new results for ternary linear codes of dimension 5 and 6*, IEEE Trans. Inf. Th. **41** (1995) 2048–2051.

[32] Tao Feng & Qing Xiang, *Strongly regular graphs from unions of cyclotomic classes*, J. Combin. Theory (B) **102** (2012) 982–995.

[33] F. Fiedler & M. Klin, *A strongly regular graph with the parameters* $(512, 73, 438, 12, 10)$ *and its dual graph*, Preprint MATH-AL-7-1998, Technische Universität Dresden, July 1998, 23 pp.

[34] D. A. Foulser & Michael J. Kallaher, *Solvable, flag-transitive, rank* 3 *collineation groups*, Geometriae Dedicata **7** (1978) 111–130.

[35] Gennian Ge, Qing Xiang & Tao Yuan, *Constructions of strongly regular Cayley graphs using index four Gauss sums*, J. Alg. Combin. **37** (2013) 313–329.

[36] J.-M. Goethals & J. J. Seidel, *Strongly regular graphs derived from combinatorial designs*, Canad. J. Math. **22** (1970) 597–614.

[37] T. A. Gulliver, *Two new optimal ternary two-weight codes and strongly regular graphs*, Discr. Math. **149** (1996) 83–92.

[38] T. A. Gulliver, *A new two-weight code and strongly regular graph*, Appl. Math. Letters **9** (1996) 17–20.

[39] N. Hamada & M. Deza, *A survey of recent works with respect to a characterization of an $(n, k, d; q)$-code meeting the Griesmer bound using a min.hyper in a finite projective geometry*, Discr. Math. **77** (1989) 75–87.

[40] N. Hamilton, *Strongly regular graphs from differences of quadrics*, Discr. Math. **256** (2002) 465–469.

[41] Raymond Hill, *On the largest size of cap in $S_{5,3}$*, Accad. Naz. Lincei, Rend. Cl. Sci. Fis. Mat. Nat. (8) **54** (1973) 378–384.

[42] R. Hill, *Caps and groups*, pp. 389–394 in: Proc. Rome 1973, Atti dei Convegni Lincei, 1976.

[43] R. Hill & E. Kolev, *A survey of recent results on optimal linear codes*, pp. 127–152 in: F.C. Holroyd, et al. (eds.), Combinatorial Designs and their Applications, CRC Press, Boca Raton, 1999.

[44] R. Hill & H. Ward, *A geometric approach to classifying Griesmer codes*, Des. Codes Cryptogr. **44** (2007) 169–196.

[45] Takuya Ikuta & Akihiro Munemasa, *A new example of non-amorphous association schemes*, Contrib. to Discr. Math. **3** (2008) 31–36.

[46] T. Ikuta & A. Munemasa, *Pseudocyclic association schemes and strongly regular graphs*, European J. Combin. **31** (2010) 1513–1519.

[47] D. B. Jaffe & J. Simonis, *New binary linear codes which are dual transforms of good codes*, IEEE Trans. Inf. Th. **45** (1999) 2136–2137.

[48] D. Jungnickel & V. D. Tonchev, *The classification of antipodal two-weight linear codes*, Finite Fields Appl. **50** (2018) 372–381.

[49] W. M. Kantor, *Exponential numbers of two-weight codes, difference sets and symmetric designs*, Discr. Math. **46** (1983) 95–98.

[50] Axel Kohnert, *Constructing two-weight codes with prescribed groups of automorphisms*, Discr. Appl. Math. **155** (2007) 1451–1457.

[51] C. L. M. de Lange, *Some new cyclotomic strongly regular graphs*, J. Alg. Combin. **4** (1995) 329–330.

[52] Martin W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. (3) **54** (1987) 477–516.

[53] J. H. van Lint & A. Schrijver, *Constructions of strongly regular graphs, two-weight codes and partial geometries by finite fields*, Combinatorica **1** (1981) 63–73.

[54] Gaojun Luo & Xiwang Cao, *A construction of linear codes and stronglyb regular graphs from q-polynomials*, Discr. Math. **340** (2017) 2262–2274.

[55] M. Martis, J. Bamberg & S. Morris, *An enumeration of certain projective ternary two-weight codes*, J. Combin. Designs **24** (2016) 21–35.

[56] R. J. McEliece & H. Rumsey, jr., *Euler products, cyclotomy and coding*, J. Number Th. **4** (1972) 302–311.

[57] Koji Momihara, *Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums*, European J. Combin. **34** (2013) 706–723.

[58] Koji Momihara, *Strongly regular Cayley graphs on* $\mathbb{F}_{2^{2(2s+2)}}$ *from cyclotomy*, Finite Fields Appl. **25** (2014) 280–292.

[59] T. Penttila & G. F. Royle, *Sets of type* (m,n) *in the affine and projective planes of order nine*, Des. Codes Cryptogr. **6** (1995) 229–245.

[60] A. Rao & N. Pinnawala, *A family of two-weight irreducible cyclic codes*, IEEE Trans. Inf. Theory **56** (2010) 2568–2570.

[61] B. G. Rodrigues, *A projective two-weight code related to the simple group Co1 of Conway*, Graphs Combin. **34** (2018) 509–521.

[62] B. Schmidt & C. White, *All two-weight irreducible cyclic codes?*, Finite Fields Appl. **8** (2002) 1–17.

[63] Leo Storme, *Linear codes meeting the Griesmer bound, minihypers and geometric applications*, Le Matematiche **59** (2004) 367–392.

[64] M. Takenaka, K. Okamoto & T. Maruta, *On optimal non-projective ternary linear codes*, Discr. Math. **308** (2008) 842–854.

[65] G. Vega, *A critical review and some remarks about one- and two-weight irreducible cyclic codes*, Finite Fields Appl. **33** (2015) 1–13.

[66] Fan Wu, *Constructions of Strongly Regular Cayley Graphs Using Even Index Gauss Sums*, J. Combin. Designs **21** (2013) 432–446.