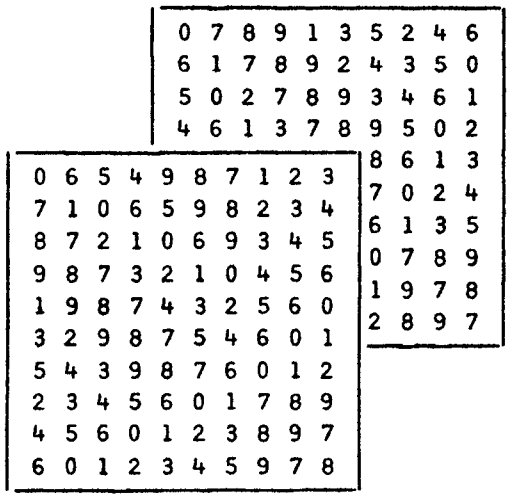
* *This research was done while the author was with the Department of Statistics, University of North Carolina at Chapel Hill, and was supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and AFOSR-68-1406.*



0	6	5	4	9	8	7	1	2	3
7	1	0	6	5	9	8	2	3	4
8	7	2	1	0	6	9	3	4	5
9	8	7	3	2	1	0	4	5	6
1	9	8	7	4	3	2	5	6	0
3	2	9	8	7	5	4	6	0	1
5	4	3	9	8	7	6	0	1	2
2	3	4	5	6	0	1	7	8	9
4	5	6	0	1	2	3	8	9	7
6	0	1	2	3	4	5	9	7	8

C O M B I N A T O R I A L
M A T H E M A T I C S
Y E A R

February 1969 - June 1970

ON t-DESIGNS AND THRESHOLD DECODING

by

J. M. Goethals*
MBLE Research Laboratory
Brussels, Belgium

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 600.29

June, 1970

ON t-DESIGNS AND THRESHOLD DECODING

by

J. M. Goethals*
MBLE Research Laboratory
Brussels, Belgium

1. INTRODUCTION.

In this paper, it is shown how some combinatorial properties of t-designs can be used to devise a very simple method of threshold decoding, which is applied to the (24,12) and (48,24) binary extended quadratic-residue codes. A basic role in this respect is played by the intersection numbers X_j^s and the occurrence numbers of j-tuples Y_j^s which are defined in the first section.

2. INTERSECTION NUMBERS OF t-DESIGNS.

A *tactical configuration* $(\lambda_t;v,k,t)$ or a *t-design* is a set V of v elements and a collection of k-subsets of V, called blocks, such that every t-subset of V is contained in exactly λ_t blocks. For $j = 0,1,\ldots,t$, the number λ_j of blocks containing any j-subset of V is a constant and we have

$$\lambda_j\,(k-j) = \lambda_{j+1}(v-j)$$

$$\lambda_0 \binom{k}{j} = \lambda_j \binom{v}{j}$$

$$\lambda_j \binom{k-j}{t-j} = \lambda_t \binom{v-j}{t-j}$$

---

* This research was done while the author was with the Department of Statistics, University of North Carolina at Chapel Hill, and was supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and AFOSR-68-1406.

where λ_0 is the total number of blocks. This well-known result ([1],[5]) may be proved by considering the *derived* tactical configurations $(\lambda_t;v-1,k-1,t-1)$ which are defined by the blocks of $(\lambda_t;v,k,t)$ containing any given element of V. The remaining blocks constitute the so-called *residual* tactical configurations $(\lambda_{t-1}-\lambda_t;v-1,k,t)$. Tactical configurations with $\lambda_t = 1$ are called *Steiner systems*.

Mendelsohn [5] defined the *intersection numbers* X_i to be the number of blocks which intersect a given block in exactly i elements, and, by counting in two different ways the number of j-tuples occuring, easily obtained the following equations

$$\sum_{i=j}^{k} \binom{i}{j} X_i = \binom{k}{j}(\lambda_j - 1), \qquad (1)$$

for $j = 0,1,2,\ldots,t$. When the intersection numbers X_i for a given block satisfy

$$X_{t+1} = X_{t+2} = \ldots = X_k = 0,$$

which is certainly the case for Steiner systems $(\lambda_t=1)$, the set of (t+1) equations (1) has an unique solution given by

$$X_j = \sum_{i=j}^{k} (-1)^{i-j} \binom{i}{j} \binom{k}{i} (\lambda_{i-1}), \qquad (2)$$

for $j = 0,1,2,\ldots,t$.

For example, the well-known Steiner system $(1;24,8,5)$ gives for any block, the intersection numbers $X_0 = 30$, $X_1 = 0$, $X_2 = 448$, $X_3 = 0$, $X_4 = 280$, $X_5 = 0$, (see [4], lemma 5.1).

By considering a given s-tuple of elements and defining the more general *intersection numbers* X_i^s to be the number of blocks which intersect the given s-tuple in exactly i elements, one easily obtains the following equations

$$\sum_{i=j}^{s} \binom{i}{j} X_i^s = \binom{s}{j} \lambda_j \tag{3}$$

for $j = 0,1,2,\ldots,\min(s,t)$. There are indeed $\binom{s}{j}$ distinct j-tuples of elements in the given s-tuple, each of which occurs λ_j times, and each block which intersects the given s-tuple in i elements contributes $\binom{i}{j}$ distinct j-tuples. Hence both members of (3) are equal. For $s \leq t$, there is an unique solution given by

$$X_j^s = \sum_{i=j}^{s} (-1)^{i-j} \binom{i}{j} \binom{s}{i} \lambda_i, \tag{4}$$

for $j = 0,1,2,\ldots,s$. Obviously $X_s^s = \lambda_s$, and for $s \leq t$ each one of the $\binom{s}{j}$ j-tuples that are contained in the given s-tuple must occur the same number of times, say Y_j^s times, that is

$$X_j^s = \binom{s}{j} Y_j^s. \tag{5}$$

Then, using the fact that

$$\binom{s}{i}\binom{i}{j} = \binom{s}{j}\binom{s-j}{i-j},$$

the set of equations (3) can be given the form

$$\sum_{i=j}^{s} \binom{s-j}{i-j} Y_i^s = \lambda_j, \tag{6}$$

in which both numbers count the number of times a given j-tuple occurs. The first member of (6) can be interpreted in the following way: there are $\binom{s-j}{i-j}$ i-tuples which are contained in the given s-tuple and which contain a given j-tuple, and each of these i-tuples occurs Y_i^s times. Again, since $s \leq t$ there is an unique solution to (6), which is given by

$$Y_j^s = \sum_{i=j}^{s} (-1)^{i-j} \binom{s-j}{i-j} \lambda_i . \tag{7}$$

These numbers Y_j^s, which could be called *occurrence numbers* of j-tuples, are given below (table 1) for the (1;24,8,5) Steiner system.

Table 1: *Occurrence numbers* Y_j^s *of* (1;24,8,5)

s \ j	0	1	2	3	4	5
0	759	-	-	-	-	-
1	506	253	-	-	-	-
2	330	176	77	-	-	-
3	210	120	56	21	-	-
4	130	80	40	16	5	-
5	78	52	28	12	4	1

It is observed that one has

$$Y_j^s = Y_{j+1}^{s+1} + Y_j^{s+1} , \tag{8}$$

which is a quite general property, as we now prove, in two different ways. Firstly, using (7), one has

$$Y_j^{s+1} + Y_{j+1}^{s+1} = \sum_{i=j}^{s+1} (-1)^{i-j} \left[\binom{s+1-j}{i-j} - \binom{s-j}{i-j-1} \right] \lambda_i$$

where the expression under brackets simply reduces to $\binom{s-j}{i-j}$, which proves

the result. But, by dropping one element from the given (s+1)-tuple, Y_{j+1}^{s+1} can be interpreted as the occurrence number of j-tuples in the derived design, and similarly Y_j^{s+1} is the occurrence number of j-tuples in the residual design, and having this in mind gives (8) an obvious interpretation since the original design is the union of the derived and residual designs.

3. THRESHOLD DECODING WITH t-DESIGNS.

Let us consider the binary code of length v which is orthogonal to the incidence vectors of a t-design $(\lambda_t;v,k,t)$. For example, the extended Golay binary code of length 24 can be defined to be orthogonal to the incidence vectors of the (1;24,8,5) Steiner system (see [1] and [3]). A decoding method for that particular code was described in [3], which will be formalized and extended to some other codes here. The basic idea consists in taking as parity check set those λ_1 incidence vectors of the t-design which contains a given element of V and which are known to form a (t-1)-design on the remaining (v-1) elements of V. Then, if the number e of errors does not exceed t-1, the number of parity check failures can be calculated exactly by means of the intersection numbers X_i^e of the (t-1)-design. For example, the intersection numbers of the (1;23,7,4), which are easily obtained from table 1, are as follows (table 2):

Table 2: *Intersection numbers* X_j^s *of* (1;23,7,4)

s \ j	0	1	2	3	4
0	253	-	-	-	-
1	176	77	-	-	-
2	120	112	21	-	-
3	80	120	48	5	-
4	52	112	72	16	1

Now, suppose two errors occured, none of which affects the digit corresponding to the fixed element of V. Then the number of parity check failures will be exactly equal to $X_1^2 = 112$. In general, when e errors occur, none of which affects the fixed digit, the number of parity check failures will be given by the summation of the intersection numbers X_j^e with odd j. For example, for $e = 3$, it will be $120 + 5 = 125$. If, on the other hand, one error affects the fixed digit and if in addition $e - 1$ other digits are corrupted by error, the number of parity check failures will be given by

$$X_0^0 - \sum_{\text{odd } j} X_j^{e-1} = \sum_{\text{even } j} X_j^{e-1},$$

since the error in the fixed position contributes to all X_0^0 parity checks. For example, for $e = 3$, it will be $253-112 = 141$. The results concerning the above example are summarized in table 3.

Table 3: *number of parity check failures; code (24,12)*

Number of errors	Fixed digit in error	Fixed digit not in error
1	253	77
2	176	112
3	141	125
4	128	128

It is observed that, provided the number of errors does not exceed 3, it can be decided whether or not the fixed digit was in error, according as the number of parity check failures is greater or less than 128. Since the rode has minimum distance 8, this decoding method uses the full error-correcting

ability of the code. Moreover, uncorrectable errors ($e = 4$) can be detected when the number of parity check failures is exactly equal to 128.

The same reasoning will now be applied to the (48,24) extended quadratic residue binary code, which can be defined to be orthogonal to the incidence vectors of a 5-design with parameters (8;48,12,5), as was shown by Assmus and Mattson [2]. Using the relations (7), the occurrence numbers are easily calculated (table 4), from which the intersection numbers x_i^s of the derived design (8;47,11,4) are obtained (table 5). Then, provided the number of errors does not exceed 4, the number of parity check failures can be calculated exactly in each case (table 6).

Table 4: *occurrence numbers* Y_j^s *of* (8;48,12,5)

s \ j	0	1	2	3	4	5
0	17296	-	-	-	-	-
1	12972	4324	-	-	-	-
2	9660	3312	1012	-	-	-
3	7140	2520	792	220	-	-
4	5236	1904	616	176	44	-
5	3808	1428	476	140	36	8

Table 5: *intersection numbers* x_j^s *of* (8;47,11,4)

s \ j	0	1	2	3	4
0	4324	-	-	-	-
1	3312	1012	-	-	-
2	2520	1584	220		-
3	1904	1848	522	44	-
4	1428	1904	840	144	8

Table 6: *number of parity check failures; code (48,24)*

Number of errors	Fixed digit in error	Fixed digit not in error
1	4324	1012
2	3312	1584
3	2740	1892
4	2426	2048

Since the code can actually correct up to 5 errors, the case $e = 5$ deserves further investigation. If the fixed digit is in error, the number of parity check failures will then be equal to $4324 - 2048 = 2276$. Suppose now the fixed digit is not affected by error, and let x be the intersection number X_5^5, which obviously cannot exceed $X_4^4 = 8$. Then, from the set of equations (3), one easily gets $X_5^5 = x$, $X_4^5 = 40-5x$, $X_3^5 = 280+10x$, $X_2^5 = 1120-10x$, $X_1^5 = 1820+5x$, $X_0^5 = 1064-x$, from which it follows that the number of parity check failures is equal to $2100 + 16x$, which cannot exceed 2228. Hence the code can be threshold decoded up to 5 errors, with a set of 4324 parity checks and a threshold comprised in the range 2228 ... 2276.

REFERENCES

[1] ASSMUS, E.F.,Jr. and MATTSON, H.F., On tactical configurations and error-correcting codes, *J. Combinatorial Theory*, 2 (1967), 243-257.

[2] ASSMUS, E.F.,Jr. and MATTSON, H.F., New 5-designs, *J. Combinatorial Theory*, 6 (1969), 122-151.

[3] GOETHALS, J.M., On the Golay perfect binary code, *J. Combinatorial Theory*, (to appear).

[4] GOETHALS, J.M. and SEIDEL, J.J., Strongly regular graphs derived from combinatorial designs, *Canadian J. Math.*, (to appear).

[5] MENDELSOHN, N.S., Some applications of intersection numbers to problems in t-designs, presented at *The Second Chapel Hill Conference on Combinatorial Mathematics and its Applications* (May 1970).