A Method for Constructing Self-Dual Codes with an Automorphism of Order 2

Stefka Bouyuklieva

Abstract—**In this paper, we investigate binary self-dual codes with an automorphism of order 2 with c cycles and f fixed points. A method for constructing such codes using self-orthogonal codes of length c and self-dual codes of length f is presented. We apply this method to construct extremal self-dual codes of lengths $40, 42, 44, 52, 54$, and 58. Some of them have weight enumerators for which self-dual codes were previously not known to exist. We prove that there do not exist self-dual $[50, 25, 10]$ and $[96, 48, 20]$ codes with an automorphism of order 2 with f fixed points for $f > 0$ in their automorphism groups.**

Index Terms—**Automorphisms, self-dual codes, weight enumerators.**

I. INTRODUCTION

A BINARY linear $[n, k]$ code C is a k-dimensional subspace of F_2^n where F_2^n is the n-dimensional vector space over the binary field F_2. The number of nonzero coordinates of a vector in F_2^n is called its weight. An $[n, k, d]$ code is an $[n, k]$ linear code with minimum nonzero weight d. An automorphism of the code C is a permutation of the coordinates of C which preserves C.

Let

$$u \cdot v = \sum_{i=1}^{n} u_i v_i \in F_2$$

for $u = (u_1, \cdots, u_n)$, $v = (v_1, \cdots, v_n) \in F_2^n$ be the inner product in F_2^n. Then if C is an $[n, k]$ code over F_2,

$$C^\perp = \{u \in F_2^n : u \cdot v = 0 \quad \text{for all } v \in C\}.$$

If $C \subseteq C^\perp$, C is termed self-orthogonal and if $C = C^\perp$, C is self-dual. A binary self-dual code in which all weights are divisible by four is termed doubly-even. If not all weights are divisible by four the code is singly-even. Self-dual codes with the largest minimum weight for a given length are called extremal. A list of possible weight enumerators of extremal self-dual codes of length up to 72 was given by Conway and Sloane in [6]. This list was extended for length up to 100by Dougherty, Gulliver, and Harada in [7]. However, the existence of some extremal self-dual codes is still unknown.

Manuscript received July 30, 1998; revised May 30, 1999. This work was supported in part by the UNESCO UVO-ROSTE Contract 875.630.9.

The author is with the Department of Pure Mathematics, Delft University of Technology, 2600 GA Delft, The Netherlands, on leave from the Faculty of Mathematics and Informatics, University of Veliko Tarnovo, 5000 Veliko Tarnovo, Bulgaria (e-mail: stefka_iliya@yahoo.com).

Communicated by A. M. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)01692-8.

A method for constructing binary self-dual codes via an automorphism of odd prime order is given by Huffman and Yorgov [10], [18], [19]. Some properties of the binary self-dual codes with an automorphism of order 2 without fixed points are proved in [3]. Two methods for constructing such codes are presented in the same work. These constructions are generalized in [5]. In this work we consider binary self-dual codes with an automorphism of order 2 with c 2-cycles and f fixed points for $0 \le f < n$, $n = 2c + f$. We investigate a construction technique for such codes.

In the next section we give some results about binary self-dual codes having an automorphism of order 2. In Section III we present a method for constructing a binary self-dual code of length $n = 2c + f$ using self-orthogonal codes of length c and a self-dual code of length f. In Section IV we obtain self-dual $[40, 20, 8]$, $[42, 21, 8]$, $[44, 22, 8]$, $[52, 16, 10]$, $[54, 27, 10]$, and $[58, 29, 10]$ codes using the new method. We prove that there do not exist self-dual $[50, 25, 10]$ and $[96, 48, 20]$ codes with an automorphism of order 2 with f fixed points for $f > 0$. For $n < 108$, there do not exist binary self-dual codes of length n and minimum distance 18 with an automorphism of order 2 with fixed points.

For the known codes, we use the notations from [6].

II. DEFINITIONS AND GENERAL RESULTS

Let C be an $[n, k = n/2]$ self-dual code. Fix n_1 and n_2 so that $n_1 + n_2 = n$. Let $\mathcal{B}$, respectively, $\mathcal{D}$, be the largest subcode of C whose support is contained entirely in the left n_1, respectively, right n_2, coordinates. Suppose $\mathcal{B}$ and $\mathcal{D}$ have dimensions k_1 and k_2, respectively. Let $k_3 = k - k_1 - k_2$. Then there exists a generator matrix for C in the form

$$\text{gen}\,(C) = \begin{pmatrix} B & O \\ O & D \\ E & F \end{pmatrix} \tag{1}$$

where B is a $k_1 \times n_1$ matrix with $\text{gen}\,(\mathcal{B}) = [B \quad O]$, D is a $k_2 \times n_2$ matrix with $\text{gen}\,(\mathcal{D}) = [O \quad D]$, O is the appropriate size-zero matrix, and $[E \quad F]$ is a $k_3 \times n$ matrix. Let $\mathcal{B}^*$ be the code of length n_1 generated by B, $\mathcal{B}_E$ the code of length n_1 generated by the rows of B and E, $\mathcal{D}^*$ the code of length n_2 generated by D, and $\mathcal{D}_F$ the code of length n_2 generated by the rows of D and F. The following result is found in [13].

Lemma 1: With the notation of the previous paragraph

(i) $k_3 = \text{rank}\,(E) = \text{rank}\,(F)$,

(ii) $k_2 = k + k_1 - n_1$, and

(iii) $\mathcal{B}_E^\perp = \mathcal{B}^*$ and $\mathcal{D}_F^\perp = \mathcal{D}^*$.

Let C be a binary self-dual $[n, n/2]$ code and

$$\sigma = (1, 2)(3, 4)\cdots(2c-1, 2c)$$

be an automorphism of C. Let

$$C_\sigma = \{v \in C \colon v\sigma = v\}.$$

Obviously, $v = (\beta_1, \beta_2, \cdots, \beta_n) \in C_\sigma$ iff $v \in C$ and $\beta_{2i-1} = \beta_{2i}$ for $i = 1, \cdots, c$. Let us denote

$$\mathcal{B} = \{v = (\alpha_1, \cdots, \alpha_n) \in C \colon \alpha_{2c+1} = \cdots = \alpha_n = 0\}$$

and $\mathcal{B}_\sigma = \mathcal{B} \cap C_\sigma$. Let

$$\mathcal{D} = \{v \in C \colon \alpha_1 = \cdots = \alpha_{2c} = 0\}.$$

Obviously, $\mathcal{D} \subset C_\sigma$. Then there exists a generator matrix for C in the form (1) where B is a $k_1 \times 2c$ matrix with $\text{gen}(\mathcal{B}) = [B \quad O]$, D is a $k_2 \times f$ matrix with $\text{gen}(\mathcal{D}) = [O \quad D]$, and $[E \quad F]$ is a $k_3 \times n$ matrix. Let $\mathcal{B}^*$ be the code of length $2c$ generated by B, $\mathcal{B}_E$ the code of length $2c$ generated by the rows of B and E, $\mathcal{D}^*$ the code of length f generated by D, and $\mathcal{D}_F$ the code of length f generated by the rows of D and F. From Lemma 1 we have

$$k_2 = k + k_1 - 2c = c + (1/2)f + k_1 - 2c = (1/2)f + k_1 - c.$$

Theorem 1: Let $\phi \colon C \to F_2^c$ be the map defined by

$$\phi(v) = (\alpha_1 + \alpha_2, \cdots, \alpha_{2c-1} + \alpha_{2c})$$

for $v = (\alpha_1, \cdots, \alpha_n) \in C$. Then ϕ is a homomorphism, $\text{Ker}\,\phi = C_\sigma$, $C' = \text{Im}\phi$ is a self-orthogonal $[c, s]$ code and $\pi(\mathcal{B}_\sigma) = (C')^\perp$, where $\pi \colon C_\sigma \to F_2^c$ is the map defined by $\pi(v) = (\beta_1, \cdots, \beta_c)$ for

$$v = (\beta_1, \beta_1, \cdots, \beta_c, \beta_c, \beta_{2c+1}, \cdots, \beta_n) \in \text{Ker}\,\phi.$$

Proof: Clearly ϕ is linear and hence ϕ is a homomorphism. Thus C' is a $[c, s]$ code for some s. To show it is self-orthogonal, let $v = (\alpha_1, \cdots, \alpha_n)$ and $w = (\beta_1, \cdots, \beta_n)$ be codewords in C. Then

$$\begin{aligned}\phi(v)\cdot\phi(w) &= \sum_{i=1}^{c}(\alpha_{2i-1}+\alpha_{2i})(\beta_{2i-1}+\beta_{2i})\\ &= \sum_{i=1}^{c}(\alpha_{2i-1}\beta_{2i-1}+\alpha_{2i}\beta_{2i})\\ &\quad+\sum_{i=1}^{c}(\alpha_{2i-1}\beta_{2i}+\alpha_{2i}\beta_{2i-1})\\ &= v\cdot w + v\cdot w\sigma = 0\end{aligned}$$

as $w\sigma \in C$.

Since $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \text{Ker}\,\phi$ iff $\alpha_{2i-1} = \alpha_{2i}$ for $1 \le i \le c$, we have $\text{Ker}\,\phi = C_\sigma$.

Let

$$w = (\beta_1, \beta_1, \cdots, \beta_c, \beta_c, 0, \cdots, 0) \in \mathcal{B}_\sigma.$$

Then

$$\phi(v)\cdot\pi(w) = \sum_{i=1}^{c}(\alpha_{2i-1}+\alpha_{2i})\beta_i = v\cdot w = 0$$

for all $v = (\alpha_1, \cdots, \alpha_n) \in C$. Hence $\pi(w) \in (C')^\perp$ for all $w \in \mathcal{B}_\sigma$ and $\pi(\mathcal{B}_\sigma) \subset (C')^\perp$.

Now let

$$w = (\beta_1, \cdots, \beta_c) \in (C')^\perp$$

and

$$w' = (\beta_1, \beta_1, \beta_2, \beta_2, \cdots, \beta_c, \beta_c, 0, \cdots, 0).$$

Then

$$v\cdot w' = \sum_{i=1}^{c}(\alpha_{2i-1}+\alpha_{2i})\beta_i = \phi(v)\cdot w = 0$$

for all $v = (\alpha_1, \cdots, \alpha_n) \in C$ and so $w' \in C$. Since the last f coordinates of w' are zeros and $w' \in C_\sigma$ we have $w' \in \mathcal{B}_\sigma$. Therefore, $w = \pi(w') \in \pi(\mathcal{B}_\sigma)$. Hence $(C')^\perp \subset \pi(\mathcal{B}_\sigma)$. So we proved that $(C')^\perp = \pi(\mathcal{B}_\sigma)$. ◇

Corollary 1.1: $\dim(C_\sigma) = k - s$ and $\dim(\mathcal{B}_\sigma) = c - s$.

Corollary 1.2: $\phi(\mathcal{B})^\perp = \pi(C_\sigma)$.

Proof: If

$$w = (\beta_1, \beta_1, \cdots, \beta_c, \beta_c, \beta_{2c+1}, \cdots, \beta_n) \in C_\sigma$$

we have

$$\pi(w)\cdot\phi(v) = \beta_1(\alpha_1+\alpha_2)+\cdots+\beta_c(\alpha_{2c-1}+\alpha_{2c}) = w\cdot v = 0$$

for any vector

$$v = (\alpha_1, \cdots, \alpha_{2c}, 0, \cdots, 0) \in \mathcal{B}.$$

Hence $\pi(C_\sigma) \subset \phi(\mathcal{B})^\perp$.

Obviously, $\text{Ker}\,\pi = \mathcal{D}$ and so

$$\begin{aligned}\dim(\pi(C_\sigma)) &= \dim(C_\sigma) - \dim(\mathcal{D})\\ &= k - s - k_2\\ &= c + (1/2)f - s - (1/2)f - k_1 + c\\ &= 2c - s - k_1.\end{aligned}$$

We have

$$\begin{aligned}\dim(\phi(\mathcal{B})^\perp) &= c - \dim(\phi(\mathcal{B}))\\ &= c - \dim(\mathcal{B}) + \dim(\mathcal{B}_\sigma)\\ &= c - k_1 + c - s\\ &= 2c - s - k_1 = \dim(\pi(C_\sigma)).\end{aligned}$$

Therefore, $\phi(\mathcal{B})^\perp = \pi(C_\sigma)$. ◇

Corollary 1.3: $s = 0$ iff $C = i_2^c \oplus \mathcal{D}^*$, where $i_2 = \{00, 11\}$.

Theorem 2: Let $\psi \colon C \to F_2^f$ $(f > 0)$ be the map defined by $\psi(v) = (\alpha_{2c+1}, \cdots, \alpha_n)$ for $v = (\alpha_1, \cdots, \alpha_n) \in C$. Then ψ is a homomorphism, $\text{Ker}\,\psi = \mathcal{B}$, $\psi(C_\sigma)$ is a self-dual $[f, (1/2)f]$ code, and $\psi(\mathcal{D}) = (\psi(C))^\perp$.

Proof: Let

$$v = (\alpha_1, \alpha_1, \alpha_2, \alpha_2, \cdots, \alpha_c, \alpha_c, \alpha_{2c+1}, \cdots, \alpha_n) \in C_\sigma$$

and

$$w = (\beta_1, \beta_1, \cdots, \beta_c, \beta_c, \beta_{2c+1}, \cdots, \beta_n) \in C_\sigma.$$

Then

$$\begin{aligned}v\cdot w &= \sum_{i=1}^{c}(\alpha_i\beta_i+\alpha_i\beta_i) + \sum_{i=2c+1}^{n}\alpha_i\beta_i\\ &= \sum_{i=2c+1}^{n}\alpha_i\beta_i = \psi(v)\cdot\psi(w) = 0.\end{aligned}$$

Hence $\psi(C_\sigma)$ is a self-orthogonal code of length f. Let $\psi|_{C_\sigma}$ be the restriction of ψ on C_σ. Obviously, $\mathrm{Ker}\,\psi|_{C_\sigma} = \mathcal{B}_\sigma$. So we have

$$\begin{aligned}\dim(\psi(C_\sigma)) &= \dim(C_\sigma) - \dim \mathcal{B}_\sigma\\ &= k - s - c + s\\ &= k - c = c + (1/2)f - c = (1/2)f.\end{aligned}$$

Hence $\psi(C_\sigma)$ is a self-dual code.

Obviously, $\psi(C) = \mathcal{D}_F$ and $\psi(\mathcal{D}) = \mathcal{D}^*$. From Lemma 1 we have $\mathcal{D}^* = \mathcal{D}_F^\perp$. ◊

Corollary 2.1: If $f > 0$, the code $\mathcal{D}^*$ contains the all-one vector.

Proof: Obviously, $\mathcal{D} \subset C_\sigma$ and so $\mathcal{D}^*$ is a subcode of $\psi(C_\sigma)$. If $v = (\alpha_1, \cdots, \alpha_n) \in C$ then

$$\begin{aligned}v \cdot v\sigma &= \sum_{i=1}^{c}(\alpha_{2i-1}\alpha_{2i} + \alpha_{2i}\alpha_{2i-1}) + \sum_{i=2c+1}^{n} \alpha_i\\ &= \sum_{i=2c+1}^{n} \alpha_i = 0.\end{aligned}$$

Hence $1 \in \mathcal{D}_F^\perp = \mathcal{D}^*$. ◊

Corollary 2.2: When $f > 0$ the minimum distance of the code C is at most f.

Corollary 2.3: There exists a generator matrix of the code C_σ in the form

$$\mathrm{gen}\,(C_\sigma) = \begin{pmatrix} B_\sigma & O\\ O & D\\ E_\sigma & F_\sigma\end{pmatrix}$$

where B_σ is a $c - s \times 2c$ matrix with $\mathrm{gen}\,(\mathcal{B}_\sigma) = [B_\sigma \;\; O]$, D is a $k_2 \times f$ matrix with $\mathrm{gen}\,(\mathcal{D}) = [O \;\; D]$, and $[E_\sigma \quad F_\sigma]$ is a $c - k_1 \times n$ matrix.

Corollary 2.4: There exists a generator matrix of the code $(C_\sigma + \mathcal{B})^\perp$ in the form

$$\mathrm{gen}\,((C_\sigma + \mathcal{B})^\perp) = H = \begin{pmatrix} B & O\\ O & D\\ O & F_\sigma\\ E_\sigma & O\\ E_1 & F_1\end{pmatrix}$$

where

$$\mathrm{gen}\,(C) = \begin{pmatrix} B & O\\ O & D\\ E_\sigma & F_\sigma\\ E_1 & F_1\end{pmatrix}$$

$\binom{E_\sigma}{E_1} = E$ and $\binom{F_\sigma}{F_1} = F$.

Proof: Obviously,

$$\begin{pmatrix} B & O\\ O & D\\ E_\sigma & F_\sigma\end{pmatrix}$$

is a generator matrix of $C_\sigma + \mathcal{B}$. As the rows of the matrices $\binom{B}{E}$ and $\binom{D}{F_\sigma}$ are linearly independent so are the rows of H. Since $C_\sigma + \mathcal{B}$ is a subcode of the self-dual code C it follows that C is a subcode of $(C_\sigma + \mathcal{B})^\perp$. $\mathcal{D}^* = \mathcal{D}_F^\perp$ and, therefore, the rows of $[0 \quad F_\sigma]$ are in $(C_\sigma + \mathcal{B})^\perp$. As the number of rows of H is

$$\begin{aligned}k_1 + (1/2)f + k_3 &= k - k_2 + (1/2)f\\ &= n - k - k_2 + (1/2)f\\ &= n - (1/2)f - k_1 = n - \dim(C_\sigma + \mathcal{B})\end{aligned}$$

we have that H is a generator matrix of the code $(C_\sigma + \mathcal{B})^\perp$.◊

Theorem 3: Let $\tau : C \to F_2^{2c}$ be the map defined by $\tau(v) = (\alpha_1, \cdots, \alpha_{2c})$ for $v = (\alpha_1, \cdots, \alpha_n) \in C$. Then τ is a homomorphism, $\mathrm{Ker}\,\tau = \mathcal{D}$, and $C_1 = \tau(C_\sigma) + \tau(\mathcal{B})$ is a self-dual code with an automorphism $\sigma = (1, 2)(3, 4) \cdots (2c - 1, 2c)$.

Proof: Let

$$v = (\alpha_1, \alpha_1, \alpha_2, \alpha_2, \cdots, \alpha_c, \alpha_c, \alpha_{2c+1}, \cdots, \alpha_n) \in C_\sigma$$

and

$$w = (\beta_1, \beta_1, \cdots, \beta_c, \beta_c, \beta_{2c+1}, \cdots, \beta_n) \in C_\sigma.$$

Then

$$\tau(v) \cdot \tau(w) = \sum_{i=1}^{c}(\alpha_i\beta_i + \alpha_i\beta_i) = 0.$$

Obviously, $\mathcal{B}^*$ is a self-orthogonal code, $\tau(C_\sigma) \subset \mathcal{B}_E = (\mathcal{B}^*)^\perp$ and so C_1 is a self-orthogonal code of length $2c$. Let $\tau|_{C_\sigma}$ be the restriction of τ on C_σ. Obviously, $\mathrm{Ker}\,\tau|_{C_\sigma} = \mathcal{D}$. Therefore,

$$\begin{aligned}\dim \tau(C_\sigma) &= \dim(C_\sigma) - \dim \mathcal{D}\\ &= k - s - k_2\\ &= k - s - (k + k_1 - 2c)\\ &= 2c - k_1 - s.\end{aligned}$$

Since $\tau(C_\sigma) \cap \mathcal{B}^*$ is the code $\tau(\mathcal{B}_\sigma)$ and τ is a monomorphism on $\mathcal{B}_\sigma$, we have

$$\begin{aligned}\dim C_1 &= \dim \tau(C_\sigma) + \dim(\mathcal{B}^*) - \dim(\tau(C_\sigma) \cap \mathcal{B}^*)\\ &= 2c - k_1 - s + k_1 - \dim \mathcal{B}_\sigma\\ &= 2c - s - c + s = c.\end{aligned}$$

It follows that C_1 is a self-dual code. ◊

III. Construction Method

Let C' be a self-orthogonal $[c, s]$ code and $\mathcal{B}'$ be its dual $[c, c - s]$ code. Let C'' be a $[c, s_1]$ subcode of C', and $\mathcal{B}''$ be its dual code. Obviously, $\mathcal{B}' \subset \mathcal{B}''$. Using the code C'' and the method from [5] we can construct a binary self-dual code C_1 of length $2c$ with an automorphism $\sigma = (1, 2)(3, 4) \cdots (2c - 1, 2c)$.

Theorem 4 [5]: Let C'' be a self-orthogonal $[c, s_1, d'']$ code, $\mathcal{B}''$ be its dual code, and $\pi' : \mathcal{B}'' \to F_2^{2c}$ be the map defined by $\pi'(v) = (\alpha_1, \alpha_1, \cdots, \alpha_c, \alpha_c)$ for $v = (\alpha_1, \alpha_2, \cdots, \alpha_c) \in \mathcal{B}''$. Let

$$M = \{(j_1, j_2), (j_3, j_4), \cdots, (j_{2r-1}, j_{2r})\}$$

be a set of r pairs of different coordinates of the code C'', $0 \le 2r \le c$, and $\phi' : C'' \to F_2^{2c}$ be the map defined by

$\phi'(v) = (\alpha'_1, \alpha''_1, \cdots, \alpha'_c, \alpha''_c)$ for $v = (\alpha_1, \ldots, \alpha_c) \in C'$, where $(\alpha'_i, \alpha''_i) = (\alpha_i, 0)$ for $i \neq j_l$, $l = 1, 2, \cdots, 2r$, and

$$(\alpha'_{j_{2i-1}}, \alpha''_{j_{2i-1}}, \alpha'_{j_{2i}}, \alpha''_{j_{2i}}) = (\alpha_{j_{2i-1}} + \alpha_{j_{2i}}, \alpha_{j_{2i}}, \alpha_{j_{2i-1}} + \alpha_{j_{2i}}, \alpha_{j_{2i-1}})$$

for $i = 1, 2, \cdots, r$. Then $C_1 = \phi'(C'') + \pi'(\mathcal{B}'')$ is a self-dual $[2c, c]$ code and $\sigma = (1, 2)(3, 4)\cdots(2c-1, 2c)$ is an automorphism of C_1.

We can take a generator matrix of C_1 in the form

$$\mathrm{gen}\,(C_1) = G_1 = \begin{pmatrix} B_\sigma \\ E_\sigma \\ B_1 \end{pmatrix}$$

where B_1, B_σ, and E_σ are matrices with, respectively, s_1, $c-s$, and $s-s_1$ rows, as B_1 generates the code $\phi'(C'')$, B_σ generates the code $\pi'(\mathcal{B}')$, and $\binom{B_\sigma}{E_\sigma}$ generates the code $\pi'(\mathcal{B}'')$.

Let $\mathcal{D}_\sigma$ be a self-dual code of length f, $f > 2(s - s_1)$, and $\mathcal{D}^*$ be an $[f, (1/2)f - s + s_1]$ subcode of $\mathcal{D}_\sigma$ with $1 \in \mathcal{D}^*$. Let D be a generator matrix of $\mathcal{D}^*$. We can take a generator matrix for the code $\mathcal{D}_\sigma$ in the form $\binom{D}{F_\sigma} = D_\sigma$.

Theorem 5: The code C_2 with a generator matrix

$$G_2 = \begin{pmatrix} O & D \\ B_\sigma & O \\ E_\sigma & F_\sigma \\ B_1 & O \end{pmatrix}$$

is a self-orthogonal $[n = 2c + f, c + (1/2)f - s + s_1]$ code. If $\phi : F_2^n \to F_2^c$ is the map defined by

$$\phi(v) = (\alpha_1 + \alpha_2, \alpha_3 + \alpha_4, \cdots, \alpha_{2c-1} + \alpha_{2c})$$

for $v = (\alpha_1, \alpha_2, \cdots, \alpha_{n-1}, \alpha_n)$ then $\phi(C_2^\perp) = C'$ and $\phi(C_2) = C''$.

Proof: From the construction of the code C_2 we have $\phi(C_2) = C''$. Let $v = (\alpha_1, \cdots, \alpha_n) \in (C_2)^\perp$ and $(\beta_1, \cdots, \beta_c) \in \mathcal{B}'$. Then

$$(\beta_1, \beta_1, \beta_2, \beta_2, \cdots, \beta_c, \beta_c, 0, \cdots, 0) \in C_2.$$

Therefore,

$$v \cdot w = (\alpha_1 + \alpha_2)\beta_1 + (\alpha_3 + \alpha_4)\beta_2 + \cdots + (\alpha_{2c-1} + \alpha_{2c})\beta_c = 0.$$

Hence $\phi(v) \in (\mathcal{B}')^\perp = C'$ and so $\phi(C_2^\perp) \subset C'$. Since

$$\begin{aligned}\dim(\phi(C_2^\perp)) &= \dim(C_2^\perp) - \dim(\mathrm{Ker}\,\phi|_{C_2^\perp}) \\ &= n - \dim(C_2) - \dim(\pi'(\mathcal{B}'') \oplus \mathcal{D}_\sigma) \\ &= 2c + f - c - (1/2)f \\ &\quad + s - s_1 - (1/2)f - c + s_1 \\ &= s = \dim(C').\end{aligned}$$

Therefore, $\phi(C_2^\perp) = C'$. ◇

We can take a generator matrix of $(C_2)^\perp$ in the form

$$\begin{pmatrix} G_1 & 0 \\ O & D_\sigma \\ E_1 & F \end{pmatrix}$$

where $\mathrm{rank}\,(E_1) = \mathrm{rank}\,(F) = s - s_1$.

Remark: The code C_2 corresponds to $C_\sigma + \mathcal{B}$ from the previous section.

Corollary 5.1: The matrix $D_1 = \binom{D_\sigma}{F}$ generates the code $(\mathcal{D}^*)^\perp$.

Proof: Obviously, the code $\mathcal{D}_1$ with a generator matrix D_1 is a subcode of $(\mathcal{D}^*)^\perp$. Besides,

$$\dim \mathcal{D}_1 + \dim \mathcal{D}^* = (1/2)f + s - s_1 + (1/2)f - s + s_1 = f.$$

Hence $\mathcal{D}_1 = (\mathcal{D}^*)^\perp$. ◇

Theorem 6: Let $v_1, v_2, \cdots, v_{s-s_1}$ be the rows of E_1, and $y_1, y_2, \cdots, y_{s-s_1}$ be the rows of F. If $\mathcal{F}_\sigma$ is the code with a generator matrix F_σ, we can take vectors $w_1 \in y_1 + \mathcal{F}_\sigma$, $w_2 \in y_2 + \mathcal{F}_\sigma, \cdots, w_{s-s_1} \in y_{s-s_1} + \mathcal{F}_\sigma$, such that the vectors $(v_1, w_1), (v_2, w_2), \cdots, (v_{s-s_1}, w_{s-s_1})$ are orthogonal to each other. Hence the matrix

$$\begin{pmatrix} & G_2 & \\ E_1 & & F_1 \end{pmatrix} \tag{2}$$

where F_1 is the matrix with rows $w_1, \cdots, w_{s-s_1}$, generates a self-dual $[2c + f, c + (1/2)f]$ code C.

Proof: Since $1 \in \mathcal{D}^*$ and $1 \in \mathcal{B}'$ then $1 \in C_2$ and so all vectors in $C_2^\perp$ have even weight. Hence any choice of w_i gives us a vector (v_i, w_i) of even weight. Let $x_1, x_2, \cdots, x_{s-s_1}$ be a basis of $\mathcal{F}_\sigma$ and $w_i = y_i + \lambda_{i,1}x_1 + \lambda_{i,2}x_2 + \cdots + \lambda_{i,s-s_1}x_{s-s_1}$. We have to solve a linear system of equations $v_k \cdot v_l = w_k \cdot w_l, 1 \le k < l \le s - s_1$. It follows that

$$\begin{aligned} v_k \cdot v_l &= \left(y_k + \sum_{i=1}^{s-s_1} \lambda_{k,i}x_i\right) \cdot \left(y_l + \sum_{j=1}^{s-s_1} \lambda_{l,j}x_j\right) \\ &= y_k \cdot y_l + \sum_{i=1}^{s-s_1} \lambda_{k,i}x_i \cdot y_l + \sum_{j=1}^{s-s_1} \lambda_{l,j}x_j \cdot y_k. \end{aligned}$$

This system has $((s-s_1)(s-s_1-1)/2)$ equations and $(s-s_1)^2$ variables. Its rank is $((s - s_1)(s - s_1 - 1)/2)$ and, therefore, the solutions depend on $((s - s_1)(s - s_1 + 1)/2)$ parameters. Obviously, the constructed code C is a self-dual code with minimum distance $d \le \min\{d(\mathcal{D}^*), 2d(\mathcal{B}')\}$. ◇

Corollary 6.1: $\phi(C) = C'$.

Corollary 6.2: $\sigma = (1, 2)\cdots(2c-1, 2c)$ is an automorphism of the code C.

Proof: Let $v = (\alpha_1, \cdots, \alpha_n)$ be a vector from C. Then

$$\phi(v) = (\alpha_1 + \alpha_2, \cdots, \alpha_{2c-1} + \alpha_{2c}) \in C' \subset \mathcal{B}'.$$

Therefore, the vector

$$w = (\alpha_1 + \alpha_2, \alpha_1 + \alpha_2, \cdots, \alpha_{2c-1} + \alpha_{2c}, \alpha_{2c-1} + \alpha_{2c}, 0, \cdots, 0)$$

belongs to C. Hence

$$v + w = (\alpha_2, \alpha_1, \alpha_4, \alpha_3, \cdots, \alpha_{2c}, \alpha_{2c-1}, \alpha_{2c+1}, \cdots, \alpha_n) = v\sigma$$

is a vector in C. ◇

IV. Results

In this section we obtain extremal self-dual codes using the method from Section III. We investigate extremal self-dual codes with an automorphism of order 2 with f fixed points for

$f > 0$. Since $d \le \min\{d(\mathcal{D}^*), 2d(\mathcal{B}')\}$, we have $f \ge d$. The code $\mathcal{D}^*$ has to be a $[f, (1/2)f - s + s_1, \ge d]$ self-orthogonal code, and $\mathcal{B}'$ has to be a $[c, c - s, \ge (1/2)d]$ code.

Some of the constructed codes have weight enumerators previously not known to exist.

A. $[40, 20, 8]$ *Codes*

Any extremal singly-even $[40, 20, 8]$ code has weight enumerator of the form

$$W(y) = 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + \cdots$$

where β is an integer, $0 \le \beta \le 10$. Codes with $0 \le \beta \le 8$ and $\beta = 10$ are given in [5], [6], and [9].

From the codes $C' = e_8 \oplus e_8$ and $\mathcal{D}_\sigma = e_8$ where e_8 is the extended Hamming code, and some $[16, 5]$ subcodes C'' of C' we obtain self-dual codes with weight enumerator W with $\beta = 0, \cdots, 8$.

In the case $C' = e_7^{2+}$ and $\mathcal{D}_\sigma = d_{12}^+$ we construct self-dual codes with weight enumerators W with $\beta = 0, \cdots, 7$.

If $C' = d_{12}^+$, $\mathcal{D}_\sigma = e_8 \oplus e_8$, and $s_1 = 0, 1, 2, 3$ we obtain self-dual codes with weight enumerators W with $\beta = 0, 1, 2, 4, 6, 8, 10$.

In all cases, we construct doubly-even self-dual $[40, 20, 8]$ codes.

B. $[42, 21, 8]$ *Codes*

The possible weight enumerators of putative or known extremal self-dual $[42, 21, 8]$ codes are

$$W_1(y) = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + \cdots, \quad 0 \le \beta \le 60$$

and

$$W_2(y) = 1 + 164y^8 + 697y^{10} + \cdots.$$

There exist self-dual codes with a weight enumerator W_1 for $\beta = 0, \cdots, 12, 14, 16, 18, 20, 24, 26, 32, 42$, and with a weight enumerator W_2 (see [3] and [7]).

Let $c = 16$, $f = 10$, and $D_\sigma = e_8 \oplus i_2$. Using subcodes of $C' = e_8 \oplus e_8$ of dimension 4 we obtain extremal self-dual codes of length 42 with weight enumerators W_1 for $\beta = 13, 14, 15, 16, 18$, and 22. The codes $C_{42,1}$, $C_{42,2}$, and $C_{42,3}$ have weight enumerators W_1 for $\beta = 13, 15$, and 22. These codes are the first known self-dual codes with these weight enumerators. They have generator matrices of type (2) as $\pi(B_\sigma)$ is a generator matrix of $e_8 \oplus e_8$, $D = (11 \cdots 1)$, and the rows of F_σ are $(11110\ldots0)$, (1100110000), (1100001100), and (1010101000) for the three codes. For the other matrices we have

$C_{42,1}$ (the rows of the matrices are broken into blocks of length 4, each of which is represented by a hexadecimal symbol) –

$B_1 - db8e27be, 35904b11, 99c036f9, 18db663c;$

$\pi(E_\sigma) - c880, c040, 2020, 6808;$

$F_1 - c00, a00, b40, e98;$

$E_1 - 60ca0000, b8480000, 0a600000, b4e20000.$

$C_{42,2}-$

$B_1 - ed1e0366, e1eeafc6, 09affaf6, 5c39c9a3;$

$\pi(E_\sigma) - 2800, 00c0, a020, 4088;$

$F_1 - c00, a00, b40, 708;$

$E_1 - e222c000, cc004888, 8282c000, 5a008888.$

$C_{42,3}-$

$B_1 - 121e44d1, 9965f95f, 53059c90, 6fc512b8;$

$\pi(E_\sigma) - 2800, a040, e020, 8008;$

$F_1 - c00, a00, b40, 708;$

$E_1 - 78880000, 36a00000, ee880000, 7e82c000.$

C. $[44, 22, 8]$ *Codes*

The possible weight enumerators for length 44 are

$$W_1(y) = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + \cdots, \quad 10 \le \beta \le 122$$

and

$$W_2(y) = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + \cdots, \quad 0 \le \beta \le 154.$$

There exist self-dual codes with a weight enumerator W_1 for $\beta = 10, \cdots, 39, 42, 52, 62, 82, 122$, and with a weight enumerator W_2 for $\beta = 0, 2, \cdots, 44, 46, 47, 48, 50, 52, \cdots, 56, 58, 62, 66, 72, 74, 82, 90, 104, 154$ (see [7]).

From the codes $C' = e_8 \oplus e_8$ and $\mathcal{D}_\sigma = d_{12}^+$, and some $[16, 3]$ subcodes C'' of C' we obtain self-dual codes with weight enumerator W_1 with $\beta = 12, \cdots, 45, 47, 48$, and 54, and codes with weight enumerator W_2 for $\beta = 7, \cdots, 38, 40, 41, 42$, and 44.

Let $C' = e_7^{2+}$ and $\mathcal{D}_\sigma = e_8 \oplus e_8$. The code $\mathcal{D}^*$ with a generator matrix

$$\begin{pmatrix} 1111111111111111 \\ 1111111100000000 \\ 1111000011110000 \\ 1100110011001100 \\ 1010101010101010 \end{pmatrix}$$

is a $[16, 5, 8]$ subcode of $e_8 \oplus e_8$. Using the $[14, 4]$ subcode of e_7^{2+} with a generator matrix

$$\begin{pmatrix} 11111110110100 \\ 11111110101010 \\ 11111110000111 \\ 00000001100110 \end{pmatrix}$$

and the set

$$M = \{(1, 12)(2, 8)(3, 10)(4, 14)(5, 13)(6, 11)(7, 9)\}$$

we construct a self-dual code with weight enumerators W_1 with $\beta = 56$. The matrix $G_{44,56}$ is a generator matrix of this code as shown at the top of the following page.

Similarly, we obtain a self-dual $[44, 22, 8]$ code with a weight enumerator W_2 with $\beta = 56$.

If $C' = d_6^{3+}$, $\mathcal{D}_\sigma = e_8$, and $s_1 = 6$ we construct self-dual codes with weight enumerator W_2 with $\beta = 1, 4, \cdots, 11$. Let $C_{44,1}$ be the self-dual code for which B_1 is the 6×36 matrix with rows (in hexadecimal) $be48b1fa3, 009de7b84, e7b7eb55a, 5c560556c, ee4eb196f,$

$$G_{44,\,56} = \left\| \begin{array}{c|c} 1111111100000000000000000000 & \\ 1111000011110000000000000000 & \\ 1100110011001100000000000000 & \\ 0000000000000011111111000000 & O \\ 0011110011000000111100110000 & \\ 0011110011000011001100001100 & \\ 0011110011000011110000000011 & \\ \hline & 1111111111111111 \\ & 1111111100000000 \\ O & 1111000011110000 \\ & 1100110011001100 \\ & 1010101010101010 \\ \hline 1100000011000000000000000000 & 1111000000000000 \\ 1100000000110000000000000000 & 1010101000000000 \\ 1100000000001100000000000000 & 0110011000000000 \\ \hline 0101011010100111010111101111 & \\ 0101101001010100011101000111 & O \\ 0101100101101011111111100101 & \\ 0000000011001101100000011000 & \\ \hline 1110100000101011000000000000 & 1100000011000000 \\ 0110000001010000011000000000 & 0000101010100000 \\ 1000001000101000111100000000 & 0001111010001000 \end{array} \right\|$$

$0398b7d42$, the rows of $\pi(E_\sigma)$ are $42800, 21080, 08020$, the rows of F_σ – $aa, f0, cc$, F_1 – $c0, a0, b4$, and of E_1 – $56c6a0000, 0669a0000, 3c05a0000$. This code has a weight enumerator W_2 with $\beta = 1$ and it is the first known code with this weight enumerator.

The codes $C_{44,40}$, $C_{44,41}$, $C_{44,43}$, $C_{44,44}$, $C_{44,45}$, $C_{44,47}$, $C_{44,48}$, and $C_{44,54}$ have weight enumerators W_1 with $\beta = 40, 41, 43, 44, 45, 47, 48$, and 54, respectively. Codes with these weight enumerators were previously not known to exist. In Table I we give the matrices B_1, $\pi(E_\sigma)$, F_σ, F_1, and E_1 for these codes.

D. $[50, 25, 10]$ *Codes*

We have $f \geq 10$ and $c = 25 - (1/2)f \leq 20$. Since $\mathcal{B}'$ is a $[c, c-s, d' \geq 5]$ code and $s \leq (1/2)c$ we have $(1/2)c \leq c-s \leq k(c, 5)$ where $k(n, d)$ denotes the largest value of k for which there exists an $[n, k, d]$ binary code. But $k(c, 5) < (1/2)c$ for $c < 16$ [2]. Therefore, $16 \leq c \leq 20$. For $c = 16$ and $c = 18$ we have $k(c, 5) = (1/2)c$ and hence C' has to be a self-dual $[c, (1/2)c, \geq 5]$ code. The extremal self-dual codes of lengths 16 and 18 have a minimum distance 4. So $c \neq 16$ and $c \neq 18$. For $c = 17$ and $c = 19$ we have $k(c, 5) = (c + 1/2)$ and hence C' has to be a self-orthogonal $[c, ((c-1)/2), \geq 5]$ code. Such codes do not exist (see [12]) and, therefore, $c \neq 17$ and $c \neq 19$.

In the case $c = 20$ we have $10 \leq 20 - s \leq 11$. The extremal self-dual codes of length 20 have minimum distance 4 and so $s \neq 10$. Let C' be a self-orthogonal $[20, 9, \geq 6]$ code with a dual distance at least 5. Then

$$\mathcal{B}' = C' \cup (v_1 + C') \cup (v_2 + C') \cup (v_1 + v_2 + C')$$

for some v_1 and v_2 with $wt(v_1) \equiv 0 \pmod 2$. The code $C' \cup (v_1 + C')$ is a self-dual $[20, 10, \geq 6]$ code. Since such a code does not exist we have $c \neq 20$. So we proved the following.

Theorem 7: If C is a binary self-dual $[50, 25, 10]$ code and σ is an automorphism of C of order 2 then σ has no fixed points.

Self-dual $[50, 25, 10]$ codes with an automorphism of order 2 without fixed points are constructed in [4].

E. $[52, 26, 10]$ *Codes*

Any extremal self-dual code of length 52 has a weight enumerator of the form

$$W(y) = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + \cdots, \quad 0 \leq \beta \leq 27.$$

It has been shown that codes exist for $\beta = 0, 1, \cdots, 5, 7$ [4], [6]–[8], [11], [16].

We have $f \geq 10$ and $c = 26 - (1/2)f \leq 21$. Since $\mathcal{B}'$ is a $[c, c-s, d' \geq 5]$ and $s \leq (1/2)c$ we have $(1/2)c \leq c - s \leq k(c, 5)$. Similarly to the previous subsection, we prove that $c \neq 10, \cdots, 20$.

Let $c = 21$. In this case, $11 \leq 21 - s \leq 12$. We can obtain a self-orthogonal $[21, 10, 6]$ code C' with a dual distance 5 from the code g_{22} by deleting the last coordinate of the vectors having

TABLE I
SELF-DUAL CODES OF LENGTH 44

code	c	s	s_1	B_1	$\pi(E_\sigma)$	F_σ	F_1	E_1
$C_{44,40}$	16	8	3	e74269f0 09afdbbe bbb8e71b	2800,4080, 2040,2020, e008	cfc,fcc,9a6, a66,96a	c00,0aa,780, 8d0,834	c6a00000,6ca0a0a0, d882a0a0,500a0000, 44880000
$C_{44,41}$	16	8	3	e84e4d8d 56030539 b7e2b72e	a800,c080, 0040,8020, a008	596,03c,a66, 69a,9a6	65a,630,47c, e76,808	1428aa00,a0a00000, 1288aa00,22220000, f6a0aa00
$C_{44,43}$	16	8	3	09935af3 59339ac3 e87e8edb	a800,2080, e040,e020, 0008	5aa,566,f3c, 3fc,99a	300,0aa,b8c, 410,2a2	f60a2882,a600a0a0, 1e880000,1e88a0a0, b4888822
$C_{44,44}$	16	8	3	e7e8af9c b2bdfac9 bb84b474	8800,2080, 4040,8020, 2008	30c,fcc,c0c, 6a6,ff0	300,af0,880, 720,2a2	72820000,6c0a0000, 9ca00000,0000aa00, 6600aa00
$C_{44,45}$	16	8	3	5596550f be71ca05 5630c950	9000,c880, c840,8020, 8808	f00,03c,956, 30c,aaa	fc0,9c0,880, 820,2a2	aa6a8888,c0aa8888, b8e28888,22e20000, 60a00000
$C_{44,47}$	16	8	3	b72153a3 0f03a0a3 0a53b1e7	b000,a800, a0c0,0020, a088	656,a5a,aaa, 96a,956	666,c9a,74c, 186,bf4	22882882,aa00aa00, 48886a00,82288282, 0aa04282
$C_{44,48}$	16	8	3	5c394b2e eb140fa5 be415af0	e800,8080, e040,8020, 2008	3c0,aaa,330, 656,3fc	c00,af0,b40, 81c,708	9c0a0000,a0a0a0a0, 14820000,0aa00000, 14280000
$C_{44,54}$	16	8	3	03f0aa03 0f6a6ffa bdd79569	9000,4000, 00c0,08a0, 8008	c30,66a,0f0, 6a6,3fc	696,630,4b0, 4e0,252	e842c000,60600000, ca604888,e8824888, 600a0000

0 on it. If $\mathcal{D}_\sigma = i_2 \oplus e_8$ and C'' is a [21, 6] subcode of C' we obtain self-dual [52, 26, 10] codes with weight enumerators W for $\beta = 0$ and 2.

F. [54, 27, 10] *Codes*

There are two possibilities for the weight enumerator of an extremal self-dual [54, 27, 10] code:

$$W_1(y) = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + \cdots, \quad 0 \le \beta \le 43$$

and

$$W_2(y) = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + \cdots, \quad 12 \le \beta \le 43$$

There exist self-dual [54, 27, 10] codes with weight enumerator W_1 for $\beta = 0, 1, \cdots, 15$ ([1], [5], [6], [9]) and W_2 for $\beta = 12, \cdots, 20$ ([1], [14], [16]).

We obtain extremal self-dual codes for this length with weight enumerators W_1 for $\beta = 1, 2, \cdots, 9, 11$ using the self-dual [22, 11, 6] code g_{22}, the self-dual [10, 5, 2] code $e_8 \oplus i_2$, and some [22, 7] subcodes of g_{22}.

G. [58, 29, 10] *Codes*

For binary self-dual [58, 29, 10] codes, two possible weight enumerators are given in [6]

$$W_1(y) = 1 + (165 - 2\gamma)y^{10} + (5078 + 2\gamma)y^{12} + \cdots \quad (0 \le \gamma \le 82)$$

and

$$W_2(y) = 1 + (319 - 24\beta - 2\gamma)y^{10} + (3132 + 152\beta + 2\gamma)y^{12} + \cdots \quad (0 \le \gamma \le 159 - 12\beta).$$

For W_1, a code exists with $\gamma = 55$ (cf. [15]).

For W_2, codes exist with $\beta = 0$ and $\gamma = 2m$, $m = 0, 16, 18, 20, 24, \cdots, 61$ (cf. [1], [5], [6], [9], [17]), $\beta = 1$ and $\gamma = 2m$, $m = 31, 32, 34, \cdots, 50$ (cf. [1]), and $\beta = 2$ and $\gamma = 2m$, $m = 22, 24, 26, 28, 30, 31, 32, 34, \cdots, 44$ (cf. [5], [17]). There is a mistake in the information about known self-dual [58, 29, 10] codes in [7].

We construct extremal self-dual codes of this length with a weight enumerator W_2 with $\beta = 0$ and $\gamma = 46, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 94$, and 98, $\beta = 1$ and $\gamma = 48, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80$, and 88, and $\beta = 2$ and $\gamma = 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88$, and 92. The codes with weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 1$ and $\gamma = 48, 56, 58, 60$, and 66, and $\beta = 2$ and $\gamma = 32, 36, 40$, and 92 are the first known codes with these weight enumerators.

Since $d = 10 \le d^* \le f$ we have $f \ge 10$. Therefore, $\mathcal{D}^* = \{\mathbf{0}, \mathbf{1}\}$ and

$$\dim(\mathcal{D}^*) = (1/2)f - s + s_1 = 1, \qquad \text{for } f < 20.$$

The dual code $\mathcal{B}'$ of the self-orthogonal $[c, s]$ code C' has to be a $[c, c-s, \ge 5]$ code. So we have $21 \le c = 1/2(58 - f) \le 24$.

Let $c = 24$ and $C' = g_{24}$ where g_{24} is the extended Golay code. Then $f = 10$, $\dim(\mathcal{D}^*) = (1/2)f - s + s_1 = 1$, and so

TABLE II
SELF-DUAL CODES OF LENGTH 58

code	B_1	$\pi(E_\sigma)$	F_σ	F_1	E_1
$C_{58,1}$	0ffe77a9e09a,e11d15915541, bd64c84b1ee4,e9d5ad5e507b, 075bacc6a077,51d483601e78, 04ae9887c5fd,ba8f82bcb03c	c38000,c84000, 292000,dc1000	690,cc0, 0f0,ff0	6a0,390, 1e0,2a8	c75228022000,2b1500a02000, 632c8aa00000,1a55aa800000
$C_{58,2}$	0ffe77a9e09a,e11d15915541, bd64c84b1ee4,e9d5ad5e507b, 075bacc6a077,51d483601e78, 04ae9887c5fd,ba8f82bcb03c	c38000,c84000, 292000,dc1000	690,cc0, 0f0,ff0	9a0,c90, 780,b38	c75228022000,2b1500a02000, 632c8aa00000,1a55aa800000
$C_{58,3}$	b7cf8ac5e4ea,0b60151b6f50, 0f0efcaba80b,0a07233b3c86, 0594040e5534,5f84bfeba8b4, b796ebb5e5b7,b06a9fdb839f	4c0000,584000, 08a000,b09000	550,f00, aa0,960	9a0,630, dd0,e98	99ce08820000,bf64a2020000, af204aa00000,912560aa0000
$C_{58,4}$	b9d7df57ea9a,0e5484179db0, e5328b217c5b,50b6a9e43f07, 096fe2fbc99e,b676e9e679f7, b00eb18a0cc7,b01e2ed8200f	fc8000,5e4000, 832000,8a1000	5a0,c30, ff0,960	030,050, 220,258	35ca80880800,c7e20a888000, 5b3722880000,b4a808800800
$C_{58,5}$	e74c815009e5,be694c987c70, efe838ae3931,bd9caabf14ec, 018aa437c7f2,0ea5d3b17d99, 030b940588f0,e0106607124f	b78000,e24000, 573000,422800	3c0,a50, 550,5a0,	650,930, 880,2a8	a30d288a0000,a0a5aaa00000, f82c82880000,8c3e022a0000
$C_{58,6}$	579b2ebf5acb,53faaebb2ffa, 51131d851944,55034c844914, b810fe83d0a0,086f2eaffac1, 57ee65657dda,0d6b4030b815	bb8000,522000, c05000,d90800	0f0,330, f00,aa0,	3f0,f50, 440,bc8	e82ca8280000,538280282000, c7c498002000,0be382880000
$C_{58,7}$	579b2ebf5acb,53faaebb2ffa, 51131d851944,55034c844914, b810fe83d0a0,086f2eaffac1, 57ee65657dda,0d6b4030b815	bb8000,522000, c05000,d90800	0f0,330, f00,aa0,	a90,630, dd0,d58	e82ca8280000,538280282000, c7c498002000,0be382880000
$C_{58,8}$	0212797c60d,081fa9f07b9, ee01c49c024,b35b54595c8, e9efe496fb8	f40000,820000, 880000,e18000, a04000,a12000	00cc,cd54, 96cc,ab2c, aa00,5b2c	3000,a1e0, ee00,4c98, 8160,81a0	7e098828000,f8abaa22000, ff828282000,24818a20000, 9ca100aa800,0323a0a0800
$C_{58,9}$	eb2ed5e7bb2,ea41884cef7, 521ca7250c3,08446f18b74, b65af2f1597	ac0000,9a0000, c10000,888000, 304000,402000	abe0,012c, 6678,66cc, 5acc,3c78	56cc,6d98, 7998,dbb4, 16f8,81d8	982a0a28000,918aa220a00, 47620808800,48aa2020a00, bde200a0a00,c1620820000
$C_{58,10}$	0dd54119561,02116dd13ca, 571709066ce,bebbfaaaf3c, b6209374300	f40000,a80000, d10000,b08000, 524000,e02000	00cc,972c, 3d2c,cc00, 6678,0198	c0cc,c72c, 88cc,81b4, e760,808c	0daaa200880,9a802a20200, 420a0a20a80,d10e0080880, 77ae8a00280,50200020280

$s_1 = 8$. Let $\mathcal{D}_\sigma = e_8 \oplus i_2$, and C'' be the [24, 8] subcode of C' with a generator matrix

$$\begin{pmatrix} 000000011010111101001111 \\ 010101010111110111111001 \\ 100111100010101001010110 \\ 011101111101110111001010 \\ 001011101100001111001010 \\ 110101101000110001011010 \\ 001011011110101000110001 \\ 101110001001100010000000 \end{pmatrix}.$$

From these codes we construct the self-dual [58, 29, 10] code $C_{58,1}$. The weight enumerator of this code is W_2 with $\beta = 2$ and $\gamma = 32$. Similarly we obtain self-dual [58, 29, 10] codes with weight enumerator W_2 with $\beta = 2$ and $\gamma = 32$, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, and 92. In Table II we give the matrices B_1, $\pi(E_\sigma)$, F_σ, F_1, and E_1 of codes $C_{58,1}$, $C_{58,2}$, $C_{58,3}$, and $C_{58,4}$ of weight enumerators W_2 with $\beta = 2$ and $\gamma = 32$, 36, 40, and 92, respectively.

Let C' be the "odd" Golay code f_{24}. From $\mathcal{D}_\sigma = e_8 \oplus i_2$ and different [24, 8] subcodes of f_{24} we obtain self-dual [58, 29, 10] codes with weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 0$, and $\gamma = 2m$, $m = 25, \cdots, 45$, and with $\beta = 1$, $\gamma = 48$, 56. The codes $C_{58,5}$, $C_{58,6}$, $C_{58,7}$, of weight enumerators W_2 with $\beta = 0$ and $\gamma = 46$, $\beta = 1$, and $\gamma = 48$, $\beta = 1$, and $\gamma = 56$, respectively, are the first known codes with these weight enumerators.

Let us consider the case $C' = g_{22}$ and $\mathcal{D}_\sigma = e_7^{2+}$ (see [6]). Then $\dim(\mathcal{D}^*) = (1/2)f - s + s_1 = s_1 - 4 = 1$ and hence $s_1 = 5$. Using these two codes and different [22, 5] subcodes C'' of g_{22}, we obtain binary self-dual [58, 29, 10] codes with weight enumerator W_2 for $\beta = 0$ and $\gamma = 52$, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 94, and 98, and $\beta = 1$ and $\gamma = 58$, 60, 62, 64, 66, 70, 74, 76, 78, and 88. In Table II we present the codes $C_{58,8}$, $C_{58,9}$, and $C_{58,10}$ with weight enumerators W_2 for $\beta = 1$ and $\gamma = 58$, 60, and 66.

H. [96, 48, 20] *Codes*

In this case, we have $f \geq 20$ and $c = 48 - (1/2)f \leq 38$. According to Brouwer's Table [2], $k(c, 10) < (1/2)c$ for $c < 37$. Only the possibility $c = 38$ remains. Since $k(38, 10) \leq 19$

the code C' has to be a self-dual $[38, 19, \geq 10]$ code. But the extremal self-dual code of length 38 has a minimum distance 8. So we proved the following theorem.

Theorem 8: If C is a binary self-dual $[96, 48, 20]$ code and σ is an automorphism of C of order 2 then σ has no fixed points.

I. Some Codes with Minimum Distance 18

Theorem 9: If C is a binary self-dual code of length n and minimum distance 18 for $n < 108$, and σ is an automorphism of C of order 2 then σ has no fixed points.

To prove the theorem, we need the following propositions:

Proposition 10: If a self-orthogonal $[n, k, \geq d]$ code with a dual distance at least d does not exist then there does not exist a self-orthogonal $[n, k-1, \geq d]$ code with a dual distance at least d.

Proof: Let C be a self-orthogonal $[n, k-1, \geq d]$ code and let its dual code have a minimum distance at least d. There exists a vector $v \in C^{\perp}$ of even weight such that $v \notin C$. Hence the code $C' = C \cup (v + C)$ is a self-orthogonal $[n, k, \geq d]$ code. Since its dual code is a subcode of $C^{\perp}$ the dual distance of C' is at least d. Such a code does not exist, and so there does not exist a self-orthogonal $[n, k-1, \geq d]$ code with a dual distance at least d. ♢

Proposition 11: If a self-dual $[2k, k, \geq d]$ code does not exist then there does not exist a self-orthogonal $[2k-1, k-1, \geq d]$ code with a dual distance at least d.

Proof: Let C be a self-orthogonal $[2k-1, k-1, \geq d]$ code and let its dual code have a minimum distance at least d. Obviously, $C^{\perp} = C \cup (\mathbf{1} + C)$. Then

$$C' = \{(0, v), v \in C\} \cup \{(1, w), w \in \mathbf{1} + C\}$$

is a self-dual code of length $2k$ and minimum distance at least d. But such a code does not exist. It follows that there does not exist a self-orthogonal $[2k-1, k-1, \geq d]$ code with a dual distance at least d. ♢

If C is a self-dual code of minimum distance 18 and σ is an automorphism of C of order 2 with C cycles and f fixed points, $f > 0$, then C' is a self-orthogonal $[c, s, \geq 10]$ code and its dual code $\mathcal{B}'$ is a $[c, c-s, \geq 9]$ code. According to Brouwer's Table [2], $k(c, 18) < (1/2)c$ for $c < 36$. There do not exist self-dual $[36, 18, 10]$, $[38, 19, 10]$, $[40, 20, 10]$, $[42, 21, 10]$, and $[44, 22, 10]$ codes. It follows that there do not exist self-orthogonal $[37, 18, 10]$, $[39, 19, 10]$, $[41, 20, 10]$, and $[43, 21, 10]$ codes with a dual distance at least 9. From Proposition 10, there do not exist self-orthogonal codes of lengths $36, 37, 38, 39, 40, 41, 42, 43, 44$, minimum distance 10, and dual distance at least 9. It follows that $c \geq 45$. In this case $f \geq 18$ and so $n = 2c + f \geq 2c + 18 \geq 108$.

V. Further Directions

It would be interesting to find extremal codes for any of the putative weight enumerators given in [7].

Particularly, there may exist a doubly-even $[72, 36, 16]$ code with an automorphism of order 2 with C cycles and f fixed points for $f = 0$ and for $c = f = 24$. If C is a doubly-even $[72, 36, 16]$ code with an automorphism of order 2 with 24 cycles and 24 fixed points $C' = g_{24}, \mathcal{D}_{\sigma}$ has to be a self-dual code of length 24, and $C'' = \mathcal{D}^* = \{\mathbf{0}, \mathbf{1}\}$.

References

[1] I. Boukliev and S. Buyuklieva, "Some new extremal self-dual codes with lengths $44, 50, 54$, and 58," *IEEE Trans. Inform. Theory*, vol. 44, pp. 809–812, Mar. 1998.

[2] A. E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[3] S. Buyuklieva, "On the binary self-dual codes with an automorphism of order 2," *Designs, Codes Cryptogr.*, vol. 12, pp. 39–48, 1997.

[4] ——, "New binary extremal self-dual codes with lengths 50 and 52," *Serdica Math. J.*, vol. 25, pp. 185–190, 1999.

[5] S. Buyuklieva and I. Boukliev, "Extremal self-dual codes with an automorphism of order 2," *IEEE Trans. Inform. Theory*, vol. 44, pp. 323–328, Jan. 1998.

[6] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, 1991.

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

[8] M. Harada, "Existence of new extremal doubly-even codes and extremal syngly-even codes," *Designs, Codes Cryptogr.*, vol. 8, pp. 273–283, 1996.

[9] M. Harada and H. Kimura, "On extremal self-dual codes," *Math. J. Okayama Univ.*, vol. 37, pp. 1–14, 1995.

[10] W. C. Huffman, "Automorphisms of codes with application to extremal doubly-even codes of length 48," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 511–521, 1982.

[11] W. C. Huffman and V. Tonchev, "The $[52, 26, 10]$ binary self-dual codes with an automorphism of order 7," in *Proc. Optimal Codes and Related Topics*, Sozopol, Bulgaria, 1998, pp. 127–136.

[12] V. Pless, "A classification of self-orthogonal codes over GF(2),," *Discr. Math.*, vol. 3, pp. 209–246, 1972.

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

[14] V. Tonchev and V. Yorgov, "The existence of certain extremal $[54, 27, 10]$ self-dual codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1628–1631, Sept. 1996.

[15] H. P. Tsai, "Existence of certain extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 501–504, 1992.

[16] ——, "Existence of some extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1829–1833, 1992.

[17] H. P. Tsai and Y. J. Jiang, "Some new extremal self-dual $[58, 29, 10]$ codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 813–814, Mar. 1998.

[18] V. Y. Yorgov, "Binary self-dual codes with automorphisms of odd order" (in Russian), *Probl. Pered. Inform.*, vol. 19, pp. 11–24, 1983.

[19] ——, "A method for constructing inequivalent self-dual codes with applications to length 56," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 77–82, 1982.