JOURNAL OF COMBINATORIAL THEORY (B) 15, 289-296 (1973)

Perfect Codes in Graphs

NORMAN BIGGS

Royal Holloway College, University of London, Egham, Surrey, England

Communicated by W. T. Tutte

Received March 12, 1973

The classical problem of the existence of perfect codes is set in a vector space. In this paper it is shown that the natural setting for the problem is the class of distance-transitive graphs. A general theory is developed that leads to a simple criterion for the existence of a perfect code in a distance-transitive graph, and it is shown that this criterion implies Lloyd's theorem in the classical case.

1. INTRODUCTION

The problem of the existence of e-error correcting perfect codes of block length m over GF(q) is set in the vector space $V(m, q)$, endowed with the Hamming metric; we shall refer to this as the classical perfect code question. It is possible to replace the vector space by a graph $\Gamma(m, q)$, whose vertices are vectors and whose edges join vectors which differ in precisely one coordinate. In fact, there is an analogous graph for all natural numbers q, not just the prime powers, so that we have a slight gain in generality. (This case is also treated, from a different viewpoint, in [5].)

It is clear that we may pose the perfect code question for any graph Γ. Let v belong to the vertex-set $V\Gamma$ and let e be a non-negative integer; define $\sum_e (v)$ to be the set of vertices of Γ whose distance from v is not greater than e. Then a perfect e-code in Γ is a subset C of $V\Gamma$ such that the sets $\sum_e (c)$, as c runs through C, form a partition of $V\Gamma$. However, the class of all graphs is too general a setting for the perfect code question, since we may construct perfect codes at will by choosing suitable (but uninteresting) graphs.

In this paper we shall try to justify the claim that the proper setting for the perfect code question is the class of distance-transitive graphs. This class contains the graphs $\Gamma(m, q)$, and many other important graphs; its members are distinguished by their remarkable symmetry. Our justification rests on the algebraic formulation of Lloyd's theorem, as it is given in [5] and [7]. This theorem gives a necessary condition for the existence of perfect codes in the classical case, and it has recently been employed by Tietäväinen [6] in showing that the only solutions to the classical problem are the obvious ones, the Hamming 1-codes (see [7]), and two exceptional codes first described by Golay [4].

The proof of Lloyd's theorem is in two parts: some theory, and some calculations involving characters. We shall show that the theory can be developed (and simplified) in the setting of a general distance-transitive graph, and that it leads to a condition on the divisibility of two polynomials which generalizes Lloyd's theorem. Our exposition will show clearly that the structure of the group of the graph is unimportant, the vital fact being that the group acts on the graph in the distance-transitive manner.

In each particular instance, the relevant calculations can be expressed in terms of the intersection array of the graph. We shall derive Lloyd's theorem in this way, using the graphs $\Gamma(m, q)$, and briefly discuss the existence of perfect codes in other graphs.

I should like to express my thanks to the University of Waterloo, at which I held a visiting appointment while this paper was written, and to Dr. P. J. Cameron of Merton College, Oxford, who first pointed out to me the similarity between Lloyd's theorem and some calculations involving distance-transitive graphs.

2. Distance-Transitive Graphs

A simple connected graph Γ with distance function ∂ is said to be *distance-transitive* if, whenever u, v, x, y are vertices of Γ satisfying $\partial(u, v) = \partial(x, y)$, then there is an automorphism g of Γ such that $g(u) = x$ and $g(v) = y$. We shall briefly review the relevant theory of distance-transitive graphs, referring the reader to [1] and [2] for details and proofs.

Let $n = | V\Gamma |$ and d be the diameter of Γ. We define $d + 1$ matrices $A_0, A_1, \ldots, A_d$, each having n rows and columns labeled by the vertices of Γ, as follows:

$$(A_h)_{uv} = \begin{cases} 1, & \text{if } \partial(u, v) = h, \\ 0, & \text{otherwise.} \end{cases}$$

The matrix $A_1 = A$ is the usual adjacency matrix of Γ. The *adjacency algebra*, $\mathcal{A}(\Gamma)$, is the algebra of polynomials in A (over $\mathbb{C}$); in the case of a distance-transitive graph this algebra has dimension $d + 1$ and the set $\{A_0, A_1, \ldots, A_d\}$ is a basis for it. The multiplication of basis elements is given by

$$A_h A_i = \sum_{j=0}^{d} s_{hij} A_j \qquad (h, i \in \{0, 1, \ldots, d\}),$$

where the numbers s_{hij} are called *intersection numbers* of Γ, and they have the following combinatorial interpretation:

$$s_{hij} = |\{w \in V\Gamma \mid \partial(u, w) = h \text{ and } \partial(v, w) = i\}| \quad \text{whenever } \partial(u, v) = j.$$

The regular representation of $\mathcal{A}(\Gamma)$ assigns to each X in $\mathcal{A}(\Gamma)$ the $(d+1) \times (d+1)$ matrix $\bar{X}$ which represents left multiplication by X in $\mathcal{A}(\Gamma)$, with respect to the basis $\{A_0, A_1, ..., A_d\}$. In particular, the matrix $\bar{A}_h$ is the matrix whose entries are $(\bar{A}_h)_{ij} = s_{hji}$. Since the algebra $\mathcal{A}(\Gamma)$ is commutative, it is permissible to use the transpose of this representation, $\hat{X} = \bar{X}^t$; we write $B_h = \hat{A}_h$, so that $(B_h)_{ij} = s_{hij}$. The matrices $\hat{X}$, as X runs through $\mathcal{A}(\Gamma)$, constitute an algebra $\hat{\mathcal{A}}(\Gamma)$ isomorphic with $\mathcal{A}(\Gamma)$, and $\hat{\mathcal{A}}(\Gamma)$ has a basis $\{B_0, B_1, ..., B_d\}$.

The triangle inequality shows that the intersection numbers s_{1ij} are zero unless $|i - j| \leqslant 1$; these numbers are the entries of the matrix $B = B_1$ (that is, $B = \hat{A}$), and consequently B is a tridiagonal matrix. Writing $c_j = s_{1,j-1,1}$, $a_j = s_{1,j,j}$, $b_j = s_{1,j+1,j}$, we have

$$B = \begin{bmatrix} 0 & 1 & & & & \\ k & a_1 & c_2 & & & \\ & b_1 & a_2 & \cdot & & \\ & & b_2 & \cdot & \cdot & \\ & & & \cdot & \cdot & c_d \\ & & & & \cdot & a_d \end{bmatrix},$$

where some simple observations have been used to deduce that $a_0 = 0$, $c_1 = 1$, and $b_0 = k$ (the valency of Γ). Each column of this matrix has sum k, so that it is sufficient and convenient to specify only the two minor diagonals, and we write

$$\iota(\Gamma) = \{k, b_1, ..., b_{d-1}; 1, c_2, ..., c_d\},$$

which we call the *intersection array* of Γ. Of course, not every array is realized by a graph; for example there are only 12 trivalent distance-transitive graphs [3].

Let $\mathbb{Q}[\lambda]$ denote the ring of polynomials in λ with rational coefficients, and let $v_0(\lambda), v_1(\lambda), ..., v_d(\lambda)$ be the elements of $\mathbb{Q}[\lambda]$ defined by the recursion

$$v_0(\lambda) = 1, \qquad v_1(\lambda) = \lambda,$$

$$c_{i+1}v_{i+1}(\lambda) + (a_i - \lambda)\, v_i(\lambda) + b_{i-1}v_{i-1}(\lambda) = 0 \quad (i = 1, 2, ..., d-1).$$

We note that $v_i(\lambda)$ is a polynomial of degree i in λ, for $0 \leqslant i \leqslant d$. If we introduce the column vector

$$\mathbf{v}(\lambda) = [v_0(\lambda), v_1(\lambda),..., v_d(\lambda)]^t,$$

then the recursion equations are those which arise when we put $v_0(\lambda) = 1$ and try to solve the equation $B\mathbf{v}(\lambda) = \lambda\mathbf{v}(\lambda)$, using one row of B at a time; we call $\{v_i(\lambda)\}$ the *eigenvector sequence* of Γ. Our equations involve all rows of B except the last one, the equation which is derived from that row being

$$(a_d - \lambda)\, v_d(\lambda) + b_{d-1}v_{d-1}(\lambda) = 0.$$

This is a polynomial equation of degree $d+1$ in λ, and it gives the condition that $\mathbf{v}(\lambda)$ be an eigenvector of B corresponding to the eigenvalue λ. In other words, it is the characteristic equation of B. Using the recursion equations, we may rewrite it in the form

$$(\lambda - k)(v_0(\lambda) + v_1(\lambda) + \cdots + v_d(\lambda)) = 0.$$

The tridiagonal form of B implies that it has $d+1$ distinct eigenvalues $\lambda_0 = k, \lambda_1 ,..., \lambda_d$, and so the above equation is a rational multiple of $(\lambda - k)(\lambda - \lambda_1) \cdots (\lambda - \lambda_d) = 0$.

Now since $\mathfrak{A}(\Gamma)$ is the algebra of polynomials in A, each matrix A_i $(0 \leqslant i \leqslant d)$ is a polynomial in A, and in fact $A_i = v_i(A)$. To see this, we note the equations

$$A_0 = I, \qquad A_1 = A,$$
$$c_{i+1}A_{i+1} + a_iA_i + b_{i-1}A_{i-1} = AA_i \qquad (i = 1, 2,..., d-1),$$

which correspond to the equations defining the eigenvector sequence. Passing from $\mathfrak{A}(\Gamma)$ to the isomorphic algebra $\hat{\mathfrak{A}}(\Gamma)$ we deduce that

$$B_i = v_i(B) \qquad (0 \leqslant i \leqslant d).$$

Finally, if we distinguish one vertex z in Γ and define a $(d+1) \times n$ matrix T as follows:

$$(T)_{iu} = \begin{cases} 1, & \text{if } \partial(z, u) = i, \\ 0, & \text{otherwise,} \end{cases}$$

then a simple calculation shows that $TA = BT$. It follows that $TX = \hat{X}T$ for each X in $\mathfrak{A}(\Gamma)$.

3. Perfect Codes

Let Γ be a simple connected graph with distance function ∂, and for each non-negative integer e and each vertex v of Γ define

$$\textstyle\sum_e (v) = \{u \in V\Gamma \mid \partial(u, v) \leqslant e\}.$$

A *perfect e-code* in Γ is a subset C of $V\Gamma$ such that the sets $\sum_e (c)$, as c runs through C, form a partition of $V\Gamma$. The graph Γ always has a perfect 0-code ($C = V\Gamma$) and a perfect d-code ($|C| = 1$), where d is the diameter of Γ; we call these the *trivial* codes. Our aim is to investigate the existence of non-trivial perfect codes in distance-transitive graphs.

Let C be a perfect e-code in Γ, and let $\mathbf{c}$ be its representative column vector; that is, $(\mathbf{c})_v = 1$ if v belongs to C, $(\mathbf{c})_v = 0$ otherwise.

Lemma 1. *With the notation of Section* 2, *let* $S_e = A_0 + A_1 + \cdots + A_e$, *and* $\mathbf{u} = [1, 1,..., 1]^t$. *Then* $S_e\mathbf{c} = \mathbf{u}$.

Proof. This follows immediately from the definition of a perfect e-code. ∎

Lemma 2. *If Γ is a distance-transitive graph, and $\hat{S}_e$ is the image of S_e in $\mathcal{Q}(\Gamma)$, then the dimension of the kernel of $\hat{S}_e$ is at least e.*

Proof. We may suppose without loss of generality that the distinguished vertex z is in C. Choose vertices $u_0 = z, u_1 ,..., u_e$ such that $\partial(z, u_i) = i$ $(1 \leqslant i \leqslant e)$; then there are automorphisms $g_1 ,..., g_e$ of Γ such that $g_i(z) = u_i$ $(1 \leqslant i \leqslant e)$ and we have $e + 1$ perfect e-codes

$$C_0 = C, \qquad C_1 = g_1(C),..., C_e = g_e(C).$$

Let $\mathbf{c}_0 , \mathbf{c}_1 ,..., \mathbf{c}_e$ be the representative column vectors for these codes, and let T be the $(d + 1) \times n$ matrix defined at the end of Section 2. We shall show that the vectors $T\mathbf{c}_0 , T\mathbf{c}_1 ,..., T\mathbf{c}_e$ are linearly independent.

The j-th component of $T\mathbf{c}_i$ is

$$\sum_{u \in V\Gamma} (T)_{ju} (\mathbf{c}_i)_u = \sum_{c \in C_i} (T)_{jc} = |\{c \in C_i \mid \partial(z, c) = j\}|.$$

But, for $0 \leqslant j \leqslant e$, C_j contains one vertex (u_j) whose distance from z is j, whereas C_i $(i \neq j)$ contains no such vertices. Hence $(T\mathbf{c}_i)_j = \delta_{ij}$ for i, j in $\{0, 1,..., e\}$, and so the vectors $T\mathbf{c}_0 , T\mathbf{c}_1 ,..., T\mathbf{c}_e$ are linearly independent.

Now, since $\hat{S}_e T = TS_e$ we have

$$\hat{S}_e(T\mathbf{c}_0 - T\mathbf{c}_i) = TS_e(\mathbf{c}_0 - \mathbf{c}_i) = T(\mathbf{u} - \mathbf{u}) = \mathbf{0} \qquad (1 \leqslant i \leqslant e),$$

and so the kernel of $\hat{S}_e$ has dimension not less than e. ▮

4. The Existence Criterion

Let Γ be a distance-transitive graph of valency k and diameter d, and let $\{v_i(\lambda)\}$ be the associated eigenvector sequence. We shall state our main result in terms of the polynomials

$$x_i(\lambda) = v_0(\lambda) + v_1(\lambda) + \cdots + v_i(\lambda) \qquad (0 \leqslant i \leqslant d).$$

If we put $\lambda = k$, then $v_i(k) = k_i$ (the number of vertices whose distance from any given vertex is i) and so

$$x_e(k) = 1 + k_1 + \cdots + k_e = |\textstyle\sum_e (v)| \quad (v \in V\Gamma),$$

$$x_d(k) = 1 + k_1 + \cdots + k_d = |V\Gamma|.$$

Thus, if there is a perfect e-code in Γ, the number $x_e(k)$ must divide $x_d(k)$. Our theorem is a much stronger version of this result.

Theorem. *If there is a perfect e-code in the distance-transitive graph Γ of diameter d, then, in the ring $\mathbb{Q}[\lambda]$ we have the condition*:

$$x_e(\lambda) \quad \textit{divides} \quad x_d(\lambda).$$

Proof. Since $S_e = A_0 + A_1 + \cdots + A_e$, it follows that

$$\hat{S}_e = B_0 + B_1 + \cdots + B_e = v_0(B) + v_1(B) + \cdots + v_e(B) = x_e(B).$$

Hence the eigenvalues of $\hat{S}_e$ are $x_e(k), x_e(\lambda_1),\ldots, x_e(\lambda_d)$, where $k, \lambda_1 ,\ldots, \lambda_d$ are the eigenvalues of B. Now, by Lemma 2, at least e eigenvalues of $\hat{S}_e$ must be zero, so that the polynomial $x_e(\lambda)$ must have at least e zeros in the set $k, \lambda_1 ,\ldots, \lambda_d$. Since $x_e(\lambda)$ is a polynomial of degree e, and $x_e(k) \neq 0$, we may say that $x_e(\lambda)$ is a rational multiple of $(\lambda - \mu_1)(\lambda - \mu_2) \cdots (\lambda - \mu_e)$, where $\{\mu_1 , \mu_2 ,\ldots, \mu_e)$ is a subset of $\{\lambda_1 , \lambda_2 ,\ldots, \lambda_d)$.

Finally, we noted in Section 2 that $x_d(\lambda)$ is a rational multiple of $(\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_d)$, and, since both $x_e(\lambda)$ and $x_d(\lambda)$ are members of $\mathbb{Q}[\lambda]$, the result follows. ▮

The form of the theorem most suitable for practical application states that the e zeros of $x_e(\lambda)$ are eigenvalues of Γ. In the next section we shall recover the classical case of Lloyd's theorem in this form.

5. Application to the Classical Problem

Let q and m be natural numbers not less than two, and set $Q = \{1, 2, \ldots, q\}$. We define a graph $\Gamma(m, q)$, whose vertex-set is $Q \times Q \times \cdots \times Q = Q^m$, and in which two vertices are adjacent if and only if they differ in precisely one coordinate. It is straightforward to check that $\Gamma(m, q)$ is a distance-transitive graph with valency $m(q-1)$ and diameter m; its intersection array is

$$\{m(q-1), (m-1)(q-1), \ldots, (q-1); 1, 2, \ldots, m\}.$$

The recursion for the eigenvector sequence of $\Gamma(m, q)$ is:

$$v_0(\lambda) = 1, \qquad v_1(\lambda) = \lambda,$$

$$(i+1)\, v_{i+1}(\lambda) + \{i(q-2) - \lambda\}\, v_i(\lambda) + \{(m-i+1)(q-1)\}\, v_{i-1}(\lambda) = 0 \qquad (i = 1, 2, \ldots, m-1).$$

To find explicit expressions for these polynomials, we continue the sequence for all $i \geqslant 0$ by means of the same recursion, and introduce the generating function

$$V(\lambda, t) = \sum_{i=0}^{\infty} v_i(\lambda)\, t^i.$$

Multiplying the recursion equation by t^i and summing, we obtain the differential equation

$$\{1 + (q-2)\,t - (q-1)\,t^2\}\,\frac{\partial V}{\partial t} = \{\lambda - m(q-1)\,t\}\, V,$$

which, with the condition $V(\lambda, 0) = 1$, has the solution

$$V(\lambda, t) = (1 + (q-1)t)^{m-\zeta}(1-t)^{\zeta}.$$

Here we have put $\zeta = m - (m + \lambda)/q$, that is, $\lambda = m(q-1) - q\zeta$.

Now we require the polynomials $x_i(\lambda) = v_0(\lambda) + \cdots + v_i(\lambda)$, and we may suppose that this sequence also is continued for all $i \geqslant 0$, and put

$$X(\lambda, t) = \sum_{i=0}^{\infty} x_i(\lambda)\, t^i.$$

Then $X = V/(1 - t)$, so

$$X(\lambda, t) = (1 + (q - 1)t)^{m-\zeta}(1 - t)^{\zeta-1}.$$

It is clear from this expression that, if ζ is any one of the integers $1, 2,..., m$, then $X(\lambda, t)$ is a polynomial of degree $m - 1$ in t, and consequently $x_m(\lambda) = 0$. Thus $x_m(\lambda)$ is a rational multiple of $(\zeta - 1)(\zeta - 2) \cdots (\zeta - m)$.

The condition for a perfect e-code in $\Gamma(m, q)$ is that $x_e(\lambda)$ should divide $x_m(\lambda)$, or that the e zeros of $x_e(\lambda)$ should be zeros of $x_m(\lambda)$. The above expression for $X(\lambda, t)$ gives

$$x_e(\lambda) = \sum_{r=0}^{e} (-1)^r \binom{m - \zeta}{e - r}\binom{\zeta - 1}{r} (q - 1)^{e-r} \qquad (0 \leqslant e < m)$$

and so this must have e zeros corresponding to ζ in the set $\{1, 2,..., m\}$. We have recovered the classical form of Lloyd's theorem.

6. Conclusion

The results of this paper may be helpful in finding non-trivial perfect codes in distance-transitive graphs, other than the graphs $\Gamma(m, q)$. It would be particularly interesting to find perfect e-codes with $e > 1$; at the moment the only examples known are the Golay codes in the classical case (these are a 3-code in $\Gamma(23, 2)$ and a 2-code in $\Gamma(11, 3)$).

We know a few examples of perfect 1-codes in distance-transitive graphs. These examples are given in a paper by the present author, entitled "Perfect codes and distance-transitive graphs," to appear in the proceedings of the British Combinatorial Conference, Aberystwyth, July, 1973 (London Mathematical Society Lecture Notes Series).

References

1. N. L. Biggs, "Finite Groups of Automorphisms" (London Math. Society Lecture Notes, No. 6), Cambridge Univ. Press, London, 1971.
2. N. L. Biggs, "Algebraic Graph Theory" (Cambridge Math. Tracts, No. 67), Cambridge Univ. Press, London, 1974.
3. N. L. Biggs and D. H. Smith, On trivalent graphs, *Bull. London Math. Soc.* **3** (1971), 155–158.
4. M. J. E. Golay, Notes on digital coding, *Proc. IRE* **37** (1949), 657.
5. H. W. Lenstra, Two theorems on perfect codes, *Discrete Math.* **3** (1972), 125–132.
6. A. Tietäväinen, On the non-existence of perfect codes over finite fields, *SIAM J. Appl. Math.* **24** (1973), 88–96.
7. J. H. van Lint, "Coding Theory" (Lecture Notes in Math., No. 201), Springer-Verlag, New York/Berlin, 1971.