M a t h e m a t i c a
B a l k a n i c a

New Series Vol. 19, 2005, Fasc. 1-2

Quasi-Symmetric 2-(37,9,8) Designs and Self - Orthogonal Codes with Automorphisms of Order 5 *

Stefka Bouyuklieva[1], *Zlatko Varbanov*[2]

No quasi-symmetric 2-$(37, 9, 8)$ design is known. We prove that if such designs exist, they arise from self-orthogonal self-complementary $[38, 18, \geq 6]$ codes with a doubly-even $[37, 17, 8]$ subcode with dual distance at least 5. In this paper, it is shown that there are exactly 5 inequivalent doubly-even $[37, 17, 8]$ codes with needed dual distance and an automorphism of order 5. After the extending of these codes, no quasi-symmetric 2-$(37, 9, 8)$ design is obtained.

AMS Subj. Classification: 05B30, 11C08, 13F20, 20B25, 94B25

Key Words: quasi-symmetric designs, self-orthogonal codes, automorphisms

1.Introduction

A 2-(v, k, λ) design is called *quasi-symmetric* with intersection numbers x and y $(x < y)$ if the number of points in the intersection of two blocks takes only two values x and y. If $x \equiv y \equiv k \pmod 2$ these designs are self-orthogonal and are closely related to self-orthogonal codes (see [5]).

Let C be a binary $[n, k, d]$ code, that is, a k-dimensional vector subspace of F_2^n with minimum weight d, where F_2 is the field of two elements. C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$ where $C^\perp$ is the dual code of C. C is *doubly-even* if all codewords of C have weight divisible by four. Any doubly-even code is self-orthogonal. A linear code C is *self-complementary* if it contains the all one's vector $(11 \ldots 1)$.

The next theorem is the main tool in our research:

Theorem 1. *Let A be the $(b \times v)$-incidence matrix of a self-orthogonal $t - (v, k, \lambda)$ design. Then:*

*Partially supported by the Bulgarian National Science Fund under Contract No MM 1304/2003

1) If k is even, the rows of A generate a self-orthogonal binary code of length v with dual distance $d^{\perp} \geq \frac{v-1}{k-1} + 1$

2) If k is odd, the rows of the matrix $(1|A)$ generate a self-orthogonal binary code of length $v+1$ with dual distance $d^{\perp} \geq \frac{v}{k} + 1$.

The paper is organized as follows. In Section 2 we prove that if A is the 148×37-incidence matrix of a quasi-symmetric $2-(37,9,8)$ design then the rows of the matrix $(1|A)$ generate a self-orthogonal $[38, 18, \geq 6]$ binary code with dual distance $d^{\perp} \geq 6$ and this code contains a doubly-even $[37, 17, 8]$ subcode with dual distance at least 5. In Section 3 we construct all inequivalent doubly-even $[37, 17, 8]$ codes with dual distance ≥ 5 having an automorphism of order 5. Unfortunately, these codes do not give us quasi-symmetric designs.

2. Quasi-symmetric 2-(37,9,8) designs and their codes

Let A be the incidence matrix of a quasi-symmetric $2-(37,9,8)$ design with intersection numbers $x=1$ and $y=3$. Since the blocks of the design are 148, A is a 148×37-matrix. According to Theorem 1, the rows of the matrix $(1|A)$ generate a self-orthogonal binary $[38, k, d]$ code C with dual distance $d^{\perp} \geq 6$, therefore $d \geq 6$. All doubly-even codewords in C have the form $(0, w)$ where $w \in F_2^{37}$. Hence $C = (0|C_0) \cup (1|v+C_0)$ where C_0 is a doubly-even $[37, k-1, \geq 8]$ code. The dimensions of the dual codes of C and C_0 are the same. Therefore if $C^{\perp} = (0|D) \cup (1|w+D)$ then $C_0^{\perp} = D \cup w + D$. It follows that the dual distance of C_0 is $d_0^{\perp} \geq 5$.

Obviously, $k \leq 19$. Let $\bar{C}$ be a self-dual $[38, 19, \geq 6]$ code such that $C \subseteq \bar{C}$. If $\bar{C}_0 = \{w \in \bar{C} : wt(w) \equiv 0 (mod\ 4)\}$ then $dim(\bar{C}_0) = 18$ and $\bar{C}_0^{\perp} = \bar{C} \cup S(\bar{C})$. We call $S(\bar{C})$ the shadow of $\bar{C}$. If $C = \bar{C}$ then $\bar{C}_0 = (0|C_0)$ and since the dual distance of $(0|C_0)$ is 1 it follows that the minimum distance of the shadow $S(C)$ is 1. But it is known (see [2]) that all vectors in the shadow of a self-dual $[38, 19, d \geq 6]$ code have weights $\equiv 3 (mod\ 4)$ and therefore the case $C = \bar{C}$ is impossible. Hence $k \leq 18$.

The sum of two different rows of $(1|A)$ is a codeword in C of weight 12 or 16. Let the sums of weight 12 are s_{12}. To compute s_{12}, we need to compute the number of the submatrices of A in the form $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. We have $\binom{37}{2}$ pairs of columns in A and any pair belongs to 8 rows. Therefore we have exactly $\binom{37}{2}\binom{8}{2}$ submatrices of the required form. On the other hand, A contains s_{12} pairs of

rows with $y = 3$ common ones and any pair contains 3 such submatrices. Hence

$$3s_{12} = \binom{37}{2}\binom{8}{2} \Rightarrow s_{12} = 6216$$

It follows that the number of the codewords of weight 12 in C is $A_{12} \geq 6216$.

By the MacWilliams identities [4], $A_{12} - 6216 = 33 \cdot 2^{k-10} - 6420 - 6A_8 - 6A_6 - \alpha + 6A_{38} \geq 0$ where $A_{10} = 148 + \alpha$. Hence

$$33 \cdot 2^{k-10} \geq 6420 + 6A_8 + 6A_6 + \alpha - 6A_{38} \geq 6420 - 6 \Rightarrow 2^{k-10} \geq \frac{6414}{33} > 194$$

It follows that $k \geq 18$ and so $k = 18$.

Then $\bar{C} = C \cup (x + C), x \notin C$. Without loss of generality $x = (0, y)$. So we have

$$\bar{C} = (0|C_0) \cup (1|v + C_0) \cup (0|y + C_0) \cup (1|v + y + C_0)$$

If $wt(y) \equiv 0(mod\ 4)$ then $\bar{C}_0 = (0|C_0) \cup (0|y + C_0)$ which is impossible as $S(\bar{C})$ does not contain vectors of weight 1. Hence $wt(y) \equiv 2(mod\ 4)$. It follows that

$$\bar{C}_0 = (0|C_0) \cup (1|v + y + C_0), \qquad \bar{C}_2 = \bar{C} \backslash \bar{C}_0 = (1|v + C_0) \cup (0|y + C_0)$$

So the all one's vector $(11 \ldots 1) \in (1|v + C_0) \subset C$ and C is a self-orthogonal self-complementary $[38, 18, \geq 6]$ code with dual distance at least 6 such that $C = (0|C_0) \cup (1|1 + C_0)$ where C_0 is a doubly-even $[37, 17, 8]$ code with dual distance at least 5.

3. Doubly-even [37,17,8] codes with dual distance 5 having an automorphism of order 5

Since the doubly-even codes with these parameters are too many, we decided to enumerate the case of such codes with an automorphism of order 5. We use the method developed by Huffman and Yorgov (see [3], [6]).

Let C_0 be a doubly-even [37,17,8] code with an automorphism σ of order 5. The permutation σ is of type (c, f) if there are exactly c independent 5-cycles and f fixed points in its decomposition. We may assume that

$$\sigma = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10) \ldots (5c - 4, 5c - 3, 5c - 2, 5c - 1, 5c)$$

Denote the cycles of σ by $\Omega_1, \ldots, \Omega_c$ and the fixed points by $\Omega_{c+1}, \ldots, \Omega_{c+f}$. Let

$$F_\sigma(C_0) = \{v \in C_0 : v\sigma = v\}$$

and

$$E_\sigma(C_0) = \{v \in C_0 : wt(v|\Omega_i) \equiv 0 (mod\ 2), i = 1, 2, \ldots, c+f\}$$

where $v|\Omega_i$ is the restriction of v on Ω_i. Then the code C_0 is a direct sum of its subcodes $F_\sigma(C_0)$ and $E_\sigma(C_0)$.

Denote by $E_\sigma(C_0)^*$ the code $E_\sigma(C_0)$ with the last f coordinates deleted. For v in $E_\sigma(C_0)^*$ we let $v|\Omega_i = (v_0, v_1, v_2, v_3, v_4)$ correspond to a polynomial $v_0+v_1x+v_2x^2+v_3x^3+v_4x^4$ from P, where P is the set of even-weight polynomials in $F_2[x]/(x^5+1)$. It turns out that P is a field with 16 elements. Thus we obtain the map $\varphi : E_\sigma(C_0)^* \to P^c$.

Clearly $v \in F_\sigma(C_0)$ if and only if $v \in C$ and v is constant on each cycle. Let $\pi : F_\sigma(C_0) \to F_2^{c+f}$ be the projection map where if $v \in F_\sigma(C_0)$, $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \ldots, c+f$.

Theorem 2. *The binary code C_0 with an automorphism σ is doubly-even if and only if the following conditions hold:*

(1) $C_\pi = \pi(F_\sigma(C_0))$ is a doubly-even $[c+f, k_\pi]$ code, and

(2) $C_\varphi = \varphi(E_\sigma(C_0)^*)$ is a self-orthogonal $[c, k_\varphi]$ code over the field P under the Hermitian type inner product

$$(u, v) = \sum_{i=1}^{c} u_i v_i^4$$

Since $dim E_\sigma(C_0)^* = dim E_\sigma(C_0) = 4 dim C_\varphi = 4k_\varphi$ we have $dim C_0 = 17 = 4k_\varphi + k_\pi$. C_π is a self-orthogonal code and therefore $k_\pi \leq (c+f)/2 = (37-4c)/2$, hence $k_\pi \leq 18-2c$. It follows that $4k_\varphi+k_\pi = 17 \leq 4k_\varphi+18-2c$ and $k_\varphi \geq \frac{2c-1}{4}$. In the same time $k_\varphi \leq \frac{c}{2}$ and therefore c must be even and $k_\varphi = \frac{c}{2}$. So C_φ is a Hermitian self-dual code of length c and $E_\sigma(C)^*$ is a self-orthogonal doubly-even $[5c, 2c, \geq 8]$ code. Since no [10,4,8] code exists, $c = 4$ or 6.

- $c = 4$. In this case C_φ is a $[4, 2, 3]$ code over $GF(16)$. We consider the elements of $P^* = P \setminus \{0\}$ in the form $\alpha^i\delta^j$, $0 \leq i \leq 4, 0 \leq j \leq 2$, where $\alpha = xe = 1 + x^2 + x^3 + x^4$ is an element of P^* of order 5 and $\delta = x + x^4$ is an element of order 3. The orthogonality condition gives us that up to equivalence $C\varphi$ has a generator matrix

$$G_\varphi = \begin{pmatrix} e & 0 & \delta & \delta^2 \\ 0 & e & \delta^2 & \delta \end{pmatrix}$$

So we have a unique up to equivalence subcode $E_\sigma(C_0)^*$ and its generator matrix is

$$G_E = \begin{pmatrix} 01111\ 00000\ 01001\ 00110 \\ 10111\ 00000\ 10100\ 00011 \\ 11011\ 00000\ 01010\ 10001 \\ 11101\ 00000\ 00101\ 11000 \\ 00000\ 01111\ 00110\ 01001 \\ 00000\ 10111\ 00011\ 10100 \\ 00000\ 11011\ 10001\ 01010 \\ 00000\ 11101\ 11000\ 00101 \end{pmatrix}$$

In this case C_π is a doubly-even self-orthogonal $[21, 9, \geq 4]$ code. There exist three inequivalent such codes and using them and the code C_φ, we obtain five inequivalent doubly-even $[37, 17, 8]$ codes with dual distance 5. The obtained self-orthogonal $[38, 18, \geq 6]$ codes $C = (0|C_0) \cap (1|1 + C_0)$ have weight enumerators
$W_{C_1}(z) = 1 + 7z^6 + 170z^8 + 420z^{10} + 6916z^{12} + \cdots$
$W_{C_2}(z) = W_{C_3}(z) = W_{C_4}(z) = 1 + 6z^6 + 165z^8 + 430z^{10} + 6942z^{12} + \cdots$
$W_{C_5}(z) = 1 + 9z^6 + 180z^8 + 400z^{10} + 6864z^{12} + \cdots$

Unfortunately, the sets of their codewords of weight 10 do not contain quasi-symmetric designs.

- $c = 6$. In this case $f = 7$ and C_0 has a generator matrix of the form

$$\begin{pmatrix} G_E & O \\ G_c & G_f \end{pmatrix}$$

where G_E is a generator matrix of $E_\sigma(C_0)^*$, O is the 12×7 zero matrix, and $(G_c\ G_f)$ is a generator matrix of $F_\sigma(C_0)$. G_f is a 5×7 matrix and it generates a binary $[7, k_f \leq 5]$ code C_f. If $x \perp C_f$ then $(00\ldots0, x) \perp C_0$. Hence $wt(x) \geq 5$ and the dual code of C_f is a $[7, 7 - k_f \geq 2, \geq 5]$ code. Such a code does not exist and therefore we do not obtain doubly-even $[37, 18, 8]$ codes with dual distance at least 5 in this case.

So there are exactly five inequivalent doubly-even [37,17,8] codes with dual distance at least 5 having an automorphism of order 5. They give us five self-orthogonal self-complementary [38,18,6] codes with dual distance 6. None of them contains a quasi-symmetric 2-(37,9,8) design. After that the next Theorem is obvious:

Theorem 3. *If a quasi-symmetric 2-(37,9,8) design exists, it does not have automorphisms of order 5.*

4. Conclusion

The problem of the existing of quasi-symmetric 2-$(37, 9, 8)$ designs is still open. We have proved some properties of the corresponding self-orthogonal codes but even after the restrictions these codes are too many for a complete enumeration. So we decided to start with the codes having an automorphism of a given prime order p. We have completed only the case $p = 5$. The same method has been used successfully for constructing quasi-symmetric designs with some other parameters (see [1]). It does not guarantee that if the required design exists we will find it but if such a design has an automorphism of the same order p then we will obtain it.

References

[1] S. Bouyuklieva, M. Harada. Extremal self-dual [50,25,10] codes with automorphisms of order 3 and quasi-symmetric 2-(49,9,6) designs, *Designs, Codes and Cryptography*, **28**, 2003, 163-169.

[2] 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.

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

[4] F. J. MacWilliams, N. J. A. Sloane. *The theory of error correcting codes*, Amsterdam: North-Holland, 1977.

[5] V. D. Tonchev. Codes, In: *The CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press, Boca Raton, 1996, 517–543.

[6] V. Y. Yorgov. A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory*, **33**, 1987, 77–82.

[1] *Department of Mathematics and Informatics*
Veliko Tarnovo University
Veliko Tarnovo 5000, BULGARIA
e-mail: stefka@uni-vt.bg

Received 30.09.2003

[2] *Department of Mathematics and Informatics*
Veliko Tarnovo University
Veliko Tarnovo 5000, BULGARIA
e-mail: vtgold@yahoo.com