Self-Dual Codes over $\mathbf{Z}_4$ and Unimodular Lattices: A Survey

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

Patrick Solé
CNRS, I3S
ESSI, BP 145
Route des Colles
06 903 Sophia Antipolis
France
Email: sole@alto.unice.fr
and
Philippe Gaborit
Laboratoire A2X
Université Bordeaux I
33400 Talence, France
Email: gaborit@math.u-bordeaux.fr

July 23, 1997

Abstract

By using Construction A modulo 4 the following remarkable unimodular lattices have been constructed: the Gosset lattice E_8, the Leech lattice, the 23 Niemeier lattices in dimension 24, the two extremal even unimodular lattices in dimension 32 with an automorphism of order 31, all the extremal unimodular lattices and the odd Leech lattice. In this survey, we review basic facts of life in the $\mathbf{Z}_4$ world, known families of

$\mathbf{Z}_4$ codes and list open problems for future directions. We give a simplified definition of Type II codes. We also demonstrate that this seemingly weaker definition is indeed equivalent to the original.

1 Introduction

Recently there has been interest in self-dual codes over the ring $\mathbf{Z}_4$ of integers modulo 4. Similarly to binary self-dual codes, self-dual codes over $\mathbf{Z}_4$ relate to combinatorial designs and unimodular lattices. In this survey, we deal with relation to unimodular lattices (for relation to designs see e.g. Section 6 and [25]). We demonstrate that self-dual codes over $\mathbf{Z}_4$ play an important role in the study of unimodular lattices. A connection between codes over $\mathbf{Z}_4$ and unimodular lattices prompted the definition of the Euclidean weight of a vector in $\mathbf{Z}_4^n$ (cf. [5]). It was shown in [5] that self-dual codes with a special divisibility property with respect to the Euclidean weight yield even unimodular lattices using Construction A_4. Self-dual codes with this property are called Type II in [6]. Type II codes are a remarkable class of self-dual codes over $\mathbf{Z}_4$. This class includes the Hensel lifted Golay code of length 24. The lifted Golay code over $\mathbf{Z}_4$ results in the Leech lattice using Construction A_4. This is according to [8] "perhaps the simplest construction of the Leech lattice". This lattice is the most interesting even unimodular lattice and plays a pivotal role in the theory of lattices and finite simple groups. A direct proof of the equivalence between this construction and Leech original construction is given in [10]. The other Type II lattices in dimension 24, the so-called **Niemeier** lattices were constructed in [4] by using a variety of techniques. For background material on lattices, the reader may consult the encyclopedic [15] and the many references therein.

This is a brief survey of relationship between self-dual codes over $\mathbf{Z}_4$ and unimodular lattices. This survey contains no proofs (with only a few exceptions). This survey is organized as follows. In Sections 2 and 3, we give definitions and basic results on self-dual codes and unimodular lattices, respectively. Most of the material in the sections is well-known, but is provided for completeness. In Section 2, we also give a simplified definition of Type II codes. We prove that this seemingly weaker definition is indeed equivalent to the original. Section 4 deals with known families of self-dual codes over $\mathbf{Z}_4$ together with several examples of remarkable self-dual codes. Section 5 explores the related lattices. Section 6 is devoted to open problems for future directions.

2 Definitions from Codes over $\mathbf{Z}_4$

2.1 Codes over $\mathbf{Z}_4$

A linear code C of length n over $\mathbf{Z}_4$ is an additive subgroup of $\mathbf{Z}_4^n$. An element of C is called a codeword of C. A *generator* matrix of C is a matrix the $\mathbf{Z}_4$-span of the rows is C. The

Hamming weight of a codeword is just the number of non-zero components. The Euclidean weights of the elements $0, 1, 2$ and 3 of $\mathbf{Z}_4$ are $0, 1, 4$ and 1, respectively and the Euclidean weight of a codeword is just the rational sum of the Euclidean weights of its components. The minimum Hamming and Euclidean weights, d_H and d_E, of C are the smallest Hamming and Euclidean weights among all non-zero codewords of C, respectively.

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two elements of $\mathbf{Z}_4^n$. We define the inner product of x and y in $\mathbf{Z}_4^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n \pmod 4$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbf{Z}_4^n |\ x \cdot y = 0 \text{ for all } y \in C\}$. C is *self-dual* if $C = C^\perp$. We say that two codes 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*. The automorphism group of C consists of all permutations and sign-changes of the coordinates that preserve C. Any code is permutation-equivalent to a code with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B_1 + 2B_2 \\ 0 & 2I_{k_2} & 2D \end{pmatrix}, \tag{1}$$

where A, B_1, B_2 and D are matrices over $\mathbf{Z}_2$. We say that a code with generator matrix (1) has *type* $4^{k_1}2^{k_2}$ (cf. [14]). The binary $[n, k_1]$ code $C^{(1)}$ with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B_1 \end{pmatrix}, \tag{2}$$

is called the *residue code* of the $\mathbf{Z}_4$ code C. The binary $[n, k_1 + k_2]$ code $C^{(2)}$ with generator matrix of the form

$$\begin{pmatrix} I_{k_1} & A & B_1 \\ 0 & I_{k_2} & D \end{pmatrix}, \tag{3}$$

is called the *torsion code* of C.

Several weight enumerators are associated with a code over $\mathbf{Z}_4$. In this survey, we deal with the symmetrized weight enumerators. The symmetrized weight enumerator (swe) of a code C over $\mathbf{Z}_4$ is given by

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

where $n_i(x)$ is the number of components of $x \in C$ that are congruent to $i \pmod 4$. Note that equivalent codes have identical swe's. Klemm [28] established the MacWilliams identities for a code over $\mathbf{Z}_4$.

Theorem 2.1 (Klemm [28])

$$swe_{C^\perp}(a, b, c) = \frac{1}{|C|} swe_C(a + 2b + c, a - c, a - 2b + c).$$

2.2 Type II Codes and Type I Codes

There are two classes of self-dual codes over $\mathbf{Z}_4$ those in which the Euclidean weights of the codewords are divisible by a constant $c > 1$, namely Type I codes and Type II codes. These classes are closely related to two classes of unimodular lattices.

Type II codes over $\mathbf{Z}_4$ were first defined in [6] as self-dual codes containing the all-ones vector and with the property that all Euclidean weights are divisible by eight. However, even if Type II codes do not contain the all-ones vector, the lattices constructed from these codes are even unimodular (see Theorem 3.4). In this survey, we say that self-dual codes with the property that all Euclidean weights are divisible by eight are *Type II*. The following lemma shall show that this seemingly weaker definition is indeed equivalent to the original. Self-dual codes which are not Type II are called *Type I*.

We have proved following useful result:

Lemma 2.2 *Any Type II code contains a vector whose components are* 1 *or* 3*.*

Proof. The conclusion is equivalent to saying that the residue code contains the all-one vector. By self-duality this, in turn, amounts to say that the torsion code has even Hamming weights. But for a vector comprising only 0 and 2, the Euclidean weight is four times the Hamming weight. The result follows by the congruence condition. □

Thus any Type II code is equivalent to a Type II code which has the all-ones vector.

Theorem 2.3 *The symmetrized weight enumerator of a Type II code belongs to the ring*

$$S \oplus \psi_{16} S,$$

where S is the ring of polynomials in $\phi_8, \theta_8, \phi_{24}$ where

$$\begin{aligned} \phi_8 &\quad \textit{is the swe of } O_8 \textit{ in [14],} \\ \theta_8 &\quad \textit{is the swe of } Q_8 \textit{ in [14],} \\ \psi_{16} &\quad \textit{is the swe of } RM(1,4) + 2RM(2,4), \\ \phi_{24} &\quad \textit{is the swe of the lifted Golay code.} \end{aligned}$$

This ring has Molien series

$$\frac{1+\lambda^{16}}{(1-\lambda^8)^2(1-\lambda^{24})} = 1 + 2\lambda^8 + 4\lambda^{16} + 7\lambda^{24} + \cdots.$$

Remark. The above theorem was fisrt proved by Bonnecaze, Solé, Bachoc and Mourrain [6], independently Calderbank and Sloane [9], under the condition that the code contains the all-ones vector. Lemma 2.2 shows the result holds without the condition.

Corollary 2.4 *A Type II code of length n exists if and only if $n \equiv 0 \pmod 8$.*

Proof. The degrees of basic polynomials of the swe of a Type II code give that if a Type II code exists then the length is a multiple of eight. There are Type II codes of length 8. □

Now we describe what is known about the classification of self-dual codes over $\mathbf{Z}_4$. In [14], Conway and Sloane began the classification and gave the classification of length up to 9 without a mass formula. They also suggested finding a mass formula. Later this was found by Gaborit [20]. Using this, Pless, Leon and Fields [35] classified Type II codes of length 16 containing the all-ones vector. By Lemma 2.2, their classification yields the classification of all Type II codes of length 16. Then all self-dual codes of length up to 15 were classified by Fields, Gaborit, Leon and Pless [19].

3 Background Material on Lattices

3.1 Definitions and Basic Results

We present brief known results on unimodular lattices. Most of the results described in this subsection are due to [15].

An n-dimensional lattice Λ in $\mathbf{R}^n$ is the set of integer linear combinations of n linearly independent vectors $v_1, \ldots, v_n$, where $\mathbf{R}^n$ is the n-dimensional Euclidean space. An n by n matrix whose rows are the n linearly independent vectors is called a generator matrix of the lattice. If two lattices differ only by a rotation, a scaling and/or a reflection, they are called *equivalent*. The *dual* lattice Λ^* is given by $\Lambda^* = \{x \in \mathbf{R}^n \mid x \cdot a \in \mathbf{Z} \text{ for all } a \in \Lambda\}$, where $x \cdot a = x_1 a_1 + \cdots + x_n a_n$ 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 $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is called *unimodular*. The theta series $\Theta_\Lambda(q)$ of a lattice Λ is the formal power series

$$\Theta_\Lambda(q) = \sum_{x \in \Lambda} q^{x \cdot x}.$$

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

If the norm $x \cdot x$ is an even integer for all $x \in \Lambda$, then Λ is said to be *even*. Unimodular lattices which are not even are called *odd*. It is known that if a unimodular lattice has the property that every norm is a multiple of some positive integer c then c is 1 or 2. The minimum norm μ of Λ is the smallest norm among all nonzero lattice points of Λ.

We describe upper bounds for unimodular lattices and present the notion of extremality for the norm.

Theorem 3.1 (Hecke, see also [15]) *If Λ is unimodular then*

$$\Theta_\Lambda(z) \in \mathbf{C}[\theta_3(z), \Delta_8(z)],$$

where $\theta_3(z) = \sum_{m=-\infty}^{\infty} q^{m^2}$ and $\Delta_8(z) = q \prod_{m=1}^{\infty} \{(1-q^{2m-1})(1-q^{4m})\}^8$.

Moreover if Λ is even unimodular then

$$\Theta_\Lambda(z) \in \mathbf{C}[E_4(z), \Delta_{24}(z)],$$

where $E_4(z)$ is the theta series of the 8-dimensional unique even unimodular lattice E_8 and $\Delta_{24}(z) = q^2 \prod_{m=1}^{\infty}(1-q^{2m})^{24}$.

This gives that n-dimensional even unimodular lattices exist if and only if $n \equiv 0 \pmod 8$. Note that there is a unique 8-dimensional even unimodular lattice E_8 which is called the Gosset lattice.

Corollary 3.2 *If Λ is an n-dimensional unimodular lattice, then the minimum norm μ is bounded by*

$$\mu \le (\lfloor \frac{n}{8} \rfloor + 1). \tag{4}$$

Moreover if Λ is an n-dimensional even unimodular lattice, then the minimum norm μ is bounded by

$$\mu \le 2(\lfloor \frac{n}{24} \rfloor + 1). \tag{5}$$

Remark. The upper bound (5) is stronger than (4).

Unimodular lattices meeting (4) with equality are said to be *extremal* unimodular lattices, and even unimodular lattices meeting (5) with equality are said to be *extremal* even unimodular lattices.

For extremal unimodular lattices, Conway, Odlyzko and Sloane [12] proved the following:

Theorem 3.3 (Conway, Odlyzko and Sloane [12]) *The only extremal unimodular lattices are $\mathbf{Z}^n$ $(1 \le n \le 7)$, E_8, D_{12}^+, $(E_7+E_7)^+$, A_{15}^+, the shorter Leech lattice O_{23} and the Leech lattice Λ_{24}.*

Extremal even unimodular lattices are known in dimension $n \le 64$ (cf. [15, Chapter 7]). The first open case is dimension $n = 72$. For $n \le 24$, extremal even unimodular lattices were classified, the numbers of the lattices are $1, 2$ and 1 for $n = 8, 16$ and 24, respectively. For $n = 32$, there are at least five inequivalent extremal even unimodular lattices (cf. [32]): those are obtained by (binary) Construction B.

Now we describe what is known about the classification. Unimodular lattices were classified for dimension $n \le 25$ (cf. [15]). The number of the unimodular lattices was given in [15, Table 2.2].

- There exists a unique 8-dimensional even unimodular lattice E_8.
- There exist two 16-dimensional even unimodular lattices, namely $E_8 + E_8$ and D_{16}^+ (cf. [39]).

- Niemeier [34] classified the 24-dimensional even unimodular lattices. There exist 24 such lattices, one of which has the minimum norm 4 (that is, extremal) and is called the Leech lattice. We say that the 23 remaining lattices are Niemeier lattices.
- Bacher and Venkov [2] have classified unimodular lattices without roots in dimensions $26, 27$ and 28 by the norm of their shadows. For instance they proved there is a unique unimodular lattice without roots in dimension 27 with a shadow containing a vector of norm $3/4$. In dimension 28 there are exactly two unimodular lattice without roots with a shadow containing a vector of norm 1.
- Koch and Venkov [32] classified unimodular lattices in dimension 32 with nachbardefekt zero.
- Kervaire [27] classified unimodular lattices in dimension 32 with a *complete* root system (i.e. spanning a sublattice is of finite index).
- Quebbemann [38] classified unimodular lattices in dimension 32 with an automorphism of order 31.

3.2 Construction A_4 and Related Results

Applying Construction A to self-dual codes over $\mathbf{Z}_4$, we have the following construction which is called Construction A_4.

Theorem 3.4 (Bonnecaze, Solé and Calderbank [5]) *Let C be a self-dual code of length n over $\mathbf{Z}_4$ with minimum Euclidean weight d_E. Then the lattice*

$$A_4(C) = \frac{1}{2}\{x \in \mathbf{Z}^n \mid x \equiv c \pmod 4 \text{ for some } c \in C\},$$

is an n-dimensional unimodular lattice. The minimum norm of $A_4(C)$ is $\min\{4, d_E/4\}$ and we have

$$\Theta_{A_4(C)}(q^4) = swe_C(\Theta_{4\mathbf{Z}}(q), \Theta_{4\mathbf{Z}+1}(q), \Theta_{4\mathbf{Z}+2}(q)).$$

Moreover if C is Type II then the lattice $A_4(C)$ is even unimodular.

In Section 5, we shall show that a number of interesting unimodular lattices are constructed from self-dual codes over $\mathbf{Z}_4$ by the above theorem.

We now describe a result on an upper bound for the Euclidean weights of Type II codes. Bonnecaze, Solé, Bachoc and Mourrain [6] showed that the minimum Euclidean weight d_E of a Type II code of length n with the all-ones vector is bounded by $d_E \leq 8(\lfloor \frac{n}{24} \rfloor + 1)$. Therefore Lemma 2.2 gives the following:

Theorem 3.5 *The minimum Euclidean weight d_E of a Type II code of length n is bounded by*

$$d_E \leq 8(\lfloor \frac{n}{24} \rfloor + 1).$$

A Type II code meeting this bound with equality is called *extremal*. Extremal Type II codes produce extremal even unimodular lattices for length $n \leq 40$ by Theorem 3.4. In particular, different extremal Type II codes of length 24 give different generator matrices of the Leech lattice.

Proposition 3.6 (Harada [26]) *Let d_E be the minimum Euclidean weight of a Type I code of length n over $\mathbf{Z}_4$.*

$$d_E \leq \begin{cases} 4(\lfloor \frac{n}{8} \rfloor + 1) & n = 1, \ldots, 7, 12, 14, 15 \text{ and } 23, \\ 4\lfloor \frac{n}{8} \rfloor & \text{otherwise}, \end{cases}$$

for length $n \leq 24$.

The above upper bound is a consequent result on Corollary 3.2.

4 Examples of Self-Dual Codes over $\mathbf{Z}_4$

We describe known families of self-dual codes.

- Klemm's code K_{4m} [28]:
  K_{4m} is a self-dual code of length $4m$ introduced by Klemm [28] with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 2 & 0 & \cdots & 0 & 2 \\ 0 & 0 & 2 & \cdots & 0 & 2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 2 & 2 \end{pmatrix}.$$

  When m is even, K_{4m} is a Type II code with $d_E = 8$. In fact one of the four inequivalent Type II codes of length 8 is K_8.

  K_{4m} determines the following unimodular lattice.

  Lemma 4.1 (Bonnecaze, Gaborit, Harada, Kitazume and Solé [4]) *The lattice $A_4(K_{4m})$ is D_{4m}^+.*

- $(u|u+v)$ construction [5]:
  Let C_1 and C_2 be binary linear codes and let

$$C_1 + 2C_2 = \{(u|u+v) \mid u \in C_1, v \in C_2\}.$$

  Then $C_1 + 2C_2$ is a linear code over $\mathbf{Z}_4$ if and only if $a * b \in C_2$ for all $a, b \in C_1$, where $*$ denotes the componentwise multiplication. In that case the residue code is C_1 and the torsion code $C_1 + C_2$. Let $C_{m,r}$ denote Reed-Muller codes $RM(r,m) + 2RM(m-r-1,m)$ where $RM(r,m)$ is the rth order binary Reed-Muller code of length 2^m. This code is a special class of the above family.

Theorem 4.2 (Bonnecaze, Solé, Bachoc and Mourrain [6]) *The code $C_{m,r}$ is a Type II code for $0 \leq r \leq (m-1)/3$ and $m \geq 3$.*

$C_{5,1}$ is an extremal Type II code of length 32.

- Extended quadratic residue codes [5], [36]:
  Let Q be the set of quadratic residues modulo p and N the set of nonquadratic residues where $p \equiv \pm 1 \pmod 8$ is a prime, and write

$$x^p - 1 = (x-1)m_Q(x)m_N(x),$$

where

$$m_Q(x) = \prod_{i \in Q}(x - \alpha^i), \quad m_Q(x) = \prod_{i \in N}(x - \alpha^i),$$

are polynomials with binary coefficients, and α is a primitive pth root of unity in an appropriate extension of $\mathbf{F}_2$. The binary quadratic residue codes $Q_2, \overline{Q_2}, N_2$ and $\overline{N_2}$ are the cyclic codes generated by $m_Q(x), (x-1)m_Q(x)$, $m_N(x)$ and $(x-1)m_N(x)$, respectively.

Let us consider a binary cyclic code generated by a polynomial $h_2(x)$ of degree m, where $h_2(x)$ divides $x^l - 1$ and l is minimal subject to this property. There is a unique monic polynomial $h(x) \in \mathbf{Z}_4[x]$ of degree m such that $h(x) \equiv h_2(x) \pmod 2$ and $h(x)$ divides $x^l - 1 \pmod 4$. We refer to $h(x)$ as the Hensel lift of $h_2(x)$. The quadratic residue codes $Q_4, \overline{Q_4}, N_4$ and $\overline{N_4}$ over $\mathbf{Z}_4$ are defined to be the cyclic codes generated by the Hensel lifts of $m_Q(x), (x-1)m_Q(x), m_N(x)$ and $(x-1)m_N(x)$, respectively.

Theorem 4.3 (Bonnecaze, Solé and Calderbank [5]) *Let $p \equiv -1 \pmod 8$. The extended quadratic residue code QR_{p+1} which is the extended code of Q_4 is a Type II code of length $p+1$.*

Remark. The extended code of C is the code obtained by adding an overall parity check to each codeword of C.

For $p = 7$ and 23, the Hensel lifts of the binary polynomials $m_Q(x)$ are

$$\begin{aligned} f_7 &= x^3 + 3x^2 + 2x + 3, \\ f_{23} &= x^{11} + 2x^{10} + 3x^9 + 3x^7 + 3x^6 + 3x^5 + 2x^4 + x + 3, \end{aligned}$$

respectively. QR_8 is equivalent to O_8, and QR_{24} and QR_{48} are extremal. The extended code of the cyclic code generated by the binary polynomial $f_{23} \pmod 2$ is the binary Golay code. Thus QR_{24} is also called the (Hensel) lifted Golay code.

- Cyclic self-dual codes [5], [7], [8], [37], [36]:
A cyclic code C of length n is a linear code with the property that if $(c_0, c_1, \ldots, c_{n-1}) \in C$ then $(c_1, \ldots, c_{n-1}, c_0) \in C$. Quadratic residue codes are a remarkable class of cyclic codes. It was shown in [8] and [36] that any cyclic code over $\mathbf{Z}_4$ is uniquely generated by polynomials fh and $2fg$ (denoted by $C = (fh, 2fg)$), where $fgh = x^n - 1$ and $|C| = 4^{\deg g} 2^{\deg h}$. For n odd, the cyclic code generated by (2) is self-dual. This trivial cyclic self-dual code is not considered in this survey.

Theorem 4.4 (Pless, Solé and Qian [37]) *Let C be a cyclic code over $\mathbf{Z}_4$, $C = (fh, 2fg)$, where $fgh = x^n - 1$ and n odd. Then C is self-dual if and only if $f = \varepsilon g^*$ and $h = \delta h^*$, where ε and δ are units and g^* is the reciprocal of g.*

Theorem 4.5 (Pless, Solé and Qian [37]) *Cyclic self-dual codes of length n exist if and only if $-1 \not\equiv 2^i \pmod{n}$ for any i.*

All cyclic self-dual codes and the extended cyclic self-dual codes were found in [37] for length up to 40.

- Double circulant codes [9], [22], [23]:
We give 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 by n circulant matrix. A code with generator matrix of the form

$$\begin{pmatrix} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I & \vdots & & R' & \\ & \gamma & & & \end{pmatrix}, \tag{6}$$

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

Theorem 4.6 (Dougherty, Gulliver and Harada [16]) *There exists no pure double circulant self-dual code over $\mathbf{Z}_4$.*

Thus we consider only bordered double circulant self-dual codes.

A remarkable Type II code O_8 in [14] of length 8 has the following generator matrix

$$\begin{pmatrix} 1000 & 2111 \\ 0100 & 3213 \\ 0010 & 3321 \\ 0001 & 3132 \end{pmatrix},$$

thus O_8 is a double circulant Type II code which is the smallest example of such codes.

Calderbank and Sloane [9] provided a class of double circulant codes D_n over $\mathbf{Z}_4$. Let $n = 2p + 2$ where p is a prime congruent to 3 (mod 8). The code D_n has generator matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 1 & & & & 0 & & & \\ \vdots & & I & & \vdots & & I + 3R + 2N & \\ 1 & & & & 0 & & & \end{pmatrix},$$

if $p \equiv 3 \pmod{16}$, or

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 1 & & & & 0 & & & \\ \vdots & & I & & \vdots & & b(I + R) & \\ 1 & & & & 0 & & & \end{pmatrix},$$

if $p \equiv 11 \pmod{16}$, where $R = (R_{ij})$, $R_{ij} = 1$ if $j - i$ is a nonzero square (mod p), or 0 otherwise; $N = (N_{ij})$, $N_{ij} = 1$ if $j - i$ is not a square (mod p), or 0 otherwise; b can be either 1 or 3; and I is the identity matrix. It is easy to see that the generator matrices can be transformed into a matrix of the form (6). D_n is a Type II double circulant code of length n over $\mathbf{Z}_4$. In particular, when p is 19 the code D_{40} is an extremal Type II code. D_{24} in [9] is not extremal, but another extremal double circulant code was given. Extremal double circulant Type II (resp. Type I) codes of length 24 were classified in [22] (resp. [23]).

- From combinatorics [24], [28]:
  Let M be an incidence matrix of a symmetric 2-(v, k, λ) design such that λ is odd and $k - \lambda \equiv 4 \pmod{8}$. Klemm [28] showed that the rows of span a code C with $< C^{\perp}, j >$ and that $< C^{\perp}, 2j >$ is self-dual, where j is the all-ones vector of length v.

  A weighing matrix $W_{n,k}$ of order n and weight k is an n by n $(0, 1, -1)$-matrix such that $W_{n,k} {W_{n,k}}^{\mathrm{t}} = kI$ where ${W_{n,k}}^{\mathrm{t}}$ is the transpose of $W_{n,k}$.

  Proposition 4.7 (Harada [24]) *Let $W_{n,k}$ be a weighing matrix of order n and weight k.*

  (1) If $n \equiv 0 \pmod{4}$ and $k \equiv 7 \pmod{8}$. Assume that the sum of all the entries in every column of $W_{n,k}$ is $\equiv 1 \pmod{4}$, then the matrix $(\ I\ ,\ W_{n,k}\ )$ generates a Type II code $C(W_{n,k})$ of length $2n$.

  (2) If $n \equiv 0 \pmod{4}$ and $k \equiv 3 \pmod{8}$. Assume that the sum of all the entries in every column of $W_{n,k}$ is $\equiv 3 \pmod{4}$ and all diagonal entries are 0. If $W_{n,k} = {W_{n,k}}^{t}$ or $-{W_{n,k}}^{t}$, then the matrix $(\ I\ ,\ W_{n,k} + 2I\ )$ generates a Type II code $C(W_{n,k})$ of length $2n$.

Remark. Conway and Sloane [14] gave a method for constructing self-dual codes over $\mathbf{Z}_4$ using skew-type Hadamard matrices. Their method is a special case of the above method.

- Other methods:
(1) Shadows [17]:
Recently shadow codes over $\mathbf{Z}_4$ have been introduced in [17]. The even weight subcode C_0 of a Type I code C is the set of codewords of C of Euclidean weights divisible by 8. C is of index 2 in $C_0^{\perp}$ and we let $C_0^{\perp} = C_0 \bigcup C_2 \bigcup C_1 \bigcup C_3$, where $C = C_0 \bigcup C_2$. With these notations define the shadow of C as $S := C_1 \bigcup C_3$. Using orthogonality relations among C_i's, several extensions of self-dual codes were given in [17]. In particular, we have the following method.

Theorem 4.8 (Dougherty, Harada and Solé [17]) *Suppose that C is a self-dual code of length $n \equiv 3 \pmod 4$. Let C^* be the code of length $n+1$ obtained by extending $C_0^{\perp}$ as follows:*

$$(0, C_0), (1, C_1), (2, C_2), (3, C_3).$$

Then if $n \equiv 7 \pmod 8$ then C^* is a Type II code and if $n \equiv 3 \pmod 8$ then C^* is a Type I code.

In particular, if C is an extremal Type I code of length 23 then the extended code C^* of length 24 is an extremal Type II code, that is $d_E = 16$.

Since an extremal Type II code of length 24 determines the Leech lattice, this method gives another Construction A_4 of the Leech lattice.

(2) A pseudo-random method [24]:
The following method generates many different generator matrices of Type II codes from existing Type II codes, increasing the chance that some of them are extremal and inequivalent.

Theorem 4.9 (Harada [24]) *Let C be a Type II code of length $8n$ with generator matrix of the form $(I \ , \ A)$ where a_i is the i-th row of A. Let Γ be a set consisting of α columns of A where $0 \leq \alpha \leq 4n$. Let $\boldsymbol{t} = (t_1, \cdots, t_{4n})$ be a $(1,0)$-vector where $t_i = 1$ if $i \in \Gamma$ and $t_i = 0$ otherwise. Let A_Γ be a matrix which has the i-th row*

$$a_i' = \begin{cases} a_i + 2\boldsymbol{t}, & \text{if } \|a_i + 2\boldsymbol{t}\| \equiv 7 \pmod 8, \\ a_i + 2\boldsymbol{t} + 2\boldsymbol{j}, & \text{otherwise,} \end{cases}$$

where $\|x\|$ denotes the Euclidean weight of x and $\boldsymbol{j}$ is the all-ones vector. Then the matrix $G = (I \ , \ A_\Gamma)$ generates a Type II code C_Γ.

5 Corresponding Unimodular Lattices

5.1 Even Unimodular Lattices

- $n = 8$:
  There are exactly four inequivalent Type II codes of length 8. The four codes give different constructions of E_8.

- $n = 16$:
  $E_8 + E_8$ and D_{16}^+ are the two even unimodular lattices in dimension 16. There are exactly 133 inequivalent Type II codes of length 16 corresponding to $E_8 + E_8$ or D_{16}^+. $C_8 \oplus C_8' = \{(c_1, c_2) \mid c_1 \in C_8, c_2 \in C_8'\}$ is a Type II code of length 16 where C_8 and C_8' are Type II codes of length 8. The code determines the lattice $E_8 + E_8$. By Lemma 4.1, the lattice $A_4(K_{16})$ is D_{16}^+. Thus there is at least one corresponding Type II code for each lattice.

- $n = 24$:
  (1) The Leech lattice:
  In [5], the lifted Golay code is shown to determine the Leech lattice. This is one of the simplest construction of this remarkable lattice. This construction motivates us to study self-dual codes, in particular Type II codes over $\mathbf{Z}_4$. Several inequivalent extremal Type II codes were found. There are nine binary doubly-even self-dual codes of length 24, one of which is the binary Golay code. The residue code $C^{(1)}$ of the lifted Golay code is the binary Golay code. An extremal Type II code corresponding to one of the remaining eight binary codes was found in [9]. For the remaining seven codes, corresponding extremal Type II codes have recently been constructed by Young and Sloane (see Postscript of [9]). An extremal Type II code was found by Theorem 4.9 from a non-extremal Type II code (cf. [24]). It was shown in [22] that there are exactly five inequivalent extremal double circulant Type II codes. Table 1 lists the first rows of R' along with the values α, β and γ in (6).

Table 1: Extremal Double Circulant Type II Codes of Length 24

Code	First row of R'	α	β	γ	Code	First row of R'	α	β	γ
$C_{24,1}$	31321121000	2	3	1	$C_{24,4}$	33331231111	2	3	1
$C_{24,2}$	13212223110	2	3	1	$C_{24,5}$	33313213111	2	3	1
$C_{24,3}$	31333321111	2	3	1					

  (2) The Niemeier lattices:
  As described above, the Leech lattice was constructed from certain extremal Type II codes over $\mathbf{Z}_4$. This raised the question to know if other even unimodular lattices in dimension 24 could be constructed in that way.

Recently Bonnecaze, Gaborit, Harada, Kitazume and Solé [4] have established the following answer.

Theorem 5.1 (Bonnecaze, Gaborit, Harada, Kitazume and Solé [4]) *Every Niemeier lattice is $A_4(C)$ for some Type II code C.*

Combining the above theorem with known results, we have the following:

Corollary 5.2 (Bonnecaze, Gaborit, Harada, Kitazume and Solé [4]) *All the n-dimensional even unimodular lattices can be constructed from Type II codes over $\mathbf{Z}_4$ by Theorem 3.4 for $n \leq 24$.*

- $n = 32$:
  A number of extremal Type II codes of length 32 were found. By a theorem of Quebbemann there are only two unimodular lattices of dimension 32 with an isomorphism of order 31 (cf. [38]). These two lattices can be constructed by Construction A_4 from $QRM(2,5)$ (the Barnes-Wall lattice BW_{32}) and from QR_{32} as was shown in [10]. The lattice constructed from QR_{32} is denoted by $BSBM_{32}$. These codes are extended cyclic self-dual codes. Three more such codes were constructed in [37]. Recently 50 new extremal Type II codes have been found in [21], which raises the number of known inequivalent extremal Type II codes to 57.

- $n = 40$:
  D_{40} in [9] is an extremal Type II code of length 40. Another one was constructed in [37] from an extended cyclic code. Later an extremal Type II code was constructed from a weighing matrix by Proposition 4.7. Recently several new extremal Type II codes have been found by Theorem 4.9 (cf. [21]).

  Nebe and Souvignier determined that the automorphism groups of the lattice $A_4(D_{40})$ and the MacKay lattice (cf. [15]) are $2 \cdot PGL_2(19)$ and $2^{20} \cdot PGL_2(19)$, respectively, showing that the two lattices are not equivalent (see Postscript of [9]). It was a question in [9] to determine if the two lattices are equivalent. Nebe also found that the MacKay lattice can be obtained from a Type II code.

- A table of codes and lattices:
  We list in Table 2 extremal Type II codes whose corresponding lattices are determined. In the table, $A_4(C)$ denotes the lattice constructed from a code C by Construction A_4, where n denotes the length and dimension of C and $A_4(C)$.

5.2 (Odd) Unimodular Lattices

- Extremal Lattices:
  Here we consider $\mathbf{Z}_4$ code constructions of the extremal unimodular lattices (see Theorem 3.3 for such lattices).

Table 2: Extremal Type II Codes and Their Lattices

n	Code C	Lattice $A_4(C)$
8	O_8	E_8
8	K_8	E_8
8	Q_8	E_8
8	K_8'	E_8
16	$C_8 \oplus C_8'$	$E_8 + E_8$
16	K_{16}	D_{16}^+
24	any extremal code	the Leech lattice
32	$QRM(2,5)$	BW_{32}
32	$C_{5,1}$	BW_{32}
32	QR_{32}	$BSBM_{32}$

Since there are self-dual codes of length $n \leq 7$ (cf. [14]), these codes determine the lattices $\mathbf{Z}^n$. In Theorem 3.3, only even unimodular lattices are E_8 and Λ_{24}. Type II codes corresponding to E_8 and Λ_{24} were found in [5]. A Type I code corresponding to O_{23} was also found in [5]. A cyclic Type I code of length 15 which determines the lattice A_{15}^+ was found in [37]. Thus the remaining lattices are D_{12}^+ and $(E_7 + E_7)^+$. However Lemma 4.1 shows that the Type I code K_{12} determines the lattice D_{12}^+. Recently all self-dual codes of length up to 15 have been classified (cf. [19]). The code [14,2]-f in [19] has minimum Euclidean weight 8, thus the corresponding lattice is a unique 14-dimensional extremal unimodular lattice.

Therefore we have the following:

Theorem 5.3 (Bonnecaze, Gaborit, Harada, Kitazume and Solé [4]) *All the extremal unimodular lattices can be constructed from self-dual codes over* $\mathbf{Z}_4$ *by Theorem 3.4.*

- Some lattices with minimum norm 2:
  All unimodular lattices with minimum norm 2 are listed in [13, Table II] for dimension $n \leq 20$. For each length (≤ 24), at least one extremal Type I code was found in [17]. The codes determine unimodular lattices with the highest minimum norm. In particular, when $n = 17$, the minimum Euclidean weight of C_{17} in [17] is 8. Thus $A_4(C_{17})$ is a unique 17-dimensional unimodular lattice with minimum norm 2 denoted by $A_{11}E_6$ in [13, Table II].
- Some lattices with minimum norm 3:
  It follows from Theorem 3.3 that there is no odd unimodular lattice with minimum norm $\mu = 3$ in dimension $n \leq 22$. There is a unique odd unimodular lattice with $\mu = 3$ in dimensions 23 and 24. These are called the shorter Leech lattice and the odd Leech

lattice, respectively. An extremal Type I cyclic code of length 23 was found in [5]. Extremal Type I codes of length 24 were constructed in [23]. These extremal Type I codes determine the above lattices with $\mu = 3$.

6 Perspectives and Open Problems

The authors hope this survey explains the context for some of the new directions being pursued by researchers in codes over $\mathbf{Z}_4$. We give a personal selection of open problems which we hope may serve as a starting and important point for further exciting discoveries.

6.1 Codes and Lattices

We described the existence of extremal Type II codes of length $n \leq 48$.

Problem 6.1 *Is there an extremal Type II code for length $n \geq 56$?*

All the n-dimensional even unimodular lattices are constructed from Type II codes over $\mathbf{Z}_4$ by Theorem 3.4 for $n \leq 24$ (see Corollary 5.2). This prompts the following problem.

Problem 6.2 *Can all the n-dimensional even unimodular lattices with $\mu \leq 4$ be constructed from Type II codes over $\mathbf{Z}_4$ by Theorem 3.4 for $n \leq 40$?*

Problem 6.3 *Determine if extremal Type II codes of length 32 described in Section 5 give new extremal even unimodular lattices.*

In [30] it was shown that (binary) Construction A is injective.

Theorem 6.4 (Kitazume, Kondo and Miyamoto [30]) *Any two inequivalent binary doubly-even self-dual codes give rise by Construction A to two inequivalent even unimodular lattices.*

Problem 6.5 *Which dimension does it holds that any two inequivalent (Type II) self-dual codes give rise by Construction A_4 to two inequivalent (even) unimodular lattices?*

As mentioned in Section 5, there are extremal Type II codes of lengths $8, 24$ and 32 which determine equivalent lattices.

6.2 Designs

Recently it was shown by computer in [25] that the codewords of some fixed Lee compositions in the lifted Golay code hold 5-designs. This cannot happen by symmetry conditions since the automorphism group of the code is $SL(2, 23)$ [11] and one of the 5-designs has parameters $(24, 10, 36)$ and its automorphism group is $PSL(2, 23)$ which is only $3-$homogeneous [29]. This creates the need of a purely combinatorial and computer-free proof of the existence of

these designs in the lifted Golay code. For codes over finite fields, the Assmus and Mattson theorem is such a method to find designs in codes (cf. [1]). This prompts the following problem.

Problem 6.6 *Is there a result for codes over* $\mathbf{Z}_4$ *analogous to the Assmus and Mattson theorem?*

We have the following trivial partial answer.

Proposition 6.7 *Let* C *be a self-dual code of type* $4^{n/2}$*, that is* $C^{(1)} = C^{(2)}$*, where* n *is the length of* C*. If the residue code* $C^{(1)}$ *is a binary extremal doubly-even self-dual code then the support of the codewords of* C *of a fixed Hamming weight such that the components are only* 0 *and* 2*, forms a* 5*-,* 3*- and* 1*-design for* $n \equiv 0$*,* 8 *and* 16 $\pmod{24}$*, respectively.*

Proof. Since $C^{(1)}$ is a binary extremal doubly-even self-dual code, by the Assmus and Mattson theorem the set of the codeword of a fixed Hamming weight forms a design. The support of the codewords of C whose components are only 0 and 2 of a fixed Hamming weight w coincide with the set of the codewords of the residue $C^{(1)}$ of weight w. □

It was shown in [5] that the support of the codewords of Hamming weight 10 in the lifted Golay code forms a 3-$(24, 10, 360)$ design using its automorphism group. By the above proposition, we can show this result without its group. Remark that the support forms a 5-$(24, 10, 36)$ design (cf. [25]).

Double circulant codes $C_{24,1}$ and $C_{24,2}$ in Table 1 have the same swe's as the lifted Golay code QR_{24}, and the residue codes $C^{(1)}$ are the Golay code. Moreover, similarly to QR_{24}, the supports of the codewords of Hamming weight 10 in $C_{24,1}$ and $C_{24,2}$ form 5-$(24, 10, 36)$ designs (cf. [22]).

Conjecture 6.8 *Suppose that* C *is an extremal Type II code of length* 24 *such that* C *has the same swe as the lifted Golay code and the residue code* $C^{(1)}$ *is the Golay code. The support of the codewords of Hamming weight* 10 *in* C *forms a* 5-$(24, 10, 36)$ *design.*

Problem 6.9 *Prove the above conjecture or find a counter-example.*

Recently Kitazume and Munemasa [31] have given a characterization of the 5-$(24, 10, 36)$ design in the lifted Golay code as follows. The stabilizer of an octad B of the Steiner system $S(5, 8, 24)$ in $PSL(2, 23)$ has 20 orbits on the set of 2-subsets of the complement of B, where an octad is a block of $S(5, 8, 24)$. It turns out that only one of the orbits on 2-subsets has the following property: if we take a representative $\{x, y\}$, then the $PSL(2, 23)$-orbit containing $B \cup \{x, y\}$ forms 5-$(24, 10, 36)$ design which is the same as the design in the lifted Golay code. Moreover they found 5-$(24, 10, \lambda)$ designs where $\lambda = 36, 72$ and $18m$ with $6 \leq m \leq 52$ from a union of $PSL(2, 23)$-orbits on 10-subsets containing an octad.

6.3 Type II Codes over $\mathbf{Z}_{2k}$

Very recently self-dual codes over $\mathbf{Z}_{2k}$ have been investigated, in particular Type II codes have been introduced by defining the Euclidean weight of a vector in $\mathbf{Z}_{2k}$ and Type II codes have been widely studied in [3].

A code of length n over a ring $\mathbf{Z}_{2k}$ is an additive subgroup of $\mathbf{Z}_{2k}^n$. We define an inner product on $\mathbf{Z}_{2k}^n$ by $x \cdot y = x_1y_1 + \cdots + x_ny_n$ where the operations take place in $\mathbf{Z}_{2k}$, and $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. The dual code of a code is defined in the usual way. A code C is *self-dual* if $C = C^{\perp}$. The Euclidean weights of the elements $0, \pm 1, \pm 2, \pm 3, \ldots, \pm(k-1), k$ of $\mathbf{Z}_{2k}$ are $0, 1, 4, 9, \ldots, (k-1)^2$, k^2, respectively. The Euclidean weight of a vector is just the rational sum of the Euclidean weights of its components. We define a *Type II* code over $\mathbf{Z}_{2k}$ as a self-dual code with all vectors having Euclidean weight a multiple of $4k$.

As an application of Construction A_4 to self-dual codes over $\mathbf{Z}_{2k}$, we have the following construction of unimodular lattices. Let ρ be a map from $\mathbf{Z}_{2k}$ to $\mathbf{Z}$ sending $0, 1, \ldots, k$ to $0, 1, \ldots, k$ and $k+1, \ldots, 2k-1$ to $1-k, \ldots, -1$, respectively.

Theorem 6.10 (Bannai, Dougherty, Harada and Oura [3]) *If C is a self-dual code of length n over $\mathbf{Z}_{2k}$, then the lattice*

$$\Lambda_{2k}(C) = \frac{1}{\sqrt{2k}}\{\rho(C) + 2k\mathbf{Z}^n\},$$

is an n-dimensional unimodular lattice, where $\rho(C) = \{(\rho(c_1), \ldots, \rho(c_n)) \mid (c_1, \ldots, c_n) \in C\}$. The minimum norm is $\min\{2k, d_E/2k\}$ where d_E is minimum Euclidean weight of C. Moreover if C is Type II then the lattice $\Lambda_{2k}(C)$ is an even unimodular lattice.

We remark when $k = 1$ this is the same as Construction A and when $k = 2$ this is the same as Construction A_4.

For every m, a Type II code over $\mathbf{Z}_{2^m}$ of length 8 were constructed by repeating the Hensel lift (cf. [8]). Moreover, for every k it was shown in [3] to exist a Type II code over $\mathbf{Z}_{2k}$ of length 8. These codes give a number of different constructions of E_8.

The most interesting dimension is 24, we have the following:

Problem 6.11 *For each k, is there a Type II code over $\mathbf{Z}_{2k}$ of length 24 with $d_E = 8k$?*

Of course, if such a code exists then the code determines the Leech lattice for $k \geq 2$. For $k = 2$, we described in this survey the existence of several inequivalent extremal Type II codes. For $k = 3$ and 4, Type II codes with $d_E = 8k$ were found in [3] and [26]. The first open case is $\mathbf{Z}_{10}$. In this case, a construction using the Chinese Remainder Theorem given in [18] might be useful.

At present, it is not known if an extremal even unimodular lattice in dimension 72 exists.

Problem 6.12 *Is there a Type II code over $\mathbf{Z}_8$ of length 72 with minimum Euclidean weight 64?*

If such a code exists then the above extremal even unimodular lattice can be constructed by Theorem 6.10. Some information about the relationship between the lattices obtained by Theorem 6.10 from the quadratic residue codes QR_{71} over $\mathbf{Z}_4$ and $\mathbf{Z}_8$ can be found in [10].

7 Acknowledgement

The second and the third authors would like to acknowledge the teachings, friendship, and support of the "Bordeaux school of Lattices" the work of which can be seen in the recent book of Martinet [33]. All the authors would like to thank Steven T. Dougherty for his reading an earlier version of this survey and helpful remarks.

References

[1] E.F. Assmus, Jr., and H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.

[2] R. Bacher and B.B. Venkov, Réseaux entiers unimodulaires sans racines en dimension 27 et 28, (to appear).

[3] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, (preprint).

[4] A. Bonnecaze, P. Gaborit, M. Harada, M. Kitazume and P. Solé, Niemeier lattices and Type II codes over $\mathbf{Z}_4$, (preprint).

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

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

[7] A.R. Calderbank, G. McGuire, P.V. Kumar and T. Helleseth, Cyclic codes over $\mathbf{Z}_4$, locator polynomials, and Newton identities, *IEEE Trans. Inform. Theory* **42** (1996), 217–226.

[8] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes and Cryptogr.* **6** (1995), 21–35.

[9] A.R. Calderbank and N.J.A. Sloane, Double circulant codes over $\mathbf{Z}_4$ and even unimodular lattices, *J. Alg. Combin.* **6** (1997), 119–131.

[10] R. Chapman and P. Solé, Universal codes and unimodular lattices, *J. de Théorie des Nombres de Bordeaux* **8** (1996), 369–376.

[11] R. Chapman, personal communication to P. Solé, 1996.

[12] J.H. Conway, A.M. Odlyzko and N.J.A. Sloane, Extremal self-dual lattices exist only in dimensions 1 to 8, 12, 14, 15, 23, and 24, *Mathematika* **25** (1978), 36–43.

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

[14] 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.

[15] J.H. Conway and N.J.A. Sloane, "Sphere Packing, Lattices and Groups (2nd ed.)," Springer-Verlag, New York, 1993.

[16] S.T. Dougherty, T.A. Gulliver and M. Harada, Type II self-dual codes over finite rings and even unimodular lattices, (submitted).

[17] S.T. Dougherty, M. Harada and P. Solé, Shadow codes over $\mathbf{Z}_4$, (submitted).

[18] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, (submitted).

[19] J. Fields, P. Gaborit, J. Leon and V. Pless, All self-dual $\mathbf{Z}_4$ of length 15 or less are known, (submitted).

[20] P. Gaborit, Mass formulas for self-dual codes over $\mathbf{Z}_4$ and $\mathbf{F}_q + u\mathbf{F}_q$ rings, *IEEE Trans. Inform. Theory* **42** (1996), 1222–1228.

[21] P. Gaborit and M. Harada, Construction of extremal Type II codes over $\mathbf{Z}_4$, (in preparation).

[22] T.A. Gulliver and M. Harada, Extremal double circulant Type II codes over $\mathbf{Z}_4$ and construction of 5-$(24, 10, 36)$ designs, (submitted).

[23] T.A. Gulliver and M. Harada, Certain self-dual codes over $\mathbf{Z}_4$ and the odd Leech lattice, *Proc. the 12-th Appl. Alg. Alg. Algorithms, and Error-Correcting Codes*, also *Lecture Notes in Computer Sciences*, (to appear).

[24] M. Harada, New extremal Type II codes over $\mathbf{Z}_4$, *Designs, Codes and Cryptogr.* (to appear).

[25] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbf{Z}_4$, (submitted).

[26] M. Harada, "Self-Dual Codes, Designs and Unimodular Lattices", Doctoral thesis, Okayama University, 1997.

[27] M. Kervaire, Unimodular lattices with a complete root system, *Ens. Math.* **40** (1994), 59–104.

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

[29] M. Kitazume, personal communication to M. Harada, 1996.

[30] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[31] M. Kitazume and A. Munemasa, New 5-designs with automorphism group $PSL(2, 23)$, (preprint).

[32] H. Koch and B.B. Venkov, Ueber ganzahlige unimodulare Gitter, *J. reine angew. Math.* **398** (1989), 144–168.

[33] J. Martinet, " Les Réseaux Parfaits des Espaces Euclidiens", Masson, Paris, 1996.

[34] H.-V. Niemeier, Definete quadratische Formen der Dimension 24 und Diskriminante 1, *J. Number Theory* **5** (1973), 142–178.

[35] V. Pless, J. Leon and J. Fields, All $\mathbf{Z}_4$ code of Type II and length 16 are known, *J. Combin. Theory Ser. A* **78** (1997), 32–50.

[36] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbf{Z}_4$, *IEEE Trans. Inform. Theory* **42** (1996), 1594–1600.

[37] V. Pless, P. Solé and Z. Qian, Cyclic self-dual $\mathbf{Z}_4$-codes, *Finite Fields and Their Appl.* **3** (1997), 48–69.

[38] H.-G. Quebbemann, Zur Klassification unimodularer Gitter mit Isometrie von Primzahlordnung, *J. reine angew. Math.* **326** (1981), 158–170.

[39] E. Witt, Eine Identität zwischen Modulformen zweiten Grades, *Abhand. Math. Semin. der Univ. Hamburg* **14** (1941), 323–337.