The Lee association scheme

P. Sole

CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

N° 591

THE LEE ASSOCIATION SCHEME

Patrick SOLE

Décembre 1986

THE LEE ASSOCIATION SCHEME

ETUDE DU SCHEMA D'ASSOCIATION DE LEE

Patrick SOLE

INRIA
Domaine de Voluceau
ROCQUENCOURT - B.P. 105
78153 LE CHESNAY CEDEX
FRANCE

PAPIER RÉCUPERÉ ET RECYCLÉ

Abstract :

In this paper we undertake a study of the Lee scheme. We give in this context a new proof of Bassalygo's generalization of Lloyd Theorem, and an asymptotic estimate of the number of zeroes of the Lloyd polynomial.

We obtain a recursion on the Lee composition distribution of the translates of a code and deduce from that an upper bound on the covering radius of a code.

We give an algebraic characterization of T-designs in this scheme, which shows that they form a special class of orthogonal arrays.

Résumé :

Dans ce travail, nous étudions le schéma d'association de Lee. Nous donnons dans ce contexte une nouvelle preuve de la généralisation par Bassalygo du théorème de Lloyd à la métrique de Lee, et une évaluation asymptotique du nombre de racines du polynôme de Lloyd.

Nous obtenons une récurrence sur la distribution de la composition de Lee des translatés d'un code, et nous en déduisons une borne supérieure sur le rayon de recouvrement d'un code.

Nous donnons une caractérisation algébrique des T-designs dans ce schéma, qui montre qu'ils forment une classe spéciale de tableaux orthogonaux.

Introduction :

The Lee metric was first introduced by Lee in [12], wich concerns mainly the topic of perfect codes, as several papers from Golomb [10], [11]. A class of negacyclic perfect codes and an engineering motivation can be found in the classical book by Berlekamp [5].

In his thesis [9], Delsarte shown that the concept of an association scheme was a natural framework to coding theory. He introduced the Hamming scheme to study the Hamming metric, and gave the definition of the Lee scheme.

In this paper we make a comparison between the two schemes, and generalize some properties of the former to the latter.

1. The Lee Metric :

Let Z_q (residues modulo q) be taken as an alphabet. We define the weight of a symbol k by :

$$W_L(k) = \text{Max}\ \{k,\ q-k\}$$

By suitably numbering the vertices of the q-gon we see that $W_L(k)$ is the length of the shortest path from 0 to k on this graph.

Then we equip the cartesian product Z_q^n with a metric by the formula :

$$d_L(x,y) = \sum_{i=1}^{n} W_L\ (|y_i-x_i|).$$

2. The Notion of association scheme :

An association scheme with t classes, in the Bose Mesner sense, [7] on the finite set X, consists of a partition $\underline{R} = (R_0,\ R_1,\dots,R_t)$ of X × X satisfying the following axioms :

A_1 $R_0 = \{(x,x)\ |x\in X\}$

A_2 $R_i^{-1} = \{(y,x)\ |(x,y)\in R_i\} = R_i$

A_3 the cardinal of $\{z\in X\ |\ (x,z) \in R_i$ et $(y,z) \in R_j\}$ is a constant

p_{ij}^k independent of the choice of (x,y) in R_k.

Let us now define the adjacency matrices indexed by X × X with entries in C ; for i = 0,1,...,t :

$$D_i = [D_i(x,y)] \text{ where } D_i(x,y) = \begin{matrix} 1 \text{ if } x\ R_i\ y \\ 0 \text{ otherwise} \end{matrix}$$

We can restate the preceding axioms in matrices terms

A'_1 $D_0 = I$

A'_2 for $i = 0, 1, \ldots t$ $D_i^t = D_i$

A'_3 $D_i D_j = \sum_{k=0}^{t} p_{ij}^k D_k$

It can be shown [9], [7] that the D_i generate and are a basis of a semi simple commutative algebra, called the Bose Mesner algebra with a basis of t+1 idem potents J_i s.t.

$$J_i J_k = \delta_{ik} J_i$$

$$\sum_{i=0}^{t+1} J_i = I$$

Then it is easy to see that there exists reals numbers $p_k(i)$ s.t.

$$D_k J_i = p_k(i) J_i$$

These $p_k(i)$ are called the "first eigenvalues" of the scheme.

The "second eigenvalues" $q_k(i)$ can be defined as follows :

$$J_k = \frac{1}{|X|} \sum_{i=0}^{t} q_k(i) D_i.$$

In matrix form, we have :

$$P_{i,k} = p_k(i) \; ; \; Q_{i,k} = q_k(i)$$

$$PQ = |X| I$$

In the Hamming scheme P is the matrix over the basis of monomials of the famous Mc Williams transform which maps weight enumerators of linear codes into those of their orthogonal dual [8], [13].

3. Definition of the Lee Scheme :

Fist, let us consider the scheme on Z_q with $s = \left[\frac{q}{2}\right]$ classes (called ordinary q-gon in [3]) :

$$x R_k^1 y \iff x-y = \pm k$$

For any vector z in Z_q^n we can define its Lee composition, denoted by lc(z) :

$$lc(z) = (c_0, c_1, \ldots, c_s)$$

where the c_i are given by :

$$c_i = |\{j \in [0..n) \;/\; z_j = \pm i\}|$$

We now define a scheme with $N = C_{n+s}^{s} - 1$ classes on Z_q^n by :

$$x R_{\underline{k}} y \text{ iff } lc(x-y) = \underline{k}$$

where $\underline{k}$ is any possible composition vector.

This scheme is called the "extension of order n" of the ordinary q-gon [9]. Obviously the Lee metric is constant on the classes of the scheme :

$$x \, R_{k} \, y \Rightarrow d_{L}(x,y) = \|k\| = k_1 + k_2 + \ldots + sk_s.$$

However the relations R''_k.

$$x \, R''_k \, y \text{ iff } d_L(x,y) = k$$

do not yield in general an association scheme, as can be seen by drawing a picture in the peculiar case $n = 2$, $i = 2$, $j = 2$, $k = 4$.

We shall denote this scheme by $L(n,q)$ [16].

4. The Bose-Mesner algebra

If we denote by $D^L_{\underline{k}}$ (resp. D^H_i) the generic adjacency matrix of the Lee (resp. Hamming) scheme, we obtain the relationship

$$D^H_i = \sum_{|h|=i} D^L_k$$

where $|h| = h_1 + h_2 + \ldots + h_s$ denote the Hamming weight of any vector of Lee composition $\underline{h}$.

That means that the Lee scheme is a "refinement" of the Hamming scheme. We can continue the comparison in the same vein.

$$J^H_i = \sum_{|h|=i} J^L_k$$

$$P^H_i(|\ell|) = \sum_{|k|=i} P^L_k(\underline{\ell})$$

Where the $P^H_i(j)$ are the celebrated Krawtchouck polynomials.

Moreover, if we define the inner product of two vectors x and y of Z^n_q in the following way

$$\langle x,y \rangle = \prod_{i=1}^{n} w^{x_i y_i}$$

where w is a $q^{\underline{th}}$ primitive root of unity over C, the following equalities hold :

$$J_{\underline{k}}(x,y) = \sum_{lc(z)=\underline{\ell}} \langle x-y, z \rangle$$

$$P_{\underline{k}}(\underline{i}) = \sum_{lc(y)=\underline{k}} \langle x-y \rangle \text{ for any } x \text{ with } \ell_c(x) = \underline{i}$$

These relations, which have analogous counterparts in the Hamming scheme, are a particular case of a phenomenon occuring for scheme (X,R) over an abelian group X, where the R_i are invariant by the translation due to the group law [8 p.23].

By using properties of the inner product one can obtain a closed form for the generating function of the $p_{\underline{k}}(\underline{i})$, [2].

If we set :

$$P_{\underline{i}}(\underline{z}) = \sum_{\underline{k}} p_{\underline{k}}(\underline{i}) \; z_1^{k_1} \ldots z_s^{k_s}$$

One obtains for q odd :

$$P_{\underline{i}}(\underline{z}) = \prod_{\ell=0}^{s} \left(1 + 2 \sum_{m=1}^{s} z_m \cos\left(\frac{2\Pi}{q} m\ell\right)\right)^{i_\ell}.$$

and q even :

$$P_{\underline{i}}(\underline{z}) = \prod_{\ell=0}^{s} \left(1+2 \sum_{m=1}^{s-1} z_m \cos\left(\frac{2\Pi}{q} m\ell\right) + (-1)^{\ell} z_s\right)^{i_\ell}$$

All these relations and the links with Krawtchouk polynomials show that the $p_{\underline{k}}(\underline{i})$ are polynomials in s variables $i_1, i_2, \ldots, i_s$ of total degree at most $|k|$.

Moreover Bannai has shown [3] that in a polynomial scheme (i.e. where the $p_k(i)$ are polynomials in <u>one</u> variable) with sufficiently many classes the $p_k(i)$ are rational numbers. Hence, the Lee scheme is not, in general, polynomial, because of the cosinus terms.

5. The "Lloyd Theorem" in Lee metric :

In this section we show the link between Bassalygo's result and the Lee scheme. Consider the generalised Lloyd polynomial in s variables :

$$\psi_e(\underline{z}) = \sum_{\|k\| \le e} p_{\underline{k}}(\underline{z})$$

We denote by $\pi_{q,n}(e)$ the number of distinct Lee compositions in the Lee sphere of radius e centered at the origin $V_{n,e}(q)$.

<u>Theorem</u> : If there exists a perfect e-error correcting code C in L(n,q) then $\psi_e(\underline{z})$ has at least $\Pi_{q,n}(e) - 1$ distinct roots.

<u>Proof</u> : We consider the matrices $\hat{D}_{\underline{i}}$ with integer entries, and size $(N+1)\times(N+1)$

$$\hat{D}_{\underline{i}}\ (\underline{j},\underline{k}) = p^{\underline{k}}_{\underline{i},\underline{j}}$$

It in well-known [5], [14] that these matrices form an algebra isomorphic to the Bose Mesner algebra and have the same left eigenvalues. In particular there is a basis which diagonalize all the $\hat{D}_{\underline{i}}$ with the <u>complete</u> system of eigenvalues :

$p_{\underline{i}}(\underline{j})$ $\underline{j}$ taking N+1 values.

We call $\underline{a}$ the vector of the inner distribution of C with entries :

$$a_{\underline{i}} = \frac{|C \cap R_{\underline{i}}|}{|C|}$$

and $\underline{k}$ the column vector with entries : ...

$$k_{\underline{i}} = \frac{|R_{\underline{i}}|}{q^n}$$

The relation :

$$(I + \sum_{\|i\| \leq e} \hat{D}_i)\ \underline{a} = \underline{k}$$

expresses the perfection of C. This is a direct generalisation of a fact already observed in the context of distance transitive graphs [6].

Now the translated code C+h (h non zero) is also perfect with inner distribution $\underline{a}_h$. Thus we have that :

$$(I + \sum_{\|i\| \leq e} \hat{D}_i)\ (\underline{a}-\underline{a}_h) = \underline{0}$$

When h runs over $V_{n,e}(q)$ with distinct Lee compositions, this yields $\pi_{q,n}(e)-1$ distinct and linearly independent eigenvectors, and, consequently, as many null eigenvalues of the "Lloyd operator" of matrix :

$$(I + \sum_{\|i\| \leq e} \hat{D}_i)$$ Q.E.D.

6. An asymptotic estimate for $\Pi_{q,n}(e)$:

For convenience we set :

$$\delta_{q,n}(e) = \Pi_{q,n}(e) - \Pi_{q,n}(e-1)$$

which is equivalent to :

$$\delta_{q,n}(e) = |\{\underline{h} \in \mathbb{N}^s | \sum_{i=1}^{s} k_i \leq n \text{ and } \sum_{i=1}^{s} i\, k_i = e\}|$$

We recall that a partition of the integer e is a finite non decreasing sequence of positive integers $\lambda_1, \lambda_2, \ldots, \lambda_r$, called "parts" such that :

$$\sum_{i=1}^{n} \lambda_i = e$$

example : 4 has 4 partitions 4 = 1+1+1+1=1+2+1=1+3=2+2

So $\delta_{q,n}(e)$ counts the number of partitions of e in at most n parts with values in [1..s] (taking k_i as the number of occurences of i in the sum).
If we put :

$$(x)_n = (1-x^n)(1-x^{n-1})\ldots(1-x)$$

We can define the Gaussian binomial coefficient of basis x by :

$$\begin{bmatrix} n \\ m \end{bmatrix} = \frac{(x)_n}{(x)_m (x)_{n-m}}$$

Then, it can be shown [1] that :

$$\sum_e \delta_{q,n}(0) \quad x^e = \begin{bmatrix} n+s \\ s \end{bmatrix} = \begin{bmatrix} n+s \\ n \end{bmatrix}$$

and, consequently :

$$\sum_e \Pi_{q,n}(e) \quad x^e = \frac{1}{1-x} \quad \begin{bmatrix} n+s \\ n \end{bmatrix}$$

If $n \geq e$ and $s \geq e$ each part is necessarily $\leq$ s and there cannot be more than n non zero parts. We have then for $\delta_{q,n}(e)$ the generating function of ordinary unrestricted partition :

$$\prod_{i=1}^{\infty} \frac{1}{1-x^i}$$

Then a deep result due to Ramanujan [1] tells us that :

$$\delta_{q,n}(e) \underset{e\infty}{\sim} \frac{1}{4e\sqrt{3}} \quad \exp \left[\Pi \sqrt{\frac{2e}{3}}\right]$$

Then, after some manipulations we obtain :

$$\Pi_{q,n}(e) \underset{e\infty}{\sim} \frac{1}{2\Pi\sqrt{2e}} \quad \exp \left[\Pi \sqrt{\frac{2e}{3}}\right]$$

7. The Lee compositions distribution of the translate of a code :

Let $B_{\underline{i}}(e)$ be the Lee composition distribution of the translate C-e

$$B_{\underline{i}}(e) = |\{a \in C | \, a \; R_{\underline{i}} e\}|$$

Let $\beta^{\underline{m}}(\underline{x})$ be the annihilator polynomial of the $\underline{m}$ $\underline{th}$ order.

$$\beta^{\underline{m}}(\underline{x}) = \frac{q^n}{|C|} \, x^{\underline{m}} \prod_{\underline{i} \in J} \prod_{\ell=1}^{s} \left(1 - \frac{x_\ell}{i_\ell}\right)$$

J is the set of indices where the dual $\underline{a}' = P^T \underline{a}$ of the inner distribution, $\underline{a}$ of the code C is nonzero. In case of C linear $\frac{1}{|C|} P^T \underline{a}$ is the inner distribution of the dual of C [2]. Let $\beta^{\underline{m}}_{\underline{i}}$ be the development of the polynomial $\beta^m(\underline{x})$ in the basis of the $P_{\underline{i}}(\underline{x})$.

We denote by $\underline{0}$ the composition of the null vector.

Theorem : The inner distribution of C-e can be obtained by the linear recurrence :

$$\sum_{\underline{i} \in J} \beta^m_{\underline{i}} B_{\underline{i}} = \delta_{\underline{0},\underline{m}} \quad \text{(Kronecker symbol)}$$

Proof : We shall admit the following result which is a straightforward generalisation from Hamming [8] to Lee scheme :

$$\sum_{e \in Z^n_q} (B'_{\underline{k}}(e))^2 = q^n |C| a'_{\underline{k}} \text{ for any } \underline{k} \neq 0$$

where $B'_k(e)$ is the dual transform of $B_{\underline{k}}(e)$, i.e :

$$B'_k(e) = \sum_{\underline{i}} p_{\underline{k}}(\underline{i}) \, B_{\underline{i}}(e)$$

From the very definition of J we have that :

$$\beta^m(\underline{k}) \, a'_{\underline{k}} = 0 \text{ for } \underline{k} \neq \underline{0}$$

Using the cited result this implies :

$$\beta^m(\underline{k}) \, B'_{\underline{k}}(e) = 0 \text{ for } k \neq \underline{0}$$

We need the following identity :

$$\sum_{\underline{i}} \alpha_{\underline{i}} A_{\underline{i}} = \frac{1}{q^n} \sum_{L} \alpha(\underline{k}) \quad A'_{\underline{k}} \text{ where } \alpha(\underline{x}) = \sum_{\underline{i}} \alpha_{\underline{i}} \; P_{\underline{i}}(x)$$

which comes simply from the fact that $P^2 = q^n$ I and

$$\langle \underline{\alpha}, \underline{A} \rangle = \frac{1}{q^n} \langle P\underline{\alpha}, P^T\underline{A} \rangle$$

where <,> denotes the ordinary inner product on $\mathbb{R}^{N+1}$

Applying this identity, with $\alpha = \beta^{\underline{m}}$ and $\underline{A} = (B_{\underline{i}}(e))_{\underline{i}}$ yields :

$$\sum_{\underline{i}} \beta^m_{\underline{i}} B_{\underline{i}}(e) = \frac{1}{q^n} \beta(\underline{0}) \; B'_{\underline{0}}(e)$$

Since $p_{\underline{0}}(\underline{x}) = 1$ we have that $B'_{\underline{0}}(e) = |C|$. Q.E.D.

8. An upper bound on covering radius :

We denote by δ' the integer :

$$\delta' = \mathrm{Max}\ \{\|i\| \mid \underline{i} \in J\}.$$

with the same notations as in the preceding paragraph. If C is linear δ' is the diameter of its dual.
We define the covering radius of C :

$$\rho = \mathrm{Max}_{e \notin C}\ d_L(e,C)$$

Theorem : $\rho \leq \delta'$

Proof : We use the recurrence on the distribution with $\underline{m} = \underline{0}$, so that $\delta_{\underline{0},\underline{m}} = 1$.

Now, all the summands in the recurrence cannot vanish together. $B_{\underline{i}}(e) \neq 0$ means that there exists an a with

$$d_L(a,e) = \|i\|$$

so that :

$$\rho \leq \|i\| \leq \delta' \qquad \text{Q.E.D.}$$

example : We take the perfect negacyclic code of length 2 over Z_{13} with generator polynomial : $g(x) = x+5$ [5]. It is self dual with "negacycle" representatives : (0,0) ; (1,5) ; (3,2) ; (6,4) we have $\rho = 2$ and $\delta' = 10$.

We remark that the number of distinct Lee composition of the dual is 3, which could not happen in Hamming scheme where $s' = e$ for a perfect code [8].

Remark : In fact a stronger result holds [15]. Let s' be the number of distinct nonzero coefficient a'_k (for $k \neq \underline{0}$) in the dual inner distribution of C then

$$\rho \leq s'$$

9. T-designs :

A T-design in a general association scheme (X,R) is a subset $Y \subset X$, such that :

$$\forall_i \in T, \quad a'_i\ (Y) = 0$$

where a'_i is the dual inner distribution.

It has been shown [8] that T-designs in the Hamming scheme for $T = \{1, 2, \ldots t\}$ are orthogonal arrays of strength t, with n constraints, q level and index $|Y| \mid q^t$.

Let T^H_τ denote the set of indices $T^H_\tau = \{\underline{i} \mid |i| \leq \tau\}$.

Proposition : a T^H_τ-design in the Lee scheme is exactly a $\{1,\ldots,\tau\}$ design in Hamming scheme.

Proof : Let A' (resp-a') denote the dual inner distribution in the Hamming (resp. Lee) scheme.

As in paragraph 4, by using the fact that the Lee scheme is a refinement of the Hamming scheme, it can be proved that :

$$A'_j = \sum_{|i|=j} a'_{\underline{i}}$$

The proposition follows by the nonnegativity of the A'_j and the $a'_{\underline{i}}$. Q.E.D.

Using the obvious bound

$$d_L \leq s.d_H$$

we see that :

$$T_\tau^L \supset T_{[\tau/s]}^H$$

so that any T-design in L(n,q) is a particular orthogonal array in H(n,q).

10. Characterization of T-designs :

We define a generalized character for a subset Y and any u in Z_q^n :

$$\chi_u(Y) = \sum_{v \in Y} \langle u,v \rangle$$

Proposition : Y is a T-design iff ($\ell c(u) \in T \Rightarrow \chi_u(Y) = 0$)

Proof : We introduce the characteristic matrices of the code C in the following way :

$$H_{\underline{k}} = [\langle a,h \rangle] \quad a \in C, \; \ell c(h) = \underline{k}$$

Using the expression of $p_{\underline{k}}(\underline{C})$ in function of inner products, we obtain :

$$H_{\underline{k}} \bar{H}_{\underline{k}}^T = [P_{\underline{k}}(\ell_c(a-b)) \quad a,b \in C]$$

Let $\underline{j}$ be the all one vector of size $|C|$

$$\|\underline{j}\, H_{\underline{k}}\|^2 = |C|\, a'_{\underline{k}} = \sum_{\ell c(u) = \underline{k}} |\chi_u(Y)|^2$$

So $a'_{\underline{k}} = 0$ iff $\chi_u(Y) = 0$ for any u such that $\ell c(u) = \underline{k}$ Q.E.D.

Example : We write the words of the same self dual perfect code in columns :

1	2	3	4	5	6	0	-1	-2	-3	-4	-5	-6
-5	3	-2	6	1	-4	0	5	-3	2	-6	-1	4

It is, from [9], an orthogonal array of strength one ; each row contain each symbol of Z_{13} exactly once.

Taking u = (1,-1) in the preceding theorem and writing the row of differences yields :

6 -1 5 -2 4 -3 0 -6 1 -5 2 -4 3

Each symbol of Z_{13} is seen exactly once.

The same result would occur with any u such that

$$W_L(u) \leq 4$$

We see that the Lee metric yields more information on the same object than the Hamming one.

11. Open problems and conclusion :

The Lee scheme bears many ressemblances with the Hamming scheme. The underlying set is an abelian group allowing us , as noticed in [9 p.23], to express the first eigenvalues in terms of inner products. In particular, this led to a closed form for the generating function of these eigenvalues, and an algebraic characterisation for the T-designs. A combinatorial characterization would depend on the size of the alphabet as can be seen by examples.

However there is a main difference : the Hamming scheme is both P and Q polynomial [9] and the Lee scheme is not, in general, as noticed in §4. We have to manipulate polynomials with irrational coefficients in many variables, instead of polynomials with rational coefficients in one variable. In particular the number of zeroes over a compact set is not easy to evaluate.

This is the reason why the Lee version of Lloyd theorem is so complicate and hard to apply. Even if we had more accurate estimates of $\pi_{q,n}(e)$, bounding the number of lattice points solution of the Lloyd equation would still remain a difficult arithmetical problem.

12. Bibliography :

[1] G. ANDREWS "The theory of partitions" Addison Wesley Encyclopedia of Math and its applications.

[2] J. ASTOLA "The theory of Lee codes" Research report 1982 University of Lappeenranta, Finland.

[3] E. BANNAI and T. ITO "Algebraic combinatorics". Benjamin Cummings.

[4] L.A. BASSALYGO "A necessary condition for the existence of perfect codes in the Lee-metric" Mat. Zametki 15, p. 313-320, 1974.

[5] E.R. BERLEKAMP "Algebraic coding theory" Revised 1984 edition Aegean Park Press.

[6] N. BIGGS "Finite groups of automorphisms". Cambridge University Press.

[7] R.C. BOSE and D.M. MESNER (1959) "On linear associative algebras corresponding to association schemes of partially balanced designs" Ann. Math. Statist. 10 p. 21-38.

[8] P. DELSARTE "Four fundamental parameters of a code and their combinarorial significance" Info and Control 1973, 23, P. 407-438.

[9] P. DELSARTE "An algebraic approach to the association schemes of coding theory" Philips Res. Rpts. Suppl 1973 N° 10.

[10] S.W. GOLOMB and L.R. WELCH "Perfect codes in the Lee metric and the packing of polyominoes" SIAM J. Appl. Math. Vol 18 N° 2 pp. 302-317, 1970.

[11] S.W. GOLOMB and L.R. WELCH "Algebraic coding and the Lee metric" in Error correcting codes. H.B. MANN ed. p. 175-194 Wiley N.Y. 1968.

[12] C.Y. LEE 'Some properties of non binary error correcting codes" IEEE transactions on Information Theory. IT-4 p. 77-82.

[13] F.J. MAC WILLIAMS (1961) Doctoral Disertation Harvard University unpublished.

[14] F.J. MAC WILLIAMS and N.J.A. SLOANE "The theory of error correcting codes" North Holland.

[15] P. SOLE "On the parameters of Lee Codes" in preparation.

[16] H. TARNANEN "An approach to constant weight and Lee codes by using the methods of association schemes" Thesis Turku University 1982. Finland.