Internat. J. Math. & Math. Sci.
Vol. 5 No. 2 (1982) 403-406

RESEARCH NOTES

INFORMATION SETS AS PERMUTATION CYCLES FOR QUADRATIC RESIDUE CODES

RICHARD A. JENSON

Department of Mathematics, Boston College
Chestnut Hill, Massachusetts

(Received August 6, 1979 and in revised form October 20, 1980)

ABSTRACT. The two cases p = 7 and p = 23 are the only known cases where the automorphism group of the [p + 1, (p + 1)/2] extended binary quadratic residue code, Q(p), properly contains PSL(2,p). These codes have some of their information sets represented as permutation cycles from Aut(Q(p)). Analysis proves that all information sets of Q(7) are so represented but those of Q(23) are not.

KEY WORDS AND PHRASES. Binary code, Automorphism group of a code, Information set, Mathieu group of degree 24, Orbit.

1980 MATHEMATICS SUBJECT CLASSIFICATION CODES. 94B.

1. INTRODUCTION.

In an earlier article [1] it was noted that information sets of a binary extended quadratic residue code often appear as cycles of permutations from the automorphism group of the code. The present study of two important cases (p = 7 and p = 23) decides whether, for each code, every information set can be found as a cycle of a code preserving permutation. These results have immediate application in the area of decoding since several techniques of decoding depend for success on knowledge of a code's information sets. Our work suggests a technique, faster than an exhaustive search, for obtaining all information sets for the codes in question.

Let p be a prime with $p \equiv \pm 1 \pmod 8$. If Q and N signify the non zero quadratic residues and non-residues mod p, define polynomials in GF (2) [X] by

$$E_Q(x) = \sum_{r\in Q} x^r$$
$$E_N(x) = \sum_{n\in N} x^n \qquad \text{if } p \equiv -1 \pmod 8$$

and

$$E_Q(x) = 1 + \sum_{r\in Q} x^r$$
$$E_N(x) = 1 + \sum_{n\in N} x^n \qquad \text{if } p \equiv 1 \pmod 8$$

where E_Q and E_N are idempotents for codes of dimension $(p + 1)/2$ and length p over the binary field. These codes, when extended by adding an overall parity check, become the $[p + 1, (p + 1)/2]$ extended quadratic residue codes $Q(p)$ and $N(p)$ hereafter referred to as QR codes. See [2] - [6].

The coordinate places of QR codes have a standard label set $L = \{0, 1, 2, \ldots p - 1, \infty\}$. A subset M, of L, is called strictly dependent for Q(p) whenever the columns of a generator matrix for Q(p) indicated by M sum to the zero column. Recall that $c \in Q(p)^{\perp}$ iff the coordinates on which c is non zero form a strictly dependent subset of L. Remember too that $PSL(2,p) \leq Aut(Q(p))$ for all p under consideration and define any permutation on L from $Aut(Q(p))$ as a $(p + 1)/2$ element if it has two cycles each of length $(p + 1)/2$.

Q(7) is a self dual, doubly even (i.e., all codewords have weight $\equiv 0 \pmod 4$), [8,4] code with automorphism group of order 1344. There are fourteen codewords of weight four and one each of weights zero and eight.

Of the $\binom{8}{4} = 70$ four element subsets (4-sets) of $L = \{0, 1, \ldots 6, \infty\}$, the fourteen codewords of weight four specify the strictly dependent 4-sets of Q(7) $(=Q(7)^{\perp})$ so that 56 information sets remain. At most 42 of these information sets could be found as cycles of 4-elements from PSL(2,7). Indeed each 4-element of PSL(2,7) belongs to one of the 21 different conjugate cyclic subgroups (see [7]) of PSL(2,7). Each such subgroup splits L into two orbits (4-sets) which are either both information sets or both strictly dependent (see [1]). Even if each subgroup gave a unique splitting and each half of a splitting were an information set, at most 42 information sets would be accounted for.

Acting on all 70 4-sets with PSL(2,7) causes three orbits of 4-sets to arise. The CAMAC system indicates the fourteen strictly dependent 4-sets form one orbit and the 42 information sets which are cycles of 4-elements of PSL(2,p) form a second orbit. The third orbit consists of the 14 information sets remaining. Acting on all 70 4-sets with the full automorphism group of Q(7), all 56 information sets appear in one orbit, proving that each information set of Q(7) is expressed as a cycle of a 4-element from Aut (Q(7)).

Q(23) is the [24, 12] code known as the extended Golay code. Its full automorphism is the Mathieu group M(24) of order (24) (23) (22) (21) (20) (48). In spite of the size of Aut (Q(23)) we shall prove that some of the information sets of Q(23) are not expressed as cycles of 12-elements from Aut (Q(23)) (=M(24)).

The self dual code Q(23) has 759 codewords of weight 8 (called octads) and the same number of weight 16 codewords. Besides the single zero codevector and the all ones codeword, there are 2576 weight 12 codewords known as dodecads. Conway [8] supplies much of the background for the following argument.

The action of M(24) on the 12-sets of L partitions the collection of 12-sets into the 5 orbits named below:

U(12) - the 12-sets which are each a dodecad
S(12) - the 12-sets which each contain exactly 1 octad
S(12+) - the 12-sets which each contain exactly 3 octads
U(12-) - the 12-sets each of which differs from a dodecad in exactly one coordinate
T(12) - the 12-sets in none of the above orbits.

An information set of Q(23), say K, and its complement L-K both belong to the same orbit since $p \equiv -1 \pmod 8$. See [1]. Furthermore, M(24)'s character table ([9]) implies all 12-elements of M(24) are conjugate in M(24). The conclusion is that all information sets of Q(23) which are cycles of 12-elements from M(24) must belong to the same orbit.

The orbits S(12), S(12+), and U(12) consist of 12-sets which contain strictly dependent sets of Q(23). The weight distribution of Q(23) implies that these are the only ways a codeword from Q(23) may be obtained in a 12-set. So the

remaining two orbits, T(12) and U(12-), are seen to hold information sets of Q(23). And it becomes clear from the earlier conclusion that only one of these two orbits holds the Q(23) information sets which appear as cycles of 12-elements from M(24). The natural question is "Which orbit is this?"

The following argument shows why the information sets of U(12-) are not cycles of 12-elements from M(24). Suppose K is a 12-set of U(12-) and $u \in Q(23)$ is a dodecad having 11 ones on K and a single one on L-K. For the sake of contradiction, now suppose that there is some 12-element, say g, in M(24) having K and L-K as its two cycles. If that were the case, the vector u + g(u) would be a codeword of Q(23) of weight four--a clear impossibility. So our result is proved.

Thus T(12) must hold the information sets of Q(23) appearing as cycles of 12-elements from M(24).

ACKNOWLEDGMENTS. The author is grateful for the assistance of Vera Pless and for the use of the CAMAC system of computer programs as implements at the University of Illinois at Chicago Circle. Also the author appreciates the insightful short cut pointed out by J.M. Goethals.

REFERENCES

1. JENSON, R.A. A Double Circulant Presentation for Quadratic Residue Codes, IEEE Transactions Information Theory, IT-26, March 1980, 223-227.

2. ASSMUS, JR., E.F., and MATTSON, JR., H.F., New 5-Designs, Journal of Combinatorial Theory, 6 (1969), 122-151.

3. BERLEKAMP, E.R., Algebraic Coding Theory, McGraw Hill, New York, 1971.

4. MACWILLIAMS, F.J., and SLOANE, N.J.A., The Theory of Error Correcting Codes, North Holland, New York, 1977.

5. PETERSON, W.W., and WELDON, E.J., Error Correcting Codes, MIT Press, Cambridge, 1972.

6. VAN LINT, J.H., Coding Theory, Springer-Verlag, New York, 1973.

7. DICKSON, L.E., Linear Groups, Dover, New York, 1958.

8. CONWAY, J.H., Three Lectures on Exceptional Groups, Finite Simple Groups, Powell and Hisman eds., Academic Press, New York, 1971.

9. FROBENIUS, F.G., Uber die Charaktere der mehrfach transitiven Gruppen, Gesammelte Abhandlungen, Band III, J.-P. Serre ed., Springer-Verlag, New York, 1968, 335-348.