Some bridges between codes and designs

Peter J. Cameron

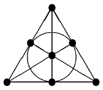
School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS, U.K.
p.j.cameron@qmw.ac.uk

Remembering Hamming and Assmus

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Hamming code

The dual code has one non-zero weight.



The Assmus–Mattson theorem gives 2-designs, $(7,3,1)$ and $(7,4,2)$.

A problem

What is the smallest number m of subsets (blocks) of $\{1,\ldots,n\}$ such that

(a) any two blocks meet in *at most* two points;

(b) any two points lie in *at least* two blocks?

Some results

Theorem (i) $m \geq n$, with equality if and only if the blocks form a biplane.

(ii) $m \leq (2+o(1))n$.

Proof (i) Count incidences between point-pairs and block pairs.

(ii) Let $n = q^2+q+1$, q a prime power, and let D be a planar difference set in $\mathbf{Z}/(n)$. Take all translates of D and $-D$.

Some values

n	3	4	5	6	7	8	9
m	4	4	7	7	7	10	11

n	10	11	12	13	14	15	16
m	11	11	16	16	16	16	16

If $r \geq 4$ and $\binom{r-1}{2} + 2 \leq n \leq \binom{r}{2}$, then

$$m \geq \min\left\{ \binom{r}{2} + 1, \left\lfloor 2\binom{n}{2} / \binom{r-1}{2} \right\rfloor + 1 \right\}.$$

A problem

We are given a set of n objects, and we know that one pair is ‘active’. We can test any subset of the objects; the test result will be positive if and only if the active pair is contained in the set being tested.

How many tests are required?

Two approaches

Scheme 1. Choose a family of sets as in the earlier problem and test these sets. Condition (b) guarantees at least two positive results, and condition (a) guarantees that these determine the active pair. $(2+o(1))n$ tests are required.

Scheme 2. It is possible to identify the active pair in at most $8\log_2 n$ tests (and at most $4\log_2 n$ if $n = 2^k - 1$) using coding theory.

The coding scheme

Suppose that $n = 2^k - 1$. There is a 2-error-correcting BCH code of length n and codimension $2k$. Imagine that the zero codeword was transmitted, and two errors were made in the positions of the active pair. We can correct the errors, i.e. identify the active pair.

Let H be a $2k \times n$ parity check matrix for the code. Use *syndrome decoding*, i.e. calculate $vH^\top$, where v is the characteristic vector of the active pair. Then v can be recovered from its syndrome.

The coding scheme

The ith bit in the syndrome is the inner product of v with the ith row of H, i.e. it is 1 if the active pair is separated by the support of the ith row. We can determine this with two tests A_i^0 and A_i^1, where A_i^ε is the set of positions where ε occurs in the ith row. So $4k$ tests are required.

The number may be smaller: if A_i^0 tests positive, then A_i^1 doesn't have to be tested.

Variations

What if some test results are incorrect?

Choose a code C of length m and dimension $2k$ that will correct the maximum number of errors likely to occur in the tests. Let G be its $2k \times m$ generator matrix. Then use $G^\top H$ instead of H in Scheme 2. $2m$ tests are required.

What if we have to identify subsets of other sizes?

Just choose a code correcting the appropriate number of errors.

Example

Suppose that we are trying to identify an active pair from a set of size 1000. The 2-error-correcting BCH code of length 1023 has codimension 20, so that 40 tests are required.

If we suspect that some tests will give the wrong result, but (say) not more than 3% of all tests in a sequence will be wrong, we could use a 2-error-correcting shortened BCH code of length 30 and dimension 20, which will yield the required information in 60 tests, correctly if at most two test results are wrong.

Who found the Hamming codes?

R. A. Fisher, The theory of confounding in factorial experiments in relation to the theory of groups, *Ann. Eugenics* **11** (1942), 341–353.

R. A. Fisher, A system of confounding for factors with more than two alternatives, giving completely orthogonal cubes and higher powers, *Ann. Eugenics* **12** (1945), 2283–290.

M. J. E. Golay, Notes on digital coding, *Proc. IEEE* **37** (1949), 657.

R. W. Hamming, Error detecting and error correcting codes, *Bell Systems Tech. J.* **29** (1950), 147–160.

Coding theory

We wish to send words of length n over an alphabet A with $|A| = q$ over a noisy channel where errors can occur.

We *assume* that, with high probability, not too many errors occur during transmission of a word.

The strategy is to send words from a *code* C, a subset of A^n. We require:

(a) *large minimum distance* d: if $d \geq 2e+1$, we can correct up to e errors;

(b) *many codewords* (subject to (a)): the transmission rate is $\log_q |C|/n$;

(c) *computationally efficient encoding and decoding* (subject to (a) and (b)).

Factorial design

We are investigating n factors which can affect the yield of some process. The ith factor can take any one of a set A_i of levels, with $|A_i| = q_i$.

We assume that only the interactions of small numbers of factors affect the yield significantly.

We impose the structure of an abelian group on A_i, and test treatment combinations lying in a subgroup B of $A_1 \times \cdots \times A_n$.

Factorial design

Let C be the annihilator of B in $A_1^* \times \cdots \times A_n^*$. (Here A_i^* is the group of characters of A_i; so C is the set of all characters of $A_i \times \ldots \times A_n$ which are trivial on B.)

Elements of C represent combinations of treatments which are confounded in the experiment. (For example, if an element of C has support in $A_i^* \cup A_j^* \cup A_k^*$, then the interaction of factors j and k cannot be distinguished from the main effect of factor i.)

Factorial design

We want

(a) *Large weight in* C so that potentially significant combinations of factors are not confounded;

(b) *Few trials* (subject to (a)): trials are expensive! This means small B, and so large C: note that

$$|C| = \frac{q_1 \cdots q_n}{|B|}.$$

(c) *simple description* which can be explained to experimenters and for which results can be analysed (subject to (a) and (b)).

Comparison

Design theorists and coding theorists are both looking for subsets C of $A_1 \times \cdots \times A_n$ with large minimum distance and large cardinality.

Coding theorists have n large, all A_i of the same size (almost always 2), and don't insist on group structure (though it does help to use a linear code).

Statisticians have n fairly small, varying alphabet size, and do require group structure.

Hamming codes satisfy both specifications!

Hamming codes

Let $V = \mathrm{GF}(q)^k$. Partition the non-zero vectors in V into equivalence classes, where two vectors are equivalent if one is a non-zero scalar multiple of the other. There are $(q^k-1)/(q-1)$ equivalence classes.

Choose one vector from each equivalence class, and let H be the $k \times (q^k-1)/(q-1)$ matrix having these vectors as columns. (For simplicity, take all vectors whose first non-zero entry is 1.) Then any two columns of H are linearly independent.

The code C with parity check matrix H thus has minimum weight 3 and so is 1-error-correcting. This is the *Hamming code* $H(k,q)$.

Fisher's Theorem on Minimal Confounding

Fisher (1942) proved that:

> A 2^n factorial scheme can be arranged in 2^{n-p} blocks of 2^p plots each, without confounding either main effects or 2-factor interactions, provided that $n < 2^p$.

Subsequently (1945), he generalized this theorem and proved that:

> A π^n factorial scheme can be arranged in π^{n-p} blocks of π^p plots each, without confounding either main effects or 2-factor interactions, provided that
>
> $$n \le (\pi^p - 1)/(\pi - 1).$$

D. J. Finney, *An Introduction to the Theory of Experimental Design*, University of Chicago Press, Chicago, 1960.

(Here π is a prime power.)

Mixed alphabets

C is a code of length n and minimum distance d over alphabets of size $q_1, \ldots, q_n$. Let $e = \lfloor (d-1)/2 \rfloor$, and assume that $q_1 \le \cdots \le q_n$.

Sphere-packing bound:

$$|C| \le \frac{\displaystyle\prod_{i=1}^{n} q_i}{\displaystyle\sum_{k=0}^{e} \sum_{i_1 < \cdots < i_k} \prod_{j=1}^{k} (q_{i_j} - 1)}.$$

Singleton bound:

$$|C| \le \prod_{i=1}^{n-d+1} q_i.$$

Plotkin bound: Let

$$\alpha = \sum_{i=1}^{n} (1 - 1/q_i).$$

If $d > \alpha$ then $|C| \le d/(d-\alpha)$.

An example

Let $n = 5$ and let the alphabet sizes be $2,2,2,2,4$. Take $d = 3$.

The sphere-packing bound gives

$$|C| \leq \frac{2 \cdot 2 \cdot 2 \cdot 2 \cdot 4}{1+1+1+1+1+3} = 8.$$

The Singleton bound gives

$$|C| \leq 2 \cdot 2 \cdot 2 = 8.$$

The Plotkin bound:

$$\alpha = \tfrac{1}{2}+\tfrac{1}{2}+\tfrac{1}{2}+\tfrac{1}{2}+\tfrac{3}{4} = \tfrac{11}{4} < 3,$$

so $|C| \leq 3/(3 - \frac{11}{4}) = 12$.

An example

Take $A_1 = \ldots = A_4 = \{0,1\}$ (the cyclic group of order 2) and $A_5 = \{0,a,b,c\}$ with $a+b+c = 0$ (the Klein group of order 4).

Then C is

00000
11110
$0011a$
$1100a$
$0101b$
$1010b$
$0110c$
$1001c$

More generally . . .

For every $a < b$ and prime power q, there is a perfect code of length $(q^b - q^a)/(q-1) + 1$ over alphabets of sizes q ($(q^b - q^a)/(q-1)$ times) and q^a (once).

This is constructed using Hamming codes. If $b = a - 1$, it meets the Singleton bound too.

Codes and projective spaces

R. C. Bose, Mathematical theory of the symmetrical factorial design, *Sankhyā* **8** (1947), 107–166.

R. C. Bose and J. N. Srivastava, On a bound useful in the theory of factorial design and error-correcting codes, *Ann. Math. Statist.* **35** (1964), 408–414.

C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Math.* **55** (1976), 119–128.

Codes and projective spaces

Let A be a $k \times n$ matrix over $\mathrm{GF}(q)$. Assume that no two columns are linearly dependent, and that A has rank k.

(a) A is the parity check matrix of a $[n, n-k]$ code

$$C = \{v \in \mathrm{GF}(q)^n : Av^\top = 0\}.$$

Elementary row operations don't affect C; column permutations and scalar multiplications replace it by an equivalent code (metric properties are unaffected). The code C has minimum weight at least 3, so is 1-error-correcting. The corresponding factorial design has q^k treatments.

Codes and projective spaces

(b) The columns of A are a set S of n points in projective space $\mathrm{PG}(k-1,q)$. Elementary row operations induce collineations of the projective space, while column permutations don't change S. The set S spans $\mathrm{PG}(k-1,q)$.

So 1-error-correcting codes (up to equivalence) correspond naturally to spanning subsets of projective space (up to collineations).

The correspondence between codes and projective spaces allows many properties to be transferred back and forth:

Codes and projective spaces

1. The Hamming codes correspond to the entire projective space. The code/projective space connection can be regarded as a generalisation of the construction of Hamming codes.

2. Supports of words of the dual code correspond to complements of hyperplane sections of S.

3. (Bose 1947) MDS codes (those which meet the Singleton bound) correspond to arcs in projective space. (This, and a bound on the size of arcs in projective planes, are in Bose's paper on factorial designs.)

4. (Greene 1976) The weight enumerator of the code is a specialisation of the Tutte polynomial of the matroid represented by the matrix. Hence the MacWilliams identities follow from matroid duality.