Hokkaido Mathematical Journal Vol. 28 (1999) p. 253–283

Self-dual codes over rings and the Chinese remainder theorem

Steven T. DOUGHERTY, Masaaki HARADA and Patrick SOLÉ

(Received June 9, 1997)

Abstract. We give some characterizations of self-dual codes over rings, specifically the ring $\mathbb{Z}_{2k}$, where $\mathbb{Z}_{2k}$ denotes the ring $\mathbb{Z}/2k\mathbb{Z}$ of integers modulo $2k$, using the Chinese Remainder Theorem, investigating Type I and Type II codes. The Chinese Remainder Theorem plays an important role in the study of self-dual codes over $\mathbb{Z}_{2k}$ when $2k$ is not a prime power, while the Hensel lift is a powerful tool when $2k$ is a prime power. In particular, we concentrate on the case $k = 3$ and use construction A to build unimodular and 3-modular lattices.

Key words: self-dual codes, codes over rings, unimodular lattices.

1. Introduction

Self-dual codes over finite fields, especially binary and ternary fields, are a well studied subject, including their relationship to lattices and designs. Recently, codes over rings have increased in importance, generating much interest in these codes, for example see [1], [2], [3], [7], [8], [11], [15], [16] and [23]. In this paper, we give some characterizations of self-dual codes over rings, specifically the ring $\mathbb{Z}_{2k}$, where $\mathbb{Z}_{2k}$ denotes the ring $\mathbb{Z}/2k\mathbb{Z}$ of integers modulo $2k$, using the Chinese Remainder Theorem. Recently, in [1] the notion of Type II codes over $\mathbb{Z}_{2k}$ has been introduced. Here, we investigate Type II codes over $\mathbb{Z}_{2k}$ using this theorem, giving special attention to the ring $\mathbb{Z}_6$.

We begin with some definitions. A code C over a ring R of length n is a subset of R^n, if it is an additive subgroup of R^n then it is called a linear code. In this paper all codes are assumed to be linear unless otherwise specified. An element of C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. We equip R^n with the standard inner-product, i.e. $[v,w] = \sum v_i w_i$. The orthogonal to a code is defined in the usual way, i.e. $C^\perp = \{v \in R^n \mid [v,w] = 0 \text{ for all } w \in C\}$ where $v = (v_1, v_2, \ldots, v_n)$ and $w = (w_1, w_2, \ldots, w_n)$. We say that a code C is *self-*

1991 Mathematics Subject Classification : Primary 94B25; Secondary 11H31.

orthogonal if $C \subseteq C^{\perp}$ and C is *self-dual* if $C = C^{\perp}$. MacWilliams relations for codes over any finite Frobenius ring are given in [23].

The paper is organized as follows. Section 2 gives some characterizations of self-dual codes over rings, specifically the ring $\mathbb{Z}_{2k}$. In Section 3, we pay attention to the ring $\mathbb{Z}_6$. Some families of self-dual codes over $\mathbb{Z}_6$ (called *senary* codes) are also introduced. Section 4 deals with unimodular lattices corresponding to senary codes. In Sections 5 and 6, we investigate self-dual codes constructed from projective planes and weighing matrices. In the final section, we introduce new weight enumerators and establish their MacWilliams relations.

2. The Chinese Remainder Theorem and Self-Dual Codes

Let R be a commutative ring (not necessarily finite) with a multiplicative identity denoted by 1. Let $I_1, I_2, \ldots, I_k$ be ideals of R such that:

1. $S_i = R/I_i$ is finite,
2. $I_j + \bigcap_{k \neq j} I_k = R$ for $1 \leq j \leq k$.

That is, the ideals are relative prime, since R is commutative.

Set $I = \cap I_i$ and $S = R/I$. Define the map

$$\Psi : S \to (R/I_1) \times (R/I_2) \times \cdots \times (R/I_k),$$

by

$$\Psi(\alpha) = (\alpha \pmod{I_1}, \alpha \pmod{I_2}, \ldots, \alpha \pmod{I_k}).$$

The map Ψ^{-1} is a ring isomorphism by the generalized Chinese Remainder Theorem.

Let $C_1, C_2, \ldots, C_k$ be codes where C_i is a code over S_i, and define the code

$$\mathrm{CRT}(C_1, C_2, \ldots, C_k) = \{\Psi^{-1}(v_1, v_2, \ldots, v_k) \mid v_i \in C_i\}.$$

We say that the code $\mathrm{CRT}(C_1, C_2, \ldots, C_k)$ is *the Chinese product* of codes $C_1, C_2, \ldots, C_k$. It is clear that $|\mathrm{CRT}(C_1, C_2, \ldots, C_k)| = \prod_{i=1}^{k} |C_i|$ and that if C_i is self-orthogonal for all i then $\mathrm{CRT}(C_1, C_2, \ldots, C_k)$ is self-orthogonal. This gives the following:

Theorem 2.1 $\mathrm{CRT}(C_1, C_2, \ldots, C_k)$ *is a self-dual code over S if and only if it is the Chinese product of self-dual codes $C_1, \ldots, C_k$ over $S_1, \ldots, S_k$, respectively.*

We have the following restriction on the length of certain self-dual codes over $\mathbb{Z}_k$.

Corollary 2.2 *Let $s = p_1^{e_1} \cdots p_j^{e_j}$ where p_i is prime for all $i = 1, \ldots, j$. Suppose that there is at least one i such that $e_i = 1$. Then, if a self-dual code C of length n over $\mathbb{Z}_s$ exists, n is even. In addition, if $p_i \equiv 3 \pmod 4$, then, if a self-dual code C of length n over $\mathbb{Z}_s$ exists, n is a multiple of four.*

Proof. If there is a self-dual code of length n over the finite field $\mathbb{F}_p$ where p is prime then n is even. Since C is the Chinese product of a self-dual codes over $\mathbb{Z}_{p_1^{e_1}}, \ldots, \mathbb{Z}_{p_j^{e_j}}$ where at least one $\mathbb{Z}_{p_i}$ is the finite field, the length n of C must be even. Moreover it is known that if there is a self-dual code of length n over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$ then n is a multiple of four (cf. [20] and [21]). □

2.1. Type II Codes over $\mathbb{Z}_{2k}$

We begin by giving some characterizations of Type II codes over $\mathbb{Z}_{2k}$ by the Chinese product.

Recently, codes over $\mathbb{Z}_4$ have grown in importance. Interesting connections with binary codes and unimodular lattices have been found. Further connections have been found with codes over $\mathbb{Z}_{2k}$ (cf. [1]). The connection between codes over $\mathbb{Z}_4$ and unimodular lattices prompted the definition of the Euclidean weight of a vector of $\mathbb{Z}_4^n$ (cf. [2] and [3]). We defined the Euclidean weights of the elements $0, \pm 1, \pm 2, \pm 3, \ldots, \pm(k-1), k$ of $\mathbb{Z}_{2k}$ as $0, 1, 4, 9, \ldots, (k-1)^2, k^2$, respectively (cf. [1]). The Euclidean weight of a vector is just the rational sum of the Euclidean weights of its components. The Hamming weight of a vector is the number of non-zero components in the vector. We defined a *Type II* code over $\mathbb{Z}_{2k}$ as a self-dual code with all codewords having Euclidean weight a multiple of $4k$, see [1] for a complete discussion of these codes. If a self-dual code is not Type II, then it is said to be *Type I*. The notion of extremality for the Euclidean weight was also given in [1].

Theorem 2.3 *Let $2k = 2^m r$ where r is odd. A code C is a Type* II *code over $\mathbb{Z}_{2k}$ if and only if it is the Chinese product of a Type* II *code over $\mathbb{Z}_{2^m}$ and a self-dual code over $\mathbb{Z}_r$.*

Proof. If $\alpha \in \mathbb{Z}_{2^m r}$ then there is a unique $0 \leq \beta < 2^m$ such that $\alpha = q2^m + \beta$ for some integer q. This implies $\alpha \equiv \beta \pmod{2^m}$ and, taking squares

$$\alpha^2 \equiv \beta^2 \pmod{2^{m+1}},$$

i.e.

$$\alpha^2 \equiv (\alpha \pmod{2^m})^2 \pmod{2^{m+1}}.$$

Then if $v = (v_i)$ is a vector over $\mathbb{Z}_{2^m r}$ with Euclidean weight divisible by $2^{m+1}r$, we have

$$\sum v_i^2 \equiv 0 \pmod{2^{m+1}r},$$

if and only if both

$$\sum (v_i \pmod{2^m})^2 \equiv 0 \pmod{2^{m+1}},$$

and

$$\sum (v_i \pmod{r})^2 \equiv 0 \pmod{r},$$

hold. □

The following corollary was shown in [1]. Here we give an alternative proof.

Corollary 2.4 *If there is a Type* II *code C of length n over $\mathbb{Z}_{2^m r}$ where r is odd, then n is a multiple of eight.*

Proof. Let $r = p_1^{e_1} \cdots p_j^{e_j}$ where p_i is prime. Then C is the Chinese product of a self-dual code over $\mathbb{Z}_{2^m}$ and codes over rings $\mathbb{Z}_{p_1^{e_1}}, \ldots, \mathbb{Z}_{p_i^{e_i}}$. It is known in [8] that if there is a Type II code of length n over $\mathbb{Z}_{2^m}$ then n must be a multiple of eight. □

Recently the notion of shadow codes over $\mathbb{Z}_4$ has been introduced by the authors [10]. Here we consider shadow codes over $\mathbb{Z}_{2k}$. Similarly to $\mathbb{Z}_4$, we pay attention to a certain subcode of index 2. The *even weight subcode* C_0 of a Type I code C over $\mathbb{Z}_{2k}$ is the set of codewords of C of Euclidean weights divisible by $4k$.

Lemma 2.5 *The subcode C_0 is $\mathbb{Z}_{2k}$-linear of index 2 in C.*

Proof. The first assertion follows by the self-duality of C using the relation

$$w_E(x+y) = w_E(x) + w_E(y) + 2(x,y), \tag{1}$$

where $w_E(x)$ denotes the Euclidean weight of a vector x. The second assertion follows by observing that every codeword y of C has an Euclidean weight divisible by $2k$. By the preceding relation we see that $C_2 := C - C_0$ is of the form $x + C_0$ where x is any codeword of C of Euclidean weight congruent to $2k$ mod $4k$ and that translation by x is a one to one map from C_0 onto C_2. □

By the preceding lemma we see that C is of index 2 in $C_0^\perp$ and we let $C_0^\perp = C \bigcup C_1 \bigcup C_3$. With these notations define the *shadow* of C as $S := C_1 \bigcup C_3$. Unlike the binary case, $C_0^\perp / C_0$ is not necessarily isomorphic to the Klein 4-group, it may be isomorphic to either the Klein 4-group or the cyclic group of order 4.

We now give some characterizations of shadow codes using the Chinese Remainder Theorem.

Lemma 2.6 *If k is an odd prime and $C = \mathrm{CRT}(B, K)$ with B a binary code and K a code over $\mathbb{Z}_k$ then $C_0 = \mathrm{CRT}(B_0, K)$, with B_0 the even weight subcode of B, that is, the doubly-even subcode.*

Proof. Follows from the fact that the Euclidean weight of a vector x is divisible by $4k$ if and only if the Hamming weight of the binary vector $(x \pmod 2)$ is doubly-even and the Euclidean weight of the vector $x \pmod k$ over $\mathbb{Z}_k$ is divisible by k, where x is an element of $\mathbb{Z}_{2k}$. □

Proposition 2.7 *Let S_b be the shadow of B defined as $B_0^\perp = B \bigcup S_b$. Then $C_0^\perp = \mathrm{CRT}(B_0^\perp, K)$ and $S = \mathrm{CRT}(S_b, K)$.*

Proof. Let x and y be elements of $\mathbb{Z}_{2k}^n$, then it is easy to see that $[x, y] = 0$ if and only if $[x \pmod 2), y \pmod 2)] = 0$ and $[x \pmod k), y \pmod k)] = 0$. By Lemma 2.6, $C_0 = \mathrm{CRT}(B_0, K)$. Thus $C_0^\perp = \mathrm{CRT}(B_0^\perp, K)$. Moreover $S = C_0^\perp - C$ is the same as $\mathrm{CRT}(B_0^\perp - B, K) = \mathrm{CRT}(S_b, K)$. □

2.2. Codes over Polynomial Rings

Let $\mathbb{F}$ be a finite field and let $\mathbb{F}[x]$ be the ring of polynomials over $\mathbb{F}$. Let $q(x)$ be a polynomial in $\mathbb{F}[x]$ such that the factorization of $q(x)$ is given by:

$$q(x) = p_1(x)p_2(x) \cdots p_r(x),$$

where $p_i(x)$ is a non-constant irreducible polynomial and $\gcd(p_i(x), p_j(x)) \in \mathbb{F}$.

Let $S_i = \mathbb{F}[x]/(p_i(x))$, i.e. S_i is a finite field, and $S = \mathbb{F}[x]/(q(x))$, which is a field only if $r = 1$. Given codes over S_i the Chinese product can be used to construct codes over S. This gives the following characterization of codes over a certain residue class ring $\mathbb{F}[x]/(q(x))$.

Proposition 2.8 *Let $q(x)$ be a polynomial in $\mathbb{F}[x]$ such that the factorization of $q(x)$ is given by:*

$$q(x) = p_1(x)p_2(x)\cdots p_r(x),$$

where $p_i(x)$ is a non-constant irreducible polynomial and $\gcd(p_i(x), p_j(x)) \in \mathbb{F}$ *for $i \neq j$. Then a code over the ring $\mathbb{F}[x]/(q(x))$ is the Chinese product of codes over some finite fields.*

Example 1. Let $\mathbb{F} = \mathbb{Z}_2$ and let $q(x) = x(x^2 + x + 1)$. This gives that S_1 is isomorphic to the finite field $\mathbb{F}_2$ with 2 elements and S_2 is isomorphic to the finite field $\mathbb{F}_4$, and S is a ring with 8 elements.

3. Senary Self-Dual Codes

In this section we concentrate on self-dual codes over $\mathbb{Z}_6$. The symmetrized weight enumerator (swe) of a senary code C is defined as:

$$swe_C(a, b, c, d) := \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)} d^{n_3(x)},$$

where $n_i(x)$ denotes the number of j such that $x_j = \pm i$. We say that two codes over $\mathbb{Z}_k$ are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called *permutation-equivalent.*

3.1. Some Families of Senary Self-Dual Codes

We introduce a few families of senary self-dual codes together with Type II codes. Note that we can regard the lifted symmetry codes and the MacKay codes as bordered double circulant codes since the matrix W is a circulant matrix.

3.1.1. Extended Cyclic Codes. The Chinese Remainder Theorem gives much information on the Chinese product codes. For example, if a permutation $\sigma \in S_n$ is an automorphism of the Chinese product $\mathrm{CRT}(B, T)$ then σ is also an automorphism of the binary code B and the ternary code

T, where S_n is the symmetry group of degree n.

In fact, the Chinese product of two cyclic codes is again a cyclic code. An extremal Type II code of length 24 was found in [1]. This code is an extended cyclic code of length 24 and the Chinese product of two extended cyclic quadratic residue codes over $\mathbb{Z}_2$ and $\mathbb{Z}_3$. The next length for Type II codes is 32. There is no ternary self-dual code of length 32 with automorphism of order 31 (cf. [14]). Thus, this gives that there is no senary extended cyclic self-dual code of length 32.

3.1.2. Lifted Symmetry Codes. We introduce families of double circulant codes. Of course, senary double circulant codes are constructed from binary and ternary double circulant codes.

Here we describe a family of codes above the Pless symmetry codes. Let q be a prime power $\equiv -1 \pmod 6$, and denote by χ the quadratic character of $\mathbb{F}_q$. We begin by recalling some basic facts about the Jacobsthal matrix which hold more generally for any odd q. This matrix $W = (W_{i,j})$ is indexed by the elements of $\mathbb{F}_q$ and has for a typical entry

$$W_{i,j} := \chi(j - i).$$

The matrix W is instrumental in building Hadamard matrices of Paley type [17, Chap. II]. We collect here the properties that we need:

(J1) $JW = WJ = 0$

(J2) $WW^T = qI - J$

(J3) $A := \sum_{i=\Box} W_{-i,1} = -1$

(J4) $B := \sum_{i=\Box} W_{i,1} = 0$

where J stands for the all-one matrix. See [17, Chap. II, Lemma 7] for proofs of (J1) and (J2). To prove (J3), (J4) observe firstly that by ($J1$) we have, knowing that -1 is not a quadratic residue, that $A + B = -1$. Secondly we have

$$B = \frac{1}{2} \sum_{x \in \mathbb{F}_q,\, x \neq 0} \chi(1 - x^2),$$

and by the character property of χ

$$B = \frac{1}{2} \sum_{x \in \mathbb{F}_q,\, x \neq 0} \chi(1 - x)\chi(1 + x) = 0,$$

the last equality coming from (J2).

Now we define the matrix S_q as

$$S_q = \begin{pmatrix} 0 & 1 \cdots 1 \\ \chi(-1) & \\ \vdots & W \\ \chi(-1) & \end{pmatrix},$$

which is $q+1$ by $q+1$ and satisfies $S_q S_q^T = qI$. Define a generator matrix of size $q+1$ by $2q+2$ over $\mathbb{Z}_6$ by the rule

$$G = (I \ , \ S_q).$$

Theorem 3.1 *The matrix G generates a self-dual code $P(n)$ of length $n = 2q+2$ over $\mathbb{Z}_6$. If furthermore $q \equiv -1 \pmod{12}$ then $P(n)$ is Type* II.

Proof. By (J1) the rows of G are pairwise orthogonal. They are isotropic by the choice of q, since the inner-product of every row with itself is $q+1$. Now in case q satisfies the congruence mod 12, the Euclidean weight of each row of G is divisible by 12 by the choice of q. This carries over to the row span by [1]. □

$P(n)$ is the Chinese product of the ternary Pless symmetry code with generator matrix G and the binary self-dual codes with generator matrix $(I \ , \ J-I)$. Thus we say that the above codes $P(n)$ are the lifted symmetry codes. Of special interest are $q=5$ yielding a Type I code above the Golay code, $q=17$ yielding a Type I code of length 36, $q=11,23$ yielding Type II codes of lengths 24 and 48.

We have obtained by computer that the symmetrized weight enumerators of the lifted symmetry codes $P(12)$ and $P(24)$ of lengths 12 and 24:

$$\begin{aligned} swe_{P(12)} = {} & d^{12} + 24c^6d^6 + 24c^{12} + 120bc^8d^3 + 120b^2c^4d^6 + 1280b^3c^6d^3 \\ & + 360b^4c^8 + 1680b^5c^4d^3 + 264b^6d^6 + 768b^6c^6 + 360b^8c^4 \\ & + 440b^9d^3 + 24b^{12} + 240abc^5d^5 + 1440ab^2c^7d^2 + 960ab^3c^3d^5 \\ & + 5760ab^4c^5d^2 + 3360ab^6c^3d^2 + 120a^2c^6d^4 + 2280a^2b^2c^4d^4 \\ & + 3360a^2b^3c^6d + 1800a^2b^4c^2d^4 + 5760a^2b^5c^4d + 1440a^2b^7c^2d \\ & + 440a^3c^9 + 960a^3bc^5d^3 + 3360a^3b^3c^3d^3 + 1680a^3b^4c^5 \end{aligned}$$

$$+ 960a^3b^5cd^3 + 1280a^3b^6c^3 + 120a^3b^8c + 15a^4d^8 + 1800a^4b^2c^4d^2$$
$$+ 2280a^4b^4c^2d^2 + 120a^4b^6d^2 + 960a^5b^3c^3d + 240a^5b^5cd$$
$$+ 32a^6d^6 + 264a^6c^6 + 120a^6b^4c^2 + 24a^6b^6 + 15a^8d^4 + a^{12},$$

$$\begin{aligned}
swe_{P(24)} = {} & d^{24} + 1104c^{12}d^{12} + 48c^{24} + 3168bc^{20}d^3 + 23760b^2c^{16}d^6 \\
& + 116160b^3c^{12}d^9 + 23760b^4c^8d^{12} + 3168b^4c^{20} + 3168b^5c^4d^{15} \\
& + 332640b^5c^{16}d^3 + 4040256b^6c^{12}d^6 + 1045440b^7c^8d^9 \\
& + 190080b^8c^4d^{12} + 23760b^8c^{16} + 4048b^9d^{15} + 7846080b^9c^{12}d^3 \\
& + 5844960b^{10}c^8d^6 + 2059200b^{11}c^4d^9 + 61824b^{12}d^{12} \\
& + 142656b^{12}c^{12} + 3326400b^{13}c^8d^3 + 3769920b^{14}c^4d^6 \\
& + 242880b^{15}d^9 + 23760b^{16}c^8 + 902880b^{17}c^4d^3 + 198352b^{18}d^6 \\
& + 3168b^{20}c^4 + 24288b^{21}d^3 + 48b^{24} + 95040ab^2c^{19}d^2 \\
& + 633600ab^3c^{15}d^5 + 3326400ab^4c^{11}d^8 + 380160ab^5c^7d^{11} \\
& + 31680ab^6c^3d^{14} + 2661120ab^6c^{15}d^2 + 41665536ab^7c^{11}d^5 \\
& + 9504000ab^8c^7d^8 + 1013760ab^9c^3d^{11} + 28245888ab^{10}c^{11}d^2 \\
& + 25470720ab^{11}c^7d^5 + 6177600ab^{12}c^3d^8 + 5702400ab^{14}c^7d^2 \\
& + 6031872ab^{15}c^3d^5 + 601920ab^{18}c^3d^2 + 18480a^2c^{18}d^4 \\
& + 95040a^2bc^{14}d^7 + 342144a^2b^2c^{10}d^{10} + 31680a^2b^3c^6d^{13} \\
& + 601920a^2b^3c^{18}d + 6177600a^2b^4c^{14}d^4 + 28702080a^2b^5c^{10}d^7 \\
& + 2566080a^2b^6c^6d^{10} + 95040a^2b^7c^2d^{13} + 5702400a^2b^7c^{14}d \\
& + 142987680a^2b^8c^{10}d^4 + 29367360a^2b^9c^6d^7 + 1672704a^2b^{10}c^2d^{10} \\
& + 28245888a^2b^{11}c^{10}d + 37224000a^2b^{12}c^6d^4 + 5702400a^2b^{13}c^2d^7 \\
& + 2661120a^2b^{15}c^6d + 2827440a^2b^{16}c^2d^4 + 95040a^2b^{19}c^2d \\
& + 3520a^3c^9d^{12} + 24288a^3c^{21} + 443520a^3bc^{17}d^3 \\
& + 1425600a^3b^2c^{13}d^6 + 3125760a^3b^3c^9d^9 + 142560a^3b^4c^5d^{12} \\
& + 902880a^3b^4c^{17} + 22809600a^3b^5c^{13}d^3 + 112464000a^3b^6c^9d^6 \\
& + 7223040a^3b^7c^5d^9 + 102960a^3b^8cd^{12} + 3326400a^3b^8c^{13} \\
& + 212115200a^3b^9c^9d^3 + 41342400a^3b^{10}c^5d^6 + 1013760a^3b^{11}cd^9 \\
& + 7846080a^3b^{12}c^9 + 22809600a^3b^{13}c^5d^3 + 1900800a^3b^{14}cd^6 \\
& + 332640a^3b^{16}c^5 + 443520a^3b^{17}cd^3 + 3168a^3b^{20}c + 66a^4d^{20} \\
& + 23760a^4c^{12}d^8 + 47520a^4bc^8d^{11} + 2827440a^4b^2c^{16}d^2
\end{aligned}$$

$$+ 9408960a^4b^3c^{12}d^5 + 17083440a^4b^4c^8d^8 + 475200a^4b^5c^4d^{11}$$
$$+ 37224000a^4b^6c^{12}d^2 + 216311040a^4b^7c^8d^5 + 10216800a^4b^8c^4d^8$$
$$+ 34320a^4b^9d^{11} + 142987680a^4b^{10}c^8d^2 + 28036800a^4b^{11}c^4d^5$$
$$+ 190080a^4b^{12}d^8 + 6177600a^4b^{14}c^4d^2 + 190080a^4b^{15}d^5$$
$$+ 18480a^4b^{18}d^2 + 190080a^5c^{15}d^4 + 380160a^5bc^{11}d^7$$
$$+ 494208a^5b^2c^7d^{10} + 6031872a^5b^3c^{15}d + 28036800a^5b^4c^{11}d^4$$
$$+ 41817600a^5b^5c^7d^7 + 696960a^5b^6c^3d^{10} + 25470720a^5b^7c^{11}d$$
$$+ 216311040a^5b^8c^7d^4 + 7223040a^5b^9c^3d^7 + 41665536a^5b^{11}c^7d$$
$$+ 9408960a^5b^{12}c^3d^4 + 633600a^5b^{15}c^3d + 198352a^6c^{18}$$
$$+ 1900800a^6bc^{14}d^3 + 2566080a^6b^2c^{10}d^6 + 1858560a^6b^3c^6d^9$$
$$+ 3769920a^6b^4c^{14} + 41342400a^6b^5c^{10}d^3 + 59000832a^6b^6c^6d^6$$
$$+ 475200a^6b^7c^2d^9 + 5844960a^6b^8c^{10} + 112464000a^6b^9c^6d^3$$
$$+ 2566080a^6b^{10}c^2d^6 + 4040256a^6b^{12}c^6 + 1425600a^6b^{13}c^2d^3$$
$$+ 23760a^6b^{16}c^2 + 15840a^7c^9d^8 + 5702400a^7b^2c^{13}d^2$$
$$+ 7223040a^7b^3c^9d^5 + 3611520a^7b^4c^5d^8 + 29367360a^7b^6c^9d^2$$
$$+ 41817600a^7b^7c^5d^5 + 166320a^7b^8cd^8 + 28702080a^7b^{10}c^5d^2$$
$$+ 380160a^7b^{11}cd^5 + 95040a^7b^{14}cd^2 + 495a^8d^{16} + 190080a^8c^{12}d^4$$
$$+ 166320a^8bc^8d^7 + 6177600a^8b^3c^{12}d + 10216800a^8b^4c^8d^4$$
$$+ 3611520a^8b^5c^4d^7 + 9504000a^8b^7c^8d + 17083440a^8b^8c^4d^4$$
$$+ 15840a^8b^9d^7 + 3326400a^8b^{11}c^4d + 23760a^8b^{12}d^4$$
$$+ 242880a^9c^{15} + 1013760a^9bc^{11}d^3 + 475200a^9b^2c^7d^6$$
$$+ 2059200a^9b^4c^{11} + 7223040a^9b^5c^7d^3 + 1858560a^9b^6c^3d^6$$
$$+ 1045440a^9b^8c^7 + 3125760a^9b^9c^3d^3 + 116160a^9b^{12}c^3$$
$$+ 1672704a^{10}b^2c^{10}d^2 + 696960a^{10}b^3c^6d^5 + 2566080a^{10}b^6c^6d^2$$
$$+ 494208a^{10}b^7c^2d^5 + 342144a^{10}b^{10}c^2d^2 + 34320a^{11}c^9d^4$$
$$+ 1013760a^{11}b^3c^9d + 475200a^{11}b^4c^5d^4 + 380160a^{11}b^7c^5d$$
$$+ 47520a^{11}b^8cd^4 + 2972a^{12}d^{12} + 61824a^{12}c^{12} + 102960a^{12}bc^8d^3$$
$$+ 190080a^{12}b^4c^8 + 142560a^{12}b^5c^4d^3 + 23760a^{12}b^8c^4$$
$$+ 3520a^{12}b^9d^3 + 1104a^{12}b^{12} + 95040a^{13}b^2c^7d^2 + 31680a^{13}b^6c^3d^2$$
$$+ 31680a^{14}b^3c^6d + 4048a^{15}c^9 + 3168a^{15}b^4c^5 + 495a^{16}d^8$$
$$+ 66a^{20}d^4 + a^{24}.$$

3.1.3. MacKay Codes. Let q be a prime power congruent to $-5 \pmod{12}$. Define a matrix B_q bordering Jacobsthal as

$$B_q = \begin{pmatrix} 2 & 1 \cdots 1 \\ 1 & \\ \vdots & W - 2I \\ 1 & \end{pmatrix}.$$

A double circulant code M_q is then introduced by its generator matrix

$$(I \ , \ B_q).$$

Theorem 3.2 *The MacKay code M_q is a self-dual Type* II *code of length $2q+2$.*

Proof. Follows from the property of W which is skew-symmetric for $q \equiv -1 \pmod 4$. Observe that the inner-product of each row with itself is this time $q+5$. □

Remark. M_q is the Chinese product of the binary doubly-even self-dual code with generator matrix $(I \ , \ J-I)$ and the ternary self-dual code with generator matrix $(I \ , \ B_q)$.

In particular $q = 19$ yields after the real construction A_6 an extremal lattice in dimension 40 [6]. For the first case $q = 7$, we have found its symmetrized weight enumerator:

$$\begin{aligned} swe_{M_7} = \ & d^{16} + 480bc^8d^7 + 1792b^3c^{12}d + 24864b^4c^8d^4 + 5376b^5c^4d^7 \\ & + 224b^6d^{10} + 25344b^7c^8d + 25536b^8c^4d^4 + 2720b^9d^7 + 5376b^{11}c^4d \\ & + 3360b^{12}d^4 + 256b^{15}d + 256ac^{15} + 2688abc^{11}d^3 + 10752ab^2c^7d^6 \\ & + 896ab^3c^3d^9 + 5376ab^4c^{11} + 166656ab^5c^7d^3 + 24192ab^6c^3d^6 \\ & + 25344ab^8c^7 + 45696ab^9c^3d^3 + 1792ab^{12}c^3 + 20160a^2b^2c^{10}d^2 \\ & + 72576a^2b^3c^6d^5 + 2016a^2b^4c^2d^8 + 282240a^2b^6c^6d^2 \\ & + 32256a^2b^7c^2d^5 + 20160a^2b^{10}c^2d^2 + 1568a^3c^9d^4 + 2688a^3bc^5d^7 \\ & + 45696a^3b^3c^9d + 185472a^3b^4c^5d^4 + 2688a^3b^5cd^7 + 166656a^3b^7c^5d \\ & + 12768a^3b^8cd^4 + 2688a^3b^{11}cd + 28a^4d^{12} + 3360a^4c^{12} \\ & + 12768a^4bc^8d^3 + 11424a^4b^2c^4d^6 + 25536a^4b^4c^8 + 185472a^4b^5c^4d^3 \end{aligned}$$

$$+ 672a^4b^6d^6 + 24864a^4b^8c^4 + 1568a^4b^9d^3 + 32256a^5b^2c^7d^2$$
$$+ 16128a^5b^3c^3d^5 + 72576a^5b^6c^3d^2 + 672a^6c^6d^4 + 24192a^6b^3c^6d$$
$$+ 11424a^6b^4c^2d^4 + 10752a^6b^7c^2d + 2720a^7c^9 + 2688a^7bc^5d^3$$
$$+ 5376a^7b^4c^5 + 2688a^7b^5cd^3 + 480a^7b^8c + 198a^8d^8$$
$$+ 2016a^8b^2c^4d^2 + 896a^9b^3c^3d + 224a^{10}c^6 + 28a^{12}d^4 + a^{16}.$$

3.1.4. A Family of Type II Codes. It is well known that there is a unique binary doubly-even self-dual code B and there is a unique ternary self-dual code T of length 8, up to equivalence. B and T have the following generator matrices:

$$G_B = \begin{pmatrix} 1000 & 0111 \\ 0100 & 1011 \\ 0010 & 1101 \\ 0001 & 1110 \end{pmatrix} \text{ and } G_T = \begin{pmatrix} 1000 & 1200 \\ 0100 & 1100 \\ 0010 & 0012 \\ 0001 & 0011 \end{pmatrix},$$

respectively. A generator matrix of the Chinese product $\mathrm{CRT}(B,T)$ of B and T is

$$\begin{pmatrix} 1000 & 4533 \\ 0100 & 1433 \\ 0010 & 3345 \\ 0001 & 3314 \end{pmatrix}.$$

The symmetrized weight enumerator of the senary code $\mathrm{CRT}(B,T)$ is

$$swe_{\mathrm{CRT}(B,T)} = d^8 + 192b^2c^4d^2 + 16b^3d^5 + 64b^6d^2 + 16ac^3d^4$$
$$+ 512ab^3c^3d + 64a^2c^6 + 96a^2bc^2d^3 + 192a^2b^4c^2$$
$$+ 96a^3b^2cd^2 + 14a^4d^4 + 16a^4b^3d + 16a^5c^3 + a^8.$$

$\bigoplus_n \mathrm{CRT}(B,T)$ is a Type II code of length $8n$ whose symmetrized weight enumerator is $swe_{\mathrm{CRT}(B,T)}{}^n$.

3.2. Properties of Senary Self-Dual Codes

Any code over $\mathbb{Z}_6$ is permutation-equivalent to a code generated by the following matrix:

$$\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} \\ 0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} \\ 0 & 0 & 3I_{k_3} & 3A_{3,4} \end{pmatrix}, \tag{2}$$

where $A_{i,j}$ are binary matrices for $i > 1$. Such a code is said to have rank $\{1^{k_1}, 2^{k_2}, 3^{k_3}\}$, see [1].

Lemma 3.3 *Let C be a senary code of rank $\{1^{k_1}, 2^{k_2}, 3^{k_3}\}$. If C is a self-dual code of length n then $k_2 = k_3$ and $k_1 + k_2 = n/2$.*

Proof. A senary self-dual code of length n has $6^{\frac{n}{2}}$ codewords. A code of rank $\{k_1, k_2, k_3\}$ has $6^{k_1} 3^{k_2} 2^{k_3}$ codewords. Hence, if the code is self-dual then k_2 must be equal to k_3 otherwise the number of codewords would not be a multiple of 6. Moreover $k_1 + k_2 = \frac{n}{2}$, since $6^{k_1} 3^{k_2} 2^{k_2} = 6^{k_1}(3 \cdot 2)^{k_2}$. □

If C is a code over $\mathbb{Z}_6$, let C_2 be the code read (mod 2) and let C_3 be the code read (mod 3). That is,

$$C_2 = \{v \mid v \equiv w \pmod 2, \quad w \in C\},$$

and

$$C_3 = \{v \mid v \equiv w \pmod 3, \quad w \in C\}.$$

The code C_2 is permutation-equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} \\ 0 & 0 & 3I_{k_3} & 3A_{3,4} \end{pmatrix}, \tag{3}$$

where $A_{i,j}$ are binary matrices for $i > 1$. Notice $3 \equiv 1 \pmod 2$ hence this code generates a binary code of dimension $k_1 + k_3 = \frac{n}{2}$. And the ternary code C_3 is permutation-equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} \\ 0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} \end{pmatrix}, \tag{4}$$

where $A_{i,j}$ are binary matrices for $i > 1$. Notice 2 is a unit in $\mathbb{Z}_3$ hence this code generates a ternary code of dimension $k_1 + k_2 = \frac{n}{2}$.

We now consider self-dual codes of length n over $\mathbb{Z}_6$ constructed from a fixed binary self-dual code C_2 and a fixed ternary self-dual code C_3 by the Chinese product. Let T be the set of all codes constructed by permuting the coordinates of C_2 and C_3. Let C_3' be a ternary code obtained from C_3 by changing the signs of certain coordinates, then it is clear that $\mathrm{CRT}(C_2, C_3)$ is equivalent to $\mathrm{CRT}(C_2, C_3')$. Moreover $\mathrm{CRT}({C_2}^{\alpha}, {C_3}^{\beta})$ is equivalent to $\mathrm{CRT}({C_2}^{\alpha(\beta)^{-1}}, C_3)$ where α and β are element of the symmetric group S_n of degree n. Of course, S_n acts on the coordinates of C_2 and C_3. Hence

$$\begin{aligned} T &= \{\mathrm{CRT}({C_2}^{\alpha}, {C_3}^{\beta}) \mid \alpha, \beta \in S_n\} \\ &= \{\mathrm{CRT}({C_2}^{\gamma}, C_3) \mid \gamma \in S_n\}. \end{aligned}$$

In addition, if γ is an element of the automorphism group $\mathrm{Aut}(C_2)$ of C_2 then $\mathrm{CRT}(C_2, C_3) = \mathrm{CRT}({C_2}^{\gamma}, C_3)$. Therefore the number N of inequivalent codes obtained from C_2 and C_3 by permuting the coordinates and changing the signs is at most

$$\frac{n!}{|\mathrm{Aut}(C_2)|},$$

where $|\mathrm{Aut}(C_2)|$ denotes the order of $\mathrm{Aut}(C_2)$.

Let $\overline{\mathrm{Aut}(C_3)}$ be the group of all permutations which preserve C_3, similarly, we have

$$N \leq \frac{n!}{|\overline{\mathrm{Aut}(C_3)}|}.$$

Thus we have

$$N \leq \min\left\{\frac{n!}{|\mathrm{Aut}(C_2)|}, \frac{n!}{|\overline{\mathrm{Aut}(C_3)}|}\right\}.$$

This gives the following upper bound on the number of inequivalent senary self-dual codes.

Proposition 3.4 *Let $\mathcal{C}_2$ and $\mathcal{C}_3$ be the sets of all inequivalent self-dual codes of length n over $\mathbb{Z}_2$ and $\mathbb{Z}_3$, respectively. Let $N_6(n)$ be the number of inequivalent self-dual codes of length n over $\mathbb{Z}_6$. Then $N_6(n)$ is bounded by*

$$N_6(n) \leq \min\left\{|\mathcal{C}_3|\left(\sum_{C_2 \in \mathcal{C}_2} \frac{n!}{|\mathrm{Aut}(C_2)|}\right), |\mathcal{C}_2|\left(\sum_{C_3 \in \mathcal{C}_3} \frac{n!}{|\overline{\mathrm{Aut}(C_3)}|}\right)\right\}. \quad (5)$$

We give a classification of self-dual codes over $\mathbb{Z}_6$ of length 4. By

Lemma 3.3, the rank of a self-dual code of length 4 is either $\{1^2\}$ or $\{1^1, 2^1, 3^1\}$. When rank is $\{1^2\}$, any code is equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 4 & 1 \end{pmatrix}.$$

When rank is $\{1^1, 2^1, 3^1\}$, it is easy to see that a generator matrix of a self-dual code can be transformed into a matrix of the form:

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 3 \end{pmatrix},$$

where $a, b, c \in \mathbb{Z}_6$. We found all self-dual codes by finding all possible (a, b, c). Then any code of rank $\{1^1, 2^1, 3^1\}$ is equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} 1 & 1 & 0 & 4 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 3 & 3 \end{pmatrix}.$$

Therefore there are exactly two inequivalent self-dual codes of length 4. Since $N_6(4) \leq 3$, the above bound (5) is always not tight in general.

All binary self-dual codes of length up to 30 and all ternary self-dual codes of length up to 20 have been classified (cf. [4] and [22]). It would be interesting to determine equivalence classes of senary self-dual codes of length up to 20 from these codes.

4. Corresponding Lattices

An n-dimensional lattice Λ in $\mathbb{R}^n$ is the set of integer linear combinations of n linearly independent vectors $v_1, \ldots, v_n$, where $\mathbb{R}^n$ is the n-dimensional Euclidean space. The *dual* lattice Λ^* is given by $\Lambda^* = \{x \in \mathbb{R}^n \mid [x, a] \in \mathbb{Z} \text{ for all } a \in \Lambda\}$, where $[x, a] = x_1 a_1 + \cdots + x_n a_n$ and $x = (x_1, \ldots, x_n)$, $a = (a_1, \ldots, a_n)$. A lattice Λ is *integral* if the inner product of any two lattice points is integral, or equivalently, if $\Lambda \subseteq \Lambda^*$. An integral lattice with $\Lambda = \Lambda^*$ is called *unimodular*. The theta series $\theta_\Lambda(q)$ of a lattice Λ is the formal power series

$$\theta_\Lambda(q) = \sum_{x\in\Lambda} q^{[x,x]}.$$

The kissing number is the first non-trivial coefficient of the theta series.

4.1. Construction A_6

Every senary code C can be attached a lattice by the formula

$$A_6(C) = \frac{1}{\sqrt{6}}(C + 6\mathbb{Z}^n).$$

Using that construction the Leech lattice was constructed anew in [1]. If C is self-dual then $A_6(C)$ is unimodular, moreover if C is Type II then $A_6(C)$ is even unimodular (cf. [1]). We observe that construction B_3 of Leech and Sloane [6, p. 148] is in fact construction A_6 applied to the code $S = -2C + 3P_n$, where C is a ternary code and P_n is the binary parity-check code of length n. In other words, S is the Chinese product of C by P_n.

Let ν_i denote the theta series of $\mathbb{Z} + \frac{i}{6}$ for $i = 1, 2, 3$. Clearly

$$\theta_{A_6(C)} = swe_C(\theta_3, \nu_1, \nu_2, \nu_3).$$

With the denotations of [6, p. 105] we have $\nu_1 = \psi_6$, $\nu_2 = \psi_3$, $\nu_3 = \theta_2$.

4.2. Even Unimodular Lattices

In Section 3, we gave a family of Type II codes $\bigoplus_n \mathrm{CRT}(B,T)$ of length $8n$. Since there is a unique 8-dimensional even unimodular lattice, up to equivalence, namely E_8, $A_6(\mathrm{CRT}(B,T))$ must be E_8. In addition, it is easy to see that $A_6(\bigoplus_n \mathrm{CRT}(B,T))$ is $E_8 + \cdots + E_8$.

The minimum norm of the lattice $A_6(P(12))$ is 1, the kissing number is 24 and the lattice is a unimodular lattice. Thus $A_6(P(12))$ is $\mathbb{Z}^{12}$. Since the code M_7 of length 16 is Type II and $d_E = 12$, $A_6(M_7)$ is a 16-dimensional even extremal unimodular lattice, that is, either $E_8 + E_8$ or D_{16}^+ by Table 16.7 of [6].

The lattice $A_6(P(24))$ is a 24-dimensional even unimodular lattice. Moreover, from $swe_{P(24)}$ of $P(24)$ in Section 3, the theta series $\theta_{A_6(P(24))}$ of the lattice $A_6(P(24))$ is $1 + 1104q^2 + \cdots$. Thus the lattice is D_{24}^+ by Table 16.1 in [6].

4.3. Odd Unimodular Lattices

From [5, Table II], there is a unique odd unimodular lattice with the minimum norm 2 in dimensions 12 and 16. By the Chinese product, we have Type I codes C_{12} and C_{16} of lengths 12 and 16 with the following generator matrices

$$\begin{pmatrix} 100000 & 231155 \\ 010000 & 141113 \\ 001000 & 112355 \\ 000100 & 151235 \\ 000010 & 513545 \\ 000001 & 355112 \end{pmatrix} \text{ and } \begin{pmatrix} 10000000 & 44411111 \\ 01000000 & 42521511 \\ 00100000 & 42512115 \\ 00010000 & 42151455 \\ 00001000 & 44511525 \\ 00000100 & 42115554 \\ 00000010 & 14422242 \\ 00000001 & 41222424 \end{pmatrix},$$

respectively. Their symmetrized weight enumerators swe_{12} and swe_{16} are

$$\begin{aligned} swe_{C_{12}} &= d^{12} + 24c^{12} + 120bc^8d^3 + 120b^2c^4d^6 + 1280b^3c^6d^3 + 360b^4c^8 \\ &+ 1680b^5c^4d^3 + 264b^6d^6 + 768b^6c^6 + 360b^8c^4 + 440b^9d^3 + 24b^{12} \\ &+ 384abc^5d^5 + 1440ab^2c^7d^2 + 960ab^3c^3d^5 + 5760ab^4c^5d^2 \\ &+ 3360ab^6c^3d^2 + 120a^2c^6d^4 + 1920a^2b^2c^4d^4 + 3360a^2b^3c^6d \\ &+ 1800a^2b^4c^2d^4 + 5760a^2b^5c^4d + 1440a^2b^7c^2d + 440a^3c^9 \\ &+ 960a^3bc^5d^3 + 3840a^3b^3c^3d^3 + 1680a^3b^4c^5 + 960a^3b^5cd^3 \\ &+ 1280a^3b^6c^3 + 120a^3b^8c + 15a^4d^8 + 1800a^4b^2c^4d^2 \\ &+ 1920a^4b^4c^2d^2 + 120a^4b^6d^2 + 960a^5b^3c^3d + 384a^5b^5cd \\ &+ 32a^6d^6 + 264a^6c^6 + 120a^6b^4c^2 + 15a^8d^4 + a^{12}, \end{aligned}$$

$$\begin{aligned} swe_{C_{16}} &= d^{16} + 40c^{12}d^4 + 144bc^8d^7 + 64bc^{14}d + 40b^2c^4d^{10} + 1712b^2c^{10}d^4 \\ &+ 1760b^3c^6d^7 + 1024b^3c^{12}d + 56b^4c^2d^{10} + 12304b^4c^8d^4 \\ &+ 2992b^5c^4d^7 + 5952b^5c^{10}d + 224b^6d^{10} + 24032b^6c^6d^4 \\ &+ 1632b^7c^2d^7 + 12032b^7c^8d + 14632b^8c^4d^4 + 2720b^9d^7 \\ &+ 9920b^9c^6d + 3696b^{10}c^2d^4 + 3072b^{11}c^4d + 3360b^{12}d^4 \\ &+ 448b^{13}c^2d + 256b^{15}d + 136ac^9d^6 + 256ac^{15} + 112abc^5d^9 \\ &+ 1376abc^{11}d^3 + 5024ab^2c^7d^6 + 448ab^2c^{13} + 352ab^3c^3d^9 \end{aligned}$$

$$
\begin{aligned}
&+ 22912ab^3c^9d^3 + 18640ab^4c^5d^6 + 3072ab^4c^{11} + 224ab^5cd^9 \\
&+ 77120ab^5c^7d^3 + 14144ab^6c^3d^6 + 9920ab^6c^9 + 82432ab^7c^5d^3 \\
&+ 2856ab^8cd^6 + 12032ab^8c^7 + 25952ab^9c^3d^3 + 5952ab^{10}c^5 \\
&+ 2688ab^{11}cd^3 + 1024ab^{12}c^3 + 64ab^{14}c + 2a^2d^{14} + 104a^2c^6d^8 \\
&+ 336a^2c^{12}d^2 + 4056a^2bc^8d^5 + 1152a^2b^2c^4d^8 + 11760a^2b^2c^{10}d^2 \\
&+ 35200a^2b^3c^6d^5 + 1392a^2b^4c^2d^8 + 77232a^2b^4c^8d^2 + 55536a^2b^5c^4d^5 \\
&+ 168a^2b^6d^8 + 136992a^2b^6c^6d^2 + 17952a^2b^7c^2d^5 + 77232a^2b^8c^4d^2 \\
&+ 952a^2b^9d^5 + 11760a^2b^{10}c^2d^2 + 336a^2b^{12}d^2 + 816a^3c^9d^4 \\
&+ 1152a^3bc^5d^7 + 2688a^3bc^{11}d + 26336a^3b^2c^7d^4 + 4192a^3b^3c^3d^7 \\
&+ 25952a^3b^3c^9d + 87472a^3b^4c^5d^4 + 1376a^3b^5cd^7 + 82432a^3b^5c^7d \\
&+ 62176a^3b^6c^3d^4 + 77120a^3b^7c^5d + 7616a^3b^8cd^4 + 22912a^3b^9c^3d \\
&+ 1376a^3b^{11}cd + 16a^4d^{12} + 360a^4c^6d^6 + 3360a^4c^{12} + 7616a^4bc^8d^3 \\
&+ 4984a^4b^2c^4d^6 + 3696a^4b^2c^{10} + 62176a^4b^3c^6d^3 + 5432a^4b^4c^2d^6 \\
&+ 14632a^4b^4c^8 + 87472a^4b^5c^4d^3 + 424a^4b^6d^6 + 24032a^4b^6c^6 \\
&+ 26336a^4b^7c^2d^3 + 12304a^4b^8c^4 + 816a^4b^9d^3 + 1712a^4b^{10}c^2 \\
&+ 40a^4b^{12} + 952a^5c^9d^2 + 2640a^5bc^5d^5 + 17952a^5b^2c^7d^2 \\
&+ 8576a^5b^3c^3d^5 + 55536a^5b^4c^5d^2 + 2640a^5b^5cd^5 + 35200a^5b^6c^3d^2 \\
&+ 4056a^5b^8cd^2 + 62a^6d^{10} + 424a^6c^6d^4 + 2856a^6bc^8d \\
&+ 5432a^6b^2c^4d^4 + 14144a^6b^3c^6d + 4984a^6b^4c^2d^4 + 18640a^6b^5c^4d \\
&+ 360a^6b^6d^4 + 5024a^6b^7c^2d + 136a^6b^9d + 2720a^7c^9 + 1376a^7bc^5d^3 \\
&+ 1632a^7b^2c^7 + 4192a^7b^3c^3d^3 + 2992a^7b^4c^5 + 1152a^7b^5cd^3 \\
&+ 1760a^7b^6c^3 + 144a^7b^8c + 94a^8d^8 + 168a^8c^6d^2 + 1392a^8b^2c^4d^2 \\
&+ 1152a^8b^4c^2d^2 + 104a^8b^6d^2 + 224a^9bc^5d + 352a^9b^3c^3d \\
&+ 112a^9b^5cd + 62a^{10}d^6 + 224a^{10}c^6 + 56a^{10}b^2c^4 + 40a^{10}b^4c^2 \\
&+ 16a^{12}d^4 + 2a^{14}d^2 + a^{16}.
\end{aligned}
$$

Thus the minimum Euclidean weights of both C_{12} and C_{16} are 12. $A_6(C_{12})$ and $A_6(C_{16})$ are the odd unimodular lattices with the minimum norm 2.

4.4. A 3-modular Lattice

Recently Gabriele Nebe [18] has found an extremal 3-modular lattice in dimension 24 from a code N over $\mathbb{Z}_6$. N has the following generator matrix:

$$\begin{pmatrix} 021504155450211000001131 \\ 011045013540150005055212 \\ 402051511014011450502145 \\ 121041050541020015551212 \\ 520540110455511555555300 \\ 511150105450203514055511 \\ 333300000000000000000000 \\ 000033330000000000000000 \\ 000000003333000000000000 \\ 000000000000333300000000 \\ 000000000000000033330000 \\ 000000000000000000003333 \end{pmatrix}.$$

We have obtained its symmetrized weight enumerator:

$$\begin{aligned} swe_N = {} & d^{24} + 626b^5c^{16}d^3 + 5668b^6c^{12}d^6 + 3060b^7c^8d^9 + 2b^8c^4d^{12} + 6b^9d^{15} \\ & + 5982b^9c^{12}d^3 + 12826b^{10}c^8d^6 + 130b^{11}c^4d^9 + 26b^{12}d^{12} \\ & + 5626b^{13}c^8d^3 + 280b^{14}c^4d^6 + 178b^{15}d^9 + 42b^{17}c^4d^3 + 154b^{18}d^6 \\ & + 12b^{21}d^3 + 6ab^2c^{19}d^2 + 1428ab^3c^{15}d^5 + 4594ab^4c^{11}d^8 \\ & + 670ab^5c^7d^{11} + 3926ab^6c^{15}d^2 + 49150ab^7c^{11}d^5 + 21474ab^8c^7d^8 \\ & + 38ab^9c^3d^{11} + 23002ab^{10}c^{11}d^2 + 67556ab^{11}c^7d^5 + 428ab^{12}c^3d^8 \\ & + 10930ab^{14}c^7d^2 + 410ab^{15}c^3d^5 + 24ab^{18}c^3d^2 + 190a^2bc^{14}d^7 \\ & + 472a^2b^2c^{10}d^{10} + 286a^2b^3c^6d^{13} + 24a^2b^3c^{18}d + 12546a^2b^4c^{14}d^4 \\ & + 29094a^2b^5c^{10}d^7 + 5518a^2b^6c^6d^{10} + 18a^2b^7c^2d^{13} + 8114a^2b^7c^{14}d \\ & + 170184a^2b^8c^{10}d^4 + 73758a^2b^9c^6d^7 + 74a^2b^{10}c^2d^{10} \\ & + 22362a^2b^{11}c^{10}d + 93322a^2b^{12}c^6d^4 + 382a^2b^{13}c^2d^7 + 4310a^2b^{15}c^6d \\ & + 188a^2b^{16}c^2d^4 + 6a^2b^{19}c^2d + 134a^3c^9d^{12} + 780a^3c^{21} + 46a^3bc^{17}d^3 \\ & + 2630a^3b^2c^{13}d^6 + 2748a^3b^3c^9d^9 + 698a^3b^4c^5d^{12} + 42a^3b^4c^{17} \\ & + 54280a^3b^5c^{13}d^3 + 124326a^3b^6c^9d^6 + 14926a^3b^7c^5d^9 + 18a^3b^8cd^{12} \\ & + 5754a^3b^8c^{13} + 252276a^3b^9c^9d^3 + 100798a^3b^{10}c^5d^6 + 42a^3b^{11}cd^9 \\ & + 5854a^3b^{12}c^9 + 59400a^3b^{13}c^5d^3 + 102a^3b^{14}cd^6 + 882a^3b^{16}c^5 \\ & + 46a^3b^{17}cd^3 + 6a^4d^{20} + 4a^4c^{12}d^8 + 56a^4bc^8d^{11} + 188a^4b^2c^{16}d^2 \\ & + 21404a^4b^3c^{12}d^5 + 17494a^4b^4c^8d^8 + 2430a^4b^5c^4d^{11} \\ & + 78730a^4b^6c^{12}d^2 + 241014a^4b^7c^8d^5 + 21738a^4b^8c^4d^8 \end{aligned}$$

$$
\begin{aligned}
&+ 172104a^4b^{10}c^8d^2 + 70556a^4b^{11}c^4d^5 + 15490a^4b^{14}c^4d^2\\
&+ 26a^4b^{15}d^5 + 26a^5c^{15}d^4 + 1190a^5bc^{11}d^7 + 842a^5b^2c^7d^{10}\\
&+ 410a^5b^3c^{15}d + 57884a^5b^4c^{11}d^4 + 39924a^5b^5c^7d^7 + 2390a^5b^6c^3d^{10}\\
&+ 58340a^5b^7c^{11}d + 247798a^5b^8c^7d^4 + 16494a^5b^9c^3d^7\\
&+ 46846a^5b^{11}c^7d + 23836a^5b^{12}c^3d^4 + 1940a^5b^{15}c^3d + 8730a^6c^{18}\\
&+ 102a^6bc^{14}d^3 + 4650a^6b^2c^{10}d^6 + 3340a^6b^3c^6d^9 + 280a^6b^4c^{14}\\
&+ 90174a^6b^5c^{10}d^3 + 51084a^6b^6c^6d^6 + 1956a^6b^7c^2d^9 + 12570a^6b^8c^{10}\\
&+ 127142a^6b^9c^6d^3 + 5034a^6b^{10}c^2d^6 + 4260a^6b^{12}c^6 + 2630a^6b^{13}c^2d^3\\
&+ 20a^7c^9d^8 + 382a^7b^2c^{13}d^2 + 11886a^7b^3c^9d^5 + 5640a^7b^4c^5d^8\\
&+ 62494a^7b^6c^9d^2 + 42356a^7b^7c^5d^5 + 598a^7b^8cd^8 + 31910a^7b^{10}c^5d^2\\
&+ 1062a^7b^{11}cd^5 + 318a^7b^{14}cd^2 + 751a^8d^{16} + 598a^8bc^8d^7\\
&+ 428a^8b^3c^{12}d + 17002a^8b^4c^8d^4 + 5128a^8b^5c^4d^7 + 19042a^8b^7c^8d\\
&+ 16726a^8b^8c^4d^4 + 20a^8b^9d^7 + 4722a^8b^{11}c^4d + 4a^8b^{12}d^4\\
&+ 10290a^9c^{15} + 42a^9bc^{11}d^3 + 1316a^9b^2c^7d^6 + 130a^9b^4c^{11}\\
&+ 13262a^9b^5c^7d^3 + 3084a^9b^6c^3d^6 + 2804a^9b^8c^7 + 2108a^9b^9c^3d^3\\
&+ 74a^{10}b^2c^{10}d^2 + 1622a^{10}b^3c^6d^5 + 4366a^{10}b^6c^6d^2 + 458a^{10}b^7c^2d^5\\
&+ 216a^{10}b^{10}c^2d^2 + 38a^{11}b^3c^9d + 1406a^{11}b^4c^5d^4 + 670a^{11}b^7c^5d\\
&+ 56a^{11}b^8cd^4 + 2452a^{12}d^{12} + 2970a^{12}c^{12} + 18a^{12}bc^8d^3 + 2a^{12}b^4c^8\\
&+ 442a^{12}b^5c^4d^3 + 6a^{12}b^9d^3 + 18a^{13}b^2c^7d^2 + 30a^{13}b^6c^3d^2\\
&+ 134a^{15}c^9 + 879a^{16}d^8z + 6a^{20}d^4 + a^{24}.
\end{aligned}
$$

5. Self-Dual Codes over Rings formed from Projective Planes

Let Π be a projective plane of order $n = \prod_{i=1}^{r} p_i$ where the p_i are distinct primes with either:
Case 1: Each $p_i = 2$ or $p_i \equiv 1 \pmod 4$ or
Case 2: Each $p_i \equiv 3 \pmod 4$.

Let C_{p_i} be the self-code over $\mathbb{F}_{p_i}$ of length $n^2 + n + 2$ or $n^2 + n + 4$ depending on the case formed as given in [9].

Theorem 5.1 *Let Π be a projective plane of order $n = \prod p_i$ where the p_i are distinct primes with the above cases, then $\mathrm{CRT}(C_{p_1}, C_{p_2}, \ldots, C_{p_r})$ is a self-dual code over the ring $\mathbb{Z}_{p_1 p_2 \ldots p_r}$ of length $n^2 + n + 2$ or $n^2 + n + 4$ for Case 1 and Case 2 respectively.*

Proof. Since each C_{p_i} is a self-dual code over $\mathbb{F}_{p_i}$ of the same length then the Chinese product gives that the code $\mathrm{CRT}(C_{p_1}, C_{p_2}, \dots, C_{p_r})$ is self-dual. □

Note for Case 2, r must be odd. If $r = 2k$ then $n \equiv \prod p_i \equiv 3^{2k} \equiv 1 \pmod 4$. Hence $n^2 + n + 1 \equiv 3 \pmod 4$ and then $n^2 + n + 4 \equiv 2 \pmod 4$ giving that there are no self-dual codes over $\mathbb{F}_{p_i}$.

Corollary 5.2 *If $n = 2p$ where p is a prime and $p \equiv 1 \pmod 4$ then a Type* II *self-dual code of length $N = n^2+n+3\pm1$ can be constructed from a projective plane of order n over $\mathbb{Z}_{2p}$. The N-dimensional even unimodular lattice obtained by Construction A has minimum norm* 2.

Of course, there are no known non-trivial examples of either Case 1 or Case 2 since all known planes have orders a power of a prime. Had a projective plane of order 10 existed its attached lattice in dimension 112 = 8.14 would have had by [6, Chap. 17, Theorem 7]. A theta series of the shape:

$$\theta_{10}(q) = E_4^{14} + \sum_{i=1}^{4} a_i E_4^{14-3i} \Delta^i,$$

where letting $t = q^2$, we denote by

$$E_4 = 1 + 240\,t + 2160\,t^2 + 6720\,t^3 + 17520\,t^4 + 30240\,t^5 + \cdots,$$

the theta series of the E_8 lattice, and by Δ the cusp form of weight 12 for the full modular group

$$\Delta = t \prod_{r\geq 1} (1 - t^r)^{24},$$

or up to order 5

$$\Delta = t - 24\,t^2 + 252\,t^3 - 1472\,t^4 + 4830\,t^5.$$

6. Weighing Matrices and Type II Codes

In this section, we deal with weighing matrices corresponding to Type II codes.

A weighing matrix $W(m,k)$ of order m and weight k is an m by m (0,1,−1)-matrix such that $W \cdot W^T = kI_m$, $k \leq m$. A weighing matrix $W(m,m)$ is just a Hadamard matrix. Weighing matrices are a generalization of Hadamard matrices. We say that two weighing matrices W_1 and W_2 of order m and weight k are equivalent if there exist monomial matrices of 0's, 1's and -1's P and Q such that $W_1 = P \cdot W_2 \cdot Q$.

We give a method for constructing self-dual codes over $\mathbb{Z}_{2n}$.

Theorem 6.1 *Let x an element of $\mathbb{Z}_{2n}$ satisfying $1 + x^2k \equiv 0 \pmod{2n}$. Let $W_{m,k}$ be a weighing matrix of order m and weight k. Then the matrix $G = (I_m \ , \ xW_{m,k})$ generates a self-dual code C over $\mathbb{Z}_{2n}$ of length $2m$. Moreover if x satisfies $1 + x^2k \equiv 0 \pmod{4n}$ then C is Type II.*

Proof. $G \cdot G^T = (1 + x^2k)I_m$. Thus if $1 + x^2k \equiv 0 \pmod{2n}$ then C is self-dual. Moreover if $1 + x^2k \equiv 0 \pmod{4n}$ then C is Type II. □

Remark. For $n = 2$, this method was given in [12].

Since the matrix S_q in the generator matrix of the lifted senary symmetry codes is a weighing matrix of order $q + 1$ and weight q, this method is a generalization of Theorem 3.1.

Example 2. All weighing matrices have been classified for order 12 (cf. [19]). There are weighing matrices $W_{12,k}$ of order 12 for every weight $1 \le k \le 12$. For $n = 3$, the matrix $(I \ , \ W_{12,11})$ generates a Type II code of length 24 with the minimum Euclidean weight 12, that is, this code is not extremal. Since there is a unique weighing matrix of weight 11, this is the same code given previously.

Example 3. For $n = 4$, the matrix $(I \ , \ 3W_{12,7})$ generates a Type II code of length 24. There are exactly three inequivalent weighing matrices of weight 7. The three inequivalent matrices are denoted by A_1, A_3 and A_8 in [19]. Since the matrix A_1 has the intersection pattern $p_6 \ge 1$ (for the definition see [19]), the Type II code with generator matrix of the form $(I \ , \ 3A_1)$ contains a codeword of Euclidean weight 16, that is the code is not extremal. Moreover we have verified by computer that the codes constructed from the remaining two weighing matrices are not extremal.

It was shown in [1] that a Type II code of length n exists if and only if $n \equiv 0 \pmod 8$. Thus we have the following restriction on the existence of weighing matrices.

Corollary 6.2 *Suppose that there is a weighing matrix of order m and weight k. If there is an element x of $\mathbb{Z}_{2n}$ satisfying $1 + x^2k \equiv 0 \pmod{4n}$*

for certain n, then $m \equiv 0 \pmod 4$.

Remark. For $n = 1$, the above corollary was shown in [13].

As a corollary to Theorem 6.1, we have the following:

Corollary 6.3 *Let α and β be elements of $\mathbb{Z}_{2n}$ satisfying $1+\alpha^2+\beta^2 k \equiv 0 \pmod{2n}$. If either $W_{m,k}$ is a skew-symmetric weighing matrix (that is, $W_{m,k} = -W_{m,k}^T$) or $W_{m,k}$ is a symmetric weighing matrix with $\alpha\beta \equiv 0 \pmod n$, then the matrix $G = (I \ , \ (\alpha I + \beta W_{m,k}))$ generates a self-dual code C over $\mathbb{Z}_{2n}$ of length $2m$. Moreover if $1 + \alpha^2 + \beta^2 k \equiv 0 \pmod{4n}$ then C is Type* II.

Proof. We have $G \cdot G^T = (1 + \alpha^2 + k\beta^2)I + \alpha\beta W_{m,k} + \alpha\beta W_{m,k}^T$. It follows from the assumptions that $G \cdot G^T = 0$. □

Remark. We can regard MacKay codes over $\mathbb{Z}_6$ described in Section 3 as a special case of the above corollary.

A similar argument to Corollary 6.2 gives the following:

Corollary 6.4 *Suppose that there are two elements α and β of $\mathbb{Z}_{2n}$ satisfying $1 + \alpha^2 + \beta^2 k \equiv 0 \pmod{4n}$ for certain n where $\beta \neq 0$.*

(1) *If there is a skew-symmetric weighing matrix of order m and weight k, then $m \equiv 0 \pmod 4$.*

(2) *If there is a symmetric weighing matrix of order m and weight k and $\alpha\beta \equiv 0 \pmod n$, then $m \equiv 0 \pmod 4$.*

7. The Complete Combined Weight Enumerator

In this section all rings will assumed to be commutative, finite and Frobenius.

Let $C_1, C_2, \ldots, C_s$ be codes of length n, where C_i is a code over the ring R_i. Let $\mathcal{C} = C_1 \times C_2 \times \cdots \times C_s$ and $\mathcal{R} = R_1 \times R_2 \times \cdots \times R_s$.

Definition 1 The complete combined weight enumerator is given by:

$$P(C_1, C_2, \ldots, C_s)(X_a) = \sum_{(c_1,c_2,\ldots,c_s)\in\mathcal{C}} \prod_{a\in\mathcal{R}} X_a^{n_a(c_1,c_2,\ldots,c_s)},$$

where $n_a(c_1, c_2, \ldots, c_s) = |\{i | a = (c_1^i, c_s^i, \ldots, c_s^i)\}|$ and c_j^i is the i-th coordinate of c_j.

7.1. The MacWilliams Relations

We will prove the MacWilliams relations for this new weight enumerator by generalizing the technique in [1], which itself is a generalization of [23].

Let G_i be a group with $f : G_1 \times G_2 \times \cdots \times G_s \to A$ where A is a complex algebra. Denote by $\widehat{G_i}$ the character group of G_i, that is $\widehat{G_i} = \{\pi | \pi$ is a character of $G_i\}$ where a character of a group is a group homomorphism from G to the Complex numbers under multiplication.

Define $\widehat{f} : \widehat{G_1} \times \widehat{G_2} \times \cdots \times \widehat{G_s} \to A$ by

$$\widehat{f}(\pi_1, \pi_2, \ldots, \pi_s) = \sum_{x_1 \in G_1} \sum_{x_2 \in G_2} \cdots \sum_{x_s \in G_s} \pi_1(x_1)\pi_2(x_2) \cdots \pi_s(x_s) f(x_1, x_2, \ldots, x_s).$$

Lemma 7.1 *The function*

$$f(x_1, x_2, \ldots, x_s) = \frac{1}{|G_1||G_2| \cdots |G_s|} \sum_{\pi_1 \in \widehat{G_1}} \sum_{\pi_1 \in \widehat{G_2}} \cdots \sum_{\pi_1 \in \widehat{G_s}} \pi_1(-x_1)\pi_2(-x_2) \cdots \pi_s(-x_s) \widehat{f}(\pi_1, \pi_2, \ldots, \pi_s).$$

Proof. We have that

$$\begin{aligned}
&\frac{1}{|G_1||G_2| \cdots |G_s|} \sum_{\pi_1 \in \widehat{G_1}} \sum_{\pi_2 \in \widehat{G_2}} \cdots \sum_{\pi_s \in \widehat{G_s}} \pi_1(-x_1)\pi_2(-x_2) \cdots \pi_s(-x_s) \widehat{f}(\pi_1, \pi_2, \ldots, \pi_s) \\
&= \frac{1}{|G_1||G_2| \cdots |G_s|} \sum_{\pi_1 \in \widehat{G_1}} \cdots \sum_{\pi_s \in \widehat{G_s}} \pi_1(-x_1)\pi_2(-x_2) \ldots \pi_s(-x_s) \sum_{a_1 \in G_1} \cdots \sum_{a_s \in G_s} \pi_1(a_1) \cdots \pi_s(a_s) f(a_1, a_2, \ldots, a_s) \\
&= \frac{1}{|G_1||G_2| \cdots |G_s|} \sum_{\pi_1 \in \widehat{G_1}} \sum_{a_1 \in G_1} \pi_1(-x_1 + a_1) \cdots \sum_{\pi_s \in \widehat{G_1}} \sum_{a_s \in G_1} \pi_s(-x_s + a_s) f(a_1, a_2, \ldots, a_s) \\
&= \frac{1}{|G_1||G_2| \cdots |G_s|} |G_1||G_2| \cdots |G_s| f(x_1, x_2, \ldots, x_s)
\end{aligned}$$

$$= f(x_1, x_2, \ldots, x_s),$$

since

$$\sum_{\pi \in \widehat{G}} \pi(g) = \begin{cases} |G| & g = 0 \\ 0 & g \neq 0. \end{cases}$$

□

This is a generalization of the Fourier inversion formula. Next we generalize the Poisson summation formula.

Before stating the next lemma we shall define $(\widehat{G} : H) = \{\pi \in \widehat{G} \mid \pi|_H = 1\}$ and note that

$$\sum_{x \in H} \pi(x) = \begin{cases} |H| & \pi \in (\widehat{G} : H) \\ 0 & \pi \notin (\widehat{G} : H) \end{cases}$$

Lemma 7.2 *Let H_i be a subgroup of G_i. For every a_i in G_i we have*

$$\sum_{x_1 \in H_1} \sum_{x_2 \in H_2} \cdots \sum_{x_s \in H_s} f(a_1 + x_1, a_2 + x_2, \ldots, a_s + x_s)$$
$$= \frac{1}{|(\widehat{G_1} : H_1)|} \frac{1}{|(\widehat{G_2} : H_2)|} \cdots \frac{1}{|(\widehat{G_s} : H_s)|} \sum_{\pi_1 \in (\widehat{G_1}:H_1)} \sum_{\pi_2 \in (\widehat{G_2}:H_2)} \cdots$$
$$\sum_{\pi_s \in (\widehat{G_s}:H_s)} \widehat{f}(\pi_1, \pi_2, \ldots, \pi_s).$$

Proof. We have that

$$\sum_{x_1 \in H_1} \cdots \sum_{x_s \in H_s} f(a_1 + x_1, \ldots, a_s + x_s)$$
$$= \sum_{x_1 \in H_1} \cdots \sum_{x_s \in H_s} \frac{1}{|G_1| \cdots |G_s|} \sum_{\pi_1 \in \widehat{G_1}} \cdots$$
$$\sum_{\pi_s \in \widehat{G_s}} \pi_1(-x_1) \cdots \pi_s(-x_s) \widehat{f}(\pi_1, \ldots, \pi_s)$$
$$= \frac{1}{|G_1| \cdots |G_s|} \sum_{x_1 \in H_1} \cdots \sum_{x_s \in H_s} \sum_{\pi_1 \in \widehat{G_1}} \cdots$$
$$\sum_{\pi_s \in \widehat{G_s}} \pi_1(-x_1) \cdots \pi_s(-x_s) \widehat{f}(\pi_1, \ldots, \pi_s)$$

$$= \frac{1}{|G_1|\cdots|G_s|} \sum_{\pi_1 \in \widehat{G_1}} \cdots \sum_{\pi_s \in \widehat{G_s}} \widehat{f}(\pi_1, \ldots, \pi_s) \sum_{x_1 \in H_1} \pi_1(-x_1) \sum_{x_s \in H_s} \pi_s(-x_s)$$

$$= \frac{1}{|G_1|\cdots|G_s|} \sum_{\pi_1 \in (\widehat{G_1}:H_1)} \cdots \sum_{\pi_s \in (\widehat{G_s}:H_s)} \widehat{f}(\pi_1, \ldots, \pi_s)|H_1|\cdots|H_s|$$

$$= \frac{1}{|(\widehat{G_1}:H_1)|\cdots|(\widehat{G_s}:H_s)|} \sum_{\pi_1 \in (\widehat{G_1}:H_1)} \cdots \sum_{\pi_s \in (\widehat{G_s}:H_s)} \widehat{f}(\pi_1, \ldots, \pi_s).$$

□

Lemma 7.3 *Suppose $f^i : G_1 \times \cdots \times G_s \to A$, with A a complex algebra, are functions with $i = 1, 2, \ldots, m$. Let $F : G_1^m \times G_2^m \times \cdots \times G_s^m \to A$ be given by*

$$F(x_1^1, \ldots, x_1^m, x_2^1, \ldots, x_2^m, \ldots, x_s^1, \ldots, x_s^m) = \prod_{i=1}^{m} f^i(x_1^i, x_2^i, \ldots, x_s^i).$$

Then $\widehat{F} = \prod_{i=1}^m \widehat{f^i}$, i.e. $\widehat{F}(\pi_1^1, \ldots, \pi_1^m, \pi_2^1, \ldots, \pi_2^m, \ldots, \pi_s^1, \ldots, \pi_s^m) = \prod_{i=1}^m \widehat{f^i}(\pi_1^i, \pi_2^i, \ldots, \pi_s^i)$.

Proof. Straightforward. □

Let $Y_1 = (a_1^1, \ldots, a_1^n) \in (R_1)^n$, $Y_2 = (a_2^1, \ldots, a_2^n) \in (R_2)^n$ and $Y_s = (a_s^1, \ldots, a_s^n) \in (R_s)^n$. Let $f : R_1 \times R_2 \times \cdots \times R_s \to A$ by $f(a_1, a_2, \ldots, a_s) = X_a$ where $a = (a_1, a_2, \ldots, a_s)$, then for $1 \le i_j \le n$ define $f^{i_1, i_2, \ldots, i_s}(a_{i_1}, a_{i_2}, \ldots, a_{i_s})$ and set

$$F(Y_1, Y_2, \ldots, Y_s) = \prod_{1 \le i_j \le |R_j|} f^{i_1, i_2, \ldots, i_s}.$$

All that remains is for find $\widehat{f^{i_1, i_2, \ldots, i_s}}(\pi_{\alpha_1}, \ldots, \pi_{\alpha_s})$ where $\pi_\alpha(z) = \chi([x, y])$ and α_i runs over the elements of R_i.

$$\widehat{f^{i_1, i_2, \ldots, i_s}}(\pi_{\alpha_1}, \ldots, \pi_{\alpha_s}) = \sum_{w_1 \in R_1} \cdots \sum_{w_s \in R_s} \prod_{i=1}^{s} \pi_{\alpha_j}(w_i) f^{i_1, i_2, \ldots, i_s}(w_1, \ldots, w_s)$$

$$= \sum_{w_1 \in R_1} \cdots \sum_{w_s \in R_s} \prod_{i=1}^{s} \chi_i(\alpha_j w_i) X_{(w_1,\ldots,w_s)}$$

Let $a, b \in \mathcal{R}$, and define the matrix T by:

$$T_{a,b} = \prod_{i=1}^{i=s} \chi_i^{a_i b_i},$$

where a_i, b_i denote the i-th coordinate of a and b respectively and χ_i is the generating character of the ring R_i (such a character exists because the ring is Frobenius).

Theorem 7.4 *Let $C_1, C_2, \ldots, C_s$ be codes over the finite Frobenius rings $R_1, R_2, \ldots, R_s$ respectively. Then*

$$P(C_1^\perp, C_2^\perp, \ldots, C_s^\perp)(X_a) = \frac{1}{|C_1||C_2|\cdots|C_s|} P(C_1, C_2, \ldots, C_s)(T(X_a)),$$

where $T(X_a)$ denotes the natural action of the matrix T.

As a corollary to this theorem we get the MacWilliams relations for the joint, complete and Hamming weight enumerators.

7.2. The Weight Enumerator and the Chinese Remainder Theorem

Let $C = \mathrm{CRT}(C_1, C_2, \ldots, C_s)$, assuming of course that the rings are such the Chinese Remainder Theorem applies. Then we have the following:

$$W_C(x_0, x_1, \ldots, x_k) = P(C_1, C_2, \ldots, C_s)(x_{crt(a)}),$$

where $a \in \mathcal{R}$ and $crt(a)$ is the unique element given by the Chinese remainder theorem that is equivalent to a_i in R_i.

Notice that the matrix of $\mathbb{Z}_2 \times \mathbb{Z}_3$ is not exactly the same as the matrix giving the MacWilliams relations for $\mathbb{Z}_6$. However they are equivalent, in that it simply replaces one generating character with another.

Note the generating character for $\mathbb{Z}_6$ is $\omega = e^{\frac{\pi i}{3}}$. Hence the matrix, indexed by $0,1,2,3,4,5$, giving the MacWilliams relations are:

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & -1 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & -1 & \omega^2 & \omega \end{pmatrix}.$$

For the complete combined weight enumerator we have $\chi_{F_2} = -1$ and $\chi_{F_3} = e^{\frac{2\pi i}{3}} = \omega^2$ then $\chi_{F_2}\chi_{F_3} = -\omega^2 = \omega^5$. Then the matrix, indexed by $00, 11, 02, 10, 01, 12$, giving the MacWilliams relations is:

$$\frac{1}{\sqrt{6}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^5 & \omega^4 & -1 & \omega^2 & \omega \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega & \omega^2 & -1 & \omega^4 & \omega^5 \end{pmatrix}.$$

This amounts to replacing the generating character $\chi(1) = \omega$ with the generating character $\chi(1) = \omega^5$.

7.3. Symmetrized Weight Enumerators

Let U_i be a group of units of the ring R_i. We say two elements of R_i are equivalent, (denoted $x \approx y$), if $x = uy$ for some $u \in R_i$. Let H_i denote the set of equivalence classes in R generated by this equivalence relation and let $H = H_1 \times H_2 \times \cdots \times H_s$.

Definition 2 The symmetrized combined weight enumerator is given by

$$S_{U_1,U_2,\ldots,U_s}(C_1, C_2, \ldots, C_s)(X_{[a]}) = \sum_{(c_1,c_2,\ldots,c_s)\in C} \prod_{[a]\in H} X_{[a]}^{n_{[a]}(c_1,c_2\ldots,c_s)},$$

where $n_{[a]} = |\{i \mid \text{for } j = 1\ldots s\ [c_j^i] = [a^i]\}|$ and c_j^i is the i-th coordinate of c_j and a^i is the i-th coordinate of a.

Note that this is a generalization of the definition given in [23].

Let $[a], [b] \in H$, and define the matrix M by

$$M_{a,b} = \prod_{i=1}^{i=s} \sum_{a\in[a_i]} \sum_{b\in[b_i]} \chi_i^{ab},$$

where a_i, b_i denote the i-th coordinate of a and b respectively and χ_i is the generating character of the ring R_i (such a character exists because the ring is Frobenius).

By specializing the variables in the previous lemmas we have the following.

Theorem 7.5 *The MacWilliams relations for the symmetrized weight enumerator are given by*

$$S_{U_1,U_2,\ldots,U_s}(C_1^\perp, C_2^\perp, \ldots, C_s^\perp)(X_{[a]}) \\ = \frac{1}{|C_1||C_2|\cdots|C_s|} S_{U_1,U_2,\ldots,U_s}(C_1, C_2, \ldots, C_s)(M(X_{[a]})),$$

where $M(X_a)$ denotes the natural action of the matrix M.

For the symmetrized weight enumerator as given in [23], the matrix giving the MacWilliams relations, indexed by $0, 1, 2, 3$, is given by:

$$\frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 2 & 2 & 1 \\ 1 & \omega + \omega^5 & \omega^2 + \omega^4 & -1 \\ 1 & \omega^2 + \omega^4 & \omega^4 + \omega^2 & 1 \\ 1 & -2 & 2 & -1 \end{pmatrix},$$

which is identical to the matrix M as given above if $U_1 = \{1\}$ and $U_2 = \{1, 2\}$, except that the matrix is indexed by [0][0], [1][1], [0][1], [1][0].

The symmetrized weight enumerator of a self-dual code over $\mathbb{Z}_6$ is held invariant by this matrix as well as the matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & \omega^4 & 0 \\ 0 & 0 & 0 & \omega^3 \end{pmatrix}.$$

The group of matrices holding the weight enumerator of a Type I code over $\mathbb{Z}_6$ is generated by these matrices. A Magma computation gives that the group has order 384 and the Molien series is given by

$$\frac{t^{40} + 2t^{36} + 2t^{32} + 4t^{28} + 3t^{24} + 3t^{20} + 4t^{16} + 3t^{12} + t^8 + 1}{(1+t^4)^2 (t^8 - t^4 + 1)(t^2 - t + 1)^2 (t^2 + t + 1)^2 (t^4 - t^2 + 1)^2 (t-1)^4 (t+1)^4 (t^2+1)^4},$$

where the denominator is also

$$(1-t^4)(1-t^8)(1-t^{12})(1-t^{24}).$$

The Taylor series is

$$1+t^4+3t^8+7t^{12}+13t^{16}+21t^{20}+35t^{24}+\cdots.$$

Hence by inspection of the denominator there are 4 primary invariants and by inspection of the numerator 24 nontrivial secondary invariants.

References

[1] Bannai E., Dougherty S.T., Harada M. and Oura M., *Type II codes, even unimodular lattices and invariant rings.* IEEE Trans. Inform. Theory, (to appear)

[2] Bonnecaze A., Solé P. and Calderbank A.R., *Quaternary quadratic residue codes and unimodular lattices.* IEEE Trans. Inform. Theory **41** (1995), 366–377.

[3] Bonnecaze A., Solé P., Bachoc C. and Mourrain B., *Type II codes over* $\mathbb{Z}_4$. IEEE Trans. Inform. Theory **43** (1997), 969–976.

[4] Conway J.H., Pless V. and Sloane N.J.A., *The binary self-dual codes of length up to 32: a revised enumeration.* J. Combin. Theory Ser. A **60** (1992), 183–195.

[5] Conway J.H. and Sloane N.J.A., *On the enumeration of lattices of determinant one.* J. Number Theory **15** (1982), 83–94.

[6] Conway J.H. and Sloane N.J.A., *Sphere Packings, Lattices and Groups.* Springer-Verlag, New York, 1993.

[7] Conway J.H. and Sloane N.J.A., *Self-dual codes over the integers modulo* 4. J. Combin. Theory Ser. A **62** (1993), 30–45.

[8] Dougherty S.T., Gulliver T.A. and Harada M., *Type II codes over finite rings and even unimodular lattices.* J. Alg. Combin., (to appear).

[9] Dougherty S.T., *Self-dual codes and symmetric designs.* (submitted).

[10] Dougherty S.T., Harada M. and Solé P., *Shadow codes over* $\mathbb{Z}_4$. Finite Fields and Their Appl., (submitted).

[11] Hammons, Jr. A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A. and Solé P., *A linear construction for certain Kerdock and Preparata codes.* Bull Amer. Math. Soc. **29** (1993), 218–222.

[12] Harada M., *New extremal Type II codes over* $\mathbb{Z}_4$. Des. Codes and Cryptogr. **13** (1998), 271–284.

[13] Harada M., *Weighing matrices and self-dual codes.* Ars Combin. **47** (1997), 65–73.

[14] Huffman W.C., *On extremal self-dual ternary codes of lengths* 28 *to* 40. IEEE Trans. Inform. Theory **38** (1992), 1395–1400.

[15] Klemm M., *Über die Identät von MacWilliams für die Gewichtsfunktion von Codes.* Archiv. Math. **49** (1987), 400–406.

[16] Klemm M., *Selbstduale Codes über dem Ring der ganzen Zahlen modulo* 4. Archiv. Math. **53** (1989), 201–207.

[17] MacWilliams F.J. and Sloane N.J.A., *The Theory of Error-Correcting Codes.* North-Holland, Amstterdam, 1977.

[18] Nebe G., *Private communication.*

[19] Ohmori H., *On the classifications of weighing matrices of order* 12. J. Combin. Math. Combin. Comput. **5** (1989), 161–216.

[20] Pless V., *The number of isotropic subspaces in a finite geometry.* Att. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **39** (1965), 418–421.

[21] Pless V., *On the uniqueness of the Golay codes.* J. Combin. Theory **5** (1969), 215–228.

[22] Pless V., Sloane N.J.A. and Ward H.N., *Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20.* IEEE Trans. Inform. Theory **26** (1980), 305–316.

[23] Wood J., *Duality for modules over finite rings and applications to coding theory.* (submitted).

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510, U.S.A.
E-mail: doughertys1@tiger.uofs.edu

Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990-8560, Japan
E-mail: harada@kszaoh3.kj.yamagata-u.ac.jp

Patrick Solé
CNRS, I3S, ESSI, BP 145
Route des Colles
06 903 Sophia Antipolis, France
E-mail: sole@essi.fr