PERFECT CODES AND DISTANCE-TRANSITIVE GRAPHS

NORMAN BIGGS

1. Introduction

Let S_k denote the set of sequences of k binary digits; in coding theory a subset C of S_k is called a binary code of block length k. If a code-word $c \in C$ is 'transmitted', and a sequence $s \in S_k$ is 'received', then the number of errors is the number of places in which s differs from c. One defines

$$\Sigma_e(c) = \{s \in S_k \mid s \text{ and } c \text{ differ in at most } e \text{ places}\},$$

and says that C is an e-error correcting code if the sets $\Sigma_e(c)$, as c runs through C, are disjoint. If these sets partition S_k, we have a perfect code.

In coding theory it is customary to introduce the vector space structure of the set S_k; however, we shall take the view that the elements of S_k are best regarded as the vertices of a graph, two vertices being adjacent whenever they differ in just one place. We denote this graph by the symbol Q_k, and note that it is the graph formed by the vertices and edges of a hypercube in k dimensions. The distance function ∂ in Q_k enables us to count errors, and we now write

$$\Sigma_e(v) = \{w \in VQ_k \mid \partial(v, w) \leq e\}.$$

In these terms, an e-error correcting binary perfect code, of block length k, is a subset C of VQ_k with the property that the sets $\Sigma_e(c)$, as c runs through C, partition VQ_k. We shall refer to C as a perfect e-code in Q_k, and we shall always take $e \geq 1$.

It is remarkable that there are relatively few pairs (k, e) for which a perfect e-code in Q_k exists [7], [8]. The complete list is:

Cambridge University Press
978-0-521-20454-5 - Combinatorics
Edited by T. P. McDonough and V. C. Mavron
Excerpt
More information

(i) $k = e$, the trivial codes with $|C| = 1$;

(ii) $k = 2e + 1$, the 'repetition' codes with $|C| = 2$;

(iii) $k = 2^r - 1$, $e = 1$, the Hamming codes [8];

(iv) $k = 23$, $e = 3$, the binary Golay code [8].

We are led to consider the possibility of replacing Q_k by other graphs. If Γ is a finite, connected, simple graph, with distance function ∂, and the sets $\Sigma_e(v)$ are defined as for Q_k, then we say that a subset C of $V\Gamma$ is a perfect e-code in Γ if the sets $\Sigma_e(c)$, $c \in C$, partition $V\Gamma$.

Now it is clear that for any given $e \geq 1$ we can construct, at will, graphs Γ which possess perfect e-codes, for we may just take a set of neighbourhoods $\Sigma_e(c)$ and join their free ends by extra edges; however, the graphs so constructed are uninteresting. We claim that the natural setting for the problem of perfect codes is the class of distance-transitive graphs [2]. This claim will be justified in Section 3, after some motivation in Section 2.

2. Perfect 1-codes in regular graphs

Suppose that Γ is regular, with valency k, and let A denote its adjacency matrix. If $\mathbf{c}$ is the column vector whose entries are 1 in positions corresponding to the vertices of a perfect 1-code in Γ, and 0 elsewhere, then

$$A\mathbf{c} = \mathbf{u} - \mathbf{c}$$

where $\mathbf{u}$ is the vector each of whose entries is 1. Let

$$\mathbf{w} = \mathbf{u} - (k + 1)\mathbf{c}.$$

Then we have

$$A\mathbf{w} = A\mathbf{u} - (k + 1)A\mathbf{c} = k\mathbf{u} - (k + 1)(\mathbf{u} - \mathbf{c}) = -\mathbf{w}.$$

In other words, -1 is an eigenvalue of A, corresponding to the eigenvector $\mathbf{w}$. Since A is a rational symmetric matrix, its minimum polynomial $\mu(t)$ belongs to the ring $\mathbf{Q}[t]$ of polynomials with rational coefficients. We call $\mu(t)$ the minimum polynomial of Γ, and we have proved:

Theorem 1. If the regular graph Γ has a perfect 1-code, then $t + 1$ is a divisor of $\mu(t)$ in the ring $\mathbf{Q}[t]$.

The result indicates that the minimum polynomial of a graph is relevant to the study of perfect codes in the graph. In the case of a distance-transitive graph, not only do we have a simple method of finding the minimum polynomial, but there is also an extension of Theorem 1 for perfect e-codes with $e > 1$.

3. Perfect e-codes in distance transitive graphs

The graph Γ is distance-transitive if whenever u, v, x, y are vertices of Γ such that $\partial(u, v) = \partial(x, y)$ then there is an automorphism of Γ taking u to x and v to y. A full treatment of the properties of such graphs may be found in [2], but we shall sketch the relevant parts of the theory here.

Associated with each distance-transitive graph Γ, having valency k and diameter d, is an intersection array

$$\iota(\Gamma) = \left\{ \begin{matrix} * & 1 & c_2 & \cdot & \cdot & \cdot & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdot & \cdot & \cdot & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdot & \cdot & \cdot & b_{d-1} & * \end{matrix} \right\};$$

from this we can calculate the eigenvector sequence $v_0(t), v_1(t), \ldots, v_d(t)$, each term of which belongs to the ring $\mathbf{Q}[t]$. The recursion defining this sequence is

$$\begin{cases} v_0(t) = 1, \quad v_1(t) = t, \\ c_i v_i(t) + (a_{i-1} - t)v_{i-1}(t) + b_{i-2}v_{i-2}(t) = 0 \quad (i = 2, \ldots, d). \end{cases}$$

For $0 \le i \le d$ we define $x_i(t) = v_0(t) + v_1(t) + \ldots + v_i(t)$; then it can be shown that the minimum polynomial of Γ is

$$\mu(t) = (t - k)x_d(t).$$

The proof of the following theorem is given in [1].

Theorem 2. _If the distance-transitive graph_ Γ _has a perfect e-code, then_ $x_e(t)$ _is a divisor of_ $\mu(t)$ _in the ring_ $\mathbf{Q}[t]$.

We notice that $x_1(t) = t + 1$, so that we have verified incidentally the result of Theorem 1 in this special case.

The graph Q_k is a distance-transitive graph, with intersection array

$$\iota(Q_k) = \left\{ \begin{matrix} * & 1 & 2 & . & . & . & k-1 & k \\ 0 & 0 & 0 & . & . & . & 0 & 0 \\ k & k-1 & k-2 & . & . & . & 1 & * \end{matrix} \right\}$$

Now it follows from [1, Section 5] that, if we write $s = \frac{1}{2}(k - t)$, then

(i) $$x_e(t) = \sum_{i=0}^{e} (-1)^i \binom{s-1}{i}\binom{k-s}{e-i},$$

(ii) $$\mu(t) = Rs(s-1)(s-2) \dots (s-k) \quad (R \text{ a rational constant}).$$

We deduce from Theorem 2 that if there is a perfect e-code in Q_k, then the polynomial on the right of (i) must have its e zeros corresponding to s in the set $\{0, 1, \dots, k\}$. This is the theorem of Lloyd [8], in the classical case, and it was by using this theorem that the list in Section 1 was proved to be complete.

It is now possible to state three reasons why the question of perfect codes should be considered in the context of distance-transitive graphs.

(a) The classical question is a special case.

(b) The theorem of Lloyd generalizes and simplifies.

(c) Other interesting examples arise.

4. Examples

Examples of perfect codes in distance-transitive graphs are rare; in fact, it is true to say that examples of distance-transitive graphs are rare! However, this merely adds interest to the examples which are known.

It is clear that the graphs Q_k can be generalized by replacing the binary 'alphabet' by an alphabet of q symbols, for any $q > 2$. This generalization is part of classical coding theory, and is treated from our present viewpoint in [1]. It is known that, apart from some perfect 1-codes, the only other code in this case is the ternary Golay 2-code [8].

In the twelve trivalent distance-transitive graphs [4] there are only two non-trivial perfect codes: the repetition 1-code in Q_3 and a 1-code in the graph with 28 vertices. The latter code is evident from the construction of the graph given in Section 1 of [4].

We now turn to the odd graphs O_k $(k \geq 3)$. The graph O_k has for its vertices the (k-1)-subsets of a (2k-1)-set, two vertices being adjacent whenever the subsets are disjoint; O_k is a distance-transitive graph with valency k and diameter $k - 1$. It can be shown that the eigenvalues of O_k are the integers $(-1)^{k-i}i$ $(1 \leq i \leq k)$, so that

$$\mu(t) = (t - k)(t + k - 1)(t - k + 2) \ldots (t + (-1)^k).$$

It is also easy to give explicit expressions for the first few terms of the eigenvector sequence, and from these we find

$$x_0(t) = 1, \quad x_1(t) = t + 1, \quad x_2(t) = t^2 + t - (k - 1),$$
$$x_3(t) = \tfrac{1}{2}(t + 1)(t^2 + t - (2k - 2)).$$

Theorem 3. Suppose that there is a perfect e-code in O_k, $(e = 1, 2, 3)$. Then

(i) $e = 1 \Rightarrow k$ is even;
(ii) $e = 2 \Rightarrow k = 4r^2 - 2r + 1$ for some natural number r;
(iii) $e = 3 \Rightarrow k = 2(4r^2 - 3r + 1)$ for some natural number r.

Proof. (i) For a 1-code in O_k we require that $t + 1$ is a factor of $\mu(t)$, and this is so if and only if k is even.

(ii) For a 2-code in O_k we require that $t^2 + t - (k - 1)$ divides $\mu(t)$. Since the zeros of $\mu(t)$ are the integers $(-1)^{k-i}i$ $(1 \leq i \leq k)$ we must have

$$t^2 + t - (k - 1) = (t - \alpha)(t - \beta),$$

where α and β are integers having the stated form. Equating co-efficients of t we get $\beta = -(\alpha + 1)$, and we may assume that $\alpha > 0$,

$\beta < 0$. Equating coefficients of unity we get

$$k - 1 = -\alpha\beta = \alpha(\alpha + 1),$$

so that $k - 1$ is even and k is odd. Since α is a positive integral zero of $\mu(t)$, $k - \alpha$ must be even, and so α is odd. Writing $\alpha = 2r - 1$, we get $k = 2r(2r - 1) + 1 = 4r^2 - 2r + 1$, as required.

(iii) This part is proved by an argument like that in (ii).

Our condition that k is even for a 1-code in O_k is a weak one, and it can be improved by the following direct argument. Let C be a subset of VO_k which is a perfect 1-code; then any two distinct vertices u, v in C satisfy $\partial(u, v) \geq 3$. But if these vertices (regarded as $(k-1)$-subsets of a $(2k-1)$-set) have $k - 2$ elements in common, then $\partial(u, v) = 2$. Consequently each set of $k - 2$ elements occurs at most once as a subset of the elements in a vertex belonging to C. Since each vertex contains $k - 1$ sets of $k - 2$ elements we have

$$|C| \leq \frac{1}{k-1} \cdot \binom{2k-1}{k-2}$$

with equality only if each $(k-2)$-set occurs exactly once in a vertex of C. But for a perfect 1-code, the $\binom{2k-1}{k-1}$ vertices are partitioned into $|C|$ sets of $k + 1$, and so

$$|C| = \frac{1}{k+1} \cdot \binom{2k-1}{k-1} = \frac{1}{k-1} \cdot \binom{2k-1}{k-2} .$$

Thus every $(k-2)$-set occurs just once in a vertex of C, and these vertices are the blocks of a Steiner system $S(k-2, k-1, 2k-1)$. (This result is due to P. J. Cameron.) There are only two such systems known: $S(2, 3, 7)$ and $S(4, 5, 11)$, giving rise to perfect 1-codes in O_4 and O_6. In fact the divisibility conditions for a Steiner system imply that $k + 1$ must be prime, which is considerably stronger than our requirement that $k + 1$ must be odd.

There are no known e-codes in O_k for $k-1 > e > 1$.

We now mention a situation which generalizes the 'repetition' codes in the classical case. We say that a connected graph Γ, of diameter d, is antipodal if $\partial(u, v) = d$ and $\partial(u, w) = d$ implies that $v = w$ or

CAMBRIDGE

Cambridge University Press
978-0-521-20454-5 - Combinatorics
Edited by T. P. McDonough and V. C. Mavron
Excerpt
More information

$\partial(v, w) = d$. The importance of this concept lies in the fact that a distance-transitive graph in which the automorphism group acts imprimitively on the vertices must be either bipartite or antipodal [6]. An antipodal distance-transitive graph Γ of odd diameter $d = 2d' + 1$ has a derived graph Γ', with diameter d', which is also distance-transitive; details of this situation are given in [3]. We find that $|V\Gamma| = r|V\Gamma'|$ for some integer $r \geq 2$, and Γ has a perfect d'-code C with $|C| = r$. Furthermore, the calculations in [3] show that, for Γ, $x_{d'}(t)$ divides $\mu(t)$, in accordance with Theorem 2.

Finally, we construct a special example. Consider the projective plane $PG(2, 3^2)$; this plane admits a unitary polarity induced by the field automorphism $\theta \mapsto \theta^3$ of $GF(3^2)$. The plane contains 91 points and 91 lines, which may be classified as follows [5]:

28 isotropic points	(points which lie on their polar lines);
63 non-isotropic points	(points which do not lie on their polar lines);
28 tangents	(lines containing 1 isotropic point and 9 non-isotropic points);
63 secants	(lines containing 4 isotropic points and 6 non-isotropic points).

We construct a graph W, whose vertices are the 63 non-isotropic points, and two are adjacent whenever each lies on the polar line of the other. Then W is a distance-transitive graph with intersection array

$$\begin{Bmatrix} * & 1 & 1 & 3 \\ 0 & 1 & 1 & 3 \\ 6 & 4 & 4 & * \end{Bmatrix}$$

and minimum polynomial

$$(t - 6)(t + 1)(t^2 - 9).$$

The graph W has a perfect 1-code, consisting of the 9 vertices corresponding to the non-isotropic points on any tangent.

References

1. N. L. Biggs. Perfect codes in graphs, J. Combinatorial Theory (B), 15 (1973), 289-96.

2. N. L. Biggs. Algebraic graph theory. Cambridge Tracts in Mathematics, 67, Cambridge University Press, London, 1974.

3. N. L. Biggs and A. D. Gardiner. On antipodal graphs. (In preparation.)

4. N. L. Biggs and D. H. Smith. On trivalent graphs, Bull. London Math. Soc., 3 (1971), 155-8.

5. P. Dembowski. Finite geometries, Springer, Berlin, 1968.

6. D. H. Smith. Primitive and imprimitive graphs, Quart. J. Math. (Oxf.), 22 (1971), 551-7.

7. A. Tietavainen. On the non-existence of perfect codes over finite fields, Siam J. Appl. Math., 24 (1973), 88-96.

8. J. H. van Lint. Coding theory. Lecture Notes in Mathematics, 201, Springer, Berlin, 1971.

Royal Holloway College,
London, England

GENERALISATION OF FISHER'S INEQUALITY TO FIELDS WITH MORE THAN ONE ELEMENT

PETER J. CAMERON

Many people (Petrenjuk, Wilson, Ray-Chaudhuri, Noda, Bannai, Delsarte, Goethals, and Seidel among them) have contributed to these results; some of the ideas arose in several places. So this article will tend to be a commentary on the facts. I define a t-design, with parameters v, k, b_t, to be a collection of k-subsets of the v-set X, called 'blocks', with the property that any t-subset is contained in precisely b_t blocks; I require the non-degeneracy condition $t \le k \le v-t$. A t-design is a t'-design for $0 \le t' \le t$. I shall use b for the number of blocks, though notation suggests b_0. Fisher's inequality states that, in a 2-design, $b \ge v$; furthermore, if equality holds, then the 2-design is called symmetric, and has the property that the size of the intersection of two blocks is constant. The generalisations I shall discuss are:

(1) In a 2s-design, $b \ge \binom{v}{s}$; if equality holds, then for distinct blocks B, B', $|B \cap B'|$ takes just s distinct values.

(2) In a (2s-2)-design in which, for distinct blocks B, B', $|B \cap B'|$ takes just s distinct values, $b \le \binom{v}{s}$.

(In (2) it is also true that the blocks carry an 'association scheme with s classes', defined in the obvious way.)

If the definition of a t-design is weakened to allow 'repeated blocks', (1) remains true, while the only counterexamples to (2) are obtained by taking a (2s-2)-design without repeated blocks in which $|B \cap B'|$ takes just $s - 1$ values (such a design has exactly $\binom{v}{s-1}$ blocks), and repeating each block the same number of times.

The only known examples of equality in (1) with $s \ge 2$ are the Steiner system $S(4, 7, 23)$ (a 4-design with $v = 23$, $k = 7$, $b_4 = 1$) and its complement.

(1) is clearly a generalisation of Fisher's inequality; (2) is slightly less obviously so - we must observe that the 'dual' of the case $s = 1$ of

(2) is the case $s = 1$ of the following strengthened version of the first part of (1):

(3) Let $\mathcal{B}$ be a collection of subsets of a set X with $|X| = v$, and s an integer, such that

(i) for $s \leq i \leq 2s$, the number of members of $\mathcal{B}$ containing an i-subset of X is a constant b_i, depending only on i;

(ii) some $B \in \mathcal{B}$ satisties $s \leq |B| \leq v - s$.

Then $|\mathcal{B}| \geq \binom{v}{s}$.

Several people have observed that the concept of a t-design can be generalised as follows. Given a finite field $\mathbf{F}$, a t-design over $\mathbf{F}$ with parameters v, k, b_t is a collection of k-dimensional subspaces of a v-dimensional vector space over $\mathbf{F}$, called 'blocks', with the property that any t-dimensional subspace is contained in precisely b_t blocks; again I require $t \leq k \leq v - t$. Replacing 'design' with 'design over $\mathbf{F}$', $|B \cap B'|$ with $\dim(B \cap B')$, and the binomial coefficient $\binom{v}{s}$ with the function $\begin{bmatrix} v \\ s \end{bmatrix}_{\mathbf{F}}$ giving the number of s-dimensional subspaces of a v-dimensional vector space over $\mathbf{F}$, statements (1) and (2) remain valid, and their proofs require only trivial modifications. Similarly (3) can easily be converted into a valid statement:

(3') Let $\mathcal{B}$ be a collection of subspaces of a vector space X over $\mathbf{F}$, with $\dim(X) = v$, and s an integer, such that

(i) for $s \leq i \leq 2s$, the number of members of $\mathcal{B}$ containing a given i-dimensional subspace of X is a constant b_i, depending only on i;

(ii) some $B \in \mathcal{B}$ satisfies $s \leq \dim(B) \leq v - s$.

Then $|\mathcal{B}| \geq \begin{bmatrix} v \\ s \end{bmatrix}_{\mathbf{F}}$.

The proof I give below is essentially that of R. M. Wilson for the original statement (3). It was communicated to me by J. Doyen.

Suppose $|\mathbf{F}| = q$; let V and W be subspaces of the vector space X over $\mathbf{F}$, with $W \supseteq V$, $\dim(X) = a$, $\dim(W) = b$, $\dim(V) = c$. The number of subspaces U of X with $\dim(U) = d \geq c$, $U \cap W = V$, is

$$\frac{(q^a - q^b)(q^a - q^{b+1})\ldots(q^a - q^{b+d-c-1})}{(q^d - q^c)(q^d - q^{c+1})\ldots(q^d - q^{d-1})} .$$