MATHEMATICS

AN ELEMENTARY PROOF OF LLOYD'S THEOREM

BY

D. M. CVETKOVIĆ AND J. H. VAN LINT

(Communicated at the meeting of September 25, 1976)

1. INTRODUCTION

Consider a set $\mathbf{F}$ of q distinct symbols which we call the *alphabet*. The elements of $\mathbf{F}^n$ will be called *words* of *length* n. Hamming distance d in $\mathbf{F}^n$ is defined by

$$d(\underline{x}, \underline{y}) := \#\{i | x_i \neq y_i,\ 1 \leqslant i \leqslant n\}.$$

A subset C of $\mathbf{F}^n$ is called a *perfect e-code* if the spheres

$$S_e(\underline{c}) := \{\underline{x} \in \mathbf{F}^n | d(\underline{x}, \underline{c}) \leqslant e\},$$

where $\underline{c}$ runs through C, form a partition of $\mathbf{F}^n$. We define the distance $d(\underline{x}, C)$ of $\underline{x}$ to the code C by

$$d(\underline{x}, C) := \min\{d(\underline{x}, \underline{c}) | \underline{c} \in C\}$$

and we denote by C_i the set

$$C_i := \{\underline{x} \in \mathbf{F}^n | d(\underline{x}, C) = i\},\ (i = 0, 1, \ldots, e).$$

Observe that if C is a perfect e-code then the sets C_i, $i = 0, 1, \ldots, e$, form a partition of the space $\mathbf{F}^n$.

In 1957 S. P. Lloyd (cf. [7]) proved a strong necessary condition for the existence of a binary (i.e. $q = 2$) perfect e-code. This theorem was generalized to the case where q is a prime power by F. J. Mac Williams (cf. [8]) and recast by A. M. Gleason (cf. Van Lint [6]). Recently P. Delsarte [4], H. W. Lenstra [5] and L. A. Bassalygo [1] proved that the theorem, which is always referred to as *Lloyd's Theorem*, holds for all q. Other generalizations were given by N. L. Biggs [2] and by D. H. Smith [10]. Although the proofs are not extremely difficult they usually involve a lot of algebraic background. In this paper we shall give a simple proof of Lloyd's Theorem which requires no further knowledge than the definitions given in this introduction and the concepts of eigenvector and eigenvalue of a square matrix (cf. [2]).

A stronger version of lemma 3.2, on which our proof is actually based, has been used in graph theory for the investigation of the existence of partitions of the vertex set of a graph, which have some properties like those of the partition $C_0, C_1, \ldots, C_e$ (see, for example, [3]). On the other hand, coding theory problems can be formulated in terms of graphs (cf. [9]) but it is not necessary, especially not in the context of this paper.

In section 2 we shall give some lemmas on matrices and do the calculations necessary for our proof. In section 3 we state Lloyd's Theorem and give the elementary proof of this theorem.

2. LEMMAS ON MATRICES

(2.1) DEFINITION: The square matrix A_k of size q^k is defined as follows. Number the rows and columns by the q-ary system from 0 to q^k-1. The entry $A_k(i,j)$ is 1 if the representations of i and j differ in exactly one digit, otherwise $A_k(i,j)=0$.

Observe that we can identify the q-ary representation of the integers 0 to q^k-1 with the elements of $\mathbf{F}^k$, where $\mathbf{F}=\{0, 1, \ldots, q-1\}$. In this terminology $A_k(i,j)=1$ if the elements corresponding to i and j have Hamming distance 1.

From the definition of A_k it is clear that

$$A_{k+1}=I_q\times(A_k-I_{q^k})+J_q\times I_{q^k}, \tag{2.2}$$

where as usual I_m denotes the identity matrix of size m, J_m the all one matrix of size m and $\times$ indicates the Kronecker product.

(2.3) LEMMA: The matrix A_k has the eigenvalues

$$-k+jq \quad (j=0, 1, \ldots, k)$$

with multiplicities

$$\binom{k}{j}(q-1)^{k-j}.$$

PROOF: The proof is by induction. For $k=1$ we have $A_1=J_q-I_q$ and then the assertion is well known. Now let the columnvector $\underline{x}$ be eigenvector of A_k belonging to the eigenvalue λ. Then by (2.2) we have

$$A_{k+1}(\underline{x}^T, \underline{x}^T, \ldots, \underline{x}^T)^T=(\lambda+q-1)(\underline{x}^T, \underline{x}^T, \ldots, \underline{x}^T)^T \tag{2.4}$$

(where on both sides $\underline{x}^T$ is repeated q times). If $(c_1, \ldots, c_q)^T$ is eigenvector of J_q with eigenvalue 0 (which eigenvalue has multiplicity $q-1$) then

$$A_{k+1}(c_1\underline{x}^T, c_2\underline{x}^T, \ldots, c_q\underline{x}^T)^T=(\lambda-1)(c_1\underline{x}^T, \ldots, c_q\underline{x}^T) \tag{2.5}$$

because $\sum c_i = 0$. The induction step now follows from (2.4) and (2.5) and well-known properties of binomial coefficients. □

The technically most difficult part of our proof is determining the eigenvalues of certain tridiagonal matrices occuring in the next section. To keep the notation compact we use the following definition.

(2.6) DEFINITION: The matrix $Q_e = Q_e(a, b, s)$ is the tridiagonal matrix given by

$$Q_e(a,b,s) := \begin{pmatrix} a & b & 0 & \cdots & 0 \\ 1 & a+(s-1) & b-s & \ddots & \vdots \\ 0 & 2 & a+2(s-1) & \ddots & 0 \\ 0 & 0 & \ddots & \ddots & b-(e-1)s \\ \vdots & \ddots & \ddots & e & a+e(s-1) \\ 0 & \cdots & 0 & & \end{pmatrix}$$

Furthermore we define

$$P_e = P_e(a,b,s) := \left(\begin{array}{ccc|c} & & & 1 \\ & Q_{e-1}(a,b,s) & & 1 \\ & & & \vdots \\ \hline 0 & 0 & \cdots\ 0\ e & 1 \end{array}\right).$$

The determinants of these matrices are denoted by $\bar{Q}_e$, resp. $\bar{P}_e$. Developing by the last row we find from (2.6)

$$\bar{Q}_e = (a+e(s-1))\bar{Q}_{e-1} - e(b-(e-1)s)\bar{Q}_{e-2}. \tag{2.7}$$

By adding all columns to the last one we find, developing by the last row

$$\bar{Q}_e = (a+es)\bar{Q}_{e-1} - e(a+b)\bar{P}_{e-1}. \tag{2.8}$$

Developing P_e by the last row yields

$$\bar{P}_e = \bar{Q}_{e-1} - e\bar{P}_{e-1}. \tag{2.9}$$

Now apply (2.9) with $e+1$ instead of e, combine with (2.9) and eliminate the $\bar{Q}$-terms using (2.8). This yields

$$\bar{P}_{e+1} = (a+es-e-1)\bar{P}_e - e(b-es)\bar{P}_{e-1}. \tag{2.10}$$

The recurrence relation (2.10) relates the determinants to well known polynomials which we now introduce.

(2.11) DEFINITION: The *Krawtchouk polynomial* K_k is defined by

$$K_k(n, u) := \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{u}{j} \binom{n-u}{k-j}.$$

We shall call the polynomial ψ_e defined by

$$\psi_e(n, x) := K_e(n-1, x-1)$$

Lloyd's polynomial of degree e.

Using well known recurrence relations for Krawtchouk polynomials (cf. e.g. [4], (4.11)) we find for the Lloyd polynomials

(2.12) $(e+1)\psi_{e+1}(n, x) =$
$$= \{e + (q-1)(n-e) - qx + 1\}\psi_e(n, x) - (q-1)(n-e)\psi_{e-1}(n, x).$$

(2.13) LEMMA: Let $s := q-1$. Then we have

$$\bar{P}_e(qy - ns, ns, s) = (-1)^e e! \psi_e(n, y)$$

PROOF: For $e=1$ and $e=2$ it is easy to check the assertion using the definitions. By substitution of the appropriate values of a and b in (2.10) and using (2.12) we see that the polynomials on both sides in (2.13) satisfy the same recurrence relation. This proves the lemma. □

3. LLOYD'S THEOREM

We first state the theorem.

(3.1) THEOREM: If a perfect e-code of length n over an alphabet of q symbols exists, then $\psi_e(n, x)$ has e distinct integral zeros among 1, 2, ..., n.

The fact that the zeros are distinct is a well known property of Krawtchouk polynomials. The interesting fact is that they are integers. The proof of (3.1) is a simple consequence of the following practically trivial lemma.

(3.2) LEMMA: Let A be a matrix of size m by m which has the form

$$A = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1k} \\ A_{21} & A_{22} & \dots & A_{2k} \\ \dots & \dots & \dots & \dots \\ A_{k1} & A_{k2} & \dots & A_{kk} \end{pmatrix}$$

where A_{ij} has size m_i by m_j ($i = 1, 2, \dots, k$; $j = 1, 2, \dots, k$). Suppose that for each i and j the matrix A_{ij} has constant row sums with sum b_{ij}. Let the matrix B have entries b_{ij}. Then each eigenvalue of B is also an eigenvalue of A.

PROOF: Let $B\underline{x} = \lambda \underline{x}$, where $\underline{x} = (x_1, x_2, \dots, x_k)^T$. Define $\underline{y}$ by

$$\underline{y}^T := (x_1, x_1, \dots, x_1, x_2, x_2, \dots, x_2, \dots, x_k, x_k, \dots, x_k)$$

where each x_i is repeated m_i times. By definition of B it is obvious that $A\underline{y} = \lambda \underline{y}$. □

We now prove Lloyd's Theorem. Assume that C is a perfect e-code of length n over an alphabet $\mathbf{F}$ of q symbols, for which we can take $\mathbf{F} = \{0, 1, \ldots, q-1\}$. Now consider the matrix A_n as defined in (2.1) where again we identify row and column numbers with elements of $\mathbf{F}^n$. We reorder the rows and columns of A_n as follows. First take the rows and columns with a number corresponding to an element of C, then successively those with numbers corresponding to elements of C_i $(i = 1, 2, \ldots, e)$. Since C is a perfect code the matrix A_n now has the form of lemma 3.2 with

(3.3) $B =$

0	ns	0	0	⋯	⋯	⋯	0	
1	$q-2$	$(n-1)s$	0	⋯	⋯	⋯	0	
0	2	$2(q-2)$	$(n-2)s$	⋯	0	⋯	0	
⋮				⋰				
				$e-1$	$(e-1)(q-2)$	$(n-e+1)s$		
⋮								
0	⋯	⋯	⋯	0	e	$ns-e$		

where $s := q-1$. We now apply lemma 3.2. The eigenvalues of A_n were determined in lemma 2.3. In $\det(B - xI_{e+1})$ we substitute $x = ns - yq$ which leads to the problem of determining $\overline{P}_e(qy - ns, ns, s)$. Then Lloyd's Theorem follows from lemma 2.13. □

Department of Mathematics
Technological University, Eindhoven

REFERENCES

1. Bassalygo, L. A. – Generalization of Lloyd's Theorem to Arbitrary Alphabet, Problems of Control and Information Theory **2**, 25–28 (1973).
2. Biggs, N. L. – Perfect Codes in Graphs, J. Comb. Theory B **15**, 289–296 (1973).
3. Petersdorf, M. and H. Sachs – Spektrum und Automorphismengruppe eines Graphen, Combinatorial Theory and its Application, III (ed. P. Erdös, A. Rényi, V. T. Sos), Budapest, 891–907 (1970).
4. Delsarte, P. – An Algebraic Approach to the Association Schemes of Coding Theory, Philips Res. Repts. Suppl. **10** (1973).
5. Lenstra, H. W. – Two Theorems on Perfect Codes, Discr. Math. **3**, 125–132 (1972).
6. Lint, J. H. van – Coding Theory, Springer Verlag, Berlin (1971).
7. Lloyd, S. P. – Binary Block Coding, Bell System Tech. J. **36**, 517–535 (1957).
8. Mac Williams, F. J. – Ph.D. Dissertation, Harvard Univ. (1961).
9. Cvetković, D. – Spectrum of the Graph of n-tuples, Univ. Beograd, Publ. Elektrotehn. Fak., Ser. Mat. Fiz., No. 274–No. 301, 91–95 (1969).
10. Smith, D. H. – An Improved Version of Lloyd's Theorem, Discr. Math. **15**, 175–184 (1976).