Self-Dual Codes

E. M. Rains and *N. J. A. Sloane*

Information Sciences Research, AT&T Labs-Research
180 Park Avenue, Florham Park, NJ 07932-0971

May 19 1998

ABSTRACT

A survey of self-dual codes, written for the *Handbook of Coding Theory*.

Self-dual codes are important because many of the best codes known are of this type and they have a rich mathematical theory. Topics covered in this chapter include codes over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_q$, $\mathbb{Z}_4$, $\mathbb{Z}_m$, shadow codes, weight enumerators, Gleason-Pierce theorem, invariant theory, Gleason theorems, bounds, mass formulae, enumeration, extremal codes, open problems. There is a comprehensive bibliography.

1. Self-dual codes over rings and fields

1.1. Inner products

There are several different kinds of self-dual codes. Let $\mathbb{F}$ be a finite set called the *alphabet* (e.g. $\mathbb{F} = \{0, 1\}$ for binary codes). A *code* C *over* $\mathbb{F}$ of *length* n is any subset of $\mathbb{F}^n$. If $\mathbb{F}$ has the structure of an additive group then C is *additive* if it is an additive subgroup of $\mathbb{F}^n$. If $\mathbb{F}$ has a ring structure then C is *linear over* $\mathbb{F}$ if it is additive and also closed under multiplication by elements of $\mathbb{F}$. (We will always assume that multiplication in $\mathbb{F}$ is commutative.)

In order to define dual codes we must equip $\mathbb{F}$ with an *inner product* (cf. [178], [201]). We denote this by $(\ ,\ )$ and require that it satisfy the following conditions:

$$\begin{aligned}
&(x + y, z) = (x, z) + (y, z)\ , \\
&(x, y + z) = (x, y) + (x, z)\ , \\
&\text{if}\ \ (x, y) = 0\ \ \text{for all } x \text{ then } y = 0\ , \\
&\text{if}\ \ (x, y) = 0\ \ \text{for all } y \text{ then } x = 0\ .
\end{aligned}$$

To define the dual of a linear code we impose the further condition that $\mathbb{F}$ has a *conjugacy* operation, or "involutory anti-automorphism" (which may be the identity), denoted by a bar, which satisfies

$$\overline{\overline{x}} = x,\ \overline{x + y} = \overline{x} + \overline{y},\ \overline{xy} = \overline{x}\,\overline{y}\ .$$

The inner product must then satisfy

$$(x, y) = \overline{(y, x)},\ (ax, y) = (x, \overline{a}y)\ .$$

The inner product of vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ in $\mathbb{F}^n$ is defined by

$$(x, y) = \sum_{i=1}^{n} (x_i, y_i)\ .$$

1.2. Families of self-dual codes

Families (2) through $(m^{\mathbb{Z}})$ include the most important families of codes we will consider in this chapter.

(2) Binary linear codes: $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$, with inner product $(x, y) = xy$, $C =$ subspace of $\mathbb{F}_2^n$.

(3) Ternary linear codes: $\mathbb{F} = \mathbb{F}_3 = \{0, 1, 2\}$, $(x, y) = xy$, $C =$ subspace of $\mathbb{F}_3^n$.

($4^{\rm H}$) Quaternary linear codes: $\mathbb{F} = \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 + \omega + 1 = 0$, $\omega^3 = 1$, $\overline{x} = x^2$ for $x \in \mathbb{F}_4$, with the Hermitian inner product $(x, y) = x\overline{y}$, C = subspace of $\mathbb{F}_4^n$. Note that for $x, y \in \mathbb{F}_4$, $(x + y)^2 = x^2 + y^2$, $x^4 = x$.

($4^{\rm E}$) Quaternary linear codes: $\mathbb{F} = \mathbb{F}_4$, but with the Euclidean inner product $(x, y) = xy$.

($4^{\rm H+}$) Quaternary additive codes: $\mathbb{F} = \mathbb{F}_4$, with $(x, y) = xy^2 + x^2y = \text{trace}(x\overline{y})$ (the trace from $\mathbb{F}_4$ to $\mathbb{F}_2$); C = additive subgroup of $\mathbb{F}_4^n$.

For completeness we should also mention family $4^{\rm E+}$, quaternary additive codes with the Euclidean trace inner product: $\mathbb{F} = \mathbb{F}_4$, with $(x, y) = xy + (xy)^2 = \text{trace}(xy)$ (the trace from $\mathbb{F}_4$ to $\mathbb{F}_2$); C = additive subgroup of $\mathbb{F}_4^n$. However, the map

$$x = \omega x_1 + \overline{\omega} x_2 \in \mathbb{F}_4^n \leftrightarrow x_1 x_2 \in \mathbb{F}_2^{2n}$$

shows that these codes are equivalent to binary codes from family 2 with a particular pairing of the coordinates. Since we don't know any interesting examples of this family other than linear codes, we shall say no more about them.

($q^{\rm H}$) Linear codes over $\mathbb{F}_q$ (or q-ary linear codes), where q is an even power of an arbitrary prime p, with $\overline{x} = x^{\sqrt{q}}$ for $x \in \mathbb{F}_q$, $(x, y) = x\overline{y}$, C = subspace of $\mathbb{F}_q^n$. Note that for $x, y \in \mathbb{F}_q$, $(x + y)^{\sqrt{q}} = x^{\sqrt{q}} + y^{\sqrt{q}}$, $x^q = x$.

($q^{\rm E}$) Linear codes over $\mathbb{F}_q$, but with $(x, y) = xy$. If q is a square, family $q^{\rm H}$ is generally preferred to $q^{\rm E}$.

($4^{\mathbb{Z}}$) $\mathbb{Z}_4$-linear codes: $\mathbb{F} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, with $(x, y) = xy \pmod 4$, C = linear subspace[1] of $\mathbb{Z}_4^n$.

($m^{\mathbb{Z}}$) $\mathbb{F} = \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, where m is an integer ≥ 2, with $(x, y) = xy \pmod m$, C = linear subspace[2] of $\mathbb{Z}_m^n$.

Note that for the families 2, 3, $4^{\mathbb{Z}}$, $m^{\mathbb{Z}}$, an additive code is automatically linear.

The following families are less important for our present purposes:

(F1) Linear codes over $\mathbb{F}_q[u]/(u^2)$, where u is an indeterminate, with $\overline{u} = -u$, $(x, y) = x\overline{y}$. (References [8] and [101] consider such codes, as well as a noncommutative variant.)

(F2) Additive codes over $\mathbb{F}_4$, with $(x, y) = x\overline{y}$.

If we relax the requirement that $\mathbb{F}$ be commutative and finite, we can add:

(F3) Linear codes over the p-adic integers.

(F4) Codes over Frobenius rings.

[1] Strictly speaking, a $\mathbb{Z}_4$-submodule.

[2] Strictly speaking, a $\mathbb{Z}_m$-submodule.

(F5) Lattices in $\mathbb{R}^n$ (see Section 14).

1.3. The dual code

Once we have specified a family of codes by giving $\mathbb{F}$ and an inner product we can define the *dual* of a code C to be

$$C^{\perp} = \{u \in \mathbb{F}^n : (u, v) = 0 \quad \text{for all} \quad v \in C\} .$$

The dual of a binary linear code (family 2) is again a binary linear code. Similarly, the dual of a code in any of families 3 through $m^{\mathbb{Z}}$ is again a code of the same family. For family $4^{\mathrm{H}+}$, the dual of an additive code is additive; if C is also linear so is $C^{\perp}$, and then $C^{\perp}$ coincides with the dual in family 4^{H}. The dual in family 4^{E} is the conjugate of the dual in family 4^{H}.

For families 2 through $m^{\mathbb{Z}}$ it is easily checked that we have

$$|C|\,|C^{\perp}| = |\mathbb{F}|^n , \tag{1}$$

which implies

$$(C^{\perp})^{\perp} = C . \tag{2}$$

In general, however, we can say only that

$$C \subseteq (C^{\perp})^{\perp} .$$

In particular, (2) does not necessarily hold for family F2 (consider, for example, the code $\{00, 11\}$ which has dual $\{00, 11, \omega\omega, \overline{\omega\omega}\}$, containing only 4 words).

1.4. Self-dual codes

If $C = C^{\perp}$ then C is said to be *self-dual*. If $C \subseteq C^{\perp}$, C is *self-orthogonal*. (In the past, some authors have used "self-orthogonal" and "weakly self-orthogonal" for these two concepts.)

In families 2 through $m^{\mathbb{Z}}$, if C is self-dual then

$$|C| = |\mathbb{F}|^{n/2} , \tag{3}$$

and if $|\mathbb{F}|$ is not a square then n must be even. In particular, if C is linear over a field, then n is even and C is a subspace of dimension $n/2$. The only families from 2 through $m^{\mathbb{Z}}$ that contain self-dual codes of odd length are $4^{\mathrm{H}+}$, $4^{\mathbb{Z}}$ and $m^{\mathbb{Z}}$ with m a square.

Remarks about the final three families. (F3): Let C be a code of length n over the p-adic integers $\mathbb{Z}_{p^\infty}$ (such codes have been studied in [46], [50]). In general it is not clear how one should define $C^\perp$. However, if when we reduce C mod p it has the same dimension over $\mathbb{F}_p$ as C had over $\mathbb{F}_{p^\infty}$, then there is a natural way to define the dual so that it satisfies

$$(C^\perp)^\perp = C, \quad \dim\ C + \dim\ C^\perp = n\ .$$

Namely, let $D = \mathbb{Q}_{p^\infty} \otimes C$ be the code over the p-adic *rationals* $\mathbb{Q}_{p^\infty}$ generated by C. Since D is a linear code over a field, $D^\perp$ exists and satisfies $(D^\perp)^\perp = D$, $\dim\ D + \dim D^\perp = n$. Now set $C^\perp = D^\perp \cap \mathbb{Z}_{p^\infty}^n$.

(F4): J. A. Wood ([331], see also [323]) has investigated codes over noncommutative finite rings $\mathbb{F}$, and has shown that the two fundamental MacWilliams theorems (Theorem 4 below and Theorems 10.4 and 10.6 of Chapter 1) hold precisely when $\mathbb{F}$ is a Frobenius ring. At present however no interesting examples of self-dual codes over noncommutative rings are known.

(F5): Unimodular lattices are analogues of self-dual codes in $\mathbb{R}^n$ — see Section 14.

2. Equivalence of codes

2.1. Equivalent codes

Codes that differ only in minor ways, such as in the order in which the coordinates are arranged, are said to be *equivalent*. The transformations that we allow in defining equivalence for the above families of codes are as follows (these are precisely the transformations that commute with the process of forming the dual).

(2) Permutations of the coordinates.

(3) Monomial transformations of the coordinates (that is, a permutation of the coordinates followed by multiplication of the coordinates by nonzero field elements).

(4^{H}) Monomials; global conjugation.

(4^{E}) Permutations; global conjugation.

($4^{\mathrm{H}+}$) Monomials; conjugation of individual coordinates.

(q^{H}) Monomials over the subgroup

$$\{x \in \mathbb{F}_q : x\overline{x} = 1\} \cong \mathbb{F}_q^*/\mathbb{F}_{\sqrt{q}}^*\ ,$$

where the star denotes the set of nonzero field elements; global multiplication by elements of $\mathbb{F}_q^*$; global action of Galois group $Gal(\mathbb{F}_q/\mathbb{F}_p)$

(q^{E}) Monomials over $\{\pm 1\}$; global multiplication by units; global action of Galois group.

($4^{\mathbb{Z}}$) Monomials over $\{\pm 1\}$.

($m^{\mathbb{Z}}$) Monomials over square roots of unity; global multiplication by units of $\mathbb{Z}_m$.

2.2. Automorphism groups

In each case, the subset of such transformations that preserves the code forms the *automorphism group* $Aut(C)$ of the code.

Let G denote the full group of all transformations listed. The order of G in the above cases is:

(2) $n!$

(3) $2^n n!$

(4^{H}) $2.3^n n!$

(4^{E}) $2.n!$

($4^{\mathrm{H}+}$) $6^n n!$

(q^{H}) $\log_p(q)(\sqrt{q}-1)(\sqrt{q}+1)^n n!$

(q^{E}) $\log_p(q)\frac{q-1}{2}2^n n!$

($4^{\mathbb{Z}}$) $2^n n!$

($m^{\mathbb{Z}}$) For $m = 5, 6, 7, 8, 9$ the orders are

$$\frac{5-1}{2}2^n n!,\ 2^n n!,\ \frac{7-1}{2}2^n n!,\ 4^n n!,\ 3.2^n n!$$

respectively.

The number of codes that are equivalent to a given code C is then

$$\frac{|G|}{|Aut(C)|}\ .$$

In most cases it is possible to determine the total number T_n (say) of distinct self-dual codes of length n in one of our families. Then

$$T_n = \sum_{\substack{\text{inequivalent}\\ C}} \frac{|G|}{|Aut(C)|}$$

where the sum is over all *inequivalent* codes. In other words

$$\sum_{\substack{\text{inequivalent}\\ C}} \frac{1}{|Aut(C)|} = \frac{T_n}{|G|}\ . \tag{4}$$

Equation (4) is called a *mass formula*. The appropriate values of T_n are:

(2)

$$\prod_{i=1}^{\frac{1}{2}n-1} (2^i + 1) \quad (n \equiv 0 \pmod 2) \tag{5}$$

($2_{\rm II}$) (weights divisible by 4):

$$2 \prod_{i=1}^{\frac{1}{2}n-2} (2^i + 1) \quad (n \equiv 0 \pmod 8) \tag{6}$$

(3)

$$2 \prod_{i=1}^{\frac{1}{2}n-1} (3^i + 1) \quad (n \equiv 0 \pmod 4) \tag{7}$$

($4^{\rm H}$)

$$\prod_{i=0}^{\frac{1}{2}n-1} (2^{2i+1} + 1) \quad (n \equiv 0 \pmod 2) \tag{8}$$

($4^{\rm E}$)

$$\prod_{i=1}^{\frac{1}{2}n-1} (4^i + 1) \quad (n \equiv 0 \pmod 2) \tag{9}$$

($4^{\rm H+}$)

$$\prod_{i=1}^{n} (2^i + 1) \tag{10}$$

($4_{\rm II}^{\rm H+}$) (all weights even):

$$2 \prod_{i=1}^{n-1} (2^i + 1) \quad (n \equiv 0 \pmod 2) \tag{11}$$

($q^{\rm H}$)

$$\prod_{i=0}^{\frac{1}{2}n-1} (q^{i+\frac{1}{2}} + 1) \quad (n \equiv 0 \pmod 2) \tag{12}$$

($q^{\rm E}$)

$$b \prod_{i=1}^{\frac{1}{2}n-1} (q^i + 1) \quad (n \equiv 0 \pmod 2) \tag{13}$$

where $b = 1$ if q is even, 2 if q is odd

($4^{\mathbb{Z}}$)

$$\sum_{k=0}^{n/2} \sigma(n,k) 2^{k(k+1)/2} \ , \tag{14}$$

where $\sigma(n,k)$, the number of binary self-orthogonal $[n,k]$ codes with all weights divisible by 4, is equal to 1 if $k = 0$, and otherwise is given by

$$\prod_{i=0}^{k-1} \frac{2^{n-2i-2} + 2^{[\frac{n}{2}]-i-1} - 1}{2^{i+1} - 1} \ , \quad \text{if} \quad n \equiv \pm 1 \pmod 8 \ ,$$

$$\prod_{i=0}^{k-1} \frac{2^{n-2i-2}-1}{2^{i+1}-1} , \quad \text{if} \quad n \equiv \pm 2 \pmod 8 ,$$

$$\prod_{i=0}^{k-1} \frac{2^{n-2i-2}-2^{[\frac{n}{2}]-i-1}-1}{2^{i+1}-1} , \quad \text{if} \quad n \equiv \pm 3 \pmod 8 ,$$

$$\left[\prod_{i=0}^{k-2} \frac{2^{n-2i-2}+2^{\frac{n}{2}-i-1}-2}{2^{i+1}-1}\right] \cdot \left[\frac{1}{2^{k-1}} + \frac{2^{n-2k}+2^{\frac{n}{2}-k}-2}{2^k-1}\right] , \quad \text{if} \quad n \equiv 0 \pmod 8 ,$$

$$\left[\prod_{i=0}^{k-2} \frac{2^{n-2i-2}-2^{\frac{n}{2}-i-1}-2}{2^{i+1}-1}\right] \cdot \left[\frac{1}{2^{k-1}} + \frac{2^{n-2k}-2^{\frac{n}{2}-k}-2}{2^k-1}\right] , \quad \text{if} \quad n \equiv 4 \pmod 8 .$$

There is a similar but even more complicated formula for T_n for self-dual codes over $\mathbb{Z}_4$ with Euclidean norms divisible by 8, see [101].

Formulae (5)–(13) are based on various sources including [134], [191], [226], [190, Chap. 19]. Equation (14) is due to Gaborit [101].

Here are two proofs of (5). (i) Let $\sigma_{n,k}$ denote the number of $[n,k]$ self-orthogonal codes C containing $\mathbf{1}$. Any such C can be extended to an $[n,k+1]$ self-orthogonal code D by adjoining any vector of $C^\perp \setminus C$, and any D will arise 2^k-1 times from different C's. So we have $\sigma_{n,1}=1$,

$$\frac{\sigma_{n,k+1}}{\sigma_{n,k}} = \frac{2^{n-2k}-1}{2^k-1} ,$$

and $\sigma_{n,n/2}$ gives (5). (ii) A more sophisticated proof can be obtained by observing that the Euclidean inner product induces a symplectic geometry structure on the space of even weight vectors modulo $\mathbf{1}$. A self-dual code is then a maximally isotropic subspace. The number of maximally isotropic subspaces of a symplectic geometry of dimension $2k$ is $\Pi_{i=1}^{k}(2^i+1)$ [34, §9.4], and we obtain (5) by noting that our symplectic geometry has dimension $n-2$. ∎

Similarly, a binary self-dual code with weights divisible by 4 is a maximally totally singular subspace of the orthogonal geometry of dimension $n-2$ induced by $\frac{1}{2}wt(v)$, which leads to (6). Equations (7), (9), (11), (13) are also obtained via orthogonal geometry, (10) via symplectic geometry, and (8) and (12) via unitary geometry.

These mass formulae are useful when one is attempting to find all inequivalent codes of a given length (compare Section 11). For example, suppose we are trying to find all binary self-dual codes of length 8. We immediately find two codes, $i_2 \oplus i_2 \oplus i_2 \oplus i_2$, where $i_2 = [11]$, and the Hamming code e_8, and then it appears that there are no others. To prove this, we compute the automorphism groups of these two codes: they have orders $2^4 4! = 384$ and $8.7.6.4 = 1344$, respectively. We also calculate $T_8/|G| = 3.5.9/8! = 3/896$ from (5), and see that indeed

$$\frac{1}{384} + \frac{1}{1344} = \frac{3}{896} ,$$

verifying that this enumeration is complete. We will return to this in Section 11.

There are also formulae that give the total number of self-dual codes containing a fixed self-orthogonal vector or code — see [190, Chapter 19].

2.3. Codes over $\mathbb{Z}_4$

Codes over rings are probably less familiar to the reader than codes over fields, and so we will add some remarks here about the first such case, codes over $\mathbb{Z}_4$, family $4^{\mathbb{Z}}$.

Any code over $\mathbb{Z}_4$ is equivalent to one with generator matrix of the form

$$\begin{bmatrix} I_{k_1} & X & Y_1 + 2Y_2 \\ 0 & 2I_{k_2} & 2Z \end{bmatrix} \tag{15}$$

where X, Y_1, Y_2, Z are binary matrices. Then C is an elementary abelian group of type $4^{k_1}2^{k_2}$, containing $2^{2k_1+k_2}$ words. We indicate this by writing $|C| = 4^{k_1}2^{k_2}$. The dual code $C^\perp$ has generator matrix

$$\begin{bmatrix} (-Y_1 + 2Y_2)^{tr} - Z^{tr}X^{tr} & Z^{tr} & I_{n-k_1-k_2} \\ 2X^{tr} & 2I_{k_2} & 0 \end{bmatrix}$$

and $|C^\perp| = 4^{n-k_1-k_2}2^{k_2}$.

There are two binary codes $C^{(1)}$ and $C^{(2)}$ associated with C, having generator matrices

$$[I_{k_1}\ X\ Y_1] \quad \text{and} \quad \begin{bmatrix} I_{k_1} & X & Y_1 \\ 0 & I_{k_2} & Z \end{bmatrix} \tag{16}$$

and parameters $[n, k_1]$ and $[n, k_1 + k_2]$ respectively. If C is self-orthogonal then $C^{(1)}$ is doubly-even and $C^{(1)} \subseteq C^{(2)} \subseteq C^{(1)\perp}$. If C is self-dual then $C^{(2)} = C^{(1)\perp}$. The next two theorems give the converse assertions.

Theorem 1. *If A, B are binary codes with $A \subseteq B$ then there is a code C over $\mathbb{Z}_4$ with $C^{(1)} = A$, $C^{(2)} = B$. If in addition A is doubly-even and $B \subseteq A^\perp$ then C can be made self-orthogonal. If $B = A^\perp$ then C is self-dual.*

Proof. Suppose A, B have generator matrices as shown in (16). Then

$$\begin{bmatrix} I & X & Y \\ 0 & 2I & 2Z \end{bmatrix} \tag{17}$$

is a generator matrix for a code C with $C^{(1)} = A$, $C^{(2)} = B$. To establish the second assertion we must modify (17) to make C self-orthogonal. This is accomplished by replacing the (j, i)th entry of (17) by the inner product modulo 4 of rows i and j, for $1 \le i \le k_1$, $1 \le j \le k_1 + k_2$, $i < j$. ∎

In this way every self-*orthogonal* doubly-even binary code corresponds to one or more self-*dual* codes over $\mathbb{Z}_4$.

Theorem 2. [101] *A code C over $\mathbb{Z}_4$ with generator matrix (15) is self-dual if and only if $C^{(1)}$ is doubly-even, $C^{(2)} = C^{(1)\perp}$, and Y_2 is chosen so that if $M = Y_1 Y_2^{tr}$, then $M_{ij} + M_{ji} \equiv \frac{1}{2} wt(v_i \cap v_j)$, where $v_1, \ldots, v_{k_1}$ are the generators of $C^{(1)}$.*

In contrast to self-dual codes over fields, self-dual codes over $\mathbb{Z}_4$ exist for all lengths, even or odd. Furthermore, a self-dual code C over $\mathbb{Z}_4$ of length n can be shortened to a self-dual code of length $n-1$ by deleting any one of its coordinates. This is accomplished as follows. If the projection of C onto the ith coordinate contains all of $\mathbb{Z}_4$, the shortened code is obtained by taking those words of C that are 0 or 2 in the ith coordinate and omitting that coordinate. If the projection of C onto the ith coordinate contains only 0 and 2, we take the words of C that are 0 on the ith coordinate and omit that coordinate.

In this way all self-dual codes over $\mathbb{Z}_4$ belong to a common "family tree", with $i_1 = \{0, 2\}$ at the root. The beginning of this tree, showing all self-dual codes of lengths $n \leq 8$, is given in Fig. 2 of [71].

3. Weight enumerators and MacWilliams theorem

3.1. Weight enumerators

The *Hamming weight* of a vector $u = (u_1, \ldots, u_n) \in \mathbb{F}^n$, denoted by $wt(u)$, is the number of nonzero components u_i.

Two other types of "weight" are useful for studying nonbinary codes. For the codes in families $4^{\mathbb{Z}}$, $m^{\mathbb{Z}}$ (and hence for 2, 3, and, if q is a prime, q^{E}) we define the *Lee weight* and *Euclidean norm* of $u \in \mathbb{F}$ by

$$\begin{aligned} \mathrm{Lee}(u) &= \min\{|u|, |\mathbb{F}| - |u|\} , \\ \mathrm{Norm}(u) &= (\mathrm{Lee}(u))^2 . \end{aligned}$$

For a vector $u = (u_1, \ldots, u_n) \in \mathbb{F}^n$, we set

$$\begin{aligned} \mathrm{Lee}(u) &= \sum_{i=1}^{n} \mathrm{Lee}(u_i) , \\ \mathrm{Norm}(u) &= \sum_{i=1}^{n} \mathrm{Norm}(u_i) . \end{aligned}$$

Of course, if u is a binary vector, $wt(u) = \mathrm{Lee}(u) = \mathrm{Norm}(u)$.

It is customary to use the symbol A_i to denote the number of vectors in a code C having Hamming weight (or Lee weight, or Euclidean norm, depending on context) equal to i. Then $\{A_0, A_1, A_2, \ldots\}$ is called the *weight distribution* of the code. The *Hamming weight enumerator* (abbreviated hwe) of C is defined to be

$$W_C(x, y) = \sum_{u \in C} x^{n - wt(u)} y^{wt(u)} = \sum_{i=0}^{n} A_i x^{n-i} y^i \ . \tag{18}$$

(The adjective "Hamming" is often omitted.) There are good reasons for taking the Hamming weight enumerator to be a homogeneous polynomial of degree n (see below). However, no information is lost if we set $x = 1$, and write it as a polynomial in the single variable y.

There is an analogous definition for nonlinear codes: for $v \in \mathbb{F}^n$, let $A_i(v)$ be the number of codewords at Hamming distance i from v. The *average Hamming weight distribution* for a nonlinear or nonadditive code is then

$$A_i = \frac{1}{|C|} \sum_{c \in C} A_i(c) \ ,$$

with associated Hamming weight enumerator

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

Much more information about a code C is supplied by its *complete weight enumerator* (abbreviated cwe) and defined as follows. Let the elements of the alphabet $\mathbb{F}$ be ξ_0, $\xi_1, \ldots, \xi_a$, and introduce corresponding indeterminates x_0, $x_1, \ldots, x_a$. Then

$$cwe_C(x_0, \ldots, x_a) = \sum_{u \in C} x_0^{n_0(u)} x_1^{n_1(u)} \cdots x_a^{n_a(u)} \ , \tag{19}$$

where $n_\nu(u)$ is the number of components of u that take the value ξ_ν.

If there is a natural way to pair up some of the symbols in $\mathbb{F}$ then we can often reduce the number of variables in the cwe without losing any essential information, by identifying indeterminates corresponding to paired symbols. The result is a *symmetrized weight enumerator* (abbreviated swe). Some examples will make this clear. For linear codes over $\mathbb{F}_4$ the symmetrized weight enumerator is

$$swe_C(x, y, z) = \sum_{u \in C} x^{n_0(u)} y^{n_1(u)} z^{N_w(u)} = cwe_C(x, y, z, z) \ , \tag{20}$$

where $n_0(u)$, $n_1(u)$ are as above and $N_w(u)$ is the number of components in u that are equal to either ω or $\overline{\omega}$. For linear codes over $\mathbb{Z}_4$, the appropriate symmetrized weight enumerator is

$$swe_C(x,y,z) = \sum_{u \in C} x^{n_0(u)} y^{n_\pm(u)} z^{n_2(z)} = cwe_C(x,y,z,y) \ , \tag{21}$$

where $n_\pm(u)$ is the number of components of u that are equal to either $+1$ or -1. There is an obvious generalization of (21) to linear codes over $\mathbb{Z}_m$.

The swe contains only about half as many variables as the complete weight enumerator, and yet still contains enough information to determine the Lee weight or norm distribution of a code.

All the weight enumerators mentioned so far can be obtained from the "full weight enumerator" of the code. This is a generating function, or formal sum (not a polynomial), listing all the codewords:

$$\sum_{u \in C} z_1^{u_1} z_2^{u_2} \cdots z_n^{u_n} \ ,$$

where we use a different indeterminate z_i for each coordinate position. To obtain the symmetrized weight enumerator of a code over $\mathbb{F}_4$, for example, we replace each occurrence of z_i^0 by x, each z_i^1 by y, and each z_i^ω or $z_i^{\overline{\omega}}$ by z.

Still further weight enumerators that have proved useful can also be obtained from the full weight enumerator. For example, the *split Hamming weight enumerator* of a code of length $n = 2m$ is

$$split_C(x,y,X,Y) = \sum_{y \in C} x^{m-l(u)} y^{l(u)} X^{m-r(u)} Y^{r(u)} \ ,$$

where $l(u)$ (resp. $r(u)$) is the Hamming weight of the left half (resp. right half) of u. Split weight enumerators have been investigated in [197], for example. Of course, the split need not be into equal parts. Multiply-split weight enumerators have been extensively used in [156].

One may also define weight enumerators for *translates* of codes: if C is a translate of a linear or additive code, its weight enumerator is

$$W_C(x,y) = \sum_{c \in C} x^{n-wt(c)} y^{wt(c)}.$$

We will use such weight enumerators later in this chapter when studying the "shadow" of a self-dual code.

The *biweight enumerator* of a code generalizes the weight enumerator to consider the overlaps of pairs of codewords, and the joint weight enumerator of two codes C and D considers

the overlaps of pairs of codewords $u \in C$ and $v \in D$. More generally, the k-fold *multiple weight enumerator* of a code considers the composition of k codewords chosen simultaneously from the code. Again there are generalizations of the MacWilliams and Gleason theorems ([188], [190, Chap. 5], [280]). The connections between multiple weight enumerators of self-dual codes and Siegel modular forms have been investigated by Duke [90], Ozeki [208], [212], [218] and Runge [263]–[266].

Ozeki [218] has recently introduced another generalization of the weight enumerator of a code C, namely its *Jacobi polynomial*. For a fixed vector $v \in \mathbb{F}^n$, this is defined by

$$Jac_{C,v}(x,z) = \sum_{u \in C} x^{wt(u)} z^{wt(u \cap v)} \ ,$$

which is essentially a split weight enumerator. These polynomials have been studied in [10], [11], [24]. They have the same relationship to Jacobi forms [93] as weight enumerators do to modular forms (cf. the remarks in Section 14).

For future reference we note the following relations between inner products and weights or norms for four of our families:

(2):

$$(u,v) = \frac{1}{2}\{wt(u+v) - wt(u) - wt(v)\} \tag{22}$$

($4^{\mathrm{H}+}$):

$$(u,v) = wt(u+v) - wt(u) - wt(v) \tag{23}$$

($4^{\mathbb{Z}}$), ($m^{\mathbb{Z}}$):

$$(u,v) = \frac{1}{2}\{\mathrm{Norm}(u+v) - \mathrm{Norm}(u) - \mathrm{Norm}(v)\} \ . \tag{24}$$

3.2. Examples of self-dual codes and their weight enumerators

The following are some key examples of self-dual codes of the different families mentioned in Section 1, together with their weight enumerators. Some of these weight enumerators will be labeled for later reference. Unless indicated otherwise, all the codes mentioned are self-dual codes of the appropriate kind.

We write $[n,k,d]_q$ to indicate a linear code of length n, dimension k and minimal distance d over the field $\mathbb{F}_q$, omitting q when it is equal to 2. $[n,k,d]_{4+}$ indicates an additive code over $\mathbb{F}_4$ containing 4^k vectors (so $k \in \frac{1}{2}\mathbb{Z}$). Usually the subscript on the symbol for a code (e.g. e_8) gives its length. We adopt the convention that parentheses in a vector mean that all

permutations indicated by the parentheses are to be applied to that vector. For example, in the definition of e_8 below, 1(1101000) stands for the seven vectors 11101000, 10110100, 10011010, etc. The generators for the hexacode in (34) could have been abbreviated as $(100)(1\omega\omega)$.

The following codes are all self-dual.

(2) The first example of a binary self-dual code is the $[2,1,2]$ repetition code $i_2 = \{00, 11\}$, with weight enumerator

$$W_{i_2}(x,y) = x^2 + y^2 = \phi_2 \quad \text{(say)} \ , \tag{25}$$

and $|Aut(i_2)| = 2$.

The $[8,4,4]$ *Hamming* code e_8 (see Section 12 of Chapter 1; [70], p. 80) generated by 1(1101000), is self-dual with weight enumerator

$$W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8 = \phi_8 \ , \tag{26}$$

and group $GA_3(2)$ of order $8.7.6.4 = 1344$.

The $[24,12,8]$ *binary Golay* code g_{24} (Section 12 of Chapter 1; [70], Chaps. 3, 11), generated by

$$1(10101110001100000000000) \ , \tag{27}$$

or equivalently by the idempotent generator

$$1(000001010011001101011111) \ , \tag{28}$$

has weight enumerator

$$W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} = \phi_{24} \ . \tag{29}$$

$Aut(g_{24})$ is the Mathieu group M_{24}, of order $24.23.22.21.20.48 = 244823040$.

All three codes i_2, e_8, g_{24} are unique in the sense that any linear or nonlinear code with the same length, size and minimal distance and containing the zero vector is linear and equivalent to the code given above [227] (see also [291]).

(3) Self-dual codes over $\mathbb{F}_3$ exist if and only if the length n is a multiple of 4 (this follows from Gleason's theorem, see (101), and is also a consequence of the argument used to prove (7) [226]). We use indeterminates x, y for the Hamming weight enumerator $W(x,y)$ and x, y, z for the cwe.

The $[4,2,3]_3$ *tetracode* t_4, generated by $\{1110, 0121\}$ (Section 7 of Chapter 1; [70] p. 81) has

$$W_{t_4}(x,y) = x^4 + 8xy^3 \tag{30}$$

and cwe $x\{x^3 + (y+z)^3\}$. $Aut(t_4) = 2.S(4)$, where $S(n)$ denotes a symmetric group of order $n!$.

The $[12, 6, 6]_3$ *ternary Golay* code g_{12} (Section 12 of Chapter 1; [70], p. 85), generated by 1(11210200000), has

$$W_{g_{12}}(x, y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12} \tag{31}$$

and (assuming the all-ones codeword is present)

$$cwe(x, y, z) = x^{12} + y^{12} + z^{12} + 22(x^6y^6 + y^6z^6 + z^6x^6) + 220(x^6y^3z^3 + x^3y^6z^3 + x^3y^3z^6) \ . \tag{32}$$

$Aut(g_{12}) = 2.M_{12}$ (where M_{12} is a Mathieu group), of order 190080.

These two codes are unique in the same sense as our binary examples [227].

(4^{H}) We use indeterminates x, y for the Hamming weight enumerator, x, y, z for the swe and x, y, z, t (corresponding to the symbols $0, 1, \omega, \overline{\omega}$) for the cwe, so that $swe(x, y, z) = cwe(x, y, z, z)$.

The $[2, 1, 2]_4$ repetition code $i_2 = \{00, 11, \omega\omega, \overline{\omega\omega}\}$ has

$$\begin{aligned} W_{i_2}(x, y) &= x^2 + 3y^2 \ , \\ swe &= x^2 + y^2 + 2z^2 \ , \\ cwe &= x^2 + y^2 + z^2 + t^2 \ , \end{aligned} \tag{33}$$

and a group of order 12.

The $[6, 3, 4]_4$ *hexacode* h_6 (Section 12 of Chapter 1, [70, p. 82]) in the form with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix} \tag{34}$$

has

$$W_{h_6}(x, y) = x^6 + 45x^2y^4 + 18y^6, \tag{35}$$

$$swe = x^6 + y^6 + 2z^6 + 15(2x^2y^2z^2 + x^2z^4 + y^2z^4) \ , \tag{36}$$

$$cwe = x^6 + y^6 + z^6 + t^6 + 15(x^2y^2z^2 + x^2y^2t^2 + x^2z^2t^2 + y^2z^2t^2) \tag{37}$$

and $Aut(h_6) = 3.S(6)$, of order 2160.

Again these codes are unique.

Of course this i_2 is simply the $\mathbb{F}_4$-span of the binary code i_2 defined above. In general, if C is defined over an alphabet $\mathbb{F}$, and $\mathbb{F}' \supseteq \mathbb{F}$ is a larger alphabet, we write $C \otimes \mathbb{F}'$ to indicate this process.

If C is a binary self-dual code then $C \otimes \mathbb{F}_4$ is a self-dual code belonging to both families 4^{H} and 4^{E}. Conversely, it is not difficult to show that if C is self-dual over $\mathbb{F}_4$ with respect to both the Hermitian and Euclidean inner products, then $C = B \otimes \mathbb{F}_4$ for some self-dual binary code B.

(4^{E}) The $[4, 2, 3]_4$ Reed-Solomon code

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \overline{\omega} \end{bmatrix}$$

has

$$\begin{aligned} W(x,y) &= x^4 + 12xy^3 + 3y^4 \ , \\ swe &= x^4 + y^4 + \ 2z^4 + 12xyz^2 \ , \\ cwe &= x^4 + y^4 + z^4 + t^4 + 12xyzt \ . \end{aligned}$$

The automorphism group is $3.S(4)$, of order 72.

($4^{\mathrm{H}+}$) The smallest example is the $[1, \frac{1}{2}, 1]_{4+}$ code $i_1 = \{0, 1\}$, with automorphism group of order 2 (conjugation). The $[12, 6, 6]_{4+}$ *dodecacode* z_{12} can be defined as the cyclic code with generator $\omega 10100100101$ ([49], see also [134]). $Aut(z_{12})$ is a semi-direct product of $Z(3)^3$ with $S(4)$ (where $Z(n)$ denotes a cyclic group of order n) and has order 648.

(q^{H}) Since the norm map from $\mathbb{F}_q$ to $\mathbb{F}_{\sqrt{q}}$ is surjective, there is an element $a \in \mathbb{F}_q$ with $a\overline{a} = -1$. Then $[1a]$ is self-dual.

(q^{E}) As in family 4^{H}, there is a restriction on n: if $q \equiv 3 \pmod 4$ then self-dual codes exist if and only if n is a multiple of 4; for other values of q, n need only be even [226]. Provided $q \not\equiv (3) \pmod 4$, $\mathbb{F}_q$ contains an element i such that $i^2 = -1$, and then $[1i]$ is self-dual.

($4^{\mathbb{Z}}$) The smallest example is the self-dual code $i_1 = \{0, 2\}$ of length 1. The *octacode* o_8 ([70], [71]) is the length 8 code generated by the vectors 3(2001011), or equivalently with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} , \tag{38}$$

having minimal Lee weight 6 and minimal norm 8,

$$swe = x^8 + 16y^8 + z^8 + 14x^4z^4 + 112xy^4z(x^2 + z^2) \ ,$$

and $|Aut(o_8)| = 2.1344$.

The most interesting property of the octacode is that when mapped to a binary code under the Gray map

$$0 \to 00, \quad 1 \to 01, \quad 2 \to 11, \quad 3 \to 10 \ , \tag{39}$$

o_8 becomes the Nordstrom-Robinson code, a nonlinear binary code of length 16, minimal distance 6, containing 256 words (Section 14 of Chapter 1, Chapter xx (Helleseth-Kumar), [99], [119]). The latter is therefore a formally self-dual binary code, see Section 3.3.

The octacode reduces mod 2 to the Hamming code e_8. There is another lift of e_8 to $\mathbb{Z}_4$, namely the code $\mathcal{E}_8$, with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 0 \end{bmatrix} \ , \tag{40}$$

but the minimal Lee weight and norm are now both only 4. However, not all binary self-dual codes lift to self-dual codes over $\mathbb{Z}_4$, e.g. $\{00, 11\}$ does not.

Theorem 3. *(a) Let C be a binary self-dual code of length n. A necessary and sufficient condition for C to be lifted to a self-dual code $\hat{C}$ over $\mathbb{Z}_4$ is that all weights in C are divisible by 4. (b) If this condition is satisfied, $\hat{C}$ can be chosen so that all norms are divisible by 8. (c) More generally, a self-dual code over $\mathbb{Z}_m$, m even, that reduces to a self-dual code* mod 2 *lifts to $\mathbb{Z}_{2m}$ precisely when all norms are divisible by $2m$, and in that case all norms in the lifted code can be arranged to be divisible by $4m$. Thus if a code lifts from $\mathbb{Z}_m$ to $\mathbb{Z}_{2m}$ then it lifts to $\mathbb{Z}_{2^k m}$ for all k. In particular, if a binary code lifts to $\mathbb{Z}_4$ then it lifts to a self-dual code over the 2-adic integers.*

Proof. (a) (Necessity) Suppose $v \in C$ has weight $wt(v) \not\equiv 0 \pmod 4$, and let $\hat{v} \in \hat{C}$ be any lift of v. Then $\mathrm{Norm}(\hat{v}) \equiv \mathrm{Norm}(v) \pmod 4$ because for integers x, y if $x \equiv y \pmod 2$ then $x^2 \equiv y^2 \pmod 4$.

(Sufficiency) Without loss of generality C has a generator matrix of the form $[IA]$ where $AA^{tr} \equiv -I \pmod 2$. Let B be any lift of A to $\mathbb{Z}_4$. We wish to find $\hat{A} = B + 2M$ such that $\hat{A}\hat{A}^{tr} \equiv -I \pmod 4$, since then we can take $\hat{C} = [I\hat{A}]$. We have

$$\hat{A}\hat{A}^{tr} \equiv BB^{tr} + 2(MB^{tr} + BM^{tr}) \pmod 4 \ .$$

The condition on C implies that $BB^{tr} + I$ has even coefficients and is zero on the diagonal. But then there exists a binary matrix M' such that $2(M' + M'^{tr}) = BB^{tr} + I$, and we take $M = M'(B^{-1})^{tr}$. This completes the proof of (a).

(b) We need to show that we can choose $\hat{A}$ so that the diagonal entries of $\hat{A}\hat{A}^{tr} + I$ are zero mod 8. Set $\hat{A}' = \hat{A} - 2L\hat{A}$, where L is symmetric, so that

$$\hat{A}'(\hat{A}')^{tr} = \hat{A}\hat{A}^{tr} + 4L + 4L^2 (\text{mod } 8) \ .$$

Let $\Delta = \frac{1}{4}(\hat{A}\hat{A}^{tr} + I)$. Then we need $L^2 + L + \Delta \ (\text{mod } 2)$ to be symmetric with zero diagonal. It is easy to see that we can accomplish this provided $\text{trace}(\Delta) \equiv 0 \ (\text{mod } 2)$ (consider, for instance, $L = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.) In fact, we have

$$1 \equiv \det(\hat{A}\hat{A}^{tr}) \equiv 1 + 4 \text{ trace } \Delta \ (\text{mod } 8)$$

so trace Δ is even.

The proof of (c) is analogous. ∎

It follows from Theorem 3 that the Golay code g_{24} can be lifted to $\mathbb{Z}_4$. Since g_{24} is an extended cyclic code, the lift can be easily performed by Graeffe's method [71], [313]. Suppose $g_2(x)$ divides $x^n - 1 \ (\text{mod } 2)$, and we wish to find a monic polynomial $g(x)$ over $\mathbb{Z}_4$ such that $g(x) \equiv g_2(x) \ (\text{mod } 2)$ and $g(x)$ divides $x^n - 1 \ (\text{mod } 4)$. Let $g_2(x) = e(x) - d(x)$, where $e(x)$ contains only even powers and $d(x)$ only odd powers. Then $g(x)$ is given by $g(x^2) = \pm(e^2(x) - d^2(x))$. Applying this technique to the generator polynomial for g_{24}, that is, to $g_2(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$ (see (27)), we obtain $g(x) = -1 + x + 2x^4 - x^5 - x^6 - x^7 - x^9 + 2x^{10} + x^{11}$, and so

$$3(3100233303210000000000) \tag{41}$$

generates a self-dual code G_{24} of length 24 which is the Golay code lifted to $\mathbb{Z}_4$. Iterating this process enables us to lift cyclic or extended cyclic codes to $\mathbb{Z}_{2^m}$ for arbitrarily large m.

(F1) Let $q = 5$. Then

$$\begin{bmatrix} 1 & -v & v & -1 & 0 & 0 \\ 0 & 1 & -v & v & -1 & 0 \\ 0 & 0 & 1 & -v & v & -1 \end{bmatrix} \tag{42}$$

where $v = (1 + u)/2$, generates a self-dual code of length 6 over $\mathbb{F}_5[u]/(u^2)$.

The matrix (42) also generates self-dual codes from family q^{H}. Suppose q is a prime power such that $v^2 - v - 1$ has no solution in $\mathbb{F}_q$, and let v be a solution in $\mathbb{F}_{q^2}$. Then (42) defines

a Hermitian self-dual code over $\mathbb{F}_{q^2}$ with minimal distance 4. In the case $q = 2$ we get the hexacode.

(F3) The 2-adic Hamming code [50] is the self-dual code of length 8 with generator matrix

$$\begin{bmatrix} 1 & \lambda & \lambda-1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & \lambda & \lambda-1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & \lambda & \lambda-1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \lambda & \lambda-1 & -1 & 1 \end{bmatrix},$$

where λ is the 2-adic integer $(1+\sqrt{-7})/2$. The 2-adic expansion of λ is

$$\lambda = 2 + 4 + 32 + 128 + 256 + 512 + 1024 + 2048 + 4096 + 32768 + \cdots$$

This is the cyclic code with generator

$$1, \lambda, \lambda - 1, -1, 0, 0, 0$$

with a 1 appended to each of the generators.

Similarly, the 2-adic self-dual Golay code of length 24 is the cyclic code with generator

$$1, 1-\lambda, -2-\lambda, -4, \lambda-4, 2\lambda-3, 2\lambda+1, \lambda+3, 4, 3-\lambda, -\lambda, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 \ ,$$

where now $\lambda = (1+\sqrt{-23})/2$, with a 1 appended to each of the 12 generators.

The 3-adic self-dual Golay code of length 12 is the cyclic code with generator

$$1, \lambda, -1, 1, \lambda-1, -1, 0, 0, 0, 0, 0 \ ,$$

where $\lambda = (1+\sqrt{-11})/2$, again with a 1 appended to each generator.

(F4) We shall not discuss these codes here, but refer the reader to Wood [331].

3.3. MacWilliams Theorems

MacWilliams ([185]; see also [190]) discovered that the Hamming weight distribution of the dual of a linear code is determined just by the Hamming weight distribution of the code. There are versions of this theorem for most of our families of codes. Although there are several ways to state these identities, the simplest formulation is always in terms of the weight enumerator polynomials (it is for this reason that we insist that the weight enumerator should be a homogeneous polynomial).

Theorem 4. (MacWilliams and others.)

(2) Three equivalent formulations of the result for binary self-dual codes are:

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y) \ , \tag{43}$$

$$\sum_{u \in C^\perp} x^{n-wt(u)} y^{wt(u)} = \frac{1}{|C|} \sum_{u \in C} (x+y)^{n-wt(u)} (x-y)^{wt(u)} \ , \tag{44}$$

and, if $\{A_0^\perp, A_1^\perp, \ldots\}$ *is the weight distribution of* $C^\perp$*,*

$$A_k^\perp = \frac{1}{|C|} \sum_{i=0}^{n} A_i P_k(i) \tag{45}$$

where

$$P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}, \quad k = 0, \ldots, n \ ,$$

is a Krawtchouk polynomial ([190], Chap. 5; etc.). There are analogous Krawtchouk polynomials for any alphabet, see [190], p. 151. For the remaining cases we give just the formulation in terms of weight enumerators.

(3)

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{|C|} W_C(x+2y, x-y) \ , \\ cwe_{C^\perp}(x,y,z) &= \frac{1}{|C|} cwe_C(x+y+z, x+\omega y+\overline{\omega} z, x+\overline{\omega} y+\omega z) \ . \end{aligned}$$

(4^{H}) *and* $(4^{\mathrm{H}+})$

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{|C|} W_C(x+3y, x-y) \ , \\ swe_{C^\perp}(x,y,z) &= \frac{1}{|C|} swe_C(x+y+2z, x+y-2z, x-y) \ , \\ cwe_{C^\perp}(x,y,z,t) &= \frac{1}{|C|} cwe_C(x+y+z+t, x+y-z-t, x-y+z-t, x-y-z+t) \ . \end{aligned}$$

(4^{E})

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{|C|} W_C(x+3y, x-y) \ , \\ swe_{C^\perp}(x,y,z) &= \frac{1}{|C|} swe_C(x+y+2z, x+y-2z, x-y) \ , \\ cwe_{C^\perp}(x,y,z,t) &= \frac{1}{|C|} cwe_{C^\perp}(x+y+z+t, x+y-z-t, x-y-z+t, x-y+z-t) \ . \end{aligned}$$

(q^{H})

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y) \ . \tag{46}$$

Let λ be a nontrivial linear functional from $\mathbb{F}_q$ to $\mathbb{F}_p$, and set

$$\chi_\beta(x) = e^{2\pi i \lambda(\beta\overline{x})/p} \ . \tag{47}$$

The cwe for $C^\perp$ is obtained from the cwe for C by replacing each x_j by

$$\sum_{k=0}^{q-1} \chi_{\xi_j}(\xi_k) x_k \ .$$

(We omit discussion of the swe, since there are several different ways in which it might be defined.)

(q^{E}) *Same as for q^{H}, but omitting the bar in (47).*

($4^{\mathbb{Z}}$)

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{|C|} W_C(x+3y, x-y) \\ swe_{C^\perp}(x,y,z) &= \frac{1}{|C|} swe_C(x+2y+z, x-y, x-2y+z) \\ cwe_{C^\perp}(x,y,z,t) &= \frac{1}{|C|} cwe_C(x+y+z+t, x+iy-z-it, x-y+z-t, x-iy-z+it) \ . \end{aligned}$$

($m^{\mathbb{Z}}$)

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

The cwe for $C^\perp$ is obtained from the cwe for C by replacing each x_j by

$$\sum_{k=0}^{m-1} e^{2\pi i jk/m} x_k \ . \tag{48}$$

Proof. We prove the result for family 2. There are analogous proofs for the other cases, cf. Section 10 of Chapter 1, Section 8 of Chapter xx (Helleseth-Kumar), [182], [190, Chap. 5].

Let f be a polynomial-valued function on $\mathbb{F}_2^n$. Define the *Fourier* (or *Hadamard*) *transform* of f by

$$\hat{f}(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{u.v} f(v), \quad u \in \mathbb{F}_2^n \ .$$

If C is a linear code it is straightforward to verify that

$$\sum_{u \in C^\perp} f(u) = \frac{1}{|C|} \sum_{u \in C} \hat{f}(u) \ . \tag{49}$$

(This is a version of the Poisson summation formula — cf. [91].) Now we set $f(u) = x^{n-wt(u)} y^{wt(u)}$, and after some algebra (the details can be found on p. 126 of [190]) discover that

$$\hat{f}(u) = (x+y)^{n-wt(u)} (x-y)^{wt(u)} \ . \tag{50}$$

Equations (49) , (50) together imply (44). ∎

Examples

(a) The *repetition* code C over a field $\mathbb{F}_q$ has Hamming weight enumerator

$$W_C(x,y) = x^n + (q-1)y^n \ ,$$

so from (46) we deduce that the dual code $C^\perp$, the *zero-sum* code, has weight enumerator

$$W_{C^\perp}(x,y) = \frac{1}{q}\left\{(x+(q-1)y)^n + (q-1)(x-y)^n\right\} \ .$$

Note that when $n=2$, $W_{C^\perp} = W_C$ (compare case (e) of Theorem 5).

(b) The binary codes i_2 and e_8 are self-dual, and indeed one easily verifies that their weight enumerators x^2+y^2 (25) and $x^8+14x^4y^4+y^8$ (26) are left unchanged if x and y are replaced by $(x+y)/\sqrt{2}$ and $(x-y)/\sqrt{2}$.

Remarks

1. The map that sends $W_C(x,y)$ to $\frac{1}{|C|}W_C(x+y,x-y)$, or that sends $\{A_0, A_1, \ldots\}$ to $\{A_0^\perp, A_1^\perp, \ldots\}$ as in (45), is often called the *MacWilliams* or *Krawtchouk* transform. A remarkable theorem of Delsarte [78] — see Chapters xx (Brouwer), yy (Camion), zz (Levenshtein) — shows that this transform is useful even for nonlinear codes.

2. For the families 2, 4^{H}, 4^{E} and $4^{\mathrm{H}+}$ all the MacWilliams transforms have order 2, as they do for the Hamming weight enumerators for families 3 and $4^{\mathbb{Z}}$ and the swe for $4^{\mathbb{Z}}$. For the cwe in families 3 and $4^{\mathbb{Z}}$ the square of the MacWilliams transform takes x_j to x_{-j}. However, this does not change the cwe of the code, and so, in all cases, if the MacWilliams transform is applied twice, the original weight enumerator is recovered.

3. The identity for the swe in family $m^{\mathbb{Z}}$ is left to the reader. For (F1) we refer to Bachoc [8] and for (F4) to Wood [331]. Duality fails for (F2) and weights are undefined in case (F3).

4. Shor and Laflamme [281] show that there is an analogue of the MacWilliams identity for quantum codes. There is also an analogue of the shadow [251].

3.4. Isodual and formally self-dual codes

Following [72], we say that a linear code which is equivalent to its dual is *isodual*. A (possibly nonlinear) code with the property that its weight enumerator coincides with its MacWilliams transform is called *formally self-dual*. An isodual code is automatically formally self-dual.

It is easy to prove that any self-dual code from family $4^{\mathbb{Z}}$ produces a formally self-dual binary code using the Gray map (39) ([99], [119]). As already mentioned in Section 3.2, the

octacode o_8 produces the (formally self-dual) Nordstrom-Robinson code in this way. Similarly,[3] a self-dual code from family $4^{\mathrm{H}+}$ produces an isodual binary code using the map

$$0 \to 00, \quad 1 \to 11, \quad \omega \to 01, \quad \overline{\omega} \to 10 \ . \tag{51}$$

We give several examples of this construction.

(i) The code d_3^+ (see Section 11.7) produces the isodual $[6, 3, 3]$ binary code with generator matrix

$$\begin{bmatrix} 11 & 11 & 00 \\ 11 & 00 & 11 \\ 10 & 10 & 10 \end{bmatrix} \ . \tag{52}$$

(The dual, which is a different code, is obtained by interchanging the last two columns.)

(ii) The shortened hexacode, h_5, (see Section 12.4) produces an isodual $[10, 5, 4]$ code.

(iii) The hexacode h_6 produces an isodual $[12, 6, 4]$ code. There is an additive but not linear version of the hexacode, h_6', found by Ran and Snyders [260], generated by $(0011\omega\overline{\omega})$, which under the map (51) produces a second, inequivalent, isodual $[12, 6, 4]$ code. As members of the family $4^{\mathrm{H}+}$, however, h_6 and h_6' are equivalent.

Further examples of formally self-dual codes will be mentioned in Remark 4 following Theorem 5. Isodual and formally self-dual codes have also been studied in [87], [109], [113], [121], [160], [190], [287] (see also [72]).

4. Restrictions on weights

4.1. Gleason-Pierce Theorem

It is elementary that in a binary self-orthogonal code the weight of every vector is even, in a ternary self-dual code the weight of every vector is a multiple of 3, and in a Hermitian self-dual code over $\mathbb{F}_4$ the weight of every vector is even. Furthermore, there are many well-known binary self-dual codes whose weights are divisible by 4 — see above. The following theorem, due to Gleason and Pierce, shows that these four are essentially the only possible nontrivial divisibility restrictions that can be imposed on the weights of self-dual codes.

Theorem 5. (Gleason and Pierce [5].) *If C is a self-dual code belonging to any of the families 2 through $m^{\mathbb{Z}}$ which has all its Hamming weights divisible by an integer $c > 1$ then one of the*

[3] We are indebted to Dave Forney for these remarks.

following holds:

(a) $|\mathbb{F}| = 2, \quad c = 2 \quad$ (*so family* 2)

(b) $|\mathbb{F}| = 2, \quad c = 4 \quad$ (*so family* 2)

(c) $|\mathbb{F}| = 3, \quad c = 3 \quad$ (*so family* 3)

(d) $|\mathbb{F}| = 4, \quad c = 2 \quad$ (*so families* 4^{H}, 4^{E}, $4^{\mathrm{H}+}$, $4^{\mathbb{Z}}$)

(e) $|\mathbb{F}| = q, \quad q$ *arbitrary*, $\quad c = 2, \quad$ and

the Hamming weight enumerator of C *is*

$$(x^2 + (q-1)y^2)^{n/2} \ .$$

Remarks. 1. The theorem may be proved by considering how the Hamming weight enumerator behaves under the MacWilliams transform — see [285] for details. An alternative proof of a somewhat more general result is given in [320] — see Theorem 13.5 of Chapter xx (Ward).

2. The same conclusion holds if "C is self-dual" is replaced by "C is formally self-dual".

3. Note that there are no nontrivial examples from families q^{H}, q^{E} or $m^{\mathbb{Z}}$.

4. There are several points to be mentioned concerning case (e). *Linear* self-dual codes with weight enumerator $(x^2 + (q-1)y^2)^{n/2}$ always exist in families 2, 4^{H}, 4^{E}, $4^{\mathrm{H}+}$, q^{H}; exist in families q^{E} and $m^{\mathbb{Z}}$ precisely when there is a square root of -1 in $\mathbb{F}_q$ or $\mathbb{Z}_m$ respectively; in particular, they never exist in families 3 or $4^{\mathbb{Z}}$.

Furthermore, it is easy to see that any linear code over $\mathbb{F}_q$ for $q > 2$ with weight enumerator $(x^2 + (q-1)y^2)^{n/2}$ is a direct sum of codes of length 2. However, in the binary case there are many examples of linear codes with weight enumerator $(x^2 + y^2)^{n/2}$ that are not self-dual: these have been classified for $n \leq 16$, see [287]. These are examples of formally self-dual codes: see Section 3.4. There are also examples from family $4^{\mathrm{H}+}$, e.g. the additive code $[1100, 0110, 0011, \omega\omega\omega\omega]$ with weight enumerator $(x^2 + 3y^2)^2$.

5. In some cases, analogous restrictions can be imposed on Euclidean norms of codewords. In particular, suppose C is a self-dual code over $\mathbb{Z}_m$ (that is, a code from families $4^{\mathbb{Z}}$ or $m^{\mathbb{Z}}$) where m is even. Then the Euclidean norms of the codewords *must* be divisible by m, and *may* be divisible by $2m$ ([9], [27], [82], see also Theorem 3).

6. Codes from family (F1) with $q = 2$ can also satisfy case (d) of the theorem, since they can be embedded in family $4^{\mathrm{H}+}$ via the map $a + bu \to a + b\omega$.

Examples

Many of the examples given in Section 3.2 satisfy one of these divisibility conditions:

(2): all self-dual codes satisfy (a), and e_8 and g_{24} satisfy (b). Note that any code satisfying (b) is self-orthogonal (from (22)).

(3): a code satisfies (c) precisely when it is self-orthogonal

(4^{H}): a code satisfies (d) precisely when it is self-orthogonal

(4^{E}): a self-dual code satisfying (d) is a linearized binary code

($4^{\mathrm{H}+}$): The dodecacode z_{12} satisfies (d). Any code satisfying (d) is self-orthogonal.

4.2. Type I and Type II codes

A binary self-dual code C with all weights divisible by 4 is called *doubly-even*[4] or of *Type II*; if we do not impose this restriction then C is *singly-even* or of *Type I*. We denote these two families by 2_{I} and 2_{II}. A Type I code may or may not also be of Type II: the classes are not mutually exclusive. We say a code is *strictly Type I* if it is not of Type II.

Similarly, we will say that a self-dual code over $\mathbb{Z}_m$, m even, from the families $4^{\mathbb{Z}}$ or $m^{\mathbb{Z}}$ is of *Type II* if the Euclidean norms are divisible by $2m$, or of *Type I* if they are divisible by m. (This terminology was introduced in [9], [27], [82].) We denote these families by $4^{\mathbb{Z}}_{\mathrm{I}}$ (or $m^{\mathbb{Z}}_{\mathrm{I}}$) and $4^{\mathbb{Z}}_{\mathrm{II}}$ (or $m^{\mathbb{Z}}_{\mathrm{II}}$).

There is one other situation where a similar distinction can be made. An additive trace-Hermitian self-dual code over $\mathbb{F}_4$ from the family $4^{\mathrm{H}+}$ is of *Type II* if the Hamming weights are even, or of *Type I* if odd weights may occur (if odd weights do occur then the code cannot be linear). We denote these two families by $4^{\mathrm{H}+}_{\mathrm{I}}$ and $4^{\mathrm{H}+}_{\mathrm{II}}$.

More generally, we will say that a binary code is *doubly-even* if all its weights are divisible by 4, or *singly-even* if its weights are even. It follows from (22) that a doubly-even code is necessarily self-orthogonal (and from (23) and (24) that Type II codes over $\mathbb{Z}_m$ and $\mathbb{F}_4$ are necessarily self-orthogonal).

In view of Theorem 5, in the past self-dual codes over $\mathbb{F}_3$ have been called *Type III* codes, and Hermitian self-dual codes over $\mathbb{F}_4$ have been called *Type IV* codes. However, we shall not use that terminology in this chapter.

[4]The unqualified term "even" has been used to denote both Type I and Type II codes, and is therefore to be avoided when speaking of self-dual codes. Use "singly-even" or "doubly-even" instead.

5. Shadows

In the three cases where we can define a Type II code (see the previous section) we can also define a certain canonical translate of a code called its shadow [69]. The weight enumerator of the shadow can be obtained from the weight enumerator of the code via a transformation analogous to the MacWilliams transform of Theorem 4.

We first discuss binary codes.

Lemma 1. *Let C be a self-orthogonal singly-even binary code, and let C_0 be the subset of doubly-even codewords. Then C_0 is a linear subcode of index 2 in C.*

Proof. From (22), $\frac{1}{2}wt(u)$ is a linear functional on C, and C_0 is its kernel.

Definition 1. [69]. The *shadow*[5] S of a self-orthogonal binary code C is

$$S = \left\{ \begin{array}{ll} C_0^{\perp} \setminus C^{\perp} & \text{if } C \text{ is singly-even} \\ C^{\perp} & \text{if } C \text{ is doubly-even} \end{array} \right\} .$$

The weight enumerator of the shadow of C will usually be denoted by $S_C(x, y)$.

Examples. (i) If C is the repetition code $\{0^n, 1^n\}$ of even length n, then if $n \equiv 0 \pmod 4$, $S = C^{\perp}$ = all even weight vectors, but if $n \equiv 2 \pmod 4$, S = all odd weight vectors. (ii) If $C = i_2 \oplus i_2 \oplus \cdots \oplus i_2$ then S is the translate of C by $1010\ldots10$. (iii) Let C be the $[22, 11, 6]$ shorter Golay code g_{22}, obtained by "subtracting" (see Section 11.3) i_2 from g_{24}, so that g_{22} consists of all words of g_{24} that begin 00 or 11, with these two coordinates deleted. Then S consists of the remaining words of g_{24} with the same two coordinates deleted.

Theorem 6. [69] *The shadow S has the following properties:*

(i) S is the set of "parity vectors" for C; that is,

$$S = \{u \in \mathbb{F}_2^n : (u, v) \equiv \frac{1}{2}wt(v) \bmod 2 \quad \text{for all} \quad v \in C\} \tag{53}$$

(ii) S is a coset of $C^{\perp}$

(iii)

$$S_C(x, y) = \frac{1}{|C|} W_C(x + y, i(x - y)) \ . \tag{54}$$

[5] A somewhat more general definition of shadow has been proposed in [35], but since it fails to possess the crucial properties (i) and (iii) of Theorem 6 we shall not discuss it here.

Proof. If C is doubly-even then (i) and (ii) are immediate, and (iii) follows from the MacWilliams transform and the fact that the weights are divisible by 4. Suppose C is singly-even, let C_0 be the doubly-even subcode, and let $C_1 = C \setminus C_0$. Then

$$C_0 \subseteq C \subseteq C^\perp \subseteq C_0^\perp \ . \tag{55}$$

The first and last inclusions have index 2, so $C_0^\perp = C^\perp \cup (a + C^\perp)$, say, where $(a, u) = 0$ for $u \in C_0$, $(a, v) = 1$ for $v \in C_1$. Thus $S = C_0^\perp \setminus C_0 = a + C_0$ has the properties stated in (i) and (ii). Also,

$$\begin{aligned} W_{C_0}(x, y) &= \frac{1}{2}\{W_C(x, y) + W_C(x, iy)\} \ , \\ W_{C_0^\perp}(x, y) &= \frac{1}{|C|}\{W_C(x + y, x - y) + W_C(x + y, i(x - y)\} \ , \end{aligned}$$

so

$$S_C(x, y) = W_{C_0^\perp} - W_{C^\perp} = \frac{1}{|C|} W_C(x + y, i(x - y)) \ . \quad \blacksquare$$

If C is a singly-even self-dual code with doubly-even subcode C_0, then $C_0^\perp$ is the union of four translates of C_0, say C_0, C_1, C_2, C_3, with

$$C = C_0 \cup C_2, \quad S = C_1 \cup C_3 \ . \tag{56}$$

When n is a multiple of 8 then $C' = C_0 \cup C_1$ and $C'' = C_0 \cup C_3$ are both Type II codes (in the notation of Chapter xx (Pless), C' and C'' are *neighbors* of C). If C has a weight 2 word then C' and C'' are equivalent.

Similar definitions for the shadow can be given in the other two cases mentioned. If C is an additive trace-Hermitian self-orthogonal code over $\mathbb{F}_4$, let C_0 be the subcode with even Hamming weights, and secondly, if C is a self-orthogonal code over $\mathbb{Z}_m$ (m even) let C_0 be the subcode with Euclidean norms divisible by $2m$. In both cases the shadow is defined by:

$$S = \begin{cases} C_0^\perp \setminus C_0 & \text{if } C \neq C_0 \\ C^\perp & \text{if } C = C_0 \ . \end{cases}$$

If C is self-dual from family $4^{\mathrm{H}+}$ then the quotient group $C_0^\perp / C_0$ is isomorphic to $Z(2) \times Z(2)$. If C is self-dual from family $m^{\mathbb{Z}}$ then $C_0^\perp / C_0$ is isomorphic to $Z(2) \times Z(2)$ if n is even and to $Z(4)$ if n is odd.

There are analogues of Theorem 6.

Theorem 7. *Let C be a self-orthogonal additive code over $\mathbb{F}_4$, with shadow S.*

(i) $S = \{u \in \mathbb{F}_4^n : (u,v) \equiv wt(v) \pmod 2 \quad \text{for all } v \in C\}$

(ii) S is a coset of $C^\perp$

(iii)

$$S_C(x,y) = \frac{1}{|C|} W_C(x+3y, y-x) \ ,$$

$$swe_S(x,y,z) = \frac{1}{|C|}\ swe_C(x+y+2z, -x-y+2z, y-x)$$

$$cwe_S(x,y,z,t) = \frac{1}{|C|} cwe_C(x+y+z+t, -x-y+z+t, -x+y-z+t, -x+y+z-t) \ .$$

Remark. It follows from Theorem 7 that there is a code equivalent to C that has $1^n \in S$. For the number of vectors of weight n in S is

$$S_C(0,1) = \frac{1}{|C|} W_C(3,1) > 0 \ .$$

All vectors of full weight are equivalent.

Theorem 8. *Let C be a self-orthogonal linear code over $\mathbb{Z}_4$, with shadow S.*

(i) $S = \{u \in \mathbb{Z}_4^n : (u,v) \equiv \frac{1}{2} \text{ Norm}(v) \pmod 4 \quad \text{for all } v \in C\}$

(ii) S is a coset of $C^\perp$

(iii) $swe_S(x,y,z) = \frac{1}{|C|} swe_C(x+2y+z, \eta(x-y), -x+2y-z)$, *where* $\eta = e^{\pi i/4}$,

$$cwe_S(x,y,z,t) = \frac{1}{|C|} cwe_C(x+y+z+t, \eta(x+iy-z-it), -(x-y+z-t), \eta(x-iy-z+it)) \ .$$

Remark. It follows that the shadow contains a vector of the form $\pm 1^n$. (For $cwe_S(0,1,0,1) = \frac{1}{|C|} cwe_C(2,0,2,0) = cwe_C(1,0,1,0) > 0$, since $0^n \in C$.) This observation, and a formula for the swe equivalent to ours, can be found in [88]. In particular, a self-dual code from family $4_{\text{II}}^{\mathbb{Z}}$ contains a vector of the form $\pm 1^n$.

Theorem 9. *Let C be a self-orthogonal linear code over $\mathbb{Z}_m$, m even, with shadow S.*

(i) $S = \{u \in \mathbb{Z}_m^n : (u,v) \equiv \frac{1}{2} \text{ Norm}(v) \pmod m \quad \text{for all } v \in C\}$

(ii) S is a coset of $C^\perp$

(iii) The cwe of S is obtained from the cwe of C by replacing each x_j by

$$\sum_{k=0}^{m-1} e^{2\pi i(j^2+2jk)/2m} x_k \ ,$$

and then dividing by $|C|$.

The proofs are analogous to that of Theorem 6.

6. Invariant theory

6.1. An introduction to invariant theory

If C is self-dual then its weight enumerator must be unchanged by the appropriate transformation from Theorem 4. As we will see, this imposes strong restrictions on the weight enumerator.

We begin by discussing the particular case of the weight enumerator $W(x,y)$ of a binary doubly-even self-dual code C. Since C is self-dual, Theorem 4 implies

$$\begin{aligned} W(x,y) &= \frac{1}{2^{n/2}} W(x+y, x-y) \\ &= W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \end{aligned} \tag{57}$$

(for $W(x,y)$ is homogeneous of degree n). Since all weights are divisible by 4, $W(x,y)$ only contains powers of y^4. Therefore

$$W(x,y) = W(x,iy) \ . \tag{58}$$

The problem we wish to solve is to find all polynomials $W(x,y)$ satisfying (57) and (58).

Invariants. Equation (57) says that $W(x,y)$ is unchanged, or *invariant*, under the linear transformation

$$T_1 : \begin{array}{l} \text{replace } x \text{ by } \dfrac{x+y}{\sqrt{2}} \ , \\ \\ \text{replace } y \text{ by } \dfrac{x-y}{\sqrt{2}} \ , \end{array}$$

or, in matrix notation,

$$T_1 : \quad \text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ .$$

Similarly, (58) says that $W(x,y)$ is also invariant under the transformation

$$T_2 : \begin{array}{l} \text{replace } x \text{ by } x \\ \\ \text{replace } y \text{ by } iy \end{array}$$

or

$$T_2 : \quad \text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \ .$$

Of course $W(x,y)$ must therefore be invariant under any combination $T_1^2, T_1T_2, T_1T_2T_1, \ldots$ of these transformations. It is not difficult to show (as we shall see in the next section) that

the matrices

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$$

when multiplied together in all possible ways produce a group $\mathcal{G}_1$ containing 192 matrices.

So our problem now says: find the polynomials $W(x, y)$ which are invariant under all 192 matrices in the group $\mathcal{G}_1$.

How many invariants? The first thing we want to know is how many invariants there are. This isn't too precise, because of course if f and g are invariants, so is any constant multiple cf and also $f + g$, $f - g$ and the product fg. Also it is enough to study the *homogeneous* invariants (in which all terms have the same degree).

So the right question to ask is: how many linearly independent, homogeneous invariants are there of each degree d? Let's call this number a_d.

A convenient way to handle the numbers $a_0, a_1, a_2, \ldots$ is by combining them into a power series or generating function

$$\Phi(\lambda) = a_0 + a_1\lambda + a_2\lambda^2 + \cdots \ .$$

Conversely, if we know $\Phi(\lambda)$, the numbers a_d can be recovered from the power series expansion of $\Phi(\lambda)$.

At this point we invoke a beautiful theorem of T. Molien, published in 1897 ([202]; see also [13], p. 21; [31], p. 110; [37], p. 301; [200], p. 259; [289], p. 86; [298], p. 29).

Theorem 10. (Molien) *For any finite group $\mathcal{G}$ of complex $m \times m$ matrices, $\Phi(\lambda)$ is given by*

$$\Phi(\lambda) = \frac{1}{|\mathcal{G}|}\sum_{A\in\mathcal{G}} \frac{1}{\det(I - \lambda A)} \ . \tag{59}$$

We call $\Phi(\lambda)$ the *Molien series* of $\mathcal{G}$. The proof of this theorem is given in the next section.

For our group $\mathcal{G}_1$, from the matrices corresponding to I, T_1, $T_2, \ldots$ we get

$$\Phi(\lambda) = \frac{1}{192}\left\{\frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + \cdots\right\} \ . \tag{60}$$

There are shortcuts, but it is quite feasible to work out the 192 terms directly (many are the same) and add them. The result is a surprise: everything collapses to give

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \ . \tag{61}$$

Interpreting $\Phi(\lambda)$. The very simple form of (61) is trying to tell us something. Expanding in powers of λ, we have

$$\begin{aligned}\Phi(\lambda) &= a_0 + a_1\lambda + a_2\lambda^2 + \cdots \\ &= (1 + \lambda^8 + \lambda^{16} + \lambda^{24} + \cdots)(1 + \lambda^{24} + \lambda^{48} + \cdots) \ . \end{aligned} \tag{62}$$

We can deduce one fact immediately: a_d is zero unless d is a multiple of 8, i.e. the degree of a homogeneous invariant must be a multiple of 8. (This already proves that the length of a doubly-even binary self-dual code must be a multiple of 8.) But we can say more. The right-hand side of (62) is exactly what we would find if there were two "basic" invariants, of degrees 8 and 24, such that all invariants are formed from sums and products of them.

This is because two invariants, θ, of degree 8, and ϕ, of degree 24, would give rise to the following invariants.

Degree d	Invariants	Number a_d
0	1	1
8	θ	1
16	θ^2	1
24	θ^3, ϕ	2
32	$\theta^4, \theta\phi$	2
40	$\theta^5, \theta^2\phi$	2
48	$\theta^6, \theta^3\phi, \phi^2$	3
$\cdots$	$\cdots$	$\cdots$

(63)

Provided all the products $\theta^i\phi^j$ are linearly independent — which is the same thing as saying that θ and ϕ are algebraically independent — the numbers a_d in (63) are exactly the coefficients in

$$\begin{aligned} &1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + 2\lambda^{40} + 3\lambda^{48} + \cdots \\ &\quad = (1 + \lambda^8 + \lambda^{16} + \lambda^{24} + \cdots)(1 + \lambda^{24} + \lambda^{48} + \cdots) \\ &\quad = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \ , \end{aligned} \tag{64}$$

which agrees with (61). So if we can find two algebraically independent invariants of degrees 8 and 24, we will have solved our problem. The answer will be that any invariant of this group is a polynomial in θ and ϕ. Now ϕ_8 (Eq. (26)) and ϕ_{24} (Eq. (29)), the weight enumerators of the Hamming and Golay codes, have degrees 8 and 24 and are invariant under the group. So we can take $\theta = \phi_8$ and $\phi = \phi_{24}$. (It's not difficult to verify that they are algebraically independent.) Actually, it is easier to work with

$$\phi'_{24} = \frac{\phi_8^3 - \phi_{24}}{42} = x^4y^4(x^4 - y^4)^4 \tag{65}$$

rather than ϕ_{24} itself. So we have proved the following theorem, discovered by Gleason in 1970.

Theorem 11. *Any invariant of the group $\mathcal{G}_1$ is a polynomial in ϕ_8 and ϕ'_{24}.*

This also gives us the solution to our original problem:

Theorem 12. *Any polynomial which satisfies Equations (57) and (58) is a polynomial in ϕ_8 and ϕ'_{24}.*

Finally, we have characterized the weight enumerator of a doubly-even binary self-dual code.

Theorem 13. (Gleason [105].) *The weight enumerator of any Type II binary self-dual code is a polynomial in ϕ_8 and ϕ'_{24}.*

Alternative proofs of this astonishing theorem are given by Berlekamp et al. [14], and Broué and Enguehard [33] (see also Assmus and Mattson [4]). But the proof given here seems to be the most informative, and the easiest to understand and to generalize.

Notice how the exponents 8 and 24 in the denominator of (61) led us to guess the degrees of the basic invariants.

This behavior is typical, and is what makes the technique exciting to use. One starts with a group of matrices $\mathcal{G}$, computes the complicated-looking sum shown in (59), and simplifies the result. Everything miraculously collapses, leaving a final expression resembling (61) (although not always quite so simple — the precise form of the final expression is given in (88), (88)). This expression then tells the degrees of the basic invariants to look for.

Finding the basic invariants. In general, finding the basic invariants is a simpler problem than finding $\Phi(\lambda)$. In our applications we can often use the weight enumerators of codes having the appropriate properties, as in the above example, or basic invariants can be found by *averaging*, using the following simple result (proved in Section 6.2).

Theorem 14. *If $f(\mathbf{x}) = f(x_1, \ldots, x_m)$ is any polynomial in m variables, and $\mathcal{G}$ is a finite group of $m \times m$ matrices, then*

$$\overline{f}(\mathbf{x}) = \frac{1}{|\mathcal{G}|} \sum_{A \in \mathcal{G}} A \circ f(\mathbf{x}) \tag{66}$$

is an invariant, where $A \circ f(\mathbf{x})$ denotes the polynomial obtained by applying the transformation A to the variables in f.

Of course $\overline{f}(\mathbf{x})$ may be zero. An example of the use of this theorem is given below.

To illustrate the use of Theorem 13, we use it to find the weight enumerator of the $[48, 24, 12]$ extended quadratic residue code XQ_{47}, using only the fact that it is a doubly-even self-dual code with minimal distance 12. This implies that the weight enumerator of the code, which is a homogeneous polynomial of degree 48, has the form

$$W(x, y) = x^{48} + A_{12}x^{36}y^{12} + \cdots \ . \tag{67}$$

The coefficients of $x^{47}y$, $x^{46}y^2, \ldots, x^{37}y^{11}$ are zero. Here A_{12} is the unknown number of codewords of weight 12. It is remarkable that, once we know Equation (67), the weight enumerator is completely determined by Theorem 13. For Theorem 13 says that $W(x, y)$ must be a polynomial in ϕ_8 and ϕ'_{24}. Since $W(x, y)$ is homogeneous of degree 48, ϕ_8 is homogeneous of degree 8, and ϕ'_{24} is homogeneous of degree 24, this polynomial must be a linear combination of ϕ_8^6, $\phi_8^3\phi'_{24}$ and ϕ'^2_{24}.

Thus Theorem 13 says that

$$W(x, y) = a_0\phi_8^6 + a_1\phi_8^3\phi'_{24} + a_2\phi'^2_{24} \ , \tag{68}$$

for some real numbers a_0, a_1, a_2. Expanding (68), we have

$$\begin{aligned} W(x, y) \ &= \ a_0(x^{48} + 84x^{44}y^4 + 2946x^{40}y^8 + \cdots) + a_1(x^{44}y^4 + 38x^{40}y^8 + \cdots) \\ &\quad + a_2(x^{40}y^8 - \cdots) \ , \end{aligned} \tag{69}$$

and equating coefficients in (67), (69) we get

$$a_0 = 1, \quad a_1 = -84, \quad a_2 = 246 \ .$$

Therefore $W(x, y)$ is uniquely determined. When these values of a_0, a_1, a_2 are substituted in (68) we find that

$$\begin{aligned} W(x, y) \ &= \ x^{48} + 17296x^{36}y^{12} + 535095x^{32}y^{16} \\ &\quad + 3995376x^{28}y^{20} + 7681680x^{24}y^{24} + 3995376x^{20}y^{28} \\ &\quad + 535095x^{16}y^{32} + 17296x^{12}y^{36} + y^{48} \ . \end{aligned} \tag{70}$$

This is certainly faster than computing W by examining each of the 2^{24} codewords.

There is a fair amount of algebra involved in computing (61). Here is a second example, simple enough for the calculations to be shown in full.

For a self-dual code from family q^{H}, from (46) the Hamming weight enumerator satisfies

$$W\left(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right) = W(x,y) \ . \tag{71}$$

Let us consider the problem of finding all polynomials which satisfy (71).

The solution proceeds as before. Equation (71) says that $W(x,y)$ must be invariant under the transformation

$$T_3: \quad \text{replace} \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } A \begin{pmatrix} x \\ y \end{pmatrix} ,$$

where

$$A = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \ . \tag{72}$$

Now $A^2 = I$, so $W(x,y)$ must be invariant under the group $\mathcal{G}_2$ consisting of the two matrices I and A.

To find how many invariants there are, we compute the Molien series $\Phi(\lambda)$ from (59). We find

$$\begin{aligned} \det(I-\lambda I) &= (1-\lambda)^2 \ , \\ \det(I-\lambda A) &= \det \begin{bmatrix} 1-\frac{\lambda}{\sqrt{q}} & -\frac{q-1}{\sqrt{q}}\lambda \\ -\frac{\lambda}{\sqrt{q}} & 1+\frac{\lambda}{\sqrt{q}} \end{bmatrix} = 1-\lambda^2 \ , \\ \Phi(\lambda) &= \frac{1}{2}\left(\frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2}\right) \\ &= \frac{1}{(1-\lambda)(1-\lambda^2)} \ . \end{aligned} \tag{73}$$

which is even simpler than (61). Equation (73) suggests that there might be two basic invariants, of degrees 1 and 2 (the exponents in the denominator). If algebraically independent invariants of degrees 1 and 2 can be found, say g and h, then (73) implies that any invariant of $\mathcal{G}_2$ is a polynomial in g and h.

This time we shall use the method of averaging to find the basic invariants. Let us average x over the group — i.e., apply Theorem 14 with $f(x,y) = x$. The matrix I leaves x unchanged, of course, and the matrix A transforms x into $(1/\sqrt{q})(x+(q-1)y)$. Therefore the average,

$$\overline{f}(x,y) = \frac{1}{2}\left[x + \frac{1}{\sqrt{q}}\{x+(q-1)y\}\right] = \frac{(\sqrt{q}+1)\{x+(\sqrt{q}-1)y\}}{2\sqrt{q}} \ ,$$

is an invariant. Of course any scalar multiple of $\overline{f}(x,y)$ is also an invariant, so we may divide by $(\sqrt{q}+1)/2\sqrt{q}$ and take

$$g = x + (\sqrt{q}-1)y \tag{74}$$

to be the basic invariant of degree 1. To get an invariant of degree 2 we average x^2 over the group, obtaining

$$\frac{1}{2}\left[x^2 + \frac{1}{q}\{x + (q-1)y\}^2\right] .$$

This can be cleaned up by subtracting $((q+1)/2q)g^2$ (which of course is an invariant), and dividing by a suitable constant. The result is

$$h = y(x-y) ,$$

the desired basic invariant of degree 2.

Finally g and h must be shown to be algebraically independent: it must be shown that no sum of the form

$$\sum_{i,j} c_{ij} g^i h^j, \quad c_{ij} \text{ complex and not all zero} , \tag{75}$$

is identically zero when expanded in powers of x and y. This can be seen by looking at the leading terms. The leading term of g is x, the leading term of h is xy, and the leading term of $g^i h^j$ is $x^{i+j}y^j$. Since distinct summands in (75) have distinct leading terms, (75) can only add to zero if all the c_{ij} are zero. Therefore g and h are algebraically independent. So we have proved:

Theorem 15. *Any invariant of the group $\mathcal{G}_2$, or equivalently any polynomial satisfying (71), or equivalently the Hamming weight enumerator of any self-dual code from family q^{H}, is a polynomial in $g = x + (\sqrt{q}-1)y$ and $h = y(x-y)$.*

At this point the reader should cry Stop!, and point out that self-dual codes from family q^{H} must have even length, and so every term in the weight enumerator must have even degree. But in Theorem 15, g has degree 1.

Thus we haven't made use of everything we know about the code. $W(x,y)$ must also be invariant under the transformation

$$\text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } B \begin{pmatrix} x \\ y \end{pmatrix} ,$$

where

$$B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I .$$

This rules out terms of odd degree. So $W(x,y)$ is now invariant under the group $\mathcal{G}_3$ generated by A and B, which consists of I, A, $-I$, $-A$. The reader can easily work out that the

new Molien series is

$$\begin{aligned}\Phi_{\mathcal{G}_3}(\lambda) &= \frac{1}{2}\{\Phi_{\mathcal{G}_2}(\lambda)+\Phi_{\mathcal{G}_2}(-\lambda)\} \\ &= \frac{1}{2}\left\{\frac{1}{(1-\lambda)(1-\lambda^2)}+\frac{1}{(1+\lambda)(1-\lambda^2)}\right\} \\ &= \frac{1}{(1-\lambda^2)^2}\ . \end{aligned} \tag{76}$$

There are now two basic invariants, both of degree 2 (matching the exponents in the denominator of (76)), say g^2 and h, or the equivalent and slightly simpler pair $g^* = x^2 + (q-1)y^2$ and $h = y(x-y)$. Hence:

Theorem 16. *The Hamming weight enumerator of any Hermitian self-dual code over $\mathbb{F}_q$ is a polynomial in g^* and h.*

The general plan of attack. As these examples have illustrated, there are two stages in using invariant theory to solve a problem.

Stage I. Convert the assumptions about the problem (e.g. the code) into algebraic constraints on polynomials (e.g. weight enumerators).

Stage II. Use the invariant theory to find all possible polynomials satisfying these constraints.

6.2. The basic theorems of invariant theory

Groups of matrices. Given a collection $A_1, \ldots, A_r$ of $m \times m$ invertible matrices, we can form a group $\mathcal{G}$ from them by multiplying them together in all possible ways. Thus $\mathcal{G}$ contains the matrices I, $A_1, A_2, \ldots, A_1A_2, \ldots, A_2A_1^{-1}A_2^{-1}A_3, \ldots$. We say that $\mathcal{G}$ is *generated* by $A_1, \ldots, A_r$. We will suppose that $\mathcal{G}$ is finite, which covers all the cases encountered in this chapter. (For infinite groups, see for example Dieudonné and Carroll [79], Rallis [257], Springer [294], Sturmfels [298], Weyl [326].)

Example. Let us show that the group $\mathcal{G}_1$ generated by the matrices

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \quad \text{and} \quad J = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$$

that was encountered in Section 6.1 does indeed have order 192. The key is to discover (by randomly multiplying matrices together) that $\mathcal{G}_1$ contains

$$J^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad E = (MJ)^3 = \tfrac{1+i}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$E^2 = i \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad R = MJ^2M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

So $\mathcal{G}_1$ contains the matrices

$$\alpha \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \alpha \begin{pmatrix} 0 & 1 \\ \pm 1 & 0 \end{pmatrix}, \quad \alpha \in \{1, i, -1, -i\},$$

which form a subgroup $\mathcal{H}_1$ of order 16. From this it is easy to see that $\mathcal{G}_1$ consists of the union of 12 cosets of $\mathcal{H}_1$:

$$\mathcal{G}_1 = \bigcup_{k=1}^{12} a_k \mathcal{H}_1 , \tag{77}$$

where $a_1, \ldots, a_6$ are respectively

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix},$$

$a_7 = \eta a_1, \ldots, a_{12} = \eta a_6$, and $\eta = (1+i)/\sqrt{2}$, an 8th root of unity. Thus $\mathcal{G}_1$ consists of the 192 matrices

$$\eta^\nu \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}, \ \eta^\nu \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}, \ \eta^\nu \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \beta \\ \alpha & -\alpha\beta \end{pmatrix}, \tag{78}$$

for $0 \le \nu \le 7$ and $\alpha, \beta \in \{1, i, -1, -i\}$.

As a check, one verifies that every matrix in (78) can be written as a product of M's and J's; that the product of two matrices in (78) is again in (78); and that the inverse of every matrix in (78) is in (78). Therefore (78) *is* a group, and is the group generated by M and J. Thus $\mathcal{G}_1$ is indeed equal to (78).

We have gone into this example in some detail to emphasize that it is important to begin by understanding the group thoroughly. (For an alternative way of studying $\mathcal{G}_1$, see [33, pp. 160–161].

Invariants. To quote Hermann Weyl [325], "the theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head." Invariant theory became one of the main branches of nineteenth century mathematics, but dropped out of fashion after Hilbert's work: see Fisher [96] and Reid [261]. In the past thirty years, however,

there has been a resurgence of interest, with applications in algebraic geometry (Dieudonné and Carroll [79], Mumford and Fogarty [205]), physics (see for example Agrawala and Belinfante [1] and the references given there), combinatorics (Doubilet et al. [80], Rota [262], Stanley [296]) and coding theory ([188], [195], [197], [198]). Recently a number of monographs (Benson [13], Bruns and Herzog [36], Smith [289], Springer [294], Sturmfels [298]) and conference proceedings ([100], [104], [172], [297]) on invariant theory have appeared.

There are several different kinds of invariants, but here an invariant is defined as follows.

Let $\mathcal{G}$ be a group of g $m \times m$ complex matrices $A_1, \ldots, A_g$, where the $(i,k)^{\text{th}}$ entry of A_α is $a_{ik}^{(\alpha)}$. In other words $\mathcal{G}$ is a group of linear transformations on the variables $x_1, \ldots, x_m$, consisting of the transformations

$$T^{(\alpha)} : \text{replace } x_i \text{ by } x_i^{(\alpha)} = \sum_{k=1}^{m} a_{ik}^{(\alpha)} x_k, \quad i = 1, \ldots, m \tag{79}$$

for $\alpha = 1, 2, \ldots, g$. It is worthwhile giving a careful description of how a polynomial $f(\mathbf{x}) = f(x_1, \ldots, x_m)$ is transformed by a matrix A_α in $\mathcal{G}$. The transformed polynomial is

$$A_\alpha \circ f(\mathbf{x}) = f(x_1^{(\alpha)}, \ldots, x_m^{(\alpha)})$$

where each $x_i^{(\alpha)}$ is replaced by $\sum_{k=1}^{m} a_{ik}^{(\alpha)} x_k$. Another way of describing this is to think of $\mathbf{x} = (x_1, \ldots, x_m)^T$ as a column vector. Then $f(\mathbf{x})$ is transformed into

$$A_\alpha \circ f(\mathbf{x}) = f(A_\alpha \mathbf{x}) \ , \tag{80}$$

where $A_\alpha \mathbf{x}$ is the usual product of a matrix and a vector. One can check that

$$B \circ (A \circ f(\mathbf{x})) = (AB) \circ f(\mathbf{x}) = f(AB\mathbf{x}) \ . \tag{81}$$

For example,

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$$

transforms $x_1^2 + x_2$ into $(x_1 + 2x_2)^2 - x_2$.

Definition. An *invariant* of $\mathcal{G}$ is a polynomial $f(\mathbf{x})$ which is unchanged by every linear transformation in $\mathcal{G}$. In other words, $f(\mathbf{x})$ is an invariant of $\mathcal{G}$ if

$$A_\alpha \circ f(\mathbf{x}) = f(A_\alpha \mathbf{x}) = f(\mathbf{x}) \tag{82}$$

for all $\alpha = 1, \ldots, g$.

Example. Let

$$\mathcal{G}_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\} ,$$

a group of order $g = 2$. Then x^2, xy and y^2 are homogeneous invariants of degree 2.

Even if $f(x)$ isn't an invariant, its average over the group,

$$\overline{f}(\mathbf{x}) = \frac{1}{g} \sum_{\alpha=1}^{g} A_\alpha \circ f(\mathbf{x}) \tag{83}$$

is, as was already stated in Theorem 14. To prove this, observe that any $A_\beta \in \mathcal{G}$ transforms the right-hand side of (83) into

$$\frac{1}{g} \sum_{\alpha=1}^{g} (A_\alpha A_\beta) \circ f(\mathbf{x}) , \tag{84}$$

by (81). As A_α runs through $\mathcal{G}$, so does $A_\alpha A_\beta$, if A_β is fixed. Therefore (84) is equal to

$$\frac{1}{g} \sum_{\gamma=1}^{g} A_\gamma \circ f(\mathbf{x}) ,$$

which is $\overline{f}(\mathbf{x})$. Therefore $\overline{f}(\mathbf{x})$ is an invariant. ∎

More generally, any symmetric function of the g polynomials $A_1 \circ f(\mathbf{x}), \ldots, A_g \circ f(\mathbf{x})$ is an invariant of $\mathcal{G}$.

Clearly, if $f(\mathbf{x})$ and $h(\mathbf{x})$ are invariants of $\mathcal{G}$, so are $f(\mathbf{x}) + h(\mathbf{x})$, $f(\mathbf{x})h(\mathbf{x})$, and $cf(\mathbf{x})$ (c complex); or in other words the set of invariants of $\mathcal{G}$, which we denote by $\mathcal{J}(\mathcal{G})$, forms a ring.

One of the main problems of invariant theory is to describe $\mathcal{J}(\mathcal{G})$. Since the transformations in $\mathcal{G}$ do not change the degree of a polynomial, it is enough to describe the homogeneous invariants (for any invariant is a sum of homogeneous invariants).

Basic invariants. Our goal is to find a "basis" for the invariants of $\mathcal{G}$, that is, a set of basic invariants such that any invariant can be expressed in terms of this set. There are two different types of bases one might look for

Definition. Polynomials $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ are called *algebraically dependent* if there is a polynomial p in r variables with complex coefficients, not all zero, such that $p(f_1(\mathbf{x}), \ldots, f_r(\mathbf{x}))$ is identically zero. Otherwise $f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})$ are *algebraically independent.* A fundamental result from algebra is (Jacobson [155], vol. 3, p. 154):

Theorem 17. *Any $m + 1$ polynomials in m variables are algebraically dependent.*

The first type of basis we might look for is a set of m algebraically independent invariants $f_1(\mathbf{x}), \ldots f_m(\mathbf{x})$. Such a set is indeed a "basis," for by Theorem 17 any invariant is algebraically dependent on $f_1, \ldots, f_m$ and so is a root of a polynomial equation in $f_1, \ldots, f_m$. The following theorem guarantees the existence of such a basis.

Theorem 18. [37, p. 357] *There always exist m algebraically independent invariants of $\mathcal{G}$.*

Proof. Consider the polynomial

$$\prod_{\alpha=1}^{g} (t - A_\alpha \circ x_i)$$

in the variables $t, x_1, \ldots, x_m$. Since one of the A_α is the identity matrix, $t = x_1$ is a zero of this polynomial. When the polynomial is expanded in powers of t, the coefficients are invariants, by the remark immediately following the proof of Theorem 14. Therefore x_1 is an algebraic function of invariants. Similarly each of $x_2, \ldots, x_m$ is an algebraic function of invariants. Now if the number of algebraically independent invariants were m' $(< m)$, the m independent variables $x_1, \ldots, x_m$ would be algebraic functions of the m' invariants, a contradiction. Therefore the number of algebraically independent invariants is at least m. But by Theorem 17 this number cannot be greater than m. ∎

Example. For the preceding group $\mathcal{G}_4$, we may take $f_1 = (x+y)^2$ and $f_2 = (x-y)^2$ as the algebraically independent invariants. Then any invariant is a root of a polynomial equation in f_1 and f_2. For example,

$$\begin{aligned} x^2 &= \tfrac{1}{4}\left(\sqrt{f_1} + \sqrt{f_2}\right)^2 , \\ xy &= \tfrac{1}{4}(f_1 - f_2) , \end{aligned}$$

and so on.

However, by far the most convenient description of the invariants is a set $f_1, \ldots, f_l$ of invariants with the property that any invariant is a *polynomial* in $f_1, \ldots, f_l$. Then $f_1, \ldots, f_l$ is called a *polynomial basis* (or an *integrity basis*) for the invariants of $\mathcal{G}$. Of course if $l > m$ then by Theorem 17 there will be polynomial equations, called *syzygies*, relating $f_1, \ldots, f_l$.

For example, $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$ form a polynomial basis for the invariants of $\mathcal{G}_4$. The syzygy relating them is

$$f_1 f_2 - f_2^2 = 0 .$$

The existence of a polynomial basis, and a method of finding it, is given by the next theorem.

Theorem 19. (Noether [206]; [326, p. 275].) *The ring of invariants of a finite group $\mathcal{G}$ of complex $m \times m$ matrices has a polynomial basis consisting of not more than $\binom{m+g}{m}$ invariants, of degree not exceeding g, where g is the order of $\mathcal{G}$. Furthermore this basis may be obtained by taking the average over $\mathcal{G}$ of all monomials*

$$x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m}$$

of total degree $\sum b_i$ not exceeding g.

Proof. Let the group $\mathcal{G}$ consist of the transformations (79). Suppose

$$f(x_1, \ldots, x_m) = \sum_e c_e x_1^{e_1} \cdots x_m^{e_m} \ ,$$

c_e complex, is any invariant of $\mathcal{G}$. (The sum extends over all $e = e_1 \cdots e_m$ for which there is nonzero term $x_1^{e_1} \cdots x_m^{e_m}$ in $f(x_1, \ldots, x_m)$.) Since $f(x_1, \ldots, x_m)$ is an invariant, it is unchanged when we average it over the group, so

$$\begin{aligned} f(x_1, \ldots, x_m) &= \frac{1}{g}\{f(x_1^{(1)}, \ldots, x_m^{(1)}) + \cdots + f(x_1^{(g)}, \ldots, x_m^{(g)})\} \\ &= \frac{1}{g} \sum_e c_e \{(x_1^{(1)})^{e_1} \cdots (x_m^{(1)})^{e_m} + \cdots + (x_1^{(g)})^{e_1} \cdots (x_m^{(g)})^{e_m}\} \\ &= \frac{1}{g} \sum_e c_e J_e \quad \text{(say)} \ . \end{aligned}$$

Every invariant is therefore a linear combination of the (infinitely many) special invariants

$$J_e = \sum_{\alpha=1}^{g} (x_1^{(\alpha)})^{e_1} \cdots (x_m^{(\alpha)})^{e_m} \ .$$

Now J_e is (apart from a constant factor) the coefficient of $u_1^{e_1} \cdots u_m^{e_m}$ in

$$P_e = \sum_{\alpha=1}^{g} (u_1 x_1^{(\alpha)} + \cdots + u_m x_m^{(\alpha)})^e \ , \tag{85}$$

where $e = e_1 + \cdots + e_m$. In other words, the P_e are the power sums of the g quantities

$$u_1 x_1^{(1)} + \cdots + u_m x_m^{(1)}, \ldots, u_1 x_1^{(g)} + \cdots + u_m x_m^{(g)} \ .$$

Any power sum P_e, $e = 1, 2, \ldots$, can be written as a polynomial with rational coefficients in the first g power sums P_1, $P_2, \ldots, P_g$. Therefore any J_e for

$$e = \sum_{i=1}^{m} e_i > g$$

(which is a coefficient of P_e) can be written as a polynomial in the special invariants

$$J_e \quad \text{with} \quad e_1 + \cdots + e_m \le g$$

(which are the coefficients of $P_1, \ldots, P_g$). Thus any invariant can be written as a polynomial in those J_e with $\sum_{i=1}^m e_i \le g$. The number of such J_e is the number of e_1, $e_2, \ldots, e_m$ with $e_i \ge 0$ and $e_1 + \cdots + e_m \le g$, which is $\binom{m+g}{m}$. Finally, $\deg J_e \le g$, and J_e is obtained by averaging $x_1^{e_1} \cdots x_m^{e_m}$ over the group. ∎

Molien's theorem. Since we know from Theorem 19 that a polynomial basis always exists, we can go ahead with confidence and try to find it, using the methods described in Section 6.1. To discover when a basis has been found, we use Molien's theorem (Theorem 10). This states that if a_d is the number of linearly independent homogeneous invariants of $\mathcal{G}$ with degree d, and

$$\Phi_{\mathcal{G}}(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d \ ,$$

then

$$\Phi_{\mathcal{G}}(\lambda) = \frac{1}{g} \sum_{\alpha=1}^{g} \frac{1}{\det(I - \lambda A_\alpha)} \ . \tag{86}$$

The proof depends on the following theorem.

Theorem 20. [200, p. 258], [277, p. 17] *The number of linearly independent invariants of $\mathcal{G}$ of degree 1 is*

$$a_1 = \frac{1}{g} \sum_{\alpha=1}^{g} \operatorname{trace}(A_\alpha) \ .$$

Proof. Let

$$S = \frac{1}{g} \sum_{\alpha=1}^{g} A_\alpha \ .$$

Changing the variables on which $\mathcal{G}$ acts from $x_1, \ldots, x_m$ to $y_1, \ldots, y_m$, where $(y_1, \ldots, y_m) = (x_1, \ldots, x_m)T^{tr}$, changes S to $S' = TST^{-1}$. We may choose T so that S' is diagonal (see [37, p. 252]). Now $S^2 = S$, $(S')^2 = S'$, hence the diagonal entries of S' are 0 or 1. So with a change of variables we may assume

$$S = \begin{bmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{bmatrix}$$

with say r 1's on the diagonal. Thus $S \circ y_i = y_i$ if $1 \le i \le r$, $S \circ y_i = 0$ if $r+1 \le i \le m$.

Any linear invariant of $\mathcal{G}$ is certainly fixed by S, so $a_1 \le r$. On the other hand, by Theorem 14,

$$S \circ y_i = \frac{1}{g} \sum_{\alpha=1}^{g} A_\alpha \circ y_i$$

is an invariant of $\mathcal{G}$ for any i, and so $a_1 \ge r$. ∎

Before proving Theorem 10 let us introduce some more notation. Equation (79) describes how A_α transforms the variables $x_1, \ldots, x_m$. The d^{th} *induced matrix*, denoted by $A_\alpha^{[d]}$, describes how A_α transforms the products of the x_i taken d at a time, namely $x_1^d, x_2^d, \ldots, x_1^{d-1}x_2, \ldots$ (Littlewood [183, p. 122]). E.g.

$$A_\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

transforms x_1^2, x_1x_2 and x_2^2 into

$$\begin{aligned} &a^2x_1^2 + 2abx_1x_2 + b^2x_2^2 \ , \\ &acx_1^2 + (ad+bc)x_1x_2 + bdx_2^2 \ , \\ &c^2x_1^2 + 2cdx_1x_2 + d^2x_2^2 \end{aligned}$$

respectively. Thus the 2^{nd} induced matrix is

$$A_\alpha^{[2]} = \begin{bmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{bmatrix} \ ,$$

Proof of Theorem 10. To prove (86), note that a_d is equal to the number of linearly independent invariants of degree 1 of $\mathcal{G}^{[d]} = \{A_\alpha^{[d]} : \alpha = 1, \ldots, g\}$. By Theorem 20,

$$a_d = \frac{1}{g} \sum_{\alpha=1}^{g} \text{trace } A_\alpha^{[d]} \ .$$

Therefore, to prove Theorem 10, it is enough to show that the trace of $A_\alpha^{[d]}$ is equal to the coefficient of λ^d in

$$\frac{1}{\det(I - \lambda A_\alpha)} = \frac{1}{(1-\lambda\omega_1)\cdots(1-\lambda\omega_m)} \ , \tag{87}$$

where $\omega_1, \ldots, \omega_m$ are the eigenvalues of A_α. By a suitable change of variables we can make

$$A_\alpha = \begin{bmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_m \end{bmatrix}, \quad A_\alpha^{[d]} = \begin{bmatrix} \omega_1^d & & & 0 & \\ & \omega_2^d & & & \\ & & \ddots & & \\ & & & \omega_1^{d-1}\omega_2 & \\ & 0 & & & \ddots \end{bmatrix} \ ,$$

and trace $A_\alpha^{[d]}$ = sum of the products of $\omega_1, \ldots, \omega_m$ taken d at a time. But this is exactly the coefficient of λ^d in the expansion of (87). ∎

It is worth remarking that the Molien series does not determine the group. For example there are two groups of 2×2 matrices of order 8 having

$$\Phi(\lambda) = \frac{1}{(1-\lambda^2)(1-\lambda^4)}$$

(namely the dihedral group D_8 and the abelian group $Z(2) \times Z(4)$). In fact there exist abstract groups $\mathcal{A}$ and $\mathcal{B}$ whose matrix representations can be paired in such a way that every representation of $\mathcal{A}$ has the same Molien series as the corresponding representation of $\mathcal{B}$ (Dade [75]).

A standard form for the basic invariants. The following notation is very useful in describing the ring $\mathcal{J}(\mathcal{G})$ of invariants of a group $\mathcal{G}$. The complex numbers are denoted by $\mathbb{C}$, and if $p(\mathbf{x})$, $q(\mathbf{x}), \ldots$ are polynomials, $\mathbb{C}[p(\mathbf{x}), q(\mathbf{x}), \ldots]$ denotes the set of all polynomials in $p(\mathbf{x}), q(\mathbf{x}), \ldots$ with complex coefficients. For example Theorem 11 just says that $\mathcal{J}(\mathcal{G}_1) = \mathbb{C}[\phi_8, \phi'_{24}]$.

Also, $\oplus$ will denote the usual direct sum operation. For example a statement like $\mathcal{J}(\mathcal{G}) = R \oplus S$ means that every invariant of $\mathcal{G}$ can be written uniquely in the form $r + s$ where $r \in R$, $s \in S$.

Using this notation we can now specify the most convenient form of polynomial basis for $\mathcal{J}(\mathcal{G})$.

Definition. A *good polynomial basis* for $\mathcal{J}(\mathcal{G})$ consists of homogeneous invariants $f_1, \ldots, f_l$ ($l \geq m$) where $f_1, \ldots, f_m$ are algebraically independent and

$$\mathcal{J}(\mathcal{G}) = \mathbb{C}[f_1, \ldots, f_m] \quad \text{if} \quad l = m \ , \tag{88}$$

or, if $l > m$,

$$\mathcal{J}(\mathcal{G}) = \mathbb{C}[f_1, \ldots, f_m] \oplus f_{m+1}\mathbb{C}[f_1, \ldots, f_m] \oplus \cdots \oplus f_l\mathbb{C}[f_1, \ldots, f_m] \ . \tag{89}$$

In words, this says that any invariant of $\mathcal{G}$ can be written as a polynomial in $f_1, \ldots, f_m$ (if $l = m$), or as such a polynomial plus f_{m+1} times another such polynomial plus $\cdots$ (if $l > m$). $f_1, \ldots, f_m$ are called *primary* invariants and $f_{m+1}, \ldots, f_l$ (if present) are *secondary* invariants.

Speaking loosely, (88) and (89) say that when describing an arbitrary invariant, $f_1, \ldots, f_m$ are "free" and can be used as often as needed, while $f_{m+1}, \ldots, f_l$ are "transients" and can each be used at most once. Equations (88) and (89) are sometimes called a *Hironaka decomposition* of $\mathcal{J}(\mathcal{G})$ ([298], p. 39).

For a good polynomial basis $f_1, \ldots, f_l$ we can say exactly what form the syzygies must take. If $l = m$ there are no syzygies. If $l > m$ there are $\binom{l-m+1}{2}$ syzygies expressing the products $f_i f_j$ $(m+1 \le i \le j \le l)$ in terms of $f_1, \ldots, f_l$.

It is important to note that the Molien series can be written down by inspection from the degrees of a good polynomial basis. Let $d_1 = \deg f_1, \ldots, d_l = \deg f_l$. Then

$$\Phi_{\mathcal{G}}(\lambda) = \frac{1}{\prod_{i=1}^{m}(1-\lambda^{d_i})}, \quad \text{if} \quad l = m \ , \tag{90}$$

or

$$\Phi_{\mathcal{G}}(\lambda) = \frac{1 + \sum_{j=l+1}^{m} \lambda^{d_j}}{\prod_{i=1}^{m}(1-\lambda^{d_i})}, \quad \text{if} \quad l > m \ . \tag{91}$$

(This is easily verified by expanding (90) and (91) in powers of λ and comparing with (88) and (89).)

Some examples will make this clear.

(1) For the group $\mathcal{G}_1$ of Section 6.1, $f_1 = \phi_8$ and $f_2 = \phi'_{24}$ form a good polynomial basis, with degrees $d_1 = 8$, $d_2 = 24$. Indeed, from Theorem 11 and (61),

$$\mathcal{J}(\mathcal{G}_1) = \mathbb{C}[\phi_8, \phi'_{24}]$$

and

$$\Phi_{\mathcal{G}_1}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \ .$$

(2) For the group $\mathcal{G}_4$ defined above, $f_1 = x^2$, $f_2 = y^2$, $f_3 = xy$ is a good polynomial basis, with $d_1 = d_2 = d_3 = 2$. The invariants can be described as

$$\mathcal{J}(\mathcal{G}_4) = \mathbb{C}[x^2, y^2] \oplus xy\mathbb{C}[x^2, y^2] \ . \tag{92}$$

In words, any invariant can be written uniquely as a polynomial in x^2 and y^2 plus xy times another such polynomial. E.g.

$$(x+y)^4 = (x^2)^2 + 6x^2y^2 + (y^2)^2 + xy(4x^2 + 4y^2) \ .$$

The Molien series is

$$\Phi_{\mathcal{G}_4}(\lambda) = \frac{1}{2}\left\{\frac{1}{(1-\lambda)^2} + \frac{1}{(1+\lambda)^2}\right\} = \frac{1+\lambda^2}{(1-\lambda^2)^2}$$

in agreement with (91) and (92). The single syzygy is $x^2 \cdot y^2 = (xy)^2$. Note that $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$ is not a good polynomial basis, for the invariant y^4 is not in the ring $\mathbb{C}[x^2, xy] \oplus y^2\mathbb{C}[x^2, xy]$.

Fortunately the following result holds.

Theorem 21. (Hochster and Eagon [133, Proposition 13]) *A good polynomial basis exists for the invariants of any finite group of complex $m \times m$ matrices.*

For the proof see [13], [36], [133] or [289].

So we know that for any group the Molien series can be put into the standard form of (90), (91) (with denominator consisting of a product of m factors $(1 - \lambda^{d_i})$ and numerator consisting of sum of powers of λ with positive coefficients); and that a good polynomial basis (88), (89) can be found whose degrees match the powers of λ occurring in the standard form of the Molien series.

On the other hand the converse is not true. It is not always true that when the Molien series has been put into the form (90), (91) (by cancelling common factors and multiplying top and bottom by new factors), then a good polynomial basis for $\mathcal{J}(\mathcal{G})$ can be found whose degrees match the powers of λ in $\Phi(\lambda)$. This is shown by the following example, due to Stanley [295].

Let $\mathcal{G}_6$ be the group of order 8 generated by the matrices $\mathrm{diag}\{-1, -1, -1\}$ and $\mathrm{diag}\{1, 1, i\}$. The Molien series is

$$\Phi_{\mathcal{G}_6}(\lambda) = \frac{1}{(1-\lambda^2)^3} \tag{93}$$

$$= \frac{1+\lambda^2}{(1-\lambda^2)^2(1-\lambda^4)} \ . \tag{94}$$

A good polynomial basis exists corresponding to (94), namely

$$\mathcal{J}(\mathcal{G}_6) = \mathbb{C}[x^2, y^2, z^4] \oplus xy\mathbb{C}[x^2, y^2, z^4] \ ,$$

but there is no good polynomial basis corresponding to (93).

Remarks. (1) Shephard and Todd [279] have characterized those groups for which (88) holds, i.e. for which a good polynomial basis exists consisting only of algebraically independent invariants. These are the groups known as "unitary groups generated by reflections." A complete list of the 37 irreducible groups (or families of groups) of this type is given in [279] and [289], p. 199.

(2) Sturmfels [298] gives an algorithm for computing a good polynomial basis for the ring of invariants of a finite group. The computer language MAGMA ([28], [29], [30]) has commands for computing Molien series and finding a good polynomial basis (and many other things).

(3) **Relative invariants.** If χ is a homomorphism from $\mathcal{G}$ into the multiplicative group of the complex numbers (i.e. a *linear character* of $\mathcal{G}$), then a polynomial $f(\mathbf{x})$ is called a *relative invariant* of $\mathcal{G}$ with respect to χ if

$$A \circ f(\mathbf{x}) = \chi(A) f(\mathbf{x}) \quad \text{for all} \quad A \in \mathcal{G} \ .$$

Molien's theorem for relative invariants states that the number of linearly independent homogeneous relative invariants with respect to χ of degree ν is the coefficient of λ^ν in the expansion of

$$\frac{1}{|\mathcal{G}|} \sum_{A \in \mathcal{G}} \frac{\overline{\chi}(A)}{\det |I - \lambda A|} \ .$$

7. Gleason's theorem and generalizations

We now make use of the machinery developed in the previous section to give a series of results that characterize the rings to which the various weight enumerators of self-dual codes belong. The first theorems of this type, for binary and ternary codes, were discovered by Gleason [105]. The results can be proved by the generalizations of the arguments used to establish Theorem 13. We remind the reader that *hwe*, *swe* and *cwe* stand for Hamming, symmetrized and complete weight enumerators, respectively. The code under consideration is denoted by C and its shadow by S.

In each case the conclusion is that the weight enumerator being considered must be an element of a certain ring R. We describe R by giving its *Molien series* (also called a *Hilbert series* or *Poincaré series*)

$$\Phi(\lambda) = \sum_{n=0}^{\infty} (\dim_{\mathbb{C}} R_n) \lambda^n \ ,$$

where R_n is the subspace of homogeneous polynomials in R of degree n. We then give a good polynomial basis for R (in the sense of (88), (88)).

In many cases R is obtained (as described in the previous sections) as the ring of invariants of a certain matrix group G. If so then we start by giving generators for G, its order, and, if it is a well-known group, a brief description. We have preferred to give natural generators for G, rather than attempting to find a minimal but less-intuitive set — in most cases two generators

would suffice. If G is a reflection group we give its number in Shephard and Todd's list ([279]; [289], page 199).

In other cases (the symmetrized weight enumerator of a Hermitian self-dual code over $\mathbb{F}_4$, (108), for example) the ring R cannot be found directly as the ring of invariants of any group, but must be obtained by collapsing the ring of complete weight enumerators.

At the end of each subsection is a table that gives, for most of the rings mentioned, a list of codes whose weight enumerators provide a polynomial basis for the ring. The weight enumerators of the codes before the semicolon are primary invariants, those after the semicolon (if present) are secondary invariants.

For example, the first line of Table (100) is equivalent to Theorem 13.

7.1. Family $2_{\rm I}$: Binary self-dual codes

hwe of code C. ([105], [14], [33], [188]) $G = G_{16} = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \cong$ dihedral group D_{16} (Shephard and Todd #2b), order 16

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^8)}$$

$$R : \frac{1}{\phi_2,\ \theta_8}\ , \tag{95}$$

where $\phi_2 = x^2 + y^2$, $\theta_8 = x^2y^2(x^2 - y^2)^2$. For example, since a Type II code is also a Type I code, the weight enumerator of g_{24}, (29), must be in this ring. It is:

$$\phi_{24} = \phi_2^{12} - 12\phi_2^8\theta_8 + 6\phi_2^4\theta_8^2 - 64\theta_8^2\ .$$

hwe of shadow S. It follows from Theorem 6 that if C has weight enumerator $W(x, y)$ then its shadow has weight enumerator $S(x, y) = W((x + y)/\sqrt{2}, i(x - y)/\sqrt{2})$. This map from W to S preserves multiplication and addition, so to evaluate it it suffices to consider the images of the generators of the above ring. We find that $x^2 + y^2$ becomes $2xy$ and $x^2y^2(x^2 - y^2)^2$ becomes $-4(x^4 - y^4)^2$. So $S(x, y)$ belongs to the ring

$$R : \frac{1}{xy,\ (x^4 - y^4)^2}\ . \tag{96}$$

In particular, every element of the shadow has weight congruent to $n/2$ mod 4 (since this is true of the generators).

The shadow must satisfy an additional constraint. If C is Type I, let $W^{(j)}(x, y)$ be the weight enumerator of coset C_j, $j = 0, \ldots, 3$ (see (56)). Then $W^{(1)}(x, y) - W^{(3)}(x, y)$ is (up to

sign) a multiplicative function on codes, i.e., if C is the direct sum of two Type I codes C' and C'', then $W^{(1)} - W^{(3)}$ for C is ± 1 times the product of the polynomials $W^{(1)} - W^{(3)}$ for C' and C''. In order for this property to still hold when one (or both) of C' and C'' is of Type II, we adopt the convention that for a Type II code, $W^{(1)} - W^{(3)}$ is simply the weight enumerator of the code.

Then the additional condition satisfied by the shadow is that (if C is Type I *or* Type II) $W^{(1)}(x,y) - W^{(3)}(x,y)$ is a relative invariant for the group G_{192} (see (98)) with respect to the character

$$\chi\left(\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right) = i^n, \quad \chi\left(\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\right) = \eta^n$$

where $\eta = (1+i)/\sqrt{2}$ [69]. An equivalent assertion is that $W^{(1)} - W^{(3)}$ is an absolute invariant for the subgroup of G_{192} with determinant 1.

It follows (see [69] for the proof) that for a Type I code $W^{(1)}(x,y) - W^{(3)}(x,y)$ lies in the following ring:

$$\Phi = \frac{1+\lambda^{18}}{(1-\lambda^8)(1-\lambda^{12})}$$
$$R : \frac{1,\ xy(x^8-y^8)(x^8-34x^4y^4+y^8)}{x^8+14x^4y^4+y^8,\ x^2y^2(x^4-y^4)^2}\ . \tag{97}$$

One of the differences between binary codes of Types I and II is that whereas the weight enumerator of the former is invariant under a group of order only 16, the weight enumerator of the latter is invariant under a group of order 192 (see Eq. (98)). The above result restores the balance to a certain extent, by requiring $W^{(1)} - W^{(3)}$ to be a relative invariant for the larger group.

7.2. Family $2_{\rm II}$: Doubly-even binary self-dual codes

hwe of C ([105], [14], [33], [188])

$$G = G_{192} = \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}\right\rangle\ , \quad \text{order } 192 \tag{98}$$

(Shephard and Todd #9)

$$\Phi = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}$$
$$R : \frac{1}{x^8+14x^4y^4+y^8,\ x^4y^4(x^4-y^4)^4}\ . \tag{99}$$

Codes whose weight enumerators give generators for the above rings:

Ring	Codes
(95)	i_2 (25), e_8 (26)
(96)	i_2 (25), e_8 (26)
(97)	e_8 (26), g_{24} (29); d_{12}^+, $(d_{10}e_7f_1)^+$ (§11.3)
(99)	e_8 (26), g_{24} (29)

(100)

Remark. The above groups G_{16} and G_{192} are also the two-dimensional real and complex Clifford groups occurring in quantum coding theory [48], [49]. At present this appears to be nothing more than a coincidence. However, in view of the other mysterious coincidences involving the Clifford groups, there may be a deeper explanation that is presently hidden (compare the remarks in Section 7.9).

7.3. Family 3: Ternary codes

hwe of C ([105]; [14], [188], [190, p. 620])

$$G = \left\langle \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}, \omega = e^{2\pi i/3} \right\rangle, \quad \text{order } 48$$

(Shephard & Todd #6)

$$\Phi = \frac{1}{(1-\lambda^4)(1-\lambda^{12})} \tag{101}$$

$$R : \frac{1}{x^4 + 8xy^3,\ y^3(x^3-y^3)^3} \tag{102}$$

cwe of C**,** $1^n \in C$ ([198]; [190, p. 617]) (This forces the length to be a multiple of 12.)

$$G = \left\langle \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \omega \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & \omega & \\ & & \omega \end{bmatrix} \right\rangle ,$$

order 2592,

$$\Phi = \frac{1+\lambda^{24}}{(1-\lambda^{12})^2(1-\lambda^{36})}$$

$$R : \frac{1,\ \beta_6\pi_9^2}{\alpha_{12},\ \beta_6^2,\ \pi_9^4} \tag{103}$$

where

$$a = x^3+y^3+z^3,\ b = x^3y^3+y^3z^3+z^3x^3,$$

$$p = 3xyz,\ \alpha_{12} = a(a^3+8p^3),$$

$$\beta_6 = a^{12} - 12b,\ \pi_9 = (x^3-y^3)(y^3-z^3)(z^3-x^3)\ .$$

cwe of C, not requiring that $1^n \in C$ [199] (Now the length is just a multiple of 4.)

$$G = \left\langle \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \omega \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & & \\ & \omega & \\ & & \omega \end{bmatrix} \right\rangle ,$$

order 96

$$\Phi = \frac{1 + 4\lambda^{12} + \lambda^{24}}{(1-\lambda^4)(1-\lambda^{12})^2} .$$

$$R : \sum_{i=0}^{6} f^{(i)} S$$

where $S = \mathbb{C}[\theta_4, \theta_6^2, t^{12}]$, $s = y + z$, $t = y - z$, $\theta_4 = x(x^3 + s^3)$, $\theta_6 = 8x^6 - 20x^3 s^3 - s^6$, $f^{(0)} = 1$, $f^{(1)} = t^2 \phi_4 \theta_6$, $\phi_4 = s(8x^3 - s^3)$, $f^{(2)} = t^4 \phi_4^2$, $f^{(3)} = t^6 \theta_6$, $f^{(4)} = t^8 \phi_4$, $f^{(5)} = t^{10} \phi_4^2 \theta_6$.

Codes:

Ring	Codes
(102)	t_4 (30), g_{12} (31)
(103)	e_3^{4+} (§11.4), g_{12} (31), $S(36)$ (§12.2); XQ_{23} (§12.2)

(104)

7.4. Family 4^{H}: Self-dual codes over $\mathbb{F}_4$ with Hermitian inner product

hwe of C ([188]; [190, p. 621]):

$$G = \left\langle \frac{1}{2} \begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle = \text{Weyl group of type } G_2 \cong \text{dihedral group } D_{12}$$

(Shephard & Todd #2b)

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^6)}$$

$$R : \frac{1}{x^2 + 3y^2,\ y^2(x^2 - y^2)^2} \tag{105}$$

cwe of C, $1^n \in C$ (There must be some word of full weight, so this is not a severe restriction)

$$G = \left\langle \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\rangle$$

order 576

$$\Phi = \frac{1 + \lambda^{12}}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \frac{1,\ (x^2-y^2)(x^2-z^2)(x^2-t^2)(y^2-z^2)(y^2-t^2)(z^2-t^2)}{x^2+y^2+z^2+t^2,\ (37),\ f_8,\ f_{12}} \tag{106}$$

where

$$\begin{aligned} f_8 &= x^8 + \cdots (4 \text{ terms}) + 14x^4y^4 + \cdots (6 \text{ terms}) + 168x^2y^2z^2t^2 = \text{cwe of } e_8 \otimes \mathbb{F}_4 \\ f_{12} &= (s_4 - 3x^2y^2 - 3z^2t^2)(s_4 - 3x^2z^2 - 3y^2t^2)(s_4 - 3x^2t^2 - 3y^2z^2) \ , \\ s_4 &= x^2y^2 + x^2z^2 + \cdots \ (6 \text{ terms}) \ . \end{aligned}$$

cwe of C, assuming $1^n \in C$ and C and $\overline{C}$ have same cwe:

$$\begin{aligned} G &= \text{previous } G \text{ together with } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\ &\cong \text{Weyl group of type } F_4 \text{ (Shephard \& Todd \#28), order 1152} \end{aligned}$$

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \frac{1}{x^2+y^2+z^2+t^2, \ (37), \ f_8, \ f_{12}} \tag{107}$$

swe of C, $1^n \in C$: (Set $t = z$ in cwe)

$$\Phi = \frac{1+\lambda^{12}}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^8)}$$

$$R : \frac{1, \{(x^2-z^2)(y^2-z^2)\}^3}{x^2+y^2+2z^2, \ (36), \ \{(x^2-z^2)(y^2-z^2)\}^2} \tag{108}$$

Remark. If we try to apply invariant theory directly to the swe, we are led to the group

$$G = \left\langle \frac{1}{2} \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ \begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \right\rangle$$

(Weyl group of type B_3, Shephard & Todd #2a) of order 48, with Molien series

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^6)} \ .$$

However, the invariant of degree 4 is

$$\delta_4 = (x^2-z^2)(y^2-z^2) \ ,$$

which cannot be obtained from the swe of any self-dual code of length 4. The ring of invariants here and the ring in (108) have the same quotient field. So there is no group whose ring of invariants is (108).

Codes:

Ring	Codes
(105)	i_2 (33), h_6 (35)
(106)	i_2 (33), h_6 (35), $e_8 \otimes \mathbb{F}_4$, $(e_7e_5)^+$ (§11.5); d'_{12}
(107)	i_2 (33), h_6 (35), $e_8 \otimes \mathbb{F}_4$, $(e_7e_5)^+$ (§11.5)
(108)	i_2 (33), h_6 (35), $e_8 \otimes \mathbb{F}_4$; $(e_7e_5)^+$ (§11.5)

(109)

Here d'_{12} is the code obtained from d^+_{12} of Section 11.3 by multiplying the last four coordinates by ω.

7.5. Family 4^{E}: Self-dual codes over $\mathbb{F}_4$ with Euclidean inner product

(This is inadequately treated in [189], where only even codes are considered.) Neither the hwe nor the swe can be obtained directly from invariant theory, but must be obtained by collapsing the cwe. Since $(v,v) = 0 \Leftrightarrow \sum v_i^2 = 0 \Leftrightarrow \sum v_i = 0 \Leftrightarrow (v, 1^n) = 0$, we may assume $1^n \in C$.

cwe of C

$$G = \left\langle \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right\rangle$$

order 192

$$\Phi = \frac{1+\lambda^{16}}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^6)(1-\lambda^8)}$$
$$R : \frac{1,\ abcd(a^2-b^2)(a^2-c^2)\cdots(c^2-d^2)}{\text{symmetric polynomials in } a^2,b^2,c^2,d^2} \tag{110}$$

where

$$a = (+x-y-z-t)/2, \qquad b = (-x+y-z-t)/2\ ,$$
$$c = (-x-y+z-t)/2, \qquad d = (-x-y-z+t)/2\ .$$

cwe of C, assuming $\overline{C}$ has same cwe as C:

$$G = \text{previous group together with } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

(Weyl group of type B_4, Shephard & Todd #2a), order 384

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^6)(1-\lambda^8)}$$
$$R : \text{symmetric polynomials in } a^2,b^2,c^2,d^2\ . \tag{111}$$

swe of C: (Set $t = z$ in the above cwe)

$$\Phi = \frac{1 + \lambda^8 + \lambda^{16}}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^6)}$$

$$R : \frac{1,\ \{(x^2-z^2)(y^2-z^2)\}^2,\ \{(x^2-z^2)(y^2-z^2)\}^4}{x^2+y^2+2z^2,\ x^4+y^4+2z^4+12xyz^2,\ z^2(x-y)^2(xy-z^2)}\ . \tag{112}$$

hwe of C: (Set $t = z = y$ in the cwe)

$$\Phi = \frac{1 + \lambda^6}{(1-\lambda^2)(1-\lambda^4)}$$

$$R : \frac{1,\ y^2(x^2-y^2)^2}{x^2+3y^2,\ y^2(x-y)^2}\ . \tag{113}$$

Rather surprisingly, (110), (112), (113) appear to be new.

Codes: The following codes will be used:

$$\begin{aligned}
&i_2 = [11],\quad cwe = x^2+y^2+z^2+t^2,\ swe = x^2+y^2+2z^2,\quad hwe = x^2+3y^2\\
&c_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \overline{\omega} \end{bmatrix},\ \text{a [4,2,3] Reed-Solomon code,}\\
&\quad cwe = x^4+y^4+z^4+t^4+12xyzt,\ swe = x^4+y^4+2z^4+12xyz^2,\\
&\quad hwe = x^4+12xy^3+3y^4\ .\\
&c_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & \omega & \overline{\omega} \\ 1 & \omega & \overline{\omega} & 0 & 0 & 0 \end{bmatrix},\\
&\quad cwe = x^6+\cdots(4\text{ terms})+6x^3yzt+\cdots(4\text{ terms})+9x^2y^2z^2+\cdots(4\text{ terms}),\\
&\quad hwe = x^6+6x^3y^3+27x^2y^4+18xy^5+12y^6\ .
\end{aligned} \tag{114}$$

Codes:

Ring	Codes
(110)	$i_2, c_4, c_6, e_8 \otimes \mathbb{F}_4; ?$
(111)	$i_2, c_4, c_6, e_8 \otimes \mathbb{F}_4$
(112)	$i_2, c_4, c_6; e_8 \otimes \mathbb{F}_4$
(113)	$i_2, c_4; c_6$

(115)

Remark. The question mark in the first line of the table indicates that we do not have a code that produces the degree 16 polynomial in the numerator of (110). Such a code would necessarily be odd and have the property that the cwe of $\overline{C}$ is not equal to that of C. Presumably a random self-dual code would do, but we would prefer to find a code with some nice structure.

7.6. Family $4_{\rm I}^{\rm H+}$: Additive self-dual codes over $\mathbb{F}_4$ using trace inner product

hwe of C:

$$G = \left\langle \frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix} \right\rangle , \quad \text{order } 2$$

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^2)}$$

$$R : \frac{1}{x+y,\ y(x-y)} \tag{116}$$

cwe of C, $1^n \in C$:

$$G = \left\langle M_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} , \quad \alpha_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\rangle , \text{order } 8$$

$$\Phi = \frac{1+\lambda^3}{(1-\lambda)(1-\lambda^2)^2(1-\lambda^4)}$$

$$R : \frac{1,\ BCD}{A, B^2+C^2,\ D^2,\ B^2C^2} \tag{117}$$

where

$$A = (x+y)/2, B = (x-y)/2, C = (z+t)/2, D = (z-t)/2 \ . \tag{118}$$

swe of C, $1^n \in C$: (Set $t = z$ in cwe)

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^4)}$$

$$R : \frac{1}{A,\ B^2+C^2,\ B^2C^2} \tag{119}$$

where

$$A = (x+y)/2, B = (x-y)/2, C = z \ . \tag{120}$$

cwe of C, $1^n \in S$: Note that $(1^n, u) = wt(u) - n_1(u) \equiv wt(u) \pmod 2$ if and only if the number of 1's in u is even. So if $1^n \in S$, the cwe is invariant under $\mathrm{diag}\{1,-1,1,1\}$.

$$G = \langle M_4,\ \mathrm{diag}\{1,-1,1,1\} \rangle \ , \quad \text{order } 6$$

$$\Phi = \frac{1}{(1-\lambda)^2(1-\lambda^2)(1-\lambda^3)}$$

$$R : \frac{1}{D,\ A+B+C,\ A^2+B^2+C^2,\ A^3+B^3+C^3} \tag{121}$$

where A, $B, \ldots$ are as in (118).

swe of C, $1^n \in S$: (Set $t = z$ in cwe)

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)}$$

$$R : \frac{1}{\text{symmetric polynomials in } A,\, B,\, C} \tag{122}$$

hwe of S:

$$\Phi : \frac{1}{(1-\lambda)(1-\lambda^2)}$$

$$R : \frac{1}{2y,\ -\frac{1}{2}(x^2-y^2)} \tag{123}$$

As a corollary, the weight of a vector in the shadow is congruent to $n \pmod 2$.

hwe of $W^{(1)} - W^{(3)}$: Again we use the terminology $W^{(i)}$, $i = 0, \ldots, 3$, for the cosets of C_0 in $C_0^{\perp}$ (as in Sect. 5)

$$G = \left\langle M_2 = \frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

with character $\chi(M_2) = 1$, $\chi(\alpha_2) = (-1)^n$ ($\text{Ker}\ \chi \cong S_3$)

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^3)}$$

$$R : \frac{1}{x^2+3y^2,\ y(x^2-y^2)}\ . \tag{124}$$

cwe of S, $1^n \in C$: Belongs to image of (117) under the map that sends (x, y, z, t) to $(x, y, z, t)\beta_4 M_4$:

$$R : \frac{1,\ ABD}{C,\ A^2+B^2,\ D^2,\ A^2B^2} \tag{125}$$

cwe of $W^{(1)} - W^{(3)}$, $1^n \in C$: $G = \langle M_4, \alpha_4, \beta_4 \rangle$ with character $\chi(M_4) = 1$, $\chi(\alpha_4) = \chi(\beta_4) = (-1)^n$, order 48

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)(1-\lambda^4)}$$

$$R : \frac{1}{D,\ A^2+B^2+C^2,\ ABC,\ A^4+B^4+C^4} \tag{126}$$

where

$$A = x + y,\ B = x - y,\ C = z + t,\ D = z - t.$$

swe of $W^{(1)} - W^{(3)}$, $1^n \in C$:

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^3)(1-\lambda^4)}$$
$$R : \frac{1}{A^2+B^2+C^2,\ ABC,\ A^4+B^4+C^4} \tag{127}$$

cwe of S, $1^n \in S$: Belongs to image of (121) under the map $x \to y$, $y \to x$, $z \to t$, $t \to z$:

$$R : \frac{1}{-D,\ A-B+C,\ A^2+B^2+C^2,\ A^3-B^3+C^3} \tag{128}$$

swe of S, $1^n \in S$: Set $D = 0$ in (128).

hwe of S, $1^n \in S$: Same as (123).

cwe of $W^{(1)} - W^{(3)}$, $1^n \in S$: $G = \langle M_4, \beta_4 = \mathrm{diag}\{1,-1,-1,-1\}\rangle$, with character $\chi(M_4) = 1$, $\chi(\beta_4) = (-1)^n$, order 12

$$\Phi = \frac{1}{(1-\lambda)^2(1-\lambda^2)(1-\lambda^3)}$$
$$R : \frac{1}{D,\ A-B-C,\ A^2+B^2+C^2,\ A^3-B^3-C^3} \tag{129}$$

Remark. We may obtain $W^{(1)} - W^{(3)}$ by applying α_4 to $W^{(0)} - W^{(2)}$, which in turn is obtained by applying β_4 to $W^{(0)} + W^{(2)}$.

7.7. Family $4_{\mathrm{II}}^{\mathrm{H}+}$: Additive even self-dual codes over $\mathbb{F}_4$ using trace inner product

hwe of C: Same as family 4^{H}, see (105).

cwe of C, $1^n \in C$:

$$G = \langle M_4, \alpha_4, \beta_4 \rangle\ , \quad \text{order } 48$$
$$\Phi = \frac{1+\lambda^4}{(1-\lambda^2)^2(1-\lambda^4)(1-\lambda^6)}$$
$$R : \frac{1,\ ABCD}{D^2,\ A^2+B^2+C^2,\ A^4+B^4+C^4,\ A^6+B^6+D^6} \tag{130}$$

swe of C, $1^n \in C$: (Set $t = z$ in cwe)

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^4)(1-\lambda^6)}$$
$$R : \frac{1}{\text{symmetric polynomials in } A^2,\ B^2,\ C^2} \tag{131}$$

cwe of C (not assuming $1^n \in C$):

$$G = \langle M_4, \beta_4 \rangle, \quad \text{order } 12$$

$$\Phi = \frac{1 + \lambda^2 + 2\lambda^4}{(1-\lambda^2)^3(1-\lambda^6)} \tag{132}$$

Codes: The following codes will be used:

$$\begin{aligned}
i_1 &= [1], \quad cwe = swe = hwe = x + y \\
i_1' &= [\omega], \quad cwe = swe = x + z \\
i_1'' &= [\overline{\omega}], \quad cwe = x + t, \ swe = x + z \\
i_2 &= [11, \omega\omega], \quad \text{see (114)} \\
i_2' &= [11, \omega\overline{\omega}], \quad cwe = x^2 + y^2 + 2zt, swe = x^2 + y^2 + 2z^2, hwe = x^3 + 3y^2 \\
c_3 &= [111, \omega\omega 0, \omega 0\omega] \\
c_4 &= [1111, \omega(\omega 00)] \\
c_4' &= [\omega\omega\omega\omega, 1(100)]
\end{aligned}$$

Ring	Codes
(116)	i_1, i_2
(117)	$i_1, i_2, i_2', c_4; c_3$
(119)	i_1, i_2, c_4
(121)	i_1', i_1'', i_2, c_3'
(122)	i_1', i_2, c_3'
(123)	i_1, i_2
(125)	$i_1, i_2, i_2', c_4; c_3$
(129)	i_1', i_1'', i_2, c_3
(130)	$i_2, i_2', c_4', h_6; c_4$
(131)	i_2, c_4', h_6

(133)

7.8. Family q^{H}: Codes over $\mathbb{F}_q$, q a square, with Hermitian inner product

The case $q = 4$ has been studied in Section 7.4. The next case is $q = 9$, but as little attention has been paid so far to codes over this field we shall not discuss the cwe or swe further. It is possible to say a little about the Hamming weight enumerator in the general case.

hwe of C (See Theorem 16):

$$G = \left\langle \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \text{ order } 4$$

$$\Phi = \frac{1}{(1-\lambda^2)^2}$$
$$R : \frac{1}{x^2 + (q-1)y^2,\ y(x-y)} \tag{134}$$

(This is somewhat unsatisfactory, since $y(x-y)$ forces a vector of weight 1, which is impossible in a self-dual code.)

7.9. Family q^{E}: Codes over $\mathbb{F}_q$ with Euclidean inner product

The cases $q = 2, 3$ and 4 have been studied in Sections 7.1, 7.3, 7.5. As q increases the results rapidly become more complicated.

We first discuss the case $q = 5$ and then say a little about the general case.

cwe of C, $q = 5$: Let $\xi = e^{2\pi i/5}$.

$$G = \left\langle \frac{1}{\sqrt{5}}(\xi^{rs})_{r,s=0,\ldots,4},\ \mathrm{diag}\{1, \xi, \xi^{-1}, \xi^{-1}, \xi\} \right\rangle , \quad \text{order } 240$$
$$\Phi = \frac{\phi(\lambda)}{(1-\lambda^4)(1-\lambda^6)(1-\lambda^{10})^2} \tag{135}$$

where $\phi(\lambda)$ is a polynomial of degree 26, with $\phi(1) = 60$. A good basis for this ring would therefore involve about 65 polynomials! Such Behavior is typical of most groups — see Huffman and Sloane [150].

swe of C, $q = 5$

$$G = \left\langle \begin{pmatrix} 1 & 2 & 2 \\ 1 & \xi+\xi^4 & \xi^2+\xi^3 \\ 1 & \xi^2+\xi^3 & \xi+\xi^4 \end{pmatrix}, \mathrm{diag}\{1, \xi, \xi^4\}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle ,$$

(the reflection group [3, 5], a three-dimensional representation of the icosahedral group, Shephard and Todd #23), order 120

$$\Phi = \frac{1}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})}$$
$$R : \frac{1}{\alpha,\ \beta,\ \gamma} \tag{136}$$

where

$$\begin{aligned} \alpha &= x^2 + 4yz \\ \beta &= x^4yz - x^2y^2z^2 - x(y^5+z^5) + 2y^3z^3 \\ \gamma &= 5x^6y^2z^2 - 4x^5(y^5+z^5) - 10x^4y^3z^3 + 10x^3(y^6z+yz^6) + 5x^2y^4z^4 \\ &\quad - 10x(y^7z^2+y^2z^7) + 6y^5z^5 + y^{10} + z^{10} . \end{aligned}$$

Codes: [12], [(100)(133)] and either

$$d_5^{2+} = [(01234)(00000), (00000)(01234), 1111111111]$$

or

$$e_{10}^{+} = [(00014)(00023), 1111111111] \tag{137}$$

for the invariant of degree 10.

In [181] it was observed that these invariants were already known to Klein [164], [165]. This paper then went on to remark that "it is worth mentioning that precisely the same invariants have recently been studied by Hirzebruch in connection with cusps of the Hilbert modular surface associated with $\mathbb{Q}(\sqrt{5})$ — see [131], p. 306. However, there does not seem to be any connection between this work and ours". An elegant explanation for this was soon found by Hirzebruch [132]. The basic idea is to take a self-dual code over $\mathbb{F}_5$ and to obtain from it (using a version of Construction A [70]) a lattice over $\mathbb{Z}[\sqrt{5}]$. The theta series of this lattice is a Hilbert modular form which can be written down from the swe of the code. This produces an isomorphism between the ring of swe's and the appropriate ring of Hilbert modular forms. The monograph [92] gives a comprehensive account of these connections.

Incidentally, we do not know if the cwe ring described by (135) collapses to (136).

hwe of C, $q = 5$: ([224]) (Set $z = y$ in swe)

$$\Phi = \frac{1 + \lambda^{10} + \lambda^{20}}{(1 - \lambda^2)(1 - \lambda^6)}$$

$$R : \frac{1,\ \overline{\gamma},\ \overline{\gamma}^2}{\overline{\alpha},\ \overline{\beta}}$$

where

$$\begin{aligned} \overline{\alpha} &= x^2 + 4y^2, \\ \overline{\beta} &= y^2(x-y)^2(x^2 + 2xy + 2y^2), \\ \overline{\gamma} &= y^4(x-y)^4(5x^2 + 12xy + 8y^2)\ . \end{aligned}$$

cwe of C, $q = 5$, $1^n \in C$: (The group is now considerably larger, but the ring of invariants is no simpler)

$$G = \langle \text{previous group},\ \text{diag}\{1, \xi, \xi^2, \xi^3, \xi^4\} \rangle$$

$\cong \pm 5^{1+2}.Sp_2(5)$, a Clifford group [20], [21], [44], [318] (see also [135]), order 30000

$$\Phi = \frac{1 + 3\lambda^{20} + 13\lambda^{30} + 18\lambda^{40} + 28\lambda^{50} + 34\lambda^{60} + 17\lambda^{70} + 4\lambda^{80} + 2\lambda^{90}}{(1-\lambda^{10})(1-\lambda^{20})^2(1-\lambda^{30})^2} \ .$$

The sum of the coefficients in the numerator is 120, so again there is no possibility of giving a good basis.

The degree 10 invariant is the cwe of either of the codes of length 10 given in (137).

cwe of C, general q: It is hard to say anything in general, but if q is an odd prime p we can at least describe the structure of the group G under which the cwe is invariant.

$$G = \left\langle M = \frac{1}{\sqrt{p}}(\xi^{rs})_{r,s=0,\ldots,p-1},\ J = \mathrm{diag}\{1, \xi, \xi^4, \xi^9, \ldots\}, -I \right\rangle \ .$$

If $1^n \in C$ then the cwe is invariant under the larger group $G^+ = \langle G, P\rangle$, where

$$P : x_j \to x_{j+1}, \quad \text{(subscripts mod } p\text{)}$$

We use $\Xi(H)$ to denote the center of a group H.

Theorem 22. *(a) Suppose $p \equiv 1 \pmod 4$. Then G has structure $Z(2) \times SL_2(p)$ and center $\Xi(G) = \langle -I\rangle$. G^+ has structure $Z(2) \times p^{1+2}\ SL_2(p)$ and $\Xi(G^+) = \langle -I, \xi I\rangle$. (b) Suppose $p \equiv 3 \pmod 4$. Then G has structure $Z(4) \times SL_2(p)$ and $\Xi(G) = \langle iI\rangle$. G^+ has structure $Z(4) \times p^{1+2}SL_2(p)$ and $\Xi(G^+) = \langle iI, \xi I\rangle$. In either case G and G^+ are preserved by the Galois group $Gal(\mathbb{Q}[\sqrt{p}, \xi]/\mathbb{Q})$.*

Remarks. (i) The group G was first studied in the present context by Gleason [105]. The groups G and G^+ (also for composite odd q, and with the appropriate modification for even q as well) are a special case of the construction in [324]. Weil obtains analogs of G^+, in which $\mathbb{F}_q$ can be replaced by any locally compact abelian group isomorphic to its Pontrjagin dual.[6]

(ii) The analogous results for $p = 2$ are given in Sections 7.1 and 7.2. (iii) In both cases (a) and (b) G^+ is the full normalizer (with coefficients restricted to $\mathbb{Q}[\sqrt{p}, \xi]$) of the extraspecial p-group $E = \langle P, Q\rangle$, where $Q = \mathrm{diag}\{1, \xi, \xi^2, \xi^3, \ldots\}$ (cf. [44]).

Proof. G normalizes E, since $MPM^{-1} = Q^{-1}$, $MQM^{-1} = P$, $JPJ^{-1} = \xi^a PQ^{-2}$, $JQJ^{-1} = \xi^b Q$ for appropriate integers a and b. (Note that $\xi I = PQP^{-1}Q^{-1} \in E$.) Thus we have a

[6] We are grateful to N. D. Elkies for this comment.

surjective homomorphism ϕ from G to $SL_2(p) : M \to \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $J \to \left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right)$. In particular G is transitive on $E/\langle \xi I \rangle$.

Suppose $G \cap E$ is nontrivial. If there were a noncentral element of E in G then by the transitivity of G it would follow that $\xi^c P \in G$ and $\xi^d Q \in G$ for some c, d. But then $\xi I \in G$. This would force the length of C to be a multiple of p, which is false (since there is always a code of length 4). Hence $G \cap E = \{I\}$.

E is irreducible, so the centralizer of E consists only of multiples of I. It follows that $\ker \phi$ consists of multiples of elements of E. But the fourth power of an element of $\ker \phi$ would be in E, and this must be I. Thus $\ker \phi$ is either $\langle -I \rangle$ or $\langle iI \rangle$. If $p \equiv 1 \pmod 4$ then $i \notin \mathbb{Q}[\sqrt{p}, \xi]$, so the first possibility obtains. It remains to show that $iI \in G$ when $p \equiv 3 \pmod 4$. The matrix $(MJ)^p M^2$ is readily verified to belong to $\ker \phi$. But $\det((MJ)^p M^2) = (\det M)^{p+2}$. Since M^2 maps x_j to x_{-j}, $\det M^2 = -1$, so $\det M = \pm i$. It follows that $(MJ)^p M^2$ is $\pm iI$. ∎

Corollary 1. *If $p \equiv 3 \pmod 4$ then a self-dual code over $\mathbb{F}_p$ must have length divisible by 4.*

Proof. $iI \in G$. ∎

The conclusion of Corollary 1 also holds for self-dual codes over $\mathbb{F}_q$, $q \equiv 3 \pmod 4$ [226].

hwe of C, general q: Belongs to the ring (134). If $q \equiv 3 \pmod 4$ we can say more ([128]):

$$G = \left\langle \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \right\rangle, \quad \text{order } 8$$

$$\Phi = \frac{1 + \lambda^4}{(1 - \lambda^4)^2}$$

$$R : \frac{1,\ x^2y^2 - 2xy^3 + y^4}{x^4 + 4(q-1)xy^3 + (q-1)(q-3)y^4,\ x^3y + (q-3)xy^3 - (q-2)y^4}$$

7.10. Family $4_{\mathrm{I}}^{\mathbb{Z}}$: Self-dual codes over $\mathbb{Z}_4$

cwe of C: ([167])

$$G = \left\langle M_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix},\ \alpha_4 = \mathrm{diag}\{1, i, 1, i\} \right\rangle, \quad \text{order } 64$$

$$\Phi = \frac{1 + \lambda^{10}}{(1 - \lambda)(1 - \lambda^4)^2(1 - \lambda^8)}$$

$$R : \frac{1,\ (BCD)^2(B^4 - C^4)}{A,\ B^4 + C^4,\ D^4,\ B^4C^4} \tag{138}$$

where

$$A = x + z,\ B = y + t,\ C = x - z,\ D = y - t\ . \tag{139}$$

swe of C: (Set $t = y$ in cwe)

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^4)(1-\lambda^8)}$$

$$R : \frac{1}{A,\ B^4 + C^4,\ B^4C^4} \tag{140}$$

hwe of C: (Set $t = z = y$ in cwe)

$$\Phi = \frac{1+\lambda^8}{(1-\lambda)(1-\lambda^4)}$$

$$R : \frac{1,\ y^4(x-y)^4}{x+y,\ y(x-y)(x^2+xy+2y^2)} \tag{141}$$

cwe, $1^n \in C$

$$G = \left\langle M_4, \alpha_4, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\rangle\ , \quad \text{order } 1024$$

$$\Phi = \frac{(1+\lambda^{12})(1+\lambda^{16})}{(1-\lambda^4)(1-\lambda^8)^2(1-\lambda^{16})}$$

$$R : \frac{(1,\ A^{12}+B^{12}+C^{12}+D^{12}) \times (1,\ \sigma_{16})}{A^4+B^4+C^4+D^4,\ A^8+B^8+C^8+D^8,\ \sigma_8,\ A^4B^4C^4D^4} \tag{142}$$

where

$$\begin{aligned} \sigma_8 &= A^4D^4 + B^4C^4\ , \\ \sigma_{16} &= (ABCD)^2(A^4B^4 + C^4D^4 - A^4C^4 - B^4D^4) \end{aligned}$$

swe of C, $\pm 1^n \in C$ (Set $t = y$ in cwe)

$$\Phi = \frac{1+\lambda^{12}}{(1-\lambda^4)(1-\lambda^8)^2}$$

$$R : \frac{1,\ A^4B^4C^4}{A^4+B^4+C^4,\ A^8\ B^8\ C^8,\ B^4C^4}\ . \tag{143}$$

This ring may also be described as $R_0 \oplus B^4C^4R_0 \oplus B^8C^8R_0$, where R_0 is the ring of symmetric polynomials in A^4, B^4, C^4.

hwe of C, $\pm 1^n \in C$: (Set $t = z = y$ in cwe)

$$\Phi = \frac{(1+\lambda^8)(1+\lambda^{12})}{(1-\lambda^4)(1-\lambda^8)}$$

$$R : \frac{(1,\ y^2(x^2+3y^2)(x^2-y^2)^2) \times (1,\ y^4(x^2-y^2)^4)}{(x^2+3y^2)^2,\ y^4(x-y)^4} \tag{144}$$

cwe of C, $1^n \in S$: If $1^n \in S$, Part (i) of Theorem 8 implies that if a vector $0^a 1^b 2^c d^d \in C$ then $b-d+2c \equiv \frac{1}{2}(b+d)+2c \pmod 4$, i.e. $b \equiv 3d \pmod 8$, and so $\beta_4 = \mathrm{diag}\{1, \eta, 1, \eta^5\} \in G$.

$$G = \langle M_4, \beta_4 \rangle, \quad \text{order } 192$$

$$\Phi = \frac{1+\lambda^{18}}{(1-\lambda)(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \frac{1,\ B^2C^2D^2(B^4-C^4)(B^4+D^4)(C^4+D^4)}{A,\ B^4+C^4-D^4,\ B^8+C^8+D^8,\ B^{12}+C^{12}-D^{12}} \tag{145}$$

swe and hwe of C, $\pm 1^n \in S$: Same as (140) and (141), respectively.

cwe of S: the image of (138) under $A \to B$, $B \to \eta C, C \to A$, $D \to \eta^3 D$

$$\Phi = \frac{(1+\lambda^{10})}{(1-\lambda)(1-\lambda^4)^2(1-\lambda^8)}$$

$$R : \frac{1,\ A^2C^2D^2(-A^4-C^4)}{B,\ A^4-C^4,\ -D^4,\ -A^4C^4} \tag{146}$$

swe of S: the image of (140) under $A \to B$, $B \to \eta C$, $C \to A$

$$\Phi = \frac{1}{(1-\lambda)(1-\lambda^4)(1-\lambda^8)}$$

$$R : \frac{1}{B,\ A^4-C^4,\ -A^4C^4} \tag{147}$$

It follows that the norms of vectors in the shadow are congruent to $n \bmod 8$.

cwe of S, $1^n \in C$: the image of (143) under $A \to B$, $B \to \eta C$, $C \to A$, $D \to \eta^3 D$.

swe of S, $\pm 1^n \in C$:

$$\Phi = \frac{1+\lambda^{12}}{(1-\lambda^4)(1-\lambda^8)^2}$$

$$R : \frac{1,\ -A^4B^4C^4}{A^4+B^4-C^4,\ A^8+B^8+C^8,\ -A^4C^4} \tag{148}$$

cwe of S, $1^n \in S$:

$$R : \frac{1,\ A^2C^2D^2(A^4+C^4)(C^4+D^4)(A^4-D^4)}{B,\ A^4-C^4+D^4,\ A^8+C^8+D^8,\ A^{12}-C^{12}+D^{12}} \tag{149}$$

swe of S, $\pm 1^n \in S$: same as (147).

cwe of $W^{(1)} - W^{(3)}$:

$$G = \langle M_4, \gamma_4 = \mathrm{diag}\{1, \eta, -1, \eta\}\rangle \ , \quad \text{order } 768 \ ,$$

with character $\chi(M_4) = i^n$, $\chi(\gamma_4) = \eta^n$

$$\Phi = \frac{1+\lambda^{18}}{(1-\lambda)(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \frac{1, A^2B^2C^2(A^4+B^4)(A^4+C^4)(B^4-C^4)}{D,\ \text{symmetric polynomials in } A^4, -B^4, -C^4} \tag{150}$$

swe of $W^{(1)} - W^{(3)}$:

$$\Phi = \frac{1+\lambda^{18}}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \text{omit } D \text{ from (150)} \tag{151}$$

(This ring has also been studied in [88].)

cwe of $W^{(1)} - W^{(3)}$ with $1^n \in C$: $G = \langle M_4, \beta_4, \gamma_4\rangle$, order 6144, with character $\chi(M_4) = i^n$, $\chi(\beta_4) = 1$, $\chi(\gamma_4) = \eta^n$; $\ker(\chi)$ has order 3072

$$\Phi = \frac{1+\lambda^{32}}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{16})}$$

$$R : \frac{1,\ A^2B^2C^2D^2(A^4+B^4)(A^4+C^4)(A^4-D^4)(B^4-C^4)(B^4+D^4)(C^4+D^4)}{\text{symmetric polynomials in } A^4, -B^4, -C^4, D^4} \tag{152}$$

swe of $W^{(1)} - W^{(3)}$ with $1^n \in C$:

$$\Phi = \frac{1}{(1-\lambda^4)(1-\lambda^8)(1-\lambda^{12})}$$

$$R : \frac{1}{\text{symmetric polynomials in } A^4,\ -B^4,\ -C^4}$$

7.11. Family $4_{\rm II}^{\mathbb{Z}}$: Type II self-dual codes over $\mathbb{Z}_4$

cwe of C, $1^n \in C$ [51], [27] In view of the remarks following Theorem 8, this is not a severe restriction.

$$G = \langle M_4, \beta_4, \gamma_4 \rangle \ , \quad \text{order } 6144$$
$$\Phi = \frac{(1+\lambda^{16})(1+\lambda^{32})}{(1-\lambda^8)^2(1-\lambda^{16})(1-\lambda^{24})}$$
$$R : \frac{(1,\ f_{16}) \times (1,\ f_{32})}{A^8+B^8+C^8+D^8,\ f_8,\ A^{16}+\cdots+D^{16},\ A^{24}+\cdots+D^{24}} \tag{153}$$

where

$$\begin{aligned} f_8 &= A^4C^4 + C^4D^4 + D^4B^4 + B^4A^4 - A^4D^4 - B^4C^4 \ , \\ f_{16} &= (ABCD)^4 \ , \\ f_{32} &= (ABCD)^2(A^4+C^4)(C^4+D^4)(D^4+B^4)(B^4+A^4)(A^4-D^4)(B^4-C^4) \end{aligned}$$

swe of C, $\pm 1^n \in C$

$$\Phi = \frac{1+\lambda^{16}}{(1-\lambda^8)^2(1-\lambda^{24})}$$
$$R : \frac{1,\ \theta_{16}}{\theta_8,\ h_8,\ \theta_{24}} \tag{154}$$

where

$$\begin{aligned} \theta_8 &= x^8 + 28x^6z^2 + 70x^4z^4 + 28x^2z^6 + z^8 + 128y^8 \ , \\ \theta_{16} &= \{x^2z^2(x^2+z^2)^2 - 4y^8\}\{(x^4+6x^2z^2+z^4)^2 - 64y^8\} \ , \\ \theta_{24} &= y^8(x^2-z^2)^8 \ , \\ h_8 &= \{xz(x^2+z^2) - 2y^4\}^2 \ . \end{aligned}$$

cwe of C, $1^n \in C$, Lee weights divisible by 4 ([51])

$$G = \left\langle M_4, \beta_4, \gamma_4, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & i & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \right\rangle$$

(Shephard & Todd #2a), order 49152

$$\Phi = \frac{1}{(1-\lambda^8)(1-\lambda^{16})^2(1-\lambda^{24})}$$
$$R : \frac{1}{f_{16},\ \text{symmetric polynomials in } A^8,\ B^8,\ C^8,\ D^8} \tag{155}$$

swe of C, $\pm 1^n \in C$, Lee weights divisible by 4 ([51]) (Set $t = y$ in cwe)

$$\Phi = \frac{1}{(1-\lambda^8)(1-\lambda^{16})(1-\lambda^{24})}$$

$$R : \frac{1}{\theta_8,\ \theta_{16},\ \theta_{24}} \tag{156}$$

However, the following result shows that the extra condition on the Lee weights may not be a good thing. For it was shown in [119] that most interesting linear codes over $\mathbb{Z}_4$ do not have linear images under the Gray map.

Theorem 23. [51] *If C is a self-dual code over $\mathbb{Z}_4$ with all Lee weights divisible by 4, then the binary image of C under the Gray map (39) is linear.*

For the proof, see [51].

Codes. The following codes will be used: i_1 and $\mathcal{D}_4^{\oplus}$ are defined in Section 11.8, and o_8 is the octacode (38). $\mathcal{J}_{10}$ is the self-dual code with generator matrix

$$\begin{bmatrix}
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 3 & 3 & 1 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2
\end{bmatrix}$$

and $|\mathcal{J}_{10}| = 4^2 2^6$ ([71]). $\mathcal{J}_{16}$ has generator matrix

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 3 & 3 & 1 & 0 & 3 & 2 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 3 & 3 & 1 & 1 & 2 & 3 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 3 & 3 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 3 & 0 & 2 & 3 & 3 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0
\end{bmatrix}$$

and $|\mathcal{J}_{16}| = 4^6 2^4$.

$\mathcal{K}_{4m}$ ($m \geq 1$, but note that $\mathcal{K}_4 \cong \mathcal{D}_4^{\oplus}$) is a self-dual code introduced by Klemm [167], having generator matrix

$$\begin{bmatrix}
1 & 1 & 1 & \dots & 1 & 1 \\
0 & 2 & 0 & \dots & 0 & 2 \\
0 & 0 & 2 & \dots & 0 & 2 \\
. & . & . & \dots & . & . \\
0 & 0 & 0 & \dots & 2 & 2
\end{bmatrix} ; \tag{157}$$

$|\mathcal{K}_{4m}| = 4^1 2^{4m-2}$, $g = 2^{4m-1}(4m)!$, $cwe = (A^{4m} + B^{4m} + C^{4m} + D^{4m})/2$ (see (139)).

Ring	Codes
(138)	i_1, $\mathcal{D}_4^{\oplus}$ in 2 versions (177), o_8; $\mathcal{J}_{10}$
(140)	$i_1, \mathcal{D}_4^{\oplus}$, o_8
(141)	$i_1, \mathcal{D}_4^{\oplus}$; o_8
(142)	$\mathcal{K}_4$, $\mathcal{K}_8$, o_8, $\mathcal{K}_{16}$; $\mathcal{K}_{12}, \mathcal{J}_{16}$
(143)	$\mathcal{K}_4$, $\mathcal{K}_8$, o_8; $\mathcal{K}_{12}$
(144)	$\mathcal{K}_4$, o_8; $\mathcal{K}_8$, $\mathcal{K}_{12}$
(153)	$\mathcal{K}_8$, o_8, $\mathcal{K}_{16}$, $\mathcal{K}_{24}$; $\mathcal{J}_{16}$,?
(154)	$\mathcal{K}_8$, o_8, $\mathcal{K}_{24}$; $\mathcal{J}_{16}$
(156)	$\mathcal{K}_8$, $\mathcal{K}_{16}$, $\mathcal{K}_{24}$

(158)

Again the question mark indicates that we do not have a satisfactory code to produce the desired polynomial.

7.12. Family $m^{\mathbb{Z}}$: Self-dual codes over $\mathbb{Z}_m$

The Hamming weight enumerator of a self-dual code over $\mathbb{Z}_m$ for general m has been considered in [128].

8. Weight enumerators of maximally self-orthogonal codes

In some cases it is possible to prove results analogous to those in Section 7 for codes which are maximally self-orthogonal yet not self-dual, the $[7, 3, 4]$ Hamming code e_7 with weight enumerator $p_7 = x^7 + 7x^3y^4$ being a typical example. A more trivial example is the zero code $z_1 = \{0\}$, with weight enumerator $p_1 = x$.

The following results are proved in [197].

For n odd, let C be an $[n, \frac{1}{2}(n-1)]$ self-orthogonal binary code. Thus $C^{\perp} = C \cup (1 + C)$. The weight enumerator of C belongs to the module $R = p_1\mathbb{C}[x^2+y^2, x^2y^2(x^2-y^2)^2] \oplus p_7\mathbb{C}[x^2+y^2, x^2y^2(x^2-y^2)^2]$, which in the notation of the previous section would be described by

$$\Phi = \frac{\lambda + \lambda^7}{(1-\lambda^2)(1-\lambda^8)}$$
$$R : \frac{p_1,\ p_7}{x^2+y^2,\ x^2y^2(x^2-y^2)^2} \tag{159}$$

(compare (95)). If in addition C is doubly-even, the module is described by:
(a) if $n = 8m - 1$,

$$\Phi = \frac{\lambda^7 + \lambda^{23}}{(1-\lambda^8)(1-\lambda^{24})}$$
$$R : \frac{p_7,\ p_{23}}{x^8 + 14x^4y^4 + y^8,\ x^4y^4(x^4-y^4)^4} \tag{160}$$

(b) if $n = 8m + 1$,

$$\Phi = \frac{\lambda + \lambda^{17}}{(1-\lambda^8)(1-\lambda^{24})}$$

$$R : \frac{p_1,\ p_{17}}{x^8 + 14x^4y^4 + y^8,\ x^4y^4(x^4 - y^4)^4} \tag{161}$$

(compare (99)). Here $p_{17} = x^{17} + 17x^{13}y^4 + 187x^9y^8 + 51x^5y^{12}$, $p_{23} = x^{23} + 506x^{15}y^8 + 1288x^{11}y^{12} + 253x^7y^{16}$.

Codes. The code g_{23} is the cyclic version of g_{24} obtained by deleting any coordinate.

Ring	Codes
(159)	$i_2, e_8; z_1, e_7$
(160)	$e_8, g_{24}; e_7, g_{23}$
(161)	$e_8, g_{24}; z_1, (d_{10}e_7)^+$

There are analogous results for ternary codes: see [198].

9. Upper bounds

Of course, we are interested not just in codes per se, but also in good (or, at the very least, interesting) codes, that is, codes with large minimal distance (Hamming, Lee, or Euclidean, as appropriate). In order to know if a particular code is good, it is necessary to know how good comparable codes could be; that is, for a given length and dimension, what is the optimal minimal distance? For general codes, this question was studied in Chapters xx (Levenshtein), yy (Brouwer) and zz (Litsyn); we are, of course, interested in self-dual codes. As one might imagine, the constraint of self-duality usually leads to stronger bounds.

We will concentrate most of our attention on binary codes (family 2), pointing out analogues to other families as they arise.

Essentially all of the bounds we will be discussing are special cases of the linear programming (or LP) bound (Section 2.5 of Chapter yy (Brouwer)); that is, they rely on the fact that both the weight enumerator of the code and the weight enumerator of its dual are nonnegative. For a self-dual code, these weight enumerators are, of course, equal. So for Type II self-dual binary codes, for instance, we have the following:

Theorem 24. *If there exists a Type II self-dual binary code of length n and minimal distance d, then there exists a homogeneous polynomial $W(x, y)$ with nonnegative (integer) coefficients*

such that

$$\begin{aligned} 2^{n/2}W(x+y,x-y) &= W(x,y) \\ W(1,y) &= 1+O(y^d) \\ W(x,iy) &= W(x,y). \end{aligned}$$

These conditions assert that the code is self-dual, that it has minimal distance d, and that it is of Type II, respectively.

The analogues for other classes of codes should be clear; in each case, the appropriate enumerator (Hamming, symmetrized, complete) is nonnegative, invariant under the appropriate transformations (see Section 7), and is zero on all terms of low weight. In some cases, we can add further constraints from shadow theory (Section 5), since the weight enumerator of the shadow of the code is also nonnegative. For instance:

Theorem 25. *If there exists a Type I self-dual binary code of length n and minimal distance d, then there exist homogeneous polynomials $W(x,y)$ and $S(x,y)$ with nonnegative (integer) coefficients such that*

$$\begin{aligned} W(x,y) &= 2^{-n/2}W(x+y,x-y) \\ W(1,y) &= 1+O(y^d) \\ S(x,y) &= 2^{-n/2}W(x+y,i(x-y)). \end{aligned}$$

Again there are analogues for each family for which shadows are well-defined (2, $4^{\mathrm{H}+}$, $4^{\mathbb{Z}}$).

Remark. For a code C from family q^{H} (linear over F_q, q a square, with Hermitian inner product), it can be shown that the polynomial

$$S(x,y) = q^{-n/2}W((\sqrt{q}-1)x+(\sqrt{q}+1)y,\ y-x)$$

has nonnegative (but not necessarily integral) coefficients; note that this agrees with the shadow enumerator for $q=4$. This can be used to strengthen the LP bound in those cases. The known proof that this is nonnegative involves constructing a quantum code Q from C ([249]); $S(x,y)$ is then the shadow enumerator of Q ([252], proved nonnegative in [253]). There is surely a more direct proof.

One way to apply the linear programming bound is to ignore the constraint that the coefficients of $W(x,y)$ be nonnegative, and simply ask that the low order coefficients be as specified.

This gives a surprisingly good bound for Type II binary codes. Recall from Theorem 13 that for C of Type II, $W(x,y)$ lies in the ring

$$R = \mathbb{C}[x^8 + 14x^4y^4 + y^8, x^4y^4(x^4 - y^4)^4],$$

and if C has length n, $W(x,y)$ has degree n. The subspace of R of degree n has dimension $D = [\frac{n}{24}] + 1$. This lets us set the first D coefficients of $W(x,y)$ arbitrarily; in particular, there exists a unique element $W^*(x,y)$ of R such that $W^*(1,y) = 1 + O(y^{4D})$. This is known as the *extremal* enumerator, since W^* has the largest minimal distance of any Type II self-dual enumerator. It follows immediately that the minimal distance of any Type II code of length n is bounded above by the minimal distance of W^*.

Theorem 26. [196] *The first nonzero coefficient of $W^*(1,y)$ occurs precisely at degree $4D$; in particular, the minimal distance of a Type II self-dual binary code of length n is at most $4[n/24] + 4$.*

In fact it is possible to use the Bürmann-Lagrange theorem (Theorem 32) to derive an explicit formula for the number of words of weight $4D$ in the extremal enumerator. Let $\mu = [n/24]$, so that $D = \mu + 1$. Then we have

Theorem 27. (Mallows and Sloane [196].) *$A^*_{4\mu+4}$, the number of codewords of minimal nonzero weight $4D = 4\mu + 4$ in the extremal weight enumerator, is given by:*

$$\binom{n}{5}\binom{5\mu - 2}{\mu - 1} \Big/ \binom{4\mu + 4}{5}, \quad \text{if} \quad n = 24\mu \ , \tag{162}$$

$$\frac{1}{4}n(n-1)(n-2)(n-4)\frac{(5\mu)!}{\mu!(4\mu+4)!}, \quad \text{if} \quad n = 24\mu + 8 \ , \tag{163}$$

$$\frac{3}{2}n(n-2)\frac{(5\mu+2)!}{\mu!(4\mu+4)!}, \quad \text{if} \quad n = 24\mu + 16 \ , \tag{164}$$

and is never zero.

For the proof, see [196] or [190], Chapter 19. There is a similar formula for Type I binary codes — see [190], Chapter 19, Problem (12).

Results similar to Theorem 26 hold for other families:

Theorem 28. *The minimal distance of a Type I binary self-dual code is at most $2[n/8] + 2$. The minimal distance of a Type II binary self-dual code is at most $4[n/24] + 4$. The minimal*

distance of a self-dual code from family 3 *is at most* $3[n/12]+3$. *The minimal distance of a self-dual code from family* 4^{H} *is at most* $2[n/6]+2$. *The minimal distance of a Type II self-dual code from family* $4^{\mathrm{H}+}$ *is at most* $2[n/6]+2$. *The minimal distance of a self-dual code from families* 4^{E}, $4^{\mathrm{H}+}$, q^{H} *or* q^{E} *is at most* $[n/2]+1$.

Note that the last bound is simply the Singleton bound, obtained from the ring $\mathbb{C}[x^2+(q-1)y^2, y(x-y)]$ of (134). As we have already remarked in Section 7.8, this is not the correct ring (that is, the smallest ring containing all Hamming enumerators of self-dual codes). In some cases ($q=4$ or $q=5$), we know a smaller ring; however, since the ring is no longer free, it is much more difficult to use. In particular, it is no longer the case that we may set the leading coefficients arbitrarily. This leads to the extremal enumerator not being unique, making it difficult to determine its first nonzero coefficient. Similarly, any attempt to make an analogous argument for families $4^{\mathbb{Z}}$ or $m^{\mathbb{Z}}$ will have the problem that, in those cases, we are primarily interested in Lee weight or Euclidean norm, forcing us to work with the symmetrized weight enumerator. This is, of course, much more difficult to deal with than the Hamming enumerator. A partial solution to this problem is provided by Theorem 34 below.

In each case it can be shown (cf. [193]) that the bounds of Theorems 26 and 28 can be met for at most finitely many n: in fact, the next coefficient ($A^*_{4\mu+8}$) *after* the leading nonzero coefficient in the extremal enumerator becomes negative for sufficiently large n. Furthermore, for any constant α, the minimal distance can be within α of the bound only finitely often. For Type II binary codes, for instance, it was shown in [193] that the A^*_{4n+8} term first goes negative when n is around 3720. Ma and Zhu [184] and Zhang [338] have recently determined precisely when the A^*_{4n+8} term first goes negative, and have obtained similar results for several other families. The following result incorporates the work of several authors.

Theorem 29. [338] *Let* C *be a self-dual code of length* n *from one of the families* 2_{I}, 2_{II}, 3, 4^{H}; *and let* $c=2,4,3,2$, *respectively, and* $\mu=[n/8]$, $[n/24]$, $[n/12]$, $[n/6]$. *Then the coefficient* $A^*_{c(\mu+2)}$ *in the extremal Hamming weight enumerator is negative if and only if:*

$$(2_{\mathrm{I}}): \quad n=8i\,(i\geq 4),\ 8i+2\,(i\geq 5),\ 8i+4\,(i\geq 6),\ 8i+6\,(i\geq 7);$$
$$(2_{\mathrm{II}}): \quad n=24i\,(i\geq 154),\ 24i+8\,(i\geq 159),\ 24i+16\,(i\geq 164);$$
$$(3): \quad n=12i\,(i\geq 70),\ 12i+4\,(i\geq 75),\ 12i+8\,(i\geq 78);$$
$$(4^{\mathrm{H}}): \quad n=6i\,(i\geq 17),\ 6i+2\,(i\geq 20),\ 6i+4\,(i\geq 22).$$

In particular, the first time $A^*_{4\mu+8}$ *goes negative for Type II codes is at* $24\times 154=3696$.

Of course other coefficients in the extremal weight enumerator may go negative before this. In the case of ternary self-dual codes, for example, family 3, the extremal Hamming weight enumerator contains a negative coefficient for lengths 72, 96, 120 and all $n \geq 144$.

The best asymptotic bound presently known for Type II codes is the following.

Theorem 30. (Krasikov and Litsyn [173].) *The minimal distance d of a Type II binary code of length n satisfies*

$$d \leq 0.166315\ldots n + o(n), \quad n \to \infty .$$

The constant in this expression is the real root of $8x^5 - 24x^4 + 40x^3 - 30x^2 + 10x - 1$.

The proof uses a variant of the linear programming bound.

For Type I binary codes, the bound of Theorem 28 is especially weak. Ward [319] has shown that the minimal distance can be $2[n/8] + 2$ precisely when n is one of 2, 4, 6, 8, 12, 14, 22 or 24. This suggests that the bound can be greatly strengthened, which is indeed the case. Conway and Sloane [69] showed that $d \leq 2[(n+6)/10]$ for $n > 72$, and Ward ([322], see also Chapter "Ward") established $d \leq n/6 + O(\log n)$. It turns out, in fact, that the "correct" bound is $4[n/24] + 4$ (except when $n + 2$ is a multiple of 24), just as for Type II codes. The key to proving this fact is the observation that we have not yet used the shadow enumerator.

Theorem 31. (Rains [250].) *Suppose C is a $[n, n/2, d]$ self-dual binary code. Then $d \leq 4[n/24] + 4$, except when $n \equiv 22 \pmod{24}$, when $d \leq 4[n/24] + 6$. If n is a multiple of 24, any code meeting the bound is of Type II. If $n \equiv 22 \pmod{24}$, any code meeting the bound can be obtained by shortening a Type II code of length $n + 2$ that also meets the bound.*

Proof (sketch). From (95), $W(x, y)$ lies in the ring $\mathbb{C}[x^2 + y^2, x^2y^2(x^2 - y^2)^2]$; consequently we can write

$$\begin{aligned} W(1, y) &= \sum_j a_j y^{2j} \\ &= \sum_i c_i (1 + y^2)^{n/2-4i} (y^2(1 - y^2)^2)^i. \end{aligned}$$

Applying the shadow transform, we have

$$\begin{aligned} S(1, y) &= \sum_j b_j y^{2j+t} \\ &= \sum_i c_i (2y)^{n/2-4i} (-(1 - y^4)/2)^i, \end{aligned}$$

where $t = ((n/2) \bmod 4)$. Suppose C had minimal distance $4[n/24]+6$. This fact determines c_i for $0 \le i \le 2[n/24]+2$, and in particular $c_{2[n/24]+2}$. On the other hand, we can also express $c_{2[n/24]+2}$ as a linear combination of the b_j for small j. It turns out that these two expressions for $c_{2[n/24]+2}$ are incompatible; in particular, we find that a certain nonnegative linear combination of the b_j is negative.

Rather than give the (somewhat messy) details of the proof, we will simply show how one can compute the coefficients in these linear combinations. This uses the Bürmann-Lagrange theorem:

Theorem 32. (Bürmann-Lagrange.) *Let $f(x)$ and $g(x)$ be formal power series, with $g(0) = 0$ and $g'(0) \neq 0$. If coefficients κ_{ij} are defined by*

$$x^j f(x) = \sum_{0 \le i} \kappa_{ij} g(x)^i,$$

then

$$\kappa_{ij} = \frac{1}{i}[\textit{coeff. of } x^{i-1} \textit{ in } [jx^{j-1}f(x) + x^j f'(x)] \left(\tfrac{x}{g(x)}\right)^i].$$

For proof and generalizations, see [327, p. 133], [106], [273], [274], [275].

For instance, to compute $c_{2[n/24]+2}$, we note that

$$\sum_i c_i (1+y^2)^{n/2-4i} (y^2(1-y^2)^2)^i = 1 + O(y^{4[n/24]+6}).$$

Dividing both sides by $(1+y^2)^{n/2}$ and substituting $y = \sqrt{Y}$, we get:

$$\sum_i c_i \left(\frac{Y(1-Y)^2}{(1+Y)^4}\right)^i = (1+Y)^{-n/2} + O(Y^{2[n/24]+3}).$$

We can then apply Bürmann-Lagrange, with

$$f(Y) = (1+Y)^{n/2}, \quad g(Y) = Y(1-Y)^2(1+Y)^{-4}$$

to obtain

$$\begin{aligned} c_i &= \frac{1}{i}[\text{coeff. of } Y^{i-1} \text{ in } [\tfrac{d}{dY}(1+Y)^{-n/2}] \left((1+Y)^4(1-Y)^{-2}\right)^i] \\ &= \frac{-n}{2i}[\text{coeff. of } Y^{i-1} \text{ in } (1+Y)^{-n/2-1+4i}(1-Y)^{-2i}] \\ &= \frac{-n}{2i}[\text{coeff. of } Y^{i-1} \text{ in } (1+Y)^{-n/2-1+6i}(1-Y^2)^{-2i}]. \end{aligned}$$

In particular, for $i = 2[n/24]+2$,

$$c_{2[n/24]+2} = \frac{-n}{4[n/24]+4}[\text{coeff. of } Y^{2[n/24]+1} \text{ in } (1+Y)^{-n/2+12[n/24]+11}(1-Y^2)^{-4[n/24]-4}].$$

It follows that $c_{2[n/24]+2} \leq 0$, with equality only when $n \equiv 22 \pmod{24}$, since all coefficients of any power series of the form $(1+Y)^a(1-Y^2)^{-b}$ are positive whenever $a, b > 0$.

Similarly, we find that the coefficients of the expansion of $c_{2[n/24]+2}$ in terms of the b_j are positive. This proves the bound, except when $n \equiv 22 \pmod{24}$; the proof that the bound holds in that case and that a code meeting the bound is even if $n \equiv 0 \pmod{24}$ is left to the reader. ∎

This bound agrees with the full linear programming bound for $n \leq 200$, and, most likely, for much larger n. However, it is likely that again it can only be attained for finitely many n.

There is also an analogue of this bound for Type I codes from family $4^{\mathrm{H}+}$.

Theorem 33. *If C is an additive self-dual code of length n and minimal distance d from family $4^{\mathrm{H}+}$, then $d \leq 2[n/6]+2$, except when $n \equiv 5 \pmod{6}$), when $d \leq 2[n/6]+3$. If n is a multiple of 6, then any code meeting the bound is even.*

We will call a code *extremal* if it meets the strongest of the applicable bounds from Theorems 28, 31, and 33. For Type II binary codes, ternary codes, and linear codes over $GF(4)$ this agrees with the historical usage. For Type I binary codes, however, "extremal" has generally been used to mean a code meeting the much weaker bound of Theorem 28; in the light of Theorem 31, it seems appropriate to change the definition.

Concerning codes over $\mathbb{Z}_4$, Bonnecaze, Solé, Bachoc and Mourrain [27] show:

Theorem 34. *Suppose C is a Type II self-dual code over $\mathbb{Z}_4$ of length n. Then the minimal Euclidean norm of C is at most*

$$8\left\lfloor \frac{n}{24} \right\rfloor + 8 \ . \tag{165}$$

The proof uses C to define an even unimodular n-dimensional lattice $\Lambda(C) = \{\frac{1}{2}u \in \mathbb{R}^n : u \pmod{4} \in C\}$, and examines its theta series.

As usual, one can derive an analogue for Type I codes:

Theorem 35. [256] *Suppose C is a Type I self-dual code over $\mathbb{Z}_4$ of length n. The minimal Euclidean norm of C is at most*

$$8\left\lfloor \frac{n}{24} \right\rfloor + 8 \ , \tag{166}$$

except when $n \equiv 23 \pmod{24}$, in which case the bound is

$$8\left\lfloor \frac{n}{24} \right\rfloor + 12 \ . \tag{167}$$

If equality holds in (167) then C is a shortened version of a Type II code of length $n+1$.

We say that codes meeting either of these bounds are *norm-extremal*. For Type II codes this agrees with the definition given in [27].

There should be an analogous concept of *Lee-extremal*, but at present we do not know what this is. Of course, the bounds (166) and (167) also apply to Lee weight. But this is not a satisfactory bound, since it is not even tight at length 24, where the highest attainable Lee weight is 12 rather than 16 (see Table XVI).

The fact that, from Theorem 31, an extremal binary code of length a multiple of 24 must be doubly-even suggests that these codes are likely to be particularly nice. Indeed, we have the following result, which is a consequence of the Assmus-Mattson theorem (see [190, Chap. 6], Theorem 11.14 of Chapter 1, Section 5 of Chapter xx (Tonchev)).

Theorem 36. *Let C be an extremal binary code of length $24m$. Then the codewords of C of any given weight form a 5-design.*

Similarly, the supports of the minimal codewords of an extremal ternary code of length $12m$ form a 5-design. For codewords of larger weight, the natural incidence structure is *almost* a 5-design, except that it may have repeated blocks. Similarly, for an extremal additive code over $\mathbb{F}_4$ of length $6m$, the supports with multiplicities of the codewords of any fixed weight form a 5-design with repeated blocks. Harada [125] has shown that the $\mathbb{Z}_4$-lift of the Golay code g_{24} also yields 5-designs. More generally, one can show that the words of any fixed symmetrized type, in any of the 13 Lee-optimal self-dual codes of length 24 over $\mathbb{Z}_4$, form a colored 5-design, possibly with repeated blocks [25]. See also [217].

10. Lower bounds

There are two ways to obtain lower bounds on the optimum minimal distance of a code of length n. The first way, naturally, is simply to construct a good code. Just as for general linear codes, there is also a nonconstructive lower bound, analogous to the Gilbert-Varshamov bound (cf. Theorems 3.1, 3.4, 3.5 of Chapter 1).

We first consider the case of self-dual binary codes (family 2).

Theorem 37. [299], [191] *Let n be any positive even integer. Let d_{GV} be the largest integer such that*

$$\sum_{\substack{0<i<d \\ 2|i}} \binom{n}{i} < 2^{n/2-1} + 1. \tag{168}$$

Then there exists a self-dual binary code of length n and minimal distance at least d_{GV}.

Proof If we can show that the expected number of nonzero vectors of weight less than d_{GV} in a *random* self-dual code of length n is less than 1, it will immediately follow that there exists *some* self-dual code of length n with no such vectors.

Let us therefore compute the average weight enumerator of the set of self-dual codes. Consider the group G of binary matrices that preserve the quadratic form I. On the vector space of even weight vectors, modulo the all 1's vector, the quadratic form becomes symplectic, and the group acts as the full symplectic group. In particular, it is therefore transitive on nonzero vectors of even weight, modulo 1^n. It follows that the expected number of vectors of weight $2i$ in a random code must be proportional to $\binom{n}{2i}$, except for $i = 0$ or $i = n/2$. Thus the average weight enumerator has the form:

$$\begin{aligned}\overline{W}(x,y) &= ax^n + b\sum_{1\le i\le n/2-1}\binom{n}{2i}x^{n-2i}y^{2i} + cy^n \\ &= ax^n + cy^n + b(\frac{1}{2}(x+y)^n + \frac{1}{2}(x-y)^n - x^n - y^n).\end{aligned}$$

Since every self-dual binary code contains the 0 vector and the all 1's vector, $\overline{W}(1,0) = \overline{W}(0,1) = 1$; since every self-dual code contains a total of $2^{n/2}$ vectors, $\overline{W}(1,1) = 2^{n/2}$. Solving for a, b, and c, we find:

$$\overline{W}(x,y) = x^n + y^n + \frac{1}{2^{n/2-1}+1}\sum_{1\le i\le n/2-1}\binom{n}{2i}x^{n-2i}y^{2i}\ .$$

Thus the average number of nonzero vectors of weight less than d is

$$\frac{1}{2^{n/2-1}+1}\sum_{\substack{0<i<d\\ 2|i}}\binom{n}{i}. \quad \blacksquare$$

Corollary 2. [299], [191] *There exists an infinite sequence of self-dual $[n_i, n_i/2, d_i]$ binary codes, such that n_i tends to infinity, and*

$$\liminf_{i\to\infty}\frac{d_i}{n_i} \ge \delta,$$

where $\delta \sim .11002786$ is the unique solution less than $\frac{1}{2}$ of

$$H_2(\delta) = -\delta\log_2(\delta) - (1-\delta)\log_2(1-\delta) = \frac{1}{2}.$$

Proof. Take the logarithm of both sides of (168), divide by n, and let n tend to infinity. The resulting inequality is

$$H_2(\delta) \leq \frac{1}{2},$$

as desired. ∎

Similar results hold if one restricts ones attention to codes of Type II:

Theorem 38. [299], [191] *Let n be any positive multiple of 8. Let d_{GV} be the largest integer such that*

$$\sum_{\substack{0<i<d \\ 4|i}} \binom{n}{i} < 2^{n/2-2} + 1 \tag{169}$$

Then there exists a doubly-even self-dual binary code of length n and minimal distance at least d_{GV}.

Proof. Again we compute the average weight enumerator. The key observation is that the function $\frac{1}{2}wt(v)$ induces a quadratic form on the space of even weight vectors modulo the all 1's vector. The group of matrices that preserve this quadratic form is transitive on the kernel of this quadratic form; that is, vectors of weight divisible by 4, modulo 1^n. This allows us to write down the average weight enumerator:

$$\overline{W}_{II}(x,y) = x^n + y^n + \frac{1}{2^{n/2-2}+1} \sum_{0<i<n/4} \binom{n}{4i} x^{n-4i} y^{4i}.$$ ∎

Asymptotically, this agrees with Corollary 2 (as well as the Gilbert-Varshamov bound). For finite n, it is actually (slightly) stronger! That is, the constraint that the code be Type II makes it easier to find good codes.

Similar arguments prove:

Theorem 39. *In each family from the list $2_{\rm I}$, $2_{\rm II}$, 3, $4^{\rm H}$, $4^{\rm E}$, $4_{\rm I}^{\rm H+}$, $4_{\rm II}^{\rm H+}$, $q^{\rm H}$ and $q^{\rm E}$ there exists a sequence of self-dual codes with length tending to infinity satisfying*

$$\liminf_{i\to\infty} \frac{d_i}{n_i} \geq \delta,$$

where

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta)\log_q(1-\delta) = \frac{1}{2}.$$

The result for families $q^{\rm H}$ and $q^{\rm E}$ was first given by Pless and Pierce [240].

Similar results hold for self-dual codes over $\mathbb{Z}_4$:

Theorem 40. *There exists a family of Type II self-dual codes over $\mathbb{Z}_4$, with length tending to infinity, such that*

$$\liminf_{i\to\infty} \frac{l_i}{2n_i} \geq \delta,$$

where l_i is the minimal Lee weight of the ith code and $\delta = H_2^{-1}(1/2)$, as before.

Theorem 41. *There exists a family of Type II self-dual codes over $\mathbb{Z}_4$, with length tending to infinity, such that*

$$\liminf_{i\to\infty} \frac{N_i}{n_i} \geq .34737283\ldots,$$

where N_i is the minimal Euclidean norm of the ith code.

11. Enumeration of self-dual codes

11.1. Gluing theory

Gluing is a technique for building up self-dual codes from smaller codes, and is especially useful when one is attempting to classify all self-dual codes of a given length. Typically one finds that there are many codes with low minimal distance and only a few with high minimal distance. Gluing theory is good at finding all the codes of low distance.

The first formal description of gluing theory appeared in [62]. It has also been used in [64], [70], [71], [180], [181], etc.

The theory applies to codes from any of the families that we have discussed in this chapter. Let $C_1, \ldots, C_t$ be self-orthogonal codes of lengths $n_1, \ldots, n_t$ with generator matrices $G_1, \ldots, G_t$. If C is a self-dual code with the generator matrix shown in Fig. 1 then we say that C is formed by *gluing* the *components* $C_1, \ldots, C_t$ together, and we write

$$C = (C_1 C_2 \ldots C_t)^+ \tag{170}$$

to indicate this process. (Whenever possible the subcodes are chosen so that every minimal weight codeword of C belongs to one of the C_i.) The codewords in C which contain a nonzero linear combination of the rows of the matrix X are called *glue words*, since these hold the components together. A glue word has the form

$$u = u_1 u_2 \ldots u_t \ , \tag{171}$$

where each glue element u_i has length n_i. Since C is self-dual, u_i is in $C_i^{\perp}$.

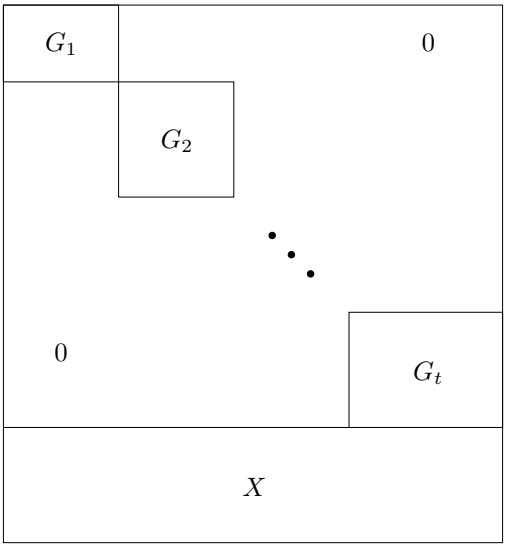

Figure 1: Generator matrix G for a code formed by gluing components $C_1, \ldots, C_t$ together. G_i is a generator matrix for C_i, and X denotes the rest of the generator matrix for C.

Let us choose coset representatives $a_0 = 0, a_1, \ldots, a_{s-1}$ for C_i in $C_i^{\perp}$, where $s = |C_i^{\perp}|/|C_i|$, so that

$$C_i^{\perp} = \bigcup_{j=0}^{s-1} (a_j + C_i) \ .$$

Then we can assume that each u_i in (171) is one of $a_0, \ldots, a_{s-1}$.

As illustrations we give the two indecomposable binary Type I self-dual codes of length 18 (see Tables II and VI), using the components from the list in Section 11.3. The first code is formed by gluing three copies of the component d_6 together:

1111 1111		
	1111 1111	
		1111 1111
010101 010110 000011	000011 010101 000011	010110 000011 000011

(172)

The three glue vectors shown are *abc*, *cab* and *bbb*.

The second code is formed by gluing together d_{10}, e_7 and a "free" (or empty) component

f_1:

1111 1111 1111 1111		
	1110100 0111010 0011101	
0101010101 0101010110	0000000 1111111	1 0

(173)

The two glue vectors shown are $a0A$ and $cd0$.

Of course a self-*dual* code has no (nonzero) glue. If a self-orthogonal code C has a component B, say, which is self-dual, then C is a direct sum $C = B \oplus C'$, where C' is again self-orthogonal.

It may happen that there is a glue word in which only one u_i is nonzero, in which case we say that the component C_i has *self-glue*, and that u is a *self-glue vector*. So if C has a single component C_1 (say) with self-glue, we write $C = C_1^+$ (compare (170)).

A basic result of gluing theory is the following.

Theorem 42. *If a self-dual code C is formed by gluing together two codes C_1 and C_2 in such a way that there is no self-glue, then the quotient groups $C_1^\perp/C_1$ and $C_2^\perp/C_2$ are isomorphic.*

We omit the easy proof. The isomorphism is given by $u_1 + C_1 \to u_2 + C_2$ whenever there is a glue vector $u_1 u_2$.

11.2. Automorphism groups of glued codes

One advantage of the gluing method is that it makes it much easier to find the automorphism group of a self-dual code C. We will denote the group by $G(C)$ rather than $Aut(C)$ in this section. It is essential that every automorphism of C takes the set of component codes $C_1, \ldots, C_t$ to itself. We will always choose the components so that this is true.

This being the case, any automorphism in $G(C)$ will effect some permutation of the C_i, so that $G(C)$ will have a normal subgroup G_{01} consisting of just those elements for which this permutation is trivial. The group of permutations of the components that are realized in this way we call $G_2(C)$ — it is isomorphic to the quotient group $G(C)/G_{01}$.

Let $G_0(C)$ be the normal subgroup of G_{01} consisting of those automorphisms which, for every i, send each glue element u_i into a vector in the same coset $u_i + C_i$, i.e. which fix the glue elements modulo the components. Then $G_{01}/G_0(C)$ is isomorphic to a group acting on

Table I: Numbers of self-dual codes of length n. (a) Indecomposable Type II, (b) total Type II, (c) indecomposable self-dual, (d) total self-dual.

n	0	2	4	6	8	10	12	14	16
a	1	–	–	–	1	–	–	–	1
b	1	–	–	–	1	–	–	–	2
c	1	1	0	0	1	0	1	1	2
d	1	1	1	1	2	2	3	4	7

n	18	20	22	24	26	28	30	32
a	–	–	–	7	–	–	–	74
b	–	–	–	9	–	–	–	85
c	2	6	8	26	45	148	457	
d	9	16	25	55	103	261	731	

the glue elements of each component: we call this group $G_1(C)$. Thus the full group $G(C)$ is compounded of the groups $G_0(C)$, $G_1(C)$ and $G_2(C)$, and has order

$$|G(C)| = |G_0(C)||G_1(C)||G_2(C)| \ . \tag{174}$$

Also $G_0(C)$ is the direct product of the groups $G_0(C_i)$. But in general $G_1(C)$ is only a subgroup of the direct product of the $G_1(C_i)$, and therefore must be computed directly for each C.

11.3. Family 2: Enumeration of binary self-dual codes

The enumeration of binary self-dual codes of length $n \leq 32$ has been carried out in a series of papers: Pless [229] for $n \leq 20$; Conway (unpublished) for Type II of length 24; Pless and Sloane [242] for $n = 22$, 24; Conway and Pless [62] for $n = 26$ to 30 and Type II of length 32 (see also Pless [232]). Some errors in the last two references were corrected in Conway, Pless and Sloane [65]. The results are summarized in Table I.

In this section we describe these codes, drawing heavily from the tables in [65].

Since (from (4)) there are at least 17493 inequivalent Type II codes of length 40, length 32 is probably a good place to stop.

Although the Type I codes of length 32 have not been classified, it is shown in [69] that there are precisely three inequivalent $[32, 16, 8]$ extremal Type I codes.

The following self-orthogonal codes will be used as components.

$d_4 : [1111]$, glue: $a = 0011$, $b = 0101$, $c = 0110$, $|G_0| = 4$, $G_1 = S(3)$ on $\{a, b, c\}$, $|G_1| = 6$.

$d_{2n} (n \geq 3)$:

$$[111100\ldots, 00111100\ldots, \ldots, \ldots 001111] \ , \tag{175}$$

glue: $a = 0101\ldots01$, $b = 0000\ldots11$, $c = 0101\ldots10$, $|G_0| = 2^{n-1}n!$, $|G_1| = 2$ (swap a and c)

$e_7 : [(1110100)]$, glue: $a = 1111111$, $G_0 = L_3(2)$, $|G_0| = 168$, $|G_1| = 1$.

e_8 is the $[8, 4, 4]$ Hamming code, see Section 3.2.

f_n : If some coordinate positions contain very few codewords, it is often best to regard these places as containing the *free* (or *empty*) *component* $f_n = \{0^n\}$. In this case we label the coordinate positions by A, B, $C, \ldots$, and use ABD for example to denote the glue word $110100\ldots$. Also $|G_0| = 1$.

The above components are important in view of the following decomposition theorem for binary codes with low minimal distance.

Theorem 43. *(a) If a self-orthogonal code C has minimal distance 2 then $C = i_2^k \oplus C'$, where C' has minimal distance at least 4. (b) If a self-orthogonal code C is generated by words of weight 4 then C is a direct sum of copies of the codes d_{2m} $(m \geq 2)$, e_7 and e_8.*

Proof. (a) Suppose C contains a word of weight 2, say $u = 1100\ldots$. Then any other word $v \in C$ must meet u evenly, so begins $00\ldots$ or $11\ldots$. Hence $C = B \oplus C'$ where $B = [11]$. (b) A set of mutually self-orthogonal words of weight 4 whose supports are linked is easily seen to be either a d_{2m} for some $m \geq 2$, or an e_7 or e_8. ∎

Remarks. (1) Suppose C is a self-dual code with minimal distance 4, and let C' be the subcode generated by words of weight 4. Then C' is as described in part (b) of the theorem, and C can be regarded as being obtained by gluing C' to some other subcode C'' (the latter may be the free component f_n).

(2) Generalizing Part (a) of the theorem, it is easy to show that any self-orthogonal code over a field $\mathbb{F}_q$ with length $n > 2$ and minimal distance 2 is decomposable ([64], Theorem 3).

The following are some additional components that will be used in Table II.

The code g_{24-m} $(m = 0, 2, 3, 4, 6, 8)$ is obtained by taking the words of the Golay code g_{24} that vanish on m digits (and then deleting those digits). For the [16,5,8] first-order Reed-Muller code g_{16} the 8 digits must be a special octad, while for g_{18} they must be an umbral hexad (see [70] for terminology). For $0 \leq m \leq 6$, g_{24-m} is a $[24 - m, 12 - m, 8]$ code.

The [24,11,8] *half-Golay code* h_{24} consists of the Golay codewords that intersect a given tetrad evenly.

The *odd Golay code* h_{24}^+ is the $[24, 12, 6]$ Type I code generated by h_{24} and an appropriate

vector of weight 6. Alternatively, the odd Golay code may be obtained as follows. Let $v \in \mathbb{F}_2^{24}$ be a fixed vector of weight 4, say $v = 1^4 0^{24}$. Then $h_{24}^+ = \{u \in g_{24} : wt(u \cap v) \text{ even}\} \bigcup \{u + v : u \in g_{24}, wt(u \cap v) \text{ odd}\}$, with generator matrix

1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	1	0	1	0
0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	0	1	1	0	0	1	0	1	0
0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	1	0	0
1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1
0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	1	1	0	1	0	1	0	0	1
0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	1	0	0	1	1	0	1	0
1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0

This code has weight enumerator $x^{24}+64x^{18}y^6+375x^{16}y^8+960x^{14}y^{10}+1296x^{12}y^{12}+960x^{10}y^{14}+375x^8y^{16}+64x^8y^{18}+y^{24}$, and $Aut(h_{24}^+)$ is the "sextet group" $2^6{:}3.S(6)$, of order $2^{10}.3^3.5 = 138240$ ([242], [70, p. 309]).

The first 11 rows of the above matrix generate h_{24}; if the last row is replaced by

0	1	1	1	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0

we get the Golay code g_{24} itself; and if the last row is replaced by

1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

we get $(d_4^6)^+$.

Under the action of $Aut(g_{24})$ there are two distinct ways to select tetrads $t = \{c, d, e, f\}$, $u = \{a, b, e, f\}$, $v = \{a, b, c, d\}$ so that $t + u + v = 0$, depending on whether $\{a, b, \ldots, f\}$ is a special hexad or an umbral hexad (see Fig. 2). Correspondingly there are two [24,10,8] *quarter-Golay codes* q_{24}^+, q_{24}^-, consisting of the codewords of g_{24} that intersect all of t, u, v evenly.

We refer to [62] and [65] for a description of the glue vectors for these codes.

Our first table (Table II) lists all indecomposable binary self-dual codes of length $n \leq 22$, together with the indecomposable Type II codes of length 24, using the + notation of (170). For these codes (and for most of those in the following tables) there is only one way to glue the specified components together without introducing additional minimal-weight words. We have therefore omitted the glue words from the table. (However, more information about these codes, including the glue words, will be given in Table VI.)

Figure 2: Two choices for a hexad (special or umbral), used to define the two $[24, 10, 8]$ quarter-Golay codes q_{24}^{+} and q_{24}^{-}.

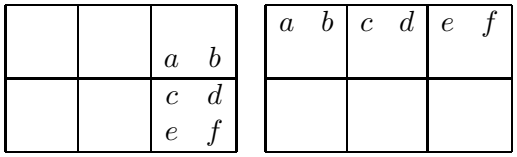

Table II: Indecomposable binary self-dual codes of length $n \le 24$ (§ indicates a Type II code. For length 24 only Type II codes are listed).

Length n	Components
2	i_2
8	$e_8^{\S}$
12	d_{12}^{+}
14	e_7^{2+}
16	$d_{16}^{\S}, d_8^{2+}$
18	$(d_{10}e_7f_1)^{+}, d_6^{3+}$
20	$d_{20}^{+}, (d_{12}d_8)^{+}, (d_8^2d_4)^{+}, (e_7^2d_6)^{+}, (d_6^3f_2)^{+}, d_4^{5+}$
22	$g_{22}^{+}, (d_{14}e_7f_1)^{+}, (d_{10}^2f_2)^{+}, (d_{10}d_6^2)^{+}, (d_8e_7d_6f_1)^{+}$, $(d_8d_6^2f_2)^{+}, (d_6^2d_4^2f_2)^{+}, (d_4^4f_3^2)^{+}$
$24^{\S}$	$g_{24}, d_{24}^{+}, d_{12}^{2+}, (d_{10}e_7^2)^{+}, d_8^{3+}, d_6^{4+}, d_4^{6+}$

The next table (Tables III and IV) gives the full list of all 85 (decomposable or indecomposable) Type II codes of length 32. This table is taken from [65], and is a corrected version of the table in [62]. The codes are labeled from C1 to C85 in the first column (using the same order as in [62] and [65]). The second column gives the components (omitting the superscripts "+" to save space).

The third and fourth columns give the orders of the groups $G_1(C)$ and $G_2(C)$, and the fifth column gives the order of the full group, using (174), where $|G_0(C)|$ is the product of the orders of the $G_0(C_i)$ for the components. The latter are given in Table V. The next column gives A_4, the number of codewords of weight 4. The weight enumerator of the code is then (from Theorem 13)

$$(x^8 + 14x^4y^4 + y^8)^4 - (56 - A_4)x^4y^4(x^4 - y^4)^4(x^8 + 14x^4y^4 + y^8) \ .$$

The last four columns give the number of self-dual codes (the "children", cf. Chapter xx (Pless)) of lengths 30, 28, 26, 24 that arise from the code.

To save space, we have omitted the glue vectors from Tables III and IV. In many cases

they are uniquely determined by the components, and in any case they can be found in full in [62], with corrections in [65].

The enumeration in Tables III and IV has been subjected to many checks, including the verification of the mass formula

$$\sum \frac{1}{|Aut(C)|} = \frac{391266122896364123}{532283035423762022400}$$

(in agreement with (4)).

Remark. There are just five Type II codes of length 32 with minimal distance 8: the quadratic residue code $C81 = q_{32}$, generated by

$$(10010001101101111000101011100 00)1 \ ;$$

the second-order Reed-Muller code $C82 = r_{32}$, generated by

$$(11100100000100000011000000000000)1 \ ;$$

and the three codes $C83 = g_{16}^{2+}$, $C84 = f_4^{8+}$ and $C85 = f_2^{16+}$. Explicit generator matrices for the last three are shown in Fig. 3.

Subtraction. Suppose for concreteness that C is a Type I code of length 26 with doubly even subcode C_0. Then we obtain a Type II code B (say) of length 32 by gluing C_0 to d_6, as follows. Write $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$, as in Section 5, where $C = C_0 \cup C_2$, the shadow of C is $C_1 \cup C_3$, and $C_i = u_i + C_0$ for $i = 1, 2, 3$. Then B is generated by

C_0	
	d_6
u_1	a
u_2	b
u_3	c

(176)

This is a special case of the following construction. Let C, D be any strictly Type I codes, of lengths n_1 and n_2, respectively, with $C_0^\perp = \cup_{i=0}^3 C_i$, $D_0^\perp = \cup_{i=0}^3 D_i$. Then $B = \cup_{i=0}^3 C_i \times D_i$ is self-dual if $n_1 + n_2 \equiv 0 \pmod 4$, and is Type II if $n_1 + n_2 \equiv 0 \pmod 8$. The weight enumerator of B is then

$$\sum_{i=0}^{3} W_{C_i}(x, y) W_{D_i}(x, y) \ .$$

Several constructions in the literature ([35], Theorems 1 and 2; [83], Theorem 3.1, for example) are special cases of this construction. In (176) we have $D = i_2^3$.

In this way any Type I code of length 26 leads to a unique (up to equivalence) Type II code of length 32.

Conversely, all Type I codes of length 26 can be obtained by choosing a d_6 inside a Type II code of length 32 and inverting the above process.

More generally, suppose B is a Type II code of length n. We choose a copy of $D = i_2^m$ so that $D_0 = d_{2m} \subset B$. Then we obtain a Type I code of length $n - 2m$ by taking the vectors v such that $vw \in B$ for some $w \in D$. We call this process *subtraction*. Every Type I code of length $n - 2m$ can be obtained in this way by starting with a unique Type II code and subtracting an appropriate d_{2m}. Of course any Type II code of length $n - 2m$ is a direct summand of some Type II code of any greater length.

Table VI shows all (decomposable or indecomposable) codes of lengths $n \leq 22$ with minimal distance $d \geq 4$, as obtained by subtracting suitable codes d_{2m} from one of the codes in Tables III and IV. The second column indicates the parent code in Tables III and IV and the d_{2m} to be subtracted. The next two columns gives the components, with a § to indicate a Type II code, and the name (if any) given to this code in [229] or [242]. The remaining columns give the orders of the glue groups G_1 and G_2, the weight distribution, and generators for the glue.

Table VII gives the self-dual codes (both Type I and Type II) of length 24 and minimal distance $d \geq 4$.

A complete list of all Type I or Type II self-dual codes of lengths $n \leq 24$ can be obtained by forming direct sums of the codes in Tables VI and VII in all possible ways with the codes i_2^m $(m = 0, 1, \ldots)$.

There are over 1000 self-dual codes of lengths 26–30 (see Table I, [62], [65]). The highest minimal distance is 6, and there are respectively 1, 3 and 13 codes with $d = 6$ of lengths 26, 28 and 30.

11.4. Family 3: Enumeration of ternary self-dual codes

Ternary self-dual codes of lengths $n \leq 20$ (and the maximal self-orthogonal codes of lengths $n \leq 19$, $n \not\equiv 0 \pmod 4$) have been enumerated by Pless [227] and Mallows, Pless and Sloane [194] for $n \leq 12$, Conway, Pless and Sloane [64] for $n \leq 16$, and Pless, Sloane and Ward [243] for $n \leq 20$. Leon, Pless and Sloane [180] give a partial enumeration of the self-dual codes of length 24, making use of the complete list of Hadamard matrices of order 24, and show that there are precisely two codes with minimal distance 9 (cf. Table XII below).

We will make use of the following components.

e_3: [111], glue: $\pm a$, $a = 120$. If the coordinates are labeled 1, 2, 3 then G_0 is generated by $(1,2,3)$ and $(1,2)$ diag$\{-1,-1,-1\}$ and has order 6; $|G_1| = 2$.

t_4 is the $[4,2,3]_3$ tetracode, and g_{12} is the $[12,6,6]_3$ ternary Golay code, see Section 3.2.

g_{10} is the $[10,4,6]_3$ code consisting of the vectors u such that $00u \in g_{12}$. If x and y are chosen so that $11x \in g_{12}$, $12y \in g_{12}$, then the glue words for g_{10} can be taken to be $\pm x$, $\pm y$, $\pm x \pm y$. $|G_0| = 360$, $|G_1| = 8$.

p_{13}: Let $Q_0, Q_1, \ldots, Q_{12}$ be the points of a projective plane of order 3, labeled so that the 13 lines are represented by the cyclic shifts $t_0, t_1, \ldots, t_{12}$ of the vector t_0 given by

Q_0	Q_1	Q_2	Q_3	Q_4	Q_5	Q_6	Q_7	Q_8	Q_9	Q_{10}	Q_{11}	Q_{12}
1	1	0	1	0	0	0	0	0	1	0	0	0

([190], p. 695, [67]). The vectors $t_0, \ldots, t_{12}$ generate a $[13,7,4]_3$ code $p_{13}^{\perp}$. The dual is p_{13}, a $[13,6,6]_3$ self-orthogonal code consisting of the vectors $\sum_{i=0}^{12} a_i t_i$ with $a_i \in \mathbb{F}_3$ and $\sum a_i = 0$, and having weight distribution $A_0 = 1$, $A_6 = 156$, $A_9 = 494$, $A_{12} = 78$. $G_0(p_{13}) \simeq PGL_3(3)$, of order 5616, $|G_1(p_{13})| = 2$. The glue words are $\pm t_0$.

The indecomposable self-dual codes of lengths $n \leq 16$ are shown in Table VIII. H_8 denotes a suitably normalized version of the Hadamard matrix of order 8.

The analogue of Theorem 43 is: any self-orthogonal ternary code generated by words of weight 3 is a direct sum of copies of e_3 and t_4. A technique for classifying self-orthogonal codes generated by words of weight 6 (using "center sets") is given in [243].

11.5. Family 4^{H}: Enumeration of Hermitian self-dual codes over $\mathbb{F}_4$

These have been classified for lengths $n \leq 16$ [64] — see Table IX.

We will make use of the following components.

d_{2n} ($n \geq 2$): generated by (175). There are 16 cosets of d_{2n} in $d_{2n}^{\perp}$, and as glue words we choose 0, $\omega^\nu a$, $\omega^\nu b$, $\omega^\nu c$, $\omega^\nu d$, $\omega^\nu e$, $\nu \in \{0,1,2\}$, where

$$\begin{aligned} a &= 1010\ldots1010 \\ b &= 0000\ldots0011 \\ c &= 1010\ldots1001 \\ d &= 1010\ldots10\omega\overline{\omega} \\ e &= 1010\ldots10\overline{\omega}\omega \end{aligned}$$

Also $|G_0| = 2^{n-1}n!$, $|G_1| = 36$ ($n = 2$), or 12 ($n \geq 3$).

$e_5 : [\omega\overline{\omega}\overline{\omega}\omega 0, 0\omega\overline{\omega}\overline{\omega}\omega]$, glue: $\omega^\nu 1$, $\nu \in \{0, 1, 2\}$, $G_0 = A(5)$, of order 60, $|G_1| = 6$.

h_6 is the hexacode, $e_7 \otimes \mathbb{F}_4$, $e_8 \otimes \mathbb{F}_4$ are $\mathbb{F}_4$-versions of the Hamming codes in Sections 3.2, and 1_n is the $[n, 1, n]_4$ repetition code.

Remarks. (1) The group orders differ slightly form those in [64], since now we are allowing conjugation in the group.

(2) The dots and double-dots in the glue column indicate multiplication by ω or ω^2, respectively.

(3) The unique distance 6 code at length 14, q_{14}, is the $[14, 7, 6]_4$ extended quadratic residue code generated by

$$1(1\omega\overline{\omega}\omega\omega\overline{\omega}\overline{\omega}\overline{\omega}\overline{\omega}\omega\omega\overline{\omega}\omega) \ .$$

(4) The analogue of Theorem 43 is: (a) any self-orthogonal code with minimal distance 2 has i_2 as a direct summand; (b) any self-orthogonal code generated by words of weight 4 is a direct sum of copies of d_4, d_6, $d_8, \ldots$, e_5, h_6, e_7 and e_8.

11.6. Family 4^{E}: Enumeration of Euclidean self-dual codes over $\mathbb{F}_4$

Although even codes of length up to 14 were classified in [189], the odd codes do not seem to have been classified.

11.7. Family $4^{\mathrm{H}+}$: Enumeration of trace self-dual additive codes over $\mathbb{F}_4$

These have been classified up to length 7 (and Type II code up to length 8) in [49], [134].

The analogue of Theorem 43 is the following. Let d_n be the code of length n generated by all even-weight binary vectors ($n \geq 2$), and let $i_2 = [11, \omega\omega]$. Then any trace self-orthogonal additive code over $\mathbb{F}_4$ generated by words of weight 2 is a direct sum of copies of i_2, d_2, d_3, $d_4, \ldots$.

d_n^+ (mentioned in Table XIV) is the code of length n, containing 2^n words, generated by d_n and $\omega\omega\ldots\omega$.

11.8. Family $4^{\mathbb{Z}}$: Enumeration of self-dual codes over $\mathbb{Z}_4$

These have been classified for lengths up to 16 in the following papers: Conway and Sloane [71] for $n \leq 9$, Fields, Gaborit, Leon and Pless [95] for $n \leq 15$, and Pless, Leon and Fields [239] for Type II codes of length 16.

In this section we will present enough component codes to state the analogue of Theorem 43.

The smallest self-dual code is $i_1 = \{0, 2\}$. If a self-orthogonal code C contains a vector of the form $2^1 0^{n-1}$ then $C = i_1 \oplus C'$ is decomposable. The next-simplest possible vectors are "tetrads", of type $\pm 1^4 0^{n-4}$. We list a number of self-orthogonal codes that are generated by tetrads; t denotes the total number of tetrads in the code.

The first four codes have the property that the associated binary code $C^{(1)}$ is the self-dual code d_{2m} of (175).

$\mathcal{D}_{2m}$ ($m \geq 2$) is generated by the tetrads $11130\ldots0$, $0011130\ldots0$, $\ldots$, $0\ldots01113$; $|\mathcal{D}_{2m}| = 4^{m-1}$, $|Aut(\mathcal{D}_{2m})| = 2.4!$ ($m = 2$) or $2^2.2^m$ ($m > 2$), $t = 2(m-1)$. $\mathcal{D}_{2m}^{\perp}/\mathcal{D}_{2m}$ is a group of type 4^2 with generators $v_1 = 0101\ldots01$, $v_2 = 00\ldots0011$.

$\mathcal{D}_{2m}^{\mathrm{O}}$ ($m \geq 2$) is generated by $\mathcal{D}_{2m}$ and the tetrad $1300\ldots0011$ (or equivalently the vector $2020\ldots20$); $|\mathcal{D}_{2m}^{\mathrm{O}}| = 4^{m-1}2$, $|Aut(\mathcal{D}_{2m}^{\mathrm{O}})| = 2^2.8$ ($m = 2$) or $2.2^{m-1}.2m$ ($m > 2$), $t = 2m$. $(\mathcal{D}_{2m}^{\mathrm{O}})^{\perp}/\mathcal{D}_{2m}^{\mathrm{O}}$ is a cyclic group of order 4 generated by v_1 (if m is odd), or a 4-group generated by v_1 and $2v_2$ (if m is even).

$\mathcal{D}_{2m}^{+}$ ($m \geq 2$, but note that $\mathcal{D}_4^{+} \simeq \mathcal{D}_4^{\mathrm{O}}$) is generated by $\mathcal{D}_{2m}$ and $2v_2$; $|\mathcal{D}_{2m}^{+}| = 4^{m-1}2$, $|Aut(\mathcal{D}_{2m}^{+})| = 2^m.2^{m+1}$, $t = 4(m-1)$. $(\mathcal{D}_{2m}^{+})^{\perp}/\mathcal{D}_{2m}^{+}$ is a 4-group generated by $2v_1$ and v_2.

$\mathcal{D}_{2m}^{\oplus}$ ($m \geq 2$) is the self-dual code generated by $\mathcal{D}_{2m}^{\mathrm{O}}$ and $\mathcal{D}_{2m}^{+}$; $|\mathcal{D}_{2m}^{\oplus}| = 4^{m-1}2^2$, $|Aut(\mathcal{D}_{2m}^{\oplus})| = 2^3.4!$ ($m = 2$) or $2^m.2^m.2m$ ($m > 2$), $t = 4m$. For use in (158) we note that there are two permutation-inequivalent versions of $\mathcal{D}_4^{\oplus}$, with generator matrices

$$\text{(a)}\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}, \quad \text{(b)}\ \begin{bmatrix} 1 & 3 & 3 & 3 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{bmatrix}. \tag{177}$$

$\mathcal{D}_4^{\oplus}$ (in either version) has $swe = x^4 + 6x^2z^2 + z^4 + 8y^4$.

$\mathcal{E}_7$ is generated by 1003110, 1010031, 1101003; $|\mathcal{E}_7| = 4^3$, $|Aut(\mathcal{E}_7)| = 2.4!$, $t = 8$. $\mathcal{E}_7^{\perp}/\mathcal{E}_7$ is a cyclic group of order 4 generated by 3111111.

$\mathcal{E}_7^{+}$ is the self-dual code generated by $\mathcal{E}_7$ and 2222222 (or equivalently by all cyclic shifts of 3110100); $|\mathcal{E}_7^{+}| = 4^3 2$, $|Aut(\mathcal{E}_7^{+})| = 2.168$, $t = 14$, $swe = x^7 + z^7 + 14y^4(x^3 + z^3) + 7x^3z^3(x + z) + 42xy^4z(x + z)$. For both $\mathcal{E}_7$ and $\mathcal{E}_7^{+}$ the associated binary code $C^{(1)}$ is the Hamming code e_7.

$\mathcal{E}_8$ is the self-dual code generated by $0u$, $u \in \mathcal{E}_7$ and 30001011. An equivalent generator matrix has already been given in (40). $|\mathcal{E}_8| = 4^4$, $g = 8.2.4! = 384$, $t = 16$, $swe = x^8 + 16y^8 + z^8 + 16y^4(x^4 + z^4) + 14x^4z^4 + 48xy^4z(x^2 + z^2) + 96x^2y^4z^2$.

Theorem 44. *Any self-orthogonal code over $\mathbb{Z}_4$ generated by vectors of the form $\pm 1^4 0^{n-4}$ is equivalent to a direct sum of copies of the codes*

$$\mathcal{D}_{2m},\ \mathcal{D}_{2m}^{\mathrm{O}},\ \mathcal{D}_{2m}^{+},\ \mathcal{D}_{2m}^{\oplus}(m=1,2,\ldots),\ \mathcal{E}_7,\ \mathcal{E}_7^{+},\ \mathcal{E}_8\ .$$

The (somewhat complicated) inclusions between the codes mentioned in the theorem can be seen in Fig. 1 of [71].

12. Extremal and optimal self-dual codes

Recall from Section 9 that we have defined a self-dual code from any of the families 2 through q^{E} to be *extremal* if it meets the strongest of the applicable bounds from Theorems 28, 31 and 33, that is, if its minimal distance d is equal to

(2_{I}) $4\left[\frac{n}{24}\right]+4+\epsilon$, where $\epsilon=-2$ if $n=2$, 4 or 6, $\epsilon=2$ if $n\equiv 22 \pmod{24}$, and $\epsilon=0$ otherwise,

(2_{II}) $4\left[\frac{n}{24}\right]+4$,

(3) $3\left[\frac{n}{12}\right]+3$,

(4^{H}) $2\left[\frac{n}{6}\right]+2$,

(4^{E}) $\left[\frac{n}{2}\right]+1$,

$(4_{\mathrm{I}}^{\mathrm{H}+})$ $2\left[\frac{n}{6}\right]+2+\epsilon'$, where $\epsilon'=-1$ if $n=1$, $\epsilon'=1$ if $n\equiv 5 \pmod 6$, and $\epsilon'=0$ otherwise,

$(4_{\mathrm{II}}^{\mathrm{H}+})$ $2\left[\frac{n}{6}\right]+2$,

(q^{H}), (q^{E}) $\left[\frac{n}{2}\right]+1$.

We also defined a code over $\mathbb{Z}_4$ to be norm-extremal if its minimal norm is

$(4^{\mathbb{Z}})$ $8\left[\frac{n}{24}\right]+8+\epsilon''$

where $\epsilon''=4$ if $n\equiv 23 \pmod 4$, $\epsilon''=0$ otherwise.

It is very likely (although we do not have a proof) that the above bounds for families 2 through q^{E} are the highest minimal distance that is permitted by the pure linear programming bound applied to the Hamming weight enumerator and (when relevant) the shadow enumerator.

In contrast, we call a code *optimal* if it has the highest minimal distance of any self-dual code of that length. An extremal code is automatically optimal.

In this section we will summarize what is presently known about extremal and optimal codes in the families we are considering. Earlier summaries of extremal codes and lattices have appeared in Chapter 7 of [70], [147]. In the tables we have tried to list all known codes with the specified minimal distance (a period indicating that the list is complete), or else to indicate

how many extremal codes are known. Whenever possible we have attempted to name at least one extremal code.

12.1. Family 2: Binary codes

Type I codes meeting the $d \leq 2[n/8] + 2$ bound of Theorem 28 (the old definition of extremal) were completely classified by Ward [319] (finishing the work begun in [196], [229], [242]): such codes exist if and only if n is 2 (i_2), 4 (i_2^2), 6 (i_2^3), 8 (e_8), 12 (d_{12}^+), 14 (e_7^{2+}), 22 (g_{22}^+) or 24 (g_{24}) — compare Tables II and VI. In each case the code is unique.

However, there are many more Type I codes that are extremal in the new sense, and they have not yet been fully classified. It is known (Theorem 29) that extremal Type II codes do not exist for lengths ≥ 3952 and presumably a similar bound applies to extremal Type I codes.

Table X shows the highest possible minimal distance for binary self-dual codes of lengths $n \leq 72$. This is based on earlier tables in Fig. 19.2 of [190], [69] and [83]. In the table d_I (resp. d_{II}) denotes the highest minimal distance of any strictly Type I (resp. Type II) self-dual code.

Remarks on Table X

The fourth column of the table gives the known codes having the indicated minimal distance. As mentioned above, a period indicates that the lists of codes is complete. (The enumeration for lengths $n \leq 32$ has already been discussed in Section 11.3.) When n is a multiple of 8 a semicolon separates the Type I and Type II codes.

In the years since the manuscript of [69] was first circulated, a large number of sequels have been written, supplying additional examples of self-dual codes in the range of Table X. The bibliography includes all the manuscripts known to us, even though inevitably not all of them will be published. It was not possible to mention all these references in the table, so instead we list them here. This list also includes a number of older papers. Readers interested in extremal self-dual codes, especially of Type I, in the range of the table should therefore consult the following: [35], [38], [39], [40], [41], [42], [43], [81], [83], [84], [85], [86], [87], [107], [108], [109], [110], [111], [113], [118], [120], [121], [122], [129], [126], [127], [130], [139], [151], [152], [153], [157], [162], [219], [221], [234], [238], [247], [267], [268], [269], [305], [307], [309], [310], [311], [312], [332], [333], [334], [335], [336], [337].

Note that if we don't distinguish between Type I and Type II codes, but just ask what is the highest minimal distance of a binary self-dual code, then the answer is known for all

$n \leq 60$.

The symbol XQ_m in any of these tables indicates an extended quadratic residue code of length $m+1$. Both quadratic residue codes and double circulant codes provide many examples of good self-dual codes (cf. Section 12 of Chapter 1, Chapter xx (Ward), Chapter yy (Pless), [190, Chapter 16]). There are two basic types of binary double circulant codes, having generator matrices of the form

$$\left[\begin{array}{ccccc|ccccc} 1 & & & & & 0 & 1 & 1 & 1 & 1 \\ & 1 & & & & 1 & & & & \\ & & 1 & & & 1 & & R & & \\ & & & 1 & & 1 & & & & \\ & & & & 1 & 1 & & & & \end{array}\right] \tag{178}$$

or

$$\left[\begin{array}{ccccc|ccccc} 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & 1 & & & & & R & & \\ & & & 1 & & & & & & \\ & & & & 1 & & & & & \end{array}\right], \tag{179}$$

where R is a circulant matrix with first row r (say). (178) is used only when the length is a multiple of 4. Such codes and their generalizations to other fields have been studied by many authors, including [12], [15], [108]–[118], [147], [153], [158], [186], [187], [190, Chap. 16], [248], [267], [308], [317], [332]–[334]. Table XI, based on [69] and [204], gives a selection of double circulant binary codes. Code H86 (from [83]) is the shortest Type I self-dual code presently known with $d = 16$. The first column gives the name of the codes, following [69], and the last column gives r, the initial row of R, in hexadecimal. The codes marked $(*)$ are not necessarily optimal. The minimal distance of the last two codes in the table was determined by Moore [203], [204]. For these two codes r has 1's at the squares modulo 43 and 67, respectively. Moore remarked that the analogous code of length 168 *might* also have been extremal. However, Aaron Gulliver (personal communication, Nov. 1997) has shown that the minimal distance of this code is at most 28.

We see from Table X that there are extremal Type I codes (in the new sense) that are not also Type II codes at lengths

$$2, 4, 6, 12, 14, 16, 18, 20, 22, 32, 36, 38, 40, 42, 44, 46, 60, 64, 66, 68$$

that such codes do not exist at length

$$8, 10, 24, 26, 28, 30, 34, 48, 50, 52, 54, 58 \tag{180}$$

and that their existence at lengths

$$56, 62, 70, 72 \tag{181}$$

is at present an open question. The nonexistence of the Type I codes of lengths in (180) is established by imposing the extra condition that the shadow enumerator must have integral coefficients.

Concerning extremal Type II codes, with $d = 4[n/24] + 4$, these exist for the following values of n:

$$8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 136$$

but their existence at lengths 72 and 96 and all greater lengths is open. For lengths 8, 24, 32, 48, 80 and 104 we can use extended quadratic residue codes, and for lengths 40, 56, 64, 88, 136 we can use double circulant codes (see Table XI).

Only one $[48, 24, 12]$ code is presently known, XQ_{47}, which is generated by $\mathbf{1}$ and

$$1(011110111100101011100100110110001010110000010000)$$

(with 1's at the nonzero squares modulo 47). Huffman [139] has shown that any Type II $[48, 24, 12]$ code with a nontrivial automorphism of odd order is equivalent to XQ_{47}. Houghten, Lam and Thiel (cf. [136]) are attempting to establish by direct search that XQ_{47} is unique. As Table X shows, if $n \geq 40$ is congruent to 8 or 16 (mod 24) there are often large numbers of extremal codes. It is easy to find $[72, 36, 12]$ Type II codes, for example XQ_{71}; [83] shows that there are at least 33 inequivalent codes with these parameters.

Concerning the existence of self-dual codes with a specified minimal distance, the following results were established in [69]. Self-dual codes with minimal distance

$d \geq 6$ exist precisely for $n \geq 22$;

$d \geq 8$ exist precisely for $n = 24, 32$, and $n \geq 36$;

$d \geq 10$ exist precisely for $n \geq 46$;

$d \geq 12$ exist[7] for $n = 48$, 56, 60 and $n \geq 64$; perhaps for $n = 62$; and do not exist for all other values of n. (As pointed out in [69], the $[58, 29, 12]$ self-dual code claimed in [15] is an error.)

Dougherty, Gulliver and Harada [83], extending work in [69], show that codes with

[7]The existence of a $[70, 35, 12]$ was not known when [69] was written, but such a code was later found by Scharlau and Schomaker [276].

$d \geq 14$ exist for $n \geq 78$; perhaps for $n = 70$, 72, 74, 76; and do not exist for all other values of n;

$d \geq 16$ exist for $n = 80$, 86, 88, 96, 100–104, 112 and $n \geq 120$ (and possibly for other values of n).

12.2. Family 3: Ternary codes

Table XII shows the highest possible minimal distance for ternary self-dual codes of lengths $n \leq 72$.

Remarks on Table XII

For the entries at lengths $n \leq 24$, see the discussion in Section 11.4.

Extremal codes exist at lengths 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 56, 60 and 64. Extremal codes do not exist at lengths 72, 96, 120 and all $n \geq 144$, because then the extremal Hamming weight enumerator contains a negative coefficient. The existence of extremal codes in the remaining cases ($n = 52$, 68, 76, ..., 140) is undecided.

In Table XII, XQ_n denotes an extended quadratic residue code of length $n+1$, and $S(n)$ denotes a Pless double circulant (or "symmetry") code of length n (see Section 5 of Chapter "coding-constructions", [18], [19], [194], [228], [230]). A $[28, 14, 9]_3$ code was discovered by Cheng and R. Scharlau [58]. Another such code was given by Kschischang and Pasupathy [174], namely the negacyclic code generated by the polynomial $(x^2+x-1)(x^6-x^4+x^3+x^2-1)(x^6-x^5-x-1)$, i.e. by the vectors

$$(20020212220200100000000000000)_- \ ,$$

where the subscript $-$ indicates that the code is negacyclic. Huffman [146] shows that there are at least 14 inequivalent $[28, 14, 9]_3$ codes with nontrivial automorphisms of odd order.

Ward [321] and Dawson [76] independently discovered that $[40, 20, 12]_3$ codes can be constructed using generator matrices of the form $[I_{20} H_{20}]$, where H_{20} is a Hadamard matrix of order 20. There are three distinct Hadamard matrices of this order, and Dawson shows that all three produce $[40, 20, 12]_3$ codes. Harada [123] shows that these three codes are inequivalent. Dawson also shows that the same construction using the Paley-Hadamard matrix of order 32 leads to a $[64, 32, 18]_3$ self-dual code. A $[64, 32, 18]_3$ code B_{24} (equivalent to Dawson's) had been constructed earlier by Beenker [12].

The codes of length 32, 44, 52, 56 and 68 can be obtained by "subtracting" (see Section 11.3) a copy of t_4 from a code of length 4 greater.

Other constructions for ternary self-dual codes can be found in Harada [123] and Ozeki [215].

12.3. Family 4^{H}: Hermitian self-dual codes over $\mathbb{F}_4$

Table XIII shows the highest possible minimal distance for Hermitian self-dual codes over $\mathbb{F}_4$ of lengths $n \leq 32$.

Remarks on Table XIII

A period in the "Codes" column indicates that the list is complete.

For the entries at lengths $n \leq 16$, see the discussion in Section 11.5.

Extremal codes exist at lengths 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 28 and 30. They do not exist at lengths 12, 24, 102, 108, 114, 120, 122 and all $n \geq 126$ (the larger n being eliminated by the presence of negative coefficients in the extremal Hamming weight enumerator). The remaining lengths $(26, 32, 34, \ldots)$ are undecided.

The $[18, 9, 8]_4$ code S_{18} generated by

$$1(1\omega\overline{\omega}\omega\omega\omega\overline{\omega}\overline{\omega}\overline{\omega}\overline{\omega}\overline{\omega}\overline{\omega}\omega\omega\omega\overline{\omega}\omega)$$

has a number of interesting properties (see [189], [67], [59], [235]). It has automorphism group $3 \times (PSL_2(16).4)$, of order 48960 [59] and is the unique $[18, 9, 8]_4$ code [148].

The long-standing question of the existence of a $[24, 12, 10]_4$ code was settled in the negative by Lam and Pless [176] (see also [141]). The code $g_{24} \otimes \mathbb{F}_4$ is an example of a $[24, 12, 8]_4$ code.

12.4. Family $4^{\mathrm{H}+}$: Additive self-dual codes over $\mathbb{F}_4$

Table XIV, taken from [49], shows the highest possible minimal distance for additive codes over $\mathbb{F}_4$ of lengths $n \leq 30$ that are self-dual with respect to the trace inner product.

Remarks on Table XIV

A period in the "Codes" column indicates that the list is complete.

Extremal Type I codes exist at lengths 1–6, 8–12, 14–18, 20–22 and 28–30, and do not exist at lengths 7, 13 and 25. Lengths 19, 23, 24, 26, 27 are undecided.

Many of the entries are copied from the table of Hermitian self-dual codes, Table XIII. The codes d_n^+ are defined in Section 11.7, h_6 is the hexacode, and h_5 is the $[5, 2.5, 3]_{4+}$ shortened hexacode, generated by $(01\omega\omega 1)$, with weight enumerator $x^5 + 10x^2y^3 + 15xy^4 + 6y^5$ and $|Aut(h_5)| = 120$. Also, c_9, c_{15}, c_{21}, c_{23}, c_{25} are cyclic codes with generators shown in Table XV. If no name is given, the code can be obtained by shortening a code of length one greater.

12.5. Family $4^{\mathbb{Z}}$: Self-dual codes over $\mathbb{Z}_4$

Table XVI gives the highest possible Hamming distance, Lee distance and Euclidean norm for codes over $\mathbb{Z}_4$ of lengths $n \le 24$. This is based on [71], [88], [95], [149], [239] and [254]. The columns headed # give the number of extremal codes.

Remarks on Table XVI

The length 16 code C_{16} is given in [239], where it is called 5_f5. It has $|Aut(C_{16})| = 2^{5+10}3^2 5.7$ and generator matrix

$$\left[\begin{array}{cccccccccc|ccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&0&1&1&1&1&1&1&0&0&0&0&1&0&0&0\\
1&1&0&1&0&0&1&1&1&1&0&0&0&1&0&0\\
1&1&1&0&1&0&1&0&1&0&1&0&0&0&1&0\\
0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&1\\
\hline
0&0&0&0&0&2&0&0&0&0&0&2&2&0&0&2\\
0&0&0&0&0&0&2&0&0&0&0&2&2&2&2&2\\
0&0&0&0&0&0&0&2&0&0&0&0&2&2&0&2\\
0&0&0&0&0&0&0&0&2&0&0&0&0&2&2&2\\
0&0&0&0&0&0&0&0&0&2&0&2&0&2&0&2\\
0&0&0&0&0&0&0&0&0&0&2&2&0&0&2&2
\end{array}\right]$$

The codes C_{17} and C_{18} mentioned in the table have generator matrices

$$\left[\begin{array}{cccccccccccccccc}
1&0&0&0&0&0&0&0&1&2&1&1&1&1&1&1&2\\
0&1&0&0&0&0&0&0&1&1&0&0&0&1&2&2&0\\
0&0&1&0&0&0&0&0&1&3&2&0&0&2&3&2&2\\
0&0&0&1&0&0&0&0&1&3&0&0&0&2&0&3&0\\
0&0&0&0&1&0&0&0&0&1&3&3&3&3&1&1&2\\
0&0&0&0&0&1&0&0&0&0&0&3&1&0&2&0&3\\
0&0&0&0&0&0&1&0&0&0&3&2&1&0&0&0&3\\
0&0&0&0&0&0&0&1&0&0&1&3&2&0&0&0&3\\
0&0&0&0&0&0&0&0&2&2&2&2&2&0&0&0&0
\end{array}\right]$$

and

$$\begin{bmatrix}
1 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 3 & 0 & 2 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 2 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 2 & 0 & 3 & 0 & 2 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 3 & 0 & 2 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 2 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 & 0 & 2 & 0 & 3 & 0 & 2 & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 3 & 3 & 0 & 3 & 3 & 3 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 3 & 0 & 3 & 3 & 0 & 3 & 1 & 3 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2
\end{bmatrix},$$

and automorphism groups of orders 576 and 144, respectively.

G_{24} was defined in (41), and G_{19} through G_{23} are shortened versions of it.

Besides the norm-extremal codes of length 8, 12, 14–24 shown in the table, there are also norm-extremal codes of lengths 32 and 48 obtained by lifting binary extended quadratic residue codes to $\mathbb{Z}_4$. The code of length 32 has minimal Lee weight 14 and minimal norm 16. Pless and Qian [241] have shown that the code of length 48 has minimal Lee weight 18 and minimal norm 24.

Further examples of good self-dual codes over $\mathbb{Z}_4$ may be found in [22], [23], [27], [51], [88], [102], [112], [115], [124], [149], [241], [244], [254].

13. Further topics

13.1. Decoding self-dual codes

The problem of decoding self-dual codes is an extremely important one for applications, but we will not discuss it here. Decoding the binary Golay code, in particular, has been studied in many papers — see [2], [66], [67], [70, Chapter 11], [233], [236], [259], [292], [315], [316]. See also [258], [314], and Section 8 of Chapter "codes-and-groups".

13.2. Applications to projective planes

There is a very nice application of self-dual codes to projective planes. If n is congruent to 2 (mod 4) then the incidence matrix of a projective plane of order n generates a self-orthogonal code C_n, which when an overall parity-check is added becomes an $[n^2+n+2, \frac{1}{2}(n^2+n+2), n+2]$ Type II self-dual binary code (see [3], [192] or Chapter "assmus" for the proof).

It was a famous unsolved problem to decide if a projective plane of order 10 could exist. The weight enumerator of C_{10} was initially studied in [192] (see also [197]). Finally, after

many years of work, Lam, Thiel and Swiercz [177] (see also [175]) succeeded in completing this project and showed that C_{10} (and hence the putative plane of order 10) does not exist.

The possibility of the existence of a plane of order 18 (or 12, but then we do not obtain a self-dual code) remains an open question.

13.3. Automorphism groups of self-dual codes

Various topics concerning the automorphism groups of self-dual codes are discussed in chapter "codes-and-groups", e.g. the full automorphism groups of extended quadratic residue codes, the occurrence of self-dual codes with a trivial group (see [39], [69], [120], [180], [207], [305]), and the existence of self-dual codes with any prescribed symmetry group ([207]).

13.4. Open problems

Do there exist $[72, 36, 16]$ or $[96, 48, 20]$ Type II self-dual binary codes? (Cf. [63], [94], [153], [245], [282]).

Fill in the other gaps in Tables X, XII, XIII. No extremal Hermitian self-dual codes over $\mathbb{F}_4$ of any length greater than 30 are presently known!

There is an interesting open question concerning self-dual codes of length 24. There exists a unique $[24, 12, 8]$ binary code, exactly two $[24, 12, 9]_3$ ternary codes, and no $[24, 12, 10]_4$ Hermitian or Euclidean self-dual code over $\mathbb{F}_4$ ([176]). But the possibility of an *additive* trace-self-dual code of length 24 over $\mathbb{F}_4$ with minimal distance 10 remains open (see Table XIV). From Theorem 33, if such a code exists then it must be even. However, all our attempts so far to construct this code have failed, so it may not exist.

When is the first time a Type I binary code has a higher minimal distance than the best Type II code of the same length? (No such example is presently known.)

In this regard it is worth mentioning that there is a $[32, 17, 8]$ binary code [60], which has the same minimal distance as the best self-dual codes of length 32, yet contains twice as many codewords. There are similar examples in the ternary case — see Chapter "Brouwer".

The Nordstrom-Robinson code (see Chapter 1) is an example of a nonlinear code that has a higher minimal distance than any self-dual (or even linear) code of the same length. However, as mentioned in Section 3.2, the Nordstrom-Robinson code should really be regarded as a self-dual linear code over $\mathbb{Z}_4$ (the octacode o_8). When is the first time a non-self-dual $[n, n/2, d]$ binary linear code has a higher minimal distance than any $[n, n/2, d']$ self-dual code? This

certainly happens at length 40, but may happen at length 36 or 38.

Is there any difference asymptotically, as $n \to \infty$, between d/n for the best binary codes, the best binary linear codes and the best binary self-dual codes?

Let Ω_n denote the collection of binary self-dual codes that have the highest possible minimal distance at length n, and let L_n, U_n be respectively the smallest and largest orders of $Aut(C)$, $C \in \Omega_n$. When (if ever) is the first time that $L_n = U_n = 1$? Is there an infinite sequence of values of n with $U_n > 1$? Show that $L_n = 1$ for all sufficiently large n.

14. Self-dual codes and lattices

There are many connections and parallels between self-dual codes and lattice sphere packings. Our original intention was to end the chapter with an account of these connections, but constraints of space and time have not permitted this. Instead, we give a brief list of some of the parallels, to whet the reader's appetite. For more information about the relationship between the two fields, see [32], [33], [92], [97], [98], [103], [285], [287] and especially [70], [73].

Coding concept	Lattice concept
Binary linear code	Lattice
Dual code	Dual lattice
Self-orthogonal code	Integral lattice
Self-dual code	Unimodular lattice
Doubly-even self-dual code	Even unimodular lattice
Hamming code e_8	Root lattice E_8 ([70], p. 120)
Hexacode h_6	Coxeter-Todd lattices K_{12} ([70], p. 127)
Binary Golay code g_{24}	Leech lattice Λ_{24} ([70], p. 131)
Minimal distance	Minimal norm
Number of minimal weight words	Kissing number
Weight enumerator $W(x, y)$	Theta series
MacWilliams identity (Eq. (33)) (weight enumerator of dual code in terms of weight enumerator of code)	Jacobi identity ([70], p. 103) (theta series of dual lattice in terms of theta series of lattice)
Gleason's theorem (Theorem 11) (weight enumerator of doubly-even code is polynomial in weight enumerators of e_8 and g_{24})	Hecke's theorem ([70], p. 187) (theta series of even unimodular lattice is polynomial in theta series of E_8 and Λ_{24})

The similarity between the theorems of Gleason and Hecke is particularly striking, and we will end the chapter by saying a little more about this. Suppose C is a binary code of length n. *Construction A* produces an n-dimensional sphere packing $\Lambda(C)$, consisting of the points $\frac{1}{\sqrt{2}}x$ for $x \in \mathbb{Z}^n$, $x \pmod 2 \in C$. If C is linear, $\Lambda(C)$ is a lattice; if C is self-dual, $\Lambda(C)$ is unimodular; and if C is Type II, $\Lambda(C)$ is an even unimodular lattice.

If C is a linear code with weight enumerator $W_C(x,y)$, then $W_C(\theta_3(2z),\theta_2(2z))$ is the theta series of $\Lambda(C)$, where

$$\theta_3(z) = \sum_{m=-\infty}^{\infty} q^{m^2}, \quad \theta_2(z) = \sum_{m=-\infty}^{\infty} q^{(m+1/2)^2} \ ,$$

where $q = e^{\pi i z}$, $\mathrm{Im}(z) > 0$. This map gives an isomorphism between (a) the ring of weight enumerators of Type I self-dual codes, $\mathbb{C}[\phi_2, \theta_8]$ (see Eq. 95), and the ring of theta series of even-dimensional unimodular lattices, $\mathbb{C}[\theta_3^2, \Delta_8]$, where

$$\Delta_8 = q \prod_{m=1}^{\infty} \{(1-q^{2m-1})(1-q^{4m})\}^8 \ ;$$

and (b) the ring of weight enumerators of Type II self-dual codes, $\mathbb{C}[\phi_8, \phi'_{24}]$ (Theorem 13), and the ring of theta series of even unimodular lattices, $\mathbb{C}[\Theta_{E_8}, \Delta_{24}]$, where

$$\begin{aligned} \Theta_{E_8}(z) &= 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^{2m} \ , \\ \Delta_{24} &= q^2 \prod_{m=1}^{\infty} (1-q^{2m})^{24} \ , \end{aligned}$$

and $\sigma_3(m)$ is the sum of the cubes of the divisors of m. For further information see [70, Chapter 7].

The bibliography also contains a number of references that are concerned with particular constructions of lattices from self-dual codes, or of properties of lattices that are analogous to properties of self-dual codes mentioned in this chapter: [8], [9], [22], [23], [26], [51], [55], [61], [68], [72], [82], [112], [163], [168], [171], [174], [193], [209], [210], [212], [213], [214], [216], [256], [270], [271], [272], [286].

Acknowledgements

Over the past 26 years NJAS has had the pleasure of collaborating with many of the people whose names are listed in the bibliography: he wishes to express his appreciation to all of them. We thank Eiichi Bannai, Dave Forney, Aaron Gulliver, Masaaki Harada, Cary Huffman, Michio Ozeki, Vera Pless and Patrick Solé for helpful comments on the manuscript of this chapter. We also thank Susan Pope for a superb typing job.

Table III: Doubly-even self-dual (or Type II) binary codes of length 32 (Part 1)

Code	Components	$\lvert G_1\rvert$	$\lvert G_2\rvert$	$\lvert G\rvert$	A_4	n_{30}	n_{28}	n_{26}	n_{24}
C1	d_{32}	1	1	$2^{30}3^6 5^3 7^2 11.13$	120	2	2	1	1
C2	$d_{24}e_8$	1	1	$2^{27}3^6 5^2 7^2 11$	80	4	3	2	2
C3	$d_{20}d_{12}$	1	1	$2^{26}3^6 5^3 7$	60	5	4	2	2
C4	$d_{18}e_7^2$	1	2	$2^{22}3^6 5.7^3$	50	5	3	2	1
C5	d_{16}^2	1	2	$2^{29}3^4 5^2 7^2$	56	3	2	1	1
C6	$d_{16}e_8^2$	1	2	$2^{27}3^4 5.7^3$	56	5	3	2	2
C7	$d_{16}d_8^2$	1	2	$2^{27}3^4 5.7$	40	6	4	2	2
C8	$d_{14}d_{10}e_7f_1$	1	1	$2^{20}3^4 5^2 7^2$	38	11	5	3	2
C9	$d_{14}d_6^3$	1	6	$2^{20}3^6 5.7$	30	6	4	2	1
C10	$d_{12}^2e_8$	1	2	$2^{25}3^5 5^2 7$	44	5	3	2	2
C11	$d_{12}^2d_8$	1	2	$2^{25}3^5 5^2$	36	6	4	2	2
C12	$d_{12}d_8^2d_4$	1	2	$2^{24}3^4 5$	28	11	7	2	2
C13	$d_{12}e_7^2d_6$	1	2	$2^{19}3^5 5.7^2$	32	9	5	3	1
C14	$d_{12}d_6^3f_2$	1	6	$2^{19}3^6 5$	24	9	4	2	1
C15	$d_{12}d_4^5$	1	120	$2^{22}3^3 5^2$	20	5	3	1	1
C16	$d_{10}^3f_2$	1	6	$2^{22}3^4 5^3$	30	5	2	1	1
C17	$d_{10}^2d_6^2$	1	4	$2^{22}3^4 5^2$	26	7	4	2	1
C18	$d_{10}e_8e_7^2$	1	2	$2^{20}3^4 5.7^3$	38	8	4	3	2
C19	$d_{10}d_8e_7d_6f_1$	1	1	$2^{19}3^4 5.7$	26	17	7	4	2
C20	$d_{10}d_8d_6^2f_2$	1	2	$2^{20}3^4 5$	22	15	6	3	2
C21	$d_{10}d_6^2d_4^2f_2$	1	4	$2^{19}3^3 5$	18	16	6	2	1
C22	$d_{10}d_4^4f_6$	6	24	$2^{19}3^3 5$	14	9	3	1	1
C23	$d_{10}g_{22}$	2	1	$2^{15}3^3 5^2 7.11$	10	4	2	1	1
C24	e_8^4	1	24	$2^{27}3^5 7^4$	56	2	1	1	1
C25	$e_8d_8^3$	1	6	$2^{25}3^5 7$	32	5	3	2	2
C26	$e_8d_6^4$	1	24	$2^{21}3^6 7$	26	5	3	2	1
C27	$e_8d_4^6$	3	720	$2^{22}3^4 5.7$	20	4	2	1	1
C28	e_8g_{24}	1	1	$2^{16}3^4 5.7^2 11.23$	14	3	1	1	1
C29	d_8^4	1	24	$2^{27}3^5$	24	3	2	1	1
C30	d_8^4	1	8	$2^{27}3^4$	24	4	2	1	1
C31	$d_8^3d_4^2$	1	6	$2^{23}3^4$	20	6	3	1	1
C32	$d_8^2e_7^2f_2$	1	4	$2^{20}3^4 7^2$	26	10	3	2	1
C33	$d_8^2d_6^2f_4$	1	4	$2^{20}3^4$	18	14	4	2	1
C34	$d_8^2d_4^4$	1	16	$2^{24}3^2$	16	8	4	1	1
C35	$d_8e_7d_6^2d_4f_1$	1	2	$2^{18}3^4 7$	20	18	7	3	1
C36	$d_8d_6^4$	1	8	$2^{21}3^5$	18	7	4	2	1
C37	$d_8d_6^2d_6d_4f_2$	1	2	$2^{18}3^4$	16	22	9	3	1
C38	$d_8d_6^2d_4^2f_4$	1	4	$2^{18}3^3$	14	20	7	2	1
C39	$d_8d_6d_4^3f_6$	2	6	$2^{17}3^3$	12	17	6	2	1
C40	$d_8d_4^6$	1	48	$2^{22}3^2$	12	7	4	1	1
C41	$d_8d_4^4f_8$	2	24	$2^{18}3^2$	10	12	4	1	1
C42	$d_8d_4^2g_{16}$	36	2	$2^{17}3^3$	8	9	3	1	1
C43	d_8h_{24}	1	1	$2^{16}3^4 5$	6	5	2	1	1
C44	$e_7^4d_4$	1	24	$2^{17}3^5 7^4$	29	4	2	1	0

Table IV: Doubly-even self-dual (or Type II) binary codes of length 32 (Part 2)

Code	Components	$\lvert G_1\rvert$	$\lvert G_2\rvert$	$\lvert G\rvert$	A_4	n_{30}	n_{28}	n_{26}	n_{24}
C45	$e_7^2 d_6^3$	1	6	$2^{16}3^6 7^2$	23	6	3	2	0
C46	$e_7 d_6^3 d_4 f_3$	1	6	$2^{15}3^5 7$	17	13	4	2	0
C47	$e_7 d_6 d_4^4 f_3$	1	24	$2^{17}3^3 7$	14	12	4	2	0
C48	$e_7 d_4^4 f_9$	18	24	$2^{15}3^4 7$	11	7	2	1	0
C49	$e_7 d_4 g_{21}$	6	1	$2^{12}3^4 5.7^2$	8	6	2	1	0
C50	$d_6^5 f_2$	1	10	$2^{16}3^5 5$	15	6	2	1	0
C51	$d_6^4 d_4^2$	1	48	$2^{20}3^5$	14	6	3	1	0
C52	$d_6^4 d_4 f_2^2$	1	8	$2^{17}3^4$	13	13	4	1	0
C53	$d_6^4 f_8$	2	24	$2^{16}3^5$	12	8	2	1	0
C54	$d_6^3 d_4^3 f_2$	1	6	$2^{16}3^4$	12	12	5	1	0
C55	$d_6^3 d_4^2 f_6$	1	6	$2^{14}3^4$	11	15	3	1	0
C56	$d_6^2 d_4^4 f_2^2$	1	8	$2^{17}3^2$	10	16	4	1	0
C57	$d_6^2 d_4^4 f_4$	2	16	$2^{19}3^2$	10	13	4	1	0
C58	$d_6^2 d_4^3 f_2 f_6$	1	12	$2^{14}3^3$	9	18	4	1	0
C59	$d_6^2 d_4^2 f_{12}$	12	4	$2^{14}3^3$	8	14	3	1	0
C60	$d_6^2 g_{20}$	4	2	$2^{15}3^3 5$	6	6	2	1	0
C61	$d_6 d_4^2 d_4^3 f_3^2$	1	12	$2^{15}3^2$	8	19	6	1	0
C62	$d_6 d_4^4 f_{10}$	2	8	$2^{15}3$	7	21	4	1	0
C63	$d_6 d_4^3 f_{14}$	8	6	$2^{13}3^2$	6	18	4	1	0
C64	$d_6 d_4^2 g_{18}$	36	2	$2^{10}3^4$	5	12	3	1	0
C65	$d_6 d_4 g_{16} f_6$	72	1	$2^{12}3^3$	4	14	4	1	0
C66	$d_6 f_{13}^2$	5616	2	$2^8 3^4 13$	3	6	2	1	0
C67	d_4^8	6	1344	$2^{23}3^2 7$	8	2	1	0	0
C68	d_4^8	1	1152	$2^{23}3^2$	8	3	1	0	0
C69	d_4^8	1	336	$2^{20}3.7$	8	2	1	0	0
C70	$d_4^6 f_8$	4	48	$2^{18}3$	6	7	2	0	0
C71	$d_4^6 f_8$	1	48	$2^{16}3$	6	9	2	0	0
C72	$d_4^4 d_4 f_{12}$	6	24	$2^{14}3^2$	5	10	2	0	0
C73	$d_4^5 f_{12}$	1	60	$2^{12}3.5$	5	6	1	0	0
C74	$d_4^4 g_{16}$	8	24	$2^{18}3$	4	7	2	0	0
C75	$d_4^4 f_{16}$	8	8	2^{14}	4	14	2	0	0
C76	$d_4^3 g_{18} f_2$	8	6	$2^{10}3^2$	3	13	2	0	0
C77	$d_4^2 q_{24}^+$	6	2	$2^{15}3^2$	2	6	1	0	0
C78	$d_4^2 q_{24}^-$	3	2	$2^{10}3^2$	2	8	1	0	0
C79	$d_4 f_4^6$	16	72	$2^{11}3^2$	2	8	1	0	0
C80	$d_4 f_7^4$	168	8	$2^8 3.7$	1	8	2	0	0
C81	q_{32}	1	1	$2^5 3.5.31$	0	1	0	0	0
C82	r_{32}	1	1	$2^{15}3^2 5.7.31$	0	1	0	0	0
C83	g_{16}^2	20160	2	$2^{15}3^2 5.7$	0	2	0	0	0
C84	f_4^8	256	336	$2^{12}3.7$	0	2	0	0	0
C85	f_2^{16}	2	11520	$2^9 3^2 5$	0	3	0	0	0

Table V: The groups G_0 for the components mentioned in Tables II, III and IV.

Component	G_0	$\lvert G_0\rvert$
d_{2m}	$2^{m-1}.S(m)$	$2^{m-1}m!$
e_7	$L_3(2)$	168
e_8	$GA_3(2)$	1344
f_n	1	1
g_{16}	2^4	16
g_{18}	$Z(3)$	3
g_{20}	M_{20}	$2^6 3.5$
g_{21}	M_{21}	$2^6 3^2 5.7$
g_{22}	M_{22}	$2^7 3^2 5.7.11$
g_{24}	M_{24}	$2^{10} 3^3 5.7.11.23$
h_{24}	$2^6 : 3S(6)$	$2^9 3^3 5$
q_{24}^+	$2^6.(S(3) \times 2^2)$	$2^9 3$
q_{24}^-	$2^2 \times S(4)$	$2^5 3$

Figure 3: Generator matrices for the $[32, 16, 8]$ Type II codes $C83 = g_{16}^{2+}$, $C84 = f_4^{8+}$ and $C85 = f_2^{16+}$.

11101000111010000000000000000000
10110100101101000000000000000000
10011010100110100000000000000000
10001101100011010000000000000000
00000000000000001101100011011000
00000000000000001010110010101100
00000000000000001001011010010110
00000000000000001000101110001011
11011000110110001101100000000000
10101100101011001010110000000000
10010110100101101001011000000000
10001011100010111000101100000000
00000000111010001110100011101000
00000000101101001011010010110100
00000000100110101001101010011010
00000000100011011000110110001101

11101000000000001110100011101000
10110100000000001011010010110100
10011010000000001001101010011010
10001101000000001000110110001101
00000000111010001110100010110100
00000000101101001011010010011010
00000000100110101001101010001101
00000000100011011000110111000110
11011000110110001101100000000000
10101100101011001010110000000000
10010110100101101001011000000000
10001011100010111000101100000000
11011000101100010000000011011000
10101100110110000000000010101100
10010110101011000000000010010110
10001011100101100000000010001011

10000000000000000111110001000100
01000000000000000111101000100010
00100000000000000111100100010001
00010000000000000111100010001000
00001000000000000100011111000100
00000100000000000100111101000100
00000010000000000010111100100010
00000001000000000001111100010001
00000000100000001000100011111000
00000000010000000100010011110100
00000000001000000010001011110010
00000000000100000001000111110001
00000000000010001000100010001111
00000000000001000100010001001111
00000000000000100010001000101111
00000000000000010001000100011111

Table VI:

Binary self-dual codes with $n \leq 22$, $d \geq 4$

n	Code	Compts.	Name	$\lvert G_1\rvert$	$\lvert G_2\rvert$	A_4	A_6	A_8	A_{10}	A_{12}	Generators for glue
0	C1(d_{32})	i_0	-	1	1						-
8	C2(d_{24})	e_8	A_8	1	1	14	0	1			-
12	C3(d_{20})	d_{12}	B_{12}	1	1	15	32	15	0	1	a
14	C4(d_{18})	e_7^2	D_{14}	1	2	14	49	49	14	0	dd
16	C5(d_{16})	d_{16}	E_{16}	1	1	28	0	198	0	28	a
	C6(d_{16})	e_8^2	$A_8 \oplus A_8$	1	2	28	0	198	0	28	-
	C7(d_{16})	d_8^2	F_{16}	1	2	12	64	102	64	12	(ab)
18	C8(d_{14})	$d_{10}e_7f_1$	I_{18}	1	1	17	51	187	187	51	aoA, cd-
	C9(d_{14})	d_6^3	H_{18}	1	6	9	75	171	171	75	$(abc), bbb$
20	C3(d_{12})	d_{20}	J_{20}	1	1	45	0	210	512	210	a
	C10(d_{12})	$d_{12}e_8$	$A_8 \oplus B_{12}$	1	1	29	32	226	448	226	a-
	C11(d_{12})	$d_{12}d_8$	K_{20}	1	1	21	48	234	416	234	(ab)
	C12(d_{12})	$d_8^2d_4$	S_{20}	1	2	13	64	242	384	242	$(ab)x, bby$
	C13(d_{12})	$e_7^2d_6$	L_{20}	1	2	17	56	238	400	238	doa, ddb
	C14(d_{12})	$d_6^3f_2$	R_{20}	1	6	9	72	246	368	246	$aaaA, cccB, (abc)$-
	C15(d_{12})	d_4^5	M_{20}	1	120	5	80	250	352	250	$(ooxyx)$
22	C8(d_{10})	$d_{14}e_7f_1$	N_{22}	1	1	28	49	246	700	700	aoA, bdA
	C16(d_{10})	$d_{10}^2f_2$	P_{22}	1	2	20	57	270	676	676	$(ao)*, cc$-
	C17(d_{10})	$d_{10}d_6^2$	Q_{22}	1	2	16	61	282	664	664	aoc, oaa, bbb
	C18(d_{10})	$e_8e_7^2$	$E_8 \oplus D_{14}$	1	2	28	49	246	700	700	$-dd$
	C19(d_{10})	$d_8e_7d_6f_1$	R_{22}	1	1	16	61	282	664	664	$odbA, boaA, aob$-
	C20(d_{10})	$d_8d_6^2f_2$	S_{22}	1	2	12	65	294	652	652	$baoA, aooAB, abb$-, occ-
	C21(d_{10})	$d_6^2d_4^2f_2$	T_{22}	1	4	8	69	306	640	640	$aoxoA, ooyyAB$, $aayo$-, $bozx$-, $obxz$-
	C22(d_{10})	$d_4^4f_6$	U_{22}	6	24	4	73	318	628	628	$oxyzBC, ozxyAC$, $ooxxAE, oyoyAD$, $ozzoAF, xxxx$-, $yyyy$-
	C23(d_{10})	g_{22}	G_{22}	2	1	0	77	330	616	616	the all-ones vector

Table VII:

Binary self-dual codes with length 24 and $d \geq 4$

Code	Components	Name	d	Code	Components	Name	d
C2(e_8)	d_{24} §	E_{24}	4	C32(d_8)	$d_8e_7^2f_2$	J_{24}	4
C6(e_8)	$d_{16}e_8$ §	—	4	C33(d_8)	$d_8d_6^2f_4$	R_{24}	4
C7(d_8)	$d_{16}d_8$	H_{24}	4	C34(d_8)	$d_8d_4^4$	T_{24}	4
C10(e_8)	d_{12}^2 §	A_{24}	4	C35(d_8)	$e_7d_6^2d_4f_1$	P_{24}	4
C11(d_8)	d_{12}^2	—	4	C26(e_8)	d_6^4 §	D_{24}	4
C12(d_8)	$d_{12}d_8d_4$	I_{24}	4	C36(d_8)	d_6^4	Q_{24}	4
C18(e_8)	$d_{10}e_7^2$ §	B_{24}	4	C37(d_8)	$d_6^2d_6d_4f_2$	S_{24}	4
C19(d_8)	$d_{10}e_7d_6f_1$	K_{24}	4	C38(d_8)	$d_6^2d_4^2f_2$	U_{24}	4
C20(d_8)	$d_{10}d_6^2f_2$	N_{24}	4	C39(d_8)	$d_6d_4^3f_6$	W_{24}	4
C24(e_8)	e_8^3 §	—	4	C27(e_8)	d_4^6 §	F_{24}	4
C25(d_8)	$e_8d_8^2$	—	4	C40(d_8)	d_4^6	V_{24}	4
C25(e_8)	d_8^3 §	C_{24}	4	C41(d_8)	$d_4^4f_8$	X_{24}	4
C29(d_8)	d_8^3	L_{24}	4	C42(d_8)	$d_4^2g_{16}$	Y_{24}	4
C30(d_8)	d_8^3	M_{24}	4	C43(d_8)	h_{24}	Z_{24}	6
C31(d_8)	$d_8^2d_4^2$	O_{24}	4	C28(e_8)	g_{24} §	G_{24}	8

Table VIII: Indecomposable ternary self-dual codes of lengths $n \leq 20$

n	Components	$\lvert G_0\rvert$	$\lvert G_1\rvert$	$\lvert G_2\rvert$	d	glue
4	t_4	48	1	1	3	–
8	–					
12	e_3^{4+}	6^4	2	24	3	$aaa0, 0\bar{a}aa$
	g_{12}	190080	1	1	6	–
16	$(e_3^4f_4)^+$	$6^4.1$	8	24	3	$(a000)(2111)$
	$(e_3^2g_{10})^+$	$6^2.360$	4	2	3	$a0x, 0ay$
	$(e_3p_{13})^+$	6.5616	2	1	3	at_0
	f_8^{2+}	1^2	$2^7.168$	2	6	$[I\lvert H_8]$
20	17 codes					
	– see [243]					

Table IX: Indecomposable Hermitian self-dual codes over $\mathbb{F}_4$ of lengths $n \leq 16$

n	Components	$\lvert G_0\rvert$	$\lvert G_1\rvert$	$\lvert G_2\rvert$	d	Glue
2	i_2	12	1	1	2	–
4	–	–	–	–	–	–
6	h_6	2160	1	1	4	–
8	e_8	8064	1	1	4	–
10	d_{10}^+	$2^4.5!$	6	1	4	d
	e_5^{2+}	60^2	6	2	4	11
12	d_{12}^+	$2^5.6!$	6	1	4	a
	$(e_7e_5)^+$	60.168	6	1	4	11
	d_6^{2+}	24^2	6	2	4	(bd)
	d_4^{3+}	4^3	54	6	4	$(0de)$
14	d_{14}^+	$2^6.7!$	6	1	4	d
	e_7^{2+}	168^2	6	2	4	11
	$(d_8e_5f_1)^+$	$2^3.4!60$	6	1	4	$d01, e10$
	$(e_5^2d_4)^+$	4.60^2	18	2	4	$01d, 10e$
	$(d_8d_6)^+$	$2^34!2^23!$	6	1	4	ab, bd
	$(d_6^2f_2)^+$	$(2^2.3!)^2$	6	2	4	$(d0)11, bb\omega\overline{\omega}$
	$(d_6d_4^2)^+$	$4^22^23!$	18	2	4	$bbb, a0d, cd0$
	$(d_4^3f_2)^+$	4^3	6	6	4	$aa011, 0aa\omega\omega, \dot{b}\ddot{b}0\omega\overline{\omega}, 0\dot{b}\ddot{b}\overline{\omega}1$
	$(d_4^21_6)^+$	4^2	108	2	4	$b00011\omega\omega, a00\overline{\omega\omega}110,$ $0b01\omega01\omega, 0a011\overline{\omega\omega}0$
	q_{14}	6552	1	1	6	–
16	31 codes (see [64])					

Table X: Highest minimal distance of binary self-dual codes

n	d_I	d_{II}	Codes
2	2		i_2.
4	2		i_2^2.
6	2		i_2^3.
8	2	4	i_2^4; e_8.
10	2		i_2^5, $e_8 i_2$.
12	4		d_{12}^+.
14	4		e_7^{2+}.
16	4	4	d_8^{2+}; d_{16}^+, e_8^2.
18	4		d_6^{3+}, $(d_{10}e_7f_1)^+$.
20	4		7 codes (Table II).
22	6		g_{22}.
24	6	8	h_{24}^+; g_{24}.
26	6		f_{13}^2 [62].
28	6		3 codes [62].
30	6		13 codes [62], [65].
32	8	8	3 codes [69]; 5 codes (Table III).
34	6		≥ 200
36	8		≥ 2
38	8		≥ 3 [69], [127]
40	8	8	≥ 22; ≥ 1000 (see text for references)
42	8		≥ 30 [83]
44	8		≥ 108 [83]
46	10		≥ 1 [69]
48	10	12	≥ 7; ≥ 1 (XQ_{47})
50	10		≥ 6
52	10		≥ 499 [152]
54	10		≥ 54
56	10 or 12	12	?; ≥ 166
58	10		≥ 80 [83]
60	12		≥ 5
62	10 or 12		?
64	12	12	≥ 5; ≥ 3270 [83]
66	12		≥ 3
68	12		≥ 65
70	12 or 14		? [121], [276]
72	12 or 14	12 or 16	?; ?

Table XI: Double circulant binary codes

Name	n	k	d	Type	Form	r (hexadecimal)
g_{22}	22	11	6	I	(179)	97
g_{24}	24	12	8	II	(178)	B7
$A_{26} = f_{13}^{2+}$	26	13	6	I	(179)	5F7
A_{28} =D1	28	14	6	I	(178)	8D
D2	34	17	6	I	(179)	1ECE
D3	36	18	8	I	(178)	2C6B
D4	38	19	8	I	(179)	5793
D5	40	20	8	II	(179)	57EB
D6	40	20	8	I	(179)	11E35
D7	40	20	8	I	(179)	B393
D8	44	22	8	I	(178)	5E6B5
D9	50	25	10	I	(179)	31C4D
D10	52	26	10	I	(178)	57F69D
D11	56	28	12	II	(178)	ADF1FF
D12	58	29	10	I	(179)	D5A89B
D12a	58	29	10	I	(179)	2DD1D3
D13	60	30	12	I	(178)	3EF6B77
D14	64	32	12	II	(178)	427BD0B
D15	64	32	12	I	(179)	2EF3DD75
D16	66	33	12	I	(179)	B2D97D9
D17	68	34	12	I	(179)	1F5C885F
D18*	72	36	12	I	(179)	2B8795E5
D19*	74	37	12	I	(179)	1439372C7
D20*	82	41	12	I	(179)	A464B919B
H86	86	43	16	I	(179)	7F7101712E2
M88	88	44	16	II	(178)	
M136	136	68	24	II	(178)	

Table XII: Highest minimal distance of ternary self-dual codes

n	d	Codes
4	3	t_4.
8	3	t_4^2.
12	6	g_{12}.
16	6	f_8^{2+}.
20	6	6 codes [243].
24	9	XQ_{23}, $S(24)$ [180].
28	9	≥ 32 [58], [123], [174], [146]
32	9	≥ 239 [146]
36	12	≥ 1 ($S(36)$)
40	12	≥ 20 [321], [76], [123], [146]
44	12	≥ 8 [123]
48	15	≥ 2 ($XQ_{47}, S(48)$)
52	12 or 15	?
56	15	≥ 1
60	18	≥ 2 ($XQ_{59}, S(60)$)
64	18	≥ 1 [12], [76]
68	15 or 18	?
72	18	≥ 1 ($XQ_{71}[74]$)

Table XIII: Highest minimal distance of Hermitian self-dual codes over $\mathbb{F}_4$

n	d	Codes
2	2	i_2.
4	2	i_2^2.
6	4	h_6.
8	4	e_8.
10	4	d_{10}^+, e_5^{2+}.
12	4	5 codes (Table IX).
14	6	q_{14}.
16	6	4 codes [64].
18	8	S_{18} [148].
20	8	2 codes [148].
22	8	≥ 38 codes [143], [145]
24	8	≥ 1 code
26	8 or 10	?
28	10	≥ 3 codes [143], [145]
30	12	XQ_{29} [189]
32	?	?

Table XIV: Highest minimal distance of additive self-dual codes over $\mathbb{F}_4$

n	d	Codes	n	d	Codes
1	1	i_1.	16	6	≥ 4 codes [64]
2	2	i_2.	17	7	
3	2	d_3^+.	18	8	S_{18}
4	2	3 codes.	19	7	
5	3	h_5.	20	8	≥ 2 codes [148]
6	4	h_6.	21	8	c_{21}
7	3		22	8	≥ 38 codes [143]
8	4	e_8	23	8–9	c_{23}
9	4	c_9	24	8–10	$g_{24} \otimes \mathbb{F}_4$
10	4	d_{10}^+ , e_5^{2+}	25	8–9	c_{25}
11	5		26	8–10	
12	6	z_{12}.	27	9–10	
13	5		28	10	
14	6	q_{14}	29	11	
15	6	c_{15}	30	12	XQ_{29}

Table XV: Generators for cyclic additive codes over $\mathbb{F}_4$

c_9 $(\omega 10100101)$
c_{15} $(\omega 11010100101011)$
c_{21} $(\overline{\omega\omega}1\omega 00111101011011000), (101110010111001011100)$
c_{23} $(\omega 01011110000000001111010)$
c_{25} $(111010\omega 010111000000000000)$

Table XVI: Highest Hamming distance (d_H), Lee distance (d_L) and Euclidean norm (Norm) of self-dual codes over $\mathbb{Z}_4$

Length	Hamming			Lee			Norm		
n	d_H	code	#	d_L	code	#	Norm	code	#
1	1	i_1	1	2	i_1	1	4	i_1	1
2	1	i_1^2	1	2	i_1^2	1	4	i_1^2	1
3	1	i_1^3	1	2	i_1^3	1	4	i_1^3	1
4	2	$D_4^{\oplus}$	1	4	$D_4^{\oplus}$	1	4	i_1^4	2
5	1	$D_4^{\oplus} i_1$	2	2	$D_4^{\oplus} i_1$	2	4	i_1^5	2
6	2	$D_6^{\oplus}$	1	4	$D_6^{\oplus}$	1	4	i_1^6	3
7	3	E_7^{+}	1	4	E_7^{+}	1	4	i_1^7	4
8	4	o_8	2	6	o_8	1	8	o_8	1
9	1	$o_8 i_1$	11	2	$o_8 i_1$	11	4	i_1^9	11
10	2	$D_4^{\oplus} D_6^{\oplus}$	5	4	$D_4^{\oplus} D_6^{\oplus}$	5	4	i_1^{10}	16
11	2	$D_4^{\oplus} E_7^{+}$	3	4	$D_4^{\oplus} E_7^{+}$	3	4	i_1^{11}	19
12	2	$D_4^{\oplus} o_8$	39	4	$D_4^{\oplus} o_8$	39	8	[95]	19
13	2	$D_6^{\oplus} E_7^{+}$	8	4	$D_6^{\oplus} E_7^{+}$	8	4	i_1^{13}	66
14	3	$(E_7^{+})^2$	4	6	[95]	1	8	[95]	35
15	3	$E_7^{+} o_8$	47	6	[95]	15	8	[95]	28
16	4	o_8^2	≥ 1	8	C_{16}	≥ 5	8	o_8^2	≥ 5
17	4	C_{17}	62	6	C_{17}	≥ 17	8	C_{17}	≥ 17
18	4	C_{18}	66	8	C_{18}	7	8	C_{18}	≥ 39
19	3	G_{19}	≥ 1	6	G_{19}	≥ 1	8	G_{19}	≥ 1
20	4	G_{20}	≥ 1	8	G_{20}	≥ 1	8	G_{20}	≥ 1
21	5	G_{21}	384	8	G_{21}	384	8	G_{21}	≥ 384
22	6	G_{22}	≥ 19367	8	G_{22}	≥ 19367	8	G_{22}	≥ 19367
23	7	G_{23}	$\geq 1.72 \times 10^6$	10	G_{23}	30	12	G_{23}	≥ 30
24	8	G_{24}	$\geq 1.47 \times 10^8$	12	G_{24}	13	16	G_{24}	≥ 50

The bibliography uses the following abbreviations for journals:

DCC = *Designs, Codes and Cryptography*

DM = *Discrete Mathematics*

JCT = *Journal of Combinatorial Theory*

PGIT = *IEEE Transactions on Information Theory*

References

[1] V. K. Agrawala and J. G. Belinfante, An algorithm for computing $SU(n)$ invariants, *BIT* **11** (1971), 1–15.

[2] O. Amrani, Y. Be'ery, A. Vardy, F.-W. Sun and H. C. A. van Tilborg, The Leech lattice and the Golay code: bounded-distance decoding and multilevel constructions, *PGIT* **40** (1994), 1030–1043.

[3] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*, Cambridge Univ. Press, 1992.

[4] ____ and H. F. Mattson, Jr., Coding and combinatorics, *SIAM Review* **16** (1974), 349–388.

[5] ____ ____ and R. J. Turyn, Research to develop the algebraic theory of codes, *Report AFCRL-67-0365*, Air Force Cambridge Res. Labs., Bedford, MA, June 1967.

[6] ____ and V. Pless, On the covering radius of extremal self-dual codes, *PGIT* **29** (1983), 359–363.

[7] L. Babai, H. Oral and K. T. Phelps, Eulerian self-dual codes, *SIAM J. Discr. Math.* **7** (1994), 323–333.

[8] C. Bachoc, Applications of coding theory to the construction of modular lattices, *JCT* **A 78** (1997), 92–119.

[9] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, preprint, June 1997.

[10] ____ S. Minashima and M. Ozeki, On Jacobi forms of weight 4, *Kyushu J. Math.* **50** (1996), 335–370.

[11] ____ and M. Ozeki, Construction of Jacobi forms from certain combinatorial polynomials, *Proc. Japan Acad.* **A 72** (1996), 359–363.

[12] G. F. M. Beenker, A note on extended quadratic residue codes over $GF(9)$ and their ternary images, *PGIT* **30** (1984), 403–405.

[13] D. J. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press, 1993.

[14] E. R. Berlekamp, F. J. MacWilliams, and N. J. A. Sloane, Gleason's theorem on self-dual codes, *PGIT* **18**, (1972), 409–414.

[15] V. K. Bhargava and C. Nguyen, Circulant codes based on the prime 29, *PGIT* **26** (1980), 363–364.

[16] ____ and J. M. Stein, (v, k, d) configurations and self-dual codes, *Inform. Contr.* **28** (1975), 352–355.

[17] ____ G. Young and A. K. Bhargava, A characterization of a $(56, 28)$ extremal self-dual code, *PGIT* **27** (1981), 258–260.

[18] I. F. Blake, Properties of generalized Pless codes, in *Proc. 12th Allerton Conf. Circuit and System Theory*, Univ. Ill., Urbana, 1974, pp. 787–789.

[19] ____ On a generalization of the Pless symmetry codes, *Inform Control* **27** (1975), 369–373.

[20] B. Bolt, T. G. Room and G. E. Wall, On Clifford collineation, transform and similarity groups I, *J. Australian Math. Soc.* **2** (1961), 60–79.

[21] ____ ____ ____ On Clifford collineation, transform and similarity groups II, *J. Australian Math. Soc.* **2** (1961), 80–96.

[22] A. Bonnecaze, A. R. Calderbank and P. Solé, Quaternary quadratic residue codes and unimodular lattices, *PGIT* **41** (1995), 366–377.

[23] ____ P. Gaborit, M. Harada, M. Kitazume and P. Solé, Niemeier lattices and Type II codes over $\mathbb{Z}_4$, preprint.

[24] ____ B. Mourrain and P. Solé, Jacobi polynomials, Type II codes, and designs, *DCC*, submitted.

[25] A. Bonnecaze, E. M. Rains and P. Solé, $\mathbb{Z}_4$ codes and 5-designs, preprint.

[26] ——— and P. Solé, Quaternary constructions of formally self-dual binary codes and unimodular lattices, in *Algebraic Coding, Lect. Notes. Comp. Sci.* **781** (1994), 194–205.

[27] ——— ——— C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *PGIT* **43** (1997), 969–976.

[28] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney, May 22, 1995.

[29] ——— ——— and G. Mathews, Programming with algebraic structures: Design of the Magma language, in *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation*, M. Giesbrecht, Ed., Association for Computing Machinery, 1994, 52–57.

[30] ——— ——— and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* **24** (1997), 235–265.

[31] N. Bourbaki, *Groups et Algèbres de Lie, Chap. 4, 5 et 6*, Hermann, Paris, 1968.

[32] M. Broué, Codes correcteurs d'erreures auto-orthogonal sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant +1, *Comptes Rendus Journ. Math. Soc. Math. France*, Univ. Sci. Tech. Languedoc, Montpellier, 1974, pp. 71–108.

[33] ——— and M. Enguehard, Polynômes des poids de certains codes et fonctions thêta de certains réseaux, *Ann. Sciént. Ec. Norm. Sup.* **5** (1972), 157–181.

[34] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Berlin, 1989.

[35] R. A. Brualdi and V. S. Pless, Weight enumerators of self-dual codes, *PGIT* **37** (1991), 1222–1225.

[36] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Univ. Press, 1993.

[37] W. Burnside, *Group Theory*, Dover, NY, 2nd ed., 1955.

[38] F. C. Bussemaker and V. D. Tonchev, New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28, *DM* **76** (1989), 45–49.

[39] ____ ____ Extremal doubly-even codes of length 40 derived from Hadamard matrices, *DM* **82** (1990), 317–321.

[40] S. Buyuklieva, New extremal self-dual codes of lengths 42 and 44, *PGIT* **43** (1997), 1607–1612.

[41] ____ On the binary self-dual codes with an automorphism of order 2, *DCC* **12** (1997), 39–48.

[42] ____ and I. Boukliev, Extremal self-dual codes with an automorphism of order 2, *PGIT* **44** (1998), 323–328.

[43] ____ and V. Y. Yorgov, Singly-even self-dual codes of length 40, *DCC* **9** (1996), 131–141.

[44] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads and extremal Euclidean line-sets, *Proc. London Math. Soc.* **75** (1997), 436–480.

[45] ____ A. R. Hammons, Jr., P. V. Kumar, N. J. A. Sloane and P. Solé, A linear construction for certain Kerdock and Preparata codes, *Bull. Amer. Math. Soc.* **29** (1993), 218–222.

[46] ____ W.-C. W. Li and B. Poonen, A 2-adic approach to the analysis of cyclic codes, *PGIT* **43** (1997), 977–986.

[47] ____ G. McGuire, P. V. Kumar and T. Helleseth, Cyclic codes over $\mathbb{Z}_4$, locator polynomials, and Newton's identities, *PGIT* **42** (1996), 217–226.

[48] ____ E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* **78** (1997) 405–409.

[49] ____ ____ ____ ____ Quantum error correction via codes over GF(4), *PGIT* **44** (1998), to appear.

[50] ____ and N. J. A. Sloane, Modular and p-adic cyclic codes, *DCC* **6** (1995), 21–35.

[51] ____ ____ Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, *J. Algebraic Combinatorics* **6** (1997), 119–131.

[52] P. Camion, Étude de codes binaires abéliens modulaires autoduaux de petites longueurs, *Revue du CETHEDEC* **79-2** (1979), 3–24.

[53] ____ B. Courteau and A. Montpetit, Coset weight enumerators of the extremal self-dual binary codes of length 32, in *EUROCODE '92*, *CISM Courses and Lectures* **339**, Springer-Verlag, NY, 1993, pp. 17–30.

[54] C. Carlet, On $\mathbb{Z}_4$-duality, *PGIT* **41** (1995), 1487–1494.

[55] R. Chapman and P. Solé, Universal codes and unimodular lattices, *J. Théorie Nombres Bordeaux* **8** (1996), 369–376.

[56] P. Charpin, Self-dual codes which are principal ideals of the group algebra $\mathbb{F}_2[\{\mathbb{F}_{2^m}, +\}]$, *J. Statist. Plann. Infer.* **56** (1996), 79–92.

[57] ____ and F. Levy-dit-Vehel, On self-dual affine-invariant codes, *JCT* **A 67** (1994), 223–244.

[58] Y. Cheng and R. Scharlau, personal communication, Sept., 1987.

[59] ____ and N. J. A. Sloane, The automorphism group of an [18,9,8] quaternary code, *DM* **83** (1990), 205–212.

[60] ____ ____ Codes from symmetry groups and a [32,17,8] code, *SIAM J. Discrete Math.* **2** (1989), 28–37.

[61] J. H. Conway, A. M. Odlyzko, and N. J. A. Sloane, Extremal self-dual lattices exist only in dimensions 1-8, 12, 14, 15, 23 and 24, *Mathematika* **25** (1978), 36–43. A revised version appears as Chapter 14 of [70].

[62] ____ and V. Pless, On the enumeration of self-dual codes, *JCT* **A 28** (1980), 26–53.

[63] ____ ____ On primes dividing the group order of a doubly-even (72,36,16) code and the group order of a quaternary (24,12,10) code, *DM* **38** (1982), 143–156.

[64] ____ ____ and N. J. A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *PGIT* **25** (1979), 312–322.

[65] ____ ____ ____ The binary self-dual codes of length up to 32: A revised enumeration, *JCT* **A 60** (1992), 183–195.

[66] ____ and N. J. A. Sloane, Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice, *PGIT* **32** (1986), 41–50.

[67] ——— ——— Low-dimensional lattices II: Subgroups of $GL(n, \mathbb{Z})$, Proc. Royal Soc. **A 419** (1988), 29–68.

[68] ——— ——— A new upper bound for the minimum of an integral lattice of determinant one, *Bull. Amer. Math. Soc.* **23** (1990), 383–387. Erratum: volume 24 (April 1991), p. 479.

[69] ——— ——— A new upper bound on the minimal distance of self-dual codes, *PGIT* **36**, (1990), 1319–1333.

[70] ——— ——— *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd edition, 1993.

[71] ——— ——— Self-dual codes over the integers modulo 4, *JCT* **A 62** (1993), 30–45.

[72] ——— ——— On lattices equivalent to their duals, *J. Number Theory* **48** (1994), 373–382.

[73] ——— ——— Codes and lattices, *PGIT*, to appear, 1998.

[74] D. Coppersmith and G. Seroussi, On the minimum distance of some quadratic residue codes, *PGIT* **30** (1984), 407–411.

[75] E. C. Dade, Answer to a question of R. Brauer, *J. Algebra* **1** (1964), 1–4.

[76] E. Dawson, Self-dual ternary codes and Hadamard matrices, *Ars Comb.* **19A** (1985), 303–308.

[77] ——— A construction for the generalized Hadamard matrices $GF(4q; EA(q))$, *J. Statist. Plann. Inf.* **11** (1985), 103–110.

[78] P. Delsarte, Bounds for unrestricted codes, by linear programming, *Philips Res. Reports* **27** (1972), 272–289.

[79] J. Dieudonné and J. B. Carroll, *Invariant Theory, Old and New*, Acad. Press, NY, 1971.

[80] P. Doubilet, G.-C. Rota and J. Stein, On the foundations of combinatorial theory. IX: Combinatorial methods in invariant theory, *Studies in Appl. Math.* **53** (1974), 185–216.

[81] S. T. Dougherty, Shadow codes and weight enumerators, *PGIT* **41** (1995), 762–768.

[82] ——— T. A. Gulliver and M. Harada, Type II self-dual codes over finite rings and even unimodular lattices, *J. Alg. Combin.*, to appear.

[83] ——— ——— ——— Extremal binary self-dual codes, *PGIT* **43** (1997), 2036–2046..

[84] ——— and M. Harada, Shadow optimal self-dual codes, *Kyushu J. Math.*, to appear.

[85] ——— ——— New extremal self-dual codes of length 68, preprint.

[86] ——— ——— Self-dual codes constructed from Hadamard matrices and symmetric designs, preprint.

[87] ——— ——— and M. Oura, Formally self-dual codes, preprint.

[88] ——— ——— and P. Solé, Shadow codes over $\mathbb{Z}_4$, *Finite Fields Applic.* to appear.

[89] ——— ——— ——— Self-dual codes over rings and the Chinese remainder theorem, preprint, 1997.

[90] W. Duke, On codes and Siegel modular forms, *Internat. Math. Res. Notices* **5** (1993), 125–136.

[91] H. Dym and H. P. McKean, *Fourier Series and Integrals*, Acad. Press, NY, 1972.

[92] W. Ebeling, *Codes and Lattices*, Vieweg, Wiesbaden, 1994.

[93] M. Eichler and D. Zagier, *The Theory of Jacobi Forms*, Birkhäuser, Boston, 1985.

[94] W. Feit, A self-dual even (96,48,16) code, *PGIT* **20** (1974), 136–138.

[95] J. Fields, P. Gaborit, J. Leon and V. Pless, All self-dual $\mathbb{Z}_4$ codes of length 15 or less are known, *PGIT* **44** (1998), 311–322.

[96] C. S. Fisher, The death of a mathematical theory: a study in the sociology of knowledge, *Archiv. Hist. Exact. Sci.* **3** (1967), 136–159.

[97] G. D. Forney, Jr., Coset codes I: introduction and geometrical classification, *PGIT* **34** (1988), 1066–1070.

[98] ——— Coset codes II: binary lattices and related codes, *PGIT* **34** (1988), 1152–1187.

[99] ——— N. J. A. Sloane and M. D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, in *Coding and Quantization: DIMACS/IEEE Workshop October 19–21, 1992*, pp. 19–26, R. Calderbank, G. D. Forney, Jr. and and N. Moayeri, Eds., Amer. Math. Soc. (1993).

[100] R. Fossum et al., editors, *Invariant Theory, Contemporary Math.* **88** Amer. Math. Soc., 1989.

[101] P. Gaborit, Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings, *PGIT* **42** (1996), 1222–1228.

[102] ____ and M. Harada, Construction of extremal Type II codes over $\mathbb{Z}_4$, *DCC*, submitted.

[103] ____ ____ and P. Solé, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, preprint.

[104] F. Gherardelli, editor, *Invariant Theory: Proceedings, Montecatini, 1982, Lect. Notes. Math.* **996**, Springer-Verlag, NY, 1983.

[105] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes, Congrés International de Mathématiques*, Gauthier-Villars, Paris, **3** (1970), 211–215.

[106] I. J. Good, Generalizations to several variables of Lagrange's expansion, with applications to stochastic processes, *Proc. Camb. Phil. Soc.* **56** (1960), 367–380.

[107] T. A. Gulliver and V. K. Bhargava, Self-dual codes based on the twin prime product 35, *Appl. Math. Lett.* **5** (1992), 95–98.

[108] ____ and M. Harada, Weight enumerators of extremal singly-even $[60, 30, 12]$ codes, *PGIT* **42** (1996), 658–659.

[109] ____ ____ Classification of extremal double circulant formally self-dual even codes, *DCC* **11** (1997), 25–35.

[110] ____ ____ Weight enumerators of double circulant codes and new extremal self-dual codes, *DCC* **11** (1997), 141–150.

[111] ____ ____ Classification of extremal double circulant self-dual codes of lengths 64 to 72, *DCC* **13** (1998), 257–269.

[112] ____ ____ Certain self-dual codes over $\mathbb{Z}_4$ and the odd Leech lattice, *Proc. 12th Appl. Alg. Algorithms and Error-Correcting Codes*, *Lect. Notes Comp. Sci.* **1225** (1997), 130–137.

[113] ____ ____ On the existence of a formally self-dual even $[70, 35, 14]$ code, *Appl. Math. Lett.* **11** (1998), 95–98.

[114] —— —— New optimal self-dual codes over $GF(7)$, *Graphs and Combin.*, to appear.

[115] —— —— Extremal double circulant Type II code over $\mathbb{Z}_4$ and construction of $5-(24,10,36)$ designs, *DM*, to appear

[116] —— —— Double circulant self-dual codes over $GF(5)$, *Ars Comb.*, to appear.

[117] —— —— Double circulant self-dual codes over $\mathbb{Z}_{2k}$, *PGIT*, submitted.

[118] —— —— and H. Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, *DM*, to appear.

[119] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *PGIT* **40** (1994), 301–319.

[120] M. Harada, Existence of new extremal doubly-even codes and extremal singly-even codes, *DCC* **8** (1996), 273–284.

[121] —— The existence of a self-dual $[70,35,12]$ code and formally self-dual codes, *Finite Fields Applic.* **3** (1997), 131–139.

[122] —— Weighing matrices and self-dual codes, *Ars Comb.* **47** (1997), 65–73.

[123] —— New extremal ternary self-dual codes, *Australasian J. Combin.*, to appear.

[124] —— New extremal Type II codes over $\mathbb{Z}_4$, *DCC* **13** (1998), 271–284.

[125] —— New 5-designs constructed from the lifted Golay code over $\mathbb{Z}_4$, *J. Combin. Designs*, to appear.

[126] —— and H. Kimura, New extremal doubly-even $[64,33,12]$ codes, *DCC* **6** (1995), 91–96.

[127] —— —— On extremal self-dual codes, *Math. J. Okayama Univ.* **37** (1995), 1–14.

[128] —— and M. Oura, On the Hamming weight enumerators of self-dual codes over $\mathbb{Z}_k$, preprint, Oct. 1997.

[129] —— and M. Ozeki, Extremal self-dual codes with the smallest covering radius, preprint.

[130] ____ and V.D. Tonchev, Singly-even self-dual codes and Hadamard matrices, in *Proc. Applied. Alg., Alg. Algorithms and Error-Correcting Codes*, ed. G. Cohen, M. Giusti and T. Mora, *Lecture Notes in Computer Science* **948** (1995), 279–284.

[131] F. Hirzebruch, The ring of Hilbert modular forms for real quadratic fields of small discriminant, in *Modular Functions of One Variable* **VI**, pp. 288–323. Proceedings, Bonn 1976, Lecture Notes in Mathematics No. 627, Springer-Verlag, NY, 1977. (*Ges. Abh.*, Vol. II, pp. 501–536.)

[132] ____ Letter to N. J. A. Sloane, Aug. 19, 1986. Reproduced in F. Hirzebruch, *Ges. Abh.*, Springer-Verlag, NY, Vol. II, 1987, pp. 796–798.

[133] M. Hochster and J. A. Eagon, Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci, *Amer. J. Math.* **93** (1971), 1020–1058.

[134] G. Höhn, Self-dual codes over the Kleinian four-group, preprint, 1996.

[135] G. Horrocks and D. Mumford, A rank 2 vector bundle on P^4 with 15,000 symmetries, *Topology* **12** (1973), 63–81.

[136] S. Houghten, C. Lam and L. Thiel, Construction of $(48, 24, 12)$ doubly-even self-dual codes, *Congr. Number* **103** (1994), 41–53.

[137] K. Huber, Codes over Gaussian integers, *PGIT* **40** (1994), 207–216.

[138] W. C. Huffman, The biweight enumerator of self-orthogonal codes, *DM* **26** (1978), 129–143.

[139] ____ Automorphisms of codes with applications to extremal doubly even codes of length 48, *PGIT* **28** (1982), 511–521.

[140] ____ Decomposing and shortening codes using automorphisms, *PGIT* **32** (1986), 833–836.

[141] ____ On the [24,12,10] quaternary code and binary codes with an automorphism having two cycles, *PGIT* **34** (1988), 486–493.

[142] ____ On the equivalence of codes and codes with an automorphism having two cycles, *DM* **83** (1990), 265–283.

[143] ____ On extremal self-dual quaternary codes of lengths 18 to 28, I, *PGIT* **36** (1990), 651–660.

[144] ____ On 3-elements in monomial automorphism groups of quaternary codes, *PGIT* **36** (1990), 660–664.

[145] ____ On extremal self-dual quaternary codes of lengths 18 to 28, II, *PGIT* **37** (1991), 1206–1216.

[146] ____ On extremal self-dual ternary codes of lengths 28 to 40, *PGIT* **38** (1992), 1395–1400.

[147] ____ On the classification of self-dual codes, *Proc. 34th Allerton Conf. Commun. Control and Computing*, October 2–4, 1996, pp. 302–311.

[148] ____ Characterization of quaternary extremal codes of lengths 18 and 20, *PGIT* **43** (1997), 1613–1616.

[149] ____ Decompositions and extremal type II codes over $\mathbb{Z}_4$, *PGIT*, **44** (1998), 800–809.

[150] ____ and N. J. A. Sloane, Most primitive groups have messy invariants, *Advances in Math.* **32** (1979), 118–127.

[151] ____ and V. D. Tonchev, The existence of extremal $[50, 25, 10]$ codes and quasi-symmetric 2-(49,9,6) designs, *DCC* **6** (1995), 97–106.

[152] ____ ____ The $[52, 26, 10]$ binary self-dual codes with an automorphism of order 7, preprint.

[153] ____ and V. Y. Yorgov, A $[72, 36, 16]$ doubly even code does not have an automorphism of order 11, *PGIT* **33** (1987), 749–752.

[154] V. I. Iorgov: see V. Y. Yorgov.

[155] N. Jacobson, *Lectures in Abstract Algebra*, 3 vols., Van Nostrand, Princeton, 1951-1964.

[156] D. B. Jaffe, Binary linear codes: new results on nonexistence. Available from http://www.math.unl.edu/∼djaffe/codes/code.ps.gz.

[157] S. N. Kapralov and V. D. Tonchev, Extremal doubly-even codes of length 64 derived from symmetric designs, *DM* **83** (1990), 285–289.

[158] M. Karlin, New binary coding results by circulants, *PGIT* **15** (1969), 81–92.

[159] G. T. Kennedy, Weight distributions of linear codes and the Gleason-Pierce theorem, *JCT* **A 67** (1994), 72–88.

[160] ____ and V. Pless, On designs and formally self-dual codes, *DCC* **4** (1994), 43–55.

[161] ____ ____ A coding theoretic approach to extending designs, *DM* **142** (1995), 155–168.

[162] H. Kimura, Extremal doubly even $(56, 28, 12)$ codes and Hadamard matrices of order 28, *Australas. J. Combin.* **10** (1994), 171–180.

[163] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[164] F. Klein, Weitere Untersuchunger über das Ikosaeder, *Math. Ann.* **12** (1877) (*Ges. Math. Abh.* III, 321–384).

[165] ____ *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*, 2nd ed., Dover, NY 1956.

[166] M. Klemm, Ueber die Identität von MacWilliams für die Gewichtsfunktion von Codes, *Archiv Math.* **49** (1987), 400-406.

[167] ____ Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4, *Archiv Math.* **53** (1989), 201–207.

[168] H. Koch, Unimodular lattices and self-dual codes, in *Proc. Intern. Congress Math., Berkeley 1986*, Amer. Math. Soc. Providence RI **1** (1987), pp. 457–465.

[169] ____ On self-dual, doubly-even codes of length 32, *JCT* **A 51** (1989), 63–76.

[170] ____ On self-dual doubly-even extremal codes, *DM* **83** (1990), 291–300.

[171] ____ and B. B. Venkov, Ueber ganzzahlige unimodulare euklidische Gitter, *J. reine angew. Math.* **398** (1989), 144–168.

[172] S. S. Koh, editor, *Invariant Theory*, *Lect. Notes Math.* **1278**, Springer-Verlag, NY, 1987.

[173] I. Krasikov and S. Litsyn, Linear programming bounds for doubly-even self-dual codes, *PGIT* **43** (1997), 1238–1244.

[174] F. R. Kschischang and S. Pasupathy, Some ternary and quaternary codes and associated sphere packings, *PGIT* **38** (1992), 227–246.

[175] C. W. H. Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly* **98** (1991) 305–318.

[176] ____ and V. Pless, There is no (24,12,10) self-dual quaternary code, *PGIT* **36** (1990), 1153–1156.

[177] ____ L. Thiel and S. Swiercz, The non-existence of finite projective planes of order 10, *Canad. J. Math.* **41** (1989), 1117–1123.

[178] S. Lang, *Algebra*, Addison-Wesley, Reading, MA, 1965.

[179] J. S. Leon, J. M. Masley and V. Pless, Duadic codes, *PGIT* **30** (1984), 709–714.

[180] ____ V. Pless and N. J. A. Sloane, On ternary self-dual codes of length 24, *PGIT* **27**, (1981), 176–180.

[181] ____ ____ ____ Self-dual codes over GF(5), *JCT* **A 32** (1982), 178–194.

[182] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, NY, 1982.

[183] D. E. Littlewood, *A University Algebra*, Dover, NY, 2nd ed., 1970.

[184] X. Ma and L. Zhu, Nonexistence of extremal doubly even self-dual codes, preprint, 1997.

[185] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **43** (1964), 485–505.

[186] ____ Orthogonal matrices over finite fields, *Amer. Math. Monthly* **76** (1969), 152–164.

[187] ____ Orthogonal circulant matrices over finite fields, and how to find them, *JCT* **10** (1971), 1–17.

[188] ____ C. L. Mallows and N. J. A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *PGIT* **18** (1972), 794–805.

[189] ____ A. M. Odlyzko, N. J. A. Sloane and H. N. Ward, Self-dual codes over GF(4), *JCT* **A 25** (1978), 288–318

[190] ____ and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[191] ____ ____ and J. G. Thompson, Good self-dual codes exist, *DM* **3** (1972), 153–162.

[192] ____ ____ ____ On the existence of a projective plane of order 10, *JCT* **A 14** (1973), 66–78.

[193] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, Upper bounds for modular forms, lattices and codes, *J. Algebra* **36** (1975), 68–76.

[194] ____ V. Pless and N. J. A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.* **31** (1976), 649–666.

[195] ____ and N. J. A. Sloane, On the invariants of a linear group of order 336, *Proc. Camb. Phil. Soc.* **74** (1973) 435–440.

[196] ____ ____ An upper bound for self-dual codes, *Information and Control* **22** (1973), 188–200.

[197] ____ ____ Weight enumerators of self-orthogonal codes, *DM* **9** (1974), 391–400.

[198] ____ ____ Weight enumerators of self-orthogonal codes over $GF(3)$, *SIAM J. Algebraic and Discrete Methods* **2** (1981), 425–460.

[199] R. J. McEliece, personal communication.

[200] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and Applications of Finite Groups*, Dover, NY, 1961.

[201] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer-Verlag, NY, 1973.

[202] T. Molien, Ueber die invarianten der linear Substitutionsgruppe, *Sitzungsber König. Akad. Wiss.*, (1897), 1152–1156.

[203] E. H. Moore, *Double Circulant Codes and Related Algebraic Structures*, Ph.D. Dissertation, Dartmouth College, July 1976.

[204] E. H. Moore, Using the group of a code to compute its minimal weights, preprint.

[205] D. Mumford and J. Fogarty, *Geometric Invariant Theory*, Springer-Verlag, NY, 2nd ed., 1982.

[206] E. Noether, Der Endlichkeitsatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1916), 89–92.

[207] H. Oral and K. T. Phelps, Almost all self-dual codes are rigid, *JCT* **A 60** (1992), 264–276.

[208] M. Ozeki, On the basis problem for Siegel modular forms of degree 2, *Acta Arith.* **31** (1976), 17–30.

[209] ——— On even unimodular positive definite quadratic lattices of rank 32, *Math. Z.* **191** (1986), 283–291.

[210] ——— On the configurations of even unimodular lattices of rank 48, *Archiv Math.* **46** (1986), 54–61.

[211] ——— Hadamard matrices and doubly even self-dual error-correcting codes, *JCT* **A 44** (1987), 274–287.

[212] ——— Examples of even unimodular extremal lattices of rank 40 and their Siegel theta-series of degree 2, *J. Number Theory* **28** (1988), 119–131.

[213] ——— Ternary code construction of even unimodular lattices, in *Theorie des Nombres, Quebec 1987*, Gruyter, Berlin, 1989, pp. 772–784.

[214] ——— On the structure of even unimodular extremal lattices of rank 40, *Rocky Mtn. J. Math.* **19** (1989), 847–862.

[215] ——— On a class of self-dual ternary codes, *Science Reports Hirosaki Univ.* **36** (1989), 184–191.

[216] ——— Quinary code construction of the Leech lattice, *Nihonkai Math. J.* **2** (1991), 155–167.

[217] ——— On intersection properties of extremal ternary codes, *JCT*, to appear.

[218] ——— On the notion of Jacobi polynomials for codes, *Math. Proc. Camb. Phil. Soc.* **121** (1997), 15–30.

[219] ____ On covering radius and coset weight distributions of extremal binary self-dual codes of length 40, *Theoret. Comp. Sci.*, to appear.

[220] G. Pasquier, The binary Golay code obtained from an extended cyclic code over F_8, *Europ J. Combinatorics* **1** (1980), 369–370.

[221] ____ A binary extremal doubly-even self-dual code $[64, 32, 12]$ obtained from an extended Reed-Solomon code over $\mathbb{F}_{16}$, *PGIT* **27** (1981), 807–808.

[222] ____ Projections et images binaries de codes sur F_{2^m}, *Rev. CETHEDEC* **2** (1981), 45–56.

[223] ____ Binary images of some self-dual codes over $GF(2^m)$ with respect to trace-orthogonal basis, *DM* **37** (1981), 127–129.

[224] N. J. Patterson, personal communication, 1980.

[225] P. M. Piret, Algebraic construction of cyclic codes over $\mathbb{Z}_8$ with a good Euclidean minimum distance, *PGIT* **41** (1995), 815–817.

[226] V. Pless, The number of isotropic subspaces in a finite geometry, Rend. Cl. Scienze fisiche, matematiche e naturali, *Acc. Naz. Lincei* **39** (1965), 418–421.

[227] ____ On the uniqueness of the Golay codes, *JCT* **5** (1968), 215–228.

[228] ____ On a new family of symmetry codes and related new five-designs, *Bull. Amer. Math. Soc.* **75** (1969), 1339–1342.

[229] ____ A classification of self-orthogonal codes over $GF(2)$, *DM* **3** (1972), 209–246.

[230] ____ Symmetry codes over $GF(3)$ and new five-designs, *JCT* **A 12** (1972), 119–142.

[231] ____ 23 does not divide the order of the group of a (72,36,16) doubly even code, *PGIT* **28** (1982), 113–117.

[232] ____ The children of the (32,16) doubly even codes, *PGIT* **24** (1978), 738–746.

[233] ____ A decoding scheme for the ternary Golay code, in *Proc. 20th Allerton Conf. Comm. Control., Univ. of Ill., Urbana, 1982*, pp. 682–687.

[234] ____ On the existence of some extremal self-dual codes, in D. M. Jackson and S. A. Vanstone, editors, *Enumeration and Design*, Academic Press, 1984, pp. 245–250.

[235] ——— Q-codes, *JCT* **A 43** (1986), 258–276.

[236] ——— Decoding the Golay codes, *PGIT* **32** (1986), 561–567.

[237] ——— Extremal codes are homogeneous, *PGIT* **35** (1989), 1329–1330.

[238] ——— Parents, children, neighbors and the shadow, *Contemporary Math.* **168** (1994), 279–290.

[239] ——— J. S. Leon and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *JCT* **A 78** (1997), 32–50.

[240] ——— and J. N. Pierce, Self-dual codes over $GF(q)$ satisfy a modified Varshamov-Gilbert bound, *Information and Control* **23** (1973), 35–40.

[241] ——— and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, *PGIT* **42** (1996), 1594–1600.

[242] ——— and N. J. A. Sloane, On the classification and enumeration of self-dual codes, *JCT* **A 18** (1975), 313–335.

[243] ——— ——— and H. N. Ward, Ternary codes of minimum weight 6 and the classification of self-dual codes of length 20, *PGIT* **26** (1980), 305–316.

[244] ——— P. Solé and Z. Qian, Cyclic self-dual $\mathbb{Z}_4$-codes, *Finite Fields Appl.* **3** (1997), 48–69.

[245] ——— and J. G. Thompson, 17 does not divide the order of a group of a (72,36,16) code, *PGIT* **28** (1982), 537–541.

[246] ——— and V. D. Tonchev, Self-dual codes over $GF(7)$, *PGIT* **33** (1987), 723–727.

[247] ——— ——— and J. Leon, On the existence of a certain $(64, 32, 12)$ extremal code, *PGIT* **39** (1993), 214–215.

[248] A. Poli and C. Rigoni, Enumeration of self-dual $2k$ circulant codes, *Lect. Notes. Comput. Sci.* **228** (1986), 61–70.

[249] E. M. Rains, Nonbinary quantum codes, preprint.

[250] ——— Shadow bounds for self-dual codes, **44** (1998), 134–139.

[251] ____ Quantum shadow enumerators, preprint.

[252] ____ Quantum weight enumerators, preprint.

[253] ____ Polynomial invariants of quantum codes, preprint.

[254] ____ Optimal self-dual codes over $\mathbb{Z}_4$, preprint.

[255] ____ Bounds for self-dual codes over $\mathbb{Z}_4$, preprint.

[256] ____ and N. J. A. Sloane, The shadow theory of modular and unimodular lattices, preprint.

[257] S. J. Rallis, New and old results in invariant theory with applications to arithmetic groups, in *Symmetric Spaces*, W. M. Boothby and G. L. Weiss, Eds., Dekker, NY, 1972, pp. 443–458.

[258] M. Ran and J. Snyders, On maximum likelihood soft decoding of binary self-dual codes, *IEEE Trans. Commun.* **41** (1993), 439–443.

[259] ____ ____ Constrained designs for maximum likelihood soft decoding of $RM(2, m)$ and the extended Golay codes, *IEEE Trans. Commun.* **43** (1995), 812–820.

[260] ____ ____ A cyclic $[6, 3, 4]$ group code and the hexacode over $GF(4)$, *PGIT* **42** (1996), 1250–1253.

[261] C. Reid, *Hilbert*, Springer-Verlag, NY, 1970.

[262] C.-G. Rota, *Combinatorial Theory and Invariant Theory*, Bowdoin College, 1971.

[263] B. Runge, On Siegel modular forms I, *J. reine angew. Math.* **436** (1993), 57–85.

[264] ____ On Siegel modular forms II, *Nagoya Math. J.* **138** (1995), 179–197.

[265] ____ Thetafunctions and Siegel-Jacobi forms, *Acta Math.* **175** (1995), 165–196.

[266] ____ Codes and Siegel modular forms, *DM* **148** (1996), 175–204.

[267] R. P. Ruseva, Uniqueness of the $[36, 18, 8]$ double circulant code, in *Proc. Internat. Workshop on Optimal Codes and Related Topics*, May 26–June 1, 1995, Sozopol, Bulgaria, 126–129.

[268] ____ New extremal self-dual codes of length 36, in *Proc. of the* 25^{th} *Spring Conf. of the UBM*, 1996, 150–153.

[269] ____ On the extremal self-dual binary codes of length 38 with an automorphism of order 7, preprint.

[270] J. A. Rush, A lower bound on packing density, *Invent. Math.* **98** (1989), 499–509.

[271] ____ A bound, and a conjecture, on the maximum lattice-packing density of a superball, *Mathematika* **40** (1993), 137–143.

[272] ____ and N. J. A. Sloane, An improvement to the Minkowski-Hlawka bound for packing superballs, *Mathematika* **34** (1987), 8–18.

[273] R. A. Sack, Interpretation of Lagrange's expansion and its generalization to several variables as integration formulas, *J. SIAM* **13** (1965), 47–59.

[274] ____ Generalization of Lagrange's expansion for functions of several implicitly defined variables, *J. SIAM* **13** (1965), 913–926.

[275] ____ Factorization of Lagrange's expansion by means of exponential generating functions, *J. SIAM* **14** (1966), 1–15.

[276] W. Scharlau and D. Schomaker, personal communication, April 1991.

[277] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, NY, 1977.

[278] P. Shankar, On BCH codes over arbitrary integer rings, *PGIT* **25** (1979), 480–483.

[279] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274–304.

[280] K. Shiromoto, A new MacWilliams type identity for linear codes, *Hokkaido Math. J.* **25** (1996), 651–656.

[281] P. W. Shor and R. Laflamme, Quantum analog of the MacWilliams identities in classical coding theory, *Phys. Rev. Lett.* **78** (1997), 1600–1602.

[282] N. J. A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code?, *PGIT* **19** (1973), 251.

[283] ____ Weight enumerators of codes, in *Combinatorics*, M. Hall Jr. and J. H. van Lint, Eds., Mathematical Centre, Amsterdam and Reidel Publishing Co., Dordrecht, Holland, 1975, pp. 115–142.

[284] ____ Error-correcting codes and invariant theory: New applications of a nineteenth-century technique, *Amer. Math. Monthly* **84** (1977), 82–107.

[285] ____ Binary codes, lattices and sphere-packings, in *Combinatorial Surveys: Proceedings of the Sixth British Combinatorial Conference*, P. J. Comeron, Ed., Academic Press, NY, 1977, pp. 117–164.

[286] ____ Codes over $GF(4)$ and complex lattices, *J. Algebra* **52** (1978), 168–181.

[287] ____ Self-dual codes and lattices, in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math., Vol 34, American Mathematical Society, Providence, RI, 1979, pp. 273–308.

[288] ____ and J. G. Thompson, Cyclic self-dual codes, *PGIT* **29** (1983), 364–366.

[289] L. Smith, *Polynomial Invariants of Finite Groups*, Peters, Wellesley, MA, 1995.

[290] ____ Polynomial invariants of finite groups. A survey of recent developments, *Bull. Amer. Math. Soc.* **34** (1997), 211–250.

[291] S. L. Snover, The uniqueness of the Nordstrom–Robinson and the Golay binary codes, Ph.D. Dissertation, Department of Mathematics, Michigan State Univ., 1973.

[292] J. Snyders and Y. Be'ery, Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes, *PGIT* **35** (1989), 963–975.

[293] E. Spence and V. D. Tonchev, Extremal self-dual codes from symmetric designs, *DM* **110** (1992), 265–268.

[294] T. A. Springer, *Invariant Theory, Lect. Notes. Math.* **585**, Springer-Verlag, NY, 1977.

[295] R. P. Stanley, personal communication.

[296] ____ Invariants of finite groups and their applications to combinatorics, *Bull. Amer. Math. Soc.* **1** (1979), 475–511.

[297] D. Stanton, editor, *Invariant Theory and Tableaux*, Springer-Verlag, NY, 1990.

[298] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, NY, 1993.

[299] J. G. Thompson, Weighted averages associated to some codes, *Scripta Math.* **29** (1973), 449-452.

[300] V. D. Tonchev, Block designs of Hadamard type and self-dual codes, *Probl. Pered. Inform.* **19** (1983), No. 4, 25–30; English translation in *Prob. Inform. Trans.* **19** (1983), 270–274.

[301] ——— On the inequivalence of certain extremal self-dual codes, *Compt. Rend. Acad. Bulg. Sci.* **36** (1983) 181–184.

[302] ——— Quasi-symmetric designs and self-dual codes, *European J. Combin.* **7** (1986) 67–73.

[303] ——— *Combinatorial Configurations*, Longman, London, 1988.

[304] ——— Symmetric designs without ovals and extremal self-dual codes, *Ann. Discr. Math.* **37** (1988) 451–458.

[305] ——— Self-orthogonal designs and extremal doubly-even codes, *JCT* **A 52** (1989), 197–205.

[306] ——— Self-orthogonal designs, *Contemporary Math.* **111** (1990), 219–235.

[307] ——— Self-dual codes and Hadamard matrices, *Discr. Appl. Math.* **33** (1991), 235–240.

[308] ——— and R. V. Raev, Cyclic 2-(17, 8, 7) designs and related doubly even codes, *Comput. Rend. Acad. Bulg. Sci.* **35** (1982).

[309] ——— and V. Y. Yorgov, The existence of certain extremal $[54, 27, 10]$ self-dual codes, *PGIT* **42** (1996), 1628–1631.

[310] H.-P. Tsai, Existence of certain extremal self-dual codes, *PGIT* **38** (1992), 501–504.

[311] ——— Existence of some extremal self-dual codes, *PGIT* **38** (1992), 1829–1833.

[312] ——— The covering radius of extremal self-dual code D11 and its application, *PGIT* **43** (1997), 316–319.

[313] J. V. Uspensky, *Theory of Equations*, McGraw-Hill, NY, 1948.

[314] A. Vardy, The Nordstrom-Robinson code: representation over $GF(4)$ and efficient decoding, *PGIT* **40** (1994), 1686–1693.

[315] ____ Even more efficient bounded-distance decoding of the hexacode, the Golay code, and the Leech lattice, *PGIT* **41** (1995), 1495–1499.

[316] ____ and Y. Be'ery, More efficient soft-decision decoding of the Golay codes, *PGIT* **37** (1991), 667–672.

[317] M. Ventou and C. Rigoni, Self-dual doubly circulant codes, *DM* **56** (1985), 291–298.

[318] G. E. Wall, On Clifford collineation, transform and similarity groups IV, *Nagoya Math. J.* **21** (1962), 199–222.

[319] H. N. Ward, A restriction on the weight enumerator of self-dual codes, *JCT* **21** (1976), 253–255.

[320] ____ Divisible codes, *Archiv Math. (Basel)* **36** (1981), 485–494.

[321] ____ personal communication.

[322] ____ A bound for divisible codes, *PGIT* **38** (1992), 191–194.

[323] ____ and J. A. Wood, Characters and the equivalence of codes, *JCT* **A 73** (1996), 348–352.

[324] A. Weil, Sur certaines groupes d'opérateurs unitaires, *Acta Math.* **11** (1964), 143–211.

[325] H. Weyl, Invariants, *Duke Math. J.* **5** (1939), 489–502.

[326] ____ *The Classical Groups*, Princeton Univ. Press, Princeton, NJ, 1946.

[327] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge Univ. Press, 4th ed., 1963.

[328] J. Wolfmann, A new construction of the binary Golay code $[24, 12, 8]$ using a group algebra over a finite field, *DM* **31** (1980), 337-338.

[329] ____ A class of doubly even self-dual binary codes, *DM* **56** (1985), 299–303.

[330] ——— A group algebra construction of binary even self-dual codes, *DM* **65** (1987), 81–89.

[331] J. A. Wood, Duality for modules over finite rings and applications to coding theory, 1996, submitted to *Amer. J. Math.*

[332] V. Y. Yorgov, Binary self-dual codes with automorphisms of odd order, *Probl. Pered. Inform.* **19** (1983); English translation in *Prob. Inform. Trans.* **19** (1983), 11–24.

[333] ——— A method for constructing inequivalent self-dual codes with applications to length 56, *PGIT* **33** (1987), 77–82.

[334] ——— Doubly-even codes of length 64, *Probl. Pered. Inform.* **22** (1986), 35–42; English translation in *Prob. Inform. Trans.* **22** (1986), 277–284.

[335] ——— and R. Ruseva, Two extremal codes of length 42 and 44, *Probl. Pered. Inform.* **29** (1993), 99–103; English translation in *Prob. Inform. Trans.* **29** (1994), 385–388.

[336] ——— and N. Yankov, On the extremal binary codes of lengths 36 and 38 with an automorphism of order 5, *Proc. of the* 5^{th} *International Workshop on Algebraic and Combinatorial Coding Theory*, June 1–7, 1996, Sozopol, Bulgaria, 307–312.

[337] ——— and N. P. Ziapkov, Doubly-even self-dual $[40, 20, 8]$ codes with an automorphism of odd order, *Probl. Pered. Inform.* **32** (1996), 41–46; English translation in *Prob. Inform. Trans.* **32** (1996), 253–257.

[338] S. Zhang, On the nonexistence of extremal self-dual codes, preprint, 1997.