Association Schemes, Orthogonal Arrays and Codes from Non-degenerate Quadrics and Hermitian Varieties in Finite Projective Geometries.

I.M. CHAKRAVARTI
Department of Statistics
University of North Carolina at Chapel Hill

0. Summary.

In this paper, we have examined the matter of coexistence of and relations between association schemes, orthogonal arrays and certain families of projective codes. The projective codes considered here, are linear spans of a nice projective set $\mathcal{P}$ in a hyperplane $\mathcal{H}$ = PG(N-1,s) - such as a quadric or a quadric with its nucleus of polarity or a Hermitian variety.

There are two ways to construct association schemes from a projective code. One due to Delsarte (1973) considers the restriction of the Hamming scheme to the code with m weights and if it satisfies Delsarte's condition, an m-class association scheme is obtained by defining two codewords to be i-th associates if the Hamming distance between them is i=0,1,...,m. The alternative approach, first used by Ray-Chaudhuri (1959) and later generalized by Mesner (1967) is to classify points (according to some geometrical criterion) in $\mathcal{H} \equiv$ PG(N-1,s) with reference to $\mathcal{P}$, into m types (say). Then, two points of the affine space EG(N,s) (for which $\mathcal{H}$ is the hyperplane at infinity) are defined to be i-th associates if the line joining the two points meet $\mathcal{H}$ at a point of type i, i=1,...,m.

In many cases, the two association schemes defined with respect to the same projective set have the same parameters. But examples are given where they do not coincide and, in fact, there are cases where one scheme exists but the other does not.

1. Introduction.

Coexistence of Codes, association schemes and orthogonal arrays and t-designs have been the subject of some interesting studies by Bose (61), Delsarte (1973 a,b), Assmus and Mattson (1974) and Calderbank and Goethals (1984).

It is well-known, for instance, that an orthogonal array of index unity is the same as the maximum distance separable (mds) code (for definitions of

codes, assocation schemes, orthogonal arrays and t-designs see MacWilliams and Sloane (1977)). Delsarte (1973) has shown that a code is an orthogonal array of strength d'-1, where d' is the *dual* distance of the code. For an unrestricted code (linear or non-linear), d' is the smallest of the subscripts of the non-zero MacWilliams transforms of the frequencies that occur in the distance-distribution of codewords. For a linear code C, d' is the same as the minimum distance of the dual code $C^{\perp}$.

An answer to the question "when does the restriction of the Hamming Association schemes to a code C is itself an association scheme?" has been provided by Delsarte (1973) for linear codes. He has shown that the restriction of the Hamming association scheme to a linear code C with s distinct weights is itself an association scheme with s classes, if and only if among the cosets of the dual code $C^{\perp}$ exactly s+1 distinct weight distributions occur. In particular, the restriction of the Hamming association scheme to a projective linear two-weight code is always a two class association scheme or equivalently, a strongly regular graph (Delsarte, 1972). Calderbank and Goethals (1984) have considered three-weight projective codes C for which the restriction of the Hamming association scheme $H_n(q)$ to C is an association scheme with three classes. They have given a set of sufficient conditions and restrictions on the three weights of C.

The restriction of the Hamming association scheme to a projective linear code C is defined by considering two codewords to be in relation R_i if the Hamming distance between the codewords is i, i=0,1,...,n, where n is the length of a codeword.

In this paper, relations between pairs of points of a finite affine geometry EG(N,s) are defined with reference to a *projective set* in the hyperplane PG(N-1,s) at infinity of the projective space PG(N,s) in which the EG(N,s) is embedded. Such a technique seems to have been first used by Ray-Chaudhuri (1959) for constructing a family of two-class association schemes on the points of $EG(3,2^h)$. Later, Mesner (1967) gave a full formal development of this geometric technique and used it to derive two extensive families of two-class associations schemes called pseudo-latin square (hyperbolic) and negative latin square (elliptic) association schemes. It is very interesting to note that the parameters of these two families of two-class association schemes are the same as those of the two families of the two-class association

schemes derived as restrictions of the Hamming association schemes to the projective two-weight codes derived by Wolfmann (1975) from hyperbolic and elliptic quadrics in a projective space of odd dimension.

2. Ray-Chaudhuri-Mesner type construction of association schemes

In Ray-Chaudhuri-Mesner technique, one first chooses a nice projective set $\mathcal{P}$ in a fixed hyperplane $\mathcal{H}$ = PG(N-1,s) of the projective space Σ = PG(N,s) of dimension N over a finite field of order s. Then one defines relations between the s^N points of the affine space A = EG(N,s) which is the complement of $\mathcal{H}$ in Σ. The line ℓ joining two points a and b of A, meets $\mathcal{H}$ at a unique point p (say). Suppose the points of $\mathcal{H}$ are of m distinct types with reference to the projective set $\mathcal{P}$. The two points a and b are defined to the i-th associates (or in relation R_i) if the point p is of type i, i=1,...,m. Here we consider $m \geq 2$ (Ray-Chaudhuri and Mesner considered only the case m = 2).

3. Association schemes, orthogonal arrays and codes from quadrics in PG(2,s).

3.1 Case s even.

Let Σ = PG(3,2^h), $\mathcal{H}$ = PG(2,2^h) and A = EG(3,2^h) and let Q_2 be a non-degenerate quadric in $\mathcal{H}$. Then it is known (see, for instance, Bose (1962)) that Q_2 has s+1 points where $s = 2^h$, and all the s+1 tangents (one at each point) of Q_2 pass through a single point 0 (not on the quadric) called the nucleus of polarity. Ray-Chaudhuri (1959) took the projective set $\mathcal{P}$ to consist of the s+1 points in Q_2 and the nucleus of polarity 0 and defined two points a and b of A to be first associates if the line joining a and b meet $\mathcal{H}$ at a point p in $\mathcal{P}$ and second associates, otherwise. He thus obtained a two-class association scheme with parameters $v = s^3$, $n_1 = (s+2)(s-1)$, $p_{11}^1 = (s-2)$, $p_{11}^2 = s+2$, $s = 2^h$.

Now, consider the 3 × (s+2) matrix M whose columns are the coordinate vectors of the (s+2) points of $\mathcal{P}$. No three columns of M are linearly dependent and hence taking all linear combinations of the coordinate vectors we get an orthogonal array OA(s^3, s+2, s, 3) of strength 3 and index unity. (Bose and Bush, 1952). This is also a maximum distance separable code C with n = s+2, k = 3, d = n-k+1 = s (see for instance, MacWilliams and Sloane (1977). That it

has two distinct non-zero weights can be seen from the following geometrical considerations. It is known (see, for instance, Bose (1962)) that each one of the s+1 tangents of a non-degenerate quadric Q_2 in a plane PG(2,s), $s = 2^h$, intersects $\mathcal{P}$ at two points - one on Q_2 and the other the nucleus of polarity 0. The s^2 other lines fall into two classes. Those lines which meet Q_2 at two points are called *intersectors* which are (s+1)s/2 in number. The other s(s-1)/2 lines called non-intersectors do not meet Q_2 at any point. Thus in the $s^3 \times (s+2)$ array A there are (s+1)(s+2)/2 row-vectors each of weight s (# of non-zero coordinates) and s(s-1)/2 row-vectors each of weight (s+2).

Thus the two non-zero weights are $w_1 = s$ and $w_2 = s+2$ with respective frequencies $f_{w_1} = (s^2-1)(s+2)/2$ and $f_{w_2} = s(s-1)^2/2$. This two-weight projective code provides a two-class association scheme (Delsarte, 1971) on $v = s^3$ codewords. Two codewords are first associates if the Hamming distance between them is s+2 and are second associates if the distance is s. Thus $n_1 = s(s-1)^2/2$ and $n_2 = (s^2-1)(s+2)/2$. The p^i_{jk} parameters can be calculated using the formulae of eigenvalues of the adjacency matrix given by Delsarte (1971) in terms of the parameters of the code and then expressing the eigenvalues in terms of p^i_{jk} parameters as given by Bose and Mesner (1959). (See, for instance, Chakravarti (1990, p. 39). Thus, one gets $p^1_{11} = s(s-2)(s-3)/4$ and $p^2_{11} = s(s-1)(s-2)/4$.

We note that this two-class association scheme is not, in general, the same as the one given by Ray-Chaudhuri. However, for s = 4, these two schemes have the same parameters.

If the $3 \times (s+2)$ matrix M is used as a parity check matrix, we get the dual code $C^\perp$ which has minimum distance 4. For s = 4, $C = C^\perp$, that is C is self-dual (see, for instance, MacWilliams, Odlyzko and Sloane (1978)).

3.2 s even; three-class association schemes

Using the same combinatorial set up in PG(3,s), $s = 2^h$, as before, but using slightly different definition of relations, we generate a 3-class association scheme. We define two points a and b of EG(3,s) to the *first*

associates if the line ab meets Q_2 at a point p, *second associates* if the line ab meets the hyperplane $\mathcal{H}$ (= PG(2,s)) at an external point (point other than the nucleus of polarity and points *on* Q_2) and *third associates* if the line ab is incident with the nucleus of polarity 0. Then from the geometrical properties of this combinatorial configuration (see, for instance, Bose (1962)) it can be shown that this defines a three-class association scheme on the s^3 points of EG(3,s) with parameters

$$v = s^3,\ s = 2^h,\ n_1 = s^2-1,\ n_2 = (s-1)^2(s+1),\ n_3 = s-1,$$

$$p_{11}^1 = s-2,\ p_{12}^1 = s(s-1),\ p_{22}^1 = (s^2-1)(s-2),$$

$$p_{11}^2 = s,\ p_{12}^2 = s^2-s-2,\ p_{22}^2 = s^3-2s^2-s+4,$$

$$p_{11}^3 = 0,\ p_{12}^3 = (s^2-1),\ p_{22}^3 = (s^2-1)(s-2).$$

The constancy of these nine parameters ensures that this is a three-class association scheme (Ray-Chaudhuri (1959)).

3.3 s odd

We now consider the case when s is odd. As before, Q_2 is a non-degenerate quadric in a distinguished hyperplane $\mathcal{H}$ = PG(2,s) of PG(3,s) and EG(3,s) is the affine space whose points are all those of PG(3,s) which are not on $\mathcal{H}$. Then, it is known (see, for instance, Bose (1962), p. 144-145) that $|Q_2| = s+1$, no three tangents of Q_2 pass through the same point and the (s+1) tangents determine by their intersections s(s+1)/2 points called *external* (hyperbolic) points. The remaining s(s-1)/2 points of $\mathcal{H}$, are called internal (elliptic) points. A line of $\mathcal{H}$ is either a tangent (which meets Q_2 exactly at one point) or an *intersector* (which meets Q_2 exactly at two points) or a non-intersector (which does not meet Q_2 at any point). There are (s+1) tangents, s(s+1)/2 intersectors and s(s-1)/2 non-intersectors. Each external point is incident with 2 tangents, (s-1)/2 intersectors and (s-1)/2 non-intersectors. Each internal point is incident with (s+1)/2 intersectors and (s+1)/2 non-intersectors. Each point on Q_2 is incident with one tangent on Q_2, and s

intersectors. Dually, each tangent is incident with one point of Q_2 and s external points; each intersector is incident with two points of Q_2, (s-1)/2 external points and (s-1)/2 internal points and each non-intersector is incident with (s+1)/2 external points and (s+1)/2 internal points.

Now we define two points a and b of EG(3,s) to be *first associates* if the line $\overline{\overline{ab}}$ meets Q_2 at a point p, *second associates* if the line $\overline{\overline{ab}}$ is incident with an *external point* and *third associates* if the line $\overline{\overline{ab}}$ is incident with an *internal point*. Then from the geometrical facts stated in the earlier paragraph, one can establish the constancy of the nine parameters $p_{11}^i(a,b)$, $p_{12}^i(a,b)$ and $p_{22}^i(a,b)$ i=1,2,3. It then follows (Ray-Chaudhuri 1959) that this defines a three-class association scheme. The parameters of this association scheme are $v = s^3$, $n_1 = s^2-1$, $n_2 = (s^3-s)/2$, $n_3 = s(s-1)^2/2$, $p_{11}^1 = s-2$,

$p_{12}^1 = s(s-1)/2$, $p_{22}^1 = s(s-1)+s(s-1)(s-3)/4$, $p_{11}^2 = s-1$,

$p_{12}^2 = 2(s-1)+ (s-1)(s-3)/2$, $p_{22}^2 = 2(s-1)(s-2)+(s-1)(s-3)^2/4$, $p_{11}^3 = s+1$,

$p_{12}^3 = (s^2-1)/2$, $p_{22}^3 = (s+1)(s-1)(s-3)/8$.

Let R be the 3 × (s+1) matrix whose (s+1) columns are the coordinate-vectors of the s+1 points on Q_2. Then the linear span of the row vectors of R generates a linear projective code C_2 with n = s+1 and k = 3. It has three non-zero weights $w_1 = s$, $w_2 = s-1$ and $w_3 = s+1$ with respective frequencies $f_{w_1} = (s^2-1)$, $f_{w_2} = s(s^2-1)/2$ and $f_{w_3} = s(s-1)^2/2$. The weights and the frequencies correspond to the intersections of Q_2 with a tangent or an intersector or a non-intersector. The minimum distance of this code is s-1. Considered as an orthogonal array, its parameters are $OA(s^3, s+1, s, 3)$. The dual code $C_2^\perp$ has minimum distance 4. If the restriction of the Hamming association scheme $H_{s+1}(s)$ to C_2, were to define a three class association scheme, then it is clear that $n_1 = s^2-1$, $n_2 = s(s^2-1)/2$ and $n_3 = s(s-1)^2/2$. These three numbers are the same as those of the 3-class association scheme we

have given earlier. The problem whether the restriction of the $H_{s+1}(s)$ to C_2 is a three class association is still under investigation.

4. Non-degenerate quadrics in PG(2t-1, s)

Taking N = 2t and Q_{2t-1} a non-degenerate quadric as the projective set in $\mathcal{H}$ = PG(2t-1, s), Mesner (1967) has constructed two families of two-class association schemes corresponding to the two cases - Q_{2t-1} hyperbolic and Q_{2t-1} elliptic. These two families called Pseudo-Latin square (hyperbolic) type and negative-Latin square (elliptic) type have the same parameters as those of the respective association schemes obtained by considering the restrictions of the Hamming association schemes to the projective codes derived by Wolfmann (1975) from hyperbolic and elliptic quadrics in PG(2t-1, s).

5. Association schemes, codes and orthogonal arrays from a non-degenerate Hermitian variety in PG(N-1, s^2)

Taking a Hermitian variety V_1 (for definitions and properties of Hermitian varieties, see Bose and Chakravarti (1966), Chakravarti (1970)), defined by the equation $s_0^{s+1} + x_1^{s+1} + x_2^{s+1} = 0$, as the projective set in a hyperplane $\mathcal{H}$ = PG(2,s^2), Mesner (1967) obtained a two-class association scheme with parameters $v = s^6$, $n_1 = (s^2-1)(s^3+1)$, $p_{11}^1 = s^2(s^2+1)-s^3-2$, $p_{11}^2 = s^2(s^2-1)$.

We generalize his construction by taking $\mathcal{H}$ = PG(N-1,s^2) and a non-degenerate Hermitian variety V_{N-2} defined by the equation $x_0^{s+1} + \ldots + x_{N-1}^{s+1} = 0$. As before, two points a and b of EG(N,s^2) are *first associates* if the line $\overline{ab}$ is incident with a point on V_{N-2}; second associates, otherwise. Then we have established that $v = s^{2N}$, $n_1 = (s^N-(-1)^N)(s^{N-1}-(-1)^{N-1})$, $p_{11}^1 = s^{2N-2}-(-s)^{N-1}(s-1)-2$ and $p_{11}^2 = s^{2N-2}-(-s)^{N-1}$. The full proof will be given elsewhere. This family of association schemes has the same parameters as those of the two-class association schemes derived as restrictions of the Hamming association schemes to two-weights codes defined as linear spans of coordinate vectors of points on a non-degenerate Hermitian variety in PG(N-1,s^2). The relations of these codes to orthogonal arrays and difference sets are described in Calderbank and Kantor (1986), and Chakravarti (1990).

REFERENCES

[1] Assmus, E.F. and Mattson, Jr. H.F., Coding and Combinatorics, *SIAM Review*, 16(3) (1974), pp. 349-388.

[2] Bose, R.C. and Bush, K., Orthogonal arrays of strength two and three. *Ann. Math. Statist.*, 23(4) (1952), pp. 508-524.

[3] Bose, R.C., On some connections between the design of experiments and information theory. *Bull. Inter. Statist. Inst.*, 38 (1961), pp. 257-271.

[4] Bose, R.C., Lecture Notes on *Combinatorial problems of Experimental Design*, Department of Statistics, University of North Carolina at Chapel Hill (1962).

[5] Bose, R.C. and Chakravarti, I.M., Hermitian varieties in a finite projective space $PG(N,q^2)$, *Canad. J. Math.*, 18 (1966), pp. 1161-1182.

[6] Bose, R.C. and Mesner, D.M., On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Statist.*, 30 (1959), pp. 21-38.

[7] Calderbank, R. and Kantor, W.M., The geometry of two-weight codes, *Bull. London Math. Soc.*, 18 (1986), pp. 97-122.

[8] Calderbank, A.R. and Goethals, J.-M., Three-weight codes and association schemes, *Philips J. Res.* 39 (1984), pp. 143-152.

[9] Chakravarti, I.M., Some properties and applications of Hermitian varieties in $PG(N,q^2)$ in the construction of strongly regular graphs (two-class association schemes) and block designs, *J. of Comb. Theory, Series B*, 11(3) (1971), pp. 268-283.

[10] Chakravarti, I.M., Families of codes with few distinct weights from singular and non-singular Hermitian varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weight codes. Coding Theory and Design theory, Part I, (D. Ray-Chaudhuri, editor). *The IMA Volumes in Mathematics and its Applications*, Vol. 20, Springer-Verlag, (1990), pp. 35-50.

[11] Delsarte, P., Weights of linear codes and strongly regular normed spaces, *Discrete Math.*, 3 (1972), pp. 27-64.

[12] Delsarte, P., An algebraic approach to the association schemes of coding theory, *Philips. Res. Rep. Suppl.*, 19 (1973).

[13] Delsarte, P., Four fundamental parameters of a code and their combinatorial significance. *Info. and Control*, 23 (1973), pp. 407-438.

[14] MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, North Holland, 1977.

[15] MacWilliams, F.J., Odlyzko, A.M., Sloane, N.J.A. and Ward, H.N., Self-dual codes over GF(4), *J. Comb. Th.*, A25 (1978), pp. 288-318.

[16] Mesner, D.M., A new family of partially balanced incomplete block designs with some latin square design properties, *Ann. Math. Statist.*, 38 (1967), pp. 571-581.

[17] Ray-Chaudhuri, D.K., On the application of the geometry of quadrics to the construction of partially balanced incomplete block designs and error correcting codes, Ph.D. dissertation submitted to the University of North Carolina at Chapel Hill (1959).

[18] Wolfmann, J., Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie, *Discrete Mathematics*, 13 (1975), pp. 185-211.

[19] Wolfmann, J., Codes projectifs à deux poids, "caps" complets et ensembles de différences, *J. Combin. Theory*, 23A (1977), pp 208-222.