# Construction of new extremal unimodular lattices

Philippe Gaborit *

July 22, 2003

**Abstract**

In this paper we construct new extremal and optimal unimodular lattices in dimensions $36, 38, 42, 45, 52, 54, 60$ and $68$. We construct them in two ways: first in the case of dimensions congruent to 4 modulo 8 by construction $B_3$ followed by density doubling, generalizing the constructions of [7, p.148] and [24] and second by applying the well known construction A to self-dual codes over $GF(5)$ and to codes over the ring $Z/25Z$. In particular the lattice in dimension 60, $P_{60q}$, generalizes the construction of the lattice $P_{48q}$. We also also give the complete weight enumerator of the extended ternary quadratic residue code of length 60 and we provide a table of the best known unimodular lattices of dimensions up to 80.

## 1 Introduction

There are many links between codes and lattices (cf [7]), and especially between self-dual codes and unimodular lattices. In particular Type II codes can be related to Type II lattices and the Leech lattice can be constructed from the Golay code. The well known Construction A is a simple way to associate a lattice to a code, in particular a unimodular lattice is associated to a self-dual code. But applying construction A directly to the fields $GF(2)$ and $GF(3)$ is not interesting if one is to obtain unimodular lattices with minimum norm higher than 2 or 3. A way to obtain a lattice with a higher norm is to construct lattices by construction A and then consider a particular lattice associated to the first one through a neighboring construction. The method was first used over $GF(2)$ to construct unimodular lattices of norm 4, in particular the Leech lattice is obtained from the Golay code and other lattices of norm 4 are constructed in dimension 32 and 40 (cf [7] for references).

*LACO, Université de Limoges, 123,av. A. Thomas, 87000 Limoges, FRANCE **Email: gaborit@unilim.fr**

The same method was also applied by Leech and Sloane ([7]) over $GF(3)$ in dimensions 24 and 48 to obtain, in dimension 24, a new construction of the Leech lattice and in dimension 48, two extremal Type II lattices of norm 6 namely $P_{48q}$ and $P_{48p}$, constructed respectively from two self-dual ternary codes: the extended ternary quadratic residue code of length 48 ($XQ_{47}$) and the Pless symmetry code $PS_{48}$. Later this construction was generalized by Ozeki in [24] to construct for dimensions congruent to 0 mod 8, Type II lattices of norm 4 or 6. Ozeki constructed in particular Type II lattices of dimensions 56 and 64 associated to extremal ternary self-dual codes of lengths 56 and 64. His construction was simplified by Conway and Sloane in [7].

In this paper we generalize the previous construction over $GF(3)$ to the case of dimensions congruent to 4 mod 8 and we construct new lattices in dimensions $52, 60$ and $68$ associated to ternary self-dual codes. In particular the proof of the minimum norm 6 of the lattice $P_{60_q}$ relies on the computtaion of the complete weight enumerator ($cwe$) of $XQ_{59}$ which was previously unknown. We also propose methods to construct self-dual codes over $GF(5)$ and over the ring $Z/25Z$ that we use with Construction A to construct new extremal unimodular lattices in dimensions $36, 38, 42, 45$ and $54$. The shadow theory of [8] is used to compute, when it is possible, the theta series of these lattices.

Note that most of these lattices were previously announced in the on-line tables of [22]. In particular the results concerning ternary construction for dimensions $52, 60$ and $68$ were previously announced and explained in [22] in June 2001 and at the Workshop on Coding and Cryptography at Singapore in Sept 2001, at the same time or earlier than the results of [15].

The paper is organized as follows: Section 2 collects basic definitions and notation, Section 3 considers the construction from self-dual ternary codes, Section 4 deals with Construction A, Section 5 gives a general table of the best known unimodular lattices up to dimension 80 and the Appendix gives explicit generator matrices of some of the codes described in the paper.

# 2 Notation and Definitions

In this section we recall some basic notions on codes, lattices and the basic construction of lattices from codes. We refer to [29] and [7] for a more general context regarding self-dual codes and lattices. We deal with codes over rings and codes over fields. A code of length $n$ and dimension $k$ over a field $K$ is a subspace of $K^n$ of dimension $k$. A code $C$ over a ring $R$ is a $R$-submodule of $R^n$. In the following we will consider that the code $C$ is over a ring of the form $Z/mZ$ for $m$ an integer. A codeword is an element of a code. Let us define the (Euclidean) scalar product of two codewords $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ by $x.y = \sum_{i=1}^{n} x_i.y_i$. The dual of $C$ is defined as $C^\perp = \{y \in (Z/mZ)^n \mid x.y = 0 \text{ for all } x \in C\}$.

A code is self-dual if and only if $C = C^{\perp}$. The Hamming weight of a codeword corresponds to the number of non zero components, the Euclidean weight $w_E(a)$ of an element $a$ of $Z/mZ$ (={0, ..., m-1}) is the minimum of $\{a^2, (m-a)^2\}$, by extension the Euclidean weight of a codeword $x$ is $\sum_{i=1}^{n} w_E(x_i)$. The Euclidean minimum weight $d_E(C)$ of a code $C$ is the minimum Euclidean weight among all the non zero codewords of $C$.

The dual of a lattice $\Lambda$ is denoted by $\Lambda^*$. A lattice $\Lambda$ is integral if $\Lambda \subset \Lambda^*$ and unimodular if $\Lambda = \Lambda^*$. A unimodular lattice whose vectors have even norm is said to be even or Type II. The minimum norm of a unimodular lattice of dimension $n$ is bounded by [28]:

$$\mu \leq 2[\frac{n}{24}] + 2,$$

except for $n = 23$ where the norm is bounded by 3. A lattice of dimension $n$ with norm $2[\frac{n}{24}] + 2$ (and $n \neq 23$) is said to be extremal. A unimodular lattice with the highest possible norm is said to be optimal.

The well known Construction A is used to associate a unimodular lattice to a self-dual code over a ring $Z/mZ$:

**Definition 2.1** *Let $C$ be a self-dual code over the ring $Z/mZ$ with minimum Euclidean weight $d_E$ then:*

$$A_m(C) = \frac{1}{\sqrt{m}}\{(x_1, ..., x_n) \in Z^n \mid (x_1 \, mod \, m, ..., x_n \, mod \, m) \in C\},$$

*is a unimodular lattice with norm $min\{\frac{d_E}{m}, m\}$.*

In the case of ternary codes one can also consider Construction $B_3$ ([7]) which associates to a ternary code the lattice $B_3(C)$:

**Definition 2.2** *Let $C$ be a $[n, k, d]$ code over $GF(3)$, then $x$ in $R^n$ is an element of $\sqrt{3}.B_3(C)$ if and only if $x = (x_1, \cdots, x_n)$ is congruent modulo 3 to a codeword of $C$ and $\sum_{i=1}^{n} x_i$ is divisible by 2.*

The theta series of a lattice $\Lambda$ is

$$\theta_\Lambda(\tau) := \sum_{x \in \Lambda} q^{(x \cdot x)} \tag{1}$$

where $\tau \in \mathfrak{h}$ the upper half complex plane and $q := e^{\pi i \tau}$, satisfies an invariance property under the transformation $\tau \to -1/\tau$, when the lattice $\Lambda$ is unimodular.

Let $\Lambda$ be a unimodular lattice. The shadow $S$ of $\Lambda$ is $S := (\Lambda_0)^* \setminus \Lambda$, where $\Lambda_0$ denotes the even sublattice of $\Lambda$. If $\Lambda$ is an odd lattice, its theta series has the following expression

$$\theta_\Lambda(\tau) = \sum_{j=0}^{[n/8]} a_j \Delta_8(q)^j \theta_3(q)^{n-8j} \tag{2}$$

and the theta series of the shadow $S$ is

$$\theta_S(\tau) = \sum_{j=0}^{[n/8]} \frac{(-1)^j}{16^j} a_j \theta_4(q^2)^{8j} \theta_2(q)^{n-8j}. \tag{3}$$

where $q := e^{\pi i \tau}$, $\Delta_8(q) = q \prod_{m=1}^{\infty} (1 - q^{2m-1})^8 (1 - q^{4m})^8$, and $\theta_2$, $\theta_3$, $\theta_4$ are the usual Jacobi theta series (see [7, Chap. 4, § 4]).

In all the following the notation $(x^a, y^b)$ stands for a vector whose first $a$ coordinates are $x$ and the $b$ last coordinates are $y$.

# 3 Unimodular lattices and self-dual codes over $GF(3)$

## 3.1 Constructions

In this section we generalize the construction of [24] to lengths $n$ congruent to 4 modulo 8. Note that in the latter paper the author remarks that his method can be generalized to lengths congruent to 4 modulo 8 without any change. It appears indeed that this affirmation is partly false since some conditions concerning the complete weight enumerators of the codes and the minimum weight have to be precised.

In the case of a self-dual ternary code, since the Hamming weight of any codeword is divisible by 3 the lattice obtained by Construction $B_3(C)$ consists of the vectors: $x = \frac{1}{\sqrt{3}}(x_1, \ldots, x_n)$ of $A_3(C)$ such that $6 \mid \sum_{i=1}^n x_i$ (6 divides $\sum_{i=1}^n x_i$). Now, for $C$ a self-dual ternary code of length $n$ and $v$ a vector of $R^n$, such that $2v$ is in $B_3(C)$, we denote by $N_3(C, v)$ the lattice obtained by taking the sublattice $B_3(C)$ of index 2 of $A_3(C)$ and by doubling its density by considering the lattice $B_3(C) \cup \{v + B_3(C)\}$. The lattice $N_3(C, v)$ is a neighbour of $A_3(C)$. This construction is described in [7] for the case of lengths a multiple of 12.

We now obtain the following construction theorem, where the maximal codewords are the words with maximal Hamming weight:

**Theorem 3.1** *Let $C$ be a self-dual ternary code of length $n$ such that $C$ contains: a codeword of the form $(1^n)$ if $n = 0$ mod 3, a codeword of the form $(1^{n-1}, 0)$ if $n = 2$ mod 3, or a codeword of the form $(1^{n-2}, 0^2)$ if $n = 1$ mod 3. The following result holds:*
*1) if $C$ is $[28, 14, 9]$ code then the lattice $N_3(C, v)$ with $v = ((\frac{1}{2})^{27}, \frac{3}{2})$ is a unimodular lattice with minimum norm 3,*
*2) if $C$ is $[36, 18, d]$ code with $d \geq 9$ and such that the maximal codewords of $C$ have only an even number of '1' then the lattice $N_3(C, v)$ for $v = ((\frac{1}{2})^{35}, -\frac{5}{2})$ is a unimodular lattice with minimum norm 4,*
*3) if $C$ is $[44, 22, d]$ code with $d \geq 9$ then the lattice $N_3(C, v)$ for $v = ((\frac{1}{2})^{42}, \frac{3}{2}, \frac{3}{2})$ is a unimodular lattice with minimum norm 4,*

*4) if $C$ is $[52,26,15]$ code then the lattice $N_3(C,v)$ for $v=((\frac{1}{2})^{51},\frac{3}{2})$ is a unimodular lattice with minimum norm 5,*
*5) if $C$ is $[60,30,d]$ code with $d\geq 15$ and such that the maximal codewords of $C$ have only an even number of $'1'$ then the lattice $N_3(C,v)$ for $v=((\frac{1}{2})^{59},-\frac{5}{2})$ is a unimodular lattice with minimum norm 6,*
*6) if $C$ is $[68,34,d]$ code with $d\geq 15$ then the lattice $N_3(C,v)$ for $v=((\frac{1}{2})^{66},\frac{3}{2},\frac{3}{2})$ is a unimodular lattice with minimum norm 6.*

**Proof.**

The proofs are similar for $k$ and $k+24$ for $k$ in {28,36,44}, therefore we only prove the cases $n=44,52$ and 60.

For $n=44$ let us consider the vectors $w=\frac{1}{\sqrt{3}}(1^{42},3^2)$, $v=\frac{w}{2}$. For $x=\frac{1}{\sqrt{3}}(x_1,\ldots,x_{44})$ a vector of $A_3(C)$ we want to prove that $L:=N_3(C,v)$ is unimodular with minimum norm 4. First we prove that $L$ is integral. Since $x\in B_3(C)$, by divisibility one gets:

$$6\mid\sum_{i=1}^{44}x_i \qquad (4)$$

and since $x$ and $w$ are in $B_3(C)$, which is integral, then $x.w\in Z$ and

$$3\ \mid\ (3(x_{43}+x_{44})+\sum_{i=1}^{42}x_i) \qquad (5).$$

From (5) one deduces that $3\mid\sum_{i=1}^{42}x_i$ and therefore by (4), $3\mid(x_{43}+x_{44})$, which implies that $v.x\in Z$, and therefore since $2v\in B_3(C)$ this shows that $N_3(C,v)$ is unimodular. Moreover two vectors of $B_3(C)$ are distant from at least $\frac{12}{3}$ since $C$ has minimum distance 9 or more, and since $L$ is unimodular the distance between two vectors is an integer. Now since the coordinates of $\sqrt{3}B_3(C)$ are integers and since the coordinates of $\sqrt{3}w$ are half integers, $d$ is greater than $\frac{44}{4\times 3}$ and hence is 4.

For $n=52$, we follow the same procedure with $w=\frac{1}{\sqrt{3}}(1^{51},3)$ and $v=\frac{w}{2}$. For $x$ any vector of $B_3(C)$ we show that $v.x\in Z$. The minimum norm is an integer greater than $\frac{52}{4\times 3}$ and therefore is 5.

For $n=60$ one takes $v=\frac{1}{\sqrt{3}}(1^{59},-\frac{5}{2})$, and the proof follows [7, 149] for dimension 48, the minimum norm is guaranteed by the even number of $'1'$ in the maximal weight codewords. $\square$

Note that two $[60,30,18]$ self-dual ternary codes are known, namely $PS_{60}$ and $XQ_{59}$. The complete weight enumerator of $PS_{60}$ has been computed in [20] but does not satisfy the condition on the even number of '1' in its extremal words. In the next subsection we compute the complete weight enumerator of $XQ_{59}$ which satisfies it.

## 3.2 Complete weight enumerator of self-dual codes over $GF(3)$

We saw in the preceding section that when the dimension of the code is a multiple of 12 (and therefore may contain the all-ones vector $\mathbf{1}$), it was of interest to know the complete weight enumerator of the code. In [20] the complete weight enumerators of the codes $XQ_{23}, PS_{24}, PS_{36}, XQ_{47}, PS_{48}$ and $PS_{60}$ are computed. These results show in particular that $PS_{36}$ and $PS_{60}$ contain codewords of the form $0^a 1^b$ with $a$ and $b$ odd. We prove next the unicity of the cwe of any $[48, 24, 15]$ self-dual ternary code with the all-ones vector inside and we give the cwe of $XQ_{59}$ which was not considered in [20].

We first recall a theorem in [20] which describes the complete weight enumerator of self-dual codes over $GF(3)$ which contain the all-ones vector $\mathbf{1}$:

**Theorem 3.2** *Let $C$ be a ternary self-dual code which contains the all-ones vector $\mathbf{1}$. Let $W_C(x, y, z)$ be the complete weight enumerator of $C$. Then:*

$$W_C(x, y, z) \in \mathcal{C}[\alpha_{12}, \beta_6^2, \delta_{36}] \oplus \beta_6\gamma_{18}\mathcal{C}[\alpha_{12}, \beta_6^2, \delta_{36}],$$

*where $\alpha_{12} = a(a^3 + 8p^3), \beta_6^2 = a^2 - 12b, \gamma_{18} = a^6 - 20a^3p^3 - 8p^6, \delta_{36} = p^3(a^3 - p^3)^3$, and $a = x^3 + y^3 + z^3, p = 3xyz, b = x^3y^3 + x^3z^3 + y^3z^3$.*

In [24] it is claimed that for dimension 48, all the $[48, 24, 15]$ self-dual ternary codes lead to Type II lattice of dimension 48 and norm 6. Although this claim is incomplete since one also needs the condition on the maximal codewords, it turns out that it is true *a posteriori* by the following proposition which fixes the complete weight enumerator of any $[48, 24, 15]$ self-dual ternary code:

**Proposition 3.3** *All extremal* $[48, 24, 15]$ *ternary self-dual codes, with the all-ones vector inside, have the same complete weight enumerator.*

**Proof.** In that case the number of independent polynomials from Theorem 3.2 for the cwe of such a code is 10. Now the condition of minimum weight 15 leads to 9 conditions. It is known from the weight enumerator that the number of codewords of maximal weight (*ie* 48) is 94. Therefore one may check for all the possibilities between 0 and 94 for the number $N$ of maximal codewords in the code with 24 $'1'$ and 24 $'-1'$. The computation shows that the only valid possibility for a weight enumerator is obtained for $N = 94$, the others leading to weight enumerators with fractional or negative terms. This gives a $10^{th}$ condition and fixes the complete enumerator of any extremal self-dual ternary $[48, 24, 15]$ code. □

Now if one considers the problem of finding the cwe of $XQ_{59}$ (with the vector $\mathbf{1}$ inside) one has to find sufficiently many coefficients of the cwe to be able to solve the system of equations (given by the preceding theorem) which generates the cwe of the code. The minimum weight 18 gives several coefficients but it is not enough and some more have to be found. We follow [20] in searching for the codewords of weight 60.

It is known from the weight enumerator of extremal ternary self-dual $[60, 30, 18]$ codes that the number of codewords of weight 60 is 41184, it is also known that the automorphism group of $XQ_{59}$ is $PSL_2(59)$. Using a simple program in Magma it is possible to find some codewords of weight 60 and then apply $PSL_2(59)$ to these codewords to construct their orbits under this group. It appears that there are exactly 2 orbits: one of order 120 generated by **1** and another of order 41064, moreover it turns out that all the codewords we find have an even number of $'1'$ and $'-1'$. Computing the exact number of codewords for each possible distribution gives sufficiently many coefficients to compute the cwe of $XQ_{59}$ of Table 1.

## 3.3 Applications

We now apply Theorem 3.1 to construct new lattices.

- dimension 28:

many $[28, 14, 9]$ self-dual codes over $GF(3)$ ([29]) are known and they all give rise to an optimal unimodular lattice of norm 3.

- dimension 36:

as far as we know, no self-dual $[36, 18, d]$ code with $d \geq 9$ and even number of '1' in its maximal words is known, such a code would lead to an extremal unimodular lattice of norm 4.

- dimension 44:

in this case also many $[44, 22, 12]$ self-dual codes are known ([29]) which all lead to extremal unimodular lattices of norm 4.

- dimension 52:

recently the first extremal $[52, 26, 15]$ self-dual code over $GF(3)$ was found by Gaborit and Otmani in [?]. This code leads to an optimal unimodular lattice of norm 5. Note that this lattice is optimal since the case of minimum norm 6 is ruled out by shadow arguments (cf Section 5). The theta series of the lattice and its shadow are:

$$\theta_\Lambda = 1 + 130624q^5 + \dots \qquad \theta_S = 104q^3 + \dots$$

- dimension 60:

as previously said there are two known self-dual $[60, 30, 18]$ codes over $GF(3)$. We prove in the preceding section that the complete weight enumerator of $XQ_{59}$ has the good property on its words of maximal weight and therefore leads to an extremal unimodular lattice of norm 6: $P_{60q}$. And since the automorphismgroup of $XQ_{59}$ is $PSL_2(59)$, the automorphism group of $P_{60q}$ contains $SL_2(59)$. The theta series of the lattice and its shadow are as follows:

$$\theta_\Lambda = 1 + 3908160q^6 + \dots \qquad \theta_S = 120q^3 + \dots$$

| $A_{ijk}/59$ | i | j | k | N. of terms |
|---|---|---|---|---|
| $\frac{1}{59}$ | 60 | 0 | 0 | 3 |
| 0 | 42 | 18 | 0 | 6 |
| 580 | 42 | 15 | 3 | 6 |
| 14210 | 42 | 12 | 6 | 6 |
| 36540 | 42 | 9 | 9 | 3 |
| 0 | 39 | 21 | 0 | 6 |
| 8120 | 39 | 18 | 3 | 6 |
| 316680 | 39 | 15 | 6 | 6 |
| 1721440 | 39 | 12 | 9 | 6 |
| 145 | 36 | 24 | 0 | 6 |
| 52780 | 36 | 21 | 3 | 6 |
| 3601220 | 36 | 18 | 6 | 6 |
| 34972260 | 36 | 15 | 9 | 6 |
| 72310630 | 36 | 12 | 12 | 3 |
| 0 | 33 | 27 | 0 | 6 |
| 190820 | 33 | 24 | 3 | 6 |
| 19305300 | 33 | 21 | 6 | 6 |
| 305502820 | 33 | 18 | 9 | 6 |
| 1133255620 | 33 | 15 | 12 | 6 |
| 408 | 30 | 30 | 0 | 3 |
| 353220 | 30 | 27 | 3 | 6 |
| 52030930 | 30 | 24 | 6 | 6 |
| 1253638100 | 30 | 21 | 9 | 6 |
| 7579015150 | 30 | 18 | 12 | 6 |
| 13591942720 | 30 | 15 | 15 | 3 |
| 72243640 | 27 | 27 | 6 | 3 |
| 2514544760 | 27 | 24 | 9 | 6 |
| 23134484940 | 27 | 21 | 12 | 6 |
| 67623713220 | 27 | 18 | 15 | 6 |
| 33433941660 | 24 | 24 | 12 | 3 |
| 148722919080 | 24 | 21 | 15 | 6 |
| 242406463530 | 24 | 18 | 18 | 3 |
| 368890513080 | 21 | 21 | 18 | 3 |

Table 1: Complete weight enumerator of the $[60, 30, 18]$ extended quadratic residue code $XQ_{59}$

**remark :** the condition of minimum distance 18 is not a necessity and could be reduced to 15 but without additional information on the number of codewords of given weight or without the automorphism group of the code, it is difficult to compute the cwe to check for $0^a1^b$ vectors with $a$ and $b$ odd.

• dimension 68: a $[68, 34, 15]$ ternary self-dual code can be easily constructed using the method described in [12] or by subtraction of a $[4, 2, 3]$ self-dual code from the $[72, 36, 18]$ extended quadratic residue code of length 72, $XQ_{72}$. This code leads to an extremal lattice of norm 6.

# 4 Some new unimodular lattices obtained by Construction A

In this section we present two methods to construct self-dual codes over rings which lead to unimodular lattices using Construction A.

## 4.1 Construction with quadratic double circulant codes

In all the following $q$ is a power of an odd prime number. We now introduce some definitions. Let $R$ be a commutative ring containing 1 and let $r$,$s$ and $t$ be elements of $R$. Following the notation of [26], we let $a$ be a one-to-one mapping of the integers $0, 1, \cdots, q-1 \cup \infty$ over the elements of $GF(q) \cup \infty$ with $a(0) = 0, a(1) = 1$ and $a(\infty) = \infty$. Then the inverse mapping $a^{-1}$ is a mapping from $GF(q) \cup \infty$ onto the integers $0, 1, \cdots, q-1 \cup \infty$. In the case where $q$ is a prime, we let $a$ be the identity. We now set the matrix $\mathcal{Q}_q(r, s, t)$ to be the $q \times q$ matrix on $R$ labeled on its rows and its columns by elements of $GF(q)$: $a_0 = 0, a_1 = 1, a_2 = a(2), \cdots, a_{q-1} = a(q-1)$, and with components $q_{ij}$. The entries $q_{ij}$ are defined in terms of quadratic residues and by the function $\chi$ (which is not necessarily a character) defined on $GF(q)$ by $\chi(a_0) = r$, $\chi(a_i) = s$ if $a_i$ is a quadratic residue in $GF(q)$ and otherwise $\chi(a_i) = t$. Then we let $q_{ij}$ equal $\chi(a_j - a_i)$. In the important case where $q$ is a prime we let $a_0 = 0, a_1 = 1, \cdots, a_{q-1} = q-1$, which leads to a circulant $\mathcal{Q}_q(r, s, t)$ matrix. We define $I$ the $q \times q$ identity matrix.

We define a quadratic double circulant code to be a $[2q, q]$ or $[2q+2, q+1]$ code over $R$ with one of the two possibly double circulant form for its generator matrix:

$$\mathcal{P}(r, s, t) = \left( \begin{array}{c|c} \quad I \quad & \mathcal{Q}(r, s, t) \end{array} \right) \qquad (6)$$

$$\mathcal{B}(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0\cdots 0 & \alpha & \beta\cdots\beta \\ \hline 0 & & \gamma & \\ 0 & & \gamma & \\ \vdots & I & \vdots & \mathcal{Q}(r,s,t) \\ \vdots & & \vdots & \\ & & & \\ 0 & & \gamma & \end{array}\right) \tag{7}$$

These two forms are also called respectively *pure* and *bordered* quadratic double circulant forms. Unless otherwise specified we always consider $\beta = \gamma = 1$ and $\alpha = r$.

This method was used by Calderbank and Sloane in [5] with $R = Z/4Z$ for $q = 19$ and construction $B(1,2,3)$ with $\alpha = 2, \gamma = 1, \beta = 3$, to obtain an even unimodular lattice of dimension 40 and norm 4. But this can also be applied in the case of $GF(5)$ with construction $\mathcal{B}_{19}(0,1,4)$ with $\alpha = 0, \gamma = \beta = 1$ or in the case of $GF(7)$ with construction $\mathcal{B}_{19}(0,5,2)$ with $\alpha = 0, \gamma = \beta = 5$. In both latter cases, one obtains an odd unimodular lattice of norm 4 and kissing number 39600. In the case of $R = GF(5)$ and $n = 19$ the construction $\mathcal{P}_{19}(2,1,3)$ leads to the first extremal unimodular lattice of dimension 38 and norm 4 with theta series:

$$\theta_\Lambda = 1 + 29260q^4 + \ldots \qquad \theta_S = 6080q^{7/2} + \ldots$$

Note that construction $\mathcal{P}_{29}(2,1,3)$ over $GF(5)$ leads to a lattice for which we could not compute the norm with Magma but whose minimum norm of the LLL-reduced basis has norm 5. If the norm was 5 it would be the unimodular lattice with the highest known norm for that dimension.

## 4.2 Experimental constructions of self-dual codes

The preceding method permits to construct the first extremal unimodular lattice of dimension 38. One of the advantage of this method is that the codes built with constructions $\mathcal{P}$ or $\mathcal{B}$ have special permutations in their automorphism groups ([10]), which therefore are also in the automorphism group of the associated lattice. Unfortunately this construction only works for some values of $q$ depending on the ring or the field of the code.

Now if one considers the problem of constructing lattice through construction A and self-dual codes for any dimension and any ring, it is of interest to use the method of [12] that we now recall to construct self-dual codes over rings.

Let $R$ be a ring. Let $C$ be a self-dual code over $R$ of length $n$. Let $G$ be a generator matrix of $C$. Now consider a $n \times n$ square matrices $M_r$ satisfying for $\lambda_r$ invertible in $R$: $M_r \cdot M_r^t = \lambda_r I_n$. For $\Pi_1, \ldots, \Pi_r$ permutations of the symmetric group $S_n$ ($r \geq 1$), consider the code $C_r$ with generator matrix $G_r$:

$$G_r = GM_1\Pi_1 \cdots M_r\Pi_r.$$

The following lemma [11] guarantees the preservation of the self-duality of the code:

**Lemma 4.1** *Let $G$ be a generator matrix of a self-dual code of length $n$ over a ring $R$, let $\lambda$ be an element of $R$ and let $M$ be a $n \times n$ matrix over $R$ satisfying $M.M^t = \lambda I$. Then the code with generator matrix $GM$ is self-dual.*

In fact for purpose of application it is simpler to take all matrices $M_i$ to be equal to the same simple matrix $M$ as follows. Let $B$ be a square $b \times b$ matrix satisfying:

$$B \cdot B^T = \lambda I_b,$$

and let $\beta$ be in $R$ such that $\beta^2 = \lambda$. We consider the block matrix $M$ consisting of $k_1$ times the matrix $B$ and $k_2$ times $\beta$ on the diagonal, with $bk_1 + k_2 = n$.

$$M = \begin{pmatrix} B & & & \\ & \ddots & & \\ & & B & \\ 0 & & & \beta I_{k_2} \end{pmatrix}.$$

Now, self-dual codes over fields have even lengths and therefore cannot be used to construct unimodular lattices of odd dimensions, but this can be done if one considers self-dual codes over rings of the form $Z/p^2Z$. In the next subsections we apply the preceding method to construct self-dual codes over $GF(5)$ and over the ring $Z/25Z$.

#### 4.2.1 Experimental constructions of self-dual codes over $GF(5)$

We use the previous construction with $B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ and $G = \begin{pmatrix} 1 & 2 & & & \\ & & 1 & 2 & \\ & & & & \ddots \end{pmatrix}$.

Then using Magma it is possible to check for the minimum norm of the lattice. We found matrices of lengths $36, 42, 54$ which lead to unimodular lattices of respective minimum norms $4, 4, 5$. We give in the appendix the generator matrices of the corresponding codes. Note that a computation with Magma showed that the lattice of dimension 36 had an automorphism group of order 544 different from the lattice constructed by G. Nebe in [22]. The theta series for the lattices are as follows:

For $n = 36$ : $\quad \theta_\Lambda = 1 + 42840q^4 + \dots \quad \theta_S = 960q^3 + \dots$

For $n = 42$ : $\quad \theta_\Lambda = 1 + 11844q^4 + \dots \quad \theta_S = 265216q^{9/2} + \dots$

For $n = 54$ : $\quad \theta_\Lambda = 1 + 95472q^5 + \dots \quad \theta_S = 2315520q^{11/2} + \dots$

Note that this method can also be used easily to construct extremal lattices of dimensions $40, 44$ and $46$.

### 4.2.2 Experimental constructions of self-dual codes over $Z/25Z$

In this case we take for generator matrix $G$ of length $n$ the direct sum of $[2,1,2]$ codes with generator matrix $(12,9)$ to which we add the trivial self-dual code of length one generated by $(5)$. We let:

$$B = \begin{pmatrix} 8 & 9 & 9 \\ 9 & 8 & 9 \\ 9 & 9 & 8 \end{pmatrix}.$$

This construction permits to construct a code over $Z/25Z$ of dimension 45 with minimum Euclidean weight 100 and therefore the first extremal lattice of dimension 45 and norm 4. It has theta series:

$$\theta_\Lambda = 1 + 5610q^4 + \ldots \quad \theta_S = 150q^{13/4} + \ldots$$

The generator matrix is given in the appendix. We also obtained many lattices of dimension 47 and norm 4 that we do not give here. Note that we also tried to construct lattices with codes over the rings $Z/4Z$ and $Z/9Z$ but that it seems that the best results were obtained through $Z/25Z$.

# 5 Tables for optimal and extremal unimodular lattices

In this section we give in table 2 and table 3 a list of the best known unimodular lattices (Type I and Type II) up to dimension 80. In the two following tables: $n, \mu$ and $Q$ respectively stand for the dimension, the minimum norm and the number of known lattices. A $'N'$ in the table means that nothing is known for the given parameters. We tried to give the names and associated references of the considered lattices.

More precise references for lattices of dimension 26 or less, can be found in [7]. These tables are based on the on-line table of unimodular lattices of the catalogue of lattices of G. Nebe and N.J.A. Sloane ([22]). Note that the on-line catalogue also provides most of the generator matrices of the lattices considered in these tables.

The upper bounds on the norm of the lattices for dimensions greater than 32 are from the Rains-Sloane bound ([28]), except improvments for $n = 33$ ([9]), $n = 34, 35$ ([3]) and $n = 49, ..., 55, 57, 72, ..., 75, 77, 79$ for which the result is obtained through computation of the theta series of the shadow (see [8]) of potential lattices with higher norm, which contain in these cases, non integer or negative coefficients.

It is easy to construct unimodular lattices of norm 3 for dimensions $29, 30, 31, 33, 34, 35, 37$ and 41 with methods developped in Section 4. Note that for dimensions greater than 40 it is difficult to check the equivalence of two lattices.

For dimension 40 many even extremal unimodular have been constructed, in particular through codes over $Z/4Z$: see preface of [7] for more references.

| $n$ | $\mu$ | Q | Lattices, Ref. |
|---|---|---|---|
| 1 | 1 | 1 | $Z$ |
| 2 | 1 | 1 | $Z^2$ |
| 3 | 1 | 1 | $Z^3$ |
| 4 | 1 | 1 | $Z^4$ |
| 5 | 1 | 1 | $Z^5$ |
| 6 | 1 | 1 | $Z^6$ |
| 7 | 1 | 1 | $Z^7$ |
| 8 | 1 | 1 | $Z^8$ |
| 9 | 1 | 2 | $E_8 + Z, Z^9$ |
| 10 | 1 | 2 | $E_8 + Z^2, Z^{10}$ |
| 11 | 1 | 2 | $E_8 + Z^3, Z^{11}$ |
| 12 | 2 | 1 | $D_{12}^+$ |
| 13 | 1 | 3 | [7] |
| 14 | 2 | 1 | $E_7^{2+}$ |
| 15 | 2 | 1 | $A_{15}^+$ |
| 16 | 2 | 1 | $D_8^2$ |
| 17 | 2 | 1 | $A_{11}E_6$ |
| 18 | 2 | 4 | [7] |
| 19 | 2 | 3 | [7] |
| 20 | 2 | 12 | [7] |
| 21 | 2 | 12 | [7] |
| 22 | 2 | 28 | [7] |
| 23 | 3 | 1 | $O_{23}$ |
| 24 | 3 | 1 | $O_{24}$ ([4]) |
| 25 | 2 | 368 | [4] |
| 26 | 3 | 1 | $S_{26}$ ([4]) |
| 27 | 3 | 3 | $T_{27}, BV_{27,1}, BV_{27,2}$ ([6],[2]) |
| 28 | 3 | 38 | [2] |
| 29 | 3 | $\geq 8900$ | [17], [9],[23] |
| 30 | 3 | $\geq 82.10^6$ | [17], [9],[23] |
| 31 | 3 | $\geq 8.10^{11}$ | [17], [9],[23] |
| 32 | 4 | 5 | [9] |
| 33 | 3 | $\geq 8.10^{20}$ | [9], [23] |
| 34 | 3 | $\geq 1$ | [22], [23] |
| 35 | 3 | $\geq 1$ | [22], [23] |
| 36 | 4 | $\geq 2$ | $N_{36}, G_{36}$ ([22],§4) |
| 37 | 3-4 | N | |
| 38 | 4 | $\geq 1$ | $G_{38}$ (§4) |
| 39 | 4 | $\geq 1$ | $GH_{39}$ ([13]) |
| 40 | 4 | $\geq 1$ | [22],§4 |
| 41 | 3-4 | N | |
| 42 | 4 | $\geq 1$ | $BN_{42}, G_{42}$ ([22], §4) |
| 43 | 4 | $\geq 1$ | $GO_{43}$ ([11]) |
| 44 | 4 | $\geq 1$ | $HKO_{44}$ ([15],§3,[14]) |
| 45 | 4 | $\geq 1$ | $G_{45}$ (§4) |
| 46 | 4 | $\geq 1$ | $H_{46}$ ([14]) |
| 47 | 4 | $\geq 1$ | $H_{47}$ ([14]) |
| 48 | -5 | N | |
| 49 | -5 | N | |
| 50 | -5 | N | |
| 51 | -5 | N | |
| 52 | 5 | $\geq 1$ | $G_{52}$ (§3) |
| 53 | -5 | N | |
| 54 | 5 | $\geq 1$ | $G_{54}$ (§4) |
| 55 | -5 | N | |
| 56 | -6 | N | |
| 57 | -5 | N | |
| 58 | -6 | N | |
| 59 | -6 | N | |
| 60 | 6 | $\geq 1$ | $P_{60q}, HKO_{60}$ (§3,[15]) |
| 61 | -6 | N | |
| 62 | -6 | N | |
| 63 | -6 | N | |
| 64 | -6 | N | |
| 65 | -6 | N | |
| 66 | -6 | N | |
| 67 | -6 | N | |
| 68 | 6 | $\geq 1$ | $HKO_{68}, G_{68}$ ([15],§3) |
| 69 | -6 | N | |
| 70 | -6 | N | |
| 71 | -6 | N | |
| 72 | -7 | N | |
| 73 | -7 | N | |
| 74 | -7 | N | |
| 75 | -7 | N | |
| 76 | -8 | N | |
| 77 | -7 | N | |
| 78 | -8 | N | |
| 79 | -7 | N | |
| 80 | -8 | N | |

Table 2: Optimal Type I unimodular lattices of dimensions $\leq 80$

| $n$ | $\mu$ | Q | Lattices, Ref |
|---|---|---|---|
| 8 | 2 | 1 | $E_8$ |
| 16 | 2 | 2 | $E_8^2, D_{16}$ |
| 24 | 4 | 1 | $L_{24}$ |
| 32 | 4 | $\geq 10^7$ | [17] (see also [18],[16]) |
| 40 | 4 | $\geq 1$ | $M_{40}, O_{40}, CS_{40}$ ([19],[25],[5]), see also ([7],[24]) |
| 48 | 6 | $\geq 3$ | $P_{48q}, P_{48p}, P_{48n}$ ([7],[21]) |
| 56 | 6 | $\geq 1$ | $L_{56,2(M)}, L_{56,2(\tilde{M})}$ ([21]) see also [24] |
| 64 | 6 | $\geq 1$ | $Q_{64}, N_{64}$ ([27],[21]) see also [24] |
| 72 | 6-8 | N | |
| 80 | 8 | $\geq 2$ | $L_{80}, M_{80}$ ([1]) |

Table 3: Extremal Type II Unimodular lattices of dimensions $\leq 80$

# References


[1] C. Bachoc and G. Nebe, Extremal lattices of minimum 8 related to the Mathieu group $M_{22}$, *J. Reine Angew. Math* **494**, (1998), pp. 155-171.

[2] R. Bacher and B. Venkov, Réseaux entiers unimodulaires sans racine en dimension 27 et 28, *L'Enseignement Mathématique*, Monographie **37** (edited by J. Martinet) (2001), pp. 212-267.

[3] C. Bachoc , G. Nebe and B.B. Venkov, Odd unimodular lattices of minimum 4, *Acta Arithm.* **101** (2002), pp. 151-158.

[4] R. E. Borcherds, The Leech and other lattices, Ph.D. Dissertation, University of Cambridge, 1984.

[5] A. R. Calderbank and N. J. A. Sloane, Double Circulant Codes over Z4 and Even Unimodular Lattices , J. Algebraic Combinatorics, 6 (1997), pp. 119–131.

[6] J. H. Conway, R.T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, ATLAS of finite groups, *Oxford Univ. Press*, (1985).

[7] J.H. Conway and N.J.A. Sloane," Sphere Packing Lattices and Groups ", third Edition, Springer-Verlag, NY, 1988.

[8] J. H. Conway and N. J. A. Sloane, A New Upper Bound for the Minimum of an Integral Lattice of Determinant One, *Bull. Amer. Math. Soc.*, 23 (1990), pp. 383–387.

[9] J. H. Conway and N. J. A. Sloane, A note on unimodular lattices, *J. Number Theory*, **72** (1998), pp. 357-362.

[10] P. Gaborit, Quadratic Double Circulant Codes over Fields, *J. Comb. Ser. A*, (2002), pp. 85–107.

[11] P. Gaborit and A. Otmani, Experimental constructions of codes over rings and construction of an optimal unimodular lattice in dimension 43, *Proceedings of the eight Algebraic and Combinatorial Coding Theory (ACCT VIII)*, Tsarkoe Selo, Russia, (2002), pp. 128-131.

[12] P. Gaborit and A. Otmani, Experimental construction of self-dual codes, to appear in *Finite Fields and Appl.*

[13] A. Gulliver and M. Harada, An optimal unimodular lattice in dimension 39, *J. Combin. Theory Ser. A*, **88** (1999), pp 158-161.

[14] M. Harada, Extremal odd unimodular lattices in dimensions $44, 46, 47$, *Hokkaido Math. J.*, **32** (2003), pp. 153-159.

[15] M. Harada, M. Kitazume and M. Ozeki, Ternary Code Construction of Unimodular Lattices and Self-Dual Codes over Z6, *J. Alg. Comb* **16** (2002), pp. 209-223.

[16] M. Kervaire, Unimodular lattices with a complete root system, *L'Enseignement Mathématique*, **40**, (1994),pp. 59-140.

[17] O. D. King, A mass formula for unimodular lattices with no roots, Math. Comp., **72**, (2003), no 242, pp. 839-863.

[18] H. Koch and B. B. Venkov, Uber ganzzaahlige unimodulare euklidische Gitter, *J. Reine Angew. Math* **398**, (1989), pp. 144-168.

[19] J. McKay, A setting for the Leech lattice, in *Finite Group '72*, North Holland-Holland, Amsterdam, (1973), pp. 117-118.

[20] C. L. Mallows, V. Pless and N. J. A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.*, **31** (4) (1976), pp. 649–666.

[21] G. Nebe , Some cyclo-quaternionic lattices, *J. Algebra*, **199**, (1998), pp. 472-498.

[22] G. Nebe and N. J. A. Sloane, *A catalogue of lattices* http://www.research.att.com/∼njas/lattices

[23] G. Nebe and B. B. Venkov, Unimodular lattices with long shadows, *J. Number Theory*, **99** (2003), no 2, pp. 307-317.

[24] M. Ozeki, Ternary code construction of even unimodular lattices, Théorie des nombres (Quebec, PQ, 1987), 772–784, de Gruyter, Berlin, 1989.

[25] M. Ozeki, Examples of even unimodular extremal lattices of rank 40 and their Siegel theta series of degree 2, *J. Number Theory* **28** (1988), pp. 119-131.

[26] V. Pless, New Symmetry Codes on GF(3), *J. Combin. Theory Ser. A* **A12** (1972), pp 119-142.

[27] H.-G. Quebbemann, A construction of integral lattices, *Math.* **31**, (1984), pp. 137-140.

[28] Rains, E. M. and Sloane, N. J. A. The shadow theory of modular and unimodular lattices, *J. Number Theory* **73** (1998) n∘ 2, 359-389.

[29] E. M. Rains and N. J. A. Sloane, "Self-dual codes", in Handbook of Coding Theory, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 177–294.

## APPENDIX

In the following we give generator matrices of some of the codes mentionned earlier. The generator matrices are given in the form $(IA)$ (except for $n = 45$), but to save space we only give the matrices $A$ as a sequence of the rows of $A$ separated by ';'.

•$n = 36$:

200420024310042000; 203224402041101320; 020004200243100420; 120242201400432013;
100410004432402004; 211220202231214410; 213223002030420340; 320242233212320144;
220002204330341203; 433341343133211021; 421143321020000002; 442324023320202340;
144323134233003410; 240343214043244023; 310023212032343034; 021001243002100030;
133114122231403200; 010331141222314032;

•$n = 42$:

000021000243001240002; 300442224204240201340; 400221322104000110320; 030020422430043142010;
040010213340043121104; 003034204031304241423; 304442321332140132001; 100142230012241014040;
230012204014131200030; 010022422043123100142; 023042122421143242004; 401242331010002024423;
302242140423401133210; 140444311332033042320; 030231421211233321330; 014012443232323400424;
003044314143114213212; 301300343200011000340; 030124003120001300000; 003001240031200013000;
000300012400312000130;

•$n = 45$: in that case we list hereafter a $23 \times 23$ matrix $A$ to which one adds on the left a $22 \times 22$ identity matrix plus a last row of zeros.

22,0,10,13,6,5,19,2,14,19,0,10,24,16,20,1,8,13,24,13,16,20,14;
4,0,15,6,13,4,3,22,5,23,9,2,0,22,10,20,19,23,6,22,20,6,10;
13,1,10,16,9,4,8,7,3,5,4,12,6,6,16,24,16,5,17,9,20,5,8;
2,0,22,22,7,3,15,8,24,16,6,13,21,19,2,17,0,14,23,11,18,3,13;
20,1,2,18,15,1,24,15,7,17,3,15,11,1,1,20,3,22,21,24,9,14,6;
16,3,12,10,18,24,14,15,2,7,0,4,23,8,17,10,5,1,21,15,1,0,0;
11,1,21,1,14,18,16,3,23,12,24,3,20,17,24,13,21,8,18,12,9,15,23;
9,0,22,3,21,4,15,2,8,12,15,4,24,0,11,20,6,12,2,9,24,9,11;
19,2,11,4,2,17,3,6,22,14,10,18,22,15,19,15,14,10,6,20,23,20,7;
14,2,13,15,10,8,10,10,3,13,1,15,17,16,9,10,6,11,14,9,3,23,8;
0,0,9,8,22,22,8,24,14,14,2,17,11,24,4,9,15,3,16,23,10,8,22;
2,3,20,23,15,22,0,4,0,19,18,23,7,12,17,0,22,20,13,8,12,12,16;
0,4,9,4,8,23,11,17,9,6,1,5,21,9,16,11,20,6,2,24,10,0,0;
14,2,0,21,17,22,5,24,1,8,4,24,6,7,15,9,5,21,14,15,13,7,9;
6,0,12,23,6,0,24,0,22,12,2,16,4,16,14,23,11,0,7,18,9,23,8;
1,0,24,2,7,9,24,12,10,21,7,18,22,17,24,7,22,18,8,13,18,4,0;
10,0,2,11,1,10,9,21,18,13,5,21,22,7,21,7,7,2,6,23,24,16,12;

19,2,15,13,23,1,22,10,12,5,21,15,2,23,10,16,20,3,11,8,1,11,6;
9,4,18,23,22,23,22,4,9,13,21,5,1,2,9,14,7,3,9,18,24,15,7;
5,1,24,14,14,4,13,4,22,9,4,6,18,3,0,11,13,15,15,8,5,2,14;
16,1,21,0,13,1,9,24,17,2,12,4,1,20,15,4,12,5,13,5,15,10,21;
1,3,10,10,2,10,1,5,11,21,11,0,0,0,13,14,13,22,24,12,14,14,11;
0,5,0,10,20,5,10,20,20,10,20,0,15,15,15,20,15,0,10,0,0,5,5;

•$n = 54$:

204221212131124324212121420; 434342231410032322023311343; 104100343414123100323434424;
011143041210233231423421114; 032441310132430410102303342; 230232404241010330120424134;
441411213412434034322022322; 334031424114130013243202324; 343443331102422113433411302;
034240121444430034231001021; 240300021041010132143212032; 223113301142224440400312432;
142211012102144100204002334; 142044140403101243332123333; 333101210243241301444043101;
212441222431233244343130104; 124044331242400141041134143; 431411143134344104411242144;
013040012213002414113104342; 132322004422444032224044134; 441222200433240204312130332;
333002320111444300214243024; 144220234441011401421241012; 034230330404403122101211433;
044142133443332201311024414; 211313134331241213131321030; 230012440113341320324300112