МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 1999
MATHEMATICS AND EDUCATION IN MATHEMATICS, 1999
Proceedings of Twenty Eighth Spring Conference of
the Union of Bulgarian Mathematicians
Montana, April 5–8, 1999

METHODS FOR CONSTRUCTING SELF-DUAL CODES

Stefka Hristova Buyuklieva

The purpose of this paper is to present some topics of the theory of self-dual codes. We have included some known results for binary, ternary and quaternary codes. We describe new methods for constructing self-dual codes over finite fields of q elements for $q = 2^t$, $t = 1, 2, ...$, and $q = 3$.

1. Introduction. Self-dual codes are an important class of codes (i) for practical reasons, since many of the best codes known are of this type, and (ii) for theoretical reasons, because of their connections with groups, lattices and designs.

A linear $[n, k]$ code C is a k-dimensional vector subspace of the vector space F_q^n, where F_q is the finite field of q elements. The parameter n is called length of C. The elements of C are called codewords and the (Hamming) weight of a codeword is the number of its non-zero coordinates. The minimum weight of C is the smallest weight among all non-zero codewords of C. An $[n, k, d; q]$ code is an $[n, k]$ code over F_q of minimum weight d. A matrix which rows form a basis of C is called a generator matrix of this code. The weight enumerator $W(y)$ of a code C is given by $W(y) = \sum_{i=0}^{n} A_i y^i$ where A_i is the number of codewords of weight i in C. Let $(u, v) : F_q^n \times F_q^n \to F_q$ be an inner product in the linear space F_q^n. Then if C is an $[n, k]$ linear code, $C^\perp = \{u \in F_q^n : (u, v) = 0$ for all $v \in C\}$. If $C \subseteq C^\perp$, C is termed self-orthogonal and if $C = C^\perp$, C is self-dual. If C is self-dual, then $k = \frac{1}{2}n$. The codes with the largest minimum distanse among all self-dual codes of given length are named extremal self-dual codes.

Let M be an $n \times n$ monomial matrix over F_q, containing exactly one nonzero element from F_q in each row and column. Then M sends a code C over F_q into the equivalent code $C' = \{uM : u \in C\}$. The set of all monomials such that $C' = C$ forms the automorphism group $Aut(C)$ of the code C. The action of M preserves weights and inner products, so that if C is self-orthogonal, so is C'. We usually specify M as a permutation of coordinates followed by multiplication by a diagonal matrix. If $M \in Aut(C)$ is a monomial matrix, which contains only 1's and 0's, we can specify it as a permutation of the n coordinates of C and consider as an element of the simmetric group S_n. We call it a permutation automorphism of C. If C is a binary code all automorphisms of C are permutation automorphisms.

A theorem of Gleason and Pierce (see [17]) implies that a self-dual code over F_q can only have all weights divisible by some integer $t > 1$ in five cases:

I	q=2,	t=2;
II	q=2,	t=4;
III	q=3,	t=3;
IV	q=4,	t=2;
V	q arbitrary,	t=2 and weight enumerator $(x^2 + (q-1)y^2)^{n/2}$.

The length of a self-dual code must be even. If $q = 2$ or 4 there is no other restriction on the length, and such codes have even weight and are of types I and IV, respectively. If $q = 2$ and the weight of every codeword is a multiple of 4, then n must be divisible by eight; these are type II codes. Finally, if $q = 3$ then the weights are multiples of 3, and n must be divisible by four: these are type III codes. The type I and type II codes are also named singly even and doubly even self-dual codes.

The paper is organized as follows. Section 2 is devoted to binary self-dual codes. We describe known methods for constructing such codes. In Section 3 we present some results about quaternary self-dual codes. In Section 4 we prove some properties of the ternary self-dual codes with a permutation automorphism of order 3 without fixed points. We give a construction technique to obtain such codes. Finally, in Section 5 we give a construction method for self-dual codes over F_q for $q = 2^t$ which possess an automorphism of order 2 without fixed points. This method is an extension of the method from [1] for the case $q = 2$.

2. Binary self-dual codes. The enumeration of binary self-dual codes of length $n \leq 32$ has been carried out in a series of papers: Pless [20] for $n \leq 20$; Pless and Sloane [21] for $n = 22$, 24; Conway and Pless [5] for $n = 26$ to 30 and Type II of length 32. For any greater length there exist a large number of such codes; for example, there are at least 17 000 inequivalent type II codes of length 40 [5]. However extremal codes seem relatively rare among these codes. In particular, there is one extremal self-dual doubly even code of length 8, two of length 16, one of length 24, and five of length 32. A list of possible weight enumerators of extremal binary self-dual codes of length up to 72 is given by Conway and Sloane in [7]. A lot of papers have provided constructions for some of the unknown codes. To obtain new extremal self-dual codes, some authors use the connection between self-dual codes and symmetric designs [13], [12], Hadamard matrices [19], [23], self-dual codes of smaller lengths [2], [4]. A method for constructing binary self-dual codes via an automorphism of odd prime order is given by Huffman and Yorgov [10], [24], [25]. In [4] we give a construction technique for binary self-dual codes with an automorphism of order 2 without fixed points.

Doubly even binary codes (type II codes) up through length 32 have been classified by the technique of complete enumeration in [5], [20], [21]. In [5] the 85 type II codes of length 32 were enumerated. For doubly even self-dual codes it is well known that $d \leq 4[\frac{n}{24}]+4$ for all n. A long-standing open question is the existence of a [72,36,16] doubly even code. Using Hadamard matrices, Tonchev [23], Ozeki [19] and other authors have found extremal doubly even self-dual codes. Kapralov and Tonchev [13] have obtained doubly even [64,32,12] codes from symmetric designs. Huffman [10] has shown that any type II [48,24,12] code with a nontrivial automorphism of odd order is equivalent to the extended quadratic residue code of this length. Yorgov has found all inequivalent extremal doubly-even codes of length n with an automorphism of odd prime order p for $n = 40$, $p > 5$ [24]; $n = 56$, $p = 13$ [25]; $n = 64$, $p = 31$ [26]. All doubly-even [40,20,8] self-dual codes with an automorphism of odd order were constructed by Yorgov and Ziapkov [27].

Although the type I codes of length 32 have not been classified, it is shown in [7] that there are precisely three inequivalent [32,16,8] extremal type I codes. For the singly even codes $d \leq 4[\frac{n}{24}]+4+\epsilon$, where $\epsilon = -2$ if $n = 2$, 4 or 6, $\epsilon = 2$ if $n \equiv 22 (\mathrm{mod}\ 24)$, and $\epsilon = 0$ otherwise. The classification of extremal double circulant self-dual codes of length up to 62, and of lengths 64 to 72, is given in [9] and [8], respectively. Huffman and Tonchev have constructed [50,25,10] self-dual codes from quasi-symmetric 2-(49,9,6) designs. All inequivalent extremal singly-even self-dual codes of length 40 with an automorphism of odd prime order are in [3]. Many extremal codes of lengths 42 and 44 are obtained using this technique [2,22].

3. Quaternary self-dual codes. We will consider two types of inner product in the vector space F_4^n over the quaternary field $F_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 + \omega + 1 = 0$ is the Euclidean inner product $(u, v) = uv = \sum_{i=1}^{n} u_i v_i$, and the Hermitian inner product $(u, v) = \sum_{i=1}^{n} u_i v_i^2$. We will call the quaternary self-dual codes with respect to Hermitian inner product Hermitian self-dual codes. For these codes we have $d \leq 2[\frac{n}{6}]+2$ [16]. Codes meeting this bound exist at lengths 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 28 and 30. They do not exist at lengths 12, 24, 102, 108, 114, 120, 122 and $n \geq 126$. The remaining lengths (26, 32, 34, ...) are undecided. The indecomposable Hermitian self-dual codes of length ≤ 16 were found in [16] and [6]. The long-standing question of the existence of a [24,12,10] code was settled in the negative by Lam and Pless [15]. In Section 5 we give a method for constructing quaternary self-dual codes which possess a permutation automorphism of order 2 without fixed points.

4. Ternary self-dual codes. Self-dual codes over F_3 are particularly interesting because they include the length 12 Golay code, quadratic residue codes, and symmetry codes. Ternary self-dual codes (type III codes) exist if and only if n is a multiple of 4. The codes with a length less than or equal to 20 have been completely classified in [6], [18]. Leon, Pless and Sloane [14] give a partial enumeration of the self-dual codes of length 24, making use of the complete list of Hadamard matrices of order 24, and show that there are precisely two codes with minimum distance 9. For the ternary self-dual codes we have $d \leq 3[\frac{n}{12}] + 3$. Codes meeting this bound exist at lengths 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 56, 60 and 64. Such codes do not exist at lengths 72, 96, 120 and all $n \geq 144$. The existence of extremal codes in the remaining cases ($n = 52$, 68, 76, ..., 140) is undecided.

Huffman [11] has given a method for constructing ternary self-dual codes with an automorphism of prime order $p \neq 3$. In this section we introduce a construction technique for ternary self-dual codes with a permutation automorphism of order 3 without fixed points. To prove some properties of these codes, we use the theory of finitely generated modules.

Let C be a ternary self-dual code of length n and $\sigma = (1,2,3)(4,5,6)\dots(n-2,n-1,n)$ be an automorphism of C. Obviously, n must be divisible by 3, and since for ternary self-dual codes n must by divisible by 4, we have $n = 12t$. Hence the dimension of C is $6t$.

We can consider C as an $F_3[x]$-module using σ by setting $f * v = vf(\sigma)$ for all $f \in F_3[x]$ and all $v \in C$. Then C is a finitely generated torsion module. For $v \in C$ we set $Ann(v) = \{f \in F_3[x], f * v = 0\}$. Obviously $Ann(v)$ is an ideal of $F_3[x]$ generated by $(x-1)^3 = x^3 - 1$, $(x-1)^2 = x^2 + x + 1$ or $(x-1)$ for any $v \in C$. So there exist vectors $v_1, \dots, v_l$ in C such that $C = C_1 \oplus C_2 \oplus \dots \oplus C_l$, where C_i is a cyclic submodule of C, generated by v_i. Let $Ann(v_1) = Ann(v_2) = \dots = Ann(v_s) = \langle x^3 - 1\rangle$, $Ann(v_{s+1}) = Ann(v_{s+2}) = \dots = Ann(v_{s+m}) = \langle x^2 + x + 1\rangle$, and $Ann(v_{s+m+1}) = \dots = Ann(v_l) = \langle x - 1\rangle$. Hence $w_i = \lambda_i v_i + \mu_i v_i\sigma + \nu_i v_i\sigma^2$, $\lambda_i, \mu_i, \nu_i \in F_3$, for any vector $w_i \in C_i$, $i = 1, \dots, s$, $w_i = \lambda_i v_i + \mu_i v_i \sigma$, $\lambda_i, \mu_i \in F_3$, for any vector $w_i \in C_i$, $i = s+1, \dots, s+m$, and $w_i = \lambda_i v_i$ for $w_i \in C_i$, $i = s+m+1, \dots, l$. It follows that for any vector v from C

$$v = w_1 + w_2 + \dots + w_l = \sum_{i=1}^{s}(\lambda_i v_i + \mu_i v_i\sigma + \nu_i v_i \sigma^2) + \sum_{i=s+1}^{s+m}(\lambda_i v_i + \mu_i v_i \sigma) + \sum_{i=s+m+1}^{l} \lambda_i v_i.$$

The vectors v_1, $v_1\sigma$, $v_1\sigma^2$, v_2, $v_2\sigma$, $v_2\sigma^2$, $\dots$, v_s, $v_s\sigma$, $v_s\sigma^2$, v_{s+1}, $v_{s+1}\sigma$, $\dots$, v_{s+m}, $v_{s+m}\sigma$, v_{s+m+1}, $\dots$, v_l are linearly independant and so they form a basis of C. Therefore $6t = \dim C = 3s + 2m + (l - s - m) = 2s + m + l$.

Lemma 4.1. *$F(C) = \{v \in C : (x-1) * v = 0\}$ and $F'(C) = \{v \in C : (x-1)^2 * v = 0\}$ are linear subspaces of C of dimensions l and $6t - s$, respectively.*

Proof. Let $w \in F(C)$ and

$$w = \sum_{i=1}^{s}(\lambda_i v_i + \mu_i v_i\sigma + \nu_i v_i \sigma^2) + \sum_{i=s+1}^{s+m}(\lambda_i v_i + \mu_i v_i \sigma) + \sum_{i=s+m+1}^{l} \lambda_i v_i.$$

Then

$$w\sigma = \sum_{i=1}^{s}(\lambda_i v_i\sigma + \mu_i v_i\sigma^2 + \nu_i v_i \sigma^3) + \sum_{i=s+1}^{s+m}(\lambda_i v_i\sigma + \mu_i v_i \sigma^2) + \sum_{i=s+m+1}^{l} \lambda_i v_i\sigma$$

$$= \sum_{i=1}^{s}(\lambda_i v_i\sigma + \mu_i v_i\sigma^2 + \nu_i v_i) + \sum_{i=s+1}^{s+m}(\lambda_i v_i\sigma - \mu_i v_i - \mu_i v_i \sigma) + \sum_{i=s+m+1}^{l} \lambda_i v_i = w.$$

It follows that $\lambda_i = \mu_i = \nu_i$ for $i = 1, \dots, s$, and $\lambda_i = -\mu_i$ for $i = s+1, \dots, s+m$, and hence

$$w = \sum_{i=1}^{s}\lambda_i(v_i + v_i\sigma + v_i\sigma^2) + \sum_{i=s+1}^{s+m}\lambda_i(v_i - v_i\sigma) + \sum_{i=s+m+1}^{l} v_i.$$

Since the vectors $v_1+v_1\sigma+v_1\sigma^2$, ..., $v_s+v_s\sigma+v_s\sigma^2$, $v_{s+1}-v_{s+1}\sigma$, ..., $v_{s+m}-v_{s+m}\sigma$, $v_{s+m+1},\dots,v_l$ are linearly independant, they form a basis of $F(C)$. It follows that $\dim F(C)=l$.

Let $w\in F'(C)$. Then

$$0=w+w\sigma+w\sigma^2=\sum_{i=1}^{s}(\lambda_i+\mu_i+\nu_i)(v_i+v_i\sigma+v_i\sigma^2).$$

It follows that $\lambda_i+\mu_i+\nu_i=0$ for $i=1,\dots,s$, and so

$$w=\sum_{i=1}^{s}\lambda_i(v_i-v_i\sigma)+\sum_{i=1}^{s}\nu_i(v_i\sigma-v_i\sigma^2)+\sum_{i=s+1}^{s+m}(\lambda_iv_i+\mu_iv_i\sigma)+\sum_{i=s+m+1}^{l}\lambda_iv_i.$$

It is easy to see that the vectors $v_1-v_1\sigma, v_1\sigma-v_1\sigma^2,\dots,v_s-v_s\sigma, v_s\sigma-v_s\sigma^2, v_{s+1}$, $v_{s+1}\sigma,\dots,v_{s+m},v_{s+m}\sigma,v_{s+m+1},\dots,v_l$ are linearly independant and belong to $F'(C)$. Hence they form a basis of $F'(C)$.

For the dimension of $F'(C)$ we have $\dim F'(C)=2s+2m+(l-s-m)=s+m+l=6t-s$.

Let us consider the map $\phi: C\to F_3^{4t}$ defined by $\phi(v)=(\beta_1+\beta_2+\beta_3,\dots,\beta_{n-2}+\beta_{n-1}+\beta_n)$ for $v=(\beta_1,\beta_2,\dots,\beta_n)\in C$. Obviously, ϕ is a homomorphism.

Lemma 4.2. *$\phi(C)$ is a self-orthogonal $[4t,s]$ ternary code with a basis $\phi(v_1),\dots,\phi(v_s)$ and* $\operatorname{Ker}\phi=F'(C)$.

Proof. For the kernel of the map ϕ we obtain $\operatorname{Ker}\phi=\{v=(\beta_1,\beta_2,\dots,\beta_n)\in C:\phi(v)=0\}=\{v\in C:\beta_{3i-2}+\beta_{3i-1}+\beta_{3i}=0, i=1,\dots,4t\}=\{v\in C: v+v\sigma+v\sigma^2=0, i=1,\dots,4t\}=F'(C)$. It follows that $\dim\phi(C)=\dim C-\dim\operatorname{Ker}\phi=6t-6t+s=s$.

Let $\alpha_1\phi(v_1)+\cdots+\alpha_s\phi(v_s)=0$. Then $\phi(\alpha_1v_1+\cdots+\alpha_sv_s)=0$ and so $v=\alpha_1v_1+\cdots+\alpha_sv_s\in\operatorname{Ker}\phi=F'(C)$. Thus

$$v=\sum_{i=1}^{s}\lambda_i(v_i-v_i\sigma)+\sum_{i=1}^{s}\mu_i(v_i\sigma-v_i\sigma^2)+\sum_{i=s+1}^{s+m}(\lambda_iv_i+\mu_iv_i\sigma)+\sum_{i=s+m+1}^{l}\lambda_iv_i$$

and we have $\alpha_i=\lambda_i=\mu_i=0$. Hence the vectors $\phi(v_1),\dots,\phi(v_s)$ are linearly independant and therefore they form a basis of $\phi(C)$.

Let $v=(\alpha_1,\alpha_2,\dots,\alpha_n)$ and $w=(\beta_1,\beta_2,\dots,\beta_n)$ are vectors from C. Since C is a self-dual code we have $(\phi(v),\phi(w))=\sum_{i=1}^{4t}(\alpha_{3i-2}+\alpha_{3i-1}+\alpha_{3i})(\beta_{3i-2}+\beta_{3i-1}+\beta_{3i})=(v,w)+(v,w\sigma)+(v,w\sigma^2)=0$. This proves that $\phi(C)$ is a self-orthogonal $[4t,s]$ code.

For $w\in F(C)$ we obviously have $w=(\alpha_1,\alpha_1,\alpha_1,\dots,\alpha_{4t},\alpha_{4t},\alpha_{4t})$. This allows us to define the map $\pi: F(C)\to F_3^{4t}$ by $\pi(w)=(\alpha_1,\alpha_2,\dots,\alpha_{4t})$. The "contracted" code $C''=\pi(F(C))$ has length $4t$ and dimension l.

Lemma 4.3. *$C''=(\phi(C))^{\perp}$ and so $l=4t-s$, $m=2t-s$.*

Proof. Let $(\alpha_1,\dots,\alpha_{4t})=\pi(v)\in C''$ and $(\gamma_1,\dots,\gamma_{4t})=\phi(w)=(\beta_1+\beta_2+\beta_3,\dots,\beta_{n-2}+\beta_{n-1}+\beta_n)\in\phi(C)$, where $v=(\alpha_1,\alpha_1,\alpha_1,\dots,\alpha_{4t},\alpha_{4t},\alpha_{4t})$ and $w=$

$(\beta_1, \beta_2, \ldots, \beta_n)$ are vectors from C. Then $(\pi(v), \phi(w)) = (v, w) = 0$. Hense the vectors in C'' are orthogonal to the vectors from $\phi(C)$.

Let $u = (\delta_1, \ldots, \delta_{4t}) \in \phi(C)^{\perp}$. Then $(w, \pi^{-1}u) = \sum_{i=1}^{4t} (\beta_{3i-2} + \beta_{3i-1} + \beta_{3i})\delta_i = (\phi(w), u) = 0$ for all $w \in C$. Hence $\pi^{-1}(u) \in C$ and so $u \in C''$ and thus $C'' = (\phi(C))^{\perp}$.

It follows that $\dim C'' + \dim \phi(C) = 4t$ and hence $\dim C'' = l = 4t - \dim \phi(C) = 4t - s$. Since $l + m + 2s = 6t$ we have $m = 6t - l - 2s = 6t - 4t + s - 2s = 2t - s$.

Let C_1 be a self-orthogonal $[4t, s]$ ternary code and C_2 be its dual code. Let $\tau_1, \tau_2 : C_1 \to F_3^{12t}$, and $\psi : C_2 \to F_3^{12t}$ are the maps defined by

$$\tau_1(v) = (\alpha_1, 0, 0, \alpha_2, 0, 0, \ldots, \alpha_{4t}, 0, 0), \quad \tau_2(v) = (0, \alpha_1, 0, 0, \alpha_2, 0, \ldots, 0, \alpha_{4t}, 0)$$

for $v = (\alpha_1, \alpha_2, \ldots, \alpha_{4t}) \in C_1$ and $\psi(w) = (\beta_1, \beta_1, \beta_1, \ldots, \beta_{4t}, \beta_{4t}, \beta_{4t})$ for $w = (\beta_1, \beta_2, \ldots, \beta_{4t}) \in C_2$. Let C_3 is a self-dual $[4t, 2t]$ subcode of C_2 containing C_1, and $\theta : C_2 \to F_3^{12t}$ be the map defined by $\theta(w) = (\beta_1, 2\beta_1, 0, \ldots, \beta_{4t}, 2\beta_{4t}, 0)$.

Theorem 4.4. *$C = \tau_1(C_1) + \tau_2(C_1) + \psi(C_2) + \theta(C_3)$ is a self-dual $[12t, 6t]$ ternary code.*

Proof. Since τ_1, τ_2, θ and ψ are monomorphisms the dimensions of codes $\tau_1(C_1)$, $\tau_2(C_1)$, $\psi(C_2)$, and $\theta(C_3)$ are s, s, $4t - s$ and $2t$, respectively. Obviously, $\tau_1(C_1) \cap \tau_2(C_1) = \{0\}$, and $(\tau_1(C_1) + \tau_2(C_1)) \cap \psi(C_2) = \{0\}$ and therefore the dimension of $\tau_1(C_1) + \tau_2(C_1) + \psi(C_2)$ is $2s + 4t - s = 4t + s$. $v \in (\tau_1(C_1) + \tau_2(C_1) + \psi(C_2)) \cap \theta(C_3)$ iff $v = (\alpha_1, 2\alpha_1, 0, \ldots, \alpha_{4t}, 2\alpha_{4t}, 0) \in \theta(C_1)$. Hence $(\tau_1(C_1) + \tau_2(C_1) + \psi(C_2)) \cap \theta(C_3) = \theta(C_1)$ and $\dim(\tau_1(C_1) + \tau_2(C_1) + \psi(C_2) + \theta(C_3)) = 4t + s + 2t - s = 6t$.

For $v_1, v_2 \in C_1$, $w_1, w_2 \in C_2$, $u_1, u_2 \in C_3$ we have $(\tau_1(v_1), \tau_1(v_2)) = (v_1, v_2) = 0$, $(\tau_2(v_1), \tau_2(v_2)) = (v_1, v_2) = 0$, $(\psi(w_1), \psi(w_2)) = 3(w_1, w_2) = 0$, $(\theta(u_1), \theta(u_2)) = (u_1, u_2) + 2(u_1, u_2) = 0$, $(\tau_1(v_1), \tau_2(v_2)) = 0$, $(\tau_1(v_1), \psi(w_1)) = (v_1, w_1) = 0$, $(\tau_1(v_1), \theta(u_1)) = (v_1, u_1) = 0$, $(\tau_2(v_1), \psi(w_1)) = (v_1, w_1) = 0$, $(\tau_2(v_1), \theta(u_1)) = 2(v_1, u_1) = 0$, $(\psi(w_1), \theta(u_1)) = (w_1, u_1) + 2(w_1, u_1) = 0$, It follows that all vectors in C are orthogonal to each other and thus C is a self-dual code.

Example. Let $t = 1$, $C_1 = \{0\}$ and so $C_2 = F_3^4$, and C_3 be the self-dual [4,2,3] code with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

Using the construction method from Theorem 4.4 we obtain the ternary self-dual [12,6,3] code $4\mathcal{E}_3(12)$ [18].

5. Self-dual codes over $GF(2^t)$ with a monomial automorphism of order 2 without fixed points. In this section we consider self-dual codes over finite fields with 2^t elements for $t \geq 1$ with respect to the Euclidean inner product $(u, v) = uv = \sum_{i=1}^{n} u_i v_i$ (Euclidian codes), and with respect to the Hermitian inner product $(u, v) = u\overline{v} = \sum_{i=1}^{n} u_i v_i^{\sqrt{q}}$ (Hermitian codes) for $q \geq 4$. We prove two theorems. The first one gives some important properties of self-dual codes over $GF(2^t)$ with an automorphism of order 2 without fixed points. The second theorem gives us a method for constructing such codes.

Theorem 5.1. *Let C be a self-dual $[n, k = \frac{n}{2}]$ code over the field F_q for $q = 2^t$ and $\sigma = (1,2)(3,4)\ldots(n-1,n)$ be a monomial automorphism of C. Let $\phi : C \to F_q^k$ be the map defined by $\phi(v) = (\alpha_1 + \alpha_2, \ldots, \alpha_{n-1} + \alpha_n)$ for $v = (\alpha_1, \ldots, \alpha_n) \in C$. Then ϕ is a homomorphism, $C' = \operatorname{Im}\phi$ is a self-orthogonal $[k, s]$ code and $C'' = \pi(\operatorname{Ker}\phi) = (\phi(C))^{\perp}$, where $\pi : \operatorname{Ker}\phi \to F_q^k$ is the map defined by $\pi(v) = (\alpha_1, \ldots, \alpha_k)$ for $v = (\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k) \in \operatorname{Ker}\phi$.*

Proof. Clearly ϕ is linear and hence ϕ is a homomorphism. Thus $\phi(C)$ is a $[k, s]$ code for some s. To show it is self-orthogonal, let $v = (\alpha_1, \ldots, \alpha_n)$ and $w = (\beta_1, \ldots, \beta_n)$ be codewords in C. Then $(\phi(v), \phi(w)) = \sum_{i=1}^{k}(\alpha_{2i-1} + \alpha_{2i})(\beta_{2i-1} + \beta_{2i})^m = \sum_{i=1}^{k}(\alpha_{2i-1} + \alpha_{2i})(\beta_{2i-1}^m + \beta_{2i}^m) = \sum_{i=1}^{k}(\alpha_{2i-1}\beta_{2i-1}^m + \alpha_{2i}\beta_{2i}^m) + \sum_{i=1}^{k}(\alpha_{2i-1}\beta_{2i}^m + \alpha_{2i}\beta_{2i-1}^m) = (v, w) + (v, w\sigma) = 0$ as $w\sigma \in C$, where $m = 1$ for Euclidian codes and $m = 2^{t-1}$ for Hermitian codes.

As $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \operatorname{Ker}\phi$ iff $\alpha_{2i-1} = \alpha_{2i}$ for $1 \le i \le k$, $\operatorname{Ker}\phi = C_1 = \{(\beta_1, \beta_1, \beta_2, \beta_2, \ldots, \beta_k, \beta_k) \in C\}$. Let $v_1, \ldots, v_t$ be a basis of C_1 and extend this to a basis $v_1, \ldots, v_t, v_{t+1}, \ldots, v_k$ of C. Define C_2 to be the code with basis $v_{t+1}, \ldots, v_k$. Thus $C = C_1 \oplus C_2$. Since $C_1 = \operatorname{Ker}\phi$, $\phi(C) = \phi(C_2)$. Furthermore the restriction of ϕ to C_2 is one-to-one as $\operatorname{Ker}\phi = C_1$ and $C_1 \cap C_2 = \{0\}$. Therefore $s = \dim \operatorname{Im}\phi = \dim C_2 = k - t$ or $s + t = k$.

The map $\pi : \operatorname{Ker}\phi \to F_2^k$ is clearly one-to-one linear map, and thus $\dim C'' = \dim \operatorname{Ker}\phi = t$. As $\dim C' = s$ and $s + t = k$, to prove that $C'' = (C')^{\perp}$, it suffices to show that a vector in C' is orthogonal to a vector in C''. Let $v = (\alpha_1, \ldots, \alpha_n) \in C$ and $w = (\beta_1, \beta_1, \beta_2, \beta_2, \ldots, \beta_k, \beta_k) \in \operatorname{Ker}\phi$. Then $(\phi(v), \pi(w)) = \sum_{i=1}^{k}(\alpha_{2i-1} + \alpha_{2i})\beta_i^m = (v, w) = 0$, $m = 1$ or $m = 2^{t-1}$.

Theorem 5.2. *Let C' be a self-orthogonal $[k, s, d']$ code, C'' be its dual code and $\psi : C'' \to F_2^{2k}$ be the map defined by $\psi(v) = (\alpha_1, \alpha_1, \ldots, \alpha_k, \alpha_k)$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C''$. Let $M = \{(j_1, j_2), (j_3, j_4), \ldots, (j_{2r-1}, j_{2r})\}$ be a set of r pairs of different coordinates of the code C', $0 \le 2r \le k$, and $\tau : C' \to F_2^{2k}$ be the map defined by $\tau(v) = (\alpha_1', \alpha_1'', \ldots, \alpha_k', \alpha_k'')$ for $v = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in C'$, where $(\alpha_i', \alpha_i'') = (\alpha_i, 0)$ for $i \ne j_l$, $l = 1, 2, \ldots, 2r$, and $(\alpha_{j_{2i-1}}', \alpha_{j_{2i-1}}'', \alpha_{j_{2i}}^{prime}, \alpha_{j_{2i}}'') = (\alpha_{j_{2i-1}} + \alpha_{j_{2i}}, \alpha_{j_{2i}}, \alpha_{j_{2i-1}} + \alpha_{j_{2i}}, \alpha_{j_{2i-1}},)$ for $i = 1, \ldots, r$. Then $C = \tau(C') + \psi(C'')$ is a self-dual $[2k, k]$ code and $\sigma = (1,2)(3,4)\ldots(2k-1, 2k)$ is an automorphism of C.*

Proof. If $u, v \in C''$ then $(\psi(u), \psi(v)) = (u, v) + (u, v) = 0$. Let $u = (\alpha_1, \ldots, \alpha_k), v = (\beta_1, \ldots, \beta_k) \in C'$, and $w = (\gamma_1, \ldots, \gamma_k) \in C''$. As $\alpha_{j_{2i-1}}'\beta_{j_{2i-1}}' + \alpha_{j_{2i-1}}''\beta_{j_{2i-1}}'' + \alpha_{j_{2i}}'\beta_{j_{2i}}' + \alpha_{j_{2i}}''\beta_{j_{2i}}'' = (\alpha_{j_{2i-1}} + \alpha_{j_{2i}})(\beta_{j_{2i-1}} + \beta_{j_{2i}})^m + \alpha_{j_{2i}}\beta_{j_{2i}}^m + (\alpha_{j_{2i-1}} + \alpha_{j_{2i}})(\beta_{j_{2i-1}} + \beta_{j_{2i}})^m + \alpha_{j_{2i-1}}\beta_{j_{2i-1}}^m = \alpha_{j_{2i}}\beta_{j_{2i}}^m + \alpha_{j_{2i-1}}\beta_{j_{2i-1}}^m$ for $i = 1, \ldots, r$, and $\alpha_i'\beta_i' + \alpha_i''\beta_i'' = \alpha_i\beta_i$ for $i \ne j_l$, $l = 1, 2, \ldots, 2r$, we have $(\tau(u), \tau(v)) = (u, v) = 0$.

It follows from the definition of τ that $\alpha_i' + \alpha_i'' = \alpha_i$ for $i = 1, 2 \ldots k$. Hence $(\tau(u), \psi(w)) = (\alpha_1' + \alpha_1'')\gamma_1^m + \ldots + (\alpha_k' + \alpha_k'')\gamma_k^m = \alpha_1\gamma_1^m + \ldots + \alpha_k\gamma_k^m = (u, v) = 0$ ($m = 1$ or 2^{t-1}). Therefore the code C is self-orthogonal.

Since τ and ψ are monomorphisms the dimensions of the codes $\tau(C')$ and $\psi(C'')$ are s and $k - s$ respectively. Obviously $\tau(C') \cap \psi(C'') = \{0\}$ and therefore the dimension of C is $s + k - s = k$. Hence the code C is self-dual.

As $\psi(w)\sigma = \psi(w) \in C$ for $w \in C''$ and $\tau(v)\sigma = \tau(v) + \psi(v) \in C$ for $v \in C'$ we have $u\sigma = \tau(v) + \psi(v) + \psi(w) = \tau(v) + \psi(v + w) \in C$ for $u = \tau(v) + \psi(w) \in C$. Therefore σ is an automorphism of C of order 2.

Examples. For $s = 0$ we have $C' = \{0\}$ and $C'' = F_q^k$. Using these codes and Theorem 2 we obtain the $[2k, k, 2]$ self-dual codes e_2^k which have generator matrix $(I_k|I_k)$ where I_k is the identity matrix. These codes are self-dual under the two types of inner product.

Let k be even and C' be the code $\{00\ldots0, 11\ldots1\}$. If we use theorem 2 we can construct a self-dual $[2k, k, 4]$ code with a generator matrix

$$\begin{pmatrix} 1111 & \ldots & & \\ & 1111 & \ldots & \\ & & \ldots & \\ & & & \ldots 1111 \\ 1010 & & & \ldots 1010 \end{pmatrix}$$

REFERENCES

[1] S. Buyuklieva, On the binary self-dual codes with an automorphism of order 2, *Designs, Codes and Cryptography*, **12**, 1997, 39–48.

[2] S. Buyuklieva, New extremal self-dual codes of lengths 42 and 44, *IEEE Trans. Inform. Theory*, **43**, 1997, 1607–1612.

[3] S. Buyuklieva, V. Yorgov, Singly-even self-dual codes of length 40, *Designs, Codes and Cryptography*, **9**, 1996, 131–141.

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

[5] J. H. Conway, V. Pless, On the enumeration of self-dual codes, *J. Combinatorial Theory*, **28-A**, 1980, 26–53.

[6] J. H. Conway, V. Pless, N. J. A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory*, **25**, 1979, 312–322.

[7] J. H. Conway, N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, **36**, 1990, 1319–1333.

[8] T. A. Gulliver, M. Harada, Classification of extremal double circulant self-dual codes of lengths 64 to 72", *Designs, Codes and Cryptography*, **13**, 1998, 257–269.

[9] M. Harada, H.Kaneta, Classification of extremal double circulant self-dual codes of length up to 62", *Discrete Mathematics*, to appear.

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

[11] W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory*, **38**, 1992, 1395–1400.

[12] W. C. Huffman, V. D. Tonchev, The existence of extremal [50,25,10] codes and quasi-symmetric 2-(49,9,6) designs",*Designs,Codes and Cryptography*, **6**, 1995, 97–106.

[13] S. Kapralov, V. Tonchev, Extremal doubly even codes of length 64 derived from symmetric designs, *Discrete Math.*, **83**, 1990, 285–289.

[14] J. S. Leon, V. Pless, N. J. A. Sloane, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory*, **27**, 1981, 176–180.

[15] C. W. H. Lam, V. Pless, There is no (24,12,10) self-dual quaternary code, *IEEE Trans. Inform. Theory*, **36**, 1990, 1153–1156.

[16] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, H. N. Ward, Self-dual codes over $GF(4)$, *J. Comb. Theory*, **25-A**, 1978, 288–318.

[17] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[18] C. L. Mallows, V. Pless, N. J. A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Applied Math.*, **31**, 1976, 649–666.
[19] M. Ozeki, Hadamard matrices and doubly even self-dual error-correcting codes, *J. Combinatorial Theory*, **44-A**, 1987, 274–287.
[20] V. Pless, A classification of self-orthogonal codes over $GF(2)$, *Discrete Mathematics*, **3**, 1972, 209–246.
[21] V. Pless, N. J. A. Sloane, On the classification and enumeration of self-dual codes, *J. Combinatorial Theory*, **18A**, 1975, 313–335.
[22] R. Ruseva, V. Yorgov, Two extremal codes of length 42 and 44 (in Russian), *Probl. Pered. Inform.*, **29**, 1993, 99–103.
[23] V. D. Tonchev, Self-dual codes and Hadamard matrices, *Discr. Appl. Math.*, **33**, 1991, 235–240.
[24] V. Yorgov, Binary self-dual codes with automorphisms of odd order (in Russian), *Probl. Pered. Inform.*, **19**, 1983, 11–24.
[25] V. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56", *IEEE Trans. Inform. Theory*, **33**, 1987, 77–82.
[26] V. Yorgov, Doubly-even extremal codes of length 64 (in Russian), *Probl. Pered. Inform.*, **22**, 1986, 277–284.
[27] V. Yorgov, N. Ziapkov, Doubly-even self-dual [40,20,8] codes with automorphisms of odd order, *Probl. Pered. Inform.*, **32**, 1996, 41–46.

Stefka Buyuklieva
Faculty of Mathematics and Informatics
University of Veliko Tarnovo
BG-5000 Veliko Tarnovo
E-mail: `lpmivt@bgcict.acad.bg`

МЕТОДИ ЗА КОНСТРУИРАНЕ НА САМОДУАЛНИ КОДОВЕ

Стефка Христова Буюклиева

Целта на тази статия е да представи някои аспекти от теорията на самодуалните кодове. Включени са някои известни резултати за кодове над полета с 2, 3 и 4 елемента. Описан е и нов метод за конструиране на самодуални кодове над крайни полета с q елемента за $q = 2^t$, $t = 1, 2 \ldots$, и $q = 3$.