MDS AND NEAR-MDS SELF-DUAL CODES
OVER LARGE PRIME FIELDS

Ilias S. Kotsireas
Department of Physics and Computer Science
Wilfrid Laurier University
University Avenue West, Waterloo, Ontario N2L 3C5, Canada

Christos Koukouvinos and Dimitris E. Simos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

(Communicated by Steven Dougherty)

Abstract. In this paper, we are interested in the construction of maximum distance separable (MDS) self-dual codes over large prime fields that arise from the solutions of systems of diophantine equations. Using this method we construct many self-dual MDS (or near-MDS) codes of lengths up to 16 over various prime fields $GF(p)$, where $p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193$ and $197$. In addition, a number of optimal codes are presented for many lengths up to 40 over small prime fields $GF(p)$. Furthermore, our results on the minimum weight of self-dual codes over prime fields give a better bound than the Pless-Pierce bound obtained from a modified Gilbert-Varshamov bound.

1. Introduction

A linear $[n, k]$ code $C$ over $GF(p)$ is a $k$-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with $p$ elements. In this paper, we consider the case where $p$ is a prime. The elements of $C$ are called codewords and the (Hamming) weight $wt(x)$ of a codeword $x$ is the number of non-zero coordinates in $x$. The minimum weight of $C$ is defined as $\min \{ wt(x) \mid 0 \neq x \in C \}$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight $d$. A matrix whose rows generate the code $C$ is called a generator matrix of $C$. The dual code $C^\perp$ of $C$ is defined as $C^\perp = \{ x \in GF(p)^n \mid x \cdot y = 0 \text{ for all } y \in C \}$. $C$ is self-dual if $C = C^\perp$. For $p \equiv 1 \pmod{4}$, a self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if $n$ is even, and for $p \equiv 3 \pmod{4}$, a self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if $n \equiv 0 \pmod{4}$ [32]. We say that self-dual codes with the largest minimum weight among self-dual codes of that length are optimal. Bounds on the minimum distance of linear codes can be found in [8] and [21].

Self-dual codes are important because many of the best codes available are of this type since they have good minimum weight properties and some of their applications can be found in the areas of combinatorics, communications, design, group and number theory. By the Gleason-Pierce theorem [39], there are divisible self-dual codes.

2000 Mathematics Subject Classification: Primary: 94B05, 94B25; Secondary: 05B20.
Key words and phrases: Self-dual codes, diophantine equations, circulant matrices, MDS codes, NMDS codes, construction.

349 c ©2009 AIMS-SDU
codes over $GF(p)$ for $p = 2, 3$ and 4. Hence much work has been done concerning
self-dual codes over these fields. For example, self-dual codes of small lengths over
$GF(2)$, $GF(3)$ and $GF(4)$ have been classified (cf. [37, Sections 11.3 – 11.6]), in
order to determine which codes exist and which weight enumerators are possible.
In addition, much is known about the largest minimum weights for self-dual codes
over these fields (cf. [37, Tables X, XII, XIII and XIV]). Moreover by applying the
Assmus Mattson theorem [4] for extremal self-dual codes over $GF(2)$, $GF(3)$ or
$GF(4)$, $t$-designs can be formed from these codes [34]. Conversely, self-dual codes
over larger fields have not been widely studied [37].

For $GF(5)$ and $GF(7)$, only self-dual codes up to length 12, and lengths 4 and 8
have been classified respectively, in [30] and [36]. The largest minimum weights of
self-dual codes over $GF(7)$ up to lengths 12 and 16 have been determined in [23].
Constructions of self-dual codes over $GF(5)$, $GF(7)$ and $GF(9)$ can be found in
[14, 16, 23, 30, 36].

However there are only a few papers [3, 5, 17] devoted to constructing self-dual
codes over fields of size greater than 9. More precisely, de Boer [6] gives [20, 10, 10]
self-dual codes over $GF(11)$ and $GF(17)$, and an [18,9,9] code over $GF(13)$. In
[5] self-dual codes over $GF(p)$ for $p = 11, 13, 17, 19, 23$ and 29 were studied. The
classification of self-dual codes over these fields for small lengths was also given in
the same paper. Some small self-dual codes with good properties over $GF(31)$ and
$GF(37)$ were presented in [17].

A $[n, k, n-k+1]_p$ linear code over $GF(p)$, is called maximum distance separable
(MDS) if it satisfies the equality in the Singleton bound, $d \leq n-k+1$ [38]. Maximum
distance separable codes (MDS codes) are at the heart of combinatorics and finite
geometries. In their book [32] Mac Williams and Sloane describe MDS codes as “one
of the most fascinating chapters in all of coding theory”. These codes can be linear
or non-linear. In this paper, we shall focus on the linear case. MDS codes have
been considered for their purely combinatorial properties. For example, they are
related to the existence of some combinatorial objects called mutually orthogonal
Latin squares and orthogonal arrays [32], and to the existence of geometric objects
called $n$-arcs [32]. One of the main problems of coding theory is determining the
maximum length of an MDS code. The following is a famous conjecture.
Main Conjecture on MDS codes. For a non-trivial $[n, k, n-k+1]$ MDS code over
$GF(q)$ we have that $n \leq q + 2$ if $q$ is even and $k = 3$ or $k = q - 1$, and $n \leq q + 1$
otherwise.

The previous conjecture has not been proven in general. It has been shown that
it holds in a number of cases, for example for codes over $GF(q)$ with $q \leq 27$, and for
codes with dimension $k \leq 5$ (for references see [26, 32] and the papers [10, 11]). In
their paper [9] Bruen, Thas, and Blokhuis show it to hold at least asymptotically.
A survey on the main conjecture for MDS codes is given in [23]. The existence and
possible structure of long MDS codes was a central theme in the address of J.A.
Thas to the International Congress of Mathematicians in 1998 [40]. Towards this
direction, Alderson gave in [1] an extendability condition on the length of MDS
codes for even $q$. Recently, improvements to the main results available concerning
MDS extensions of linear MDS codes have appeared in [2].

The Singleton defect of an $[n, k, d]$ code $C$ defined as $s(C) = n - k + 1 - d$
measures how far $C$ is away from being MDS. A code $C$ with Singleton defect
$s(C) = 1$, that is a $[n, k, n-k]$ code is called almost MDS (AMDS for short) [6].
An \([n, k, n-k]\) AMDS code for which the dual is also an AMDS code, that is \(s(C) = s(C^\perp) = 1\) is called a near-MDS code (NMDS for short) [12].

The importance of NMDS codes is that there exist NMDS codes which are considerably longer than the longest possible MDS codes for a given size of the code and the alphabet. Also, these codes have good error detecting capabilities [13] and can sometimes produce \(t\)-designs [12]. NMDS codes of maximal length over \(GF(q)\), \(8 \leq q \leq 11\) have been found in [33]. Now we consider the weight enumerators of self-dual codes over \(GF(p)\).

**Theorem 1** (MacWilliams, Mallows and Sloane [31]). The weight enumerator of a self-dual code over \(GF(p)\) is an element of

\[C[(x + (\sqrt{p} - 1)y)^2, y(x-y)].\]

Hence we have a trivial upper bound \(d \leq n/2 +1\) which coincides with the Singleton bound for an \([n, n/2, d]\) code. However, the weight enumerator \(W_p(n)\) of a self-dual \([n, n/2, n/2 +1]\) code over \(GF(p)\) is uniquely determined.

Recently, some authors (for instance [17] and [28]) have constructed MDS self-dual codes over large finite fields \(GF(p)\) for small lengths. In particular, 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 [17] and MDS self-dual codes of lengths \(2n \leq 10\) for \(p = 41\) are constructed in [28]. MDS self-dual codes for lengths 8, 10, 12 and 16 for several finite fields have been constructed via orthogonal designs and generalized orthogonal designs in [24]. A construction of MDS self-dual codes over Galois rings has appeared in [29], whereas MDS and NMDS self-dual codes of lengths up to 12 have been found.

In this paper, we give an efficient construction method for self-dual codes over large prime fields \(GF(p)\) based on solutions of systems of diophantine equations. Using this method we construct many self-dual MDS and NMDS codes of lengths up to 16 over various prime fields \(GF(p)\), where \(p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193\) and 197. Furthermore, we present a theoretical result pertaining to the systems of diophantine equations which exemplifies a connection of the solvability of these systems with quadratic residues. Finally, we improve the Pless-Pierce bound obtained from a modified Gilbert-Varshamov bound on the minimum weight of self-dual codes over prime fields.

### 2. Self-dual codes via solutions of diophantine equations

Self-dual codes via solutions of systems of diophantine equations have been constructed in [17, 18, 20]. We recall these methods in this section, and refine them under an appropriate algebraic formalism. We shall give a method for the construction of self-dual codes with generator matrix \(G\), an \(n \times 2n\) matrix, of the form \(G = [cI_n, M]\) using one, two or four circulant matrices with a system of diophantine equations.

In order to present this method for constructing suitable circulant or block circulant matrices \(M\) of order \(n\) with elements from \(GF(p)\) satisfying \(MM^T = -cI_n\) for some \(c \neq 0 \pmod p\), we shall need some basic definitions from design theory. A matrix \(M\) over \(GF(p)\) satisfying \(MM^T = -cA\) for a non-zero element \(c\) is called an orthogonal design over \(GF(p)\) [15].
Let \( A = \{ A_j : A_j = \{ a_{j1}, a_{j2}, \ldots, a_{jn} \}, j = 1, \ldots, l \} \) be a set of \( l \) sequences of length \( n \). The non-periodic autocorrelation function, over \( GF(p) \), \( N_A(s) \) (abbreviated as NPAF) of the above sequences is defined as

\[
N_A(s) = \left( \sum_{j=1}^{l} \sum_{i=1}^{n-s} a_{ji} a_{j,i+s} \right) \pmod{p}, \quad s = 0, 1, \ldots, n - 1
\]

and the periodic autocorrelation function, over \( GF(p) \), \( P_A(s) \) (abbreviated as PAF) is defined, reducing \( i + s \) modulo \( n \), as

\[
P_A(s) = \left( \sum_{j=1}^{l} \sum_{i=1}^{n} a_{ji} a_{j,i+s} \right) \pmod{p}, \quad s = 0, 1, \ldots, n - 1.
\]

It is easy to show that \( P_A(s) = P_A(n - s) \) and thus we only have to check \( P_A(s) \) for all \( s = 0, 1, \ldots, [n/2] \), where \([x]\) is the integer part of \( x \). For the results of this paper PAF is sufficient, in general. However NPAF sequences imply PAF sequences exist, the NPAF sequence being padded at the end with sufficient zeros to make longer lengths. Hence NPAF can give more general results. A circulant matrix \( E \) of order \( n \) with first row \( e_{11}, e_{12}, \ldots, e_{1n} \) will be denoted by \( E = \text{circ}(e_{11}, e_{12}, \ldots, e_{1n}) \).

### 2.1. Diophantine Equations and Circulant Construction

Let \( M = \text{circ}(m_1, m_2, \ldots, m_n) \) be a circulant matrix of order \( n \) with elements from \( GF(p) \) satisfying \( MM^T = fI_n \) where \( f \equiv -c^2 \pmod{p} \), and \( c \) is nonzero element of \( GF(p) \). To find such matrices we have to solve the system of diophantine equations arising from relation (2). Define the system of algebraic equations \( S^{(1)}_{(n,p,c)} \) over \( GF(p) \) for the one circulant construction as follows:

\[
S^{(1)}_{(n,p,c)} = \begin{cases} 
    P_M(0) + c^2 \equiv 0 \pmod{p}, \\
    P_M(s) \equiv 0 \pmod{p}, 
\end{cases} \quad s = 1, \ldots, [n/2].
\]

The system \( S^{(1)}_{(n,p,c)} \) has \( n \) unknowns and \([n/2] + 1\) equations. In detail, \( S^{(1)}_{(n,p,c)} \) is defined as:

\[
S^{(1)}_{(n,p,c)} = \begin{cases} 
    \left( \sum_{i=1}^{n} m_i^2 \right) + c^2 \equiv 0 \pmod{p}, \\
    \left( \sum_{i=1}^{n} m_i m_{i+s} \right) \equiv 0 \pmod{p}, \quad s = 1, \ldots, [n/2] 
\end{cases}
\]

where \( i + s \) is taken modulo \( n \), when needed.

Any solution of the system \( S^{(1)}_{(n,p,c)} \) of \([n/2] + 1\) diophantine equations gives a generator matrix \( G \) of the form \( G = [cI_n \; M] \) for a \([2n, n]\) self-dual code over \( GF(p) \) since \( GG^T = [cI_n \; M][cI_n \; M]^T = c^2 I_n + MM^T \) and \( MM^T = -c^2 I_n \).

**Example 1.** Let \( M = \text{circ}(m_1, m_2, m_3, m_4, m_5, m_6, m_7) \). We built up the system of diophantine equations as it is shown in method 2.1 for \( c = 1 \) and \( p = 37 \).

\[
S^{(1)}_{(7,37,1)} = \begin{cases} 
    P_M(0) + 1 \equiv 0 \pmod{37}, \\
    P_M(s) \equiv 0 \pmod{37}, \quad s = 1, 2, 3,
\end{cases} \quad \Rightarrow
\]
A solution of this system of four diophantine equations is $m_1 = 1, m_2 = 1, m_3 = 15, m_4 = 29, m_5 = 10, m_6 = 14, m_7 = 35$. Thus

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 15 & 29 & 10 & 14 & 35 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 35 & 1 & 1 & 15 & 29 & 10 & 14 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 14 & 35 & 1 & 1 & 15 & 29 & 10 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 10 & 14 & 35 & 1 & 1 & 15 & 29 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 29 & 10 & 14 & 35 & 1 & 1 & 15 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 15 & 29 & 10 & 14 & 35 & 1 & 1 \end{bmatrix}.$$ 

The matrix $\mathbf{G}$ generates a linear $[14, 7, 8]$ self-dual MDS code over $\mathbb{F}_{37}$ with weight enumerator $W(x, y) = x^{14} + 108108 x^6 y^8 + 2090088 x^5 y^9 + 38630592 x^4 y^{10} + 504608832 x^3 y^{11} + 4542167448 x^2 y^{12} + 25156386864 xy^{13} + 64687885200 y^{14}$.

Now we present a theoretical result pertaining to the system $S_{1}(n, p, 1)$ which exemplifies a connection of the solvability of these systems with quadratic residues.

**Lemma 1.** Let $n$ be a positive integer and $c = 1$. Then for any prime $p \geq 3$ we have: $S_{1}(n, p, 1)$ has solutions over $\mathbb{F}_p$ if and only if $(p - 1) \equiv 0 \pmod{4}$.

**Proof.** Adding the $\lfloor n/2 \rfloor$ equations of $S_{1}(n, p, 1)$ together, we obtain

$$\sum_{s=1}^{\lfloor n/2 \rfloor} P_M(s) \equiv 0 \pmod{p},$$

which is equivalent to

$$e_2 \equiv 0 \pmod{p},$$

where $e_2$ denotes the second elementary symmetric function in the $n$ variables $m_1, \ldots, m_n$ and $M = \text{circ}(m_1, m_2, \ldots, m_n)$. Note that for $n$ even, the equation $P_M(n/2) \equiv 0 \pmod{p}$ is actually equal to

$$2 \left( \sum_{i=1}^{n/2} m_i m_{i+n/2} \right) \equiv 0 \pmod{p}$$

and since $(2, p) = 1$, we can discard the factor of 2.

The Jacobi-Trudi formula $e_2 = \frac{1}{2}(p_1^2 - p_2)$ (where $p_1, p_2$ are power-sums in the $n$ variables $m_1, \ldots, m_n$) then implies that

$$p_1^2 - p_2 \equiv 0 \pmod{p}$$

and using the first equation of $S_{1}(n, p, 1)$, this becomes

$$p_1^2 \equiv -1 \pmod{p}.$$
The above congruence has a solution if and only if \((p - 1) \equiv 0 \pmod{4}\), i.e. \(-1\) is a quadratic residue of primes of the form \(4k + 1\) and a quadratic non-residue of primes of the form \(4k + 3\), see \([27]\) for instance.

In some cases, it seems that it is possible to establish a formula for the number of solutions of a \(S_{(n,p,1)}^{1}\) system, for a specific \(n\) and for all primes \(p\). We mention one such case in the following remark for \(n = 4\):

**Remark 1.** The sequence of the (nonzero) numbers of solutions of \(S_{(4,p,1)}^{1}\) is given by:

\[|S_{(4,p,1)}| = 4^2 \cdot a_n\]

where \(a_n\) is the sequence A005098 of Sloane’s Integer Encyclopedia of Integer Sequences: i.e. the sequence 1, 3, 4, 7, 9, 10, 13, 15, 18, 22, 24, 25, 27, 28, 34, 37, 39, 43, 45, 48, 49, 57, 58, 60, 64, 67, 69, 70, 73, 78, 79, 84, 87, 88, 93, 97, 99, 100, 102, 105, 108, 112, 114, 115, 127, 130, 135, 139, 142, 144, 148, 150, 153, 154, 160, 163, 165, 168, 169, 175, 177, 183, ..., defined by numbers \(n\) such that \(4n + 1\) is prime.

**Remark 2.** We note that although we have not proved the above statement, it predicts exactly the computational results obtained for all odd primes \(1 \pmod{4}\), s.t. \(p \leq 541\).

### 2.2. Diophantine Equations and Two Block Circulant Construction

Let \(M\) be a \(2n \times 2n\) matrix constructed from two circulant matrices say \(A_1 = circ(a_{11}, a_{12}, \ldots, a_{1n})\) and \(A_2 = circ(a_{21}, a_{22}, \ldots, a_{2n})\) of order \(n\) in the form

\[
M = \begin{pmatrix}
    A_1 & A_2 \\
    -A_2^T & A_1^T
\end{pmatrix}
\]

with elements from \(GF(p)\) satisfying \(MM^T = fI_{2n}\) where \(f \equiv -c^2 \pmod{p}\), and \(c\) is nonzero element of \(GF(p)\). To find such matrices we have again to solve the system of diophantine equations arising from relation (2). Define the system of algebraic equations \(S_{(n,p,c)}^{2}\) over \(GF(p)\) for the two block circulant construction as follows:

\[
S_{(n,p,c)}^{2} = \begin{cases}
    P_A(0) + c^2 \equiv 0 \pmod{p}, \\
    P_A(s) \equiv 0 \pmod{p}, & s = 1, \ldots, [n/2].
\end{cases}
\]

The system \(S_{(n,p,c)}^{2}\) has \(2n\) unknowns and \([n/2] + 1\) equations. In detail, \(S_{(n,p,c)}^{2}\) is defined as:

\[
S_{(n,p,c)}^{2} = \begin{cases}
    \left( \sum_{j=1}^{n} a_{ji}^2 \right) + c^2 \equiv 0 \pmod{p}, \\
    \left( \sum_{j=1}^{n} a_{ji}a_{ji+s} \right) \equiv 0 \pmod{p}, & s = 1, \ldots, [n/2]
\end{cases}
\]

where \(i + s\) is taken modulo \(n\), when needed.

Any solution of the system \(S_{(n,p,c)}^{2}\) of \([n/2] + 1\) diophantine equations gives a generator matrix \(G\) of the form \(G = [cI_{2n}, M]\) for a \([4n, 2n]\) self-dual code over \(GF(p)\) since \(GG^T = [cI_{2n}, M][cI_{2n}, M]^T = c^2I_{2n} + MM^T\) and \(MM^T = -c^2I_{2n}\).
Example 2. Let $A_1 = circ(a_{11}, a_{12}, a_{13})$ and $A_2 = circ(a_{21}, a_{22}, a_{23})$. We built up a system of diophantine equations as it is shown in method 2.2 for $c = 1$ and $p = 41$.

$$S^{a}_{(3,41,1)} = \begin{cases} \begin{align*} P_A(0) + 1 &\equiv 0 \pmod{41}, \\ P_A(s) &\equiv 0 \pmod{41}, \quad s = 1. \end{align*} \end{cases} \Rightarrow$$

$$S^{a}_{(3,41,1)} = \begin{cases} \sum_{i=1}^{2} \sum_{j=1}^{3} a^2_{ji} + 1 &\equiv 0 \pmod{41}, \\ \sum_{i=1}^{2} \sum_{j=1}^{3} a_{ji}a_{j,i+s} &\equiv 0 \pmod{41}, \quad s = 1. \end{cases}$$

where $i + s$ is taken modulo 3, when needed.

A solution of this system of two diophantine equations is $a_{11} = 1, a_{12} = 1, a_{13} = 5, a_{21} = 1, a_{22} = 12, a_{23} = 14$. Thus

$$G = [I_6 \ M] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 5 & 1 & 12 & 14 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5 & 1 & 1 & 14 & 1 & 12 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 5 & 1 & 12 & 14 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 40 & 27 & 29 & 1 & 5 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 29 & 40 & 27 & 1 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 27 & 29 & 40 & 5 & 1 & 1 \end{pmatrix}.$$  

The matrix $G$ generates a linear [12,6,7] self-dual MDS code over $GF(41)$ with weight enumerator $W(x, y) = x^{12} + 31680 x^3 y^7 + 673200 x^4 y^8 + 12152800 x^5 y^9 + 145685760 x^6 y^{10} + 1059593280 x y^{11} + 3531967520 y^{12}$.

2.3. DIOPHANTINE EQUATIONS AND FOUR BLOCK CIRCULANT CONSTRUCTION. Let $M$ be a $4n \times 4n$ matrix, constructed from four circulant matrices say $A_i = circ(a_{i1}, a_{i2}, \ldots, a_{in})$, $i = 1, 2, 3, 4$ of order $n$ in the form

$$M = \begin{pmatrix} A_1 & A_2 R & A_3 R & A_4 R \\ -A_2 R & A_1 & A_2 R & -A_3 R \\ A_3 R & -A_2 R & A_1 & A_2 R \\ -A_4 R & A_3 R & -A_2 R & A_1 \end{pmatrix},$$

where $R = (r_{ij})$ is the back diagonal matrix, with elements from $GF(p)$ satisfying $MM^T = f I_{4n}$ where $f = -c^2 \pmod{p}$, and $c$ is nonzero element of $GF(p)$. To find such matrices we have again to solve the system of diophantine equations arising from relation (2). Define the system of algebraic equations $S^{a}_{(n,p,c)}$ over $GF(p)$ for the four block circulant construction as follows:

$$S^{a}_{(n,p,c)} = \begin{cases} \begin{align*} P_A(0) + c^2 &\equiv 0 \pmod{p}, \\ P_A(s) &\equiv 0 \pmod{p}, \quad s = 1, \ldots, [n/2]. \end{align*} \end{cases}$$

The system $S^{a}_{(n,p,c)}$ has $4n$ unknowns and $[n/2] + 1$ equations. In detail, $S^{a}_{(n,p,c)}$ is defined as:

$$S^{a}_{(n,p,c)} = \begin{cases} \sum_{i=1}^{4} \sum_{j=1}^{n} a^2_{ji} + c^2 &\equiv 0 \pmod{p}, \\ \sum_{i=1}^{4} \sum_{j=1}^{n} a_{ji}a_{j,i+s} &\equiv 0 \pmod{p}, \quad s = 1, \ldots, [n/2] \end{cases}$$

where $i + s$ is taken modulo $n$, when needed.
Any solution of the system $S^4_{(n,p,c)}$ of $[n/2] + 1$ diophantine equations gives a generator matrix $G$ of the form $G = [cI_{4n} M]$ for a $[8n, 4n]$ self-dual code over $GF(p)$ since $GG^T = [cI_{4n} M][cI_{4n} M]^T = c^2 I_{4n} + MM^T$ and $MM^T = -c^2 I_{4n}$.

**Example 3.** Let $A_1 = circ(a_{11}, a_{12})$, $A_2 = circ(a_{21}, a_{22})$, $A_3 = circ(a_{31}, a_{32})$, $A_4 = circ(a_{41}, a_{42})$. We built up a system of diophantine equations as it is shown in method 2.3 for $c = 1$ and $p = 17$.

$$S^4_{(2,17,1)} = \begin{cases} P_a(0) + 1 \equiv 0 \pmod{17}, \\ P_a(s) \equiv 0 \pmod{17}, \quad s = 1. \end{cases}$$

$$S^4_{(2,17,1)} = \left\{ \begin{array}{l}
\sum_{j=1}^{4} \sum_{i=1}^{2} a_{j,i}^2 + 1 \equiv 0 \pmod{17}, \\
\sum_{j=1}^{4} \sum_{i=1}^{2} a_{j,i} a_{j,i+s} \equiv 0 \pmod{17}, \quad s = 1.
\end{array} \right.$$

where $i + s$ is taken modulo 2, when needed.

A solution of this system of two diophantine equations is $a_{11} = 0, a_{12} = 0, a_{21} = 7, a_{22} = 5, a_{31} = 15, a_{32} = 6, a_{41} = 12, a_{42} = 8$. Thus

$$G = [I_8 M] = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$  

The matrix $G$ generates a linear $[16, 8, 7]$ self-dual code over $GF(17)$ with weight enumerator $W(x, y) = x^{16} + 3072 x^6 y^6 + 5440 x^5 y^8 + 81152 x^7 y^8 + 1327872 x^8 y^{10} + 11092480 x^9 y^{11} + 73017728 x^{10} y^{12} + 362163200 x^{11} y^{13} + 1239102208 x^{12} y^{14} + 2644584960 x^{13} y^{15} + 2644379328 y^{16}$.

3. Results

In this section, we summarize the results we have obtained from our computational search. We have constructed over 3 million self-dual codes using the methods described in sections 2.1, 2.2 and 2.3. We have used Magma, a computer algebra system for symbolic computation developed at the University of Sydney, to compute the minimum distance of the aforementioned self-dual codes [7, 22]. The generator matrices and the corresponding weight enumerators for the following MDS (or near-MDS) self-dual codes can be retrieved through Prof. C. Koukouvinos webpage [http://www.math.ntua.gr/~ckoukov].

3.1. Results from the one block circulant construction.

**Lemma 2.** There exist $[2n, n, n + 1]$ MDS self-dual codes using the one block circulant construction over $GF(p)$ for:

(i) length $2n = 10$ and $p = 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197$;
(ii) length $2n = 14$ and $p = 13, 29, 37, 41$. 

Advances in Mathematics of Communications  Volume 3, No. 4 (2009), 349–361
We give a similar lemma for near-MDS self-dual codes, for the cases we have not found MDS self-dual codes.

**Lemma 3.** There exist \([2n, n, n]\) near-MDS self-dual codes using the one block circulant construction over \(GF(p)\) for:

(i) length \(2n = 8\) and \(p = 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, 193, 197;\)
(ii) length \(2n = 12\) and \(p = 13, 17, 29, 37, 41, 53, 61;\)
(iii) length \(2n = 14\) and \(p = 17, 41, 53, 61;\)
(iv) length \(2n = 16\) and \(p = 13, 19, 29.\)

### 3.2. Results from the two block circulant construction.

**Lemma 4.** There exist \([4n, 2n, 2n + 1]\) MDS self-dual codes using the two block circulant construction over \(GF(p)\) for:

(i) length \(4n = 12\) and \(p = 11, 19, 23, 29, 31, 37, 41.\)

We give a similar lemma for near-MDS self-dual codes, for the cases we have not found MDS self-dual codes.

**Lemma 5.** There exist \([4n, 2n, 2n]\) near-MDS self-dual codes using the two block circulant construction over \(GF(p)\) for:

(i) length \(4n = 12\) and \(p = 3, 5, 7, 13, 17;\)
(ii) length \(4n = 16\) and \(p = 11, 13, 17, 19.\)

### 3.3. Results from the four block circulant construction.

**Lemma 6.** There exist \([8n, 4n, 4n + 1]\) near-MDS self-dual codes using the four block circulant construction over \(GF(p)\) for:

(i) length \(8n = 16\) and \(p = 17, 29.\)

**Remark 3.** From the results presented in this section, it appears that the main conjecture for \([n, k, n - k + 1]\) MDS codes over \(GF(p)\) (mentioned earlier) is true for self-dual codes.

### 3.4. Optimal self-dual codes over small prime fields.

A self-dual code \(C\) is called extremal or optimal if \(C\) has the largest possible minimum weight.

#### 3.4.1. Extremal ternary self-dual codes from diophantine equations.

The known bounds of \(d\) for \(p = 3\) are given in [37] and [41]. In particular the following theorem is known.

**Theorem 2** (Tonchev [41]). The minimum distance \(d\) of a ternary self-dual \([n, n/2]\) code \(C\) satisfies

\[
d \leq 3 \left[ \frac{n}{12} \right] + 3.
\]

We note that over \(GF(3)\) we have reconstructed all extremal (optimal) \([n, n/2]\) ternary self-dual codes for lengths \(12 \leq n \leq 40\) through solutions of systems of diophantine equations. In particular we found the following codes.
3.4.2. Optimal self-dual codes from diophantine equations over prime fields $GF(5)$ and $GF(7)$. Now we give results of $[n,n/2]$ self-dual codes for other prime fields comparing them with the best available known bounds using the tables provided by Brouwer [8] and Grassl [21]. Bounds in these tables are given in a range of lower-upper bound, in the same form that can be found in [21]. Lower bounds are constructive while the upper bounds have been found via linear programming or by shortening and considering truncation to existing codes. Therefore, a code is considered to be optimal if it achieves the largest possible minimum weight among self-dual codes, i.e. it reaches the lower constructive bound of these tables.

NMDS or MDS codes of smaller lengths over larger prime fields are not listed in the following tables, since they have been given earlier. If a code is not listed in these tables it means that this was not a permissible value of the corresponding system of diophantine equations, thus we had no solutions for this case.

**Notation.** We denote with $n$ the length of self-dual codes, while with $d_{\text{max}}(n)$ we denote the largest minimum weight we have found. The lower and upper bounds of the tables [8, 21] are denoted by $[Lb,Ub]$.

| Length | $p = 5$ | $p = 7$ |
|--------|---------|---------|
| $n$    | $d_{\text{max}}(n)$ | $d_{\text{max}}(n)$ |
| $d_{\text{max}}(n)$ | $[Lb,Ub]$ | $[Lb,Ub]$ |
| 14     | 6       | 6       |
| 16     | -       | 7       |
| 18     | 7       | 7-8     |
| 20     | 8       | 8-9     |
| 22     | 8       | 8-10    |
| 24     | 9       | 9-10    |

Table 2. Optimal self-dual codes of lengths $20 \leq n \leq 24$

We now give some self-dual codes of larger lengths over $GF(5)$ with good minimum weight properties.

| Length | $p = 5$ |
|--------|---------|
| $n$    | $d_{\text{max}}(n)$ | $[Lb,Ub]$ |
| 26     | 9       | 10-11   |
| 28     | 10      | 11-12   |
| 30     | 10      | 12      |
| 32     | 10      | 11-13   |
| 34     | 10      | 11-14   |

Table 3. Good self-dual codes of lengths $26 \leq n \leq 34$
3.5. Improving the Pless-Pierce bound on the minimum weight of self-dual codes. Recently, Kim and Lee [28] used the Pless-Pierce bound [35] on the minimum weight of self-dual codes as a criterion to value their results on self-dual (near) MDS codes over large finite fields and improved it for some values (cf. [28, Table 1]).

In this section, our results (appearing in bold faces) on the minimum weight of \([n, n/2]\) optimal or MDS self-dual codes over prime fields give a better bound than the Pless-Pierce bound (appearing in the parenthesis) obtained from a modified Gilbert-Varshamov bound.

\[
\begin{array}{|c|c|}
\hline
n & p = 5 \\
\hline
14 & 6 (4) \\
16 & 6 (5) \\
18 & 7 (6) \\
20 & 8 (6) \\
22 & 8 (6) \\
24 & 9 (7) \\
26 & 9 (7) \\
28 & 10 (8) \\
30 & 10 (8) \\
32 & 10 (8) \\
34 & 10 (9) \\
\hline
\end{array}
\]

Table 4. Minimum weights of self-dual codes of lengths 14 ≤ \(n\) ≤ 34 over GF(5)

\[
\begin{array}{|c|c|}
\hline
n & p = 7 \\
\hline
16 & 7 (6) \\
20 & 9 (7) \\
24 & 10 (8) \\
\hline
\end{array}
\]

Table 5. Minimum weights of optimal self-dual codes of lengths \(n\) ≤ 24 over GF(7)

\[
\begin{array}{|c|c|}
\hline
n & p = 41 \\
\hline
12 & 7 (6) \\
\hline
\end{array}
\]

Table 6. Minimum weight of an \([12, 6]\) MDS code over GF(41)

Acknowledgements

All computations in C and Magma have been performed remotely at SHARCnet high performance computing clusters. The research of the first author was supported by an NSERC grant while the research of the third author was supported by a scholarship awarded by the Secretariat of the Research Committee of National Technical University of Athens.
References

[1] T. L. Alderson, Extending MDS codes, Ann. Comb., 9 (2005), 125–135.
[2] T. L. Alderson, A. A. Bruen and R. Silverman, Maximum distance separable codes and arcs in projective spaces, J. Combin. Theory Ser. A, 114 (2007), 1101–1117.
[3] K. T. Arasu and T. A. Gulliver, Self-dual codes over \( \mathbb{F}_p \) and weighing matrices, IEEE Trans. Inform. Theory, 47 (2001), 2051–2055.
[4] E. F. Assmus Jr. and H. F. Mattson Jr., New 5-designs, J. Combin. Theory Ser. A, 6 (1969), 122–151.
[5] 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.
[6] M. A. de Boer, Almost MDS codes, Des. Codes Cryptogr., 9 (1996), 143–155.
[7] W. Bosma and J. J. Cannon, “Handbook of Magma Functions,” 2.9 edition, School of Mathematics and Statistics, University of Sydney, 2002.
[8] A. E. Brouwer, Bounds on linear codes, in “Handbook of Coding Theory” (eds. V. Pless and W.C. Huffman), Elsevier, North-Holland, Amsterdam, (1998), 295–401.
[9] A. A. Bruen, J. A. Thas and A. Blokhuis, On M.D.S. codes, arcs in PG(n, q) with q even, and a solution of three fundamental problems of B. Segre, Invent. Math., 92 (1988), 441–459.
[10] J. M. Chao and H. Kaneta, Classical arcs in PG(r, q) for 11 ≤ q ≤ 19, Discrete Math., 174 (1997), 87–94.
[11] J. M. Chao and H. Kaneta, Classical arcs in PG(r, q) for 23 ≤ q ≤ 29, Discrete Math., 226 (2001), 377–385.
[12] S. Dodunekov and I. N. Landjev, On near-MDS codes, J. Geom., 54 (1995), 30–43.
[13] R. Dodunekova, S. M. Dodunekov and T. Kløve, Almost-MDS and near-MDS codes for error detection, IEEE Trans. Inform. Theory, 43 (1997), 285–290.
[14] P. Gaborit, Quadratic double circulant codes over fields, J. Combin. Theory Ser. A, 97 (2002), 85–107.
[15] S. Georgiou, M. Harada and C. Koukouvinos, Orthogonal designs and Type II codes over \( \mathbb{Z}_2k \), Des. Codes Cryptogr., 25 (2002), 163–174.
[16] S. Georgiou and C. Koukouvinos, Self-dual codes over GF(7) and orthogonal designs, Utilitas Math., 60 (2001), 79–89.
[17] S. Georgiou and C. Koukouvinos, MDS self-dual codes over large prime fields, Finite Fields Appl., 8 (2002), 455–470.
[18] S. Georgiou and C. Koukouvinos, Self-orthogonal and self-dual codes constructed via combinatorial designs and diophantine equations, Des. Codes Cryptogr., 32 (2004), 193–206.
[19] S. Georgiou and C. Koukouvinos, Self-dual codes over \( \mathbb{F}_p \) and orthogonal designs, J. Combin. Math. Combin. Comput., 50 (2004), 159–177.
[20] S. Georgiou and C. Koukouvinos, Combinatorial designs and codes over some prime fields, J. Statist. Plann. Inference, 135 (2005), 93–106.
[21] M. Grassl, Bounds on the minimum distance of linear codes, http://www.codetables.de.
[22] M. Grassl, Searching for linear codes with large minimum distance, in “Discovering Mathematics with Magma” (eds. W. Bosma and J. Cannon), Springer, Berlin, 2006.
[23] T. A. Gulliver and M. Harada, New optimal self-dual codes over GF(7), Graphs and Combin., 15 (1999), 175–186.
[24] M. Harada and H. Kharaghani, Orthogonal designs and MDS self-dual codes, Australas. J. Combin., 35 (2006), 57–67.
[25] J. W. P. Hirschfeld, Complete arcs, Discrete Math., 174 (1997), 177–184.
[26] J. W. P. Hirschfeld and J. A. Thas, “General Galois Geometries,” Oxford University Press, Oxford, 1991.
[27] K. Ireland and M. Rosen, “A Classical introduction to Modern Number Theory,” 2nd edition, Springer-Verlag, New York, 1990.
[28] 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.
[29] J.-L. Kim and Y. Lee, Construction of MDS self-dual codes over Galois rings, Des. Codes Cryptogr., 45 (2007), 247–258.
[30] 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.
[31] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, Generalizations of Gleason’s theorem on weight enumerators of self-dual codes, IEEE Trans. Inform. Theory, 18 (1972), 794–805.
F. J. MacWilliams and N. J. A. Sloane, “The Theory of Error-Correcting Codes,” North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

S. Marcugini, A. Milani and F. Pambianco, NMDS codes of maximal length over \( F_q \), \( 8 \leq q \leq 11 \), IEEE Trans. Inform. Theory, 48 (2002), 963–966.

V. S. Pless, W. C. Huffman and R. A. Brualdi, An introduction to algebraic codes, in “Handbook of Coding Theory” (eds. V. Pless and W.C. Huffman), Elsevier, North-Holland, Amsterdam, (1998), 3–139.

V. Pless and J. N. Pierce, Self-dual codes over \( GF(q) \) satisfy a modified Varshamo-Gilbert bound, Inform. and Control, 23 (1973), 35–40.

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

E. M. Rains and N. J. A. Sloane, Self-dual codes, in “Handbook of Coding Theory” (eds. V. Pless and W.C. Huffman), Elsevier, North-Holland, Amsterdam, (1998), 177–294.

R. C. Singleton, Maximum distance separable \( q \)-nary codes, IEEE Trans. Inform. Theory, 10 (1964), 116–118.

N. J. A. Sloane, Self-dual codes and lattices, relations between combinatorics and other parts of mathematics, in “Proceedings of Symposium on Pure Mathematics,” Amer. Math. Soc., Providence, RI, 34 (1979), 273–308.

J. A. Thas, Finite geometries, varieties and codes, in “Proceedings of the International Congress of Mathematicians” (Berlin, 1998), Doc. Math., 3 (1998), 397–408.

V. D. Tonchev, Codes, in “The CRC Handbook of Combinatorial Designs” (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, Fla., (1996), 517–543.

Received May 2009; revised October 2009.

E-mail address: ikotsire@wlu.ca
E-mail address: ckoukouv@math.ntua.gr
E-mail address: dsimos@math.ntua.gr