Experimental constructions of self-dual codes

Philippe Gaborit
LACO, Université de Limoges
123, Av. A. Thomas,
87000 Limoges, France
Email: gaborit@unilim.fr,

Ayoub Otmani
LACO, Université de Limoges
123, Av. A. Thomas,
87000 Limoges, France
Email: otmani@unilim.fr

January 1, 2002

Proposed running head: Constructions of self-dual codes

Corresponding author:
Philippe Gaborit
LACO, Université de Limoges
123, av. A. Thomas,
87000 Limoges,
France.
email: gaborit@unilim.fr

Abstract

We give a general experimental method generalizing the codes of [7] to construct self-dual codes. We consider the particular fields $GF(2), GF(3), GF(4)$ (both Euclidean and Hermitian cases), $GF(5)$ and $GF(7)$. We give experimental tables of the best known self-dual codes over the previous alphabets up to the maximal reachable lengths to compute the minimum distance. These tables regularly fill gaps between known codes with good parameters such as the quadratic residue codes, the Pless symmetry codes [43] or the quadratic double circulant codes [13]. Many new codes with better parameters than already known codes are constructed, in particular the first extremal self-dual ternary $[52, 26, 15]$ and $[78, 39, 18]$ codes and the first self-dual binary $[114, 57, 18]$ and $[116, 58, 18]$ codes are constructed. We also give the weight of the Pless symmetry codes of length 84 and update tables for quadratic residue codes over $GF(4), GF(5)$ and $GF(7)$ and obtain in particular a $[62, 31, 20]$ code over $GF(5)$.

Keywords: self-dual codes, construction of codes, quadratic residue codes, Pless symmetry codes.

1 Introduction

Self-dual codes have been studied in many papers in the last forty years. In particular self-dual binary codes have been classified up to length 30 and self-dual doubly even codes up to length 32 ([42], [46],[8]). Self-dual ternary codes have been classified up to length 20 ([10],[47]) and also for length 24 for extremal ones ([35]). Self-dual Hermitian quaternary codes have been classified up to length 16 ([10]) and extremal codes for lengths 18 and 20 ([29]). One may also find results for small lengths over $GF(4)$ (Euclidean) in [33], over $GF(5)$ in [36] and over $GF(7)$ in [48]. A review of all these results can be found in [49].

Nevertheless only a few non trivial infinite families of such codes are known, especially quadratic residue codes and derived codes such as quadratic double circulant codes [13], Pless symmetry codes [43] or codes constructed from Hadamard matrices. One should also mention duadic codes over $GF(2)$ [42] and their generalization over $GF(4)$ [34] and also Reed-Muller codes, but these families only give a few self-dual codes with real good parameters.

For lengths for which no codes of the previous families are known it is not always easy to construct codes with good parameters. In that case the best method used seems to be the search of such codes in a double circulant form [38]. Many good codes were found this way, especially in the binary case ([30],[9]). In particular double circulant self-dual codes were classified up to length 72 by Gulliver and Harada [18]. Another recent method introduced by Harada consists in double extension of codes [22], this was also used by Kim in [32] for self-dual codes over $GF(4)$. It is also possible to use a mixed theoretical-computational method for special length and to search for codes with special subgroup in their automorphism groups as it was done by W.C. Huffman for $GF(3)$ and $GF(4)$ in [29] and [27].

In recent recent years there was a burst of activity using these methods to produce good self-dual codes of not too high lengths over various alphabets. Unfortunately these methods have their difficulties. For instance when one is searching for double circulant codes one needs to find a row which satisfies a reciprocal orthogonality with its permuted coordinates, which makes it more and more difficult as the length increases. The second method of double extension needs to start from a code which has already a not low length if one is to obtain a code with good minimum distance. Finally the third method mentioned produced many good codes but needs a special study for each new length or alphabet considered, which makes it not so easy to handle if one is to consider many lengths and many alphabets.

In this paper we propose a new experimental method to construct quickly and easily 'good' self-dual codes of any length over any alphabet. The term 'good' meaning that the minimum distance of the code is exactly or very close to the highest known minimum distance for a self-dual code of a particular length. This method generalizes the binary codes construction of [5]-[7] to any alphabet and mainly relies on computation. We use this method to construct self-dual codes over $GF(2), GF(3), GF(4), GF(5)$ and $GF(7)$. The codes we obtain fill more or less regularly gaps between codes constructed with the previously mentioned families, which seems to indicate that the codes are 'good' indeed. The method enables us to find codes with better minimum distance than previously known codes and many of them equal or improve on the tables by Brouwer [4]. In particular the first $[52, 26, 15]$ self-dual ternary code, the first $[76, 38, 14]$ binary self-dual code and many new quaternary codes of lengths 40 or more for which very little is known are also constructed. For each alphabet considered we give a table for the codes we construct and also a table with the highest known minimum weight for self-dual codes. An on-line table with these results and explicit generator matrices for the self-dual codes with highest known minimum distance can be found at http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html. We also update tables of weights of extended quadratic residue codes over $GF(4), GF(5)$ and $GF(7)$. The weights of the Pless symmetry code of length 84 and the Beenker code of length 88 are also given. All the computations, which sometimes have lasted more than three weeks, were done with MAGMA [3].

The material is organized as follows. Section 2 collects definitions and notation. Section 3 establishes the general construction used to construct self-dual codes. Section $4, 5, 6, 7$ and 8 consider respectively constructions over the fields $GF(2), GF(3), GF(4), GF(5)$ and $GF(7)$. Eventually Section 9 updates the minimum weight tables of quadratic residue codes over $GF(4), GF(5)$ and $GF(7)$.

2 Notation and Definitions

We refer to the Chapter by Rains and Sloane in the Handbook of Coding Theory [49] for more precise notation and definitions relating to self-dual codes. A linear $[n, k]$ code C of length n and dimension k over the Galois field with q elements $GF(q)$ is a linear subspace of dimension k of $GF(q)^n$. An element of C is called a codeword. The (Hamming) weight $w(x)$ of a codeword $x = (x_1, ..., x_n)$ is the number of its non-zero coordinates and the minimum distance $d(\mathbf{C})$ of a code $\mathbf{C}$ is defined by: $d(C) = min\{w(x-y) | x, y \in \mathbf{C}\}$. There are two possible kinds of scalar product. The Euclidean scalar product is understood with respect to the form: $x.y = \sum x_i.y_i$. For $x \to \bar{x}$ an involution defined on $GF(q)$ the Hermitian scalar product is defined by $x.y = \sum x_i.\bar{y_i}$. Each kind of scalar product defines a different notion of duality. The dual of a code $\mathbf{C}$ is denoted by $\mathbf{C}^\perp$. A code $\mathbf{C}$ is called Euclidean (resp. Hermitian) self-dual if and only if $\mathbf{C} = \mathbf{C}^\perp$ for the Euclidean (resp. Hermitian) scalar product. For instance over $GF(4) = \{0, 1, w, w^2\}$ the Frobenius map $x \to x^2$ defines an involution and there are two different kind of dualities which lead to different self-dual codes ([49]). Type II code are binary self-dual codes all whose codewords have weight a multiple of 4, Type I codes are binary self-dual codes which are not Type II. Ternary self-dual codes are also called Type III codes and eventually Type IV codes stand for Hermitian self-dual codes over $GF(4)$.

Two codes over $GF(q)$ are said to be *monomially equivalent* if they differ only by a monomial transformation (*ie* a permutation of the coordinates followed by a multiplication of the coordinates by a non zero element of $GF(q)$). We remark that the monomial transformations do not necessarily respect self-duality and in particular two Euclidean self-dual codes over $GF(4)$ are said to be equivalent if they differ only by a permutation ([15]). Let $\mathbf{C}$ be a self-dual code of length n and minimum distance $d(C)$. Then bounds are known for the minimum distance ([49]) depending on the duality. For binary self-dual codes:

$$d(C) \leq \begin{cases} 4\left[\frac{n}{24}\right] + 4, & \text{if } n \neq 22 \pmod{24}, \\ 4\left[\frac{n}{24}\right] + 6, & \text{if } n = 22 \pmod{24}. \end{cases}$$

The minimum distance of a self-dual ternary code $\mathbf{C}$ satisfies: $d(\mathbf{C}) \leq 3\left[\frac{n}{12}\right] + 3$ and for Hermitian self-dual quaternary codes: $d(\mathbf{C}) \leq 2\left[\frac{n}{6}\right] + 2$. Recently it was proven in [15] that for Euclidean self-dual codes: $d(\mathbf{C}) \leq 4\left[\frac{n}{12}\right] + 4$. A self-dual code meeting one of the previous bounds according to its self-duality is said to be *extremal*. No general bound is known for self-dual codes over alphabets with 5 or more element except the singleton bound $d(C) \leq \frac{n}{2} + 1$. A code is called *optimal* if it has the highest possible minimum weight for its length and dimension.

In the following tables, we denote by n, the length of a code and by d its minimum distance. In the case where the bound is not tight we give a upper and a lower bound. A Q will stand for the number of known non-equivalent codes for the lower bound of a given length. Most of the time the number of known codes will only be 1, since it is very difficult to prove that two codes of high length are inequivalent even if several codes are known with the same parameters. A *sub* in the table means (unless otherwise specified) that the code is obtained by subtraction of a small code from a code of the next higher length in the Table (cf [49]). Of course more than one inequivalent code may potentially be obtained depending on the columns chosen, but at least one is obtained this way. The small codes we use for subtraction are the unique codes with parameters $[2,1,2], [4,2,3], [2,1,2], [2,1,2]$ and $[4,2,3]$ over the respective fields $GF(2), GF(3), GF(4), GF(5)$ and $GF(7)$. The symbol XQ_p denotes the extended quadratic residue code of length $p+1$ over the alphabet considered in a given section. The symbol QDC_q denotes the quadratic double circulant code of length q over a given alphabet as defined in [13].

3 General construction

Let R be a ring. Let $\mathbf{C}$ be a self-dual code over $\mathbf{R}$ of length n. Let $\mathbf{G}$ be a generator matrix of $\mathbf{C}$. Now define $n \times n$ square matrices M_r satisfying for λ_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 ($r \geq 1$), we consider the codes $\mathbf{C}_r$ with generator matrices G_r:

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

These codes can also be seen as the alternative action on the original generator matrix of confusing matrices M_i and diffusion permutation matrices. In fact this action keeps the self-duality of the code as we show it in the next proposition.

Proposition 3.1 *If the code* $\mathbf{C}$ *is self-dual then so is* $\mathbf{C}_r$*.*

This proposition is straightforward from the following lemma:

Lemma 3.2 *Let G be a generator matrix of a self-dual code of length n over a ring R and let M be a $n \times n$ matrix over R satisfying $M.M^t = \lambda I$, with λ an invertible element of R. Then the code with generator matrix GM is self-dual.*

Proof. The code with generator matrix GM has the same number of vectors as the code with generator matrix G since M is invertible. The code with generator matrix G is self-dual so that $G.G^t = 0$. Hence $GM.(GM)^t = G.(MM^t)G^t = \lambda GG^t = 0$ which proves the self-duality of the code with generator matrix GM. $\square$

In fact we are interested in simple constructions of codes and in particular by simple matrices M_i. Most of the time we will take all matrices M_i to be equal to the same simple matrix M.

Let B be a square $b \times b$ matrix satisfying:

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

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

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

In the remainder we identify the set $\{1, \ldots, n\}$ with the quotient ring $\mathbf{Z}/n\mathbf{Z}$ and each permutation π acting on $\mathbf{Z}/n\mathbf{Z}$ is associated with a $n \times n$ permutation matrix $\Pi = (\delta_{i,\pi(j)})$ where $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise. We say that a sequence of permutations $\pi_1, \ldots, \pi_r$ belongs to one of the three following families f_j ($1 \leq j \leq 3$) if there exists an *invertible* element a in $\mathbf{Z}_n$ such that for any $1 \leq i \leq r$, π_i satisfies the relations:

$$\begin{aligned} f_1 &: \quad \forall z \in \mathbf{Z}_n, \quad \pi_i(z) = a \cdot (z+1). \\ f_2 &: \quad \forall z \in \mathbf{Z}_n, \quad \pi_i(z) = a^i \cdot (z+1). \\ f_3 &: \quad \forall z \in \mathbf{Z}_n, \quad \pi_i(z) = a^i \cdot (z+i). \end{aligned}$$

Any sequence of permutations that belongs to the family f_i is completely determined by a and r. Therefore, we say that a code is obtained from the construction $(f_i; a; r)$ when it is constructed from a sequence belonging to f_i. Notice that when the sequence $\pi_1, \ldots, \pi_r$ belongs to f_1, we have $\pi_i = \pi_1$ and when it belongs to f_2 then $\pi_i = \pi_1^i$.

Example. Suppose $n = 4$ and consider the square matrix M over $GF(3)$ constructed from the 2×2 square matrix $B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Let $\mathbf{C}$ be the self-dual code over $GF(3)$ defined by the matrix $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$. Let π be the transformation of $\mathbf{Z}_4$ into $\mathbf{Z}_4$ that satisfies $\pi(z) = 3(z+1)$ for all z in $\mathbf{Z}_4$. Obviously π is a permutation of S_4 and corresponds to the matrix

$$\Pi = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The code C_2 obtained from the construction (f_1;3;2) by starting from G has then the following generator matrix:

$$G_2 = GM\Pi M\Pi = \begin{pmatrix} 2 & 0 & 2 & 2 \\ 0 & 2 & 2 & 1 \end{pmatrix} \text{ where } M = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

In the next sections we consider the alphabets $GF(2), GF(3), GF(4), GF(5)$ and $GF(7)$. In each case we will give the matrices B, the permutation family used and the codes we start from.

4 Self-dual codes over $GF(2)$

Self-dual codes over $GF(2)$ received a lot of attention in the past forty years. In this section we extend tables for best known self-dual codes of [9],[12] and [49] to length 130. These results show that our construction very often leads to the best known codes for most of the lengths we consider and even leads to codes with previously unknown parameters. In particular we give new Type I codes with minimum distance 16 for previously unknown lengths and also the first $[114, 57, 18]$ and $[116, 58, 18]$ self-dual codes.

For length 76, one $[76, 38, 14]$ code was previously known in [1] (although the generator matrix given in that paper is false and is corrected in [21]). The computation of the number of words of weights 14 and 16 of our code shows that the weight enumerator W_{76} of the $[76, 38, 14]$ code corresponds to the weight enumerator W_1 of [12] with $\beta = 0$:

$$W_{76}(y) = 1 + 4750y^{14} + 79895y^{16} + 915800y^{18} + \dots.$$

In fact we checked with MAGMA that our code had also the same automorphism group order 19 that the code of [1] (generated by 4 cycles of size 19) but that they were not equivalent.

Concerning length 78, several $[78, 38, 14]$ codes are known ([1],[21]). We found one for which computation shows that the number of codewords of weight 14 and 16 of the code are respectively 3497 and 62868. So that the weight enumerator is of type $W_{78,1}$ of [12] with $\alpha = 0$ and $\beta = -26$, a previously unknown weight enumerator. It has an automorphism group order of 13.

The results obtained by our construction are presented in Table 1 and Table 2 extends and updates the table of [12] for lengths between 60 and 130. The $[60, 30, 12]$ code of Table 1 has an automorphism group of order 30 and is therefore not equivalent to all the previously known $[60, 30, 12]$ codes which are all obtained by double circulant constructions and therefore have an automorphism group of order at least 58. In Table 2 the notation *sub(C)* means a code obtained from subtraction of the code C, and Ka_{120} stands for the $[120, 60, 20]$ quadratic double circulant code of [30].

Over $GF(2)$ we set $B = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ and $G = \begin{pmatrix} 1 & 1 & & \\ & & \ddots & \\ & & & 1 \quad 1 \end{pmatrix}$.

A '$*$' in the table means that the code is obtained by taking for B the 6×6 matrix B_6:

$$B_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

5 Self-dual codes over $GF(3)$

Over $GF(3)$ self-dual codes are defined for lengths a multiple of 4. They have been classified up to length 20 in [10] and [47], moreover extremal codes are also known for length 24 ([35]). We refer the reader to [49] for more references on codes of lengths $28, 32, 40$ and 44. The two main families of good codes known are essentially the extended quadratic residue codes and also the Pless symmetry codes [43] along with the Beenker codes ([2]) (which can both be seen as quadratic double circulant codes [13]). Extremal self-dual codes are known up to length 64, except for length 52 ([49]). The results obtained by our construction are presented in Table 3. We construct extremal Type III codes up to length 56 except for length 48. The

n	d	construction $(f_i;a;r)$
2	2	(f_1;1;1)
4	2	(f_1;1;1)
6	2	(f_1;1;1)
8	2	(f_1;1;1)
10	2	(f_1;1;1)
12	4	(f_1;1;4)
14	4	(f_1;1;4)
16	4	(f_1;1;4)
18	4	(f_1;1;4)
20	4	(f_1;1;4)
22	6	(f_1;1;20)
24	6	(f_1;1;3)
26	6	(f_1;1;76)
28	6	(f_1;1;4)
30	6	(f_1;1;17)
32	8	(f_1;3;3)
34	6	(f_1;1;10)
36	8	(f_1;1;8)
38	8	(f_1;1;116)
40	8	(f_1;1;8)
42	8	(f_1;1;94)
44	8	(f_1;1;8)
46	8	(f_1;1;10)
48	8	(f_1;1;12)
50	8	(f_1;1;12)
52	10	(f_1;1;19)
54	10	*(f_1;5;9)
56	10	(f_1;1;10)
58	10	(f_1;1;112)
60	12	(f_1;1;78)
62	10	(f_1;1;21)
64	12	(f_1;3;11)
66	12	*(f_1;7;23)
68	12	(f_1;1;11)
70	10	(f_1;1;18)
72	12	(f_1;1;11)
74	12	(f_1;1;234)
76	14	(f_1;65;276)
78	14	*(f_2;61;3820)
80	14	(f_1;43;38)
82	12	(f_1;1;24)
84	14	(f_1;1;14)
86	12	(f_1;1;18)
88	14	(f_1;1;20)
90	14	*(f_1;7;15)
92	14	(f_1;1;21)
94	14	(f_1;1;85)
96	16	(f_1;13;114)
98	14	(f_1;1;36)
100	16	(f_1;1;97)
102	16	*(f_1;5;10)
104	16	(f_1;1;25)
106	14	(f_1;1;21)
108	16	(f_1;1;21)
110	16	(f_1;1;37)
112	16	(f_1;1;20)
114	18	*(f_1;25;75)
116	18	(f_1;1;26)
118	16	(f_1;1;25)
120	18	(f_1;1;112)
122	16	(f_1;1;21)
124	18	(f_1;1;23)
126	18	*(f_1;5;19)
128	18	(f_1;3;27)
130	18	(f_1;1;44)

Table 1: Self-dual codes constructed over $GF(2)$

n	d	Q	Codes, ref	n	d	Q	Codes, ref
60	12	≥ 6	[16],[23] ,Table 1	96	16,18	≥ 1	Table 1
62	12	≥ 1	[23]	98	14,16,18	≥ 1	Table 1,sub
64	12	≥ 5	[12]	100	16,18	≥ 1	Table 1,sub
66	12	≥ 3	[12]	102	18	≥ 1	sub(XQ_{103})
68	12	≥ 65	[12]	104	16,18,20	≥ 1	Table 1
70	12,14	≥ 1	[22]	106	14,16,18	≥ 1	Table 1,sub
72	12,14	≥ 1	[9], Table 1	108	16,18,20	≥ 1	Table 1
74	12,14	≥ 1	Table 1, sub	110	16,18,20	≥ 1	Table 1
76	14	≥ 2	[1],Table 1	112	16,18,20	≥ 1	Table 1, sub
78	14	≥ 50	sub,[1], Table 1, [21]	114	18,20	≥ 1	Table 1
80	14,16	≥ 1	[9], Table 1	116	18,20	≥ 1	Table 1
82	14,16	≥ 1	[12]	118	18,20,22	≥ 1	sub(Ka_{120})
84	14,16	≥ 1	[12], Table 1	120	18,20,22	≥ 1	Table 1
86	16	≥ 1	[12]	122	16-24	≥ 1	Table 1,sub
88	14,16	≥ 1	[12],Table 1	124	18-24	≥ 1	Table 1
90	14,16	≥ 1	[12],Table 1	126	18-24	≥ 1	sub(XQ_{127}),Table 1
92	16	≥ 2	[15],[11]	128	18-24	≥ 1	Table 1
94	14,16,18	≥ 1	[12],Table 1	130	18-24	≥ 1	Table 1

Table 2: Highest weight of Type I codes over $GF(2)$

code of length 52 is the first known for that length. The $[76, 38, 18]$ code is the first code with these parameters. Extremal ternary self-dual codes can be used to construct unimodular lattices and in particular the $[52, 26, 15]$ and $[56, 28, 15]$ codes lead to unimodular lattices of dimensions 52 and 56 with respective norm 5 and 6 ([41],[14]). We also computed the minimum weight of the Pless symmetry code of length 84 (PS_{84}) and the Beenker code of length 88 which both have distance 21 and therefore are not extremal. The codes XQ_{83} and PS_{84} are not equivalent since their automorphism groups are different. All these results are presented in Table 4 which updates the table of [49]. The next possibilities to obtain extremal ternary codes are PS_{96}, PS_{108} and XQ_{107}, in fact we found words in these codes of weights respectively 24, 27 and 27 showing that these codes are not extremal.

For the construction we take $k_2 = 0$ and $B = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. We start from a code with matrix $G = \begin{pmatrix} 1 & 0 & 1 & 1 & & & & & \\ 0 & 1 & 1 & 2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & 1 & 0 & 1 & 1 \\ & & & & & 0 & 1 & 1 & 2 \end{pmatrix}$

6 Self-dual codes over $GF(4)$

6.1 Euclidean case

Euclidean self-dual codes have only been recently considered as more attention was brought to Hermitian self-dual codes (or Type IV codes). In order to preserve Euclidean self-duality two self-dual Euclidean codes are said to be equivalent if they differ only by a permutation. The bound on the weight of Euclidean codes $d(\mathbf{C}) \leq 4\left[\frac{n}{12}\right] + 4$ ([15]) is asymptotically identical to the bound of Type IV codes but, up to now, is not met after length 20. Euclidean self-dual codes have been classified up to length 10 in [33]. The two main known infinite families are the extended quadratic residue codes of length $q+1$ for q a power of an odd prime congruent to 3 modulo 8 ([37]), and the quadratic double circulant codes of lengths $2q+2$ and $2q$ for q a power of an odd prime congruent to -1 modulo 8 ([13]). For certain lengths it also possible to consider duadic codes [44]. Besides these codes few were known with good minimum weight. In Table 5 we give the results we obtained by our construction. One can remark that the codes obtained regularly fill the minimum distance between QR and QDC codes which seems to indicate that the construction is efficient. Some of the codes we obtain even beat the tables by Brouwer [4]. The first table for Euclidean self-dual codes is presented in Table 6. In the case of lengths close to a multiple of 12 the upper bound in the table is the upper on general linear codes by Brouwer [4]. Note also that one can also consider the Gray image of these codes to obtain self-dual binary codes of double length

n	d	construction $(f_i; a; r)$
24	9	(f_1;1;8)
28	9	(f_1;1;8)
32	9	(f_1;1;9)
36	12	(f_2;29;22)
40	12	(f_1;1;59)
44	12	(f_1;1;12)
48	12	(f_1;1;14)
52	15	(f_3;7;187)
56	15	(f_1;43;49)
60	15	(f_1;1;16)
64	15	(f_1;1;16)
68	15	(f_2;3;4)
72	15	(f_2;5;4)
76	18	(f_1;1;35)
80	18	(f_1;1;19)
84	18	(f_1;1;17)
88	18	(f_1;1;17)

Table 3: Self-dual codes constructed over $GF(3)$

n	d	Q	Codes, ref
4	3	1	[10]
8	3	1	[10]
12	6	1	XQ_{11}, [10]
16	6	1	[10]
20	6	6	[47]
24	9	2	XQ_{23},PS_{24} ([35])
28	9	≥ 32	[49]
32	9	≥ 239	[49]
36	12	≥ 1	PS_{36}
40	12	≥ 20	[49]
44	12	≥ 8	[49]
48	15	≥ 2	XQ_{47},PS_{48}
52	15	≥ 1	Table 3
56	15	≥ 1	sub, Table 3
60	18	≥ 2	XQ_{59},PS_{60}
64	18	≥ 1	Be_{64}
68	15 or 18	≥ 1	Table 3
72	18	≥ 1	XQ_{71}
76	18 or 21	≥ 1	Table 3
80	18 or 21	≥ 1	sub, Table 3
84	21 or 24	≥ 2	XQ_{83},PS_{84}
88	21 or 24	≥ 1	Be_{88}

Table 4: Highest weight of self-dual codes over $GF(3)$

([15]). For the matrix M we let ω be in $GF(4)$ such that $\omega^2+\omega+1=0$ and $\omega^3=1$ and take: $B=\begin{pmatrix}1 & \omega\\ \omega & 1\end{pmatrix}$ and $G=\begin{pmatrix}1 & 1 & & & \\ & & 1 & 1 & \\ & & & & \ddots\end{pmatrix}$.

n	d	construction $(f_i;a;r)$	n	d	construction $(f_i;a;r)$
2	2	$(f_i$;1;1)	38	11	$(f_2$;5;74)
4	2	$(f_i$;1;1)	40	12	$(f_1$;1;7)
6	3	$(f_i$;1;2)	42	12	$(f_2$;11;17)
8	4	$(f_i$;1;2)	44	12	$(f_2$;3;11)
10	4	$(f_i$;1;2)	46	13	$(f_2$;35,83)
12	4	$(f_i$;1;2)	48	12	$(f_2$;5;5)
14	6	$(f_i$;1;3)	50	14	$(f_2$;11;14)
16	6	$(f_i$;1;3)	52	14	$(f_2$;3;22)
18	6	$(f_i$;1;3)	54	14	$(f_2$;7;7)
20	6	$(f_i$;1;3)	56	14	$(f_1$;1;15)
22	8	$(f_1$;1;8)	58	15	$(f_1$;1;244)
24	8	$(f_2$;5;6)	60	15	$(f_2$;7;54)
26	8	$(f_1$;1;5)	62	16	$(f_2$;3;14)
28	8	$(f_1$;1;5)	64	16	$(f_1$;5,12)
30	10	$(f_2$;11;15)	66	16	$(f_1$;1,11)
32	10	$(f_2$;13;6)	68	17	$(f_1$;1,145)
34	10	$(f_2$;3;8)	70	18	$(f_1$;43;448)
36	10	$(f_2$;5;21)	72	18	$(f_2$;7;728)

Table 5: Euclidean self-dual codes constructed over $GF(4)$

6.2 Hermitian case

Type IV codes have been classified up to length 16 in [39] and [10]. The weight of these codes is even. Extremal codes of lengths 18 and 20 have been classified in [29]. The main infinite families are still the extended quadratic residue code of length $q+1$ with q a power of an odd prime congruent to 5 modulo 8 and quadratic double circulant codes of lengths $2q+2$ and $2q$ for q a power of an odd prime congruent to 1 modulo 8. In certain cases one may also define duadic codes (see [44]). In Table 7 we give the results we obtained by our construction. The $[28,14,10]$ code we find has an odd automorphism group and is therefore equivalent to one of the code of [26] and [28]. One can remark that as for the Euclidean case the codes obtained regularly fill the minimum distance between QR and QDC codes which seems to indicate that the construction is efficient. Some of the codes we obtain even

n	d	Q	Codes,ref
2	2	1	
4	3	1	XQ_3
6	3	1	[33]
8	4	3	[33]
10	4	4	[33]
12	6	≥ 1	XQ_{11}
14	6	≥ 1	QDC_{14}
16	6	≥ 5	QDC_{16}, [33]
18	6-7	≥ 1	Table 5
20	8	≥ 1	XQ_{19}
22	8	≥ 1	Table 5
24	8-10	≥ 1	Table 5
26	8-10	≥ 1	Table 5
28	9-11	≥ 1	XQ_{27} [37]
30	10-12	≥ 1	Table 5
32	10-12	≥ 1	Table 5
34	10-12	≥ 1	Table 5
36	10-14	≥ 1	Table 5

n	d	Q	Codes,ref
38	11-15	≥ 1	Table 5
40	12-16	≥ 1	Table 5
42	12-16	≥ 1	Table 5
44	14-16	≥ 1	XQ_{43}
46	14-16	≥ 1	QDC_{46}
48	14-18	≥ 1	QDC_{48}
50	14-19	≥ 1	Table 5
52	14-20	≥ 1	Table 5
54	14-20	≥ 1	Table 5
56	14-20	≥ 1	Table 5
58	15-20	≥ 1	Table 5
60	15-23	≥ 1	XQ_{59}, Table 5
62	16-23	≥ 1	QDC_{62}, Table 5
64	16-24	≥ 1	QDC_{64}, Table 5
66	16-24	≥ 1	Table 5
68	18-24	≥ 1	XQ_{67}
70	18-24	≥ 1	Table 5
72	18-28	≥ 1	Table 5

Table 6: Euclidean self-dual codes over $GF(4)$

n	d	construction $(f_i; a; r)$
2	2	$(f_1$;1;1)
4	2	$(f_1$;1;1)
6	4	$(f_1$;1;3)
8	4	$(f_1$;1;3)
10	4	$(f_1$;1;3)
12	4	$(f_1$;1;3)
14	6	$(f_1$;1;6)
16	6	$(f_1$;1;4)
18	6	$(f_1$;1;6)
20	8	$(f_1$;1;5)
22	8	$(f_1$;1;125)
24	8	$(f_1$;1;5)
26	8	$(f_1$;1;11)
28	10	$(f_1$;5;45)
30	8	$(f_1$;1;80)
32	10	$(f_1$;1;7)
34	10	$(f_1$;1;81)
36	10	$(f_1$;1;7)
38	10	$(f_1$;1;9)
40	12	$(f_1$;1;14)
42	10	$(f_1$;1,9)
44	12	$(f_1$;1,10)
46	12	$(f_1$;1,16)
48	14	$(f_2$;17,57)
50	12	$(f_1$;1,11)
52	14	$(f_1$;1,15)
54	14	$(f_1$;1,694)
56	14	$(f_1$;1;11)
58	14	$(f_1$;1;25)
60	16	$(f_1$;1;51)
62	14	$(f_1$;1;14)
64	16	$(f_1$;1;14)
66	16	$(f_1$;1;26)
68	18	$(f_1$;1;1282)
70	18	$(f_1$;1;16)
72	18	$(f_1$; 1;15)

Table 7: Construction of Hermitian self-dual codes over $GF(4)$

beat the tables by Brouwer [4]. An updated table of [49] for Hermitian self-dual codes is presented in Table 8.

For the construction we take: $B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & \omega & \omega^2 & 0 \\ 1 & \omega^2 & \omega & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $G = \begin{pmatrix} 1 & 1 & & & \\ & & 1 & 1 & \\ & & & & \ddots \end{pmatrix}$. In the case where the length is not a multiple of 4 we complete the matrix M by ones.

7 Self-dual code over $GF(5)$

Self-dual codes over $GF(5)$ are studied in [36] by Leon, Pless and Sloane. They classify the codes up to length 12, they also define a notion of extremal code related to weight enumerators but except for small lengths (up to length 16) this notion is unpractical, since the bounds in [4] are better. They also give some examples of construction using Hadamard matrices which have been generalized for length congruent to 2 mod 4 in [13]. In [20] partial classifications of self-dual double circulant codes for lengths $14, 16, 18, 20, 22$ and 24 are done.

n	d	Q	Codes, ref	n	d	Q	Codes, ref
2	2	1	[10]	38	12 or 14	≥ 1	XQ_{37}, [17]
4	2	1	[10]	40	12 or 14	≥ 1	[17],Table 7
6	4	1	XQ_5 , [10]	42	12-16	≥ 1	[44]
8	4	1	[10]	44	12-16	≥ 1	Table 7
10	4	2	[10]	46	12-16	≥ 1	Table 7, sub
12	4	5	[10]	48	14-18	≥ 1	Table 7
14	6	1	[10]	50	12-18	≥ 1	QDC_{50},Table 7,sub
16	6	4	[10]	52	14-18	≥ 1	Table 7, sub
18	8	1	[39],[29]	54	16-20	≥ 1	XQ_{53}
20	8	2	[29]	56	14-20	≥ 1	Table 7
22	8	≥ 46	[26],[28],[32]	58	14-20	≥ 1	Table 7, sub
24	8	≥ 17	[17],[32]	60	16-22	≥ 1	Table 7, sub
26	8 or 10	≥ 49	[17],[32]	62	18-22	≥ 1	XQ_{61}
28	10	≥ 3	[26],[28]	64	16-22	≥ 1	Table 7
30	12	≥ 1	XQ_{29} [39]	66	16-24	≥ 1	Table 7
32	10 or 12	≥ 19	[17],[32]	68	16-24	≥ 1	Table 7, sub
34	10 or 12	≥ 105	QDC_{34},[17],[32]	70	18-24	≥ 1	Table 7
36	12 or 14	≥ 1	QDC_{36},[17]	72	18-26	≥ 1	Table 7

Table 8: Hermitian self-dual codes over $GF(4)$

More recently in [24] the classification was extended to length 16. We now give the exact number of known codes up to equivalence presented in [36],[20] and [13] for small lengths.

For length 14 there are 3 inequivalent $[14,7,6]$ codes: the code R_{14} (equivalent to the code $C_{14,5}$ of [20]), the code $C_{14,4}$ of [20] equivalent to QDC_{14} and the code $C_{14,1}$ of [20]. These three codes have respective automorphism group orders: $48, 168$ and 56. For length 16 the code Q_{16} of [36], the code $C_{16,1}$ of [20] and QDC_{16} are equivalent with an automorphism group order equal to 1344 and there is only one such code [24]. For length 18 the $[18,9,7]$ code of Table 9 is equivalent to the code of [20] and has an automorphism group of order 72. No $[18,9,8]$ code exists [24]. For length 20, 4 inequivalent $[20,10,8]$ codes are known: XQ_{19},QDC_{20} and the codes $C_{20,1}$ (equivalent to $C_{20,3}$) and $C_{20,5}$ of [20] of respective automorphism group orders $13680, 11520, 7680$ and 320. For length 22 at least 6 inequivalent codes are given in [20]. We found at least 10 inequivalent $[22,11,8]$ codes with our construction whose constructions are $\{(f_1;1;73),(f_1;1;17),(f_1;1;34),(f_1;1;21),(f_1;1;4),(f_1;1;6),(f_1;1;59),(f_1;1;44),(f_1;1;27),(f_1;1;28)\}$. A unique code $[24,12,9]$ ([36]) is known, it has an automorphism group of order 10560, it can also be seen as QDC_{24}. The $[26,13,9]$ and $[28,14,10]$ codes of Table 9 are the first self-dual codes with these parameters and have respective automorphism group orders 104 and 112.

No general bounds on the minimum weight are known except the Singleton bound which gives for a $[n, \frac{n}{2}, d]$ code: $d \leq \frac{n}{2}+1$. The best known bounds are then taken in Brouwer's on-line tables [4]. We give in Table 9 the codes obtained by our construction and Table 10 gives the highest minimum distance known for self-dual codes over $GF(5)$.

For this alphabet we let $B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ and $G = \begin{pmatrix} 1 & 2 & & & \\ & & 1 & 2 & \\ & & & & \ddots \end{pmatrix}$.

8 Self-dual codes over $GF(7)$

Self-dual codes over $GF(7)$ have been studied in [48] by Pless and Tonchev. They classify the codes up to length 8. Examples of good double circulant self-dual codes are given in [19]. And recently the classification has been extended to 12 in [25]. For length 20, the codes $C_{20,1}$ and $C_{20,4}$ of [19] are both equivalent to XQ_{19}. Few is known on these codes and no general bounds for the minimum Hamming distance is known except there again the Singleton bound. In the following Table 11 gives the codes obtained by our construction and Table 12 gives the highest minimum weight known for self-dual codes over $GF(7)$. For

n	d	construction $(f_i; a; r)$
2	2	(f_1;1;1)
4	2	(f_1;1;1)
6	4	(f_1;1;2)
8	4	(f_1;1;2)
10	4	(f_1;1;2)
12	4	(f_1;1;2)
14	6	(f_1;1;3)
16	6	(f_1;1;3)
18	7	(f_1;1;9)
20	8	(f_1;1;5)
22	8	(f_1;1;4)
24	8	(f_1;1;4)
26	9	(f_1;1;200)
28	10	(f_1;1;18)
30	10	(f_1;1;9)
32	10	(f_1;1;9)
34	11	(f_2;11;23)

n	d	construction $(f_i; a; r)$
36	12	(f_1;1;110)
38	12	(f_1;1;11)
40	12	(f_1;1;35)
42	12	(f_1;1;9)
44	13	(f_2;5;135)
46	14	(f_1;1;17)
48	14	(f_1;1;95)
50	14	(f_1;1;12)
52	15	(f_1;29;93)
54	16	(f_1;7;174)
56	16	(f_1;1;123)
58	16	(f_1;1;10)
60	16	(f_1;1;12)
62	16	(f_1;1;10)
64	17	(f_1;1;1365)
66	17	(f_1;1;14)
68	18	(f_1;1;20)
70	18	(f_1;1,28)

Table 9: Construction for self-dual codes over $GF(5)$

n	d	Q	Codes,ref
2	2	1	[36]
4	2	1	[36]
6	4	1	[36]
8	4	1	[36]
10	4	3	[36]
12	6	1	XQ_{11}, [36]
14	6	3	QDC_{14},[36],[20],[24]
16	7	1	QDC_{16}, [36], [24]
18	7	≥ 1	[20], [24]
20	8-9	≥ 4	XQ_{19},QDC_{20},[20]
22	8-10	≥ 10	[20], Table 9
24	9-10	≥ 1	QDC_{24}
26	9-11	≥ 1	Table 9
28	10-12	≥ 1	Table 9
30	10-12	≥ 1	Table 9
32	10-13	≥ 1	XQ_{31},Table 9
34	11-14	≥ 1	Table 9

n	d	Q	Codes,ref
36	12-15	≥ 1	Table 9
38	12-16	≥ 1	QDC_{38},Table 9
40	13-17	≥ 1	QDC_{40}
42	12-18	≥ 1	Table 9
44	13-19	≥ 1	Table 9
46	14-20	≥ 1	QDC_{46},Table 9
48	14-20	≥ 1	QDC_{48},Table 9
50	14-20	≥ 1	Table 9
52	15-21	≥ 1	Table 9
54	16-22	≥ 1	Table 9
56	16-23	≥ 1	Table 9
58	16-24	≥ 1	QDC_{58},Table 9,sub
60	18-24	≥ 2	XQ_{59},QDC_{60}
62	16-25	≥ 1	QDC_{62}, sub
64	18-26	≥ 1	QDC_{64}
66	16-27	≥ 1	Table 9
68	18-28	≥ 1	Table 9
70	18-29	≥ 1	Table 9

Table 10: Table of self-dual codes over $GF(5)$

our construction we let $B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ and $G = \begin{pmatrix} 1 & 0 & 2 & 3 & & & & & \\ 0 & 1 & 4 & 2 & & & & & \\ & & & & 1 & 0 & 2 & 3 & \\ & & & & 0 & 1 & 4 & 2 & \\ & & & & & & & & \ddots \end{pmatrix}$.

n	d	construction $(f_i; a; r)$
4	3	(f_1;1;1)
8	4	(f_1;1;2)
12	6	(f_1;1;3)
16	6	(f_1;1;3)
20	8	(f_1;1;10)
24	9	(f_1;1;25)
28	10	(f_1;1;11)
32	11	(f_1;1;54)
36	12	(f_1;1;32)
40	13	(f_1;1;74)
44	14	(f_1;1;26)
48	15	(f_1;1;94)
52	15	(f_1;1;11)
56	16	(f_1;1;10)

Table 11: Codes obtained over $GF(7)$

9 New weights of extended quadratic residue codes

In this section we update the tables of minimum weight of quadratic residue codes over $GF(4), GF(5)$ and $GF(7)$. A '?' in the tables indicates the weight obtained before the computation could finish.

•$GF(4)$

In table 13 we give the minimum weights of the extended quadratic residue codes over $GF(4)$ up to length 68. The weights for lengths 62 and 68 were not previously known. We also correct the weights for lengths 44 and 54 incorrectly reported in [31]. Extended quadratic residue codes of length $n = p + 1$ are Euclidean self-dual when $p = 3 \bmod 8$ and Hermitian self-dual when $p = 5 \bmod 8$ (see [44]).

•$GF(5)$

n	d	Q	Codes
4	3	1	[48]
8	5	1	QDC_8, [48]
12	6	8	QDC_{12}, [19], [25]
16	7-8	≥ 1	[19]
20	9-10	≥ 1	XQ_{19}
24	9-11	≥ 1	QDC_{24}
28	10-13	≥ 1	QDC_{28}, Table 11,sub
32	13-14	≥ 1	XQ_{31}
36	12-16	≥ 1	QDC_{36}, Table 11
40	13-18	≥ 1	QDC_{40}, Table 11
44	14-19	≥ 1	Table 11,sub
48	17-21	≥ 1	XQ_{47}
52	15-23	≥ 1	Table 11
56	16-29	≥ 1	Table 11

Table 12: Highest weight of self-dual codes over $GF(7)$

The weights of the quadratic residue codes over $GF(5)$ were known up to length 32, we extend the table up to length 62. The codes of lengths 20 and 60 are self-dual.

•$GF(7)$

The weights of the quadratic residue codes over $GF(7)$ were known up to length 32, we extend the table up to length 54. Using the notation of [13] the extended quadratic residue codes over $GF(7)$ of lengths $20, 32$ and 48 with respective generator matrices the extensions of $Q_{19}(0,1,4), Q_{31}(0,2,3)$ and $Q_{47}(0,1,4)$ are self-dual.

References

[1] A. Baartmans and V. Yorgov, "Some new extremal codes of length 76 and 78", *Proc. 7th Int. Workshop Alg. and Combin. Coding Theory, 18-24 June, Bulgaria*, (2000), pp. 51-54.

[2] G. Beenker, "A note on Extended Quadratic Residue Codes over GF(9) and Their Ternary Images ", *IEEE Trans. Inform. Theory* **30**, (1984), pp. 403-405.

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

n	d
6	4
12	6
20	8
30	12
38	12
44	14
54	16
60	15
62	18
68	18
84	23?

Table 13: Extended Quadratic Residue Codes over $GF(4)$

n	d
12	6
20	8
30	12
32	10
42	14
60	18
62	20
72	22?

Table 14: Extended Quadratic Residue Codes over $GF(5)$

n	d
8	4
20	9
30	12
32	13
38	12
48	17
54	18
60	20?

Table 15: Extended Quadratic Residue Codes over $GF(7)$

[4] A.E. Brouwer, "Bounds on the size of linear codes", *Handbook of coding theory*, edited by V. Pless and W.C. Huffman, North Holland, 1998.

[5] J.C. Carlach, A.Otmani, and C.Vervoux, "A new scheme for building good self-dual block codes," *in Proc. 2000 IEEE Int. Symp. on Information Theory (ISIT 2000)*, Sorrento, Italy, 25-30 June 2000, pp. 476.

[6] J-C. Carlach and A. Otmani, "A systematic construction of self-dual codes", *submitted to IEEE Inf. Theory.*

[7] J.C. Carlach, C.Vervoux, "A new family of block Turbo-Codes," *Proc. 13th Applicable Algebra in Engineering Communication and Computing (AAECC 13)*, Hawaii, USA, 14-19 November 1999, pp. 15.

[8] J.H. Conway and V. S. Pless, "On the enumeration of self-dual codes", *J. Combin. Theory Ser. A* **28** (1980), pp. 26-53.

[9] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimum distance of self-dual codes", *IEEE Trans. Inform. Theory* **36**, (1990), pp. 1319-1333.

[10] J.H. Conway, V. Pless and N.J.A. Sloane, "Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16", *IEEE Trans. Inform. Theory*, **25**, (1979), pp. 312-322.

[11] , Dontcheva, personal communication.

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

[13] P. Gaborit, "Quadratic Double Circulant Codes over Fields" *to appear in J. Combin. Theory Ser. A.*

[14] P. Gaborit, "Construction of extremal unimodular lattices" *preprint.*

[15] P. Gaborit, V. Pless, P. Solé and A.O.L. Atkin, "Type II codes over F_4", *to appear in Finite Fields and Applications.*

[16] T. A. Gulliver and M. Harada, "Weight enumerators of extremal singly-even $[60, 30, 12]$ codes", *IEEE Trans. Inform. Theory*, **42**, (1996), pp. 658-659.

[17] T. A. Gulliver, "Optimal double circulant self-dual codes over F_4" , *IEEE Trans. Inform. Theory*, **46**, (2000), pp. 271-274.

[18] T. A. Gulliver, M. Harada and H. Kaneta, "Classification of extremal double circulant self-dual codes of length up to 62",*Discrete Math.*, **188**,(1998), pp. 127-136.

[19] T. A. Gulliver and M. Harada, "New optimal self-dual codes over GF(7)",*Graphs & Combin.*, **15**,(1999), pp. 175-186.

[20] T. A. Gulliver and M. Harada, "Double-circulant self-dual codes over GF(5)", *Graphs & Combin.*, **56**,(2000), pp. 3-13.

[21] T. A. Gulliver, M. Harada and J-L. Kim, "Construction of new extremal self-dual codes", *preprint*.

[22] M. Harada, "The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes", *Finite Fields and Their Appl.*, **3**, (1996), pp. 131-139.

[23] M. Harada, "Construction of an extremal self-dual code of length 62", *IEEE Trans. Inform. Theory*, **45**, (1999), pp. 1232-1233.

[24] M. Harada and P. Ostergard, "On the classification of self-dual codes over F_5", *preprint*.

[25] M. Harada and P. Ostergard, "Self-dual and Maximal Self-Orthogonal Codes over F_7", *preprint*.

[26] W. C. Huffman, "On extremal self-dual quaternary codes of length 18 to 28,I", *IEEE Trans. Inform. Theory*, **36**, (1990), pp. 651-660.

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

[28] W. C. Huffman, "On extremal self-dual quaternary codes of length 18 to 28,I", *IEEE Trans. Inform. Theory*, **37**, (1991), prp. 1206-1216.

[29] W. C. Huffman, "Characterization of quaternary extremal codes of lengths 18 and 20", *IEEE Trans. Inform. Theory*, **43**, (1997), pp. 316-319.

[30] M. Karlin, " New binary coding results by circulant", *IEEE Trans. Inform. Theory* **15**, (1969), pp. 81-92.

[31] M. Karlin, V. K. Bhargava, and S. E. Tavares, "A note on extended quadratic residue code and their binary images", *Inform. Contr.*, **38** (1978), pp. 148-153.

[32] J.-L. Kim, "New self-dual codes over $GF(4)$ with the highest known minimum weights", *IEEE Trans. Inform. Theory* **47**, (2001), pp. 1575-1580.

[33] D. K. Kim, H. K. Kim and J.-L. Kim, "New extremal type I codes over $GF(4)$", *preprint*.

[34] J.S. Leon, J.M. Masley and V.S. Pless, "Duadic codes", *IEEE Trans. Inform. Theory*, **30**, (1984), pp. 709-714.

[35] J.S. Leon, V. S. Pless and N.J.A. Sloane, "On ternary self-dual codes of length 24", *IEEE Trans. Inform. Theory*, **27**, (1981), pp. 176-180.

[36] J.S. Leon, V. S. Pless and N.J.A. Sloane, "Self-dual codes over GF(5)" *J. Combin. Theory Ser. A* **32** (1982), pp. 178-194.

[37] J. H. van Lint and F. J. MacWilliams, "Generalized quadratic residue codes", *IEEE Trans. Inform. Theory*, **24**, (1978), pp. 730-737.

[38] F.J. MacWilliams, "Orthogonal circulant matrices over finite fields and how to find them", *J. Combin. Theory Ser. A* **10** (1971), pp. 1-17.

[39] F.J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane and H. N. Ward, "Self-dual codes over $GF(4)$", *J. Combin. Theory Ser. A* **25** (1978), pp. 288-318.

[40] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam 1977.

[41] M. Ozeki, "Ternary code construction of even unimodular lattices", *Conf. Inter. Theorie des Nomb., Univ. Laval, Quebec, 5-18 juillet 1987*, pp. 772-784.

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

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

[44] V. Pless, "Q-Codes", *J. Combin. Theory Ser. A* **43** (1986), pp. 258-276.

[45] V. Pless, "Coding Constructions", *Handbook of coding theory*, edited by V. Pless and W.C. Huffman, North Holland, 1998.

[46] 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.

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

[48] V. S. Pless and V. D. Tonchev, "Self-dual codes over GF(7)", *IEEE Trans. Inform. Theory* **33**, (1987), pp. 723-727.

[49] 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.