Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 325–329*

A combinatorial construction of an M_{12}-invariant code [1]

Jürgen Bierbrauer jbierbra@mtu.edu
Department of Mathematical Sciences Michigan Technological University Houghton, Michigan 49931 (USA)

Stefano Marcugini, Fernanda Pambianco
{stefano.marcugini, fernanda.pambianco}@unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy

Abstract. In this work we summarized some recent results to be included in a forthcoming paper [2]. A ternary $[66, 10, 36]_3$-code admitting the Mathieu group M_{12} as a group of automorphisms has recently been constructed by N. Pace, see [3]. We give a construction of the Pace code in terms of M_{12} as well as a combinatorial description in terms of the small Witt design, the Steiner system $S(5, 6, 12)$. We also present a proof that the Pace code does indeed have minimum distance 36.

1 Introduction

A large number of important mathematical objects are related to the Mathieu groups. It came as a surprise when N. Pace found yet another such exceptional object, a $[66, 10, 36]_3$-code whose group of automorphisms is $Z_2 \times M_{12}$ (see [3]). We present here two constructions for this code, an algebraic construction which starts from the group M_{12} in its natural action as a group of permutations on 12 letters, and a combinatorial construction in terms of the Witt design $S(5, 6, 12)$. We also prove that the code has parameters as claimed. In the next section we start by recalling some of the basic properties of M_{12} and the small Witt design $S(5, 6, 12)$.

2 The ternary Golay code, M_{12} and $S(5, 6, 12)$

The Mathieu group M_{12} is sharply 5-transitive on 12 letters and therefore has order $12 \times 11 \times 10 \times 9 \times 8$. It is best understood in terms of the ternary Golay code $[12, 6, 6]_3$. The ternary Golay code has a generator matrix $(I|P)$ where I

[1]This research was supported in part by Ministry for Education, University and Research of Italy (MIUR) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INDAM).

is the $(6, 6)$-unit matrix and

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 2 & 1 & 2 \\ 1 & 1 & 2 & 0 & 2 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 1 & 2 & 2 & 1 & 1 & 0 \end{pmatrix}.$$

The group M_{12} acts in terms of monomial operations on the ternary Golay code. Here we identify the 12 letters with the columns of the generator matrix and consider the action of M_{12} as a group of permutations on those 12 letters $\{1, 2, \ldots, 12\}$. It is generated by h_1, h_2, h_3, h_4 and g where

$$h_1 = (2, 3, 5, 6, 4)(8, 9, 11, 12, 10), h_2 = (2, 3)(4, 5)(8, 9)(10, 11),$$

$$h_3 = (3, 5, 4, 6)(9, 11, 10, 12), h_4 = (1, 2)(5, 6)(7, 8)(11, 12),$$

$$g = (5, 12)(6, 11)(7, 8)(9, 10).$$

The group $H = \langle h_1, h_2, h_3, h_4 \rangle$ of order 120 is the stabilizer of $\{1, 2, 3, 4, 5, 6\}$.

Call a 6-set an **information set** if the corresponding submatrix is invertible, call it a **block** if the submatrix has rank 5. The terminology derives from the fact that the blocks define a Steiner system $S(5, 6, 12)$, the small Witt design. There are 132 blocks and $12 \times 11 \times 6$ information sets. The complement of a block is a block as well. The stabilizer of each 5-set is S_5, the stabilizer of a block has order $10 \times 9 \times 8 = 720 = 6!$ and the stabilizer of an information set has order 5! The stabilizer of a 2-set has order 1440. This stabilizer is the group $P\Gamma L(2, 9) \cong Aut(A_6)$. In the sequel we identify the 12 letters with a basis $\{v_1, \ldots, v_{12}\}$ of a vector space $V = V(12, 3)$ over the field with three elements and consider the corresponding action of M_{12} on V.

3 The 10-dimensional module of M_{12}

Clearly M_{12} acts on an 11-dimensional submodule of V, the **augmentation ideal** $I = \{\sum_{i=1}^{12} a_i v_i | \sum a_i = 0\}$ and on a 1-dimensional submodule generated by the **diagonal** $\Delta = v_1 + \cdots + v_{12}$. As we are in characteristic 3, we have $\Delta \in I$, and M_{12} acts on the 10-dimensional factor space $Z = I/\langle \Delta \rangle$. The $u_i = v_i - v_{12}, i \leq 11$ are a basis of I and $z_i = \overline{u_i} = u_i + \Delta \mathbb{F}_3, i \leq 10$ are a basis of Z. Here $\sum_{i=1}^{11} u_i = \Delta$, hence $z_{11} = -z_1 - \cdots - z_{10}$.

4 The Pace code

We consider the action of M_{12} on the 10-dimensional $\mathbb{F}_3$-vector space Z with its basis $z_i = \overline{u_i} = v_i - v_{12} + \Delta\mathbb{F}_3, i = 1, \ldots, 10$. Recall that it is induced by the permutation representation on $\{v_1, \ldots, v_{12}\}$. This action defines embeddings of M_{12} in $GL(10,3)$ and in $PGL(10,3)$. For each orbit of M_{12} we consider the projective ternary code whose generator matrix has as columns representatives of the projective points constituting the orbit.

Definition 1. *Let* $X \subset \{1, 2, \ldots, 12\}, |X| = 6$.
Define $v_X = \sum_{i \in X} v_i, z_X = \overline{v_X}$.

It is in fact clear that $v_X \in I$, and $z_X \in Z$ is therefore defined.

Proposition 2. *The* $z_X \in Z$ *where* X *varies over the blocks of* $S(5,6,12)$ *form an orbit of length* 132 *in* Z*. In the action on projective points (in* $PG(9,3)$*), this yields an orbit of length* 66.

Proof. Clearly M_{12} permutes the z_X in the same way as it permutes the blocks X. This yields an orbit of length 132 in $Z = V(10,3)$. If $\overline{X}$ is the complement of X, then $v_{\overline{X}} + v_X = \Delta$, hence $z_{\overline{X}} = -z_X$. It follows that M_{12} acts transitively on the 66 points in $PG(9,3)$ generated by the z_X (block X and its complement generating the same projective point). □

Definition 3. *Let* C *be the* $[66,10]_3$*-code whose generator matrix has as columns representatives of the orbit of* M_{12} *on the* z_X *where* X *is a block.*

This is one way of representing the Pace code. Observe that each complementary pair of blocks contributes one column of the generator matrix. We may use as representatives the vectors z_X where X varies over the 66 blocks X not containing the letter 12. As the stabilizer of a block in M_{12} is S_6 it follows that the stabilizer of a point in the orbit equals the stabilizer of a complementary pair of blocks and is twice as large as S_6. The stabilizer is $P\Gamma L(2,9)$, of order $2 \times 6!$

5 A combinatorial description

We introduce some notation.

Definition 4. *Let* $\mathcal{B}$ *be a family of subsets (blocks) of a* v*-element set* Ω*. Let* $A, B \subset \Omega$ *be disjoint subsets,* $|A| = a, |B| = b$*. Define a matrix* G *with* $k = v - a - b$ *rows and* n *columns where* n *is the number of blocks disjoint from* A*. Here we identify the rows of* G *with the points* $i \in \Omega \setminus (A \cup B)$ *and the columns with the blocks* X *disjoint from* A*. The entry in row* i *and column* X *is* $= 1$ *if* $i \in X$*, it is* $= 0$ *otherwise. As the entries of* G *are* $0, 1$ *we can consider them as elements of an arbitrary finite field* K*. Define* $\mathcal{C} = C_{A,B}(\mathcal{B}, K)$ *to be the code generated by* G *over* K*.*

In words: the column of G indexed by $X \in \mathcal{B}$ is the characteristic function of the set $X \setminus B$. We write $C_{a,b}(\mathcal{B}, K)$ instead if the choice of the subsets A, B does not matter. This is the case in particular if the automorphism group of $\mathcal{B}$ is $(a+b)$-transitive. Code $\mathcal{C}$ is a K-linear code of length n. Its designed dimension is k but the true dimension may be smaller. We have no clue what the minimum distance is. Observe that $C_{A,B}(\mathcal{B}, K)$ is a subcode of $C_{A,\emptyset}(\mathcal{B}, K)$: a generator matrix of the smaller code arises from the generator matrix of the larger code by omitting some $|B|$ rows.

Proposition 5. *The Pace code from Definition 3 is monomially equivalent to* $C_{1,1}(S(5,6,12), \mathbb{F}_3)$.

Proof. The generator matrix of Definition 3 has rows indexed by $i \in \{1, \ldots, 10\}$ and columns indexed by blocks X of $S(5,6,12)$ not containing the letter 12. If also $11 \notin X$, then the corresponding column is the characteristic function of X. Let $11 \in X$. As $z_{11} = -z_1 - \cdots - z_{10}$ the entries in this column are $= 0$ if $i \in X, = 2$ if $i \notin X$. Taking the negative of this column, we obtain the characteristic function of $\overline{X} \setminus \{12\}$. We arrive at the generator matrix of $C_{A,B}(S(5,6,12), \mathbb{F}_3)$ where $A = \{11\}, B = \{12\}$. □

6 Combinatorial properties of the small Witt design

The following elementary properties of the Steiner system $S(5,6,12)$ will be used in the sequel.

Lemma 6. *Let* $\Omega = \{1, 2, \ldots, 12\}$ *and* $A, B \subset \Omega, |A| = a, |B| = b$ *and such that* $A \cap B = \emptyset, a + b \leq 5$. *Let* $i(a,b)$ *be the number of blocks which contain* A *and are disjoint from* B. *Then* $i(b,a) = i(a,b)$ *and*

$$i(5,0) = 1, i(4,0) = 4, i(3,0) = 12, i(2,0) = 30, i(1,0) = 66,$$

$$i(1,1) = 36, i(2,1) = 18, i(3,1) = 8, i(4,1) = 3, i(2,2) = 10, i(3,2) = 5.$$

Proof. $i(5,0) = 1$ is the definition of a Steiner 5-design, $i(b,a) = i(a,b)$ follows from the fact that the complements of blocks are blocks. The rest follows from obvious counting arguments. □

The following combinatorial lemmas may be verified by direct calculations using coordinates.

Lemma 7. *A family of five 3-subsets of a 6-set contains at least two 3-subsets which meet in 2 points.*

Lemma 8. *Let* $U \subset \{1, 2, \ldots, 11\}$ *such that* $|U| = 6$. *The number of blocks* $B \in \mathcal{B}$ *such that* $|B \cap U| = 3$ *is* 20 *if* U *is a block, it is* 30 *if* U *is not a block.*

Lemma 9. *Let* $\Omega = \{1, 2, \ldots, 12\}$ *and* $\Omega = A \cup B \cup C$ *where* $|A| = |B| = |C| = 4$ *and* $P \in C$. *The number of blocks which meet each of* A, B, C *in cardinality* 2 *and avoid* P *is at most* 18.

7 The parameters of the Pace code

Theorem 10. *The Pace code is a self-orthogonal* $[66, 10, 36]_3$*-code.*

In the remainder of this section we prove Theorem 10. We use the Pace code in the form $C = C_{A,B}(S(5,6,12), \mathbb{F}_3)$ where $A = \{12\}, B = \{11\}$, see Definition 4. The length is $n = i(0,1) = 66$, the designed dimension is $k = 10$. Let $\mathcal{B}$ be the blocks of $S(5,6,12)$ not containing 12. Observe that the columns of G are the characteristic functions of $X \setminus \{11\}$ where $X \in \mathcal{B}$. Let $r_i, 1 \leq i \leq 10$ be the rows of the generator matrix of Definition 4. The codewords of C have the form $\sum_{i \in U} r_i - \sum_{j \in V} r_j$, where U, V are disjoint subsets of $\{1, \dots, 10\}$. The number of zeroes of this codeword is the **nullity** $\nu(U, V)$, the number of blocks $X \in \mathcal{B}$ satisfying the condition that $|X \cap U|$ and $|X \cap V|$ have the same congruence mod 3. Let $c \in \{0, 1, 2\}$ be this congruence. We need to show that $\nu(U, V) \leq 30$ for all (U, V) except when $U = V = \emptyset$. This will prove the claim that the nonzero weights are ≥ 36 and also that the dimension is 10.

Let $u = |U|, v = |V|$, let W be the complement of $U \cup V$ in $\{1, \dots, 11\}, w = |W|$. Observe $u + v + w = 11, w > 0$. We have $\nu(U, V) = \sum_c k_c(u, v, w)$, where $k_c(u, v, w)$ is the number of $X \in \mathcal{B}$ meeting each of U, V, W in a cardinality congruent to c mod 3. Observe that $k_c(u, v, w)$ is symmetric in its arguments as long as the side condition $w > 0$ is satisfied. The weight of r_i is $i(1, 1) = 36$ (this is case $u = 1, v = 0$). In particular $r_i \cdot r_i = 0$. Also $r_i \cdot r_j = 0$ for $i \neq j$ as $i(2, 1) = 18$ is a multiple of 3. It follows that C is self-orthogonal. All codeword weights and nullities are therefore multiples of 3.

It may be verified that $\nu(U, V) < 33$ in a case by case analysis, starting from large values of u. If $u = 10$ then $v = 0, w = 1$ and $\nu(10, 0) = k_0(10, 0, 1) = i(0, 2) = 30$. Cases $u \in \{6, 7, 8, 9\}$are similar.

Let $u = 5$. By symmetry it can be assumed $3 \leq v \leq 5$. In case $v = 5$ we have $k_1(5, 5, 1) \leq 10, k_0(5, 5, 1) \leq 20$, and in case $v = 4$ we have $k_2(5, 4, 2) \leq 12, k_1(5, 4, 2) \leq 2 + 10 = 12, k_0(5, 4, 2) \leq 8$, hence $\nu(5, 4) < 33$. As $k_2(5, 3, 3) \leq 18, k_1(5, 3, 3) \leq 9$ and $k_0(5, 3, 3) \leq 1 + 2 \times 2$ we have $\nu(5, 3) < 33$. The final case to consider is $(u, v, w) = (4, 4, 3)$. In case $c = 0$ we have that X meets two of the subsets U, V, W in cardinality 3. If $W \subset X$, there are at most two such blocks. There are at most four blocks meeting each of U, V in cardinality 3. It follows $k_0(4, 4, 3) \leq 6$. If $c = 1$, then either $U \subset X$ or $V \subset X$. It follows $k_1(4, 4, 3) \leq 6$. The most difficult case is $c = 2$. Lemma 9 states $k_2(4, 4, 3) \leq 18$. We are done.

References

[1] J. Bierbrauer, *Introduction to Coding Theory,* Chapman and Hall/ CRC Press 2004.

[2] J. Bierbrauer, S. Marcugini, F. Pambianco, Some codes with large automorphism groups, preprint.

[3] N. Pace, New ternary linear codes from projectivity groups, *Discr. Math.* 331, (2014), 22-26.