AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **35** (2006), Pages 57–67

Orthogonal designs and MDS self-dual codes

Masaaki Harada

Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560
Japan

Hadi Kharaghani

Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, AB
Canada T1K 3M4

Abstract

Orthogonal designs and generalized orthogonal designs are shown to be useful in construction of self-dual codes over large fields. For lengths $8, 10, 12$ and 16, MDS self-dual codes over large fields are constructed from some orthogonal designs and generalized orthogonal designs. For length 14, some MDS self-dual codes over large fields are also constructed.

1 Introduction

An $[n,k]_p$ code C (or an $[n,k]$ $\mathbb{F}_p$-code) is a k-dimensional vector subspace of $\mathbb{F}_p^n$ where $\mathbb{F}_p$ denotes the finite field of odd prime order p. The elements of C are called codewords and the (Hamming) weight $\mathrm{wt}(x)$ of a codeword x is the number of non-zero coordinates in x. The minimum weight of C is defined as $\min\{\mathrm{wt}(x)|0 \neq x \in C\}$. An $[n,k,d]_p$ (resp. $[n,k,d]$) code is an $[n,k]_p$ (resp. $[n,k]$) code with minimum weight d. A matrix whose rows are linearly independent and generate the code C is called a generator matrix of C. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_p^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y$ denotes the standard inner product. A code C is *self-dual* if $C = C^\perp$. A self-dual $[n, n/2]$ code is called a self-dual code of length n. A self-dual $\mathbb{F}_p$-code of length n exists iff n is even for $p \equiv 1 \pmod 4$, and $n \equiv 0 \pmod 4$ for $p \equiv 3 \pmod 4$ (cf. [9, Chapter 19]). By the Singleton bound, $d \leq n - k + 1$. A code meeting the Singleton bound is called MDS (cf. e.g., [9]). In this sense, MDS codes are optimal. We refer the reader to [9] for more details and terminologies on codes.

An *orthogonal design* of order n and of type $(s_1, s_2, \ldots, s_u)$ $(s_i > 0)$, denoted $OD(n; s_1, s_2, \ldots, s_u)$, on the commuting variables $x_1, x_2, \ldots, x_u$ is an n by n matrix

A with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_u\}$ such that

$$AA^t = \left(\sum_{i=1}^{u} s_i x_i^2 \right) I,$$

where A^t denotes the transpose of A and I is the identity matrix of order n. We refer the reader to [5] for details on orthogonal designs. Let B be an n by n matrix on the commuting variables $x_1, x_2, \ldots, x_t$ where each variable appears in each row or column in the form $\pm a_{ij} x_i$, $i = 1, 2, \ldots, t$, $j = 1, 2, \ldots, u_i$ and $\sum_{i=0}^{t} u_i = n$ where u_0 is the number of 0's in each row or column. Then B is called a *generalized orthogonal design* if

$$BB^t = \left(\sum_{i=1}^{t} s_i x_i^2 \right) I,$$

where $s_i = \sum_{j=1}^{u_i} a_{ij}^2$ (cf. [3]).

Recently some authors like [3] and [7] have constructed MDS self-dual codes over large finite fields $\mathbb{F}_p$ ($p \geq 31$) for small lengths. More precisely, MDS self-dual codes of lengths $4, 8, 12$ for $p = 31$ and MDS self-dual codes of lengths $2n \leq 14$ for $p = 37$ are constructed in [3] and MDS self-dual codes of lengths $2n \leq 10$ for $p = 41$, are constructed in [7]. In particular, in [3], using orthogonal designs and generalized orthogonal designs, MDS self-dual codes are constructed. It is well known that symmetric designs can be used to construct binary self-dual codes. In addition, Hadamard matrices and weighing matrices can be used to construct ternary self-dual codes (cf. e.g., [13] and the references therein). For a larger alphabet, it is natural to adopt orthogonal designs instead of these matrices.

In this paper, we give some generalized orthogonal designs. Using some orthogonal designs and generalized orthogonal designs, MDS self-dual codes over large fields are constructed for lengths $8, 10, 12$ and 16. More precisely, it is shown that an MDS self-dual $[8, 4, 5]_p$ code exists if $p \leq 499$ and $p \neq 3, 5$, that an MDS self-dual $[10, 5, 6]_p$ code exists if $p \leq 499$ ($\equiv 1 \pmod 4$) and $p \neq 5$, and that an MDS self-dual $[12, 6, 7]_p$ code exists for $19 \leq p \leq 499$. For lengths 14 and 16, MDS self-dual $\mathbb{F}_p$-codes are constructed for many prime numbers p.

2 MDS Self-Dual [8, 4, 5] Codes

In this section, we construct some MDS self-dual codes of length 8 using an orthogonal design of order 4.

The following matrix

$$M = \begin{pmatrix} a & b & a & c \\ -b & a & c & -a \\ -a & -c & a & b \\ -c & a & -b & a \end{pmatrix}$$

is an $OD(4; 2, 1, 1)$. By replacing a, b, c in the generator matrix (I , M) by some elements s, t, u of $\mathbb{F}_p$, we have self-dual $\mathbb{F}_p$-codes of length 8 denoted by $C_{8,p}(s, t, u)$ if $1 + 2s^2 + t^2 + u^2 = 0$.

Table 1: MDS self-dual $[8,4,5]$ codes

p	(s,t,u)	p	(s,t,u)	p	(s,t,u)	p	(s,t,u)	p	(s,t,u)
41	$(1,1,18)$	43	$(1,2,6)$	47	$(1,4,13)$	53	$(1,1,7)$	59	$(1,6,16)$
61	$(1,1,22)$	67	$(1,2,23)$	71	$(1,2,8)$	73	$(1,1,19)$	79	$(1,2,25)$
83	$(1,4,8)$	89	$(1,1,21)$	97	$(1,1,44)$	101	$(1,1,20)$	103	$(1,3,20)$
107	$(1,2,10)$	109	$(1,1,43)$	113	$(1,1,30)$	127	$(1,2,45)$	131	$(1,4,51)$
137	$(1,1,63)$	139	$(1,3,31)$	149	$(1,1,61)$	151	$(1,2,12)$	157	$(1,1,56)$
163	$(1,2,51)$	167	$(1,6,63)$	173	$(1,1,13)$	179	$(1,2,72)$	181	$(1,1,38)$
191	$(1,2,39)$	193	$(1,1,31)$	197	$(1,1,28)$	199	$(1,3,28)$	211	$(1,2,41)$
223	$(1,3,65)$	227	$(1,6,85)$	229	$(1,1,15)$	233	$(1,1,55)$	239	$(1,2,94)$
241	$(1,1,113)$	251	$(1,4,105)$	257	$(1,1,32)$	263	$(1,2,16)$	269	$(1,1,105)$
271	$(1,3,114)$	277	$(1,1,120)$	281	$(1,1,106)$	283	$(1,3,105)$	293	$(1,1,17)$
307	$(1,3,70)$	311	$(1,4,35)$	313	$(1,1,50)$	317	$(1,1,89)$	331	$(1,2,18)$
337	$(1,1,41)$	347	$(1,2,149)$	349	$(1,1,77)$	353	$(1,1,84)$	359	$(1,2,102)$
367	$(1,3,33)$	373	$(1,1,165)$	379	$(1,2,55)$	383	$(1,6,55)$	389	$(1,1,159)$
397	$(1,1,126)$	401	$(1,1,40)$	409	$(1,1,123)$	419	$(1,4,20)$	421	$(1,1,58)$
431	$(1,2,83)$	433	$(1,1,75)$	439	$(1,3,192)$	443	$(1,2,128)$	449	$(1,1,134)$
457	$(1,1,218)$	461	$(1,1,96)$	463	$(1,2,161)$	467	$(1,4,43)$	479	$(1,4,192)$
487	$(1,2,207)$	491	$(1,2,22)$	499	$(1,2,196)$				

It was verified in [3] that $C_{8,31}(1,3,9)$ is an MDS self-dual $[8,4,5]_{31}$ code and $C_{8,37}(1,12,1)$ is an MDS self-dual $[8,4,5]_{37}$ code. We have found more MDS self-dual codes $C_{8,p}(s,t,u)$ for all prime numbers p $(41 \le p \le 499)$. The values (s,t,u) are listed in Table 1. All calculations for the minimum weights and the self-duality were done by MAGMA. We have ended our search at prime number $p = 499$. It is not difficult to continue the search for larger fields, but it is rather impractical to do so and thus $p = 499$ is a good place to stop the search. Note that the weight distribution of an MDS code is completely determined [9, Chapter 11], thus we do not list the weight distributions of our codes. Some MDS self-dual $\mathbb{F}_p$-codes can be also found in [7] for $p = 41, 53$.

It is known that no MDS self-dual $[8,4,5]_p$ code exists if $p = 3,5$ and an MDS self-dual $[8,4,5]_p$ code exists if $p = 7,11,13,17,19,23,29$ ([1], [8], [10], [11]). Hence we have the following:

Proposition 1. *Suppose that p is an odd prime number ≤ 499. An MDS self-dual $[8,4,5]_p$ code exists if and only if $p \ne 3,5$.*

3 MDS Self-Dual [10, 5, 6] Codes

We need the following easy lemma.

Lemma 2. *An orthogonal design M of order n, $n \ne 1,2$ and $n \not\equiv 0 \pmod 4$ has zero entries and thus any $[2n,n]_p$ code with generator matrix $(\ I\ ,\ M\ )$ obtained by replacing the variables in M with elements of $\mathbb{F}_p$ cannot become a (self-dual) MDS code.*

Hence, in this section, we construct MDS self-dual codes from generalized orthogonal designs. The following matrix

$$M_{5,1} = \begin{pmatrix} 24a & 48a & -16a & 24a & 3a \\ -3a & 24a & 48a & -16a & 24a \\ -24a & -3a & 24a & 48a & -16a \\ 16a & -24a & -3a & 24a & 48a \\ -48a & 16a & -24a & -3a & 24a \end{pmatrix}$$

is a generalized orthogonal design $GOD(5; 3, 16, 24, 24, 48)$ which is a negacyclic matrix. Recall that an m by m negacyclic matrix has the form

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ -r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ -r_{m-2} & -r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ -r_1 & -r_2 & -r_3 & \cdots & r_0 \end{pmatrix}.$$

By replacing a in the generator matrix $(I \ , \ M_{5,1})$ by some element s of $\mathbb{F}_p$, we have found MDS self-dual codes $C_{10,p}(s)$ for all prime numbers p with $37 \leq p \leq 499$ except $p \neq 61$. The values s are listed in Table 2.

Table 2: MDS self-dual $[10, 5, 6]$ codes $C_{10,p}(s)$

p	s	p	s	p	s	p	s	p	s	p	s
37	9	41	18	53	17	73	16	89	33	97	6
101	25	109	47	113	41	137	59	149	74	157	33
173	24	181	62	193	5	197	3	229	2	233	10
241	5	257	84	269	116	277	108	281	93	293	89
313	133	317	111	337	19	349	48	353	128	373	124
389	30	397	25	401	118	409	58	421	104	433	152
449	205	457	193	461	37						

We now give an infinite family of generalized orthogonal designs of order 5.

Proposition 3. *Let $M_{5,2}$ be the negacyclic matrix with first row*

$$(-(a^2+2a)(a+1), (a^2-a-1)(a+1), (a^2+2a)(a+1), \\ -a(a^2+2a), a(a^2+2a)(1+a)).$$

Then $M_{5,2}$ is a generalized orthogonal design of order 5.

Proof. This follows from the fact that

$$M_{5,2}M_{5,2}^t = (1 + 4a + 12a^2 + 22a^3 + 30a^4 + 28a^5 + 17a^6 + 6a^7 + a^8)I.$$

□

Table 3: MDS self-dual $[10, 5, 6]$ codes $D_{10,p}(s)$

p	s	p	s	p	s	p	s	p	s	p	s
37	34	53	17	61	1	73	30	97	45	101	72
109	42	113	27	137	19	149	40	173	15	181	78
193	68	197	43	229	27	233	37	269	125	277	126
281	198	293	220	313	100	317	173	337	248	349	263
353	144	389	120	397	137	401	38	409	28	433	36
449	43	457	359								

By replacing a in the generator matrix $(\ I\ ,\ M_{5,2}\ )$ by some element s of $\mathbb{F}_p$, we have found MDS self-dual codes $D_{10,p}(s)$ for many prime numbers p $(37 \le p \le 499)$. The values s are listed in Table 3.

It is well known that no MDS self-dual $[10, 5, 6]_p$ code exists if $p = 5$ [8] and an MDS self-dual $[10, 5, 6]_p$ code exists if $p = 13, 17, 29$ [1]. Some MDS self-dual $\mathbb{F}_p$-codes can be also found in [3] and [7] for $p = 37, 41, 53$. From the codes found in this section, we have the following:

Proposition 4. *Suppose that p is an odd prime number ≤ 499 and $p \equiv 1 \pmod 4$. An MDS self-dual $[10, 5, 6]_p$ code exists if and only if $p \ne 5$.*

4 MDS Self-Dual [12, 6, 7] Codes

In this section, we first give an infinite family of generalized orthogonal designs of order 6. Then they are used to construct MDS self-dual codes.

Proposition 5. *Suppose that $a = bd - cb - dc - 6$. Then the following matrix*

$$M_{6,1} = \begin{pmatrix} ax & 3x & 2x & bx & cx & dx \\ -2x & ax & 3x & -dx & bx & cx \\ -3x & -2x & ax & -cx & -dx & bx \\ -bx & dx & cx & ax & -2x & -3x \\ -cx & -bx & dx & 3x & ax & -2x \\ -dx & -cx & -bx & 2x & 3x & ax \end{pmatrix}$$

is a generalized orthogonal design of order 6.

Proof. We find that $M_{6,1}M_{6,1}^t = (a^2+b^2+c^2+d^2+13)x^2 I$ from the assumption that $a = bd - cb - dc - 6$. □

By replacing a, b, c, d, x in the generator matrix $(\ I\ ,\ M_{6,1}\ )$ by some elements of $\mathbb{F}_p$, we have self-dual $\mathbb{F}_p$-codes of length 12 denoted by $C_{12,p}(a, b, c, d, x)$ if $(a^2 + b^2 + c^2 + d^2 + 13)x^2 + 1 = 0$. We have found MDS self-dual codes $C_{12,p}(a, b, c, d, x)$ for all prime numbers p $(31 \le p \le 499)$ where $a = bd - cb - dc - 6$. For the primes numbers p, the codes satisfy $b = 1$ and thus we list the values (c, d, x) in Table 4. For $p = 31, 37$, our MDS self-dual $[12, 6, 7]$ codes have larger minimum weights than the codes in [4, Table 2].

Table 4: MDS self-dual $[12, 6, 7]$ codes

p	(c, d, x)	p	(c, d, x)	p	(c, d, x)	p	(c, d, x)
31	$(2, 29, 15)$	37	$(2, 2, 11)$	41	$(2, 2, 1)$	43	$(1, 7, 11)$
47	$(2, 7, 22)$	53	$(1, 12, 26)$	59	$(1, 5, 23)$	61	$(2, 7, 13)$
67	$(1, 7, 4)$	71	$(1, 2, 33)$	73	$(1, 5, 25)$	79	$(1, 2, 6)$
83	$(1, 5, 22)$	89	$(1, 2, 27)$	97	$(1, 3, 44)$	101	$(1, 2, 7)$
103	$(1, 3, 39)$	107	$(1, 2, 15)$	109	$(1, 3, 18)$	113	$(1, 9, 25)$
127	$(1, 5, 25)$	131	$(1, 2, 24)$	137	$(1, 2, 31)$	139	$(1, 2, 66)$
149	$(1, 2, 33)$	151	$(1, 3, 53)$	157	$(1, 2, 40)$	163	$(1, 2, 71)$
167	$(1, 2, 19)$	173	$(1, 3, 52)$	179	$(1, 3, 75)$	181	$(1, 3, 32)$
191	$(1, 3, 15)$	193	$(1, 8, 22)$	197	$(1, 10, 20)$	199	$(1, 2, 26)$
211	$(1, 5, 8)$	223	$(1, 7, 51)$	227	$(1, 2, 64)$	229	$(1, 2, 60)$
233	$(1, 5, 97)$	239	$(1, 3, 6)$	241	$(1, 7, 89)$	251	$(1, 8, 10)$
257	$(1, 2, 88)$	263	$(1, 3, 67)$	269	$(1, 3, 96)$	271	$(1, 3, 40)$
277	$(1, 5, 100)$	281	$(1, 2, 93)$	283	$(1, 2, 107)$	293	$(1, 2, 39)$
307	$(1, 3, 85)$	311	$(1, 2, 47)$	313	$(1, 7, 6)$	317	$(1, 3, 63)$
331	$(1, 3, 125)$	337	$(1, 7, 29)$	347	$(1, 2, 103)$	349	$(1, 2, 137)$
353	$(1, 2, 39)$	359	$(1, 5, 11)$	367	$(1, 2, 134)$	373	$(1, 2, 76)$
379	$(1, 2, 163)$	383	$(1, 5, 163)$	389	$(1, 2, 179)$	397	$(1, 3, 22)$
401	$(1, 3, 104)$	409	$(1, 2, 64)$	419	$(1, 2, 97)$	421	$(1, 2, 69)$
431	$(1, 2, 197)$	433	$(1, 2, 196)$	439	$(1, 2, 70)$	443	$(1, 3, 209)$
449	$(1, 5, 59)$	457	$(1, 2, 25)$	461	$(1, 2, 38)$	463	$(1, 9, 200)$
467	$(1, 3, 37)$	479	$(1, 2, 233)$	487	$(1, 2, 173)$	491	$(1, 3, 127)$
499	$(1, 2, 114)$						

Proposition 6. *Suppose that p is an odd prime number $19 \leq p \leq 499$. Then an MDS self-dual $[12, 6, 7]_p$ code exists.*

Remark 7. It is known that no MDS self-dual $[12, 6, 7]_p$ code exists if $p = 3, 5, 7$ and an MDS self-dual $[12, 6, 7]_p$ code exists if $p = 11, 19, 23, 29$ ([1], [6], [8], [10]). For $p = 31, 37$, MDS self-dual $[12, 6, 7]_p$ codes can be constructed from some generalized orthogonal designs [3]. Note that $GOD(6; 1, 3, 3, 6, 13, 15)$ given in [3, p. 466] contains the misprints in their entries and the $(3, 5)$- and $(3, 6)$-entries in the matrix should be $3a$ and $-13a$, respectively.

5 MDS Self-Dual [14, 7, 8] Codes

We have found generalized orthogonal designs of order 7. As an example, we give a generalized orthogonal design $GOD(7; 2, 3, 8, 10, 14, 18)$ below:

$$M_{7,1} = \begin{pmatrix} -18a & -12a & -8a & 14a & -10a & 3a & 2a \\ 2a & -18a & -12a & -8a & 14a & -10a & 3a \\ 3a & 2a & -18a & -12a & -8a & 14a & -10a \\ -10a & 3a & 2a & -18a & -12a & -8a & 14a \\ 14a & -10a & 3a & 2a & -18a & -12a & -8a \\ -8a & 14a & -10a & 3a & 2a & -18a & -12a \\ -12a & -8a & 14a & -10a & 3a & 2a & -18a \end{pmatrix}.$$

Using generalized orthogonal designs with no zero entries, we were able to construct some self-dual codes. However, we were unable to find any self-dual code with minimum weight 7 or 8. To remedy this, we considered generalized orthogonal designs having one zero entry as follows:

$$M_{7,2} = \begin{pmatrix} 16a & 12a & -8a & -13a & 8a & -12a & 0 \\ 0 & 16a & 12a & -8a & -13a & 8a & -12a \\ 12a & 0 & 16a & 12a & -8a & -13a & 8a \\ -8a & 12a & 0 & 16a & 12a & -8a & -13a \\ 13a & -8a & 12a & 0 & 16a & 12a & -8a \\ 8a & 13a & -8a & 12a & 0 & 16a & 12a \\ -12a & 8a & 13a & -8a & 12a & 0 & 16a \end{pmatrix}.$$

Let $C_{14,p}(s)$ be the code with generator matrix $(\ I\ ,\ M_{7,2}\ )$ after replacing a in the matrix by some element s of $\mathbb{F}_p$. The code $C_{14,p}(s)$ cannot become an MDS code but we have found self-dual $[14,7,7]$ codes for many prime numbers with $13 \le p \le 499$ and $p \equiv 1 \pmod 4$ and the values s are listed in Table 5. Note that no self-dual $[14,7,7]$ code can be obtained in this way for the other prime numbers.

Table 5: Self-dual $[14,7,7]$ codes $C_{14,p}(s)$

p	s	p	s	p	s	p	s	p	s	p	s
53	12	61	13	73	11	89	38	101	31	113	20
137	6	149	55	173	39	181	68	193	76	197	82
229	20	233	13	241	77	257	36	269	25	277	103
281	66	293	126	313	98	317	7	337	53	349	113
353	111	373	35	389	157	397	98	401	56	409	122
421	1	433	173	449	168	457	12	461	205		

A *double circulant* code has a generator matrix of the form $(\ I\ ,\ R\ )$ where R is an n by n circulant matrix. An MDS self-dual $[14,7,8]_p$ code can be found in [1] and [3] for $p = 13$ and 37, respectively, by this construction method. In this paper, we construct MDS self-dual $[14,7,8]_p$ codes for $29 \le p \le 499$ and $p \equiv 1 \pmod 4$ as double circulant codes. The first rows r for R in the generator matrices are listed in Table 6. We have the following:

Proposition 8. *Suppose that p is an odd prime number with $29 \le p \le 499$ and $p \equiv 1 \pmod 4$. Then an MDS self-dual $[14,7,8]_p$ code exists.*

Table 6: Double circulant MDS self-dual $[14, 7, 8]$ codes

p	r	p	r
29	$(1, 3, 23, 19, 25, 27, 6)$	37	$(1, 1, 4, 26, 31, 11, 31)$
41	$(1, 1, 3, 26, 20, 38, 25)$	53	$(1, 1, 12, 29, 27, 25, 34)$
61	$(1, 1, 9, 50, 19, 8, 23)$	73	$(1, 1, 9, 47, 57, 29, 48)$
89	$(1, 1, 10, 46, 53, 84, 38)$	97	$(1, 1, 5, 76, 65, 93, 72)$
101	$(41, 34, 98, 24, 98, 100, 100)$	109	$(1, 1, 3, 101, 8, 51, 86)$
113	$(23, 47, 9, 15, 2, 1, 1)$	137	$(1, 1, 2, 19, 51, 136, 27)$
149	$(52, 33, 53, 120, 147, 148, 148)$	157	$(1, 1, 2, 33, 39, 32, 21)$
173	$(1, 1, 2, 76, 140, 161, 58)$	181	$(1, 1, 3, 58, 128, 85, 105)$
193	$(1, 1, 2, 7, 131, 82, 50)$	197	$(1, 1, 2, 74, 92, 84, 154)$
229	$(1, 1, 2, 42, 110, 9, 186)$	233	$(1, 1, 2, 62, 87, 185, 217)$
241	$(1, 1, 2, 48, 227, 56, 83)$	257	$(1, 1, 2, 105, 66, 155, 200)$
269	$(1, 1, 2, 54, 114, 164, 15)$	277	$(1, 1, 2, 141, 94, 61, 194)$
281	$(1, 1, 2, 117, 65, 137, 11)$	293	$(1, 1, 2, 7, 217, 257, 256)$
313	$(1, 1, 4, 121, 65, 162, 297)$	317	$(1, 1, 2, 146, 70, 83, 217)$
337	$(1, 1, 3, 230, 54, 119, 118)$	349	$(1, 1, 2, 20, 88, 332, 41)$
353	$(1, 1, 3, 231, 72, 129, 227)$	373	$(1, 1, 2, 223, 335, 238, 215)$
389	$(1, 1, 2, 181, 64, 248, 7)$	397	$(1, 1, 2, 69, 88, 301, 269)$
401	$(1, 1, 3, 89, 395, 308, 25)$	409	$(1, 1, 2, 23, 161, 346, 141)$
421	$(1, 1, 3, 21, 41, 332, 414)$	433	$(1, 1, 2, 227, 306, 187, 321)$
449	$(1, 1, 2, 136, 231, 19, 441)$	457	$(1, 1, 2, 116, 34, 149, 45)$
461	$(1, 1, 2, 134, 403, 202, 131)$		

6 MDS Self-Dual [16, 8, 9] Codes

The following matrix

$$M_{8,1} = \begin{pmatrix} 3a & -4b & -4b & 3a & 4b & 3a & 4b & 3a \\ -4b & 3a & 3a & -4b & 3a & 4b & 3a & 4b \\ 4b & -3a & 3a & -4b & 4b & 3a & -4b & -3a \\ -3a & 4b & -4b & 3a & 3a & 4b & -3a & -4b \\ -4b & -3a & -4b & -3a & 3a & -4b & -4b & 3a \\ -3a & -4b & -3a & -4b & -4b & 3a & 3a & -4b \\ -4b & -3a & 4b & 3a & 4b & -3a & 3a & -4b \\ -3a & -4b & 3a & 4b & -3a & 4b & -4b & 3a \end{pmatrix}$$

is a generalized orthogonal design [3]. By replacing a, b in the generator matrix $(\ I\ ,\ M_{8,1}\ )$ with some elements s, t of $\mathbb{F}_p$, we have $\mathbb{F}_p$-codes $C_{16,p}(s, t)$ of length 16. It was verified in [3] that $C_{16,11}(2, 1)$ is a self-dual $[16, 8, 8]_{11}$ code. In general, we have the following:

Proposition 9. *The code $C_{16,p}(s, t)$ cannot be an MDS code for any prime number p and any elements $s, t \in \mathbb{F}_p$.*

Proof. Let r_i be the i-th row of the generator matrix of the code $C_{16,p}(s, t)$. It is easy to see that the weight of $r_1 + r_2 + r_3 + r_4$ is at most 8. □

Table 7: Self-dual $[16, 8, 8]$ codes $C_{16,p}(s, t)$

p	(s,t)	p	(s,t)	p	(s,t)	p	(s,t)	p	(s,t)
13	$(5,2)$	17	$(3,3)$	19	$(1,7)$	23	$(1,9)$	29	$(3,12)$
31	$(1,11)$	37	$(2,12)$	41	$(1,10)$	43	$(1,17)$	47	$(3,12)$
53	$(1,26)$	59	$(1,21)$	61	$(3,20)$	67	$(2,19)$	71	$(3,4)$
73	$(2,9)$	79	$(1,31)$	83	$(2,26)$	89	$(5,2)$	97	$(6,32)$
101	$(1,1)$	103	$(1,37)$	107	$(2,46)$	109	$(2,52)$	113	$(2,13)$
127	$(5,22)$	131	$(1,51)$	137	$(1,33)$	139	$(4,22)$	149	$(1,28)$
151	$(3,46)$	157	$(1,10)$	163	$(1,59)$	167	$(1,7)$	173	$(1,76)$
179	$(1,52)$	181	$(1,89)$	191	$(1,56)$	193	$(2,7)$	197	$(1,62)$
199	$(1,77)$	211	$(2,33)$	223	$(2,75)$	227	$(1,9)$	229	$(1,71)$
233	$(1,60)$	239	$(1,87)$	241	$(2,107)$	251	$(1,11)$	257	$(3,23)$
263	$(5,8)$	269	$(1,117)$	271	$(2,20)$	277	$(3,22)$	281	$(2,23)$
283	$(1,109)$	293	$(1,2)$	307	$(3,113)$	311	$(1,90)$	313	$(3,29)$
317	$(1,19)$	331	$(1,121)$	337	$(1,28)$	347	$(1,102)$	349	$(1,58)$
353	$(8,128)$	359	$(2,162)$	367	$(5,7)$	373	$(1,69)$	379	$(2,179)$
383	$(1,147)$	389	$(3,1)$	397	$(1,132)$	401	$(2,2)$	409	$(5,36)$
419	$(4,77)$	421	$(7,20)$	431	$(1,17)$	433	$(1,180)$	439	$(1,161)$
443	$(4,46)$	449	$(4,214)$	457	$(7,151)$	461	$(5,92)$	463	$(1,81)$
467	$(1,105)$	479	$(1,21)$	487	$(1,12)$	491	$(2,161)$	499	$(1,191)$

We have found a self-dual $[16, 8, 8]$ code $C_{16,p}(s, t)$ for every p $(13 \leq p \leq 499)$ where the values (s, t) are listed in Table 7.

Now, using other generalized orthogonal designs, we have constructed MDS self-dual codes. Let $M_{8,i}$ $(i = 2, 3, \ldots, 8)$ be the negacyclic matrices with the first rows

$$
\begin{aligned}
&(10a, 10a, 6a, -5a, 8a, -5a, 4a, 5a),\\
&(a, 17a, -11a, -7a, -9a, -3a, -5a, 2a),\\
&(12a, 18a, -7a, 10a, -2a, 2a, 7a, 2a),\\
&(a, 9a, 7a, -4a, 5a, -4a, a, 2a),\\
&(a, 8a, -9a, -7a, -7a, 2a, -5a, 4a),\\
&(a, 7a, -4a, -7a, -8a, 5a, -6a, -a),\\
&(13a, 12a, 7a, -9a, a, 10a, -9a, 4a),
\end{aligned}
$$

respectively. Then these are generalized orthogonal designs. By replacing a in the generator matrix $(\ I\ ,\ M_{8,i}\ )$ $(i = 2, \ldots, 8)$ with some element s of $\mathbb{F}_p$, we have MDS self-dual $[16, 8, 9]_p$ codes denoted by $D_{16,p}(s)$, $E_{16,p}(s)$, $F_{16,p}(s)$, $G_{16,p}(s)$, $H_{16,p}(s)$, $I_{16,p}(s)$, $J_{16,p}(s)$, respectively. The values s are listed in Table 8. Note that no MDS self-dual codes were obtained in this way for the other prime numbers. Therefore we have the following:

Proposition 10. *For prime numbers* $p = 79$, 149, 199, 211, 223, 227, 229, 241, 251, 257, 263, 269, 277, 281, 283, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 379, 383, 389, 401, 409, 419, 421, 431, 433, 439, 443, 449, 461, 463, 479, 491, 499, *there is an MDS self-dual* $[16, 8, 9]_p$ *code.*

We constructed some more negacyclic generalized orthogonal designs, but were unsuccessful in finding any MDS self-dual codes for any other prime numbers. Due to computational limitations, we have been able to accomplish a search for MDS self-dual codes of length 14 only by using the double circulant codes. From our experience for lengths greater than 16 the most manageable strategy is to use negacyclic generalized orthogonal designs and the double circulant codes.

Table 8: MDS self-dual $[16, 8, 9]$ codes

$D_{16,p}(s)$		$E_{16,p}(s)$		$F_{16,p}(s)$		$G_{16,p}(s)$		$H_{16,p}(s)$		$I_{16,p}(s)$		$J_{16,p}(s)$	
p	s	p	s	p	s	p	s	p	s	p	s	p	s
79	39	211	26	349	76	223	49	281	63	199	17	149	29
227	45	227	110	359	3	227	52	313	109	227	9	227	94
241	87	263	38	379	17	263	85	337	88	257	64	229	66
331	59	269	83	389	39	277	102	349	8	307	148	241	45
349	57	331	2	431	160	307	72	389	39	349	49	251	124
401	19	347	51	439	23	317	151	401	46	367	165	283	138
419	68	353	115	443	44	347	13	421	76	383	47	311	80
431	195	401	121	449	221	409	180	433	36	419	162	421	24
463	176	409	145	461	91	419	172	461	187	421	147	439	152
479	7	443	185	463	141	443	182					491	6
		491	149	479	74	449	28						
				499	126	491	143						
						499	51						

Acknowledgment. The second listed author is supported by an NSERC grant. The authors would like to thank the anonymous referee for the useful comments.

References

[1] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos, On self-dual codes over some prime fields, *Discrete Math.* **262** (2003), 37–58.

[2] S. Georgiou, M. Harada and C. Koukouvinos, Orthogonal designs and Type II codes over $\mathbb{Z}_{2k}$, *Des. Codes and Cryptogr.* **25** (2002), 163–174.

[3] S. Georgiou and C. Koukouvinos, MDS self-dual codes over large prime fields, *Finite Fields Appl.* **8** (2002), 455–470.

[4] S. Georgiou and C. Koukouvinos, Self-dual codes over F_p and orthogonal designs, *J. Combin. Math. Combin. Comput.* **50** (2004), 159–177.

[5] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York, 1979.

[6] M. Harada and P.R.J. Östergård, Self-dual and maximal self-orthogonal codes over $\mathbb{F}_7$, *Discrete Math.* **256** (2002), 471–477.

[7] J.-L. Kim and Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, *J. Combin. Theory Ser. A* **105** (2004), 79–95.

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

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

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

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

[12] J. Seberry and R. Craigen, Orthogonal Designs, in *CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz, (Eds.), CRC Press, Boca Raton, 1996, pp. 400–406.

[13] V.D. Tonchev, Codes and Designs, in *Handbook of Coding Theory*, V. Pless and W.C. Huffman, (Eds.), Amsterdam, Elsevier, 1998, pp. 1229–1267.

(Received 24 Oct 2004)