A bound for certain s-extremal lattices and codes

Philippe Gaborit*

Abstract

In this paper we introduce the notion of s-extremal lattice for unimodular Type I lattices. We give a bound on the existence of certain such s-extremal lattices: an s-extremal lattice of dimension n and minimal even norm μ must satisfy $n < 12\mu$. This partly answers an open question by Elkies. We give an equivalent bound for s-extremal self-dual codes: an s-extremal codes with doubly even minimum distance d and length n must satisfy $n < 6d$. Eventually we classify all the 41 extremal binary $[36, 18, 8]$ self-dual codes.

Keywords: unimodular lattices, self-dual codes, modular forms, classification, shadow.

1 Introduction

The class of unimodular lattices has been studied for a long time and contains many interesting lattices. In particular it is possible to give bound on the minimum norm of such lattices. If L is a unimodular lattice Λ with theta series

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

where $\tau \in \mathfrak{h}$ the upper half complex plane and $q := e^{\pi i \tau}$, its theta series satisfies an invariance property under the transformation $\tau \to -1/\tau$. If the lattice is moreover even, then its theta series is invariant under the action of the full modular group $SL(2, \mathbb{Z})$, this result permits to show that the minimum norm μ of an even unimodular lattice satisfies:

$$\mu \leq 2[n/24] + 2 \tag{2}$$

*LACO, Université de Limoges, 123, av. A. Thomas, 87000 Limoges, France; email: gaborit@unilim.fr; Fax: (33) 5 55 45 73 22

where n is the dimension of the lattice. The first case where this bound is not known to be tight is $n = 72$.

In the case of odd unimodular lattices no satisfactory bound was known until the introduction of shadow theory by Conway and Sloane in [5].

Let L be a unimodular lattice. The shadow S of L is $S := (L_0)^* \setminus L$, where L_0 denotes the even sublattice of L. If L is an odd lattice, its theta series has the following expression

$$\theta_L(\tau) = \sum_{j=0}^{[n/8]} c_j \Delta_8(q)^j \theta_3(q)^{n-8j} \tag{3}$$

and the theta series of the shadow S is

$$\theta_S(\tau) = \sum_{j=0}^{[n/8]} \frac{(-1)^j}{16^j} c_j \theta_4(q^2)^{8j} \theta_2(q)^{n-8j}. \tag{4}$$

where $q := e^{\pi i \tau}$, $\Delta_8(q) = q \prod_{m=1}^{\infty}(1-q^{2m-1})^8(1-q^{4m})^8$, and θ_2, θ_3, θ_4 are the usual Jacobi theta series (see [5, Chap. 4, § 4]).

This notion was used to prove new bounds for odd unimodular lattices, the most efficient is the bound by Rains and Sloane [20] which states that except for the short Leech lattice in dimension 23 all odd unimodular lattices also satisfy the bound (2) for even lattices.

Another point of view on the shadow was proposed by Elkies who studies in [7] the minimum norm of the shadow. If we denote as usual by μ the minimum norm of L and by σ, four times the minimum norm of its shadow, Elkies shows that $\sigma \leq n$ and the only lattice with $\sigma = n$ is $\mathbb{Z}^n$. He also considers the case where $\sigma = n - 8$ for which he gives the short list from the classification of unimodular lattices up to dimension 24. The next cases $\sigma = n - 16$ and $\sigma = n - 24$ were first considered by Gaulter in [10] who gives two large upper bounds for the existence of such lattices. Then Nebe and Venkov consider in [16] more precisely the case $\sigma = n - 16$ for which they give a tight upper bound of $n \leq 46$ for the existence of such lattice. In particular Elkies asks in [7] a natural question: is it possible to find a general bound on the existence of a lattice which satisfies $\sigma = n - 8k$?

In this paper we give such a bound in the case of odd k. More precisely we propose to study simultaneously the parameters σ and μ as it was proposed for codes by Bachoc and the author in [1]. We show that $8\mu + \sigma \leq n + 8$ except in the case $n = 23$ and $\mu = 3$ for which $\sigma = 15$. The lattice which satisfy equality in the bound are called s-extremal. We show that for even μ, s-extremal lattices exist only if $n < 12\mu$. We also give an equivalent bound for s-extremal codes: if an s-extremal code of length n has a doubly-even minimum distance d then $n < 6d$. Eventually we give a recursive algorithm which enables us to classify all the 41 extremal $[36, 18, 8]$ self-dual codes. We deduce from this classification new classification results for s-extremal codes.

The paper is organized as follows: Section 2 deals with s-extremal lattices, their definition and the bound, in Section 3 we list known s-extremal lattices, Section 4 is concerned with the bound for s-extremal codes and at least we classify the $[36, 18, 8]$ self-dual codes in Section 5.

2 S-extremal lattices

We first give a theorem and a definition for s-extremal lattices.

Theorem 2.1 *Let L be a unimodular lattice, assumed not to be of Type II, of minimum norm μ, and let S be its shadow, of minimum norm σ. Then, $8\mu + \sigma \leq 8 + n$, unless $n = 23$ and $\mu = 3$, in which case $\sigma = 15$.*

Definition 2.2 *A lattice which parameters (μ, σ) satisfy equality in the previous bounds is said to be s-extremal. In that case, the theta series θ_L and θ_S are uniquely determined.*

Remark: From Theorem 2.1, the only case for which $8\mu + \sigma > 8 + n$ is the special case of the short Leech lattice O_{23}.

Proof of theorem 2.1: From (4), the norms in S are congruent to $\frac{n}{4}$ mod 2. Let us denote a_i the number of vectors of norm i in L and b_i the number of vectors of norm $\frac{i}{4}$ in S. Let us define σ' by $\sigma = n - 8\sigma'$. From (3) and (4), the conditions

$$\begin{cases} a_0 = 1 \\ a_i = 0 \text{ for } 1 \leq i \leq \mu - 1 \\ b_{n-8j} = 0 \text{ for } \sigma' + 1 \leq j \leq [n/8] \end{cases} \tag{5}$$

are linear and independant conditions on the $[n/8]+1$ coefficients c_i. Their number is $\mu + [n/8] - \sigma'$, which is greater or equal to $[n/8] + 1$ if and only if $8\mu + \sigma \geq 8 + n$.

We now assume that the inequality $8\mu + \sigma \geq 8 + n$ holds. From the previous discussion, the theta series of L and S are uniquely determined. Let $t := 8 + n - 8\mu$. We have:

$$\begin{cases} \theta_L = 1 + a_\mu q^\mu + a_{\mu+1} q^{\mu+1} + \dots \\ \theta_S = b_t q^t + b_{t+8} q^{t+8} + \dots \end{cases} \tag{6}$$

where b_t is not assumed to be non-zero.

In the following we discuss the possibility that $b_t = 0$.

From (4), $b_t = \frac{(-1)^j}{16^{\mu-1}} c_{\mu-1}$ and $c_i = 0$ for all $i > \mu - 1$. Dividing (3) by θ_3^n one then gets:

$$\sum_{j=0}^{\mu-1} c_j \left(\frac{\Delta_8}{\theta_3^8}\right)^j = \frac{1}{\theta_3^n} + \frac{1}{\theta_3^n}\{a_\mu q^\mu + \cdots\} \tag{7}$$

Hence the coefficients $c_0, \cdots c_{\mu-1}, -a_\mu$ are the coefficients of $\frac{1}{\theta_3^n}$ developped on $\left(\frac{\Delta}{\theta_3^8}\right)^j$. As in [20] the Bürman-Lagrange formula [21] allows us to calculate:

$$c_{\mu-1} = \frac{1}{(\mu-1)!}\frac{\partial^{\mu-2}}{\partial q^{\mu-2}}\left(\frac{\partial}{\partial q}\left(\theta_3^{-n}\right)\left(\frac{q\theta_3^8}{\Delta_8}\right)^{\mu-1}\right)_{q=0} = \frac{1}{(\mu-1)!}\frac{\partial^{\mu-2}}{\partial q^{\mu-2}}\left(-n\frac{\theta_3'}{\theta_3^{n-8\mu+9}}\left(\frac{q}{\Delta_8}\right)^{\mu-1}\right)_{q=0}$$

Replacing θ_3 and Δ_8 we obtain

$$c_{\mu-1} = \frac{-n}{\mu-1}\left\{\text{coeff. of } q^{\mu-2} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{m=1}^\infty [(1-q^{2m})(1+q^{2m-1})]^{n-8\mu+8}[(1-q^{2m-1})(1-q^{4m})]^{8\mu-8}}\right\}$$

$$= \frac{-n}{\mu-1}\left\{\text{coeff. of } q^{\mu-2} \text{ in: } \frac{\theta_3'/\theta_3}{S_1}\right\}$$

with $S_1 = \prod_{m=1}^\infty (1-q^{2m})^{n-8\mu+8}(1-q^{4m-2})^{8\mu-8}(1-q^{4m})^{8\mu-8}(1+q^{2m-1})^{2n-24\mu+24}$.

By considering the product form of θ_3 we remark that the q-expansion of the series θ_3'/θ_3 is alternated with all coefficients non null and positive for even powers of q. We now notice that from the bound of [20]: $n - 8\mu + 8 \geq 0$ and that the q-expansions of the series $\frac{1}{1-q^{2m}}, \frac{1}{1-q^{4m-2}}, \frac{1}{1-q^{4m}}$ have only even powers of q with positive terms. Hence since the product of an alternated series with a series with only positive terms for even powers of q is still alternated, the sign of a_μ is related to $2n - 24\mu + 24$.

If $2n - 24\mu + 24 \geq 0$ the q-expansion of the series $(1+q^{2m-1})^{-(2n-24\mu+24)}$ is alternated and therefore since the product of two alternated series is still alternated and that θ_3'/θ_3 has only non null coefficients, we deduce that $c_{\mu-1} \neq 0$ (and therefore $b_t \neq 0$).

If $2n - 24\mu + 24 \leq -4$ then one gets:

$$c_{\mu-1} = \frac{-n}{\mu-1}\left\{\text{coeff. of } q^{\mu-2} \text{ in: } \frac{\theta_3' \prod_{m=1}^{\infty}(1+q^{2m-1})^{-(2n-24\mu+26)}}{\prod_{m=1}^{\infty}(1-q^{2m})^{n-8\mu+9}(1-q^{4m-2})^{8\mu-8}(1-q^{4m})^{8\mu-8}}\right\}$$

since $-(2n-24\mu+26) \geq 2$, $c_{\mu-1} \neq 0$.

From the bound of [20] the last possibility $2n - 24\mu + 24 = -2$ (or equivalently $2n-24\mu+26 = 0$) may only happen for $n = 24k+11, \mu = 2k+2$ or $n = 23, \mu = 3$. We then have :

$$c_{\mu-1} = \frac{-n}{\mu-1}\left\{\text{coeff. of } q^{\mu-2} \text{ in: } \frac{\theta_3'}{\prod_{m=1}^{\infty}(1-q^{2m})^{n-8\mu+9}(1-q^{4m-2})^{8\mu-8}(1-q^{4m})^{8\mu-8}}\right\}$$

In the case where $n = 24k+11$ and $\mu = 2k+2$ since μ is even we deduce from the q-expansion of the series that $c_{\mu-1}$ is non null. The second case corresponds to the short Leech lattice for which $b_7 = 0$ but $b_{15} \neq 0$.

This concludes the proof.

□

The following theorem gives a bound on the existence of s-extremal lattices in the case of even minimum norms. Note that as we will see in the next section for $\mu = 4$, this bound is tight.

Theorem 2.3 *Let L be an s-extremal lattice with parameters (μ, σ) of dimension n, if μ is even then $n < 12\mu$.*

Proof: The proof is similar to the proof of the previous theorem. Let L be an s-extremal lattice then $c_{[n/8]} = \cdots = c_\mu = 0$ and dividing (3) by θ_3^n one gets:

$$\sum_{j=0}^{\mu-1} c_j \left(\frac{\Delta}{\theta_3^8}\right)^j = \frac{1}{\theta_3^n} + \frac{1}{\theta_3^n}\{a_\mu q^\mu + \cdots\} \tag{8}$$

Hence the coefficients $c_0, \cdots c_{\mu-1}, -a_\mu$ are the coefficients of $\frac{1}{\theta_3^n}$ developped on $\left(\frac{\Delta}{\theta_3^8}\right)^j$. The Bürman-Lagrange formula allows us to calculate:

$$-a_\mu = \frac{1}{\mu!}\frac{\partial^{\mu-1}}{\partial q^{\mu-1}}\left(\frac{\partial}{\partial q}\left(\theta_3^{-n}\right)\left(\frac{q\theta_3^8}{\Delta_8}\right)^\mu\right)_{q=0} = \frac{1}{\mu!}\frac{\partial^{\mu-1}}{\partial q^{\mu-1}}\left(n\frac{\theta_3'}{\theta_3^{n+1-8\mu}}\left(\frac{q}{\Delta_8}\right)^\mu\right)_{q=0}$$

Replacing θ_3 and Δ_8 we obtain:

$$a_\mu = \frac{n}{\mu}\left\{\text{coeff. of } q^{\mu-1} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{m=1}^\infty[(1-q^{2m})(1+q^{2m-1})]^{n-8\mu}[(1-q^{2m-1})(1-q^{4m})]^{8\mu}}\right\}$$

$$= \frac{n}{\mu}\left\{\text{coeff. of } q^{\mu-1} \text{ in: } \frac{\theta_3'/\theta_3}{\prod_{m=1}^\infty(1-q^{2m})^{n-8\mu}(1-q^{4m-2})^{8\mu}(1-q^{4m})^{8\mu}(1+q^{2m-1})^{2n-24\mu}}\right\}$$

We already saw that the series θ_3'/θ_3 is alternated with positive terms for even powers of q and that the q-expansions of the series $\frac{1}{1-q^{2m}}, \frac{1}{1-q^{4m-2}}, \frac{1}{1-q^{4m}}$ had only even power of q with positive terms. We remark moreover that from [20] $n - 8\mu \geq 0$ for $n \geq 32$ (the case $n \leq 31$ and even μ corresponds to the case $\mu = 2$ considerered by Elkies) . Now since the product of an alternated series with a series with only positive terms for even powers of q is still alternated, the sign of a_μ is related to $2n - 24\mu$.

If $2n - 24\mu \geq 0$ the q expansion of the series $\frac{1}{(1+q^{2n-24d})}$ is alternated and since from the q expansion of θ_3'/θ_3 the term a_μ is non null, we deduce that the sign of a_μ is $(-1)^{\mu-1}$ and that s-extremal lattices for even μ and $n \geq 12\mu$ can not exist. □

3 Examples of s-extremal lattices

• $\mu = 2$

Such lattices exist up to dimension 23, this case has been completely classified by Elkies in [7] from the classification of unimodular lattices up to dimension 24.

• $\mu = 3$

This case has been considered in [16], such lattices exist up to dimension 46. A questionmark in the table means that no lattice is known at present.

n	num	ref	n	num	ref
23	1	[16]	35	≥ 1	[16]
24	1	[16]	36	?	
25	0		37	?	
26	1	[16]	38	?	
27	2	[16]	39	?	
28	36	[16]	40	≥ 1	[1]
29	≥ 1	[16]	41	?	
30	≥ 1	[16]	42	?	
31	≥ 1	[16]	43	?	
32	≥ 1	[16]	44	0	[16]
33	≥ 1	[16]	45	0	[16]
34	≥ 1	[16]	46	1	[16]

- $\mu = 4$

In that case, such lattices exist up to dimension 47. We list known lattices for $\mu = 4$:

n	num	ref
32	3	[5]
36	≥ 2	[15],[8]
37	?	
38	≥ 1	[8]
39	≥ 1	[11]
40	≥ 1	[8]
41	?	
42	≥ 1	[15],[8]
43	?	
44	?	
45	?	
46	≥ 1	[13]
47	≥ 1	[13]

- $\mu = 5$

In that case, it is not known up to which dimension such lattices do exist. The only known lattice is for dimension 54 in [8].

- $\mu \geq 6$

In that case no such lattice is known.

4 S-extremal codes

We now give for s-extremal codes a bound equivalent to the bound of Theorem 2.3. Let C be a self-dual binary code, which is assumed not to be doubly even and let S be its shadow. We denote W_C and W_S the weight enumerators of C and S. From [5], there exists $c_0, \ldots, c_{[n/8]} \in \mathbb{R}$ such that:

$$\begin{cases} W_C(x,y) & = \sum_{i=0}^{[n/8]} c_i (x^2+y^2)^{\frac{n}{2}-4i}\{x^2y^2(x^2-y^2)^2\}^i \\ W_S(x,y) & = \sum_{i=0}^{[n/8]} c_i (-1)^i 2^{\frac{n}{2}-6i}(xy)^{\frac{n}{2}-4i}(x^4-y^4)^{2i} \end{cases} \tag{9}$$

We denote d the minimum weight of C and s the minimum weight of its shadow. The following theorem and definition are from [1]:

Theorem 4.1 *Let C be a self-dual binary code, assumed not to be doubly even, of minimum weight d, and let S be its shadow, of minimum weight s. Then, $2d+s \leq 4+\frac{n}{2}$, unless $n \equiv 22 \mod 24$ and $d = 4[n/24]+6$, in which case $2d+s = 8+\frac{n}{2}$.*

Definition 4.2 *A code which parameters (d,s) satisfy equality in the previous bounds is said to be s-extremal. In that case, the polynomials W_C and W_S are uniquely determined.*

The following theorem gives a bound on the existence of such s-extremal codes. Note that as for lattices for $d=8$, this bound is tight in the sense that such exist for $n=44$ and $n=46$ corresponds to the special case of a $[46,23,10]$ code with $s=11$.

Theorem 4.3 *Let C be an s-extremal code with parameters (s,d) of length n, if $d \equiv 0 \pmod 4$ then $n < 6d$.*

Proof: Let C be an s-extremal codes with parameters (s,d) with $d \equiv 0 \pmod 4$ then one may assume that the equality $2d+s = 4+\frac{n}{2}$ holds. The weight enumerators of C and S are uniquely determined. Bürman-Lagrange formula allows us to calculate the coefficients of these polynomials. Let $t := 4+\frac{n}{2}-2d$. We have:

$$\begin{cases} W_C(x,y) = 1 + a_d x^{n-d}y^d + a_{d+2}x^{n-d-2}y^{d+2} + \ldots \\ W_S(x,y) = b_t x^{n-t}y^t + b_{t+4}x^{n-t-4}y^{t+4} + \ldots \end{cases} \tag{10}$$

We now prove that if $d \equiv 0 \pmod 4$ and $n \geq 6d$ then then $a_d < 0$, which proves the theorem since all the coefficients have to be greater or equal to zero.

We have in (9) $c_i = 0$ for all $i > \frac{d}{2} - 1$. Setting $x = 1$ and dividing by $(1+y^2)^{\frac{n}{2}}$ the first equation of (9) leads to:

$$\sum_{i=0}^{\frac{d}{2}-1} c_i \left\{ \frac{y(1-y^2)}{(1+y^2)^2} \right\}^{2i} = \frac{1}{(1+y^2)^{\frac{n}{2}}} + \frac{1}{(1+y^2)^{\frac{n}{2}}} \{a_d y^d + \dots\}$$

Let $g(y) := \frac{y(1-y^2)}{(1+y^2)^2}$. From this last expression, we see that $c_0, c_1, \dots, c_{\frac{d}{2}-1}, -a_d$ are the first coefficients of the development of $\frac{1}{(1+y^2)^{\frac{n}{2}}}$ as a series in $g(y)$. From the Bürman-Lagrange formula, we obtain:

$$-a_d = \frac{1}{d!} \frac{\partial^{d-1}}{\partial y^{d-1}} \left(\frac{\partial}{\partial y} \left(\frac{1}{(1+y^2)^{\frac{n}{2}}} \right) \left(\frac{(1+y^2)^2}{1-y^2} \right)^d \right)_{y=0}$$

which, after simplification, becomes:

$$a_d = \frac{n}{d} \left\{ \text{coeff. of } y^{d-2} \text{ in: } \frac{1}{(1+y^2)^{\frac{n}{2}-2d+1}(1-y^2)^d} \right\}.$$

Let us write $n = 6d + 2\alpha$, with $\alpha \geq 0$ then the previous formula becomes:

$$a_d = \frac{n}{d} \left\{ \text{coeff. of } y^{d-2} \text{ in: } \frac{1}{(1+y^2)^{1+\alpha}(1-y^4)^d} \right\},$$

and, finally, leads to :

$$\begin{aligned} a_d &= \frac{n}{d} \sum_{\substack{j,k \in \mathbb{N} \\ j+2k = \frac{d}{2}-1}} (-1)^j \binom{\alpha+j}{j} \binom{d+k+1}{k} \\ &= \frac{n}{d} (-1)^{\frac{d}{2}-1} \sum_{\substack{j,k \in \mathbb{N} \\ j+2k = \frac{d}{2}-1}} \binom{\alpha+j}{j} \binom{d+k+1}{k} \end{aligned}$$

which shows that a_d is negative for $d \equiv 0 \pmod 4$.

$\square$

5 Extension and truncation of self-dual codes

In this section we present an algorithm to find all self-dual binary inequivalent $[n+2, \frac{n}{2}+1, d+2]$ codes from all inequivalent binary self-dual $[n, \frac{n}{2}, d]$ codes. As an application we classify the 41 $[36, 18, 8]$ self-dual codes and deduce some classification for s-extremal codes with $d = 6$ and $d = 8$.

5.1 A recursive algorithm to classify self-dual codes

Assume C_{n+2} is a $[n+2, \frac{n}{2}+1, d+2]$ self-dual code with $d \geq 2$ then up to equivalence a generator matrix of C_{n+2} can be written as:

$$G = \begin{bmatrix} 1 & 1 & y \\ 0 & 0 & D \\ 0 & 1 & z \end{bmatrix},$$

where y is a codeword of length n and weight d and where D is a certain subcode $[n, \frac{n}{2}-1]$ of C_{n+2}, truncated on its first two coordinates, and where z is a certain truncated codeword of C_{n+2}.

We remark that the code with generator matrix

$$\begin{bmatrix} \text{y} \\ \text{D} \end{bmatrix}$$

is a self-dual $[n, \frac{n}{2}, d]$ code. This remak implies that a self-dual $[n, \frac{n}{2}, d]$ code can be associated to any self-dual $[n+2, \frac{n}{2}+1, d+2]$ code.

Now conversely suppose that one starts from a $[n, \frac{n}{2}, d]$ code C_n obtained as before by truncation of two columns and getting rid of an appropriate row of a $[n+2, \frac{n}{2}+1, d+2]$ code C_{n+2}. Then one can choose as generator matrix of C_n a matrix of the form:

$$\begin{bmatrix} \text{y'} \\ \text{E} \end{bmatrix}$$

where y' a word of weight d.

If one considers the set MC of all the $[n+2, \frac{n}{2}]$ codes C with generator matrices of the form:

$$\begin{bmatrix} 1 & 1 & y' \\ a_1 & a_1 & \\ \vdots & \vdots & E \\ a_{n-1} & a_{n-1} & \end{bmatrix}$$

where $a_i \in \{0,1\}$, one will necessarily construct a subcode of C_{n+2} of dimension n since any codeword of C_n extended either by 00 or by 11 is in C_{n+2}. To find C_{n+2} back it is then sufficient to complete all the codes C of MC by one of the three non nul elements of $C^\perp/C$.

Hence we have proven that if one knows a subcode $[n, \frac{n}{2}, d]$ C_n of a $[n+2, \frac{n}{2}+1, d+2]$ code C_{n+2}, it is possible to rebuild the code C_{n+2} by this method, and this up to equivalence.

Therefore, if rather than starting from a unique $[n, \frac{n}{2}, d]$ code, one starts from the set of all inequivalent $[n, \frac{n}{2}, d]$ self-dual codes, one can rebuild all the $[n+2, \frac{n}{2}+1, d+2]$ self-dual codes.

Now if one proceeds simply as previously described, one has to consider 2^{n-1} possibilities for the a_i. Meanwhile by noticing that necessarily all the words of weight d of the $[n, n/2, d]$ code have to be extended in codewords of weight $d+2$, it is then possible to considerably fasten the algorithm by considering not only one vector of weight d but the code generated by the vectors of weight d. If this subcode has dimension k it is then sufficient to consider 2^{n-k} possibilities for the a_i and not 2^{n-1} and this only once for each code.

We now sum up the algorithm to compute recursively all the $[n+2, \frac{n}{2}+1, d+2]$ self-dual codes from all the $[n, \frac{n}{2}, d]$ self-dual codes:

• Start from the set S_n of all the $[n, \frac{n}{2}, d]$ self-dual codes up to permutation and for each code C_n of S_n do:

• List all the words of weight d and construct the subcode C_d of dimension k generated by these words. Construct a generator matrix G_d of C_d composed only with words of weight d.

• Let E be a code of dimension $n-k$ with generator matrix G_E such that $C_n = C_d + E$, construct the extended codes C with generator matrices:

$$\begin{bmatrix} 1 & 1 & \\ \vdots & \vdots & G_d \\ 1 & 1 & \\ a_1 & a_1 & \\ \vdots & \vdots & G_E \\ a_{n-k} & a_{n-k} & \end{bmatrix}$$

such that $a_i \in \{0,1\}, (1 \leq i \leq n-k)$.

• Complete all the previous codes C by non nul elements of $C^{\perp}/C$ in order to obtain a self-dual code and check for codes with minimum distance $d+2$. For codes with weight $d+2$ check for the equivalence with already obtained self-dual $[n+2, \frac{n}{2}+1, d+2]$ codes.

5.2 Classification of the $[36, 18, 8]$ self-dual codes

In [3] all the self-dual codes of length 32 are classified. These results are available at http://www.cs.umanitoba.ca/~umbilou1/ . Starting from the 2482 $[32, 16, 4]$ codes we constructed the 938 $[34, 17, 6]$ self-dual codes. Note that this result was announced in [3] and that these codes can also be found at the same address. Now starting from all the 938 $[34, 17, 6]$ codes we obtain:

Theorem 5.1 *There are exactly* 41 *self-dual* $[36, 18, 8]$ *codes.*

These codes are available at http://www.unilim.fr/pages_perso/philippe.gaborit.
Remark: Until now only 15 binary self-dual codes were known from [14].

From [5] two weight and shadow enumerators are possible:

$W_1 = 1 + 225y^8 + 2016y^{10} + \cdots$
$S_1 = 42y^6 + 3780y^{10} + \cdots$

and

$W_2 = 1 + 289y^8 + 1632y^{10} + \cdots$
$S_2 = y^2 + 34y^6 + \cdots$

Among the 41 codes 25 have weight enumerator W_1 with automorphism group orders $\{6, 8, 18, 24(2), 32(2), 36(2), 48(3), 64, 96(3), 240, 288, 384(2), 864, 2304, 2688, 10752, 12960\}$ and 16 with weight enumerator W_2 and automorphism group orders $\{12, 24, 32, 34, 48(3), 64, 80, 96, 128(2), 240, 384, 1536, 34560\}$.

Remark: If one uses the previous algorithm on the $[36, 18, 8]$ codes, one can construct more than 900 inequivalent $[38, 19, 8]$ self-dual codes.

5.3 Classification of certain s-extremal codes

We now use these previous classification to deduce:

Proposition 5.2 *There are exactly:*
- 16 *s-extremal* $[34, 17, 6]$ *codes,*
- 5 *s-extremal* $[36, 18, 6]$ *codes,*
- 25 *s-extremal* $[36, 18, 8]$ *codes.*

Proof: The number of s-extremal $[34, 17, 6]$ and $[36, 18, 8]$ codes can be read directly from the classification of $[34, 17, 6]$ and $[36, 18, 8]$ self-dual codes.
Now let C be an s-extremal $[36, 18, 6]$ code, then its shadow has weight 8 and hence C has a self-dual neighbor build from its doubly even subcode (as in [1]) with minimum 8.
Since the notion of neighbor is reflexive this remark implies that all the $[36, 18, 6]$ s-extremal codes can be obtained as neighbors of all the $[36, 18, 8]$ and the result follow from this computation. $\square$

ACKNOWLEDGEMENT

We thank C. Bachoc for helpful conversations. All the computations were done with the MAGMA system [4].

References

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A*, 105 (2004), no. 1, pp. 15–34.

[2] R. A. Brualdi and V. S. Pless, Weight Enumerators of Self-Dual Codes, *IEEE Trans. Inf. Th.*, **37** (1991), pp. 1222-1225.

[3] R. T. Bilous and G. H. J. van Rees, An enumeration of self-dual codes of length 32, *Des. Codes Cryptogr.* 26 (2002), no. 1-3, pp. 61–86.

[4] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney, 1995.

[5] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inf. Th.*, **36** (1990), pp. 1319-1333.

[6] S.T. Dougherty, T. A. Gulliver and M. Harada, Extremal binary self-dual codes, *IEEE Trans. Inform. Theory*, **43**, (1997), pp. 2036-2047.

[7] N. Elkies, Lattices and codes with long shadows, *Math. Res. Lett.* **2** (1995) no. 5, pp. 643-651.

[8] P. Gaborit, Construction of new unimodular lattices, *Eur. J. Comb.*, 25 (2004), no. 4,pp. 549–564

[9] P. Gaborit and A. Otmani, Experimental constructions of self-dual codes, *Finite Fields Appl.*, 9 (2003), no. 3, pp. 372–394.

[10] M. Gaulter, Lattices without short characteristic vectors, *Math. Res. Lett.*, **5** (1998) no. 3, pp. 353-362.

[11] Gulliver, T. Aaron; Harada, Masaaki , An optimal unimodular lattice in dimension 39. *J. Combin. Theory Ser. A* 88 (1999), no. 1, pp. 158–161.

[12] M. Harada, New extremal self-dual codes of lengths 36 and 38, *IEEE Trans. Inform. Theory*, **45**, (1999), pp. 2541-2543.

[13] M. Harada, Extremal odd unimodular lattices in dimensions 44, 46 and 47. *Hokkaido Math. J.*, 32 (2003), no. 1, pp. 153–159.

[14] J.-L. Kim, New extremal self-dual codes of lengths 36,38 and 58, *IEEE Trans. Inform. Theory*, **47**, (2001), n.4, pp. 1575-1580.

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

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

[17] V. Pless, *Introduction to the Theory of Error Correcting Codes*, Wiley, New York, 3^{rd} edition, 1998.

[18] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Math.* **3** (1972) pp. 209-246.

[19] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, *J. Combin. Theory Ser. A* **A18** (1975), pp. 313-335.

[20] 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.

[21] E.T. Whittaker and G.N. Watson, *A course of Modern Analysis*, 4th edition, New-York, Cambridge University Press, 1963.