ON A NEW FAMILY OF SYMMETRY CODES AND RELATED NEW FIVE-DESIGNS

BY VERA PLESS

Communicated by Wallace Givens, May 15, 1969

For every prime $p \equiv -1$ (3) we define a self-orthogonal $(2p+2, p+1)$ code over GF (3). It can be shown that the group leaving a $(2p+2, p+1)$ code invariant is $\mathrm{PSL}_2(p)$. The minimum weights of the first five codes in the family are determined and lead to new 5-designs.

Let t, r, and n be integers with $t \leqq r \leqq n$. A λ; $t-r-n$ design D is a collection of subsets of the n integers, each subset containing r elements, such that any t-subset of the n integers is contained in the same number λ of subsets in D. Some designs, a 1; $5-6-12$, a 1; $5-8-24$, and a 48; $5-12-24$ associated with the Mathieu groups M_{12} and M_{24}, have been known for a long time. Recently, [1] and [5], 2; $5-6-12$ and 2; $5-8-24$ designs have been found. Using coding theory [2] other 5-designs were found for $n=24$ and $n=48$. We have found new 5-designs for $n=36$ and $n=60$ and a number of r's. Also we found new 5-designs for $n=24$ and $n=48$ which are not equivalent to the ones mentioned above. Two t-designs are called equivalent if there is a permutation of the n integers so that the subsets of D go onto subsets in D.

Let V_{2p+2} be a vector space over GF(3) with a fixed, orthonormal basis. We call a subspace of this space an error correcting code. We define a family of codes of $\dim(p+1)$ (referred to as $(2p+2, p+1)$ codes) by a basis (I, S_p) where S_p is given below.

$$S_p = \begin{array}{c|ccccc|} & \infty & 0 & 1 \cdots & j \cdots & (p-1) \\ \infty & 0 & 1 & 1 & 1 & 1 \\ 0 & \chi(-1) & \chi(0) & \chi(1) & \chi(j) & \chi(p-1) \\ 1 & \chi(-1) & & & & \\ \vdots & & & & & \\ i & \chi(-1) & & & \chi(j-i) & \\ \vdots & & & & & \\ (p-1) & \chi(-1) & & & & \end{array}$$

where $\chi(0)=0$, $\chi(\text{a square})=1$, $\chi(\text{a nonsquare})=-1$. We refer to the code generated by (I, S_p) as $C(p)$.

An important concept in coding is the weight of a vector v, this is the number of nonzero components it has. The linear transformations of interest here are the monomial transformations. The matrix of such a transformation has exactly one nonzero element in any row or column. Two codes are said to be equivalent if one is obtained from the other by a monomial transformation. Let $G(p)$ be the group of monomial transformations leaving $C(p)$ invariant.

THEOREM 1. *The code $C(p)$ is self orthogonal for all p; hence the weight of any vector in $C(p)$ is divisible by* 3.

This follows from the fact that S_p is self orthogonal over the reals [4, pp. 209, 210]; hence over GF(3), and every basis vector is self orthogonal.

THEOREM 2. *The group $G(p)$ contains a subgroup isomorphic to R where R modulo $\{I, -I\}$ is isomorphic to* $\mathrm{PSL}_2(p)$.

THEOREM 3. *For $p \equiv 1$ (4), $(-S_p, I)$ is also a basis of $C(p)$. For $p \equiv 3(4)$, (S_p, I) is also a basis of $C(p)$.*

In general if (I, S_p) is a basis of a code, $(-S_p^T, I)$ is the basis of the orthogonal code, which is $C(p)$ again since it is self orthogonal. The result then follows if we note that $S_p = S_p^T$ for $p \equiv 1(4)$ [4, p. 210] and $S_p = -S_p^T$ for $p \equiv 3(4)$ [4, p. 209].

COROLLARY. *If $p \equiv 1(4)$, $G(p)$ contains a subgroup isomorphic to Z_4R where $Z_4R = RZ_4$ and $R \cap Z_4 = \{I, -I\}$, and if $p \equiv -1(4)$, $G(p)$ contains a subgroup $Z_2 \times R$. In both cases R is as in Theorem* 2.

We use this theorem and the following lemma in determining the minimum weights of the first five codes.

LEMMA. (a) *The weight of the basis vectors of (I, S_p) is $p+1$.*
(b) *The weight of a linear combination of* 2 *basis vectors is $(p+7)/2$.*
(c) *The weight of a linear combination of* 3 *basis vectors is $\geqq (p+7)/2$.*
(d) *No linear combination of the rows of S_p is* 0.

The proof of this lemma depends on the fact that $S_pS_p^T = pI_{p+1}$ over the reals [4, pp. 209, 210], $S_pS_p^T = -I_{p+1}$ over GF (3) and hence is nonsingular over GF (3). Part (c) follows from parts (a) and (b).

We relate t-designs to codes as in (2). The minimum weight in a code, denoted by d, is the weight of the nonzero vector in the code of smallest weight.

Case I. $p = 5$. This is a (12, 6) code.

By the use of Theorem 3 and the lemma it can be shown that $d=6$. Hence this code is equivalent to the Golay code (7). It is known that its minimum weight vectors hold $1; 5-6-12$ designs (1) and (7).

Case II. $p=11$. This is a (24, 12) code:

Again Theorem 3 and the lemma show that $d=9$. Hence by the Assmus-Mattson Theorem (2) the vectors of weights 9, 12, and 15 hold 5-designs. They also hold 4, 3, 2, and 1 designs. There is a (24, 12) quadratic residue code with the same d as $C(11)$, however, since the entire group of the quadratic residue code (2) and its associated $6; 5-9-24$ design (3) is $PSL_2(23)$, and since $C(11)$ is invariant under PSL_2 (11) which is not contained in PSL_2 (23), this implies that the two codes are not equivalent and the two 5-designs are not equivalent.

Case III. Let $p=17$. This is a (36, 18) code.

By Theorem 3 and the lemma we can say that all linear combinations of the basis vectors except 4 or 5 at a time have weight $\geqq 12$. All linear combinations taken 4 at a time were calculated on a computer and found to have weight $\geqq 12$. Again Theorem 3 and the lemma tell us that linear combinations taken 5 at a time have weight $\geqq 12$. Hence $d=12$.

By the Assmus-Mattson Theorem (2), the vectors of weights 12, 15, 18 and 21 hold 5-designs. These are the first 5-designs found for these parameters. These vectors also hold 4, 3, 2 and 1-designs.

Case IV. Let $p=23$. Here we have a (48, 24) code.

It was shown, in part by computer, that $d=15$. Arguing as before, we need only determine linear combinations taken 4, 5, and 6 at a time by computer. Again we have (2) that the vectors of weights 15, 18, 21, 24, and 27 hold 5-designs; also 4, 3, 2 and 1-designs.

There is a (48, 24) quadratic residue code with the same d as C (23), (2), however, (2) the entire group of this quadratic residue code and also of its $5-15-48$ design (3) is $PSL_2(47)$, and since C (23) is invariant under $PSL_2(23)$ which is not contained in $PSL_2(47)$, this implies that the two codes are not equivalent and their two 5-designs are not equivalent.

Case V. Let $p=29$. Here we have a (60, 30) code.

It was shown, in part by computer, that $d=18$.

As before it can be argued that the only linear combinations to be determined on a computer are those taken 4, 5, 6, and 7 at a time.

By the Assmus-Mattson theorem again the vectors of weights 18, 21, 24, 27, 30, and 33 hold 5-designs; also 4 and lower designs. These are the first 5-designs found for these parameters.

It should be noted that a $t-r-24$ ($t'-r'-48$) design associated with C (11) (C (23)) has the same λ as the $t-r-24$ ($t'-r'-48$) design associated with the quadratic residue (24, 12) ((48, 24)) code. This is due to the fact that for these codes the Mac Williams formulas have a unique solution by the theorem in [6].

Note that the five codes above have $d=(p+7)/2$. This is just equal to the weight of linear combinations of the basis vectors taken 2 at a time. If all the codes of the family were to have this same property, then this would be the first constructive family of codes with k/n and d/n both bounded away from zero. Also the associated 5-designs would provide the first infinite family of 5-designs.

The computer calculations were shortened by the fact that the matrix S_p is invariant under the cyclic shift. I am very grateful to Mrs. Minja Choe for her expert programming. Her acute comments led to a reduction of the number of combinations needed.

I wish to acknowledge helpful discussions with Dr. E. F. Assmus, Jr., Professor A. M. Gleason, Dr. H. F. Mattson, Jr., Mr. John Pierce, and Dr. Richard Turyn.

Bibliography

1. E. F. Assmus and H. F. Mattson, Jr., *Disjoint Steiner systems associated with the Mathieu groups*, Bull. Amer. Math. Soc. **72** (1966), 843–845.

2. ———, *New 5-designs*, J. Combinatorial Theory 6 (1969), 122–151.

3. H. F. Mattson, Private communication.

4. M. Hall, Jr., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.

5. D. R. Hughes, *On t-designs and groups*, Amer. J. Math. **87** (1965), 761–778.

6. V. Pless, *Power moment identities on weight distributions in error correcting codes*, Information and Control 6 (1963), 147–152.

7. ———, *On the uniqueness of the Golay codes*, J. Combinatorial Theory 5 (1968), 215–228.

Air Force Cambridge Research Laboratories, L. G. Hanscom Field, Bedford, Massachusetts 01730