SOME NEW SELF-DUAL [96, 48, 16] CODES WITH AN AUTOMORPHISM OF ORDER 15*

NIKOLAY I. YANKOV

ABSTRACT: *A new method for constructing binary self-dual codes with an automorphism of order pq for $p \neq q$ was developed in [1]. We use this method to construct new doubly-even self-dual [96, 48, 16] codes having an automorphism of order 15 with 6 cycles of length 15 and two cycles of length 3. More than 100000 new such codes are obtain. We found exactly 219 different values of the parameter in the weight distribution of these codes of which 211 are new.*

KEYWORDS: *automorphisms, construction, self-dual codes*

1. Introduction

A *linear* $[n,k]$ code C is a k-dimensional subspace of the vector space $GF(q)^n$, where $GF(q)$ is the finite field of q elements. The elements of C are called *codewords* and the (Hamming) weight of a codeword is the number of its nonzero coordinate positions. The *minimum weight* d of C is the smallest weight among all nonzero codewords of C, and C is called a $[n,k,d]$ code.

A matrix which rows form a basis of C is called the *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. The dual code of C is $C^{\perp} = \{u \in F_q^n : (u,v) = 0 \text{ for all } v \in C\}$. The *dual code* $C^{\perp}$ is a

* This work is supported by Shumen University under Project RD-08-234/12.03.2014

linear $[n, n-k]$ code. We call the code C *self-orthogonal* if $C \subseteq C^{\perp}$. If $C = C^{\perp}$ then the code C is termed *self-dual*.

Two binary codes are *equivalent* if one can be obtained from the other by a permutation of coordinates. The permutation $\sigma \in S_n$ is an automorphism of C, if $C = \sigma(C)$. The set of all automorphisms of C forms a group, called the *automorphism group* $Aut(C)$ of C. For two different primes $p < q$ we say that an automorphism σ of order pq is of *type* $pq-(c, t_p, t_q, f)$ if it has c cycles of length pq, t_p cycles of length p, t_q cycles of length q and f fixed points in its decomposition into disjoint cycles.

A self-dual code C is *doubly-even* if all codewords of C have a weight divisible by four and *singly-even* if there is at least one codeword of weight congruent 2 modulo 4. Rains in [1] proved that the minimum distance d of a binary self-dual $[n, k, d]$ code satisfies the following bound:

$$d \le 4\lfloor n/24 \rfloor + 4, \quad \text{if } n \not\equiv 22 \pmod{24},$$
$$d \le 4\lfloor n/24 \rfloor + 6, \quad \text{if } n \equiv 22 \pmod{24}.$$

Codes achieving this bound are called extremal. If n is a multiple of 24, then a self-dual code meeting the bound must be doubly-even (see [2]). Moreover, for any nonzero weight w in such a code, the codewords of weight w form a 5-design [3]. This is one reason why extremal codes of length *24m* are of particular interest. Unfortunately, only for $m = 1$ and $m = 2$ such codes are known, namely the $[24, 12, 8]$ extended Golay code and the $[48, 24, 12]$ extended quadratic residue code. Thus the existence of no other extremal code of length *24m* is known. For $n = 96,$ only the primes 2, 3 and 5 may divide the order of the automorphism group of the extremal code. We focus our attention on the case of an automorphism of order 15. In [1] it is proved that a binary doubly-even [96, 48, 20] self-dual code with an automorphism of order 15 does not exist. The question of finding a doubly-even self-dual $[96, 48, 16]$ code first

appears in [4] where also the first such code was constructed. In recent years such codes with an automorphism of order 23 are constructed in [5] and [6]; four codes are known from [7]; ten more codes are constructed in [8] and a code with an automorphism of order $2^6 3^2 5 \times 31$ is constructed in [9]. We will construct many new doubly-even self-dual $[96, 48, 16]$ codes with an automorphism of order 15 using a method for constructing binary self-dual codes invariant under the action of a cyclic group of order pq for odd primes $p \neq q$. The structure of the note is as follows. We begin with short description of the method in Section 2 (for more details and proves we refer the reader to [1]). In Section 3 we apply this method to obtain codes with $n = 96, k = 48$ and minimum distance 16 having an automorphism of type 15-(6, 0, 2, 0).

2. Self-dual codes with an automorphism of order pq for $p < q$ odd primes

We consider the case $r = pq$ for different odd primes p and q such that 2 is a primitive root modulo p and modulo q. The ground field is $\mathbb{F}_2$. Then

$$x^r - 1 = (x-1)Q_p(x)Q_q(x)Q_r(x) = (1+x)(1+x+\cdots+x^{p-1})(1+x+\cdots+x^{q-1})Q_r(x),$$

where $Q_i(x)$ is the i-th cyclotomic polynomial. Moreover, both $Q_p(x)$ and $Q_q(x)$ are irreducible over $\mathbb{F}_2$ since 2 is a primitive root modulo p and modulo q as well. Finally, if

$$Q_r(x) = g_3(x)\ldots g_s(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x)$$

is the factorization of the r-th cyclotomic polynomial into irreducible factors over $\mathbb{F}_2$, then these factors have the same degree, namely $\frac{\phi(r)}{s-2+2t} = \frac{(p-1)(q-1)}{s-2+2t}$, where ϕ is Euler's phi function.

Let the code C be a binary self-dual codes possessing an automorphism of order pq.

$$\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+t_q} \Omega_{c+t_q+1} \dots \Omega_{c+t_q+t_p} \Omega_{c+t_q+t_p+1} \dots \Omega_{c+t_q+t_p+f},$$

where $\Omega_i = ((i-1)r+1,\dots,ir)$ are the pq−cycles for $i = 1,\dots,c$, $\Omega_{c+i} = (cr+(i-1)q+1,\dots,cr+iq)$ − cycles of length q for $i = 1,\dots,t_q$, $\Omega_{c+t_q+i} = (cr+t_q q+(i-1)p+1,\dots,cr+t_q q+ip)$ − cycles of length p for $i = 1,\dots,t_p$, and $\Omega_{c+t_q+t_p+i} = (c+t_q+t_p+i)$ are the fixed points for $i = 1,\dots,f$.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$ and $E_\sigma(C) = \{v \in C : wt(v \mid \Omega_i) \equiv 0 \pmod 2, i = 1,\dots,c+t_q+t_p\}$, where $v \mid \Omega_i$ is the restriction of v on Ω_i. With this notation we have the following.

Theorem 1 ([1]) The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$.

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the binary field $\mathbb{F}_2$, and let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+t_q+t_p+f}$ be the projection map, i.e., $(\pi(v))_i = v_j$ for some $j \in \Omega_i$ and $i = 1,2,\dots, \ c+t_q+t_p+f$.

Clearly, $v \in F_\sigma(C)$ iff $v \in C$ and v is constant on each cycle of σ.

Theorem 2 ([1]) If C is a binary self-dual code with an automorphism σ of odd order then $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c+t_q+t_p+f$.

Consider the factor ring $\mathcal{R} = \mathbb{F}_2[x] / \langle x^r - 1 \rangle$, where $\langle x^r - 1 \rangle$ is the principal ideal in $\mathbb{F}_2[x]$ generated by $x^r - 1$. Let $x^r - 1 = f_0(x) f_1(x) \dots f_s(x)$ be the factorization of $x^r - 1$ into

irreducible factors $f_i(x)$ over $\mathbb{F}_2$ where $f_0(x)=x-1$. Let $I_j=\left\langle \frac{x^r-1}{f_j(x)} \right\rangle$ be the ideal of $\mathcal{R}$ generated by $\frac{x^r-1}{f_j(x)}$ for $j=0,1,\ldots,s$. By $e_j(x)$ we denote the generator idempotent of I_j; i.e., $e_j(x)$ is the identity of the two-sided ideal I_j.

With these notations we have the following result (see [10]).

Theorem 3 (i) $\mathcal{R}=I_0\oplus I_1\oplus\cdots\oplus I_s$.

(ii) I_j is a field which is isomorphic to the field $\mathbb{F}_{l^{deg(f_j(x))}}$ for $j=0,1,\ldots,s$.

(iii) $e_i(x)e_j(x)=0$ for $i\neq j$.

(iv) $\sum_{j=0}^{s} e_j(x)=1$.

There is a decomposition (see [11]) $x^r-1=g_0(x)g_1(x)\cdots g_m(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x)$, where $s=m+2t$ and $\{g_0,g_1,\ldots g_m,h_1,h_1^*,\ldots,h_t,h_t^*\}=\{f_0,f_1,\ldots,f_s\}$. Furthermore, $h_i^*(x)$ is the reciprocal polynomial of $h_i(x)$, $h_i^*\neq h_i$ for $i=1,\ldots,t$ and $g_i(x)$ coincides with its reciprocal polynomial where $g_0(x)=f_0(x)=x-1$. We denote the field $\left\langle \frac{x^r-1}{g_j(x)} \right\rangle$ by G_j for $j=0,1,\ldots,m$, $\left\langle \frac{x^r-1}{h_j(x)} \right\rangle$ by H_j for $j=1,\ldots,t$, and $\left\langle \frac{x^r-1}{h_j^*(x)} \right\rangle$ by H_j^* for $j=1,\ldots,t$.

Let $E_\sigma(C)^*$ be the shortened code of $E_\sigma(C)$ obtained by removing the last $t_q q + t_p p + f$ coordinates from the codewords having 0's there. Next we define a map $\varphi : \mathbb{F}_2^{cr} \to \mathcal{R}^c$ by $\phi(v) = (v_0(x), v_1(x), \ldots, v_{c-1}(x)) \in \mathcal{R}^c$, where $v_i(x) = \sum_{j=0}^{r-1} v_{ij} x^j$ and $(v_{i0}, \ldots, v_{i,c-1}) = v|_{\Omega_i}$. Clearly, $\varphi(C)$ is a linear code over the ring $\mathcal{R}$ of length c. Moreover, we have $\phi(C)^\perp = \phi(C^\perp)$ where the dual code $C^\perp$ over $\mathbb{F}_2$ is taken under the Euclidean inner product, and the dual code $\phi(C)^\perp$ in $\mathcal{R}^c$ is taken with respect to the Hermitian inner product: $\langle u, v \rangle = \sum_{i=0}^{c-1} u_i \overline{v}_i \in \mathcal{R}^c$, $\overline{v}_i = v_i(x^{-1}) = v_i(x^{r-1})$. In particular, the code C is self-dual if and only if $\phi(C)$ is self-dual over $\mathcal{R}$ with respect to the Hermitian inner product.

Let $C_\varphi = \varphi(E_\sigma(C)^*)$. Since $E_\sigma(C)^*$ is a binary quasi-cyclic code of length *cr* and index c, C_φ is a linear code over the ring $\mathcal{R}$ of length c. Moreover $C_\varphi = (\bigoplus_{i=0}^{m} M_i) \oplus (\bigoplus_{j=1}^{t} (M'_j \oplus M''_j))$, where M_i is a linear code over the field G_i, $i = 1, \ldots, m$, M'_j is a linear code over H_j and M''_j is a linear code over H_j^*, $j = 1, \ldots, t$. For the dimensions we have

$$\dim E_\sigma(C)^* = \dim C_\phi =$$

$$= (p-1)\dim M_1 + (q-1)\dim M_2 + \frac{(p-1)(q-1)}{s-2+2t}\left(\sum_{i=3}^{s} \dim M_i + \sum_{j=1}^{t} (\dim M'_j + \dim M''_j)\right).$$

Since $E_\sigma(C)^*$ is a self-orthogonal code, C_φ is also self-orthogonal over the ring $\mathcal{R}$ with respect to the Hermitian inner product. This means that M_i are self-orthogonal codes of length c

over G_i for $i = 1,\ldots,m$ (with respect to the Hermitian inner product) and, for $1 \le j \le t$, we have $M_j'' \subseteq (M_j')^{\perp}$ with respect to the Euclidean inner product. This forces $\dim M_i \le c/2$ for $i = 1,2,\ldots,s$ and $\dim M_j' + \dim M_j'' \le c$.

It follows that

$$\dim E_\sigma(C)^* \le (p-1)\frac{c}{2} + (q-1)\frac{c}{2} + \frac{(p-1)(q-1)}{s-2+2t}\left((s-2)\frac{c}{2} + tc\right) = \frac{c(pq-1)}{2}.$$

3. Doubly-even self-dual [96, 48, 16] codes with an automorphism of type 15−(6, 0, 2, 0)

Let *C* be a doubly-even self-dual [96, 48, 16] code having an automorphism of type 15−(6, 0, 2, 0). The weight distribution of such a code has the form (see [7])

$$W(y) = 1 + (-28086 + \alpha)y^{16} + (3666432 - 16\alpha)y^{20} + (366474560 + 120\alpha)y^{24} + \cdots,$$

where α is an integer parameter. Codes with $\alpha = 36918$, 37332, 37608, 37884, 38022, 38160, 38298, 38436, 38574, 38712, 38850, 38988, 39126, 39264, 39402, 39540, 39678, 39816, 39954, 40092, 40230, 40368, 40506, 40920, 41334 are known from [5]; $\alpha = 37500$, 37524, 37584, 37598 are from [7]; the code in [4] has the weight enumerator corresponding to $\alpha = 37722$. Also the value $\alpha = 41106$ is known from [8] and $\alpha = 36864$, 36876, 36888, 36900, 36912, 36936, 36948, 36960, 36972, 36984 are from [9].

We have that M_1 is a Hermitian self-orthogonal $[6, 2, \ge 2]$ code over the field $G_1 \cong \mathbb{F}_4$, M_2 is a Hermitian self-dual $[6, 3, d_2]$ code over $G_2 \cong \mathbb{F}_{16}$, M' is a linear $[6, k', d']$ code over $H \cong \mathbb{F}_{16}$ and $M'' = (M')^{\perp}$ is its dual code with respect to the Euclidean inner product. Moreover, the code *C* has a generator matrix in the form

$$G = \begin{pmatrix} \pi^{-1}(C_\pi) & \\ \varphi^{-1}(M') & 0 \\ \varphi^{-1}(M'') & 0 \\ \varphi^{-1}(M_2) & 0 \\ \varphi^{-1}(M_1) & 0 \\ \varphi^{-1}(D) & \varphi^{-1}(I_2) \end{pmatrix}, \quad (1)$$

where the matrix $\begin{pmatrix} \text{gen}M_1 \\ D \end{pmatrix}$ generates the dual code of M_1 over G_1, and I_2 is the identity matrix over the quaternary field P_3. For the generator matrices of the codes M', M'', M_2 and C_π we refer the reader to [1]. In short 47 doubly-even self-orthogonal $[96, 40, 20]$ codes $C_{96,40,1}, \ldots, C_{96,40,47}$ were constructed and we continue to add the last 8 rows in G (coming from $\varphi^{-1}(M_1)$ and $\varphi^{-1}(D_1)$) to obtain $[96, 48, 16]$ codes. Since in every previous step we impose the restriction that the minimum distance of the code is 20 we cannot give full classification. We have four possible generator matrices for M_1:

$$G_1 = \begin{pmatrix} e_1 & 0 & e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & e_1 & 0 & 0 \end{pmatrix}, G_2 = \begin{pmatrix} e_1 & 0 & e_1 & e_1 & e_1 & 0 \\ 0 & e_1 & e_1 & xe_1 & x^2e_1 & 0 \end{pmatrix},$$

$$G_3 = \begin{pmatrix} e_1 & 0 & e_1 & 0 & 0 & 0 \\ 0 & e_1 & 0 & e_1 & e_1 & e_1 \end{pmatrix}, G_4 = \begin{pmatrix} e_1 & 0 & 0 & e_1 & e_1 & e_1 \\ 0 & e_1 & e_1 & 0 & e_1 & e_1 \end{pmatrix}.$$

Table 1: The values of α and the number of [96, 48, 16] codes with that α obtained

α	#	α	#	α	#	α	#	α	#	α	#	α	#
35316	1	36006	46	36486	596	36966	1660	37446	1039	37926	164	38406	16
35376	2	36012	61	36492	589	36972	1757	37452	1078	37932	179	38412	12
35442	1	36036	53	36516	668	36996	1664	37476	977	37956	167	38436	5
35502	1	36042	66	36522	729	37002	1593	37482	945	37962	171	38442	5
35562	2	36066	74	36546	766	37026	1673	37506	950	37986	124	38466	5

35586	2	36072	66	36552	738	37032	1597	37512	1036	37992	142	38472	9
35592	4	36096	71	36576	795	37056	1797	37536	870	38016	127	38496	5
35622	3	36102	68	36582	798	37062	1819	37542	890	38022	114	38502	2
35646	6	36126	124	36606	918	37086	1686	37566	807	38046	92	38526	4
35652	1	36132	106	36612	936	37092	1613	37572	753	38052	110	38532	5
35676	9	36156	133	36636	925	37116	1625	37596	720	38076	79	38556	3
35682	8	36162	134	36642	960	37122	1647	37602	746	38082	89	38562	2
35706	6	36186	145	36666	1027	37146	1719	37626	636	38106	74	38586	6
35712	2	36192	142	36672	1037	37152	1730	37632	696	38112	60	38592	2
35736	7	36216	197	36696	1174	37176	1602	37656	632	38136	63	38616	2
35742	7	36222	192	36702	1172	37182	1640	37662	580	38142	57	38622	1
35766	13	36246	246	36726	1146	37206	1618	37686	544	38166	38	38646	2
35772	11	36252	231	36732	1232	37212	1603	37692	569	38172	54	38652	2
35796	10	36276	238	36756	1223	37236	1610	37716	461	38196	52	38706	1
35802	5	36282	233	36762	1305	37242	1643	37722	459	38202	26	38712	1
35826	16	36306	295	36786	1410	37266	1345	37746	390	38226	33	38736	2
35832	12	36312	285	36792	1381	37272	1467	37752	431	38232	37	38742	1
35856	18	36336	376	36816	1360	37296	1359	37776	380	38256	27	38802	1
35862	21	36342	336	36822	1400	37302	1440	37782	420	38262	29	38862	1
35886	14	36366	356	36846	1446	37326	1401	37806	296	38286	26	38886	1
35892	20	36372	381	36852	1435	37332	1476	37812	310	38292	23	38916	1
35916	26	36396	378	36876	1529	37356	1256	37836	263	38316	24	38922	1
35922	24	36402	414	36882	1553	37362	1326	37842	277	38322	22		
35946	32	36426	510	36906	1467	37386	1164	37866	253	38346	20		
35952	24	36432	485	36912	1525	37392	1223	37872	229	38352	12		
35976	46	36456	529	36936	1582	37416	1200	37896	229	38376	10		
35982	37	36462	579	36942	1574	37422	1211	37902	240	38382	16		

After considering all permutation $\tau \in S_6$ of the columns of $G_1, \ldots, G_4$ and all right cyclic shift in all 6 six columns we found codes only when $\text{gen}\, M_1 = G_3$. The next theorem is a summary of the results we have obtained.

Theorem 4 There exist at least 114966 binary doubly-even $[96, 48, 16]$ self-dual codes with an automorphism of type 15-(6, 0, 2, 0).

114171 of the obtained codes have automorphism groups of order 15; 763 have automorphism groups of order 30, and 32 codes have groups of order 45. The 219 values of the parameter α in the weight distribution $W(y)$ and the number of the constructed codes are displayed in Table 1. Of all 219 only 8 values: 36876, 36912, 36936, 36972, 37332, 38022, 38436, 38712 were previously know, so we obtain 211 new values of the parameter.

REFERENCES

1. **Bouyuklieva St., W. Willems and N. Yankov**, On the Automorphisms of Order 15 for a Binary Self-Dual [96, 48, 20] code. // arXiv:1403.4735 [cs.IT], 2014.
2. **Rains E.M.**, Shadow bounds for self-dual-codes. // IEEE Trans. Inform. Theory, vol. 44, pp. 134–139, 1998.
3. **Assmus E.F. and H.F. Mattson,** New 5-designs. // J. Combin. Theory, vol. 6, pp. 122–151, 1969.
4. **Feit W.**, A self-dual even (96, 48, 16) code. // IEEE Trans. Inform. Theory, vol. 20, pp. 136–138, 1974.
5. **Dontcheva R.**, Doubly-even self-dual code of length 96. // IEEE Trans. Inf. Theory, vol. 48, no. 2, pp. 557–561, 2002.
6. **Yorgova R. and A. Wassermann**, Binary self-dual codes with automorphisms of order 23. // Des. Codes Cryptogr., vol. 48, no. 2, pp. 155–164, 2007.
7. **S. T. Dougherty, T. A. Gulliver, and M. Harada**, Extremal binary self-dual codes. // IEEE Trans. Inf. Theory, vol. 43, pp. 2036–2047, 1997.
8. **Kaya A. and B. Yildiz**, Extension theorems for self-dual codes over rings and new binary self-dual codes. // arXiv:1404.0195 [cs.IT], 2014.
9. **Kaya A., B. Yildiz, and I. Siap**, New extremal binary self-dual codes of length 68 from quadratic residue codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. // Finite Fields Their Appl., vol. 29, pp. 160–177, 2014.
10. **Huffman W.C., V. Pless**, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge 2003.
11. **Ling S., P. Sole**, On the algebraic structure of quasi-cyclic codes I: Finite fields. // IEEE Trans. Inform. Theory, vol. 47, pp. 2751–2760, 2001.