ON THE CLASSIFICATION OF SELF-DUAL \([20, 10, 9]\) CODES OVER GF(7)

MASAAKI HARADA AND AKIHIRO MUNEMASA

In memory of Yutaka Hiramine

Abstract. It is shown that there is a unique self-dual \([20, 10, 9]\) code \(C\) over GF(7) such that the lattice obtained from \(C\) by Construction A is isomorphic to the 20-dimensional unimodular lattice \(D_{20}^+\) up to equivalence. This is done by converting the classification of such self-dual codes to that of skew-Hadamard matrices of order 20.

1. Introduction

Let GF\((p)\) be the finite field of order \(p\), where \(p\) is prime. As described in [15], self-dual codes are an important class of linear codes for both theoretical and practical reasons. For \(p \equiv 1 \pmod{4}\), a self-dual code of length \(n\) over GF\((p)\) exists if and only if \(n\) is even, and for \(p \equiv 3 \pmod{4}\), a self-dual code of length \(n\) over GF\((p)\) exists if and only if \(n \equiv 0 \pmod{4}\). It is a fundamental problem to classify self-dual codes over GF\((p)\) and determine the largest minimum weight among self-dual codes over GF\((p)\) for a fixed length. Much work has been done towards classifying self-dual codes over GF\((p)\) and determining the largest minimum weight among self-dual codes of a given length over GF\((p)\) for \(p = 2\) and 3 (see [15]).

Self-dual codes over GF\((7)\) have been classified for lengths up to 12 (see [7]), and the largest minimum weight \(d_7(n)\) among self-dual codes of length \(n\) over GF\((7)\) has been determined for \(n \leq 28\) (see [5, Table 2]). For example, it is known that \(d_7(20) = 9\). Some self-dual \([20, 10, 9]\) codes over GF\((7)\) can be found in [4, Table 6] and [5, Table 7]. As described in [10], it is an open problem to determine whether such a code is unique or not.

There are 12 nonisomorphic 20-dimensional unimodular lattices having minimum norm 2 (see [2, Table 16.7]). The lattice \(D_{20}^+\) is one of

2010 Mathematics Subject Classification. 94B05.

Key words and phrases. self-dual code, skew-Hadamard matrix, unimodular lattice.
the 20-dimensional unimodular lattices having minimum norm 2. Let $A_7(C)$ denote the unimodular lattice obtained from a self-dual code $C$ over $GF(7)$ by Construction A.

In this paper, we convert the classification of self-dual $[20, 10, 9]$ codes $C$ over $GF(7)$ such that $A_7(C)$ is isomorphic to $D_{20}^+$ to that of skew-Hadamard matrices of order 20. The main aim of this paper is to give the following partial classification of self-dual $[20, 10, 9]$ codes over $GF(7)$.

**Theorem 1.** Up to equivalence, there is a unique self-dual $[20, 10, 9]$ code $C$ over $GF(7)$ such that $A_7(C)$ is isomorphic to $D_{20}^+$.

All computer calculations in this paper were done by MAGMA [1].

2. **Preliminaries**

In this section, we give definitions and notions on self-dual codes, unimodular lattices and skew-Hadamard matrices. Some basic facts on these subjects are also provided.

2.1. **Self-dual codes.** An $[n, k]$ code $C$ over $GF(p)$ is a $k$-dimensional subspace of $GF(p)^n$. The value $n$ is called the length of $C$. The weight $wt(x)$ of a vector $x \in GF(p)^n$ is the number of non-zero components of $x$. A vector of $C$ is called a codeword of $C$. The minimum non-zero weight of all codewords in $C$ is called the minimum weight of $C$ and an $[n, k]$ code with minimum weight $d$ is called an $[n, k, d]$ code. The weight enumerator $W(C)$ of $C$ is given by $W(C) = \sum_{i=0}^{n} A_i y^i$, where $A_i$ is the number of codewords of weight $i$ in $C$. The dual code $C^\perp$ of $C$ is defined as

$$C^\perp = \{ x \in GF(p)^n \mid x \cdot y = 0 \text{ for all } y \in C \},$$

under the standard inner product $x \cdot y$. A code $C$ is called self-dual if $C = C^\perp$. Two codes $C$ and $C'$ are equivalent if there exists a $(1, -1, 0)$-monomial matrix $M$ with $C' = \{ cM \mid c \in C \}$.

2.2. **Unimodular lattices.** An $n$-dimensional (Euclidean) lattice is a discrete subgroup of rank $n$ in $\mathbb{R}^n$. A lattice $L$ is unimodular if $L = L^*$, where the dual lattice $L^*$ is defined as

$$L^* = \{ x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z} \text{ for all } y \in L \},$$

under the standard inner product $(x, y)$. The norm $\|x\|^2$ of a vector $x \in \mathbb{R}^n$ is $(x, x)$. The minimum norm of $L$ is the smallest norm among all nonzero vectors of $L$. Two lattices $L$ and $L'$ are isomorphic, denoted $L \cong L'$, if there exists an orthogonal matrix $A$ with $L' = \{ xA \mid x \in L \}$. 
Let $C$ be a code of length $n$ over $\text{GF}(p)$ and let $\varepsilon_1, \ldots, \varepsilon_n$ be an orthogonal basis of $\mathbb{R}^n$ satisfying $(\varepsilon_i, \varepsilon_j) = p \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta. Then we define the lattice $A_p(C)$ obtained from $C$ by Construction A as

$$A_p(C) = \left\{ \frac{1}{p} \sum_{i=1}^{n} x_i \varepsilon_i \mid x = (x_1, \ldots, x_n) \in \mathbb{Z}^n, \ x \mod p \in C \right\}.$$ 

It is known that $A_p(C)$ is unimodular if and only if $C$ is self-dual. A set $\{f_1, \ldots, f_n\}$ of $n$ vectors $f_1, \ldots, f_n$ in an $n$-dimensional lattice $L$ with $(f_i, f_j) = k \delta_{i,j}$ is called a $k$-frame of $L$. Clearly, if a unimodular lattice $L$ contains a $p$-frame, then there is a self-dual code $C$ over $\text{GF}(p)$ with $A_p(C) \cong L$ (see [6]).

Let $C$ be a self-dual $[20, 10, d]$ code over $\text{GF}(7)$ with $d \in \{8, 9\}$. Then it is easy to see that $A_7(C)$ has minimum norm 2. It is known that there are 12 nonisomorphic 20-dimensional unimodular lattices having minimum norm 2 (see [2, Table 16.7]). These 12 lattices have distinct components (see [2, Table 16.7] for the components). The 20-dimensional unimodular lattice $D_{20}^+$ with minimum norm 2 has component $D_{20}$. The lattices $D_{20}$ and $D_{20}^+$ are defined as follows:

$$D_{20} = \left\{ \sum_{i=1}^{20} \alpha_i \varepsilon_i \mid (\alpha_1, \ldots, \alpha_{20}) \in \mathbb{Z}^{20}, \ \sum_{i=1}^{20} \alpha_i \equiv 0 \pmod{2} \right\},$$

$$D_{20}^+ = \langle D_{20}, 1 \rangle,$$

where $\varepsilon_i = (\delta_{1,i}, \ldots, \delta_{20,i}) \ (1 \leq i \leq 20)$ and 1 denotes the all-one vector. Note that $D_{20}$ is the even sublattice of $D_{20}^+$, that is, the sublattice consisting of vectors of even norm in $D_{20}^+$.

### 2.3. Skew-Hadamard matrices

A Hadamard matrix of order $n$ is an $n \times n$ $(1, -1)$-matrix $H$ such that $HH^\top = nI$, where $I$ is the identity matrix and $H^\top$ denotes the transposed matrix of $H$. It is well known that the order $n$ is necessarily 1, 2, or a multiple of 4. Two Hadamard matrices $H$ and $K$ are said to be equivalent if there are $(1, -1, 0)$-monomial matrices $P$ and $Q$ with $K = PHQ$. All Hadamard matrices of orders up to 32 have been classified (see [8, Chap. 7] for orders up to 28 and [9] for order 32, see also [17]).

A Hadamard matrix $H$ of order $n$ is called a skew-Hadamard matrix if $H + H^\top = 2I$. Skew-Hadamard matrices are a class of Hadamard matrices, which has been widely studied (see e.g., [3], [11]). The numbers of inequivalent skew-Hadamard matrices of orders 4, 8, 12, 16, 20, 24 are 1, 1, 1, 3, 2, 11, respectively [11]. As an example, we give two inequivalent skew-Hadamard matrices $S_1$ and $S_2$ of order 20 in Figure 1, where
we use $+$, $-$ to denote $1$, $-1$, respectively. Note that $S_1$ is equivalent to the Paley Hadamard matrix. Moreover, we have verified by Magma that $S_2$ is equivalent to had.20.tonchevit in [17].

\[
S_1 = \begin{pmatrix}
\end{pmatrix}
\]

\[
S_2 = \begin{pmatrix}
\end{pmatrix}
\]

**Figure 1.** Skew-Hadamard matrices of order 20

The following lemma can be proved in the same manner as [13, Lemma 3].
Lemma 2. Let $F$ be a square matrix all of whose entries are integers. If $FF^T = kI$ and $p$ is a prime divisor of $k$ such that $p^2 \nmid k$, then $F$ generates a self-dual code over $GF(p)$.

Hence, the code over $GF(7)$ generated by the row vectors of $H + 2I$ is self-dual, where $H$ is a skew-Hadamard matrix of order 20.

3. Proof of Theorem 1

In this section, we give a proof of Theorem 1, which is the main result of this paper.

Lemma 3. Let $C$ be a self-dual $[20, 10, 9]$ code over $GF(7)$. If $\xi \in A_7(C)$ and $\|\xi\|^2 = 2$, then

$$|\{i \mid 1 \leq i \leq 20, \ |(\xi, \varepsilon_i)| \geq 2\}| \leq 1.$$

Proof. Write

$$\xi = \frac{1}{7} \sum_{i=1}^{20} x_i \varepsilon_i, \ x = (x_1, \ldots, x_n) \in \mathbb{Z}^{20}, \ x \mod 7 \in C.$$

Since for each $j \in \{1, \ldots, 20\},$

$$x_j^2 = 7\|\frac{1}{7}x_j \varepsilon_j\|^2 \leq 7\|\frac{1}{7} \sum_{i=1}^{20} x_i \varepsilon_i\|^2 = 7\|\xi\|^2 = 14,$$

we have

(1) \hspace{1cm} x_j \equiv 0 \pmod{7} \iff x_j = 0 \iff (\xi, \varepsilon_j) = 0.

Set

$$a_1 = |\{i \mid 1 \leq i \leq 20, \ |(\xi, \varepsilon_i)| = 1\}|,$$

$$a_2 = |\{i \mid 1 \leq i \leq 20, \ |(\xi, \varepsilon_i)| \geq 2\}|.$$

Then by (1) we have

$$a_1 + a_2 = \text{wt}(x) \geq 9,$$

and we have

$$a_1 + 4a_2 \leq \sum_{i=1}^{20} (\xi, \varepsilon_i)^2 = 7\|\xi\|^2.$$
Thus $a_2 \leq \frac{5}{3}$, and hence $a_2 \leq 1$. 

**Proposition 4.** Let $C$ be a self-dual $[20, 10, 9]$ code over $\text{GF}(7)$ with $A_7(C) \cong D^+_2$. Then there exists a skew-Hadamard matrix $H$ of order 20 such that $C$ is generated by the row vectors of $H + 2I$ over $\text{GF}(7)$.

**Proof.** Let $\Psi : A_7(C) \to D^+_2$ be an isomorphism. Since $\|\Psi(\varepsilon_j)\|^2 = \|\varepsilon_j\|^2 = 7$ is odd, $\Psi(\varepsilon_j) \notin D_{20}$. Thus $\Psi(\varepsilon_j) \in \frac{1}{2} \mathbf{1} + D_{20} \subset \frac{1}{2}(1 + 2\mathbb{Z})^{20}$, and hence there exist odd integers $f_{i,j}$ such that

$$\Psi(\varepsilon_j) = \frac{1}{2} \sum_{i=1}^{20} f_{i,j} e_i.$$ 

Let $F$ denote the $20 \times 20$ matrix whose $(i, j)$ entry is $f_{i,j}$. Then $F^T F = 28 \mathbf{1}$. In particular,

$$\sum_{h=1}^{20} f_{h,i}^2 = 28.$$ 

Since $f_{h,i}$ are odd integers, we see that there exists a unique $h_i$ such that $f_{h_i,i} = \pm 3$.

We claim that the mapping $i \mapsto h_i$ is a bijection from $\{1, \ldots, 20\}$ to itself. Indeed, suppose, for example, $h_1 = h_2 = 1$. Replacing $\varepsilon_1, \varepsilon_2$ by $-\varepsilon_1, -\varepsilon_2$, respectively, if necessary, we may assume $f_{1,1} = f_{1,2} = 3$. Since $f_{h,1} = \pm 1$ and $f_{h,2} = \pm 1$ for all $h \in \{2, \ldots, 20\}$ and

$$0 = \sum_{h=1}^{20} f_{h,1} f_{h,2}$$

$$= 9 + \sum_{h=2}^{20} f_{h,1} f_{h,2}$$

$$= 9 + \sum_{h=2}^{20} f_{h,1} f_{h,2}$$

$$= 9 + |\{h \mid 2 \leq h \leq 20, f_{h,1} = f_{h,2}\}|$$

$$- |\{h \mid 2 \leq h \leq 20, f_{h,1} = -f_{h,2}\}|$$

$$= 9 + |\{h \mid 2 \leq h \leq 20, f_{h,1} = f_{h,2}\}|$$

$$- (19 - |\{h \mid 2 \leq h \leq 20, f_{h,1} = f_{h,2}\}|)$$

$$= -10 + 2|\{h \mid 2 \leq h \leq 20, f_{h,1} = f_{h,2}\}|,$$

we see that there exists $h \in \{2, \ldots, 20\}$ such that $f_{h,1} = f_{h,2}$. Set $\xi = \Psi^{-1}(e_1 + f_{h,1} e_h)$. Then $\|\xi\|^2 = \|e_1 + f_{h,1} e_h\|^2 = 2$. However, for $i = 1, 2$, we have

$$(\xi, \varepsilon_i) = (\Psi(\xi), \Psi(\varepsilon_i)).$$
ON THE CLASSIFICATION OF SELF-DUAL [20, 10, 9] CODES OVER GF(7)

\[ \begin{aligned}
&= (e_1 + f_{h,1} e_h, \frac{1}{2} \sum_{j=1}^{20} f_{j,i} e_j) \\
&= \frac{1}{2} (f_{1,i} + f_{h,1} f_{h,i}) \\
&= 2.
\end{aligned} \]

This contradicts Lemma 3, and completes the proof of the claim.

Now we may assume without loss of generality

\[ f_{h,i} = \begin{cases} 
3 & \text{if } h = i, \\
\pm 1 & \text{otherwise}.
\end{cases} \]

Set \( H = F - 2I \). Then all the entries of \( H \) are \( \pm 1 \), and the diagonal entries are 1.

We claim \( H + H^\top = 2I \). To prove this, we need to show \( f_{h,i} + f_{i,h} = 0 \) for \( 1 \leq h < i \leq 20 \). Suppose \( f_{h,i} = f_{i,h} \) for some \( 1 \leq h < i \leq 20 \). Set \( \xi = \Psi^{-1}(e_h + f_{i,h} e_i) \). Then \( \|\xi\|^2 = \|e_h + e_i\|^2 = 2 \), and

\[ (\xi, \varepsilon_i) = (\Psi(\xi), \Psi(\varepsilon_i)) = (e_h + f_{i,h} e_i, \frac{1}{2} \sum_{j=1}^{20} f_{j,i} e_j) = \frac{1}{2} (f_{h,i} + f_{i,h} f_{i,i}) = 2 f_{i,h}. \]

Similarly,

\[ (\xi, \varepsilon_h) = (\Psi(\xi), \Psi(\varepsilon_h)) = (e_h + f_{i,h} e_i, \frac{1}{2} \sum_{j=1}^{20} f_{j,h} e_j) = \frac{1}{2} (f_{h,h} + f_{i,h}^2) = 2. \]

These contradict Lemma 3, and complete the proof of the claim.

Since

\[ H^\top H = (F^\top - 2I)(F - 2I) = 28I - 2(H^\top + H + 4I) + 4I = 20I, \]

\( H \) is a Hadamard matrix.
Finally, since

\[ D_{20}^2 \ni 2e_i \]

\[ = \frac{1}{14} \sum_{h=1}^{20} 28 \delta_{h,i} e_h \]

\[ = \frac{1}{14} \sum_{h=1}^{20} \sum_{j=1}^{20} f_{i,j} f_{h,j} e_h \]

\[ = \frac{1}{7} \sum_{j=1}^{20} f_{i,j} \sum_{h=1}^{20} f_{h,j} e_h \]

\[ = \frac{1}{7} \sum_{j=1}^{20} f_{i,j} \Psi(\varepsilon_j) \]

\[ = \Psi(\frac{1}{7} \sum_{j=1}^{20} f_{i,j} \varepsilon_j), \]

we have

\[ \frac{1}{7} \sum_{j=1}^{20} f_{i,j} \varepsilon_j \in A_7(C). \]

Thus the \( i \)-th row of \( F = H + 2I \) belongs to \( C \). The fact that \( F \) generates the self-dual code \( C \) follows from Lemma 2.

We say that skew-Hadamard matrices \( H \) and \( H' \) of order \( n \) are skew-Hadamard equivalent if there exists a \((1, -1, 0)\)-monomial matrix \( P \) with \( PHP^\top = H' \). Let \( H \) and \( H' \) be skew-Hadamard matrices of order 20. Let \( C(H) \) denote the code over \( \text{GF}(7) \) generated by the row vectors of \( H + 2I \). If \( H \) and \( H' \) are skew-Hadamard equivalent, then \( C(H) \) and \( C(H') \) are equivalent. By Proposition 4, we can convert the classification of self-dual \([20, 10, 9]\) codes \( C \) over \( \text{GF}(7) \) with \( A_7(C) \cong D_{20}^2 \) to that of skew-Hadamard matrices of order 20, up to skew-Hadamard equivalence. The existence of a skew-Hadamard matrix of order \( n \) is equivalent to the existence of a doubly regular tournament of order \( n - 1 \) [16]. It is known that there are two doubly regular tournaments of order 19, up to isomorphism (see [12]). This implies that there are two skew-Hadamard matrices of order 20, up to skew-Hadamard equivalence. Indeed, let \( H \) be a skew-Hadamard matrix of order 20 and let \( D \) be the diagonal matrix whose diagonal entries are the first row of \( H \). Then

\[ DHD = \begin{pmatrix} 1 & 1 \\ -1^\top & M \end{pmatrix}. \]
ON THE CLASSIFICATION OF SELF-DUAL [20, 10, 9] CODES OVER GF(7)

Here the 19 × 19 (1, 0)-matrix \((M + J)/2 - I\) is the adjacency matrix of a doubly regular tournament of order 19, where \(J\) is the 19 × 19 all-one matrix. Hence, isomorphic doubly regular tournaments of order 19 give skew-Hadamard matrices of order 20, which are skew-Hadamard equivalent. The matrices \(S_1\) and \(S_2\) in Figure 1 give the two skew-Hadamard matrices of order 20, up to skew-Hadamard equivalence.

We have verified by MAGMA that the two self-dual codes \(C(S_1)\) and \(C(S_2)\) have the following weight enumerators:

\[
W(C(S_1)) = 1 + 6840y^9 + 47880y^{10} + 200640y^{11} + 957600y^{12} + 3625200y^{13} + 10766160y^{14} + 25701984y^{15} + 48495600y^{16} + 68276880y^{17} + 68299680y^{18} + 43155840y^{19} + 12940944y^{20},
\]

\[
W(C(S_2)) = 1 + 1080y^8 + 5040y^9 + 40320y^{10} + 215760y^{11} + 977040y^{12} + 3571200y^{13} + 10751040y^{14} + 25814304y^{15} + 48431880y^{16} + 68208840y^{17} + 68403000y^{18} + 43106160y^{19} + 12949584y^{20},
\]

respectively. In particular, \(C(S_1)\) is a \([20, 10, 9]\) code, while \(C(S_2)\) has minimum weight 8. By Proposition 4, \(C(S_1)\) is a unique self-dual \([20, 10, 9]\) code over GF(7) with \(A_7(C) \cong D_{20}^+\). This completes the proof of Theorem 1.

4. SOME OTHER CONSTRUCTIONS OF SELF-DUAL [20, 10, 9] CODES

Finally, in this section, we investigate some other constructions of self-dual \([20, 10, 9]\) codes over GF(7). In the above classification, we employed \((1, -1, 0)\)-monomial matrices in the definition for equivalence of codes. In some earlier work, a weaker equivalence is used. We say that two codes \(C\) and \(C'\) over GF(7) are monomially equivalent if there exists a monomial matrix \(M\) over GF(7) with \(C' = \{cM \mid c \in C\}\). Clearly, if \(C\) and \(C'\) are equivalent, then they are monomially equivalent.

Note that \(D_{20}^+\) is the unique 20-dimensional unimodular lattice with minimum norm 2 and kissing number 760. For a given self-dual \([20, 10, 9]\) code \(C\) over GF(7), one can determine whether \(A_7(C)\) is isomorphic to \(D_{20}^+\) or not, by computing the kissing number of \(A_7(C)\) by MAGMA. If \(A_7(C)\) is isomorphic to \(D_{20}^+\), then by Theorem 1, we have that \(C\) is equivalent to \(C(S_1)\).

- Some self-dual \([20, 10, 9]\) codes over GF(7) were constructed in [4, Table 6] and [5, Table 7] as double circulant codes and
quasi-twisted self-dual codes, respectively (see [5] for the construction). It was verified by MAGMA that all double circulant self-dual [20, 10, 9] codes and all quasi-twisted self-dual [20, 10, 9] codes are monomially equivalent [5, Section 4.3].

By exhaustive search, we have verified that $A_7(C) \cong D_{20}^+$ for all double circulant self-dual [20, 10, 9] codes $C$. Also, we have verified that $A_7(C) \cong D_{20}^+$ for all quasi-twisted self-dual [20, 10, 9] codes $C$.

- Let $A$ and $B$ be $5 \times 5$ circulant (resp. negacirculant) matrices. A [20, 10] code over $\text{GF}(7)$ with the following generator matrix

\[
\begin{pmatrix}
I & A & B \\
-B^\top & A^\top \\
\end{pmatrix}
\]

is called a four-circulant (resp. four-negacirculant) code. By exhaustive search, we have verified that $A_7(C) \cong D_{20}^+$ for all four-circulant self-dual [20, 10, 9] codes $C$. Also, we have verified that $A_7(C) \cong D_{20}^+$ for all four-negacirculant self-dual [20, 10, 9] codes $C$.

- Let $C$ be a self-dual code of length 20 over $\text{GF}(7)$. Let $x$ be a vector with $x \cdot x = 0$. Then $C_x = \langle C \cap \langle x \rangle^\perp, x \rangle$ is a self-dual code over $\text{GF}(7)$. By exhaustive search, we have verified that $A_7(C(S_1)_x) \cong D_{20}^+$ for all $x$ with $x \cdot x = 0$.

Moreover, our extensive search failed to discover a self-dual [20, 10, 9] code $C$ over $\text{GF}(7)$ with $A_7(C) \not\cong D_{20}^+$. We are lead to conjecture that $C(S_1)$ is a unique self-dual [20, 10, 9] code over $\text{GF}(7)$.

**Acknowledgments.** The authors would like to thank Sho Suda for useful discussions. This work is supported by JSPS KAKENHI Grant Number 26610032.

**References**


ON THE CLASSIFICATION OF SELF-DUAL [20,10,9] CODES OVER GF(7)


Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan
E-mail address: mharada@m.tohoku.ac.jp

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan
E-mail address: munemasa@math.is.tohoku.ac.jp