Discrete Mathematics 15 (1976) 175–184.

AN IMPROVED VERSION OF LLOYD'S THEOREM

D.H. SMITH

Department of Mathematics and Computer Science, Glamorgan Polytechnic, Treforest, Wales, U.K.

Received 12 December 1974
Revised 23 September 1975

The generalisation of Lloyd's theorem to distance-transitive graphs can be improved in the case of antipodal graphs by looking at the derived graph. In the case of binary perfect codes the roots of the Lloyd polynomial are even integers. This can be applied to give a short proof of the binary perfect code theorem.

1. Introduction

In this paper we show that the generalisation of Lloyd's theorem to distance-transitive graphs given by Biggs [1] can be improved in the case of an antipodal distance-transitive graph. In particular, this shows that the roots of the Lloyd polynomial in the case of binary perfect codes are all even integers.

As an example we give a simple proof that there are no non-trivial perfect binary e-codes with $e \geqslant 2$ other than the binary Golay code. The proof has the advantage that it deals with all values of $e \geqslant 2$ simultaneously and does not require a reference to a computer search.

2. Antipodal 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 $g(u) = x$, $g(v) = y$. We suppose that Γ has diameter d, valency k, vertex set $V\Gamma$ and, if we fix a vertex z, we let

We call a distance-transitive graph *antipodal* if for all $u, v \in \Gamma_0(z) \cup \Gamma_d(z)$ either $\partial(u, v) = d$ or $u = v$. For an account of the basic results on antipodal distance-transitive graphs we refer the reader to [9].

For an antipodal distance-transitive graph Γ we can define a *derived graph* Γ'. The vertices of Γ' are the sets $\Gamma_0(z) \cup \Gamma_d(z)$ $(z \in V\Gamma)$, and vertices $\Gamma_0(z) \cup \Gamma_d(z)$ and $\Gamma_0(z') \cup \Gamma_d(z')$ are adjacent in Γ' if and only if there are vertices $v \in \Gamma_0(z) \cup \Gamma_d(z)$ and $v' \in \Gamma_0(z') \cup \Gamma_d(z')$ such that $\partial(v, v') = 1$ in Γ. It is proved in [9, Lemma 7 and Theorem 3] that if $d > 2$, Γ' is distance-transitive with valency k and diameter $[\frac{1}{2}d]$.

If u, v are two vertices of a distance-transitive graph Γ such that $\partial(u, v) = i$ we define the *intersection numbers*

$$c_i = |\Gamma_{i-1}(u) \cap \Gamma_1(v)|,$$

$$a_i = |\Gamma_i(u) \cap \Gamma_1(v)|,$$

$$b_i = |\Gamma_{i+1}(u) \cap \Gamma_1(v)|,$$

and define the *intersection matrix* of the graph to be the $(d+1) \times (d+1)$ tridiagonal matrix with main diagonals given by the intersection array

$$\begin{Bmatrix} * & 1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & * \end{Bmatrix}.$$

For a full account of properties of the intersection matrices of distance-transitive graphs see [2].

Lemma 2.1. *If $d > 2$ and the derived graph Γ' of Γ has intersection numbers c_i', a_i', b_i', then for $1 \leqslant i < [\frac{1}{2}d]$, $c_i' = c_i$, $a_i' = a_i$, $b_i' = b_i$.*

Proof. This follows easily from [9, Lemma 8] (see Appendix 2). A proof may be found in [3, Proposition 4.2].

3. Perfect codes in antipodal distance-transitive graphs

Let $\Sigma_e(v) = \{u \in V\Gamma: \partial(u, v) \leqslant e\}$. A *perfect e-code* in Γ is a subset C of $V\Gamma$ such that the sets $\Sigma_e(c)$ $(c \in C)$ form a partition of $V\Gamma$. In [1] Biggs defines the *eigenvector sequence* $\{v_i(\lambda)\}$ by

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

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

If $x_e(\lambda) = \Sigma_{i=0}^{e} v_i(\lambda)$ then the principal result of [1] is that if Γ contains a perfect e-code then the roots of $x_e(\lambda)$ are eigenvalues of the intersection matrix of Γ.

The following two lemmas have been proved independently by Heden [6].

Lemma 3.1. *If Γ is an antipodal distance-transitive graph containing a perfect code C then if $u \in C$ every vertex of $\Gamma_d(u)$ is in C.*

Proof. This is the remark following Theorem 1 of [5].

Lemma 3.2. *If there exists a perfect e-code C in the antipodal distance-transitive graph Γ, then the set of vertices $\Gamma_0(c) \cup \Gamma_d(c)$ $(c \in C)$ of Γ' is a perfect e-code C' in Γ'.*

Proof. The result is clear if $d = 2e + 1$. Suppose $d > 2e + 1$ and suppose that vertices $\Gamma_0(c_1) \cup \Gamma_d(c_1)$, $\Gamma_0(c_2) \cup \Gamma_d(c_2)$ in C' are at distance $f < 2e + 1$ in Γ'. From [9, Lemma 3] (see Appendix 2) we see that

$$\Gamma_0(c_2) \cup \Gamma_d(c_2) \subset \Gamma_f(c_1) \cup \Gamma_{d-f}(c_1)$$

and so there exist $c_3 \in \Gamma_0(c_1) \cup \Gamma_d(c_1)$, $c_4 \in \Gamma_0(c_2) \cup \Gamma_d(c_2)$ such that $\partial(c_3, c_4) = f < 2e + 1$ in Γ, which is impossible.

Also $|C'| = |C|/(k_0 + k_d)$, $|V\Gamma'| = |V\Gamma|/(k_0 + k_d)$ and it follows from Lemma 2.1 that, if $d > 2e + 1$, the number of vertices in the spheres of radius e is the same in both cases and so the code C' is perfect.

Lemma 3.3. *If Γ is an antipodal distance-transitive graph with derived graph Γ' then the polynomial $x_e(\lambda)$ is the same in both cases $(e < \frac{1}{2}(d-1))$*

Proof. This follows immediately from Lemma 2.1.

Theorem 3.4. *If an antipodal distance-transitive graph Γ contains a perfect e-code C $(e < \frac{1}{2}(d-1))$ then the roots of the polynomial $x_e(\lambda)$ are eigenvalues of the derived graph Γ'.*

Proof. This follows from Lemma 3.3, Lemma 3.2 and an application of Biggs' result to the graph Γ'.

Since the intersection matrix of Γ has $d+1$ eigenvalues and the intersection matrix of Γ' has $[\frac{1}{2}(d+2)]$ eigenvalues the result of Theorem 3.4 will be a stronger result than that given by Biggs.

Note. Hammond [4] has extended the definition of nearly perfect codes to distance-transitive graphs and proved an analogue of Biggs' result. He proves a result similar to our Lemma 3.2 for a nearly perfect code in an antipodal graph with $k_d < k_e/k$. By looking at the derived graph in the same way as we have done for perfect codes a similar improvement in Hammond's main result is possible. The improvement applies to nearly perfect binary codes.

4. Lloyd's theorem for binary perfect codes

Using the same notation as [1] we let $Q = \{1, 2, \ldots, q\}$ and define a graph $\Gamma(n, q)$ whose vertex set is Q^n, and in which two vertices are adjacent if and only if they differ in precisely one coordinate. $\Gamma(n, q)$ is distance-transitive. If $q > 2$, $\Gamma(n, q)$ is not antipodal, but $\Gamma(n, 2)$ which corresponds to the case of binary codes is antipodal and so Theorem 3.4 applies.

The derived graph of $\Gamma(n, 2)$, which we denote by $\Gamma(n, 2)/2$, has intersection array

$$\begin{Bmatrix} * & 1 & 2 & \ldots & \frac{1}{2}(n-3) & \frac{1}{2}(n-1) \\ 0 & 0 & 0 & \ldots & 0 & \frac{1}{2}(n+1) \\ n & n-1 & n-2 & \ldots & \frac{1}{2}(n+3) & * \end{Bmatrix} \qquad (n \text{ odd}),$$

or

$$\begin{Bmatrix} * & 1 & 2 & \ldots & \frac{1}{2}n-1 & n \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ n & n-1 & n-2 & \ldots & \frac{1}{2}n+1 & * \end{Bmatrix} \qquad (n \text{ even}).$$

Lemma 4.1. *The eigenvalues of the intersection matrix of* $\Gamma(n, 2)/2$ *are*

$$n, -n, n-4, -(n-4), \ldots, 4, -4, 0 \qquad (n \equiv 0 \pmod 4),$$

$$n, -(n-2), n-4, -(n-6), \ldots, -3, 1 \qquad (n \equiv 1 \pmod 4),$$

$$n, -n, n-4, -(n-4), \ldots, 6, -6, 2, -2 \qquad (n \equiv 2 \pmod 4),$$

$$n, -(n-2), n-4, -(n-6), \ldots, 3, -1 \qquad (n \equiv 3 \pmod 4).$$

Proof. See Appendix 1.

Now let

$$\psi_e(x) = \sum_{i=0}^{e} (-1)^i \binom{n-x}{e-i}\binom{x-1}{i}$$

denote the Lloyd polynomial in the binary case. It is shown in [1, Section 5] that $x_e(\lambda) = \psi_e(x)$ where $x = \frac{1}{2}(n - \lambda)$. Then Theorem 3.4, Lemma 4.1 and $x = \frac{1}{2}(n - \lambda)$ give us:

Theorem 4.2. *If $\Gamma(n, 2)$ contains a perfect e-code then the roots of $\psi_e(x)$ are even integers in $[1, n]$.*

5. The binary perfect code theorem

We can use Theorem 4.2 to give a short unified proof that the Golay code is the only non-trivial binary perfect e-code with $e \geqslant 2$ (see [7, 10]).

We suppose that $e \geqslant 2$ and, to exclude trivial codes, $n > 2e + 1$. The necessary conditions for the existence of a perfect e-code that we shall use are Theorem 4.2 and the sphere packing condition

$$\sum_{i=0}^{e} \binom{n}{i} = 2^K \,. \tag{5.1}$$

$\psi_e(x)$ and its zeros $x_1 < x_2 < \ldots < x_e$ have the following properties [7]:

$$\psi_e(0) = \sum_{i=0}^{e} \binom{n}{i} \,, \tag{5.2}$$

$$\psi_e(1) = \binom{n-1}{e} \,, \tag{5.3}$$

$$\sum_{i=1}^{e} x_i = \tfrac{1}{2} e(n+1) \,, \tag{5.4}$$

$$\prod_{i=1}^{e} x_i = e!\, 2^{-e}\, \psi_e(0) \,, \tag{5.5}$$

$$\prod_{i=1}^{e} (x_i - 1) = e!\, 2^{-e}\, \psi_e(1) \,. \tag{5.6}$$

$$(5.7)\qquad \prod_{i=1}^{e}(x_i - 2) = e!\,2^{-e}\,\psi_e(2)$$
$$= (n-2e-1)\,2^{-e}(n-2)(n-3)\ldots(n-e)\,.$$

We follow initially the method of [7].

Lemma 5.1. *If* $\Gamma(n,2)$ *contains a perfect e-code* $(e \geqslant 2)$ *then* $n < \frac{1}{2}(17e^2) + \frac{1}{2}e - 1$.

Proof. Let $a_2(n) = \max\{m \in \mathbf{N}: m \mid n,\ 2 \nmid m\}$ and define n_1 and n_2 to be 2-equivalent if $a_2(n_1) = a_2(n_2)$. Let C be a perfect e-code $(e < \frac{1}{2}(n-1))$. From (5.1), (5.2), (5.5) we have

$$(5.8)\qquad \prod_{i=1}^{e} x_i = e!\,2^{K-e}$$

and so $a_2(x_1)\,a_2(x_2)\ldots a_2(x_e) = a_2(e!) < e!$.

It follows that two of the zeros x_i, x_j which are 2-equivalent and so $2x_1 \leqslant x_e$ which gives

$$(5.9)\qquad x_1 x_e \leqslant \tfrac{1}{9}(x_1 + x_e)^2\,.$$

From (5.2), (5.5), (5.9) and the arithmetic-geometric mean inequality we have

$$(5.10)\qquad 2^{-e}n(n-1)\ldots(n-e+1) < e!\,2^{-e}\psi_e(0)$$
$$= \prod_{i=1}^{e} x_i \leqslant \tfrac{8}{9}\left(\frac{x_1+x_e}{2}\right)^2\left(\frac{x_2+x_3+\ldots+x_{e-1}}{e-2}\right)^{e-2}$$
$$\leqslant \tfrac{8}{9}\left(\frac{x_1+\ldots+x_e}{e}\right)^e \leqslant \tfrac{8}{9}\left(\frac{n+1}{2}\right)^e\,.$$

Hence

$$\left(\frac{n-e+1}{n+1}\right)^e < \frac{n(n-1)\ldots(n-e+1)}{(n+1)^e} < \tfrac{8}{9}$$

so $n < e/[1-(\frac{8}{9})^{1/e}] - 1$. Since

$$(1-\tfrac{1}{9})^{1/e} = 1 - \frac{1}{9e} + \frac{1}{2!9\cdot 9}\,\frac{1}{e}\left(\frac{1-e}{e}\right)$$

$$- \frac{1}{3!9\cdot 9\cdot 9} \frac{1}{e} \left(\frac{1-e}{e}\right)\left(\frac{1-2e}{e}\right) + \dots ,$$

$$1-(\tfrac{8}{9})^{1/e} > \frac{1}{9e}\sum_{i=0}^{\infty}\frac{(e-1)^i\, 9^{-i}e^{-i}}{(i+1)} > \frac{1}{9e}\sum_{i=0}^{\infty}(e-1)^i\, 9^{-i}e^{-i}2^{-i}$$

$$= \frac{2}{17e+1},$$

and we have

(5.11) $\quad n < \tfrac{1}{2}(17e^2) + \tfrac{1}{2}e - 1 .$

Lemma 5.2. *If* $\Gamma(n, 2)$ *contains a perfect* e*-code with* $n > 2e + 1$ *and* $e \geqslant 2$ *then* $n = 2^{e+1}s + 2e + 1$ $(s = 1, 2, \dots)$ *and so* $n \geqslant 2^{e+1} + 2e + 1$.

Proof. From (5.3), (5.6), (5.7),

$$\prod_{i=1}^{e}(x_i - 2)/\prod_{i=1}^{e}(x_i - 1) = \psi_e(2)/\psi_e(1) = (n - 2e - 1)/(n - 1)$$

and then since Theorem 4.2 tells us that $x_1, \dots, x_e$ are all even integers we see that n is odd and so $2^{e+1} \mid (n - 2e - 1)$ and the result follows.

We note that if $n - 1 = 2^h a_2(n - 1)$ then

(5.12) $\quad 2^{e+h} \mid (n - 2e - 1) .$

Table 1

e	Bound of (5.11)	$n = 2^{e+1}s + 2e + 1$	Values remaining after applying (5.12)	Values remaining after applying (5.10)	Values remaining after applying (5.1)
2	$n < 34$	13 21 29	21	21	–
3	$n < 77$	23 39 55 71	23 39 55 71	23 39	23
4	$n < 139$	41 73 105 137	137	–	–
5	$n < 214$	75 139 203	75 139 203	75	–
6	$n < 308$	141 269	269	–	–
7	$n < 419$	271	271	–	–
8	$n < 547$	529	–	–	–

Combining the results of Lemma 5.1 and Lemma 5.2 we see that no perfect e-code with $n > 2e + 1$ can exist with $e \geqslant 9$. To deal with the cases $2 \leqslant e \leqslant 8$ we have only to consider the values of n of the form $2^{e+1}s + 2e + 1$ ($s = 1, 2, \ldots$) with $n < \frac{1}{2}(17e^2) + \frac{1}{2}e - 1$. These can be eliminated as shown in Table 1. Hence we have

Theorem 5.3. *The Golay code with $n = 23$, $e = 3$ is the only non-trivial binary perfect code with $e \geqslant 2$.*

Appendix 1. Proof of Lemma 4.1

Let $B^{(n)}$ denote the intersection matrix of $\Gamma(n, 2)/2$ and let $\Delta_n = |B^{(n)} - \lambda I|$ ($B^{(n)}$ has $[\frac{1}{2}n] + 1$ rows).

Case 1: n odd. $B^{(3)}$ has eigenvalues 3, -1, $B^{(5)}$ has eigenvalues 5, -3, 1.

Add row i to row $i + 2$ starting from the beginning and then subtract column $j + 2$ from column j starting from the beginning. Adding the penultimate row to the last row and substracting the last column from the penultimate column we obtain

$$\Delta_n = (n - \lambda)\begin{vmatrix} -\lambda & 1 & & & 0 & \\ n-2 & -\lambda & 2 & & & \\ & n-3 & -\lambda & 3 & & \\ & & & \ddots & & \\ & & & & -\lambda & \frac{1}{2}(n-3) \\ 0 & & & & \frac{1}{2}(n+1) & -\lambda - \frac{1}{2}(n-1) \end{vmatrix}$$

and we note that the determinant is the same as Δ_{n-2} except that the element in the last row and column is $-\lambda - \frac{1}{2}(n - 1)$ instead of $-\lambda + \frac{1}{2}(n - 1)$. Again, add row i to row $i + 2$ starting from the beginning and subtract column $j + 2$ from column j starting from the beginning. Subtract the penultimate row from the last row and add the last column to the penultimate column, and we obtain $\Delta_n = (n - \lambda)(-(n - 2) - \lambda)\,\Delta_{n-4}$ and the result follows.

Case 2: n even. $B^{(4)}$ has eigenvalues 0, 4, -4, $B^{(6)}$ has eigenvalues 6, -6, 2, -2.

Add row i to row $i + 2$ starting from the beginning, subtract column

$j+2$ from column j starting from the beginning and we obtain

$$\Delta_n = (\lambda^2 - n^2)\begin{vmatrix} -\lambda & 1 & & & & 0 \\ n-2 & -\lambda & 2 & & & \\ & n-3 & -\lambda & 3 & & \\ & & & \ddots & & \\ & & & & -\lambda & \frac{1}{2}n-2 \\ 0 & & & & \frac{1}{2}n+1 & -\lambda \end{vmatrix}.$$

Repeat the above operations and we obtain

$$\Delta_n = (\lambda^2 - n^2)\begin{vmatrix} -\lambda & 1 & & & & 0 \\ n-4 & -\lambda & 2 & & & \\ & n-5 & -\lambda & 3 & & \\ & & & \ddots & & \\ & & & & -\lambda & \frac{1}{2}n-3 \\ & & & & \frac{1}{2}n & -\lambda & \frac{1}{2}n-2 \\ 0 & & & & & n-2 & -\lambda \end{vmatrix}$$

Since $(n-4)(\frac{1}{2}n-1) = (n-2)(\frac{1}{2}n-2)$ the determinant is equal to Δ_{n-4} and we obtain $\Delta_n = (\lambda^2 - n^2)\,\Delta_{n-4}$.

Appendix 2.

For the convenience of the reader we repeat here the statement of [9, Lemma 8]. *If Γ is an antipodal distance-transitive graph ($d > 2$) then for $i = 1, 2, \ldots, [\frac{1}{2}(d-1)]$, $\Gamma_i(u)$ consists of one vertex from each of k_i distinct sets $\Gamma_0(u_j) \cup \Gamma_d(u_j)$ ($j = 1, 2, \ldots, k_i$) and*

$$\Gamma_{d-i}(u) = \left\{ \bigcup_{j=1}^{k_i} (\Gamma_0(u_j) \cup \Gamma_d(u_j)) \setminus \Gamma_i(u) \right\}.$$

Acknowledgment

I am grateful to O. Heden for a copy of [6] and for pointing out to me that Theorem 4.2 can also be obtained from a result of Roos [8].

References

[1] N.L. Biggs, Perfect codes in graphs, J. Combin. Theory 15 (B) (1973) 289–296.
[2] N.L. Biggs, Algebraic Graph Theory (Cambridge Univ. Press, London, 1974).

[3] A. Gardiner, Antipodal covering graphs, J. Combin. Theo. 16 (B) (1974) 255–273.
[4] P. Hammond, Nearly perfect codes in distance-regular graphs, Discrete Math. 14 (1976) 41–56.
[5] P. Hammond and D.H. Smith, Perfect codes in the graphs O_k, J. Combin. Theory 19 (B) (1975) 239–255.
[6] O. Heden, Perfect codes in antipodal distance-transitive graphs, unpublished.
[7] J.H. van Lint, Recent results on perfect codes and related topics, in: Proc. Advanced Study Institute, Nijenrode Castle, Breukelen, Mathematical Centre Tracts 55 (Mathematical Centre, Amsterdam, 1974) 158–178.
[8] J.E. Roos, An algebraic study of group and nongroup error-correcting codes, Information and Control 8 (1965) 195–214.
[9] D.H. Smith, Primitive and unprimitive graphs, Quart. J. Math. Oxford (2) 22 (1971) 551–557.
[10] A. Tietäväinen and A. Perko, There are no unknown perfect binary codes, Ann. Univ. Turku. Ser. A. I (1971) 148.