Journal of Algebraic Combinatorics **9** (1999), 233–250

Type II Self-Dual Codes over Finite Rings and Even Unimodular Lattices

STEVEN T. DOUGHERTY doughertys1@tiger.uofs.edu
Department of Mathematics, University of Scranton, Scranton, PA 18510

T. AARON GULLIVER gulliver@elec.canterbury.ac.nz
Department of Electrical and Electronic Engineering, University of Canterbury, Private Bag 4800, Christchurch, New Zealand

MASAAKI HARADA* mharada@sci.kj.yamagata-u.ac.jp
Department of Mathematical Sciences, Yamagata University, Yamagata 990, Japan

Received September 23, 1997

Abstract. In this paper, we investigate self-dual codes over finite rings, specifically the ring $\mathbb{Z}_{2^m}$ of integers modulo 2^m. Type II codes over $\mathbb{Z}_{2^m}$ are introduced as self-dual codes with Euclidean weights which are a multiple of 2^{m+1}. We describe a relationship between Type II codes and even unimodular lattices. This relationship provides much information on Type II codes. Double circulant Type II codes over $\mathbb{Z}_{2^m}$ are also studied.

Keywords: self-dual code over finite ring, Type II code, double circulant code, even unimodular lattice

1. Introduction

In this paper, we consider self-dual codes over rings, specifically the ring $\mathbb{Z}_{2^m}$ where $\mathbb{Z}_k$ denotes the ring $\mathbb{Z}/k\mathbb{Z}$ of integers modulo k. A code of length n over the ring $\mathbb{Z}_k$ is a subset of $\mathbb{Z}_k^n$, and if the code is an additive subgroup of $\mathbb{Z}_k^n$ then it is a linear code. Unless otherwise stated all codes will be linear. We define an inner product on $\mathbb{Z}_k^n$ by $[x, y] = x_1y_1 + \cdots + x_ny_n \pmod k$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. The orthogonal to a code is defined in the usual way, i.e., $C^\perp = \{v \in \mathbb{Z}_k^n \mid [v, w] = 0 \text{ for all } w \in C\}$. MacWilliams relations for codes over any Frobenius ring are given in [17]. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and C is *self-dual* if $C = C^\perp$. In this paper, two codes over $\mathbb{Z}_k$ are said to be *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*.

The paper is organized as follows. Section 2 examines the existence of self-dual codes over $\mathbb{Z}_k$. Section 3 introduces Type II codes over $\mathbb{Z}_{2^m}$ as self-dual codes with Euclidean weights which are a multiple of 2^{m+1}, and relates these codes with self-orthogonal codes over $\mathbb{Z}_{2^{m+1}}$. In Section 4, we show a relationship between Type II codes over $\mathbb{Z}_{2^m}$ and

*Formerly with the Department of Mathematics, Okayama University, Okayama 700, Japan.

even unimodular lattices. This is a natural generalization of the result in [2]. The above relationship provides much information on Type II codes. In Section 5, we investigate Type II double circulant codes over $\mathbb{Z}_{2^m}$ giving many examples of extremal Type II codes over $\mathbb{Z}_{2^m}$ for $m = 3, 4$ and 5. Section 6 describes the existence of Type II codes of small lengths over $\mathbb{Z}_{2^m}$ for all m.

We refer the reader to [6] and [17] for any elementary facts about codes over finite rings that are used in this paper. For example, any code C over $\mathbb{Z}_k$ has $|C||C^{\perp}| = k^n$.

2. Self-dual codes over $\mathbf{Z}_k$

Self-dual codes over fields are a well studied subject, see [11] for an extensive bibliography. Recently, self-dual codes over $\mathbb{Z}_4$ have been studied, see [1, 2, 6, 8–10, 14, 15]. Cyclic codes over $\mathbb{Z}_k$ have been discussed by a number of authors, see, e.g., [3] and the references given therein. In this section, we examine the existence of self-dual codes over $\mathbb{Z}_k$.

Lemma 2.1 *If k is a square then there exist self-dual codes over $\mathbb{Z}_k$ for all lengths.*

Proof: If $k = r^2$ then the matrix (r) generates a self-dual code of length 1. □

Lemma 2.2 *If C is a self-dual code of odd length over $\mathbb{Z}_k$ then k is a square.*

Proof: Let C be a self-dual code of odd length n over $\mathbb{Z}_k$ so that $|C|^2 = k^n$. Then $|C| = k^{\frac{n}{2}}$, and since n is odd, k must be a square. □

Now consider self-dual codes over $\mathbb{Z}_{2^m}$. If m is odd then 2^m is not a square and by the previous lemma there are no self-dual codes of odd length.

If m is odd then the following matrix

$$\begin{pmatrix} 2^{\frac{m-1}{2}} & 2^{\frac{m-1}{2}} \\ 0 & 2^{\frac{m+1}{2}} \end{pmatrix},$$

generates a code that is self-orthogonal with $2^{\frac{m+1}{2}} 2^{\frac{m-1}{2}} = 2^m$ vectors and therefore is self-dual. Using the well-known direct product construction, self-dual codes can be constructed for all even lengths.

If m is even then 2^m is a square and self-dual codes exist over $\mathbb{Z}_{2^m}$ for all positive lengths.

Theorem 2.3 *There exist self-dual codes over $\mathbb{Z}_{2^m}$ for all lengths if m is even. There exist self-dual codes over $\mathbb{Z}_{2^m}$, m odd, for all lengths n if and only if n is even.*

It is not true that there are self-dual codes over $\mathbb{Z}_k$ for all even lengths for all k. For example, for $k = 6$ there are only two self-orthogonal vectors of length 2 and hence no self-dual code of length 2.

Theorem 2.4 *Let k be an integer that is not a square and assume $k > 1$. If there exists an element $\gamma \in \mathbb{Z}_k$ with $\gamma^2 = -1$ then there exist self-dual codes of length n over $\mathbb{Z}_k$ if and only*

if n is even. If there exist $x, y \in \mathbb{Z}_k$ with $x^2 + y^2 + 1 = 0$ then there exist self-dual codes over $\mathbb{Z}_k$ for all lengths $n \equiv 0 \pmod 4$.

Proof: If there exists $\gamma \in \mathbb{Z}_k$ with $\gamma^2 = -1$ then $(1, \gamma)$ generates a code with k vectors which is self-orthogonal. Hence, there exist self-dual codes of all even lengths over $\mathbb{Z}_k$. Since k is not a square then there are no self-dual codes of odd length by Theorem 2.2. If there exists $x, y \in \mathbb{Z}_k$ with $x^2 + y^2 + 1 = 0$ then the matrix

$$\begin{pmatrix} 1 & 0 & x & y \\ 0 & 1 & y & -x \end{pmatrix},$$

generates a code with k^2 vectors which is self-orthogonal, and therefore is a self-dual code of length 4. □

3. Type II codes over $\mathbf{Z}_{2^m}$

Type II codes over $\mathbb{Z}_4$ have recently been introduced in [1]. In this section, we introduce Type II codes over $\mathbb{Z}_{2^m}$, and relate Type II codes over $\mathbb{Z}_{2^m}$ to self-orthogonal codes over $\mathbb{Z}_{2^{m+1}}$. Cyclic codes over $\mathbb{Z}_{2^m}$ have been discussed in [3].

An application of codes over $\mathbb{Z}_4$ to unimodular lattices prompted the definition of the Euclidean weight of a vector of $\mathbb{Z}_4^n$ (cf. [2]). It is natural to define the Euclidean weights of the elements $0, \pm 1, \pm 2, \pm 3, \ldots, \pm(2^{m-1} - 1), 2^{m-1}$ of $\mathbb{Z}_{2^m}$ as $0, 1, 4, 9, \ldots, (2^{m-1} - 1)^2$, $(2^{m-1})^2$, respectively. 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 define a *Type II* code over $\mathbb{Z}_{2^m}$ as a self-dual code with all vectors having Euclidean weight a multiple of 2^{m+1}. For $m = 1$ this is the standard definition of a Type II code. Note that for $m = 2$ the standard definition of a Type II code requires that it contain the all-one vector as well.

Any code over $\mathbb{Z}_{2^m}$ is permutation-equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,m+1} \\ 0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} & \cdots & \cdots & 2A_{2,m+1} \\ 0 & 0 & 4I_{k_3} & 4A_{3,4} & \cdots & \cdots & 4A_{3,m+1} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 2^{m-1}I_{k_m} & 2^{m-1}A_{m,m+1} \end{pmatrix}, \tag{1}$$

where the matrices $A_{i,j}$ are binary matrices for $i > 1$.

A code of this form is said to be of *type* $\{k_1, k_2, k_3, \ldots, k_m\}$ and it has

$$\prod_{j=1}^{m} (2^{m-j+1})^{k_j},$$

vectors.

Define a map $\Phi : \mathbb{Z}_{2^{m+1}}^n \to \mathbb{Z}_{2^m}^n$ by

$$\Phi(v_1, v_2, \ldots, v_n) = (v_1 \pmod{2^m}, v_2 \pmod{2^m}, \ldots, v_n \pmod{2^m}).$$

For a code C of length n over $\mathbb{Z}_{2^{m+1}}$ we denote its image under this map by $\Phi(C)$.

Lemma 3.1 *The image of a self-orthogonal vector is a vector whose Euclidean weight is a multiple of* 2^{m+1}.

Proof: For v_i in $\mathbb{Z}_{2^{m+1}}$ we have that $v_i^2 \equiv (v_i \pmod{2^m})^2 \pmod{2^{m+1}}$. □

Lemma 3.2 *For C a code over $\mathbb{Z}_{2^{m+1}}$, $\Phi(C^\perp) \subseteq \Phi(C)^\perp$.*

Proof: If $v \in C^\perp$ then $[v, w] = 0$ for all w in C. It is easy to see that $\Phi(v)$ and $\Phi(w)$ are orthogonal in $\mathbb{Z}_{2^m}^n$. Hence $\Phi(v) \in \Phi(C)^\perp$. □

Theorem 3.3 *If C is a self-orthogonal code over $\mathbb{Z}_{2^{m+1}}$ then $\Phi(C)$ is a self-orthogonal code over $\mathbb{Z}_{2^m}$ such that the Euclidean weights of all vectors are a multiple of* 2^{m+1}.

Proof: Follows from the previous lemmas. □

Theorem 3.4 *If C is a code of type $\{k_1, k_2, k_3, \ldots, k_m\}$ over $\mathbb{Z}_{2^m}$, then $\Phi(C)$ is a code of type $\{k_1, k_2, \ldots, k_{m-1}\}$ over $\mathbb{Z}_{2^{m-1}}$.*

Proof: Any vector in C is a linear combination of the rows of a generator matrix of C. Any vector in $\Phi(C)$ is a linear combination of those rows read modulo 2^{m-1}. Hence a generator matrix of $\Phi(C)$ is

$$\begin{pmatrix}
I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,m+1} \\
0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} & \cdots & \cdots & 2A_{2,m+1} \\
0 & 0 & 4I_{k_3} & 4A_{3,4} & \cdots & \cdots & 4A_{3,m+1} \\
\vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\
\vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 2^{m-2}I_{k_m-1} & 2^{m-2}A_{m-1,m}
\end{pmatrix},$$

which corresponds to a code of the required type. □

Note that a generator matrix of a self-orthogonal code over $\mathbb{Z}_{2^{m-1}}$ does not necessarily generate a self-orthogonal code over $\mathbb{Z}_{2^m}$ since the vectors may not be orthogonal.

Corollary 3.5 *If C is a self-orthogonal code of type $\{k_1, k_2, k_3, \ldots, k_m, k_{m+1}\}$ over $\mathbb{Z}_{2^{m+1}}$ of length n with $(2^{m+1})^{k_1}(2^m)^{k_2}\cdots(2)^{k_m} = (2^m)^{\frac{n}{2}}$ then $\Phi(C)$ is a Type II code over $\mathbb{Z}_{2^m}$.*

Proof: The code $\Phi(C)$ is self-orthogonal by Theorem 3.3 and has type $\{k_1, k_2, k_3, \ldots, k_m\}$ by Theorem 3.4, with $(2^{m+1})^{k_1}(2^m)^{k_2}\cdots(2)^{k_m} = (2^m)^{\frac{n}{2}}$. Therefore, $\Phi(C)$ is self-dual. □

4. Type II codes over $\mathbf{Z}_{2^m}$ and even unimodular lattices

A relationship between Type II codes over $\mathbb{Z}_4$ and even unimodular lattices was given in [1] and [2]. In this section, we consider a relationship between Type II codes over $\mathbb{Z}_{2^m}$ and even unimodular lattices. This is a natural generalization of the above result.

Recall that a Type II code over $\mathbb{Z}_{2^m}$ is a self-dual code which has all Euclidean weights divisible by 2^{m+1}. The minimum Euclidean weight d_E of C is the smallest Euclidean weight among all non-zero codewords of C. For $m = 1$ and 2, an upper bound on d_E was given in [12] and [1], respectively.

An n-dimensional lattice Λ in $\mathbb{R}^n$ is the set of integer linear combinations of n linearly independent vectors $v_1, \ldots, v_n$. An $n \times n$ matrix whose rows are the n linearly independent vectors is called a generator matrix of the lattice. The *dual* lattice Λ^* is given by $\Lambda^* = \{x \in \mathbb{R}^n \mid [x, a] \in \mathbb{Z} \text{ for all } a \in \Lambda\}$. 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 $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is called *unimodular*. If the norm $[x, x]$ is an even integer for all $x \in \Lambda$, then Λ is called *even*. The minimum norm of Λ is the smallest norm among all nonzero lattice points of Λ.

Applying Construction A in [7] to self-dual codes over $\mathbb{Z}_{2^m}$, we have the following construction of even unimodular lattices.

Theorem 4.1 *If C is a self-dual code of length n over $\mathbb{Z}_{2^m}$, then the lattice*

$$\Lambda_{2^m}(C) = \frac{1}{\sqrt{2^m}}\{C + 2^m\mathbb{Z}^n\},$$

is an n-dimensional unimodular lattice. The minimum norm is $\min\{2^m, d_E/2^m\}$ where d_E is the minimum Euclidean weight of C. Moreover, if C is Type II then the lattice $\Lambda_{2^m}(C)$ is even unimodular.

Proof: If $a_1, a_2 \in \Lambda_{2^m}(C)$ then $a_i = (c_i + 2^m z_i)/\sqrt{2^m}$ where $c_i \in C$ and $z_i \in \mathbb{Z}^n$ for $i = 1, 2$. Since C is self-dual, the inner product of a_1 and a_2 is

$$[a_1, a_2] = \frac{1}{2^m}\{[c_1, c_2] + 2^m[z_1, c_2] + 2^m[c_1, z_2] + 2^{2m}[z_1, z_2]\} \in \mathbb{Z},$$

thus $\Lambda_{2^m}(C)$ is integral. If C has a generator matrix of the form (1), then the generator matrix of the lattice can be written as

$$\frac{1}{\sqrt{2^m}}\begin{pmatrix} I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \cdots & \cdots & A_{1,m+1} \\ 0 & 2I_{k_2} & 2A_{2,3} & 2A_{2,4} & \cdots & \cdots & 2A_{2,m+1} \\ 0 & 0 & 4I_{k_3} & 4A_{3,4} & \cdots & \cdots & 4A_{3,m+1} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 2^{m-1}I_{k_m} & 2^{m-1}A_{m,m+1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 2^m I_{n-k} \end{pmatrix}, \tag{2}$$

where $k = k_1 + \cdots + k_m$. Thus the determinant of the matrix (2) is 1 and $\Lambda_{2^m}(C)$ is unimodular. It is easy see that $[a_i, a_i] \geq [c_i/\sqrt{2^m}, c_i/\sqrt{2^m}]$ where $a_i = (c_i + 2^m z_i)/\sqrt{2^m}$. Thus the minimum norm is $\min\{2^m, d_E/2^m\}$.

In addition, if C is Type II then since the Euclidean weights are divisible by 2^{m+1}, we have

$$[a_1, a_1] = \frac{1}{2^m}\{[c_1, c_1] + 2^{2m}[z_1, z_1] + 2^{m+1}[c_1, z_1]\} \in 2\mathbb{Z},$$

so that the lattice is even. □

Remark It was suggested in [1] that a construction similar to Theorem 4.1 be considered in order to construct unimodular lattices with minimum norm $\mu > 4$.

Theorem 4.1 provides much information on Type II codes over $\mathbb{Z}_{2^m}$. For example, the following corollary characterizes divisible self-dual codes over $\mathbb{Z}_{2^m}$ in terms of their Euclidean weights.

Corollary 4.2 *Suppose that C is a self-dual code over $\mathbb{Z}_{2^m}$. The greatest common divisor c of Euclidean weights of all codewords of C is either 2^m or 2^{m+1}.*

Proof: If a unimodular lattice has the property that every norm is a multiple of some positive integer d, then d is either 1 or 2 (cf. [13]). If C is self-dual then $\Lambda_{2^m}(C)$ is unimodular. Thus c must be either 2^m or 2^{m+1}. □

Moreover, Theorem 4.1 gives the following restriction on the length of a Type II code.

Corollary 4.3 *If there exists a Type II code C of length n over $\mathbb{Z}_{2^m}$, then n is a multiple of eight.*

Proof: An even unimodular lattice of dimension n can be constructed from C by Theorem 4.1. Even unimodular lattices exist if and only if the dimension is a multiple of eight. Thus n must be a multiple of eight. □

Now let us consider the converse assertion. Calderbank and Sloane [3] investigated cyclic codes of length n over the ring $\mathbb{Z}_{p^a}$ and over the p-adic numbers, where p is a prime not dividing n. In particular, they constructed remarkable cyclic codes over $\mathbb{Z}_{2^m}$ of length 7 for any m. By appending a 1 to the generator vectors of the above codes, Hamming codes $\mathcal{H}_{2^m}$ over $\mathbb{Z}_{2^m}$ of length 8 are constructed. It was shown in [3] that the codes $\mathcal{H}_{2^m}$ are self-dual codes. Moreover, it can easily be seen that all their Euclidean weights are divisible by 2^{m+1}. Thus there exists a Type II code of length 8 over $\mathbb{Z}_{2^m}$, which gives the following proposition.

Proposition 4.4 *There exists a Type II code over $\mathbb{Z}_{2^m}$ of length n if and only if $n \equiv 0 \pmod 8$.*

We now investigate the minimum Euclidean weight of Type II codes over $\mathbb{Z}_{2^m}$. The minimum norm μ of an n-dimensional even unimodular lattice is bounded by $\mu \le 2\lfloor \frac{n}{24} \rfloor + 2$ and even unimodular lattices with $\mu = 2\lfloor \frac{n}{24} \rfloor + 2$ are called *extremal* (cf. [7]). The minimum norm of the lattices constructed from Type II codes C gives directly an upper bound on the minimum Euclidean weight of C.

Proposition 4.5 *Let d_E be the minimum Euclidean weight of a Type II code of length $8n$ over $\mathbb{Z}_{2^m}$. If $\lfloor \frac{n}{3} \rfloor \le 2^{m-1} - 2$, then*

$$d_E \le 2^{m+1}\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right). \tag{3}$$

Proof: Suppose that there exists a Type II code C with minimum Euclidean weight $d_E = 2^{m+1}(\lfloor \frac{n}{3} \rfloor + 2)$. The minimum norm μ of the even unimodular lattice $\Lambda_{2^m}(C)$ constructed from C is $\min\{2^m, 2\lfloor \frac{n}{3} \rfloor + 4\}$. From the assumption, $\mu = 2\lfloor \frac{n}{3} \rfloor + 4$, which is a contradiction. □

When $m = 1$ and 2, the above bound (3) holds without the assumption $\lfloor \frac{n}{3} \rfloor \le 2^{m-1} - 2$. For $m = 1$, (3) is the well-known bound on binary doubly-even self-dual codes, given by Mallows and Sloane [12]. The bound with $m = 2$ was presented in [1]. We conjecture that $d_E \le 2^{m+1}(\lfloor \frac{n}{3} \rfloor + 1)$ for all $m \ge 1$ without the assumption.

A Type II code meeting this bound with equality is called *extremal*. Extremal codes have the largest minimum Euclidean weight among all Type II codes of that length. All Type II codes of lengths 8 and 16 are extremal.

The minimum Hamming weight of a Hamming code $\mathcal{H}_{2^m}$ is always 4 and for the first few values of m, the minimum Lee weights were determined in [3]. By Proposition 4.5, the minimum Euclidean weight of $\mathcal{H}_{2^m}$ is always 2^{m+1}.

5. Double circulant codes

We begin by characterizing the generator matrices of double circulant codes. A *pure double circulant* code of length $2n$ has a generator matrix of the form (I, R) where I is the identity

matrix of order n and R is an $n \times n$ circulant matrix

$$R = \begin{pmatrix} r_0 & r_1 & \cdots & \cdots & r_{n-1} \\ r_{n-1} & r_0 & \cdots & \cdots & r_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ r_1 & r_2 & \cdots & r_{n-1} & r_0 \end{pmatrix}.$$

A code with generator matrix of the form

$$\begin{pmatrix} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I & \vdots & & R' & \\ & \gamma & & & \end{pmatrix}, \tag{4}$$

where R' is an $(n-1) \times (n-1)$ circulant matrix, is called a *bordered double circulant* code of length $2n$. These two families of codes are collectively called *double circulant* codes.

5.1. Preliminaries

We first prove the non-existence of pure double circulant self-dual codes.

Theorem 5.1 *There exists no pure double circulant self-dual code over $\mathbb{Z}_{2^m}$ for $m \geq 2$.*

Proof: Suppose that there exists a pure double circulant self-dual code C with generator matrix of the form (I, R). Since C is self-dual, $RR^T = -I$ over $\mathbb{Z}_{2^m}$, so then

$$\sum_{0 \leq i \leq n-1} r_i^2 = -1 \quad \text{and} \quad \sum_{i \neq j} r_i r_j = 0.$$

Thus we have

$$\begin{aligned} (r_0 + r_1 + \cdots + r_{n-1})^2 &= r_0^2 + r_1^2 + \cdots + r_{n-1}^2 \\ &= -1. \end{aligned}$$

Therefore, -1 must be a quadratic residue in $\mathbb{Z}_{2^m}$. However, -1 is not a quadratic residue in $\mathbb{Z}_{2^m}$ for $m \geq 2$, which is a contradiction. □

Remark Similarly, if -1 is not a quadratic residue in a finite ring then there is no pure double circulant self-dual code over this ring.

Remark Conditions for the existence of double circulant self-dual codes over a finite field $GF(p)$ were given in [16]. It is known that pure double circulant self-dual codes exist for $m = 1$ (cf., e.g., [11]).

We now present two lemmas which are useful in checking the equivalences of bordered double circulant self-dual codes. These lemmas can easily be proven.

Lemma 5.2 *Let C, C', C'' and C''' be codes with generator matrices of the form (I, A), (I, A'), (I, A'') and (I, A'''), respectively, where*

$$A = \begin{pmatrix} \alpha & \beta & \cdots & \beta \\ \gamma & & & \\ \vdots & & R & \\ \gamma & & & \end{pmatrix}, \quad A' = \begin{pmatrix} -\alpha & \beta & \cdots & \beta \\ -\gamma & & & \\ \vdots & & R & \\ -\gamma & & & \end{pmatrix},$$

$$A'' = \begin{pmatrix} -\alpha & -\beta & \cdots & -\beta \\ \gamma & & & \\ \vdots & & R & \\ \gamma & & & \end{pmatrix} \quad \text{and} \quad A''' = \begin{pmatrix} \alpha & -\beta & \cdots & -\beta \\ -\gamma & & & \\ \vdots & & R & \\ -\gamma & & & \end{pmatrix},$$

and R is a square matrix. Then C, C', C'' and C''' are equivalent.

Lemma 5.3 *If the matrix (I, A) generates a self-dual code C, then the matrices $(I, -A)$, (I, A^T) and $(I, -A^T)$ generate self-dual codes which are equivalent to C, where A^T denotes the transpose of the matrix A.*

5.2. An infinite family of double circulant Type II codes

We discuss lengths for which there exist Type II double circulant codes over $\mathbb{Z}_{2^m}$. First, we provide a result required for a subsequent construction, namely if $p \equiv 7 \pmod 8$ then

$$1 + px^2 \equiv 0 \pmod{2^m},$$

has solutions for all $m > 0$, and if $p \equiv 3 \pmod 8$ then

$$5 + px^2 \equiv 0 \pmod{2^m},$$

has solutions for all $m > 0$.

Although the following lemma can be obtained from Hensel's Lemma, we give an elementary proof to emphasize the forms of solutions.

Lemma 5.4 *Suppose that p and q are odd. If a is a solution to $q + px^2 \equiv 0 \pmod{2^m}$, with $m \geq 3$ then either a or $a + 2^{m-1}$ is a solution to $q + px^2 \equiv 0 \pmod{2^{m+1}}$.*

Proof: Let a be a positive integer such that $q + pa^2 \equiv 0 \pmod{2^m}$, or $q + pa^2 = r2^m$ for some integer r. If r is even, say $r = 2k$, then

$$q + pa^2 = k2^{m+1} \equiv 0 \pmod{2^{m+1}},$$

If r is odd, say $r = 2j + 1$, then

$$\begin{aligned} q + p(a + 2^{m-1})^2 &= q + p(a^2 + a2^m + 2^{2m-2}) \\ &= 2^m(2j + 1 + pa + p2^{m-2}) \\ &\equiv 0 \pmod{2^{m+1}}, \end{aligned}$$

since a is odd. □

Proposition 5.5 *If $p \equiv 7 \pmod 8$, then there exists a solution for*

$$1 + px^2 \equiv 0 \pmod{2^m},$$

for all $m > 0$. If $p \equiv 3 \pmod 8$, then there exists a solution for

$$5 + px^2 \equiv 0 \pmod{2^m},$$

for all $m > 0$.

Proof: It is easily verified that $x = 1$ is a solution for $m = 1, 2$ and 3 in both cases. The previous lemma shows that if there is a solution for $m \geq 3$, there is one for $m + 1$. Hence by induction there is a solution for all $m > 0$. □

We now consider certain weighing matrices of order n and weight $n - 1$. A weighing matrix $W_{n,k}$ of order n and weight k is an n by n $(0, 1, -1)$-matrix such that $W_{n,k}W_{n,k}^T = kI$, where $W_{n,k}^T$ is the transpose of $W_{n,k}$.

The following is a well-known method for constructing bordered circulant weighing matrices. Suppose that $n = p + 1$ is a multiple of 4 where p is a prime. Let $P' = (p_{ij})$ be a $p \times p$ matrix where

$$p_{ij} = \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } j - i \text{ is a nonzero square } (\text{mod } p), \\ -1 & \text{otherwise.} \end{cases}$$

The matrix P' is called a Jacobsthal matrix (cf. [11]). Now consider the bordered circulant matrix

$$P_n = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & P' & \\ -1 & & & \end{pmatrix}.$$

Clearly $P_n P_n^T = pI$ over the integers and $P_n = -P_n^T$, so that P_n is a weighing matrix of order $n = p + 1$ and weight p.

(1) The case $p \equiv 7 \pmod 8$: Consider a bordered double circulant code of length $2n$ over $\mathbb{Z}_{2^m}$ with generator matrix of the form (I, xP_n). We denote this code by $D_{2^m}^{2n}(x)$. Since all distinct rows of xP_n are orthogonal over $\mathbb{Z}$, if $1 + px^2 \equiv 0 \pmod{2^m}$ then $D_{2^m}^{2n}(x)$ is self-dual. Moreover, if $1 + px^2 \equiv 0 \pmod{2^{m+1}}$ then $D_{2^m}^{2n}(x)$ is a Type II code. It follows from Proposition 5.5 that if $p \equiv 7 \pmod 8$ then there is an integer a satisfying $1 + pa^2 \equiv 0 \pmod{2^{m+1}}$ for $m > 0$. Thus the generator matrices (I, aP_n) generate Type II bordered double circulant codes for all $m > 0$.
(2) The case $p \equiv 3 \pmod 8$: Consider the matrix $G = (I, 2I + xP_n)$. Since $P_n = -P_n^T$, it must be that $GG^T = (5 + px^2)I$. By Proposition 5.5, G generates a Type II bordered double circulant code $D_{2^m}^{2n}(x)$.

Thus we have an infinite family of Type II bordered double circulant codes.

Theorem 5.6 *Suppose that p is a prime number with $p \equiv 3 \pmod 4$, and let $n = p + 1$. Then there exists a Type II bordered double circulant code of length $2n$ over $\mathbb{Z}_{2^m}$ for all $m > 0$.*

Remark When $m = 2$, the above double circulant codes were given in [9].

Corollary 5.7 *Suppose that there exists a weighing matrix W of order $n \equiv 0 \pmod 4$ and weight $k \equiv 3 \pmod 4$.*
(1) *If $k \equiv 7 \pmod 8$, then there exists an integer x_m such that the matrix $(I, x_m W)$ generates a Type II code over $\mathbb{Z}_{2^m}$ for every $m > 0$.*
(2) *If $k \equiv 3 \pmod 8$. If $W = -W^T$, then there exists an integer x_m such that the matrix $(I, 2I + x_m W)$ generates a Type II code over $\mathbb{Z}_{2^m}$ for every $m > 0$.*

5.3. Double circulant codes of length 8 over Z_8

Here we classify Type II bordered double circulant codes of length 8 over $\mathbb{Z}_8$. By exhaustive search, we have found all distinct double circulant Type II codes of length 8. For these codes, the first rows of R' and the values of α, β and γ of the generator matrices (4) are given

Table 1. Double circulant Type II codes of length 8.

Code	First row of R'	α	β	γ	Code	First row of R'	α	β	γ
$C_{8,1}$	761	2	3	3	$C_{8,17}$	721	6	3	3
$C_{8,2}$	761	2	5	5	$C_{8,18}$	721	6	5	5
$C_{8,3}$	761	6	3	5	$C_{8,19}$	721	2	3	5
$C_{8,4}$	761	6	5	3	$C_{8,20}$	721	2	5	3
$C_{8,5}$	671	2	3	3	$C_{8,21}$	271	6	3	3
$C_{8,6}$	671	2	5	5	$C_{8,22}$	271	6	5	5
$C_{8,7}$	671	6	3	5	$C_{8,23}$	271	2	3	5
$C_{8,8}$	671	6	5	3	$C_{8,24}$	271	2	5	3
$C_{8,9}$	653	2	3	3	$C_{8,25}$	532	6	3	3
$C_{8,10}$	653	2	5	5	$C_{8,26}$	532	6	5	5
$C_{8,11}$	653	6	3	5	$C_{8,27}$	532	2	3	5
$C_{8,12}$	653	6	5	3	$C_{8,28}$	532	2	5	3
$C_{8,13}$	563	2	3	3	$C_{8,29}$	352	6	3	3
$C_{8,14}$	563	2	5	5	$C_{8,30}$	352	6	5	5
$C_{8,15}$	563	6	3	5	$C_{8,31}$	352	2	3	5
$C_{8,16}$	563	6	5	3	$C_{8,32}$	352	2	5	3

Table 2. Weight distributions of length 8 double circulant codes.

	W_H		W_E
Weight	Frequency	Weight	Frequency
0	1	0	1
4	14	16	240
5	336	32	1472
6	672	48	1568
7	1680	64	702
8	1393	80	112
		128	1

in Table 1. These codes have identical Hamming weight distributions W_H and identical Euclidean weight distributions W_E. W_H and W_E are listed in Table 2.

From Lemma 5.2, the four codes $C_{8,4i+1}$, $C_{8,4i+2}$, $C_{8,4i+3}$ and $C_{8,4i+4}$ are equivalent for $0 \le i \le 7$. In addition, it follows from Lemma 5.3 that the four codes $C_{8,1}$, $C_{8,5}$, $C_{8,18}$ and $C_{8,22}$ are equivalent, and the four codes $C_{8,9}$, $C_{8,13}$, $C_{8,30}$ and $C_{8,26}$ are equivalent. Thus the equivalence of only two codes, $C_{8,1}$ and $C_{8,9}$, needs to be checked further. Using the following method, we have determined the inequivalence of these codes. Let $d_i(\varepsilon)$ be the number of pairs (x, y) of codewords x and y, of Hamming weight i, such that the Euclidean weight of a vector $x - y$ is ε. Note that $d_i(0) = A_i$ and $\sum_\varepsilon d_i(\varepsilon) = A_i^2$ where A_i denotes

Table 3. Classification of double circulant codes of length 8.

Code	$d_5(0)$	$d_5(16)$	$d_5(32)$	$d_5(48)$	$d_5(64)$	$d_5(80)$	$d_5(96)$	$d_5(112)$	$d_5(128)$
$C_{8,1}$	336	12032	58208	31168	11152	0	0	0	0
$C_{8,9}$	336	11648	59360	30016	11536	0	0	0	0

the number of codewords of Hamming weight i. Since the Euclidean weights of codewords $x - y$ and $y - x$ are the same, the numbers $d_i(\varepsilon)$ are invariant under the equivalence of codes over $\mathbb{Z}_8$ for each i and ε.

For codes $C_{8,1}$ and $C_{8,9}$, we have obtained the numbers $d_5(\varepsilon)$ for $\varepsilon = 0, 16, \ldots, 128$, and the results are given in Table 3. This table establishes that there exists exactly two inequivalent double circulant self-dual codes of length 8 over $\mathbb{Z}_8$.

5.4. *Double circulant codes of length 16 over Z_8*

By exhaustive search, we have found all distinct double circulant Type II codes of length 16 over $\mathbb{Z}_8$. The only values of α for which there exist bordered double circulant Type II codes are 0 and 4.

We first consider only double circulant codes with $\alpha = 0$. Due to space limitations, we list in Table 4 only those codes which must be checked further for equivalences. The corresponding Euclidean weight distributions, W_j, are given in Table 5. Note that the borders for these codes are $(\alpha, \beta, \gamma) = (0, 3, 3)$. The distinct codes can be determined using Lemmas 5.2 and 5.3.

We now classify the double circulant codes with weight distributions W_i for $1 \le i \le 6$. Obviously, there exists a unique double circulant code, up to equivalence, for W_3 and W_6. Let R_1 and R_2 be circulant matrices with first rows (3731110) and (3171310), respectively.

Table 4. Length 16 double circulant Type II codes with $\alpha = 0$.

Code	First row of R'	W	Code	First row of R'	W
$C_{16,1}$	3731110	W_1	$C_{16,11}$	7353510	W_5
$C_{16,2}$	3171310	W_1	$C_{16,12}$	5571330	W_5
$C_{16,3}$	7113310	W_1	$C_{16,13}$	5135730	W_5
$C_{16,4}$	7753110	W_2	$C_{16,14}$	5535330	W_6
$C_{16,5}$	7317510	W_2	$C_{16,15}$	3775110	W_7
$C_{16,6}$	5171730	W_2	$C_{16,16}$	7157310	W_7
$C_{16,7}$	7717110	W_3	$C_{16,17}$	3375510	W_7
$C_{16,8}$	3135310	W_4	$C_{16,18}$	3571710	W_7
$C_{16,9}$	3331510	W_4	$C_{16,19}$	3535710	W_7
$C_{16,10}$	5331130	W_4	$C_{16,20}$	5375130	W_7

Table 5. Weight distributions of length 16 double circulant codes with $\alpha = 0$.

Weight	W_1 Frequency	W_2 Frequency	W_3 Frequency	W_4 Frequency	W_5 Frequency	W_6 Frequency	W_7 Frequency
0	1	1	1	1	1	1	1
16	480	480	480	480	480	480	480
32	58976	59368	59368	58976	58976	58976	58976
48	732152	729072	728904	732320	732152	732320	732152
64	2866004	2876196	2877148	2865052	2866004	2865052	2866396
80	4972248	4954272	4952256	4974264	4972416	4974432	4970120
96	4641960	4659376	4660944	4640392	4641344	4639776	4646552
112	2480520	2472512	2473296	2479736	2481136	2480352	2475704
128	831326	831606	829254	833678	831606	833958	833566
144	168872	169600	171168	167304	168032	166464	168760
160	22936	23272	23048	23160	23328	23552	22824
176	1568	1232	1064	1736	1624	1792	1456
192	172	228	284	116	116	60	228
256	1	1	1	1	1	1	1

Since R_1 and R_2 are R' of the generator matrices of $C_{16,1}$ and $C_{16,2}$, these codes are equivalent if there exist permutation matrices P and Q such that $R_1 = PR_2Q$. The following matrices

$$P = \begin{pmatrix} 1000000 \\ 0000010 \\ 0001000 \\ 0100000 \\ 0000001 \\ 0000100 \\ 0010000 \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} 0010000 \\ 0000010 \\ 0100000 \\ 0000100 \\ 1000000 \\ 0001000 \\ 0000001 \end{pmatrix},$$

satisfy the equality $R_1 = PR_2Q$, and so establish the equivalence of $C_{16,1}$ and $C_{16,2}$. In this way, it can be determined that $C_{16,i}$, $C_{16,i+1}$ and $C_{16,i+2}$ are equivalent when $i = 1, 4, 8$ and 11. Therefore, we obtain a complete classification of the Type II double circulant codes with weight distributions W_i for $1 \le i \le 6$.

We now investigate the six codes with weight distribution W_7. Since there exist permutation matrices P and Q such that $R_{16} = PR_{17}Q$, where R_{16} and R_{17} are R' of codes C_{16} and C_{17}, respectively, the two codes are equivalent. Similarly, C_{19} and C_{20} can be shown to be equivalent. For codes $C_{16,15}$, $C_{16,16}$ $C_{16,18}$ and $C_{16,19}$, we have calculated $d_7(\varepsilon)$. The values of $d_7(16)$ for these four codes are 2520, 2520, 2184 and 2184, respectively. Thus there are at least two inequivalent codes. Since the two codes $C_{16,i}$ and $C_{16,i+1}$, for both

$i = 15$ and 18, have identical values of $d_7(\varepsilon)$, additional values were calculated for $d_j(\varepsilon)$ for $4 \le j \le 9$. However, these were also found to be identical. If two codes are equivalent then there is an equivalent map from one to the other. We have tested several maps, but have been unable to determine the equivalence or inequivalence of these codes.

Next we consider double circulant codes with $(\alpha, \beta, \gamma) = (4, 3, 3)$. Twenty codes need to be checked for equivalences, and these codes can be obtained from those in Table 4 by replacing 0 in the first row of R' with 4. We denote the code obtained from $C_{16,i}$ by $C'_{16,i}$. The Euclidean weight distributions are listed in Table 6, and the codes corresponding to these distributions are given in Table 7.

The above arguments for codes with $\alpha = 0$ show that there exists a unique Type II double circulant code with W_i $(i = 8, 9, 12$ and $13)$. Moreover, codes in the following groups are equivalent: $(C'_{16,4}, C'_{16,5}, C'_{16,6})$, $(C'_{16,11}, C'_{16,12}, C'_{16,13})$, $(C'_{16,16}, C'_{16,17})$ and $(C'_{16,19}, C'_{16,20})$.

Table 6. Weight distributions of length 16 double circulant codes with $\alpha = 4$.

Weight	W_8 Frequency	W_9 Frequency	W_{10} Frequency	W_{11} Frequency	W_{12} Frequency	W_{13} Frequency
0	1	1	1	1	1	1
16	480	480	480	480	480	480
32	58752	59144	58752	58752	58752	58752
48	733888	730808	733552	733888	733888	733216
64	2860344	2870536	2862444	2860736	2860540	2864348
80	4982136	4963992	4976928	4980008	4980960	4972896
96	4632440	4650472	4638880	4637032	4635744	4642016
112	2484664	2476040	2480576	2479848	2479008	2482144
128	831830	831830	833286	834070	837990	828582
144	167752	169320	166912	167640	163776	170048
160	23048	22992	23776	22936	24224	23328
176	1768	1376	1488	1656	1824	1152
192	112	224	140	168	28	252
256	1	1	1	1	1	1

Table 7. Length 16 double circulant codes with $\alpha = 4$.

W	Codes
W_8	$C'_{16,1}, C'_{16,2}, C'_{16,3}$
W_9	$C'_{16,8}, C'_{16,9}, C'_{16,10}$
W_{10}	$C'_{16,4}, C'_{16,5}, C'_{16,6}, C'_{16,11}, C'_{16,12}, C'_{16,13}$
W_{11}	$C'_{16,15}, C'_{16,16}, C'_{16,17}, C'_{16,18}, C'_{16,19}, C'_{16,20}$
W_{12}	$C'_{16,7}$
W_{13}	$C'_{16,14}$

Table 8. $d_i(\varepsilon)$ for length 16 double circulant codes with $\alpha = 4$.

Code	$d_7(0)$	$d_7(16)$	$d_7(32)$	$d_7(48)$	$d_7(64)$	$d_7(80)$	$d_7(96)$	$d_7(112)$	$d_7(128)$
$C'_{16,4}$	1344	2800	65184	207648	646800	286720	488208	12208	95424
$C'_{16,11}$	1344	2744	64960	208096	646912	286328	488320	12208	95424
$C'_{16,15}$	1400	1568	58856	226072	639352	412776	474712	69552	75712
$C'_{16,16}$	1400	1568	58856	226072	639352	412776	474712	69552	75712
$C'_{16,18}$	1400	2016	61992	218848	643608	406616	483448	67704	74368
$C'_{16,19}$	1400	2016	61992	218848	643608	406616	483448	67704	74368

Further, Table 8 gives the values $d_7(\varepsilon)$ ($\varepsilon = 0, 16, \ldots, 128$) for $C'_{16,4}$, $C'_{16,11}$, $C'_{16,15}$, $C'_{16,16}$, $C'_{16,18}$ and $C'_{16,19}$. This table establishes that there exists at least 8 inequivalent Type II bordered double circulant codes with $\alpha = 4$.

5.5. *Extremal Type II codes of other lengths*

The most remarkable length for extremal Type II codes is 24, because of the connection with the Leech lattice (cf. Lemma 6.1).

Proposition 5.8 *There is no extremal double circulant Type II code over $\mathbb{Z}_8$ of length* 24.

Proof: The possible borders (α, β, γ) of length 24 are only $(\pm 2, \pm 1, \pm 1)$ since the first row of the generator matrix must be self-orthogonal. Thus the Euclidean weight of the first row of the generator matrix (4) is only 16, so the code cannot be extremal. □

It seems infeasible to construct all distinct Type II double circulant codes over $\mathbb{Z}_8$ of larger lengths. For length $2n = 48$, we have determined that $D_8^{48}(3)$ contains vectors of Euclidean weight 32 and so is not extremal.

5.6. *Examples of Type II codes over Z_{16} and Z_{32}*

Here we give examples of Type II double circulant codes over $\mathbb{Z}_{16}$ and $\mathbb{Z}_{32}$. First, some examples of Type II bordered double circulant codes over $\mathbb{Z}_{16}$ of length 8 are given in Table 9. This table also contains the Euclidean weight distributions of the six codes, and establishes that these codes are inequivalent.

We now present Type II codes over $\mathbb{Z}_{32}$ of the same length. For borders $(\alpha, \beta, \gamma) = (6, 3, 3)$, the eight codes with first row (18 7 1), (15 9 2), (31 25 2), (29 26 3), (11 10 5), (27 21 10), (26 19 13), (23 18 17) are Type II codes. Moreover, we have verified that these codes have different Euclidean weight distributions and so are inequivalent.

Table 9. Type II double circulant codes of length 8 over $\mathbb{Z}_{16}$.

(α, β, γ)	(2, 3, 3)	(2, 3, 3)	(2, 3, 3)	(6, 3, 3)	(6, 3, 3)	(6, 3, 3)
First row	7 6 1	14 13 3	14 11 5	7 2 1	15 9 2	11 10 5
Weight	Frequency	Frequency	Frequency	Frequency	Frequency	Frequency
0	1	1	1	1	1	1
32	240	240	240	240	240	240
64	2160	2160	2160	2160	2160	2160
96	6272	6272	6272	6272	6272	6272
128	12560	12560	12560	12560	12560	12560
160	14024	14000	14096	13968	14016	13992
192	14464	14560	14176	14688	14496	14592
224	8188	8080	8560	7904	8144	8024
256	5130	5070	5070	5150	5150	5150
288	1776	2016	1536	2016	1776	1896
320	552	336	720	368	560	464
352	156	240	144	192	144	168
384	12	0	0	16	16	16
512	1	1	1	1	1	1

6. Type II codes over $\mathbf{Z}_{2^m}$ of small lengths and related even unimodular lattices

In this section, we consider Type II codes over $\mathbb{Z}_{2^m}$ of small lengths.

In Section 4, we described the Hamming codes $\mathcal{H}_{2^m}$ as Type II codes of length 8. Theorem 5.6 describes the existence of Type II bordered double circulant codes of length 8. Thus we obtain two infinite families of Type II codes of length 8. Applying Theorem 4.1 to the above codes, we obtain an infinite number of alternative constructions of the unique 8-dimensional even unimodular lattice, which is called the Gosset lattice E_8.

Now consider Type II codes of length 16. $\mathcal{H}_{2^m} \oplus \mathcal{H}_{2^m}$ is a Type II code over $\mathbb{Z}_{2^m}$ of length 16. There exist Type II bordered double circulant codes $D_{2^m}^{16}(x)$ over $\mathbb{Z}_{2^m}$ for any m. For every code C over $\mathbb{Z}_{2^m}$, there is an associated binary code $C^{(1)} = \{c \pmod 2 \mid c \in C\}$. It is easy to see that the binary codes associated with $\mathcal{H}_{2^m} \oplus \mathcal{H}_{2^m}$ and $D_{2^m}^{16}(x)$ are doubly-even self-dual codes. Moreover, they are e_8^2 and d_{16}^+ in [5], respectively. Thus $\mathcal{H}_{2^m} \oplus \mathcal{H}_{2^m}$ and $D_{2^m}^{16}(x)$ are inequivalent for each m. The lattice $\Lambda_{2^m}(\mathcal{H}_{2^m} \oplus \mathcal{H}_{2^m})$ is the even unimodular lattice $E_8 \oplus E_8$, which is one of the two even unimodular lattices of dimension 16.

For the Leech lattice, we have the following lemma.

Lemma 6.1 *Suppose that there exists an extremal Type II code C of length* 24 *over* $\mathbb{Z}_{2^m}$. *Then the Leech lattice can be constructed from C by Theorem* 4.1 *for* $m \geq 2$.

Proof: The lattice constructed from C by Theorem 4.1 is an even unimodular lattice of dimension 24 with minimum norm 4, which must be the Leech lattice. □

For $m = 2$, several extremal Type II codes of length 24 were constructed in [2] and [4]. These codes gave simple alternative constructions of the Leech lattice.

The lifted Golay codes of length 24 over $\mathbb{Z}_{2^m}$ were constructed from the binary Golay code by Hensel lifting (cf. [3]). The lifted Golay codes are Type II codes; however, we have verified that the lifted Golay code over $\mathbb{Z}_8$ is not extremal by computer. In addition, it is shown in Proposition 5.8 that there is no extremal Type II double circulant code over $\mathbb{Z}_8$ of length 24. For $m = 1$ and 2, there are extremal Type II double circulant codes over $\mathbb{Z}_{2^m}$ of length 24 and the Hensel lifted Golay code over $\mathbb{Z}_4$ is extremal. Thus it would be worthwhile to construct extremal Type II codes over $\mathbb{Z}_8$ of length 24.

Acknowledgments

The authors would like to thank Eiichi Bannai, Akihiro Munemasa and Takashi Tasaka for helpful comments. This work was supported in part by a grant from the Japan Society for the Promotion of Science.

References

1. A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, "Type II codes over $\mathbf{Z}_4$," *IEEE Trans. Inform. Theory* **43** (1997), 969–976.
2. A. Bonnecaze, P. Solé, and A.R. Calderbank, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory* **41** (1995), 366–377.
3. A.R. Calderbank and N.J.A. Sloane, "Modular and p-adic cyclic codes," *Designs, Codes and Cryptogr.* **6** (1995), 21–35.
4. A.R. Calderbank and N.J.A. Sloane, "Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices," *J. Alg. Combin.* **6** (1997), 119–131.
5. J.H. Conway, V. Pless, and N.J.A. Sloane, "The binary self-dual codes of length up to 32: A revised enumeration," *J. Combin. Theory Ser. A* **60** (1992), 183–195.
6. J.H. Conway and N.J.A. Sloane, "Self-dual codes over the integers modulo 4," *J. Combin. Theory Ser. A* **62** (1993), 30–45.
7. J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups*, 2nd edition, Springer-Verlag, New York, 1993.
8. 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," *IEEE Trans. Inform. Theory* **40** (1994), 301–319.
9. M. Harada, "New extremal Type II codes over $\mathbb{Z}_4$," *Designs, Codes and Cryptogr.* **13** (1998), 271–284.
10. M. Klemm, "Selbstduale codes über dem Ring der ganzen Zahlen modulo 4," *Arch. Math.* **53** (1989), 201–207.
11. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.
12. C.L. Mallows and N.J.A. Sloane, "An upper bound for self-dual codes," *Inform. Control* **22** (1973), 188–200.
13. O.T.O. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, New York, 1971.
14. V. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over Z_4," *IEEE Trans. Inform. Theory* **42** (1996), 1594–1600.
15. V. Pless, P. Solé, and Z. Qian, "Cyclic self-dual Z_4-codes," *Finite Fields and Their Appl.* **3** (1997), 48–69.
16. M. Ventou and C. Rigoni, "Self-dual doubly circulant codes," *Discrete Math.* **56** (1985), 291–298.
17. J.A. Wood, "Duality for modules over finite rings and applications to coding theory," submitted.