all i, if and only if, $(\tilde{v}_{12}\sigma^k, \tilde{v}_0\sigma^{r+i}) = (\tilde{v}_{12}\sigma^l, \tilde{v}_0\sigma^{s+i})$ for all i. Again we can deduce from Table II that the latter equality holds if and only if $l - k \equiv s - r \pmod{17}$.

To see that we do not need to consider U_1 with a W_2 whose (i, j) is equal to $(11, 13)$ note that

$$\begin{matrix} (0) & (v_9) & (v_0) & (v_{12}) \\ (v_9) & (0) & (v_{12}) & (v_0) \\ (0) & (\tilde{v}_9) & (\tilde{v}_{11}) & (\tilde{v}_{13}) \\ (\tilde{v}_9) & (0) & (\tilde{v}_{13}) & (\tilde{v}_{11}) \end{matrix}$$

is sent onto

$$\begin{matrix} (0) & (v_9) & (v_0) & (v_{12}) \\ (v_9) & (0) & (v_{12}) & (v_0) \\ (0) & (v_9) & (v_5) & (v_7) \\ (v_9) & (0) & (v_7) & (v_5) \end{matrix}$$

by $\bar{\rho}$ followed by $\bar{\tau} = (\tau, \tau, \tau, \tau)$. We de not need to consider a U_1 with a W_2 whose (i, j) is (13, 11) for similar reasons. The U_1 basis with $(i, j) = (2, 14)$ is equivalent under $\bar{\tau}$ to the U_2 basis with $(i, j) = (0, 12)$, so only one of these needs to be examined. Note that applying $\bar{\rho}$ to the U_2-basis followed by interchanging the last two blocks preserves the U_2-basis. Hence all $U_2 - W_2$-bases with $(i, j) = \{(0, 12), (7, 5), (4, 6), (13, 11)\}$ are equivalent. Similarly we need only consider a U_2-basis whose W_2-basis has an (i, j) equal to one of (12, 0), (5, 7), (6, 4), or (11, 13). A U_2-basis whose W_2-basis has $(i, j) = (1, 3)$ is equivalent to one whose $(i, j) = (8, 10)$, and one with $(i, j) = (3, 1)$ is equivalent to one with $(i, j) = (10, 8)$. Q.E.D.

We generated, on a computer, the bases described in Theorem 1 and computed linear combinations of vectors until we located a vector of weight 12. The program was set to stop on finding a vector of weight 12 or less, but no vectors of weight lower than 12 were found. Since we have so many bases to examine and since a (72, 36) code has 2^{36} vectors in it, we had to choose judicious linear combinations in order to terminate in a reasonable amount of time. For this reason every time we computed a basis as described in Theorem 1, we chose another basis of the same space which was better for reducing the number of linear combinations necessary to find a low weight vector. We generated all the bases according to the form given in Theorem 1; namely, we first chose a basis of U_1 or U_2 and then added a basis of W_2 for the necessary pairs (i, j). For each pair (i, j) we computed the 17^3 bases given by the choices of k, l, and r with s being determined by the equation $k + s = r + l$. For each such basis, we computed another basis, referred to as the test basis, of the following form:

C_1	C_2	C_3	C_4	69	70	71	72
$\{I\}$	$\{0\}$	$\{X\}$	$\{Y\}$	1	0	0	0
$\{0\}$	$\{I\}$	$\{W\}$	$\{Z\}$	0	1	0	0
h	h	0	h	0	0	1	0
h	h	h	0	0	0	0	1

.

The braces denote a 17×17 circulant with I being the identity matrix. The test basis is equivalent to the matrix constructed as follows. The first 17 rows of this matrix are linear combinations of the second portions of the U_1 or U_2 basis with the second portion of the W_2 basis and one of the vectors from the basis of D. The second 17 rows are analogously constructed from the first portion of the U_1 or U_2 bases with the first portion of the W_2 basis and another vector from the basis of D. With the test basis we first checked for vectors which have weight zero on the first block and weights 1, 2, 3, 4, 5 on the second block and have total weight 12 or less. We needed to test for only one vector of this type in a shift class of the second block. Whenever we found a low weight vector with weight zero on the first block, then we did not need to check those bases with the same U_1 or U_2 basis, the same (i, j) and the same (k, l) as this low weight vector will be in the spaces generated by all such bases. This cuts down on a considerable amount of checking. If no vectors of low weight were found with zero on the first block, we checked for vectors of weight one on the first block and weights 0 through 4 on the second block, then weight 2 on the first block and weights 0 through 4 on the second block. In the situation where the weight on the first block is not zero, we consider one vector in each shift class in the first block. Although this way of taking linear combinations is not exhaustive, the time for an exhaustive search would have been prohibitive and indeed it was unnecessary, we always found a weight 12 vector. This demonstrates the next theorem.

Theorem 2: If C is a doubly even (72, 36, 16) code, then there is no element of order 17 in $G(C)$.

ACKNOWLEDGMENT

We want to thank Thom Grace for much programming help and ingenuity. In addition to constructing the very efficient programs, which were necessary to be able to handle our large number of bases, he noted that we did not need to consider several bases whenever we had located a low weight vector with weight zero on the first block. The CAMAC system at the University of Illinois at Chicago Circle Computing Center was used to compute orbits of vectors under a group.

REFERENCES

[1] R. P. Anstee, M. Hall, Jr., and J. G. Thompson, "Planes of order 10 do not have a collineation of order 5," *J. Combinatorial Theory*, series A-29, 39–58, 1980.

[2] E. F. Assmus, Jr., and H. F. Mattson, Jr., "New 5-designs," *J. Combinatorial Theory*, vol. 6, pp. 122–151, March 1969.

[3] J. H. Conway and V. Pless, "On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code," to appear in *Discrete Math*.

[4] W. Feit, "A self-dual even (96, 48, 16) code," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 136–138, 1974.

[5] A. M. Gleason, "Weight polynomials of self-dual codes and the MacWilliams identities, *Act. Congr. Int. Math.*, vol. 3, pp. 211–215, 1970. (Paris: Gauthier-Villiars, 1971.)

[6] C. Hering, "On codes and projective designs," Kyoto University Mathematics Research Institute Seminar Notes, 344, Feb. 1979.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: Elsevier/North Holland, 1977.

[8] V. Pless, "23 does not divide the order of the group of a (72, 36, 16) doubly even code," preprint.

[9] N. J. A. Sloane, "Is there a (72, 36) $d = 16$ self-dual code?," *IEEE Trans. Inform. Theory*, vol. IT-19, p. 251, 1973.

Minimal Permutation Sets for Decoding the Binary Golay Codes

DANIEL M. GORDON

***Abstract*—For permutation decoding of an e error-correcting linear code, a set of permutations which move all error vectors of weight $\leq e$ out of the information places is needed. A method of finding minimal decoding sets is given, along with minimal sets obtained with this method for the binary Golay codes.**

Manuscript received April 7, 1981; revised June 1981. This work was supported in part under a Richter Grant.

The author is with the California Institute of Technology, Pasadena, CA 91126.

0018-9448/82/0500-0541$00.75

I. Introduction

Let $\boldsymbol{C}$ be an $[n, k, d]$ binary code with a parity check matrix of the form $H = [I \mid A]$. In [1, p. 513] it is shown that for a received vector $\boldsymbol{y} = y_0 \cdots y_{n-1}$ with an error vector $\boldsymbol{e}$ of weight $\leq t$, where $2t + 1 \leq d$, the syndrome $S = Hy^T$ has weight t, if and only if the information symbols $y_r \cdots y_{n-1}$, $r = n - k$, are correct. In this case, the nonzero digits of the syndrome correspond to those of the error vector.

This theorem is the basis for the method of permutation decoding as introduced by MacWilliams. For any permutation $\boldsymbol{a}$ in the automorphism group of $\boldsymbol{C}$, if $S^a = H(\boldsymbol{ay})^T$ has weight $\leq t$, then $\boldsymbol{y}$ may be decoded as $\boldsymbol{c} = \boldsymbol{a}^{-1}(\boldsymbol{y} + S_0^a \cdots S_{r-1}^a 0 \cdots 0)$. All that is needed is a set of permutations from the automorphism group which move the nonzero digits of every possible error vector out of the information places into the check digits $y_0 \cdots y_{r-1}$. For convenience a minimal set is desired, but few such sets were known for multierror-correcting codes.

The method described below, which is applicable to any code with a sufficiently large and well-understood automorphism group, is demonstrated by applying it to the codes $\boldsymbol{G}_{23}$ and $\boldsymbol{G}_{24}$.

II. Coverings

It is inconvenient to deal with permutations at first; therefore, we look at the unordered r-tuple on n numbers representing the inverse image of the first r digits under a permutation (i.e., the bits moved by a permutation out of the information digits). Consider the set of r-tuples obtained from a decoding set of permutations. Since each error vector is brought by at least one permutation into the check digits, and each error vector decodable by the Golay codes can be represented by a 1-, 2-, or 3-tuple, every 3-tuple must occur in at least one r-tuple. The set of r-tuples is said to *cover* all 3-tuples.

$N(t, k, v)$ is defined to be the minimal number of k-tuples needed to cover all t-tuples on v digits. If we find $N(e, r, n)$, then we have a lower bound on the order of a minimal set of permutations. This is only a bound, since there may not be any permutation in the automorphism group corresponding to a given r-tuple.

The following theorem is a well-known basic result for coverings, given for example in [2].

Theorem: $N(t, k, v) \geq (v/k) \cdot N(t-1, k-1, v-1)$.

Proof: The total number of digits in the set is $k \cdot N(t, k, v)$. Each digit must appear at least once with every $(t-1)$-tuple; namely, $N(t-1, k-1, v-1)$ times. Since there are v digits, the above bound holds.

Since $N(1, k, v) = \lceil v/k \rceil$, the theorem shows

$$N(t, k, v) \geq \left\lceil \frac{v}{k} \left\lceil \frac{v-1}{k-1} \cdots \left\lceil \frac{v-t+1}{k-t+1} \right\rceil \cdots \right\rceil \right\rceil.$$

For the Golay codes this yields

$$N(3, 11, 23) \geq 15$$

$$N(3, 12, 24) \geq 14.$$

These bounds are, in this case, tight. This can be seen for $N(3, 12, 24)$ by taking the Steiner system $S(3, 4, 8)$, which has fourteen blocks, and identifying each of its eight symbols with three of the numbers $0, 1, \cdots, 23$ to obtain a covering of the desired type. For $N(3, 11, 23)$ no such shortcut was available, but a computer-aided search resulted in a covering set of fifteen 11-tuples.

III. Orbits and Permutations

The automorphism groups of $\boldsymbol{G}_{23}$ and $\boldsymbol{G}_{24}$ are M_{23} and M_{24}, respectively. An r-tuple corresponds to a permutation in the automorphism group, if and only if it is in the same orbit as the r-tuple corresponding to the identity permutation, namely, $0, 1, \cdots, 10$ for $\boldsymbol{G}_{23}$, and $\infty, 0, \cdots, 10$ for $\boldsymbol{G}_{24}$. Conway, in [3], describes the orbits of M_{24}. The desired one is T_{12}, all 12-tuples distance four from a codeword of weight twelve containing no codewords of weight eight.

To find a covering set with all blocks in T_{12}, a computer program tried random permutations on the original covering set, checking if the permuted set (which clearly still covers all 3-tuples) was satisfactory. The number of trials that would be needed can be estimated by assuming that the permuted blocks are randomly distributed. This is false, but a reasonable approximation. The chance of any block being in T_{12} is $|T_{12}| / \binom{24}{12}$ equals 0.377. Since seven of the blocks of the covering set are complements of the other seven, and the complement of a 12-tuple in T_{12} is another element of T_{12}, it was only necessary to check half of the blocks. More time was saved by making the first block the identity 12-tuple, and choosing the permutations to fix it setwise. The expected number of trials was then $(1/0.377)^6 = 346$. Only 22 were actually needed.

The corresponding orbit in M_{23} is T_{11}, which consists of 11-tuples distance three from a weight twelve codeword containing no weight seven codewords. The chance of a random 11-tuple being in T_{11} is also 0.377, so the expected number of trials was $(1/0.377)^{14} = 842\,252$. It took approximately 360 000 trials.

Once these single-orbit sets had been found, it was shown that minimal sets exist of order 15 for $\boldsymbol{G}_{23}$ and 14 for $\boldsymbol{G}_{24}$. All that remained was to actually find them. This was done by collecting a generating set of permutations from each automorphism group which moved as few elements as possible between the check and information digits: the involutions. The computer program took each r-tuple and went through the permutations, applying the one which took the most digits of the r-tuple into the check digits. This was continued until all the digits were in the check places. The permutations used were composed, forming the permutation corresponding to the r-tuple. The permutations so obtained, along with the covering sets, are listed in Tables I and II.

TABLE I
Coverings and Permutations for G_{23}

0	1	2	3	4	5	6	7	8	9	10
1	3	6	11	12	16	17	18	19	20	21
1	2	3	6	10	11	13	14	15	21	22
0	1	5	7	9	11	12	13	14	16	19
0	1	5	7	9	15	17	18	20	21	22
1	2	4	8	10	11	12	15	16	19	22
1	2	4	8	10	13	14	17	18	20	21
0	6	8	9	10	12	14	15	16	17	20
2	4	5	6	7	12	13	16	17	20	22
0	2	3	4	9	12	14	16	18	21	22
0	2	3	4	9	11	13	15	17	19	20
3	5	7	8	10	12	13	15	16	18	21
3	5	7	8	10	11	14	17	19	20	22
2	4	5	6	7	11	14	15	18	19	21
0	6	8	9	10	11	13	18	19	21	22

e

(0 21 9 18 4 19 6 3)(2 20 7 14 16 10 15 11)(5 17 8 12)(13 22)
(0 14 9 19 18 21 5 11 8 17 12 22 4 20 15 7 16 13 2 10 1 3)
(0 8 11 5 1)(2 22 20 21 15 18 16 10 13 4 12 3 14 9 7)(6 17 19)
(0 7 8 22 10 14 15 1 2 11 16 12 18 6 17)(3 13 19 21 5)(4 20 9)
(0 12 7 18 21 15 3 20 13 17 16)(1 9 19 5 22 4 6 14 11 10 2)
(0 21 9 11 20 6 16 18 2 1 4)(3 13 10 8 5 17 7 19 15 22 14)
(0 7 20 4 13 17 5 19 15 3 14)(1 18 22 12 2 11 16 9 10 8 6)
(0 13 1 18 14 20 9 12 4 5 6)(2 7 8 15 11 16 10 17 3 19 22)
(0 7 22)(1 20 13 11 19 18)(2 9)(4 6 14)(5 12)(8 17 15 21 10 16)
(0 9 1 17 5 15)(2 4 7 21 11 3)(6 20)(8 14 13)(10 12 19)(16 22)
(0 18 7 10 8 2 21 5 9 15 4 16 6 11 14 20 17 19 22 13 1 12 3)
(0 14 1 22 6 17)(2 19)(3 8 10)(4 18 11)(5 9 12 16 15 20)(13 21)
(0 11 2 7 5 4 9 22 13 17 16 18 10 14)(1 12 20 15 8 19 6)(3 21)
(1 17 16 21 8)(2 22 4 19 6)(3 14 12 11 10)(5 18 7 15 13)

TABLE II
COVERINGS AND PERMUTATIONS FOR G_{24}

∞	0	1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20	21	22
2	3	4	7	8	10	11	12	13	17	18	19
∞	0	1	5	6	9	14	15	16	20	21	22
∞	0	1	5	6	9	11	12	13	17	18	19
2	3	4	7	8	10	14	15	16	20	21	22
∞	0	1	7	8	10	14	15	16	17	18	19
2	3	4	5	6	9	11	12	13	20	21	22
∞	0	1	2	3	4	11	12	13	14	15	16
5	6	7	8	9	10	11	12	13	14	15	16
∞	0	1	7	8	10	11	12	13	20	21	22
2	3	4	5	6	9	14	15	16	17	18	19
∞	0	1	2	3	4	17	18	19	20	21	22
5	6	7	8	9	10	17	18	19	20	21	22

e

(0 14)(1 11)(2 19)(3 17)(4 16)(5 15)(6 12)(7 18)(8 20)(9 21)(10 13)(22 ∞)
(0 16 20 13 7 4 8)(1 22 11 9 18 ∞ 21 12 6 17 5 15 14 19)(2 10)
(0 4 15 3 14 1 9)(2 17 21 6 10 11 22)(5 8 18 20 7 16 ∞)
(2 20 16 21 13 6 4 12)(3 19 5 8 15 14 18 9)(7 17)(10 22 11 ∞)
(0 11 16 6 18 19 20 9 13 22 5 17 12 14 10 8 2 7 1 21 ∞ 15 4)
(0 6 20 14 8 9 13 11 17 2 19)(1 5 21 12 16 3 15 ∞ 4 18 10)
(0 20 4 7 12 5 6)(1 15 16 17 18 21 3)(2 10 22 ∞ 13 8 11)
(0 6 16 1 9 17 19 11 8 22 14 ∞ 5 15 2)(4 10 20 21 12)(7 18 13)
(0 16 4 20 19 17 18 15 3 22 11 9)(1 14 10 ∞ 21 12 6 7 8 5 2 13)
(0 5 11 2 21 3 12)(1 8 10 6 18 22 9 13 4 14 15 20 7 ∞)(16 17)
(0 15 1 12 20 19 3 9 2 10 18 ∞ 21 17)(4 8 16 6 7 11 14)(13 22)
(0 4 5 11 15 13 19)(1 7 22 2 3 8 20)(6 14 18 9 17 10 21)
(0 13 18 1 21 7 6 ∞ 11 16 15 17 8 4 12 20 9 3 19 10 2 14 22)

REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland Publishing, 1977, pp. 512–514.

[2] A. E. Brouwer, "Packing and covering of $\binom{k}{t}$-sets," in *Packing and Covering in Combinatorics*, A. Schrijver, Ed. Amsterdam: Mathematical Centre Tracts, 1979, pp. 89–97.

[3] J. H. Conway, "Three lectures on exceptional groups," in *Finite Simple Groups*, M. B. Powell and G. Higman, Eds. New York: Academic, 1971, pp. 223, 235.

[4] F. J. MacWilliams, "Permutation Decoding of Systematic Codes," *Bell Syst. Tech. J.*, vol. 43, 485–505, 1964.

The Merit Factor of Long Low Autocorrelation Binary Sequences

MARCEL J. E. GOLAY

Abstract—**The asymptotic "merit factor," i.e, the ratio of central to sidelobe energy of extremely long, optimally low autocorrelation sequences, formerly calculated as $2e^2 = 14.778 \cdots$ with the use of an ergodicity hypothesis and a convenient, but faulty, approximation, is recalculated without that approximation and is established at 12.32 $\cdots$.**

INTRODUCTION

Several communication engineering problems have led to a mathematical effort seemingly out of proportion to the scope of their originally intended applications. One of these, concerning coding theory, has been associated with a rebirth of activity in group and combinatorial theory. Another problem, one concerning secure communication, namely the replacement of a single radar pulse by a binary sequence of pulses in phase or 180° out-of-phase with each other for the sake of peak power reduction, has led to the mathematical problem of devising binary sequences of $+1$'s and -1's having minimal autocorrelations. This latter problem has usually been considered from the standpoint of finding sequences whose autocorrelations do not exceed a certain number [1]–[4]. It has also been considered from the standpoint of finding, for any given number N of elements, the one or the few general or skewsymmetric sequences with the highest ratio of N^2 over twice the sum of the squares of the $N-1$ off-peak autocorrelations of the sequence [4], [5]. This ratio, which has been termed the "merit factor" or "F" of a binary sequence, is used for certain purposes as the criterion of "goodness" for sequences. This criterion has one drawback and two advantages. The drawback is that, when making a computer search for optimally low autocorrelation sequences, one may not, as one can do in a search for sequences having no autocorrelations exceeding a given maximal value, discontinue the search as soon as that value is found to be exceeded by a single autocorrelation of the particular sequence being tried, and then proceed to another sequence: a few occasional high autocorrelation values may be compensated by the low values of all others, and the examination of the particular sequence tried must be continued somewhat further.

On the other hand, the merit factor has the engineering advantage that it is closely connected with the signal to self-generated noise ratio of a communication or radar system in which coded pulses are transmitted and received. And it has the further mathematical advantage of lending itself to the analytical manipulations which follow wherein what was termed in the original publication [5] the "postulate of mathematical ergodicity" is invoked again to show, without the need for the approximation previously resorted to, that this optimal merit factor approaches the value 12.32 $\cdots$ as N increases without bound.

Manuscript received February 13, 1978; revised February 25, 1981.
The author is with the Perkin-Elmer Corporation, Norwalk, CT.

0018-9448/82/0500-0543$00.75