МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2016
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2016
Proceedings of the Forty Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Pleven, April 6–10, 2016

A CONNECTION BETWEEN THREE $[44, 22, 8]$ SELF-DUAL CODES, MATHIEU GROUPS M_{22}, M_{23}, AND SELF-ORTHOGONAL DESIGNS*

Nikolay Yankov

A connection between three particular binary self-dual $[44, 22, 8]$ codes with large automorphism groups, Mathieu groups M_{22}, M_{21} and self-orthogonal designs with parameters 3-$(22, 8, 12)$, 2-$(21, 8, 28)$ and 1-$(23, 8, 80)$ is established.

1. Introduction. Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. A linear $[n, k]_q$ *code* C is a k-dimensional subspace of $\mathbb{F}_q^n$. We call the codes *binary* if $q = 2$. The number of the nonzero coordinates of a vector in $\mathbb{F}_q^n$ is called its *weight*. An $[n, k, d]_q$ code is an $[n, k]_q$ linear code with minimum nonzero weight d.

Let $(u, v) = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_2$ for $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ be the inner product in $\mathbb{F}_2^n$. Then if C is a binary $[n, k]$ code, its *dual* $C^\perp = \{u \in \mathbb{F}_2^n \mid (u, v) = 0 \text{ for all } v \in C\}$ is a $[n, n-k]$ binary code. If $C \subseteq C^\perp$, the code C is termed *self-orthogonal*, in case of $C = C^\perp$, C is called *self-dual*.

Two binary codes are *equivalent* if one can be obtained from the other by a permutation of the coordinate positions. The permutation $\sigma \in S_n$ is an *automorphism* of C, if $C = \sigma(C)$. The set of all automorphisms of a code forms a group called *the automorphism group* $\mathrm{Aut}(C)$. If a code C have an automorphism σ of odd prime order p, where σ has c independent p-cycles and f fixed points, then σ is said to be of *type* p-(c, f).

For a finite set of *points* $X = \{x_1, x_2, \ldots, x_v\}$ and a family $\mathcal{D} = \{B_1, B_2, \ldots, B_b\}$ of k-element subsets of X called *blocks*, we say that $\mathcal{D}$ is a $t-(v, k, \lambda)$-*block design* if every t-element subset of X is contained in exactly λ blocks from $\mathcal{D}$.

Every point from X is contained in a fixed number r of blocks. Sometimes a design is denoted by its five parameters (v, b, r, k, λ). Evidently, from this definition it follows that the parameters of a design satisfy the equations $bk = vr$ and $\lambda(v-1) = r(k-1)$.

An incidence matrix of a $t-(v, k, \lambda)$-design $\mathcal{D}$ is a $v \times b$ matrix $A = (a_{ij})$, where $a_{ij} = 1$ if and only if $x_i \in B_j$. *An automorphism* of a design is a permutation on the point set that preserves the block set. A group obtained under composition of automorphisms is *the full automorphism group* of a design, which we denote by $\mathrm{Aut}(\mathcal{D})$.

* **2010 Mathematics Subject Classification:** 94B05.
Key words: self-dual codes, automorphisms, optimal codes.
This research is partially supported by Shumen University under Project No RD-08-144/08.02.2016.

Block intersection numbers of a design $\mathcal{D}$ is the cardinality of the intersections of any two distinct blocks, $|B_i \cap B_j|$, $i \neq j$. A t-(v, k, λ) design is called *self-orthogonal* if the block intersection numbers have the same parity as the block size k, i.e. $|B_i \cap B_j| \equiv k (\text{mod } 2)$.

A Steiner system $S(v, k, t)$ is a rank 2 geometry with v points, such that each block contains exactly k points and each set of t points is incident with a unique block. The Steiner system $S(5, 8, 24)$ is also called the *Witt design* [13].

The first sporadic groups were discovered by E. Mathieu in 1861 and 1873 [9, 10]. The *Mathieu groups* are five sporadic simple groups M_n, that are multiply transitive permutation groups on n objects for $n = 11, 12, 22, 23$. By taking the Mathieu groups as a tower of extensions of the unique projective plain of order 4, their Steiner systems can be obtained [2].

There is a connection between self-dual codes and self-orthogonal designs given by next theorem.

Theorem 1 ([11]). *Let A be the incidence matrix of a self-orthogonal t-(v, k, λ) design then: a) when k is even, the rows of A generate binary self-orthogonal code of length v and dual distance $d^\perp \geq \dfrac{v-1}{k-1} + 1$.*
b) when k is odd, the rows of the matrix $(\mathbf{1}\ A)$ (where $\mathbf{1}$ is an all-one column) generate binary self-orthogonal code with length $v+1$ and dual distance $d^\perp \geq \dfrac{v}{k} + 1$.

Self-dual codes with an automorphism of odd prime order are an extensively studied subject. Although such codes are classified up to length 50 [14], there are still unusual codes, as for example, the three self-dual one $[44, 22, 8]$, with largest automorphism groups, possessing also the largest values of the parameter β in their weight enumerators. In [5] the following question remained unanswered: Which of the constructed self-dual $[44, 22, 8]$ codes with an automorphism of odd prime order have connections with combinatorial designs?

2. Main results. The weight enumerators of the extremal self-dual codes of length 44 are known [1]:

$$W_{44,1} = 1 + (44 + 4\beta)y^8 + (976 - 8\beta)y^{10} + (12289 - 20\beta)y^{12} + \dots, \quad 10 \leq \beta \leq 122,$$

$$W_{44,2} = 1 + (44 + 4\beta)y^8 + (1232 - 8\beta)y^{10} + (10241 - 20\beta)y^{12} + \dots, \quad 0 \leq \beta \leq 154.$$

All such codes with an automorphism of odd prime order are classified [5], whereby three of the codes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ standout by possessing the largest possible (or known) values of β and very large automorphism group:

(1) $\quad \mathcal{C}_1 \ : \ \beta = 154$ for $W_{44,2}, |\text{Aut}(\mathcal{C}_1)| = 786839961600 = 2^{16} \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11^2,$

(2) $\quad \mathcal{C}_2 \ : \ \beta = 122$ for $W_{44,1}, |\text{Aut}(\mathcal{C}_2)| = 3251404800 = 2^{15} \cdot 3^4 \cdot 5^2 \cdot 7^2,$

(3) $\quad \mathcal{C}_3 \ : \ \beta = 104$ for $W_{44,2}, |\text{Aut}(\mathcal{C}_3)| = 116121600 = 2^{13} \cdot 3^4 \cdot 5^2 \cdot 7.$

We take a look at the structure of these codes and prove a connection to Mathieu groups M_{22}, M_{21} and self-orthogonal designs with parameters 3-$(22, 8, 12)$, 2-$(21, 8, 28)$ and 1-$(23, 8, 80)$.

2.1. A connection between M_{22}, 3-$(22, 8, 12)$ self-orthogonal design and the code $\mathcal{C}_1$. The code $\mathcal{C}_1$ with weight $W_{44,2}$ for $\beta = 154$ was first constructed by V. Yorgov and R. Russeva in [15] as a code with an automorphism of order 11.

Theorem 2. *The code $\mathcal{C}_1$ has a generator matrix of the form* $\begin{pmatrix} D_1 & O \\ O & D_1 \\ \mathbf{1} & \mathbf{1} \\ X & X \end{pmatrix}$, *where*

$$D_1 = \begin{pmatrix} 1111111100000000000000 \\ 1111000011110000000000 \\ 1111000000001111000000 \\ 1110100010000010011000 \\ 1110100000010001000011 \\ 1110010000100100010010 \\ 1110010000010010100100 \\ 1110001000100001001100 \\ 1101100000011000001100 \\ 1011100001001000010010 \end{pmatrix}$$

results from the incidence matrix of a 3-$(22, 8, 12)$ *self-orthogonal design with* 330 *blocks,* $\mathbf{1}$ *is the all-one vector of length* 22, $X = (0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,1,0,1,0,1)$ *and O is a 10×22 zero matrix.*

Proof. We can take the generator matrix of $\mathcal{C}_1$ and compute all codewords of minimum weight 8. There are exactly 660 such codewords and it turns out that after a permutation we can split the 44 coordinate positions into two sets of 22 coordinates: $K_1 = \{1, \ldots, 22\}$ and $K_2 = \{23, \ldots, 44\}$ such that the first 330 minimum weight codewords have supports that are entirely in K_1 and the rest 330 minimum weight codewords have supports in K_2. We take the first set of words and remove their coordinates which are in the set K_2 and we denote the resulting 330×22 matrix by $\mathcal{D}_1$. Taking every set of three different coordinate position in $\mathcal{D}_1$, the number of words with support containing this three coordinates is always 12. Then $\mathcal{D}_1^T$ is an incidence matrix of a 3-$(22, 8, 12)$ design with $b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}} = 12.\frac{22.21.20}{8.7.6} = 330$ blocks. Since there are no 10-weight codewords in $\mathcal{C}_1$ and the code is self-dual, we can conclude that the cardinality w of the intersection of the support of two distinctive rows of $\mathcal{D}_1$ is $16 - 2w = 8$, 12, or 16. Therefore, $w = 4, 2, 0$ and this design is self-orthogonal. Taking the liner independent rows of $\mathcal{D}_1$ we found the matrix D_1. $\square$

Design with these parameters appear with number 6 in [12, Table 2] as a residual of the Witt system $S(5, 8, 24)$ [12]. It is known that the automorphism group of $S(5, 8, 24)$ (generated by the 8-weight words of the extended $[24, 12, 8]$ binary Golay code $\mathcal{G}_{24}$) is the same as $\mathrm{Aut}(\mathcal{G}_{24})$, that is the largest Mathieu group M_{24}. Taking the subgroup of M_{24} that fixes every duo, the result is the group $C_2 \times M_{22}$ with cardinality 887040. Also if the code G_{24} is shortened by two coordinates that from a duo, the result is a self-orthogonal $[22, 10, 8]$ code with automorphism group $C_2 \times M_{22}$ containing exactly 330 codewords of weight 8. Thus the automorphism group of the 3-$(22, 8, 12)$ design is exactly $C_2 \times M_{22}$ and so the automorphism group of a code generated by a direct sum of two such designs is $(C_2 \times M_{22})^2$. As we have seen in (1) we have the same cardinality and by using MAGMA [8] we have computed that the structure of the automorphism group is

$$\mathrm{Aut}(\mathcal{C}_1) = (C_2 \times M_{22})^2.$$

2.2. *A connection between M_{21}, 2-$(21, 8, 28)$ self-orthogonal design and the code $\mathcal{C}_2$.* The second code $\mathcal{C}_2$ with $\beta = 122$ in $W_{44,1}$ first appear in a paper of S. Bouyuklieva [4]. Taking the 532 words of weight 8, it turns out that there are two coordinate positions $1 \leq i < j \leq 42$ in which all these words have equal values. Removing all codewords with two ones in coordinates i, j and the two columns i and j, we are left with 420 words of weight 8 and 42 coordinate positions. Further the 42 coordinates can be split into two classes of 21 and we have a matrix in the form

$$\begin{pmatrix} \mathcal{D}_2 & O \\ O & \mathcal{D}_2 \end{pmatrix},$$

where $\mathcal{D}_2^T$ is an incidence matrix of a 2-$(21, 8, 28)$ block design with $b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}} = 28.\frac{21.20}{8.7} =$ 210 blocks, O is an appropriate zero matrix. This design is also self-orthogonal. We give the matrix resulting from the liner independent rows of $\mathcal{D}_2$,namely

$$D_2 = \begin{pmatrix} 100000000111110010010 \\ 010000000101101010101 \\ 001000000111001111000 \\ 000100000110010101110 \\ 000010000101011001011 \\ 000001000100110111001 \\ 000000100011101001110 \\ 000000010001110100111 \\ 000000001011010011101 \end{pmatrix}.$$

The above block design is numbered 10 in [12, Table 2] and is a residual from the Witt system $S(5, 8, 24)$ [12]. Its automorphism group is the Mathieu group M_{21}. The group structure of $\mathrm{Aut}(\mathcal{C}_2)$ is $C_2 \times (C_2 \times M_{21})^2$.

2.3. *A connection between M_{21}, 2-$(21, 8, 28)$ and 1-$(23, 8, 80)$ self-orthogonal designs and the code $\mathcal{C}_3$.* This code with weight enumerator $W_{44,1}$ for $\beta = 122$ is also constructed by S. Bouyuklieva in [4]. It has 460 codewords of weight 8. The coordinate positions can be split into two classes: the first set having 21 coordinate positions and 210 words with nonzero coordinates in this class. Similar to §2.2 this leads to the incidence matrix $\mathcal{D}_2^T$ of a self-orthogonal 2-$(21, 8, 28)$ design. The second class of coordinates leads to an incidence matrix $\mathcal{D}_3^T$ of a self-orthogonal 1-$(23, 8, 80)$ design. The group structure for this code is $\mathrm{Aut}(C) = (M_{21}) \times (C_2^4 \times C_3 \times A_5)$.

3. Conclusion. In a research by V. Tonchev [6, p.728], starting from the Witt system $S(5, 8, 24)$ and taking successive derived or residual designs, the designs in Table 1 are obtained. We have found a connection between the three self-dual $[44, 22, 8]$ codes and the two designs denoted in bold font.

Table 1. Derived and residual of the Witt system $S(5, 8, 24)$

			5-(24, 8, 1)			
		4-(23, 7, 1)		4-(23, 8, 4)		
	3-(22, 6, 1)		3-(22, 7, 4)		**3-(22, 8, 12)**	
2-(21, 5, 1)		2-(21, 6, 4)		2-(21, 7, 12)		**2-(21, 8, 28)**

The following open questions remain for the self-dual codes of length 44:

1. Prove the nonexistence of (or construct) a binary self-dual $[44, 22, 8]$ with weight enumerator:

   - $W_{44,1}$ for $\beta = 69, 71, 73, 75, \dots, 81, 83, 84, 85, 87, 88, 89, 91, \dots, 121$;
   - $W_{44,2}$ for $\beta = 57, 63, 65, 67, 69, 71, 73, 75, 77, \dots, 81, 83, 84, 85, 87, 88, 89, 91, \dots, 103, 105, \dots, 153$.

2. Are the constructed codes with weight enumerator $W_{44,1}$ for $\beta = 61, 63, 68, 72, 82, 86, 90, 122$ and $W_{44,2}$ for $\beta = 59, 61, 66, 68, 70, 86, 90, 104, 154$ unique examples of codes with their weight enumerator?

Remark. For computing the automorphism groups of the codes in this research we have used the software system Q-extensions by Iliya Bouyukliev [3].

REFERENCES

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

[2] M. Aschbacher. Sporadic Groups. Cambridge Tracts in Mathematics, Cambridge University Press, 1994.

[3] I. Bouyukliev. About the code equivalence. In: Advances in Coding Theory and Cryptography, Series on coding theory and cryptology, vol. 3, 2007, World Scientific Publishing, 126–151.

[4] S. Buyuklieva. New extremal self-dual codes of lengths 42 and 44. *IEEE Transactions on Information Theory*, **43**, No 5 (1997), 1607–1612.

[5] S. Bouyuklieva, N. Yankov, R. Russeva. On the classification of binary self-dual $[44, 22, 8]$ codes with an automorphism of order 3 or 7, *Int. J. Inf. Coding Theory*, **2**, No 1 (2011), 21–37.

[6] R. Graham, M. Grötschel, L. e. Lovász. Handbook of Combinatorics, Elsevier, 1995, vol. 1.

[7] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, **11** (2005), 451–490.

[8] MAGMA. MAGMA Calc, Computational Algebra Group, School of Mathematics and Statistics, University of Sydney. Available: `http://magma.maths.usyd.edu.au/calc/`. Accessed November 15, 2015.

[9] É. Mathieu. Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables. *Journal de Mathématiques Pures et Appliquées*, **6** (1861), 241–323.

[10] É. Mathieu. Sur la fonction cinq fois transitive de 24 quantités. *Journal de Mathématiques Pures et Appliquées*, **18** (1873), 25–46.

[11] V. Tonchev. Combinatorial configurations: designs, codes, graphs. Longman Scientific & Technical, 1988.

[12] V. Tonchev. Self-orthogonal designs, *Contemporary Math*, **111** (1990), 219–235.

[13] E. Witt. Die 5-Fach transitiven Gruppen von Mathieu. *Abh. Math. Sem. Univ. Hamburg*, **12** (1938), 256–264.

[14] N. Yankov, M. H. Lee. Classification of self-dual codes of length 50 with an automorphism of odd prime order. *Designs, Codes, and Cryptography*, **74**, No 3 (2015), 571–579.
[15] V. Yorgov, R. P. Russeva. Two Extremal Codes of Length 42 and 44. *Problems of Information Transmission*, **29**, No 4 (1993), 385–388.

Nikolay Ivanov Yankov
University of Shumen
Faculty of Mathematics and Informatics
115, Universitetska Str.
9712 Shumen, Bulgaria
e-mail: jankov_niki@yahoo.com

ВРЪЗКА МЕЖДУ ТРИ САМОДУАЛНИ [44, 22, 8] КОДА, ГРУПИТЕ НА МАТИЙО M_{22}, M_{23} И САМООРТОГОНАЛНИ ДИЗАЙНИ

Николай Иванов Янков

Доказана е връзка между три интересни двоични самодуални кодове с параметри [44, 22, 8] имащи големи групи от автоморфизми, групите на Матийо M_{22}, M_{21} и самоортогонални блок-дизайни с параметри 3-(22, 8, 12), 2-(21, 8, 28) и 1-(23, 8, 80).