View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

JOURNAL OF COMBINATORIAL THEORY 11, 178–186 (1971)

# On the Golay Perfect Binary Code

J.-M. GOETHALS

*MBLE Research Laboratory, Ave. Van Becelaere, 2, B 1170, Brussels, Belgium*

*Communicated by N. G. de Bruijn*

Received June 20, 1969

Some combinatorial properties of the Golay binary code are emphasized and used for two main purposes. First, a new nonlinear code having 256 code words of length 16 at mutual distance 6 is exhibited. Second, a majority decoding method, quite similar to Massey's threshold decoding, is devised for the Golay code and various related codes.

## 1. INTRODUCTION

Assmus and Mattson [1–4] recently pointed out connections between perfect codes and some tactical configurations. Among known perfect codes, the two Golay codes [10, 19] are of special interest, at least for two reasons. First, they constitute the only known examples of perfect $e$-error-correcting-codes, $e \neq 1$, except for the trivial example of repetition codes. Second, their automorphism groups are strongly related with the Mathieu groups [23]. These connections, first pointed out by Paige [16], were recently set up by Assmus and Mattson [3]. Recently discovered graphs [9] and simple groups [8, 11] are connected with the extended Golay (24, 12) binary code. The combinatorial properties of this latter code will be emphasized and used here for two main purposes:

(1) It will be shown to contain a non-linear code of length 16, having 256 code vectors at mutual distance at least 6. The weight distribution of this code is derived and is shown to be translation-invariant, hence giving the distance properties. Dropping one digit, a code equivalent to the Nordstrom-Robinson optimum code [15], analyzed by Robinson [22], is easily obtained. The distance structure of this code was studied by Preparata [20], who recently proved [21] the converse of our statement, that is that the Golay code is an extension of the Nordstrom-Robinson non-linear code.

(2) A majority step-by-step decoding method, quite similar to Massey's threshold decoding [14], will be devised. It applies to several codes derived from the extended Golay (24, 12) code.

## 2. The Tactical Configurations of the (24, 12) Code

A *tactical configuration* ($\lambda$; $t$, $d$, $n$), or a *t-design*, [4, 12], is a collection of subsets, or blocks, each of cardinality $d$, of a set $S$ of cardinality $n$, such that every subset of $S$ of cardinality $t$ is contained is exactly $\lambda$ distinct blocks. A (1; t, $d$, $n$) configuration is a *Steiner system.*

The weight distribution of the Golay code is well known [13, 18]. From this weight distribution, one easily deduces [17, p. 70] that the extended (24, 12) code exactly contains

759 vectors of weight 8,<br>
2576 vectors of weight 12,<br>
759 vectors of weight 16,<br>
1 vector of weight 24.

Each of these collections of vectors forms a 5-design. The (24, 12) code thus contains 3 non-trivial designs, namely

$$(1;\ 5,\ 8,\ 24), \tag{1}$$
$$(48;\ 5,\ 12,\ 24), \tag{2}$$
$$(78;\ 5,\ 16,\ 24), \tag{3}$$

the first of which is the well-known Steiner system having the Mathieu group $M_{24}$ as automorphism group [23]. The code (24, 12] itself and thus also each of the above designs has $M_{24}$ as automorphism group [3]. Note that (1) and (3) are complementary, while (2) is self-complementary.

A number of Balanced Incomplete Block Designs (BIBD) can be derived from these designs. A first series is given in Table I, where $v$, $k$, $b$, $r$ are the classic parameters, and $\lambda_i$ is the number of times each $i$-tuple appears in the design. Design number 1 is the Steiner (5, 8, 24) system, of which number 2 and 3 are the residual designs on 23 points; again, number 4 and 5 are residuals of number 2 on 22 points, etc. Higman and Sims [11] recently exhibited a simple group of degree 100, where the design number 4 plays a central role. The symmetric design number 7 is, of course, the projective plane of order 4. We emphasize that two other series of BIBD on 21 22, and 23 points could be obtained in a similar way from the two other 5-designs. Further details are given in [9].

TABLE I

Some BIBD Derived from the (5, 8, 24) Steiner System

| No. | $v$ | $k$ | $b$ | $r$ | $\lambda_2$ | $\lambda_3$ | $\lambda_4$ | $\lambda_5$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 24 | 8 | 759 | 253 | 77 | 21 | 5 | 1 |
| 2 | 23 | 7 | 253 | 77 | 21 | 5 | 1 | |
| 3 | 23 | 8 | 506 | 176 | 56 | 16 | 4 | |
| 4 | 22 | 6 | 77 | 21 | 5 | 1 | | |
| 5 | 22 | 7 | 176 | 56 | 16 | 4 | | |
| 6 | 22 | 8 | 330 | 120 | 40 | 12 | | |
| 7 | 21 | 5 | 21 | 5 | 1 | | | |
| 8 | 21 | 6 | 56 | 16 | 4 | | | |
| 9 | 21 | 7 | 120 | 40 | 12 | | | |
| 10 | 21 | 8 | 210 | 80 | 28 | | | |

## 3. Some Subcodes of the (24, 12) Code

We first prove two lemmas which will be useful later :

Lemma 1. *Let $A$ be a linear code $(n, k, d)$, that is of length $n$, dimension $k$, and minimum distance $d$, and let its dual code have minimum weight $w$. Then $A$ contains a proper subcode of length $n - w$, dimension $k + 1 - w$, and minimum distance at least $d$.*

*Proof.* Since the dual code has minimum weight $w$, every set of $w - 1$ coordinate functions is linearly independent, while at least one set of $w$ coordinates is dependent. Hence the subcode of $A$, all of whose vectors have zero as coordinate in these $w$ positions, has simension $k - (w - 1) = k + 1 - w$. Since it is a subcode of $A$, its minimum distance is at least $d$.

Lemma 2. *Let $A$ be a linear binary code $(n, k, d)$, whose dual code has minimum weight $w$; and let there exist $N$ binary vectors of length $w$ and even weight whose mutual distance does not exceed $d'$. Then, there exists a set of $N \cdot 2^{k+1-w}$ vectors of length $n - w$, whose mutual distance is at least $d - d'$.*

*Proof.* According to the preceding lemma, $A$ contains a linear code $B$ of dimension $k + 1 - w$, effective length $n - w$, and minimum distance at least $d$. The code $A$ is partitionned into $2^{w-1}$ cosets, with respect to the subcode $B$, each coset being a "translation" of the code $B$, entirely characterized by a given fixed vector of length $w$ (necessarily of even weight), in the $w$ coordinate positions where $B$ is zero. Dropping these $w$ positions, one obtains $2^{w-1}$ non-linear codes, with the same distance properties as $B$.

Let us denote these coset codes by $B_0$, $B_1$, $B_2$,..., and the corresponding vectors of length $w$, by $v_0$, $v_1$, $v_2$,... . We emphasize that two vectors, of length $n - w$, in the same $B_i$ are at least distance $d$ apart, while two vectors belonging to distinct coset codes $B_i$, $B_j$, have mutual distance at least $d - d'$, if $d'$ is the mutual distance of the corresponding $v_i$, $v_j$. Now, the announced result easily follows by taking the union of the $N$ coset codes $B_i$ whose corresponding $v_i$ have mutual distance not exceeding $d'$.

REMARK. The code obtained in Lemma 2 is, in general, non-linear. It is linear if and only if the $N$ vectors $v_i$ of length $w$ form a linear space. It is well known that the binary (24, 12) code is self-dual [19], which implies that each vector of the code intersects the other vectors in an even number of points. Applying Lemma 1, one deduces that $A(24, 12, 8)$ contains a linear subcode $B(16, 5, 8)$, that is of minimum distance at least 8. This minimum distance is exactly 8, since, from the properties of the Steiner (5, 8, 24) system, (design 1, Table I), one deduces [9 Lemma 5.1] that each octuple intersects 280 octuples in 4 points, 448 octuples in 2 points, and 30 octuples in no point. These last 30 vectors of weight 8 thus belong to $B(16, 5, 8)$, which in addition contains one vector of weight 16 and the null-vector. From the properties of the automorphism group [5, Problem 15.3], this code is easily shown to be equivalent to the first-order Reed-Muller code of length 16. From an analysis of the above-mentioned 5-designs (1), (2), (3), it can be shown that the weight distribution in the coset codes $B_i$ is as in Table II, where coset weight means the weight of the vector $v_i$ of length 8 associated with the coset code $B_i$, as defined in Lemma 2.

TABLE II

Weight Distributions in Coset Codes of the (24, 12) Code

| | Weight distribution | | | | | | |
|---|---|---|---|---|---|---|---|
| Coset weight | 0 | 4 | 6 | 8 | 10 | 12 | 16 |
| 0 and 8 | 1 | — | — | 30 | — | — | 1 |
| 2 and 6 | — | — | 16 | — | 16 | — | — |
| 4 | — | 4 | — | 24 | — | 4 | — |

THEOREM 3. *The extended Golay code contains a non-linear code* (16, 8, 6), *that is, containing* $2^8 = 256$ *vectors of length* 16 *at mutual distance at least* 6.

*Proof.* Consider the following eight vectors of length 8: the null-vector and seven vectors, each of weight 2, having a given non-zero coordinate in common. These eight vectors of even weight are at a mutual distance exactly equal to 2. Hence, applying Lemma 2 to the self-dual (24, 12, 8) code, one obtains the announced result.

THEOREM 4. (i) *The above-defined non-linear code has the weight distribution given in Table III.*

(ii) *This weight distribution is invariant under any translation which brings a non-zero vector of the code to the all-zero vector. Thus, the weight distribution of the code gives the distance properties.*

TABLE III

Weight Distribution of the Non-linear (16, 8) Code

| 0 | 6 | 8 | 10 | 16 |
|---|---|---|---|---|
| 1 | 112 | 30 | 112 | 1 |

*Proof.* (i) The weight distribution is easily deduced from Table II, since our non-linear code was defined as the union of one coset code of coset weight 0 and seven coset codes of coset weight 2.

(ii) From the way the coset codes were chosen, it is clear that any translation which brings a non-zero vector to the null-vector will result in a new set of coset codes of respective weights 0 (1 time) and 2 (7 times). The announced result easily follows.

REMARKS. According to Calabi and Myrvaagnes [6], a linear code (16, 8, 6) cannot exist. The preceding discussion shows that such a non-linear code exists. By dropping one digit, one obtains a (15, 8, 5) non-linear code, which is equivalent to the Nordstrom-Robinson code [15], of which a decoding method has been devised [22]. It is interesting to note that our non-linear code (16, 8, 6) has a triply transitive automorphism group, hence implying the existence of the 3-designs (4; 3, 6, 16), (3; 3, 8, 16), and (24; 3, 10, 16). This group has order

$$| M_{24} |/24.23.11 = 16.15.14.12 \qquad (4)$$

and is (16, 1) isomorphic with $A_7$, the alternating group on 7 letters [7]. If $A$ is a linear code $(n, k)$ over GF(2) and $B$ its dual code, and if $A_i$, $B_i$

denote the number of vectors of weight $i$ in $A$, $B$ respectively, one has, according to MacWilliam's relations [13],

$$\sum_{i=0}^{n-r} \binom{n-i}{r} A_i = 2^{n-k} \sum_{j=0}^{r} \binom{n-j}{n-r} B_j . \tag{5}$$

It is quite surprising that the weight distribution (Table III) of our nonlinear code (16, 8) satisfies (5) with $A_i = B_i$, just as a self-dual linear code.

## 4. Majority Decoding of the Golay Code

As recalled above, the (24, 12) code is self-dual. Any set of vectors of the code can thus be chosen as parity checks for the code itself. Let us take as parity checks the 253 vectors of weight 8 passing through a given point (see design 1, Table I), These 253 vectors, except for the fixed coordinate, together form the $b$ rows of design 2. From the properties of the configuration, one easily deduces that, when one error occurs, the number of parity check failures will be 253 or 77, according as the fixed digit is in error or not. On the other hand, if two errors occur, the number of parity check failures will be $253 - 77 = 176$ in the first case, and $2(77 - 21) = 112$ in the second case, as the two columns involved in the latter case contain 21 times (1, 1), and (77 − 21) times (1, 0) and (0, 1) as rows. Finally, in case of 3 errors, there will be $253 - 112 = 141$ parity check failures in the first case, and

$$1 \times 5 + 3(77 - 2 \times 21 + 1 \times 5) = 125$$

in the second case. For the same reasoning as above shows that, in the latter case, the odd weight patterns appearing in the 3 involved columns are: (1, 1, 1) appearing 5 times and each 1-tuple of type (1, 0, 0) appearing

$$77 - 2 \times 21 + 1 \times 5 = 40$$

times.

Putting these numbers in a table (Table IV), one easily sees that whether or not the fixed digit was in error can be decided by a majority vote on the parity checks provided not more than 3 errors occurred. This procedure is quite similar to Massey's threshold decoding, based on "orthogonal checks sets" [14].

The (23, 12) code is obtained from the preceding one by dropping one digit, while its dual code (23, 11) is the subcode of (24, 12) all of whose vectors have zero in the above dropped position. This last code contains design 3 of Table I. Let us take as parity checks for the code (23, 12) the 176 vectors of weight 8 passing through a given point. With the same reasoning as above, the number of parity check failures is easily obtained (Table V). Again, it can be decided by a majority vote whether or not the fixed digit was in error, provided not more than 3 errors occurred.

TABLE IV

Number of Parity Check Failures; Code (24, 12)

| | Fixed digit | |
|---|---|---|
| Number of errors | in error | not in error |
| 1 | 253 | 77 |
| 2 | 176 | 112 |
| 3 | 141 | 125 |

TABLE V

Number of Parity Check Failures; Code (23, 12)

| | Fixed digit | |
|---|---|---|
| Number of errors | in error | not in error |
| 1 | 176 | 56 |
| 2 | 120 | 80 |
| 3 | 96 | 88 |

Since the automorphism groups of these codes are (multiply) transitive, such majority decisions can be done for each digit, resulting in a step-by-step decoding.

A number of related codes can be decoded in the same way. Some of them are given below, with the number of the BIBD of Table I which can be taken as parity check set.

(23, 11, 8) : design 2; up to 3 errors,
(22, 12, 6) : design 6; up to 2 errors,
(22, 11, 6) : design 4; up to 2 errors.

This last code is self-dual and consists of those vectors of (24, 12, 8) which have either two zeros, or two ones in two given positions.

## 5. Conclusion

Our investigation of the combinatorial properties of the Golay code led to two interesting results, the second of which could have some practical significance.

The method used here to prove the existence of our non-linear (16, 8, 6) code could be used to find some other "good" non-linear codes and thus have more significance than the result itself. Nevertherless, the exhibited combinatorial properties of this non-linear code could suggest simpler decoding methods than the one proposed by Robinson [22].

The majority decoding of the Golay code, as devised here, could be of great practical interest, since the previously known decoding methods for the Golay code either do not use the full error-correcting ability of the code, or are not easy to implement. Implementation of our method, being quite similar to Massey's threshold decoding, has not been discussed.

## References

1. E. F. Assmus, Jr., and H. F. Mattson, Steiner systems and perfect codes, University of North Carolina, Institute of Statistics Mimeo Series No. 484.1, 1966.
2. E. F. Assmus, Jr. and H. F. Mattson, Disjoint systems associated with the Mathieu groups, *Bull. Amer. Math. Soc.* **72** (1966), 843–845.
3. E. F. Assmus, Jr. and H. F. Mattson, Perfect codes and the Mathieu groups, *Arch. Math. (Basel)* **17** (1966), 121–135.
4. E. F. Assmus, Jr. and H. F. Mattson, On tactical configurations and error-correcting codes, *J. Combinatorial Theory* **2** (1967), 243–257.
5. E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill, New York, 1968.
6. L. Calabi and E. Myrvaagnes, On the minimal weight of binary group codes, *IEEE Trans. Information Theory* **IT-10** (1964), 385–387.
7. R. D. Carmichael, "Introduction to the Theory of Groups of Finite Order," Ginn, Boston, 1937; reprinted by Dover, New York, 1956.
8. J. H. Conway, A perfect group of order 8,315,553,613,086,720,000 and the sporadic simple groups, *Proc. Nat. Acad. Sci. U.S.A.* **61** (1968), 398–400.
9. J. M. Goethals and J. J. Seidel, Strongly regular graphs derived from combinatorial designs, *Canad. J. Math.* **22** (1970), 597–614.
10. M. Golay, Notes on digital coding, *Proc. I.R.E.* **37** (1949), 637.
11. D. G. Higman and C. C. Sims, A simple group of order 44,353,000, *Math. Z.* **105** (1968), 110–113.
12. D. R. Hughes, On *t*-designs and groups, *Amer. J. Math.* **87** (1965), 761–778.
13. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell. System Tech. J.* **42** (1963), 79–94.
14. J. L. Massey, "Threshold Decoding," M.I.T. Press, Cambridge, Mass., 1963.
15. A. W. Nordstrom and J. P. Robinson, An optimum nonlinear code, *Information and Control* **11** (1967), 613–616.
16. L. J. Paige, A note on the Mathieu groups, *Canad. J. Math.* **9** (1957), 15–18.

17. W. W. Peterson, "Error-Correcting Codes," M.I.T. Press, Cambridge, Mass., 1961.

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

19. V. Pless, On the uniqueness of the Golay codes, *J. Combinatorial Theory* **5** (1968), 215–228.

20. F. P. Preparata, Weight and distance structure of Nordstrom-Robinson quadratic code, *Information and Control* **12** (1968), 466–473.

21. F. P. Preparata, A new look at the Golay (23, 12) code, *IEEE Trans. Information Theory* **IT-16** (1970), 510–511.

22. J. P. Robinson, Analysis of Nordstrom's optimum quadratic code, *Proc. Hawaii Intern. Conf. System Sciences* (1968), 157–161.

23. E. Witt, Die 5-fach transitive Gruppen von Mathieu, über Steinersche Systeme, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 256–264, 265–275.