Skew Hadamard Designs and Their Codes

Jon-Lark Kim[1] and Patrick Solé[2]

[1] Department of Mathematics, University of Louisville
Louisville KY 40292, USA,
jl.kim@louisville.edu,

[2] CNRS, I3S, Les Algorithmes - bt. Euclide B, BP.121, 2000
route des Lucioles, 06 903 Sophia Antipolis Cedex, France,
sole@unice.fr

Abstract. Skew Hadamard designs $(4n-1, 2n-1, n-1)$ are associated to order $4n$ skew Hadamard matrices in the natural way. We study the codes spanned by their incidence matrices A and by $I+A$ and show that they are self-dual after extension (resp. extension and augmentation) over fields of characteristic dividing n. Quadratic Residues codes are obtained in the case of the Paley matrix. Results on the $p-$rank of skew Hadamard designs are rederived in that way. Codes from skew Hadamard designs are classified. A new optimal self-dual code over $\mathbb{F}_5$ is constructed in length 20. Six new inequivalent $[56, 28, 16]$ self-dual codes over $\mathbb{F}_7$ are obtained from skew Hadamard matrices of order 56, improving the only known quadratic double circulant code of length 56 over $\mathbb{F}_7$.

1 Introduction

In $[2, 1]$ a systematic study of the codes of the designs of Hadamard matrices was undertaken. With a Hadamard matrix H of order $4n$ can be attached a $3-$design $\mathcal{T}$ of parameters $3-(4n, 2n, n-1)$. The derived design $\mathbf{D}$ has parameters $2-(4n-1, 2n-1, n-1)$. The code $C_p(\mathcal{T})$ is self-orthogonal. If, furthermore, H is skew Hadamard (or SH), then $C_p(\mathcal{T})$ is self-dual [11].

In this article we give an independent coding theoretic proof of the latter result. We study the codes spanned by the incidence matrices of $\mathbf{D}$ and of its complement and show that they are self dual after extension (resp. extension and augmentation) over fields of characteristic dividing n. Quadratic Residues codes are obtained in the case of the Paley matrix. We classify self-dual codes from skew Hadamard matrices of order $4n$ $(2 \le n \le 7)$ and enumerate self-dual codes from skew Hadamard matrices of order $4n$ $(8 \le n \le 15,\ n = 18, 21)$. In particular, a new optimal self-dual code over $\mathbb{F}_5$ is constructed in length 20. We also find six new inequivalent $[56, 28, 16]$ self-dual codes over $\mathbb{F}_7$ from skew Hadamard matrices of order 56. These are inequivalent to the only known quadratic double circulant code of length 56 over $\mathbb{F}_7$ [3].

2 Skew Hadamard Designs

Let A be the incidence matrix of a skew Hadamard design of parameters $(4n-1, 2n-1, n-1)$ over a field F of characteristic p. By definition it is a matrix A of order $4n-1$ satisfying

$$AA^T = nI + (n-1)J \tag{1}$$

and

$$AJ = JA = (2n-1)J. \tag{2}$$

The skewness property translates into A being the adjacency of a tournament digraph, that is,

$$A + A^T + I = J. \tag{3}$$

In all the article, we assume that p divides n. As a consequence

$$AA^T = -J.$$

The following result is proved in [11] building on Sylvester's law of nullity for a matrix product [12, Thm. 5.6.2, Thm. 5.6.5].

Proposition 1. *(T.S. Michael) The $p-$rank of A (resp. $J-A$) is $2n$ (resp. $2n-1$).*

We give an independent proof based on coding theory. Let $C(A) = \langle A^+ \rangle$ denote the $F-$ span of A^+, which is A extended by an all-one column. In the notations of [2] this is the code $C_p(\mathcal{T})$ of the $3-$ design $\mathcal{T}$. Let $D(A)$ denote $\langle (I+A)^- \rangle$ augmented by the all-one vector. Here M^- denotes M extended by an all-zero column. By $rk(M)$ we denote the rank of M over F. The following result implies the preceding proposition.

Proposition 2. *The codes $C(A)$ and $D(A)$ are self-dual over F.*

Proof. First, we observe that $\langle I + A \rangle$ is self-orthogonal by computing, using equations (1) and (3), the product $(A+I)(A+I)^T = AA^T + J = O$. Hence $rk(A+I) \leq 2n-1$. By a similar argument $C(A)$ is self-orthogonal and $rk(A) \leq 2n$. Adding up these two bounds we obtain

$$rk(A+I) + rk(A) \leq 4n-1. \tag{4}$$

Next, the eigenspaces of A wrt 0 and -1 are disjoint, and this entails

$$rk(A+I) + rk(A) \geq 4n-1. \tag{5}$$

Equations (4) and (5) together imply that equality holds in all preceding inequalities.

Note that in general for an arbitrary Hadamard matrix one has only an upper bound on the $p-$rank [2, Th. 7.4.1]. The next result is well-known for QR codes over $GF(2)$ of length a multiple of 8.

Corollary 1. *When $F = GF(2)$ the codes $C(A)$ and $D(A)$ are Type II. Further $\langle I + A^T\rangle$ is the even part of $\langle A\rangle$. In fact $\langle A\rangle = \langle I + A^T\rangle \oplus \mathbf{1}$.*

Proof. The first statement is immediate by the fact that all rows of A have weight $2n - 1$. The second statement comes from the relation

$$A(I + A^T)^T = A(J - A)^T = A(J - A^T) = nJ = O,$$

a direct consequence of equations (2) and (1). This implies that $\langle I+A^T\rangle \subseteq \langle A\rangle^\perp$. This bound is an equality by dimension count. Hence $\langle I+A^T\rangle^\perp = \langle A\rangle$. The code $\langle I + A^T\rangle$ is even, being self-orthogonal. The result follows.

3 Extended QR Codes from Paley Hadamard Matrices

We recall a definition of a Quadratic Residue (QR) code of prime length l over $GF(p)$, where p is another prime which is a quadratic residue mod l (here we interchange p and l in [10, Ch. 16]). Let Q be the set of quadratic residues modulo l, and N the set of nonresidues modulo l. The set Q is closed under multiplication by p as $p \in Q$. Let α be a primitive lth root of unity in some extension of $GF(p)$. Let $q(x) = \prod_{r\in Q}(x - \alpha^r)$. Define the *QR code* $\mathcal{Q}$ to be the cyclic code of length l over $GF(p)$ with generator polynomial $q(x)$. Define $\theta := \sum_{i=1}^{l-1} \left(\frac{i}{l}\right) \alpha^i$ to be the Gaussian sum, where α is a primitive lth root of unity in some extension of $GF(p)$ and $\left(\frac{i}{l}\right)$ is the Legendre symbol. Note that $\theta \in GF(p)$. Further the following is known [10, Ch. 16].

Lemma 1. *If $l \equiv -1 \pmod 4$, then $\theta^2 = -l$.*

Proposition 3. *Let $l := 4n - 1$ be a prime and p be a prime dividing n such that p is a quadratic residue mod l. Suppose H is the Paley Hadamard matrix of order $4n$. Let A be the associated incidence matrix from H. Then $C(A)$ is the extended quadratic residue code $\hat{\mathcal{Q}}$ over $GF(p)$.*

Proof. First we calculate the idempotent of the quadratic residue code $\mathcal{Q}$ of a prime length l over $GF(p)$ in terms of residues and nonresidues mod l. In fact, the idempotent of the quadratic residue code $\mathcal{Q}$ of a prime length l over $GF(p)$ is given in [10, Theorem 4, Ch. 16] as follows.

$$E_q(x) = \frac{1}{2}\left(1 + \frac{1}{l}\right) + \frac{1}{2}\left(\frac{1}{l} - \frac{1}{\theta}\right)\sum_{r\in Q} x^r + \frac{1}{2}\left(\frac{1}{l} + \frac{1}{\theta}\right)\sum_{n\in N} x^n.$$

Here θ is the Gaussian sum given above. Then θ satisfies $\theta^2 = -l$ by Lemma 1. As $l \equiv -1 \pmod p$, we get $\theta^2 = 1 \pmod p$, so $\theta = \pm 1$. If $\theta = -1$ then we choose the primitive element α so that $\theta = 1$ (for example, let $\beta := \alpha^c$ where $\left(\frac{c}{l}\right) = -1$. Then the Gaussian sum based on β becomes 1). Hence $E_q(x) = -\sum_{r\in Q} x^r$. It is not difficult to check that the extended code $\hat{\mathcal{Q}}$ is the same as $C(A)$.

A duadic code is a class of cyclic codes generalizing quadratic residue codes [7]. A *multiplier* μ_a of $\mathbb{F}_p[x]/(x^n-1)$ is a ring automorphism induced by $x \mapsto x^a$. A *cyclotomic coset* is an orbit of μ_p on $\mathbb{Z}_n$, where assume n and p are coprime. A *splitting* is a partition of $\mathbb{Z}_n \setminus 0$ into two unions of cyclotomic cosets U_1 and U_2 swapped by a multiplier. Attached duadic codes have characteristic sets U_1, U_2 (odd-like case) or U_1+0, U_2+0 (even like case). Extension of odd like duadic codes are self dual when $a=-1$. Quadratic Residue codes correspond to U_i the set of squares of $\mathbb{Z}_n$, for n prime.

In [14] Pless related binary duadic codes to cyclic even tournaments. The adjacency matrix A of a tournament digraph is called **cyclic** [14] if each row of A is a cyclic shift of the previous row and **even** if $AA^T \equiv I \pmod 2$.

We note that our matrix A is not even as $AA^T \equiv -J \pmod p$. But if we assume that A is cyclic, then we obtain duadic codes over $GF(p)$ from A as follows.

Lemma 2. [7, Theorem 6.4.1] *Let C be any $[n,(n-1)/2]$ cyclic code over $GF(q)$, where q is a power of a prime p. Then C is self-orthogonal if and only if C is an even-like duadic code whose splitting is given by μ_{-1}.*

Proposition 4. *Suppose that A is the cyclic incidence matrix of a skew Hadamard design of parameters $(4n-1, 2n-1, n-1)$. Let $C_1 := \langle I+A \rangle$ be the code over F generated by the rows of $I+A$ and let $C_2 := \langle I+A^T \rangle$. Similarly let $D_1 := \langle A^T \rangle$ and $D_2 := \langle A \rangle$. Then the following hold.*

1. *C_i $(i=1,2)$ is an even-like duadic code over F whose splitting is given by μ_{-1}.*
2. *D_i is the odd-like duadic code of C_i $(i=1,2)$ whose splitting is given by μ_{-1}.*

Proof. We have shown in the proof of Proposition 2 that C_1 (similarly C_2) is self-orthogonal over F with dimension $2n-1$. Hence the first statement follows from Lemma 2. Following the proof of Corollary 1, we see that C_i is a codimension one subcode of D_i $(i=1,2)$. As $\mathbf{1}$ is not in C_i $(i=1,2)$, D_i is the odd-like duadic code of C_i $(i=1,2)$.

Applying the square root bound of duadic codes (cf. [7, Theorem 6.5.2]), we get the square root bound of duadic codes from the cyclic incidence matrix of a skew Hadamard design of parameters $(4n-1, 2n-1, n-1)$.

Corollary 2. (Square Root Bound) *Let D_i $(i=1,2)$ of length $4n-1$ be as above. Let d_0 be their (common) minimum odd-like weight. Then the following hold.*

1. *$d_0^2 - d_0 + 1 \geq 4n-1$.*
2. *Suppose $d_0^2 - d_0 + 1 = 4n-1$ where $d_0 > 2$, then for $i=1,2$*
   (a) *d_0 is the minimum weight of D_i.*

(b) *the supports of the minimum weight codewords of* D_i *form a cyclic projective plane of order* $d_0 - 1$.
(c) *the minimum weight codewords of* D_i *are multiples of binary vectors.*
(d) *there are exactly* $(4n-1)(p-1)$ *minimum weight codewords in* D_i.

Generalizations of the last two results to the case when $\mathbf{D}$ is an abelian difference set are in [18].

4 Their Codes

In this section, we classify or enumerate self-dual codes from SH matrices of reasonable sizes. In the following, we do not mention the case when H is the Paley Hadamard (PH) matrix, as this leads to quadratic residue codes.

4.1 $n = 2$ or 3

There is a unique SH matrix of order 8 [9], whose $C(A)$ is the binary Hamming $[8, 4, 4]$ code. Similarly there is a unique SH matrix of order 12 [9], whose $C(A)$ is the ternary Golay $[12, 6, 6]$ code. These can be explained from Proposition 3.

4.2 $n = 4$

It is well known that there are two SH matrices of order 16. These matrices can be constructed from the adjacency matrix A of the unique 2-class association scheme of order 15 [5] and its transpose A^T. We construct two inequivalent extremal Type II $[16, 8, 4]$ codes of length 16 from $C(A)$ and $C(A^T)$. As there exist only two such codes, we have shown that every extremal Type II code of length 16 can be obtained from a SH matrix of order 16.

4.3 $n = 5$

It is known that there are exactly two SH matrices, one being PH. Again these matrices can be obtained from the two 2-class Association schemes [5]. We construct two inequivalent optimal $[20, 10, 8]$ self-dual codes over $GF(5)$. More precisely, No. 2 of [5] is not of Paley type and gives a new $[20, 10, 8]$ self-dual code SH_{20} over $GF(5)$ by construction $C(A)$. Its order of the automorphism group is $2^9 \cdot 3 \cdot 5$. Previously there were known only two self-dual $[20, 10, 8]$ codes over $GF(5)$, denoted by QDC_{20} and XQ_{19} [4] whose group orders are $2^8 \cdot 3^2 \cdot 5$ and $2^4 \cdot 3^2 \cdot 5 \cdot 19$, respectively. We recall that there are three inequivalent Hadamard matrices of order 20 [20]. We have checked that the second and the third Hadamard matrices in [20] produce SH_{20} and XQ_{19}, respectively while the first Hadamard matrix in [20] produce QDC_{20}. Therefore we have shown the following.

Proposition 5. *There exist at least three optimal* $[20, 10, 8]$ *self-dual codes over* $GF(5)$*, all of which are from Hadamard matrices of order* 20*, two being from skew Hadamard matrices of order* 20.

4.4 $n = 6$

There are (up to equivalence) 16 SH matrices, one being PH. We use the classification given by Spence [21]. Binary and ternary codes of length 24 are obtained as follows. Assmus and Key [1] described in detail the binary and ternary codes from Hadamard matrices of order 24, but they did not consider which codes are from skew Hadamard matrices. We have checked that there are exactly six Type II codes from the 16 SH matrices, one of them is the extended Golay code G_{24} of length 24 and the other have minimum weight 4. For detail, see Table 1. Here the first column refers to the binary Type II codes from [15] and the second column refers to the indices of the skew Hadamard matrices in [21].

Further the 16 SH matrices produce exactly 9 Type III codes of length 24. Two such codes are the extended QR code of length 24 and the symmetry code of length 24.

Table 1. Type II codes from the 16 skew Hadamard matrices of order 24

Codes [15]	skew Hadamard matrices [21]
F_{24}	$\{1, 3, 11, 12\}$
D_{24}	$\{2, 4, 7, 8, 13\}$
C_{24}	$\{5, 9, 10\}$
A_{24}	$\{6\}$
E_{24}	$\{15\}$
G_{24}	$\{14, 16\}$

4.5 $n = 7$

The 65 skew Hadamard matrices of order 28 in [21, p. 239–243] is reduced to the 54 inequivalent SH matrices, one being PH [21]. For example, the SH matrix with No. 11 in [21] is equivalent to the SH matrix with No. 7in [21] since both come from the Hadamard matrix with No. 233 in [21, p. 217].

We consider codes over $GF(7)$ of length 28. Each matrix using the construction $C(A)$ produces a self-dual $[28, 14, 9]$ code over $GF(7)$ and the 54 codes obtained this way are all inequivalent as one might expect. In Table 2, we describe the orders of the permutation automorphism groups of the 54 codes. It is interesting to compare the orders of the SH matrices with those of the corresponding codes. For example, the orders of the automorphism groups of the SH matrices with No. 1 and 2 [21] are 2 and 1 respectively while the group orders of the corresponding codes are 12 and 6 respectively. In most cases, the group order of the code is $6\times$(the group order of the SH matrix).

We note that these codes have minimum weight one less than the best known $[28, 14, 10]$ codes [4].

Table 2. Orders of the permutation automorphism groups of self-dual $[28, 14, 9]$ codes over $GF(7)$ from the 54 SH matrices of order 28

|PAut(C)|	skew Hadamard matrices [21]
6	$\{2, 7, 8, 9, 16\}$
12	$\{1, 3, 4, 6, 17, 29, 30, 31, 34, 37\}$
18	$\{5, 12, 23, 33, 42, 45, 46, 47, 51, 53\}$
24	$\{14, 44\}$
36	$\{13, 19, 24, 26, 28, 35, 38, 40, 43\}$
48	$\{10, 20\}$
54	$\{41\}$
72	$\{21, 22, 25, 49, 50, 55, 56, 58, 60, 61, 62\}$
144	$\{36\}$
162	$\{57\}$
6552	$\{63\}$
176904	$\{65\}$

4.6 $n = 8$

There are ≥ 6 SH matrices, one being PH [19]. We only get binary Type II codes of length 32 by Corollary 1. It is known [7] that there are exactly two binary extended duadic self-dual codes of length 32, one of which is the extended binary QR code of length 32. The QR code is constructed from the PH matrix of order 32 by Proposition 4. We omit the detail.

4.7 $n = 9$

There are ≥ 18 SH matrices of order 36 [9]. Using the file in [9], the 15th and 16th matrices with construction $C(A)$ produce two inequivalent $[36, 18, 9]$ ternary self-dual codes (see Table 3). On the other hand, the rest matrices with construction $C(A)$ produce inequivalent $[36, 18, 6]$ ternary self-dual codes. Other constructions $D(A)$, $C(A^T)$, and $D(A^T)$ produce the same set of codes as $C(A)$. We mention that there is only one known ternary self-dual code of length 36 with $d = 12$, called the Pless symmetry code.

Table 3. Two self-dual $[36, 18, 9]$ codes over $GF(3)$ from the SH matrices of order 36

skew Hadamard matrices [9]	Weight Enumerator	|PAut(C)|
$\{15\}$	$1 + 208y^9 + 40968y^{12} + 1407744y^{15} + \cdots$	8
$\{16\}$	$1 + 544y^9 + 37944y^{12} + 1419840y^{15} + \cdots$	8

4.8 $n = 10$

There are ≥ 22 SH matrices of order 40 [9]. Over $GF(2)$, construction $C(A)$ produces exactly 8 inequivalent extremal Type II binary $[40, 20, 8]$ codes while the rest are Type II $[40, 20, 4]$ codes. Similarly, over $GF(5)$ we obtain one $[40, 20, 11]$ self-dual code, 12 $[40, 20, 10]$ self-dual codes, and 9 $[40, 20, 8]$ self-dual codes. All of these codes over $GF(5)$ are inequivalent. See Table 4 for detail, where the third column follows the index of the matrices in [9], and $12(\cong 2)$ (similarly for two others) means that the corresponding binary codes are equivalent. We remark that the 8 binary Type II codes in the third row of Table 4 have automorphism group orders $64, 1, 768, 32768, 768, 12, 1536, 8$, respectively.

We note that the quadratic double circulant (self-dual) code of length 40 over $GF(5)$ has the largest known minimum distance 13 [3], which is, therefore, two larger than the above best code.

Table 4. Self-dual $[40, 20]$ codes from the 22 SH matrices of order 40

Over $GF(q)$	Min. Dis. d	skew Hadamard matrices [9]
$q = 2$	$d = 4$	$\{2, 3, 4, 6, 8, 9, 12(\cong 2), 14(\cong 6), 15, 16(\cong 6), 18, 19, 21, 22\}$
	$d = 8$	$\{1, 5, 7, 10, 11, 13, 17, 20\}$
	$d = 8$	$\{5, 6, 7, 9, 13, 14, 15, 20, 22\}$
$q = 5$	$d = 10$	$\{1, 2, 4, 8, 10, 11, 12, 16, 17, 18, 19, 21\}$
	$d = 11$	$\{3\}$

4.9 $n = 11$

There are ≥ 59 SH matrices of order 44 [9]. We consider self-dual codes over $GF(11)$ by construction $C(A)$. More precisely, we get exactly 9 $[44, 22, 14]$ self-dual codes, 37 $[44, 22, 13]$ self-dual codes, 10 $[44, 22, 12]$ self-dual codes, and 3 $[44, 22, 11]$ self-dual codes. See Table 5 for detail.

Table 5. Self-dual $[44, 22]$ codes over $GF(11)$ from the 59 SH matrices of order 44

Min. Dis. d	skew Hadamard matrices [9]
$d = 11$	$\{9, 12, 39\}$
$d = 12$	$\{6, 8, 11, 13, 14, 23, 35, 36, 42, 49\}$
$d = 13$	the rest
$d = 14$	$\{1, 5, 18, 19, 28, 29, 44, 51, 56\}$

4.10 $n = 12$ or 13

The PH matrix of order 48 is the only known SH matrix of that order [9]. Since 2 and 3 are quadratic residues modulo 47, $C(A)$ are quadratic residue codes over $GF(2)$ or $GF(3)$ by Proposition 3.

Let us consider $n = 13$. There are ≥ 561 SH matrices of order 52. The first SH matrix of order 52 in [9] gives a self-dual $[52, 26, 16]$ code over $GF(13)$. This minimum distance is somewhat high. We do not compare this with other possible codes since few self-dual codes over $GF(13)$ are known. We stop considering remaining matrices due to a computational complexity.

4.11 $n = 14$

In [8] 75 SH matrices of order 56 are given. We consider self-dual codes over $GF(2)$ and $GF(7)$. Interesting codes are obtained. In particular, we have checked that there are exactly five extremal Type II $[56, 28, 12]$ codes from the 75 SH matrices and that only three of the five are inequivalent and they have group orders 24, 168, 168, respectively. It is known that there are 16 Type II $[56, 26, 12]$ codes with automorphism of order 13 [22]. So our codes are inequivalent to these codes. Later, Harada [6] constructed at least 1135 Type II $[56, 26, 12]$ codes from self-orthogonal 3-$(56, 12, 65)$ designs. It will be interesting to check the equivalence of our codes with his codes.

On the other hand, there are self-dual codes over $GF(7)$ with minimum distance d from 10 to 16. The detail is given in Table 6. There is only one known (quadratic double circulant) self-dual code, denoted by $C_{7,56}$, over $GF(7)$ with minimum distance $d = 16$ [4], [3]. We have checked by Magma that the six nonequivalent codes with $d = 16$ in Table 6 are not equivalent to $C_{7,56}$. We observe that none of these six codes obtained in length $56 = 1 + 55$ is the extended quadratic residue code of length 56 over $GF(7)$.

Since 7 (resp. 2) is not a square (mod 55), the 75 self-dual codes from SH matrices over $GF(7)$ (resp. $GF(2)$) are not even-like duadic codes.

As a summary, we have the following.

Proposition 6. *1. There are exactly five extremal Type II* $[56, 28, 12]$ *codes from the known* 75 *SH matrices of order* 56*, three of which are not equivalent to each other.*

2. There exist at least seven inequivalent $[56, 28, 16]$ *self-dual codes over* $GF(7)$*, six of which are from SH matrices of order* 56*.*

4.12 $n = 15$

There are ≥ 22 SH matrices of order 60 [8]. Since $15 = 3 \cdot 5$, we have self-dual codes over $GF(3)$ and $GF(5)$. More precisely, we obtain 14 ternary self-dual $[60, 30, 12]$ codes and 8 ternary self-dual $[60, 30, 9]$ codes. We have checked that the 22 codes are all inequivalent. We remark that the best known two ternary

Table 6. Self-dual $[56, 28]$ codes from the 75 SH matrices of order 56

Over $GF(q)$	Min. Dis. d	skew Hadamard matrices [9]
	$d = 4$	the rest
$q = 2$	$d = 8$	$\{2, 3, 10(\cong 2), 12, 17, 21, 24(\cong 12), 25, 26(\cong 17), 37(\cong 3), 40(\cong 3), 47(\cong 17), 50, 51, 53, 54, 55, 56(\cong 55), 57(\cong 53), 58, 59, 61(\cong 54), 62(\cong 53), 63(\cong 55), 64(\cong 54), 68, 69, 70, 71, 72(\cong 50), 73(\cong 51), 74(\cong 58), 75(\cong 59)\}$
	$d = 12$	$\{52, 60(\cong 52), 65, 66(\cong 52), 67\}$
	$d = 10$	$\{2, 3, 48, 49\}$
	$d = 11$	$\{1, 4, 5, 24\}$
	$d = 12$	$\{6, 40, 47, 63, 66, 72\}$
$q = 7$	$d = 13$	$\{9, 10, 12, 13, 15, 17, 20, 21, 23, 25, 26, 29, 30, 33, 37, 38\}$
	$d = 14$	$\{11, 14, 16, 42, 45, 53, 57, 58, 65, 72, 73, 75\}$
	$d = 15$	the rest
	$d = 16$	$\{18, 22, 31, 36, 62, 68\}$

self-dual codes of length 60 have minimum distance 18 [4]. Over $GF(5)$ we obtain seven self-dual $[60, 30, 15]$ codes, eight self-dual $[60, 30, 14]$ codes, four self-dual $[60, 30, 13]$ codes, two self-dual $[60, 30, 12]$ codes, and one self-dual $[60, 30, 10]$ codes. The best known two self-dual codes over $GF(5)$ of length 60 is 18 [4].

Table 7. Self-dual $[60, 30]$ codes from the 22 SH matrices of order 60

Over $GF(q)$	Min. Dis. d	skew Hadamard matrices [8]
$q = 3$	$d = 9$	$\{1, 5, 7, 13, 14, 16, 18, 19\}$
	$d = 12$	$\{2, 3, 4, 6, 8, 9, 10, 11, 12, 15, 17, 20, 21, 22\}$
	$d = 10$	$\{8\}$
	$d = 12$	$\{12, 17\}$
$q = 5$	$d = 13$	$\{13, 14, 15, 16\}$
	$d = 14$	$\{1, 2, 3, 4, 5, 10, 11, 21\}$
	$d = 15$	$\{6, 7, 9, 18, 19, 20, 22\}$

4.13 $n = 18$

There are at least ≥ 990 SH matrices of order 72 [8]. We have checked that these produce Type II codes with minimum distance $d = 4, 8$, and 12. In fact, we have plenty of Type II $[72, 36, 12]$ codes with distinct weight enumerators. More detail will be added. $d = 16$ is open for Type II codes of length 72. We also have Type III codes with minimum distances in the set $\{9, 12, 15\}$. The extended quadratic residue code XQ_{71} over $GF(3)$ has $d = 18$, and this is the only known code.

4.14 $n = 21$

There are at least ≥ 720 SH (non PH) matrices of order 84 [9]. We obtain Type III codes with minimum distances in the set $\{9, 15, 18\}$. The optimal distance (obtained for QR_{83}) is 21.

5 Conclusion and Open Problems

In this paper, we have given a coding theoretic proof of Michael's result [11] that the p-rank of a skew Hadamard design $\mathbf{D}$ of parameters $(4n-1, 2n-1, n-1)$ over a field of characteristic p where $p|n$ is $2n$. We thus have shown that the extension of the corresponding incidence matrix produces self-dual codes over $\mathbb{F}_p$. We also have classified self-dual codes from skew Hadamard matrices of order $4n$ $(2 \leq n \leq 7)$ and have enumerated self-dual codes from skew Hadamard matrices of order $4n$ $(8 \leq n \leq 15,\ n = 18, 21)$. In particular, we have a new optimal self-dual $[20, 10, 8]$ code over $\mathbb{F}_5$ and six new optimal self-dual $[56, 28, 16]$ codes over $\mathbb{F}_7$.

We list some interesting problems for future work as follows.

1. Study self-dual codes over rings, in particular, over $\mathbb{Z}_4$ from SH matrices.
2. Give exhaustive lists of SH matrices for $n = 8$ and $n = 16$.
3. Is there a square Root bound for self-dual codes from SH matrices?
4. Are there Abelian codes from SH matrices?

Acknowledgement: Both authors are thankful to T.S. Michael for providing reference [12] and to E. Spence for explaining his paper [21]. The first author acknowledges partial support by a Project Completion Grant from the University of Louisville.

References

1. Assmus, Jr. E. F., Key, J. D.: Hadamard Matrices and Their Designs: A Coding-Theoretic Approach. Transactions of the American Mathematical Society. **330** No. 1 (1992) 269–293.
2. Assmus, Jr. E. F., Key, J. D.: *Designs and their Codes.* Cambridge (1992).
3. Gaborit, P.: Quadratic double circulant codes over fields. J. Combin. Th. A **97** (2002) 85–107.
4. Gaborit, P.: `http://www.unilim.fr/pages_perso/philippe.gaborit/SD/`
5. Hanaki, A, Miyamoto, I.: `http://kissme.shinshu-u.ac.jp/as/`
6. Harada, M: Self-orthogonal 3-$(56, 12, 65)$ designs and extremal doubly-even self-dual codes of length 56, Designs, Codes, and Crypt., **38** (2006) 5–16.
7. Huffman, W.C., Pless, V.S.: *Fundamentals of Error-correcting Codes.* Cambridge: Cambridge University Press, (2003).
8. Kotsireas, I: `http://www.medicis.polytechnique.fr/~kotsirea/`
9. Koukouvinos, C.: `http://www.math.ntua.gr/people/ckoukouv/hadamard.htm`

10. MacWilliams,F.J., Sloane, N.J.A.: *The Theory of Error Correcting Codes.* (1981) North Holland.
11. Michael, T.S.: The p-ranks of skew Hadamard designs. J. of Comb. Theory series A. **73** (1996) 170–171.
12. Mirsky, L.: *An Introduction to Linear Algebra.* Dover edition, 1990.
13. Pless, V.: On a new family of symmetry codes and related new 5-designs. Bull. AMS. **75** (1969) 1339–1342.
14. Pless, V.: Duadic codes and generalizations. Eurocode '92 (Udine, 1992), 3–15, CISM Courses and Lectures, 339, Springer, Vienna, (1993).
15. Pless, V., Sloane, N.J.A.: On the classification and enumeration of self-dual codes. J. Combin. Th. A **18** (1975) 313–335.
16. Rains, E., Sloane, N.J.A.: Self-dual codes. in the Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, (1998), 177-294.
17. Reid, K.B., Brown, E.: Doubly regular tournaments are equivalent to skew Hadamard matrices. J. of Comb. Theory series A. **12** (1972) 332–338.
18. J.J. Rushanan, Duadic Codes and Difference Sets, J. of Comb. Theory series A. **57** (1991) 254–261.
19. Seberry, J., Yamada, M.: Hadamard matrices, sequences, and block designs in: J.H. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory: A Collection of Surveys, John Wiley, New York, (1992) 431–560.
20. Spence, E.: `http://www.maths.gla.ac.uk/~es/hadamard.html`
21. Spence, E.: Classification of Hadamard matrices of order 24 and 28. Discrete Math. **140** No. 1-3 (1995) 185–243.
22. Yorgov, V: A method for constructing inequivalent self-dual codes with applications to length 56, IEEE Trans. Inform. Theory, **33** (1987) 72-82.