ON THE APPLICATION OF THE GEOMETRY OF QUADRICS TO THE CONSTRUCTION OF PARTIALLY BALANCED INCOMPLETE BLOCK DESIGNS AND ERROR CORRECTING BINARY CODES

by

D. K. Ray-Chaudhuri

University of North Carolina

This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF 49(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

Institute of Statistics
Mimeograph Series No. 230
June, 1959

ACKNOWLEDGMENTS

It is a great pleasure to express my deep gratitude to Professor R. C. Bose, for suggesting the problem herein considered and providing guidance and encouragement during the course of my investigation.

My thanks are due to the United States Air Force for its financial assistance during my stay in Chapel Hill.

To Miss Marianne Byrd, Miss Jane Rogers and Mrs. Ouida Taylor I am extremely grateful for their skillful and quick typing of the manuscript. To Miss Martha Jordan I extend thanks for a variety of forms of aid.

Finally, I wish to express my deep indebtedness to Professor S. N. Roy whose fascinating lectures in the Indian Statistical Institute at Calcutta in the year 1956 inspired me to come to Chapel Hill for higher studies and research in Statistics.

TABLE OF CONTENTS

	Page
Acknowledgments	ii
Introduction	v
Notation	ix
CHAPTER	
I. SOME PRELIMINARY RESULTS ON THE GEOMETRY OF QUADRICS IN FINITE PROJECTIVE SPACE	1
1. Summary	1
2. Quadrics in finite projective geometry	1
3. Conjugate points, polar space and tangent space	7
4. Stereographic projection and its use	21
5. Linear spaces contained in a nondegenerate quadric Q_n in PG(n,s)	26
6. Canonical forms of quadrics	29
7. Nucleus of polarity of a quadric in PG(2k, 2^m)	34
II. SOME CLASSES OF PBIB DESIGNS WITH TWO ASSOCIATE CLASSES OBTAINED FROM THE CONFIGURATION OF LINEAR SPACES CONTAINED IN A QUADRIC	38
1. Summary	38
2. Introduction	39
3. PBIB designs from the configuration of generators for blocks and points for treatments of a quadric	43
4. PBIB designs from the configuration of points of a quadric for blocks and generators of a quadric for treatments	54
5. PBIB designs from the configuration of generators on generators	60
6. PBIB designs from the configuration of lines and points of PG(3,s) truncated by a quadric	64
7. Concluding remarks	68

CHAPTER		Page
III.	SOME CLASSES OF PBIB DESIGNS WITH THREE ASSOCIATE CLASSES	69
	1. Summary.	69
	2. A theorem on three associate PBIB designs.	70
	3. Some PBIB designs with three associate classes obtained from the configuration of generators and points of a cone	74
	4. Some PBIB designs with three associate classes obtained from the configuration of secants and external points of a quadric.	84
IV.	A CLASS OF TWO ERROR CORRECTING CODES WITH RATE OF TRANSMISSION ARBITRARILY CLOSE TO UNITY AND FRACTIONAL REPLICATIONS PRESERVING MAIN EFFECTS AND TWO FACTOR INTERACTIONS	94
	1. Summary.	94
	2. General problem of information theory.	95
	3. Binary channel	98
	4. Statement of the problem	100
	5. Some prelimary results on group codes.	103
	6. Relationship between error-correcting binary group codes and fractional replications of factorial experiments at two levels.	106
	7. A correspondence between the points of PG(n,2) and the elements of $GF(2^{n+1})$	109
	8. An R_4-set in PG(2m-1, 2) containing $(2^m - 1)$ points and a sequence of two error correcting codes with asymptotic rate of transmission equal to unity	111
	9. An R_4-set in PG(2m, 2) containing $2^m + N_4(m - 1)$ points and a sequence of two error correcting codes with asymptotic rate of transmission equal to unity. .	115
	10. Examples illustrating the method of constructing R_4-sets.	121
BIBLIOGRAPHY		124

INTRODUCTION

The theory of linear spaces in finite projective geometry has been used very profitably by several authors in solving combinatorial problems of statistical interest. The properties of linear spaces have been used for the construction of (i) balanced incomplete block designs (Bose [2]), (ii) partially balanced incomplete block (PBIB) designs (Bose and Nair [7]), (iii) set of orthogonal latin squares (Bose and Nair [8]), (iv) designs with block confounding or fractional replication which preserve all main effects and interactions up to a certain order (Bose [3]) and (v) orthogonal arrays. Bose [3] first used the properties of quadric surfaces in finite projective geometry of two and three dimensions for constructing experimental designs. Primrose [21]* studied some properties of a quadric in a general finite projective space and used them to construct series of balanced incomplete block designs which, however, do not include any design with parameters in the practical range. The works of Bose and Primrose suggested that a detailed study of quadrics in a general finite projective space will be very useful for solving combinatorial problems of statistical origin. In this thesis an attempt is made to study the quadrics in finite projective space systematically and the results so obtained in the theory of quadrics are applied for the construction of PBIB designs. A detailed summary of the work done in each chapter is given in the beginning of

---

*The numbers in square brackets refer to the bibliography listed at the end.

that chapter. Below we give only a very brief summary of the work done in various chapters of the thesis.

In chapter I the theory of quadrics is dealt with. Several new results have been obtained. The general formula for the number of p-flats contained in a nondegenerate quadric $PG(n,s)$, the finite projective geometry of n dimensions based on a Galois field $GF(s)$, is obtained for the elliptic as well as the hyperbolic quadric. The canonical forms for elliptic and hyperbolic nondegenerate quadrics are obtained. The polar of a k-flat with respect to a nondegenerate quadric is defined and various properties of the polar spaces are derived. The properties of the nucleus of polarity of a nondegenerate quadric in $PG(2k,2^m)$ are studied.

In chapter II several series of PBIB designs with two associate classes are given. PBIB designs were introduced by Bose and Nair [7] to fulfill the need of incomplete block designs which do not require too many replications. PBIB designs have been used very profitably in experimental situations when the complete blocks cannot be used and also no balanced incomplete block design exists for the particular parameters of interest. Various authors (Bose and Nair [7], Bose [4], Bose and Clatworthy [5], Bose and Shimamato [9], Bose, Shrikhande and Bhattacharya [10], Bose, Clatworthy and Shrikhande [6], J. Roy and R. Laha [22], and many others) have made an almost exhaustive treatment of the problem of construction of PBIB designs with two associate classes with parameters in the practical range. In chapter II we have

given a very general method of constructing PBIB designs using classes of sets in PG(n,s) . A series of two associate PBIB designs is obtained from the configuration of generators and points of a nondegenerate quadric taking generators for blocks and points for treatments. Three other series of two associate PBIB designs are obtained. These series contain many designs with r and k not greater than 10. Of these designs several are new and the rest are already obtained by other authors by different methods.

In chapter III two series of PBIB designs with 3 associate classes are given. These two series are obtained from the configuration of generators and points of a cone and the configuration of secants and external points of a quadric in the finite projective plane. These two series contain 8 new designs with r and k not greater than 10.

In chapter IV we have considered the problem of construction of error correcting binary codes which is also a combinatorial problem of statistical interest. From the general existence theorems of Shannon [23] which are completed and extended by various authors [1, 18, 20, 16, 27] it is known that under certain conditions it is possible to find a method of encoding which transmits information through a noisy channel with probability of correct transmission of the message arbitrarily close to unity and also with a rate of transmission arbitrarily close to the capacity of the channel. However, no method is known for actual construction of codes with the required characteristic. Slepian [25] considers the problem of construction of (n,k) binary group codes with n places

and k information places which maximizes the probability of correct transmission of the message. Slepian solved his problem only for small values of n and k. Knebler [19] obtained a general solution of Slepian's problem for $k = 3$ and 4. However, the codes obtained by Slepian and Knebler have poor rate of transmission. In this chapter we have obtained a class of two error correcting binary group codes with rate of transmission arbitrarily close to unity. Denoting by $N_t(m)$ the maximum number of points that can be packed in $PG(m,2)$ such that no t of the points lie in a $(t-2)$-flat, it is shown that a t-error correcting (n,k) group code exists if and only if $N_t(n-k-1) \geq n$. Two error correcting codes are constructed for (i) $n = 2^m - 1$, $k = 2^m - 1 - 2m$, (ii) $n = 2^m + N_4(m-1)$, $k = 2^m + N_4(m-1) - 1 - 2m$. A theorem is proved showing that a $\frac{1}{2^k}$ fraction of a 2^n experiment preserving main effects and interactions up to $(t-1)$th order exists if and only if a t-error correcting (n,k) binary group code exists.

NOTATION

Standard Symbol	Meaning of the Symbol
$\cup$	Union (of sets)
$\cap$	Intersection (of sets)
$\subset$	'is a subset of'
$\in$	'belongs to'
$\notin$	'does not belong to'
$\Longrightarrow$	'implies'
$\not\subset$	'is not a subset of'
$\{P\}$	the set containing the single point P
EG(n,s)	Finite Euclidean geometry based on a Galois field GF(s)
PG(n,s)	Finite projective geometry based on a Galois field GF(s)

CHAPTER I

SOME PRELIMINARY RESULTS ON THE GEOMETRY OF QUADRICS IN FINITE PROJECTIVE SPACE

1. Summary.

The theory of quadrics in finite projective geometry is found to be very useful in the study of combinatorial problems of statistical interest. In this chapter a brief systematic treatment of the theory of quadrics in finite projective geometry is presented and some new results in the theory of quadrics are derived. Several properties of the polar spaces are proved. The explicit formulae for the number of p-flats contained in nondegenerate quadrics in $PG(n,s)$, the finite projective geometry of n dimensions based on a Galois field $GF(s)$, are obtained. The canonical forms for the elliptic and hyperbolic nondegenerate quadrics and several properties of the nucleus of polarity of a nondegenerate quadric in $PG(2k, 2^m)$ are given. The results obtained in this chapter are used in the later chapters to construct PBIB designs and error-correcting codes.

2. Quadrics in finite projective geometry.

Quadric

A quadric Q in $PG(n,s)$, the finite projective geometry of n dimensions based on a Galois field $GF(s)$, where s is a prime power, is the set of all points $x' = (x'_0, x'_1, \ldots, x'_n)$ which satisfies the equation

$$(1) \qquad \sum_{j \geq i=0}^{n} a_{ij} x_i x_j = 0$$

where a_{ij}'s are elements of $GF(s)$ and the operations of addition and multiplication are in $GF(s)$. The expression $\sum_{j \geq i=0}^{n} a_{ij} x_i x_j$ is said to be the quadratic form or, in short, the form of Q. If the characteristic of the field $GF(s)$ is not 2, then it is possible to write the equation of any quadric Q as

$$(2) \qquad \sum_{i,j=0}^{n} a_{ij} x_i x_j = 0$$

where $$a_{ij} = a_{ji} \quad , \quad i,j = 0,1,\ldots,n \quad .$$

In this case in matrix notation the equation of Q can be written as

$$(3) \qquad (1 \times \overline{n+1}) \; (\overline{n+1} \times \overline{n+1}) \; (\overline{n+1} \times 1) = 0$$

where A is a symmetric matrix. However, if the characteristic of the field is (2), the equation of Q cannot always be written in the form (3). Since we are especially interested in the case of a field with characteristic 2, we shall use the form (1) of the equation of Q.

Example

Consider Q in $PG(2, 2^2)$ with the equation

$$x_0^2 + x_1 x_2 = 0 \quad .$$

The elements of $GF(2^2)$ can be represented as $0,1,t$ and t^2, the minimum function being $1 + t + t^2$. Then it can easily be checked that Q consists of the following 5 points

$$P_1 = (0\ 0\ 1)$$
$$P_2 = (0\ 1\ 0)$$
$$P_3 = (1\ 1\ 1)$$
$$P_4 = (1\ t\ t^2)$$
$$P_5 = (1\ t^2\ t) \quad .$$

Degenerate Quadric

A quadric Q in $PG(n,s)$ is said to be degenerate if there exists a nonsingular transformation

$$\underset{(\overline{n+1}\ x\ 1)}{\underline{x}} = \underset{(\overline{n+1}\ x\ \overline{n+1})}{B}\ \underset{(\overline{n+1}\ x\ 1)}{y}$$

which transforms the form of Q to $\sum_{j\geq i=0}^{r} c_{ij}\, y_i y_j$, $r < n$.

Nondegenerate Quadric

A quadric Q is said to be nondegenerate if it is not degenerate. The form of a quadric is said to be nondegenerate in $PG(n,s)$ if the corresponding quadric is nondegenerate in $PG(n,s)$.

Rank of a Quadric

A quadric Q in $PG(n,s)$ is said to have rank r if there exists a nonsingular transformation

$$\underset{(\overline{n+1}\ x\ 1)}{\underline{x}} = \underset{(\overline{n+1}\ x\ \overline{n+1})}{B}\ \underset{(\overline{n+1}\ x\ 1)}{\underline{y}}$$

which transforms the form of Q to $\sum_{j\geq i=0}^{r-1} a_{ij}\, y_i y_j$ which is a nondegenerate form in $PG(r-1, s)$.

It is easily seen that a quadric Q_n in $PG(n,s)$ is nondegenerate if and only if the rank of Q is $(n + 1)$. If the characteristic of the

field is not 2, the rank of a quadric Q is equal to the rank of the symmetric matrix of its form. However, this is not true if the characteristic is not 2. The following example will make it clear.

Example

Consider Q_2 in PG(2,2) with the equation

$$x_0^2 + x_1^2 + x_2^2 = 0 \quad .$$

The matrix of the form of Q_2 is

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which has rank 3. However, the rank of Q_2 is 1 since the nonsingular transformation

$$y_1 = x_1 + x_2 + x_3$$
$$y_2 = x_2$$
$$y_3 = x_3$$

reduces the form of Q_2 to y_1^2 .

Cone

A quadric Q in PG(n,s) of rank r is said to be a cone of order $(n + 1 - r)$.

Vertex and base of a cone

Consider a cone Q in PG(n,s) of order $(n + 1 - r)$. Then there exists a nonsingular transformation which transforms Q to Q'_{r-1} with the equation

$$\sum_{j \geq i=0}^{r-1} c_{ij}\, y_i y_j = 0$$

where Q'_{r-1} is a nondegenerate quadric in PG(r-1, s). The (n-r)-flat Σ_{n-r} determined by the equations

$$y_o = y_1 = \ldots = y_{r-1} = 0$$

is said to be the vertex of the cone. Any (r-1)-flat Σ_{r-1} which does not intersect the vertex Σ_{n-r} is called the base of the cone. In particular the (r-1)-flat Σ_{r-1} determined by the equation

$$y_r = y_{r+1} = \ldots = y_n = 0$$

is a base of the cone. If P is a point of the cone lying on the base, then the (n-r+1)-flat determined by the vertex Σ_{n-r} and the point P is completely contained in the cone.

Example

Consider the quadric Q in PG(3,3) with the equation

$$x_1^2 + x_2^2 + x_3^2 = 0 \quad .$$

Obviously Q has rank 3. So Q is a cone of order 1 in PG(3,3). The plane Σ_2 determined by the equation

$$x_o = 0$$

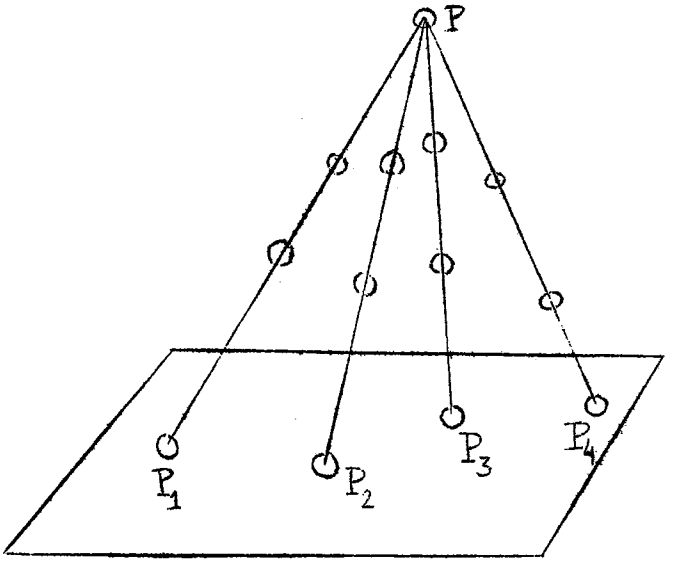
is a base of the cone. The base contains the following four points of the cone.

$$P_1 = (0\ 1\ 1\ 1)$$
$$P_2 = (0\ 1\ 2\ 1)$$
$$P_3 = (0\ 1\ 2\ 2)$$
$$P_5 = (0\ 1\ 1\ 2) \quad .$$

The vertex is the point

$$P = (1\ 0\ 0\ 0) \quad .$$

The cone consists of the 13 points lying on the lines PP_1, PP_2, PP_3 and PP_4. The cone can be represented by the following diagram.



Hyperbolic and elliptic nondegenerate quadrics

It has been shown by Primrose [21] that every nondegenerate quadric in PG(2k, s) contains linear spaces of dimensionality (k - 1) and does not contain any linear space of higher dimensionality. So with respect to the maximum dimensionality of a linear space contained in the quadric, the nondegenerate quadrics in PG(2k, s) belong to only one type. However, the nondegenerate quadrics in PG(2k-1, s) belong to two different types, hyperbolic or elliptic. If a nondegenerate quadric in PG(2k-1, s) contains (k-1)-flats and does not contain any linear space of higher dimensionality, then the quadric is said to be a

hyperbolic nondegenerate quadric. If a nondegenerate quadric in PG(2k-1, s) contains (k-2)-flats and does not contain any linear space of higher dimensionality, then the quadric is said to be elliptic. Primrose [21] uses the words unruled and ruled quadric, for elliptic and hyperbolic quadrics. Tallini [26] uses the names elliptic and hyperbolic quadrics.

3. Conjugate points, polar space and tangent space.

Conjugate points

Consider a quadric Q in $PG(n, s)$ with the form $\sum_{j \geq i=0}^{n} a_{ij} x_i x_j$. A point

$$\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n)$$

is said to be conjugate to a point

$$\beta = (\beta_0, \beta_1, \ldots, \beta_n) \quad \text{with respect to} \quad Q$$

if $$\sum_{j \geq i=0}^{n} a_{ij}(\alpha_i \beta_j + \alpha_j \beta_i) = 0 \quad .$$

Obviously the relationship of conjugacy is symmetrical, i.e., if α is conjugate to β, then β is conjugate to α.

Polar space of a point

The polar space of a point α with respect to Q is the set of all points which are conjugate to α with respect to Q. If

$$\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_n) \quad ,$$

it is easily seen that the polar space of α is an (n-1)-flat determined by the equation

$$(1) \qquad \sum_{j \geq i=0}^{n} a_{ij}(\alpha_i x_j + x_i \alpha_j) = 0 \quad .$$

If the characteristic of the field is 2, every point is self conjugate and the equation of the polar of α reduces to

$$(2) \qquad \sum_{j > i=0}^{n} a_{ij}(\alpha_i x_j + \alpha_j x_i) = 0 \quad .$$

If the characteristic of the field GF(s) is not 2, a point is self conjugate if and only if it is a point of the quadric. In this case the equation of the polar of α can be written as

$$(3) \qquad \sum_{i,j=0}^{n} a'_{ij} \alpha_i x_j = 0$$

where

$$a'_{ii} = a_{ii}$$

$$a'_{ij} = a_{ij} \qquad i \neq j,\ i,j = 0,1,\ldots,n \ .$$

In matrix notation the equation of the polar can be written as

$$(4) \qquad \underset{(1 \times \overline{n+1})}{x'} \quad \underset{(\overline{n+1} \times \overline{n+1})}{A} \quad \underset{(\overline{n+1} \times 1)}{\alpha} = 0$$

where A is a symmetric matrix. Since our treatment will cover both the cases of characteristic of the field equal to 2 and the characteristic not equal to 2, we shall use the equation (1) for the polar of α . The polar of a point α will be denoted by $\tau(\alpha)$.

Tangent space

If α is a point of the quadric Q , the polar of α with respect to Q is said to be the tangent space of Q at the point α .

Conjugacy of two linear spaces

Two linear spaces Σ_p and Σ_q are said to be mutually conjugate with respect to a quadric Q if every point of Σ_p is conjugate to every point of Σ_q with respect to Q.

Polar of a p-flat

The polar space of a p-flat Σ_p with respect to a quadric Q is the set of all points which are conjugate to every point of Σ_p with respect to Q.

Lemma 3.1.1

If a point P is conjugate to the points $A_o, A_1, \ldots, A_p$ with respect to a quadric Q, then P is conjugate to the linear space determined by the points $A_o, A_1, \ldots, A_p$.

Proof. We have to show that P is conjugate to every point of the linear space determined by the points $A_o, A_1, \ldots, A_p$. Since P is conjugate to the points $A_o, A_1, \ldots, A_p$, the polar hyperplane of P contains all the points of $A_o, A_1, \ldots, A_p$. Then by a fundamental property of linear space, the polar hyperplane of α contains the linear space determined by the points $A_o, A_1, \ldots, A_p$. Hence the lemma follows.

All the considerations in the following are with respect to a fixed quadric Q in $PG(n,s)$.

Theorem 3.1

The polar of a p-flat Σ_p is the intersection of the polars of $A_o, A_1, \ldots, A_p$ where $A_o, A_1, \ldots, A_p$ are $(p+1)$ independent points in Σ_p.

Proof. Let

$$\tau(\Sigma_p) = \text{polar of } \Sigma_p$$

$$\tau(A_i) = \text{polar of } A_i \ , \ i = 0,1,\ldots,p \ .$$

Let $$\tau'(\Sigma_p) = \tau(A_o) \cap \tau(A_1) \cap \ldots \cap \tau(A_p) \quad .$$

To prove the theorem we need to show that

$$\tau(\Sigma_p) = \tau'(\Sigma_p) \quad .$$

Let α be a point of $\tau(\Sigma_p)$. Then α is conjugate to the points $A_o, A_1, \ldots, A_p$ since all these points belong to Σ_p . So we have

(5) $$\alpha \in \tau(A_i) \ , \quad i = 0,1,2,\ldots,p \quad .$$

From (5) it follows that

(6) $$\alpha \in \tau'(\Sigma_p) \quad .$$

So we have

(7) $$\tau(\Sigma_p) \subset \tau'(\Sigma_p) \quad .$$

Conversely let

$$\alpha \in \tau'(\Sigma_p) \quad .$$

Then α is conjugate to the points $A_o, A_1, \ldots, A_p$. So by lemma 3.1.1 α is conjugate to the p-flat Σ_p . Hence

$$\alpha \in \tau(\Sigma_p) \quad .$$

So we have

(8) $$\tau'(\Sigma_p) \subset \tau(\Sigma_p) \quad .$$

The theorem follows from (7) and (8).

Theorem 3.2

Let $A_o, A_1, \ldots, A_p$ be independent points of a quadric Q in $PG(n,s)$. The p-flat Σ_p determined by these points is completely contained in the quadric if and only if the $(p+1)$ points are pairwise conjugate.

Proof. Sufficiency. We shall prove sufficiency by induction. First we shall prove the result for $p = 1$. Let

$$A_o = (\alpha_o, \alpha_1, \ldots, \alpha_n)$$
$$A_1 = (\beta_o, \beta_1, \ldots, \beta_n)$$

and the form of Q be $\sum_{j \geq i=o}^{n} a_{ij} x_i x_j$.

Since A_o and A_1 are points of the quadric and are mutually conjugate, we have the following.

$$\sum_{j \geq i=0}^{n} a_{ij} \alpha_i \alpha_j = 0$$
$$\sum_{j \geq i=0}^{n} a_{ij} \beta_i \beta_j = 0 \qquad (9)$$
$$\sum_{j \geq i=0}^{n} a_{ij} (\alpha_i \beta_j + \alpha_j \beta_i) = 0 \quad .$$

Any point on the line $A_o A_1$ other than A_o and A_1 can be represented as

$$A_o + \lambda A_1 = (\alpha_o + \lambda\beta_o, \alpha_1 + \lambda\beta_1, \ldots, \alpha_n + \lambda\beta_n)$$

where λ is a non-zero element of $GF(s)$.

Using the equations (9) it can be easily seen that for any non-zero element λ, $A_o + \lambda A_1$ is a point of Q. Hence the line $A_o A_1$ is contained in Q.

Now suppose the result is true for $(p - 1)$, i.e., if A_o, A_1, ..., A_{p-1} are points of the quadric and pairwise conjugate, the $(p-1)$-flat Σ_{p-1} determined by these points is contained in Q. Any point of Σ_p not lying on Σ_{p-1} can be represented as $A_p + \lambda A$ where A is a point of Σ_{p-1} and λ is any element of $GF(s)$. Both A_p and A are points of the quadric and by assumption A_p is conjugate to A_o, A_1, ..., A_{p-1}. Hence by lemma 3.1.1 A_p is conjugate to A. So from the first part of the proof the line A_pA is contained in Q. So $A_p + \lambda A$ is a point of Q. Hence the p-flat Σ_p is contained in Q. This completes the proof of sufficiency.

Necessity. Assume that the p-flat Σ_p determined by A_o, A_1, ..., A_p is completely contained in Q. If possible, suppose A_i and A_j are not mutually conjugate, $i \neq j$, $i,j = 0,1,\ldots,p$. Without any loss of generality let us assume $i = 0$ and $j = 1$. Then we have

$$(10) \qquad \sum_{j \geq i=0}^{n} a_{ij}(\alpha_i\beta_j + \alpha_j\beta_i) \neq 0 \quad .$$

Using (10) and the fact that A_o and A_1 are points of the quadric, it is easy to see that the point $A_o + \lambda A_1$ is not a point of Q for some non-zero λ which contradicts the assumption that Σ_p is contained in Q.

Corollary 3.2.1

Let Σ_p and Σ_q be two linear spaces which are contained in the quadric Q and are mutually conjugate with respect to Q. Then the linear space determined by Σ_p and Σ_q is contained in Q.

Theorem 3.3

Let Q_n be a nondegenerate quadric in $PG(n,s)$ and P be a point of the quadric Q_n. Let $\tau(P)$ be the tangent space at P and π be an $(n-1)$-flat not passing through P. Then

1) $Q_n \cap \tau(P)$ is a cone of order 1 on the $(n-1)$-flat $\tau(P)$.

2) $Q_n \cap \tau(P) \cap \pi$ is a nondegenerate quadric in $PG(n-2, s)$ which is elliptic or hyperbolic according as Q_n is elliptic or hyperbolic.

Proof. (1) Let R be any point of $\tau(p) \cap Q_n$. Then P and R are mutually conjugate and both are points of the quadric. So by theorem 3.2, the line PR is contained in the quadric. Using this geometrical fact, we shall prove the theorem algebraically. Let the form of Q_n be $\sum_{j \geq i=0}^{n} a_{ij} x_i x_j$. Let

$$P = (\alpha_0, \alpha_1, \ldots, \alpha_n)$$

and the equation of $\tau(P)$ be

$$\sum_{i=0}^{n} c_{1i} x_i = 0 \quad .$$

Let the equation of π be

$$\sum_{i=0}^{n} c_{oi} x_i = 0 \quad .$$

The following two relations follow easily.

$$\text{(11)} \qquad \sum_{i=0}^{n} c_{1i} \alpha_i = 0 \qquad \sum_{i=0}^{n} c_{oi} \alpha_i \neq 0 \quad .$$

Let $C_j = (c_{j0}, c_{j1}, \ldots, c_{jn})$, $j = 1,2,\ldots,n$,

be n independent points on the $(n-1)$-flat Σ_{n-1} with the equation

$$\sum_{i=0}^{n} \alpha_i x_i = 0 \quad .$$

Consider the transformation

$$y_j = c_{j0}x_0 + c_{j1}x_1 + \ldots + c_{jn}x_n \ , \quad j = 0,1,2,\ldots,n \ .$$

It can easily be seen that the transformation is nonsingular. Under this transformation

P goes to $P' = (1\ 0\ 0\ \ldots\ 0)$,

$\tau(P)$ goes to the $(n-1)$-flat τ' with the equation $y_1 = 0$,

π goes to the $(n-1)$-flat π' with the equation $y_0 = 0$

and the form of Q_n goes to $\sum_{j \geq i=0}^{n} b_{ij}\, y_i y_j$ (say) .

$Q_n \cap \tau(P)$ is transformed to a quadric Q'_{n-1} on the $(n-1)$-flat τ' and has the equation

$$(12) \quad b_{00}y_0^2 + y_0(b_{02}y_2 + b_3y_3 + \ldots + b_{on}y_n) + \sum_{j \geq i=2}^{n} b_{ij}\, y_i y_j = 0 \ .$$

Using the fact that the $(n-1)$-flat with the equation $y_1 = 0$ is the tangent space at the point P' , we can easily get that

$$b_{00} = b_{02} = b_{03} = \ldots = b_{on} = 0 \quad .$$

So the equation of Q'_{n-1} reduces to

$$(13) \qquad \sum_{j \geq i=2}^{n} b_{ij}\, y_i y_j = 0 \quad .$$

To prove part (1) of the theorem it is sufficient to show that the form

$\sum_{j\geq i=2}^{n} b_{ij}\, y_i y_j$ is nondegenerate in PG(n-2, s). It can easily be shown that if $\sum_{j\geq i=2}^{n} b_{ij}\, y_i y_j$ is degenerate in PG(n-2, s), then Q_n is degenerate in PG(n,s) which is a contradiction. This completes the proof of part (1).

(2) Under the transformation used in part (1), $Q_n \cap \tau(P) \cap \pi$ goes to the quadric Q'_{n-2} in the (n-2)-flat, $y_o = y_1 = 0$, with the equation

$$\sum_{j\geq i=2}^{n} b_{ij}\, y_i y_j = 0 \quad .$$

We have already shown that Q'_{n-2} is a nondegenerate quadric in PG(n-2, s). Hence $Q_n \cap \tau(P) \cap \pi$ is a nondegenerate quadric in PG(n-2, s). It remains to show that $Q_n \cap \tau(P) \cap \pi$ is elliptic or hyperbolic according as Q_n is elliptic or hyperbolic for $n = 2k - 1$. Assume Q_n is elliptic. If possible, suppose $Q_n \cap \tau(P) \cap \pi$ is hyperbolic. Then $Q_n \cap \tau(P) \cap \pi$ contains a (k-2)-flat Σ_{k-2}. The point P and Σ_{k-2} are mutually conjugate and are contained in Q_n. Hence by corollary 3.2 the (k-1)-flat determined by Σ_{k-2} and P is contained in Q_n. This contradicts the fact that Q_n is elliptic. Hence $Q_n \cap \tau(P) \cap \pi$ is elliptic. Similarly we can show that if Q_n is hyperbolic, $Q_n \cap \tau(P) \cap \pi$ is hyperbolic in PG(n-2, s).

Lemma 3.3.a

Let Q_n be a nondegenerate quadric in PG(n,s). Let Σ_{k-1} be any (k-1)-flat contained in Q_n and Σ_{n-k} be an (n-k)-flat not intersecting Σ_{k-1}. Suppose the following hold.

(1) $\tau(\Sigma_{k-1})$, the polar of Σ_{k-1} is an (n-k)-flat

(2) $\tau(\Sigma_{k-1}) \bigcap \Sigma_{n-k}$ is an (n-2k)-flat

(3) $Q_n \bigcap \tau(\Sigma_{k-1}) \bigcap \Sigma_{n-k}$ is a nondegenerate quadric Q_{n-2k} in PG(n-2k, s). Then for any k-flat Σ_k contained in Q_n and an (n-k-1)-flat Σ_{n-k-1} not intersecting Σ_k

(1) $\tau(\Sigma_k)$ is an (n-k-1)-flat

(2) $\tau(\Sigma_k) \bigcap \Sigma_{n-k-1}$ is an (n-2k-2)-flat.

Proof. Let Σ_{k-1} be any (k-1)-flat in Σ_k and P_k is a point of Σ_k not contained in Σ_{k-1} . Then the k-flat Σ_k is determined by Σ_{k-1} and P_k . We shall write this fact symbolically as

$$\Sigma_k = P_k \oplus \Sigma_{k-1} \quad .$$

By theorem 3.1

$$\tau(\Sigma_k) = \tau(P_k) \bigcap \tau(\Sigma_{k-1}) \quad .$$

$\tau(P_k)$ is an (n-1)-flat and $\tau(\Sigma_{k-1})$ is an (n-k)-flat. Hence $\tau(\Sigma_k)$ is an (n-k-1)-flat unless

(14) $$\tau(\Sigma_{k-1}) \subset \tau(P_k) \quad .$$

If possible, suppose (14) is true. Let Σ_{n-k} be an (n-k)-flat such that

(1) $\Sigma_{n-k} \bigcap \Sigma_{k-1} = \Phi$, the null set

(2) $P_k \in \Sigma_{n-k}$.

Let $p(n)$ denote the maximum dimensionality of a linear space contained in Q_n . Since $Q_n \bigcap \tau(\Sigma_{k-1}) \bigcap \Sigma_{n-k}$ is a nondegenerate quadric in PG(n-2k, s) , there exists a $p(n-2k)$-flat $\Sigma_{p(n-2k)}$ such that

$$\Sigma_{p(n-2k)} \subset Q_n \cap \tau(\Sigma_{k-1}) \cap \Sigma_{n-k}$$

and

$$P_k \notin \Sigma_{p(n-2k)}$$

since from (14) $\tau(\Sigma_{k-1}) \subset \tau(P_k)$

and

$$\Sigma_{p(n-2k)} \subset \tau(\Sigma_{k-1}) \ ,$$

(15) $$\Sigma_{p(n-2k)} \subset \tau(P_k) \ .$$

From (15), we have

$$\Sigma_{p(n-2k)} \subset \tau(P_k) \cap \tau(\Sigma_{k-1}) = \tau(\Sigma_k) \ .$$

Hence $\Sigma_{p(n-2k)}$ and Σ_k are mutually conjugate. Also both the linear spaces are contained in Q_n. Hence by corollary 3.2.1

$$\Sigma_{p(n-2k)} \oplus \Sigma_k \subset Q_n \ .$$

It is easy to see that

$$\Sigma_{p(n-2k)} \cap \Sigma_k = \Phi \ , \text{ the null set.}$$

Hence $\Sigma_{p(n-2k)} \oplus \Sigma_k$ is a $p(n-2k) + k + 1$ -flat ,

so we have

(16) $$p(n) = p(n - 2k) + k + 1 \ .$$

However, it is known that

(17) $$p(n) = p(n - 2k) + k \ .$$

So (16) contradicts (17). So (14) cannot be true. This establishes the first part of the lemma, i.e., that $\tau(\Sigma_k)$ is an (n-k-1)-flat. It remains to prove that $\tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is an (n-2k-2)-flat. Since

$$\Sigma_k \subset \tau(\Sigma_k)$$

and

$$\Sigma_k \cap \Sigma_{n-k-1} = \Phi \ , \text{ from hypothesis ,}$$

we have

(18) $\tau(\Sigma_k) \neq \Sigma_{n-k-1}$.

Part two of the lemma follows immediately from (18) and the fact that $\tau(\Sigma_k)$ is an (n-k-1)-flat.

Theorem 3.3.a

Let Σ_k be a k-flat contained in a nondegenerate quadric Q_n in PG(n, s). Let Σ_{n-k-1} be an (n-k-1)-flat not intersecting Σ_k . Then

(1) $\tau(\Sigma_k)$ is an (n-k-1)-flat, $\tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is an (n-2k-2)-flat and $Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is a nondegenerate quadric Q_{n-2k-2} in PG(n - 2k - 2, s) which is elliptic or hyperbolic according as Q_n is elliptic or hyperbolic

(2) $Q_n \cap \tau(\Sigma_k)$ is a cone of order (k+1) on the (n-k-1)-flat $\tau(\Sigma_k)$ with Σ_k as the vertex.

Proof. We shall prove the theorem by finite induction on k . We have proved the theorem for k = 0 in theorem 3.3. Hence it will be sufficient to show that if the theorem is assumed to be true for (k-1), it is true for k . The proof given here holds for the case when the characteristic of the field is 2 as well as for the case when the characteristic is not 2. However, it is possible to give a shorter proof for the case when the characteristic is not 2.

Assume that the theorem is true for k - 1 . Then by lemma 3.3.a $\tau(\Sigma_k)$ is an (n-k-1)-flat and $\tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is an (n-2k-2)-flat. Let $\tau(\Sigma_k)$ be determined by the following (k + 1) independent equations.

$$(19) \qquad \sum_{j=0}^{n} c_{ij}\, x_j = 0 \quad , \quad i = 0,1,2,\ldots,k \quad .$$

Let Σ_{n-k-1} be determined by the equations

$$(20) \qquad \sum_{j=0}^{n} c_{ij}\, x_j = 0 \quad , \quad i = n-k,\ n-k+1,\ \ldots,\ n \quad .$$

Consider the $(n-k-1)$-flat determined by the equations

$$(21) \qquad \sum_{j=0}^{n} \alpha_{ij}\, x_j = 0 \quad , \quad i = 0,1,\ldots,k \quad ,$$

where $$A_i = (\alpha_{io}, \alpha_{il}, \ldots, \alpha_{in}) \quad , \quad i = 0,1,\ldots,k$$

are $(k+1)$ independent points in Σ_k . The points

$$c_i = (c_{io}, c_{il}, \ldots, c_{ij}) \quad , \quad i = 0,1,\ldots,k$$

belong to the $(n-k-1)$-flat (21). Let $c_o, c_1, \ldots, c_k, c_{k+1}, \ldots, c_{n-k-1}$ be a set of $(n-k)$ independent points lying on the $(n-k-1)$-flat (21). Consider the transformation

$$y_i = \underset{(1 \times \overline{n+1})(\overline{n+1} \times 1)}{c_i'\ \underline{x}} \quad .$$

It can be easily seen that this transformation is a nonsingular one. Under this transformation $\tau(\Sigma_k)$ goes to the $(n-k-1)$-flat τ' with the equations $y_i = 0$, $i = 0,1,\ldots,k$,

Σ_{n-k-1} goes to Σ'_{n-k-1} determined by the equations

$$y_{n-k} = y_{n-k+1} = \ldots = y_n = 0 \quad ,$$

Q_n goes to Q_n' with the equation $\sum_{j \geq i=0}^{n} b_{ij}\, y_i y_j = 0$,

the point A_i goes to the point $B_i = (0,0,\ldots,0,\beta_{in-k}, \ldots,\beta_{in})$,

$$i = 0,1,\ldots,k \ ,$$

$Q_n \cap (\Sigma_k) \cap \Sigma_{n-k-1}$ goes to Q'_{n-2k-2} with the equation

$$(22) \qquad \sum_{j \geq i = k+1}^{n-k-1} b_{ij}\, y_i\, y_j = 0$$

and $Q_n \cap \tau(\Sigma_k)$ goes to Q'_{n-2k-1} with the equation

$$(23) \qquad \sum_{j \geq i = k+1}^{n-k-1} b_{ij}\, y_i y_j + \text{terms involving } y_{n-k}, y_{n-k+1}, \ldots, y_n = 0 .$$

It can be shown that if the form of the quadric Q'_{n-2k-2} is degenerate in PG(n-2k-2,s), then Q'_n is also degenerate. Hence Q'_{n-2k-2} is nondegenerate. So $Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is nondegenerate in PG(n-2k-2, s).

Also by a corresponding method used in the proof of theorem 3.3, it can be shown that $Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k}$ is elliptic or hyperbolic according as Q_n is elliptic or hyperbolic. This completes the proof of part (1). To prove part (2), it is sufficient to show that the coefficients of $y_{n-k}, y_{n-k+1}, \ldots, y_n$ in (23) are all zero. Let Σ'_k be the k-flat determined by $B_o, B_1, \ldots, B_k$. Σ'_k is contained in Q'_{n-2k-1}. Also if P' is any point of Q'_{n-2k-1}, the (k+1)-flat

$$\Sigma'_{k+1} = P' \oplus \Sigma'_k$$

is contained in Q'_{n-2k-1}. Using this fact we can show that all the terms involving $y_{n-k}, y_{n-k+1}, \ldots, y_n$ in (23) are zero.

Theorem 3.4

Let Σ_k be a k-flat contained in a nondegenerate quadric Q_n in PG(n,s). Let Σ_p be any linear space which is contained in Q_n and contains Σ_k. Then Σ_p is contained in $\tau(\Sigma_k)$, the polar of Σ_k.

Proof. Let $A_0, A_1, \ldots, A_k$ be $(k+1)$ independent points in Σ_k. Since Σ_k is contained in Q_n, these points must be pairwise conjugate by theorem 3.2. Let the p-flat Σ_p be determined by the $(p+1)$ independent points $A_0, A_1, \ldots, A_k, A_{k+1}, \ldots, A_p$. Since Σ_p is contained in Q_n, these points are also pairwise conjugate. By theorem 3.1

$$\tau(\Sigma_k) = \bigcap_{i=0}^{k} \tau(A_i) \quad .$$

Since A_i is conjugate to A_j, $i \neq j$, $i,j = 0,1,\ldots,p$, we have

$$A_j \in \tau(A_i) \quad .$$

Hence

$$A_j \in \tau(\Sigma_k) \quad , \quad j = 0,1,\ldots,p \quad . \tag{24}$$

From (24) it follows that

$$\Sigma_p \subset \tau(\Sigma_k) \quad .$$

Corollary 3.4

The tangent hyperplane through a point P of a nondegenerate quadric Q contains all the linear spaces that contain P and are contained in Q.

4. Stereographic projection and its use

Let O be a point in PG(n,s) and π be an (n-1)-flat not passing through O. Let P be a point other than O. The line OP intersects π at a point P'. P' is called the stereograph projection of P on π through O. The stereographic projection of a set A in PG(n,s) on π through O is defined to be the set of all points which are stereographic projections of the points of A on π through O.

The stereographic projection of A on π through O will be denoted by $S_{O,\pi}(A)$. If O and A are assumed to be fixed, $S_{O,\pi}(A)$ will be written as $S(A)$. If C is a set of points containing O, then the stereographic projection of the set $C - \{O\}$ through O will be written as $S(C)$ for convenience.

Lemma 4.1.1

Let P be a point on a nondegenerate quadric Q_n in $PG(n,s)$ and τ be the tangent space at P and π be an $(n-1)$-flat not passing through P. In the following any stereographic projection is on π through P. Then

(a) $S(Q_n \cap \tau)$ is Q_{n-2}, a nondegenerate quadric on the $(n-2)$-flat $\tau \cap \pi$.

(b) If Σ_p is a p-flat containing P and contained in Q_n, then

$$S(\Sigma_p) \doteq \Sigma_{p-1} \text{ , a } (p-1)\text{-flat}$$

and $$S(\Sigma_p) \subset Q_{n-2} .$$

(c) If Σ_p is a p-flat not containing P and contained in $Q_n \cap \tau$, then $S(\Sigma_p) = \Sigma_p'$, a p-flat

and $$S(\Sigma_p) \subset Q_{n-2} .$$

(d) If Σ_p is a p-flat contained in Q_n but not in τ, then

$$S(\Sigma_p) = \Sigma_p'$$

and $$S(\Sigma_p) \not\subset Q_{n-2} .$$

Proof. (a) We have shown in theorem 3.3 that $Q_n \cap \tau \cap \pi$ is a nondegenerate quadric Q_{n-2} in PG(n-2, s). Hence it will be sufficient to show that

(1) $$S(Q_n \cap \tau) = Q_n \cap \tau \cap \pi \quad .$$

(1) follows immediately from the definition of sterographic projection.

(b) Since $P \in \Sigma_p$

and $\Sigma_p \subset Q_n$

by corollary 3.4 $\Sigma_p \subset \tau(P)$.

So we have $\Sigma_p \subset Q_n \cap \tau$.

It follows that $S(\Sigma_p) \subset S(Q_n \cap \tau) = Q_{n-2}$.

Now to prove (b) it is sufficient to show that

(2) $$S(\Sigma_p) = \Sigma_{p-1} \text{ , a } (p-1)\text{-flat.}$$

It is easy to check that

$$S(\Sigma_p) = \Sigma_p \cap \pi \quad .$$

Hence (2) follows from the fact that Σ_p is not contained in π .

(c) Let

$$\Sigma_{p+1} = P \oplus \Sigma_p$$

and $$\Sigma_p' = \Sigma_{p+1} \cap \pi \quad .$$

It is easy to check that

$$S(\Sigma_p) = \Sigma_p' \quad .$$

Since $\Sigma_p \subset \tau(P)$

by corollary 3.4 $\Sigma_{p+1} \subset Q_n \cap \tau(P)$.

So $\Sigma_p' \subset Q_n \cap \tau(P) \cap \pi = Q_{n-2}$.

(d) Let $\Sigma_{p+1} = P \oplus \Sigma_p$

and $\Sigma_p' = \Sigma_{p+1} \cap \pi$.

It is easy to check that

$$S(\Sigma_p) = \Sigma_p' .$$

To show that $S(\Sigma_p) \not\subset Q_{n-2}$

it is sufficient to show that

(3) $$\Sigma_p' \not\subset \tau \cap \pi .$$

(3) follows immediately from the fact that

$$\Sigma_p \not\subset \tau .$$

Stereographic projection of a class of sets

Let $\mathcal{Q}$ be a class of sets in PG(n,s) . Let P be a given point and π be an (n-1)-flat not passing through P . The stereographic projection of the class $\mathcal{Q}$ on π through O is defined to be the class consisting of the sets which are the stereographic projections on π through P of the sets of $\mathcal{Q}$ and is denoted by $S(\mathcal{Q})$.

Lemma 4.1.2

Let $\mathcal{Q}$ be a class of distinct p-flats passing through a point P in PG(n,s) and π be an (n-1)-flat not passing through P . Then there exists a one to one correspondence between the two classes $\mathcal{Q}$ and $S(\mathcal{Q})$.

Proof. Let Ω be any set in the class . Let Ω be made to correspond to $S(\Omega)$. We shall show that this correspondence is unique.

It will be sufficient to show that for any two different sets Ω and Ω' of the class

(4) $$S(\Omega) \neq S(\Omega') \quad .$$

If possible, suppose (4) is not true. Then

$$S(\Omega) = S(\Omega') \quad .$$

Since $\Omega \neq \Omega'$

there exists a point R belonging to Ω but not belonging to Ω' .

Let $R' = S(R)$, the sterographic projection of R .

Then $R' \in S(\Omega')$, $P \in \Omega'$,

so the line PR' is contained in Ω' . Obviously R is a point on the line PR' . Hence R is a point of Ω' which is a contradiction.

Theorem 4.1

Let P be a point of a nondegenerate quadric Q_n in $PG(n,s)$, $\tau(P)$ be the tangent space at P and π be an $(n-1)$-flat not passing through P . Let $\mathcal{L}_{n,p}$ denote the class of p-flats contained in Q_n and passing through P and $\mathcal{U}_{n,p}$ be the class of all p-flats of Q_n . Then there exists a one to one correspondence between the classes $\mathcal{L}_{n,p}$ and $\mathcal{U}_{n-2,p-1}$ and hence the number of elements in each class is the same.

Proof. Since each p-flat of $\mathcal{L}_{n,p}$ passes through P , by lemma 4.1.2 it will be sufficient to show that

(5) $$S(\mathcal{L}_{n,p}) = \mathcal{U}_{n-2,p-1} \quad .$$

We shall show that (5) is true if for Q_{n-2} we take the nondegenerate quadric $Q_n \cap \tau(P) \cap \pi$ in $PG(n-2, s)$.

Let $\Sigma_p \in \mathcal{L}_{n,p}$

and $S(\Sigma_p) = \Omega$, $\Omega \in S(\mathcal{L}_{n,p})$.

By part (b) of lemma 4.1.1

$$\Omega = \Sigma_{p-1} \subset Q_{n-2} .$$

Hence $\Omega \in \mathcal{Q}_{n-2,p-1}$.

It follows that

(6) $$S(\mathcal{L}_{n,p}) \subset \mathcal{Q}_{n-2,p-1} .$$

Conversely let $\Sigma_{p-1} \in \mathcal{Q}_{n-2,p-1}$.

Then it can be easily seen that

$$\Sigma_p = P \oplus \Sigma_{p-1} \subset Q_n$$

and $S(\Sigma_p) = \Sigma_{p-1}$.

Hence

(7) $$\Sigma_{p-1} \in S(\mathcal{L}_{n,p}) \quad \text{and} \quad \mathcal{Q}_{n-2,p-1} \subset S(\mathcal{L}_{n,p}) .$$

(5) follows from (6) and (7).

5. Linear spaces contained in a nondegenerate quadric Q_n in PG(n,s)

Theorem 5.1

Let $N(p,n)$ denote the number of different p-flats contained in a nondegenerate quadric Q_n in $PG(n,s)$. Then

$$N(p,n) = \begin{cases} \Phi(p,k) & \text{, for } n = 2k,\ p \leq k-1 , \\ \Phi_1(p,k) & \text{, for } n = 2k-1 ,\ Q_n \text{ elliptic and } p \leq k-2 , \\ \Phi_2(p,k) & \text{, for } n = 2k-1 ,\ Q_n \text{ hyperbolic and } p \leq k-1 , \end{cases}$$

where $$\Phi(p,k) = \prod_{r=0}^{p} \frac{(s^{2(k-p+r)} - 1)}{(s^{p+1-r} - 1)} \quad , \quad p \leq k - 1$$

$$\Phi_1(p,k) = \prod_{r=0}^{p} \frac{(s^{n-2p+2r} + s^{k-p+r-1} - s^{k-p+r} - 1)}{(s^{p+1-r} - 1)} \quad , \quad p \leq k - 2$$

$$\Phi_2(p,k) = \prod_{r=0}^{p} \frac{(s^{n-2p+2r} - s^{k-p+r-1} + s^{k-p+r} - 1)}{(s^{p+1-r} - 1)} \quad , \quad p \leq k - 1 \, ,$$

The expressions for $N(o,n)$ were obtained by Primrose [21] .

Proof. First we shall establish the following difference equation.

(1) $$N(p,n) = \frac{N(p-1,\, n-2)N(o,n)(s - 1)}{(s^{p+1} - 1)} \quad .$$

Let P be a point of Q_n . From theorem 4.1 it follows that the number of p-flats contained in Q_n and passing through P is $N(p-1,\, n-2)$. Let us count the points in the p-flats contained in Q_n. Every p-flat contributes $\frac{s^{p+1} - 1}{s - 1}$ points and the number of p-flats contained in Q_n is $N(p,n)$. Hence this collection of p-flats contain $N(p,n)\frac{s^{p+1} - 1}{s - 1}$ points which are not all different. In this collection every point will be repeated as many times as there are p-flats of Q_n passing through a point. Through every point of Q_n there passes $N(p-1,\, n-2)$ p-flats and the number of points of Q_n is $N(o,n)$. Hence the collection of p-flats of Q_n contains $N(o,n)N(p-1,\, n-2)$ points. Hence (1) follows.

Primrose [21] has obtained the following formulae.

$$\Phi(o,k) = \frac{s^{2k} - 1}{s - 1}$$

(2)
$$\Phi_1(o,k) = \frac{(s^{2k} + s^{k-1} - s^k + 1)}{(s - 1)}$$

$$\Phi_2(o,k) = \frac{(s^{2k} - s^{k-1} + s^k - 1)}{(s - 1)} \quad .$$

Applying the difference equation (1) repeatedly and using the formulae (2), we get the required expressions for $\Phi(p,k)$, $\Phi_1(p,k)$ and $\Phi_2(p,k)$.

Theorem 5.2

The number of p-flats contained in a nondegenerate quadric Q_n in PG(n,s) which pass through a given k-flat Σ_k contained in Q_n is $N(p-k-1, n-2k-2)$, where $N(p,n)$ denotes the number of p-flats contained in a nondegenerate quadric of the type (elliptic or hyperbolic) of Q_n .

Proof. Let $\tau(\Sigma_k)$ denote the polar of Σ_k and Σ_{n-k-1} be an (n-k-1)-flat which does not intersect Σ_k . Let $\mathcal{L}_{k,p}$ denote the class of p-flats contained in Q_n and passing through Σ_k . Let $\mathcal{D}_{k,p}$ denote the class of (p-k-1)-flats contained in $Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k-1}$. By theorem 3.3a it is known that $Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k-1}$ is a nondegenerate quadric Q_{n-2k-2} in PG(n - 2k - 2, s) . Hence to prove the theorem it will be sufficient to show that there is a one to one correspondence between the classes $\mathcal{L}_{k,p}$ and $\mathcal{D}_{k,p}$ of p-flats.

Let $\Sigma_p \in \mathcal{L}_{k,p}$.

Then

(3) $\Sigma_k \subset \Sigma_p$.

(4) $\Sigma_k \cap \Sigma_{n-k-1} = \Phi$, the null set .

From (3) and (4) it follows that

$$\Sigma_p \not\subset \Sigma_{n-k-1} \quad .$$

So $\Sigma_p \cap \Sigma_{n-k-1}$ has dimensionality at least equal to (p-k-1). Since

$$\Sigma_k \cap \Sigma_{n-k-1} = \Phi$$

the dimensionality of $\Sigma_p \cap \Sigma_{n-k-1}$ cannot exceed (p-k-1). Hence $\Sigma_p \cap \Sigma_{n-k-1}$ is a (p-k-1)-flat Σ_{p-k-1} . Since

$$\Sigma_k \subset \Sigma_p \subset Q_n$$

by theorem (3.4) $\Sigma_p \subset \tau(\Sigma_k)$.

So $\Sigma_p \cap \Sigma_{n-k-1} \subset Q_n \cap \tau(\Sigma_k) \cap \Sigma_{n-k-1} = Q_{n-2k-2}$.

So $\Sigma_{p-k-1} \in \mathcal{D}_{k,p}$.

Let us make Σ_p of $\mathcal{Q}_{k,p}$ correspond to Σ_{p-k-1} of $\mathcal{D}_{k,p}$. It can easily be seen that the correspondence is unique.

6. Canonical forms of quadrics

Consider a quadric Q in PG(n,s) with rank r . Let $\sum_{j \geq i=0}^{n} a_{ij} x_i x_j$ be the form of Q . It is known that if the characteristic of the field is not 2, then by a nonsingular transformation

$$\underset{(\overline{n+1} \times 1)}{x} = \underset{(\overline{n+1} \times \overline{n+1})}{B} \; \underset{(\overline{n+1} \times 1)}{y}$$

the form of Q can be reduced to the canonical form $\sum_{t=0}^{r-1} \lambda_i y_i^2$ where λ's are non-zero elements of the field. It is shown by Dickson [15] that a

nondegenerate quadric Q_n in $PG(n, 2^m)$ can be reduced to one of the following canonical forms:

(1) $x_0^2 + x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0$, $n = 2k$

(2) $x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0$, $n = 2k - 1$

(3) $\lambda(x_1^2 + x_2^2) + x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0$, $n = 2k - 1$

where $\lambda(x_1^2 + x_2^2) + x_1x_2$ is irreducible in $GF(2^m)$. In the following theorem we have obtained certain canonical forms for the elliptic and hyperbolic nondegenerate quadrics in $PG(2k-1, s)$ for any prime power s .

Theorem 6.1

Let $GF(s)$ be a Galois field with characteristic not equal to 2. Let α be a non-zero element of $GF(s)$ such that $-\alpha$ is a square and β be a non-zero element such that $-\beta$ is a square. Let λ be an element of $GF(2^m)$ such that $\lambda(x_1^2 + x_2^2) + x_1x_2$ is irreducible in $GF(2^m)$. Then

(1) The quadric Q_{2k-1} in $PG(2k-1, s)$, $s \neq 2^m$, with the equation

$$x_1^2 + \alpha x_2^2 + x_3^2 + \alpha x_4^2 + \ldots + x_{2k-1}^2 + \alpha x_{2k}^2 = 0$$

is a hyperbolic nondegenerate quadric.

(2) The quadric Q_{2k-1} in $PG(2k-1,s)$, $s \neq 2^m$, with the equation

$$x_1^2 + \beta x_2^2 + x_3^2 + \alpha x_4^2 + \ldots + x_{2k-1}^2 + \alpha x_{2k}^2 = 0$$

is an elliptic nondegenerate quadric.

(3) The quadric Q_{2k-1} in $PG(2k-1, 2^m)$ with the equation

$$x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0$$

is a hyperbolic nondegenerate quadric.

(4) The quadric Q_{2k-1} in $PG(2k-1, 2^m)$ with the equation

$$\lambda(x_1^2 + x_2^2) + x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0$$

is an elliptic nondegenerate quadric.

Proof. (1) It is obvious that Q_{2k-1} is nondegenerate. We shall show that Q_{2k-1} is hyperbolic by finite induction on k. First we prove the result for $k = 1$. Since $-\alpha$ is a square element of $GF(s)$, there exists an element λ of $GF(s)$ such that

$$-\alpha = \lambda^2 \quad .$$

The equation of Q_1 is

$$x_1^2 + \alpha x_2^2 = 0 \quad .$$

It can be easily seen that Q_1 contains the two points $(\lambda, 1)$ and $(-\lambda, 1)$. Since Q_1 contains linear space of dimensionality 0 $(= k-1)$ i.e. points, Q_1 is hyperbolic. Assume that Q_{2k-3} is hyperbolic. Consider the nonsingular transformation

$$y_i = x_i \quad , \quad i = 1,2,\ldots,2k-2 \ .$$

$$y_{2k-1} = x_{2k-1} + \lambda x_{2k}$$

$$y_{2k} = x_{2k-1} - \lambda x_{2k} \quad .$$

It is easy to see that under this transformation Q_{2k-1} transforms to Q'_{2k-1} with the equation

$$y_1^2 + \alpha y_2^2 + y_3^2 + \alpha y_4^2 + \ldots + y_{2k-3}^2 + \alpha y_{2k-2}^2 + y_{2k-1}y_{2k} = 0 \quad .$$

Since the incidence properties in a projective geometry remain invariant over nonsingular transformations, it is sufficient to show that Q'_{2k-1} is hyperbolic. Consider the point

$$P = (0\ 0\ \ldots\ 0\ 1\ 0)$$

of Q'_{2k-1} . The equation of $\tau(P)$ is obviously

$$y_{2k} = 0 \quad .$$

Let π be the (n-1)-flat with the equation

$$y_{2k-1} = 0 \quad .$$

Then $Q'_{2k-1} \cap \tau \cap \pi$ has the equation

$$y_1^2 + \alpha y_2^2 + y_3^2 + \alpha y_4^2 + \ldots + y_{2k-3}^2 + \alpha y_{2k-2}^2 = 0 \quad .$$

By assumption $Q'_{2k-1} \cap \tau \cap \pi$ is hyperbolic and hence contains a (k-2)-flat Σ_{k-2} . The point P and the (k-2)-flat Σ_{k-2} are both contained in the quadric Q'_{2k-1} and are mutually conjugate. Hence by corollary 3.2 the (k-1)-flat $P \oplus \Sigma_{k-2}$ is contained in Q'_{2k-1} . Hence Q'_{2k-1} is hyperbolic.

(2) We shall prove the result by induction on k . First we prove the result for $k = 1$. The quadric Q_1 in $PG(1, s)$ with the equation

$$x_1^2 + \beta x_2^2 = 0$$

will be elliptic if Q_1 does not contain any point. If possible, suppose Q_1 contains a point (x'_1, x'_2) . Then $x'_2 \neq 0$. We can easily get

$$\frac{x'_1}{x'_2}^2 = -\beta$$

which contradicts the assumption that $-\beta$ is a non-square element. Hence Q_1 is elliptic.

Assume that the result is true for $(k - 1)$ so that Q_{2k-3} is

a nondegenerate elliptic quadric. Applying the nonsingular transformation used in part 1, we can transform Q_{2k-1} to Q'_{2k-1} with the equation

$$y_1^2 + \beta y_2^2 + y_3^2 + \alpha y_4^2 + \ldots + y_{2k-3}^2 + \alpha y_{2k-2}^2 + y_{2k-1}y_{2k} = 0 \quad .$$

As before it will be sufficient to show that Q'_{2k-1} is elliptic. If possible, suppose Q'_{2k-1} is hyperbolic. Then Q'_{2k-1} contains (k-1)-flats. Consider the point

$$P = (0\ 0\ \ldots\ 0\ 1\ 0) \quad .$$

The equation of $\tau(P)$ is

$$y_{2k} = 0 \quad .$$

Let π be the (n-1)-flat with the equation

$$y_{2k-1} = 0 \quad .$$

Then the equation of $Q'_{2k-1} \cap \tau \cap \pi$ is

$$y_1^2 + \beta y_2^2 + y_3^2 + \alpha y_4^2 + \ldots + y_{2k-3}^2 + \alpha y_{2k-2}^2 = 0 \quad ,$$

which is elliptic by induction assumption. By theorem 3.5.2 the number of p-flats passing through a point P of a nondegenerate quadric and contained in the quadric is equal for every point P of the quadric. Since Q'_{2k-1} contains (k-1)-flats, it follows that there exists a (k-1)-flat Σ_{k-1} contained in Q'_{2k-1} and passing through P. By theorem 3.4 Σ_{k-1} is contained in $Q'_{2k-1} \cap \tau(P)$. Hence Σ_{k-1} intersects $Q'_{2k-1} \cap \tau(P) \cap \pi$ in a (k-2)-flat Σ_{k-2}. So $Q'_{2k-1} \cap \tau(P) \cap \pi$ contains a (k-2)-flat Σ_{k-2}. This contradicts the assumption that $Q'_{2k-1} \cap \tau(P) \cap \pi$ is elliptic. This completes the proof of part (2).

Parts (3) and (4) of the theorem can be proved by arguments exactly similar to arguments used in parts (1) and (2) respectively.

7. Nucleus of polarity of a quadric in $PG(2k, 2^m)$.

Theorem 7.1

For every nondegenerate quadric Q_{2k} in $PG(2k, 2^m)$ there exists a point S not lying on the quadric such that every line through S intersects the quadric Q_{2k} in a single point. The point S is called the nucleus of polarity of Q_{2k}. For $PG(2, 2^m)$ this result was proved by Bose [3, p. 158].

Proof. Let Q'_{2k} be a nondegenerate quadric in $PG(2k, 2^m)$. Then according to Dickson [15] there exists a nonsingular transformation which transforms Q'_{2k} to Q_{2k} with the equation

$$x_0^2 + x_1x_2 + x_3x_4 + \ldots + x_{2k-1}x_{2k} = 0 \quad .$$

Since the incidence properties in a projective geometry are invariant over nonsingular transformations, it will be sufficient to prove the theorem for Q_{2k}. Let

$$S = (1\ 0\ 0\ \ldots\ 0) \quad .$$

We shall show that S possesses the required properties with respect to Q_{2k}. Obviously S is not a point of Q_{2k}. Let R be any other point not in Q_{2k}. It is easily seen that S and R are mutually conjugate. Then by theorem 7.2, which follows, the line SR intersects the quadric in a single point. Let R' be a point of the quadric. It is easy to see that S and R' are mutually conjugate.

If possible, suppose the line SR' intersects the quadric in another point R'' of Q_{2k}. Since S and R' are mutually conjugate, the point S occurs in $\tau(R')$, the tangent space at R'. Also $\tau(R')$ contains R'. So the line SR' is contained in $\tau(R')$. Hence R'' occurs in $\tau(R')$ and R' and R'' are mutually conjugate. R' and R'' are points of the quadric and are mutually conjugate. So by theorem 3.2 the line $R''R'$ is contained in Q_{2k}. So S is a point of Q_{2k} which is a contradiction.

Theorem 7.2

Let P and R be two points of $PG(2k, 2^m)$ not lying on a nondegenerate quadric Q_{2k} in $PG(2k, 2^m)$. The line PR intersects the quadric in a single point if and only if the points P and R are mutually conjugate.

Proof. Sufficiency. Let

$$P = (\alpha_o, \alpha_1, \ldots, \alpha_n)$$

$$R = (\beta_o, \beta_1, \ldots, \beta_n) \quad .$$

Let the equation of Q_{2k} be

$$\sum_{j \geq i=0}^{n} a_{ij} x_i x_j = 0 \quad .$$

Since P and R are not points of the quadric and are mutually conjugate, we have the following.

$$\sum_{j \geq i=0}^{n} a_{ij}\, \alpha_i \alpha_j \neq 0 \quad , \quad n = 2k$$

(1)
$$\sum_{j \geq i=0}^{n} a_{ij}\, \beta_i \beta_j \neq 0$$

$$\sum_{j \geq i=0}^{n} a_{ij}(\alpha_i \beta_j + \alpha_j \beta_i) = 0 \quad .$$

Any point on the line PR other than P and R can be expressed as

$$P + \lambda R = (\alpha_o + \lambda\beta_o, \alpha_1 + \lambda\beta_1, \ldots, \alpha_n + \lambda\beta_n)$$

where λ is a non-zero element of $GF(2^m)$. So the line PR will intersect Q_{2k} in a single point if the equation

(2)
$$\sum_{j \geq i=0}^{n} a_{ij}(\alpha_i + \lambda\beta_i)(\alpha_j + \lambda\beta_j) = 0$$

has a single solution in λ.

Using (1), (2) can be simplified as

(3)
$$\sum_{j \geq i=0}^{n} a_{ij}\, \alpha_i \alpha_j + \lambda^2 \sum_{j \geq i=0}^{2k} a_{ij}\, \beta_i \beta_j = 0 \quad .$$

From (1) and the fact that in $GF(2^m)$ every non-zero element has a unique square root, it follows that (3) has a unique solution in λ.

Necessity. Assume that the line PR intersects the quadric Q_{2k} in a single point R'. If possible, suppose P and R are not mutually conjugate. Noting that every point is self conjugate, it follows that R' and P cannot be mutually conjugate. Let

$$R' = (\alpha_o, \alpha_1, \ldots, \alpha_n)$$
$$P = (\beta_o, \beta_1, \ldots, \beta_n) \quad .$$

Then we have

$$\sum_{j \geq i=0}^{n} a_{ij}\, \alpha_i \alpha_j = 0$$

$$\sum_{j \geq i=0}^{n} a_{ij}\, \beta_i \beta_j \neq 0 \qquad (4)$$

$$\sum_{j \geq i=0}^{n} a_{ij}(\alpha_i \beta_j + \alpha_j \beta_i) \neq 0 \quad .$$

Let $$R'' = P + \lambda R'$$

where

$$\lambda = - \frac{\sum_{j \geq i=0}^{n} a_{ij}\, \beta_i \beta_j}{\sum_{j \geq i=0}^{n} a_{ij}(\alpha_i \beta_j + \alpha_j \beta_i)} \quad .$$

It can easily be seen that R'' is a point of Q_{2k}. This contradicts the assumption that the line PR intersects Q_{2k} in a single point. This completes the proof of necessity.

Theorem 7.3

If P is a point not lying on a quadric Q_n in $PG(n,s)$ and R is a point of the quadric such that P and R are not mutually conjugate, then the line PR intersects the quadric in two points.

Proof is very simple and hence is omitted.

CHAPTER II

SOME CLASSES OF PBIB DESIGNS WITH TWO ASSOCIATE CLASSES OBTAINED FROM THE CONFIGURATION OF LINEAR SPACES CONTAINED IN A QUADRIC

1. Summary

In the present chapter a general method of constructing Partially Balanced Incomplete Block Designs is debeloped. Let B and D be two classes of linear spaces in PG(n,s) such that every member of each class intersects a nondegenerate quadric Q_n in PG(n,s) in a quadric of the same nature. Then the configuration of the two classes B and D provides a PBIB design. The configuration of the generators and points of a nondegenerate quadric Q_n in PG(n,s) gives a class of PBIB design with two associate classes. Many other series with two associate classes are obtained. These series contain several new PBIB designs with r and k not greater than 10.

2. Introduction.

PBIB designs with two associate classes were introduced by Bose and Nair [7]. Bose and Shimamato [9] have rephrased the definition so as to stress the distinction between the association scheme and the design. Bose and Shimamato defintion for the PBIB design with m associate classes is substantially as follows.

A PBIB design with m associate classes is an arrangement of v treatments in b blocks such that

(1) Each of the v treatments is replicated r times in b blocks each of size k and no treatment occurs more than once in every block.

(2) There exists a relationship of association between every pair of the v treatments satisfying the following conditions:

(a) Any two treatments are either first associates or second associates ... or m-th associates.

(b) Each treatment has n_1 first associates, n_2 second associates, ... n_m m-th associates.

(c) Given any two treatments which are i-th associates, the number p^i_{jk} of treatments which are j-th associates of the first and k-th associates of the second is independent of the pair of treatments with which we start. Furthermore $p^i_{jk} = p^i_{kj}$, for $i,j,k = 1,2,...m$.

(3) Any pair of treatments which are i-th associates occur together in exactly λ_i blocks for $i = 1,2,...m$.

Bose and Clatworthy [5] have given a less demanding definition for the PBIB design with two associate classes which is as follows:

A PBIB design with two associate classes is an arrangement of v treatments in b blocks such that

(1) Each of the v treatments is replicated r times in b blocks each of size k and no treatment occurs more than once in any block.

(2) There exists a relationship of association between the v treatments satisfying the following conditions:

(a) Any two treatments are either first associates or second associates.

(b) Each treatment has n_1 first associates and n_2 second associates.

(c) For any pair of the v treatments which are i-th associate the number p_{11}^i of treatments common to the first associates of the first and first associates of the second is independent of the pair of treatments with which we start, i = 1,2.

(3) Any pair of treatments which are i-th associates occurs in exactly λ_i blocks, i=1,2.

Since it is easier to check the conditions of Bose-Clatworthy definition, we shall use this definition. The following relations hold between the parameters of a PBIB design and are useful for computing some parameters when others are known.

$$vr = bk ,$$

$$v = n_1+n_2+\ldots+n_m+1 ,$$

$$r(k-1) = \lambda_1 n_1+\lambda_2 n_2+\ldots+\lambda_m n_m ,$$

$$\text{(2.1)} \qquad \sum_{k=1}^{m} p_{jk}^i = \begin{cases} n_i-1, & \text{for } i = j \\ n_j, & \text{for } i \neq j \end{cases} \qquad i,j=1,2,\ldots m,$$

$$n_i p_{jk}^i = n_j p_{ik}^j , \quad i,j,k = 1,2,\ldots m.$$

A general method of constructing PBIB designs.

Let B denote the class consisting of the sets $B_1, B_2, \ldots B_b$ where B_j, $j=1,2,\ldots b$, is a set of points in PG(n,s). Let V denote another class consisting of the sets $V_1, V_2, \ldots V_v$ where V_i, $i=1,2,\ldots v$ is a set of points in PG(n,s). These two classes generate a design D(B,V) with the following incidence matrix

$$\underset{(vxb)}{N} = \underset{vxb}{((n_{ij}))}$$

where

$n_{ij} = 1$, if the sets V_i and B_j intersect each other,

0, if the sets V_i and B_j do not intersect.

Then we have the following.

$$r_i = \sum_{j=1}^{b} n_{ij} = \text{Number of sets of the class B which intersect } V_i.$$

$$k_j = \sum_{i=1}^{v} n_{ij} = \text{Number of sets of the class V which intersect } B_j.$$

$$\lambda_{ii'} = \sum_{j=1}^{b} n_{ij}n_{i'j} = \text{Number of sets of the class B which intersect both } V_i \text{ and } V_{i'},\ i \neq i' = 1,2,\ldots v.$$

Let $C_1, C_2, \ldots C_m$ be m classes of sets in PG (n,s) such that

$$V_i \cap V_{i'} \in C_j, \text{ for some } j, j=1,2,\ldots m.$$

The sets V_i and $V_{i'}$ are said to be j-th associates if

$$V_i \cap V_{i'} \in C_j,\ j=1,2,\ldots m.$$

Let $p^t_{uv}(V_i,V_{i'})$ denote the number of sets of the class V which are u-th associates of V_i and v-th associates of $V_{i'}$, $i \neq i'$, $i,i'=1,2,\ldots v$, $t,u,v = 1,2,\ldots m$.

Theorem 2.1

The design D(B,V) is a PBIB design with two associate classes if the following are true.

(1) Any two sets are either first associates or second associates ... or m-th associates.

(2) Each set $V_i(i=1,2,\ldots v)$ has n_1 first associates, n_2 second associates, ... n_m m-th associates.

(3) $p^t_{uv}(V_i,V_{i'})$ is independent of the t-th associate pair of sets $(V_i,V_{i'})$ and $p^t_{uv} = p^t_{vu}$, $t,v,u = 1,2,\ldots m$.

(4) $r_i = r$, $i = 1,2,\ldots v$ and $k_j = k$, $j=1,2,\ldots b$.

(5) For any pair of t-th associate sets $(v_i,V_{i'})$ $\lambda_{ii'} = \lambda_t$, $t = 1,2,\ldots m$.

Proof is obvious and hence omitted. As a consequence of Bose-Clatworthy definition of PBIB designs with two associate classes we have the following result which for the sake of reference is presented as corollary 2.1.

Corollary 2.1

The design D(B,V) is a PBIB design with two associate classes if the conditions (1), (2), (4) and (5) are satisfied for m=2 and the following condition (3)' is satisfied instead of (3).

(3)'. The number $p^t_{11}(V_i,V_{i'})$ is equal for every pair of t-th associate sets $(v_i,V_{i'})$, t=1,2.

3. PBIB designs from the configuration of generators for blocks and points for treatments of the quadric.

Definition. Generator. A line which is contained in a quadric is called a generator of the quadric.

Lemma 3.1.1

Let P_1 and P_2 be two points of a nondegenerate quadric Q_n in PG(n,s) such that the line P_1P_2 is not a generator. The number of points P such that both the lines PP_1 and PP_2 are generators of the quadric is N(0,n-2) where N(p,n) denotes the number of p-flats contained in a non-degenerate quadric of the type of Q_n(elliptic or hyperbolic) in PG (n,s).

Proof. Since the line P_1P_2 is not a generator, by theorem 3.2 of Chapter I the points P_1 and P_2 are not mutually conjugate. Let τ_1 and τ_2 denote the tangent spaces at P_1 and P_2 respectively. Let P be a point of Q_n such that both PP_1 and PP_2 are generators of Q_n. Since PP_1 is a generator, by theorem 3.2 of Chapter I P must be conjugate to P_1. Hence P must be a point of τ_1. Similarly, P must be a point of τ_2. Hence P is a point of $Q_n \cap \tau_1 \cap \tau_2$. Conversely if P is a point of $Q_n \cap \tau_1 \cap \tau_2$, P is conjugate to both P_1 and P_2 and hence both PP_1 and PP_2 are generators of Q_n. It follows from the above argument that the required number is equal to the number of points in $Q_n \cap \tau_1 \cap \tau_2$.

Since P_1 and P_2 are mutually not conjugate τ_2 does not pass through τ_1. So τ_1 is a tangent space at P_1 and τ_2 is an (n-1)-flat

not passing through P_1. By theorem 3.3 of Chapter I $Q_n \cap \tau_1 \cap \tau_2$ is a nondegenerate quadric Q_{n-2} in PG(n-2,s) which is elliptic or hyperbolic according Q_n is elliptic or hyperbolic. Hence the lemma follows.

Lemma 3.1.2

Let P_1 and P_2 be two points of Q_n in PG(n,s) such that P_1P_2 is a generator of Q_n. Then the number of points P other than P_1 and P_2 such that both PP_1 and PP_2 are generators of Q_n is

$$(s-1) + s^2N(0,n-4)$$

where N(p,n) has the same meaning as in lemma 3.1.1.

Proof. Let τ_1 and τ_2 be the tangent spaces at P_1 and P_2 respectively. Let Σ_{n-2} be an (n-2)-flat not intersecting the line Σ_1 determined by P_1 and P_2. Let P be a point of Q_n other than P_1 and P_2. As in the proof of lemma 3.3.1, we can show that both PP_1 and PP_2 are generators of Q_n if and only if P is a point of $Q_n \cap \tau_1 \cap \tau_2$. Hence the required number of points is equal to the number of points of $Q_n \cap \tau_1 \cap \tau_2$ other than P_1 and P_2. By theorem 3.1 of Chapter I

$$\tau_1 \cap \tau_2 = \tau(\Sigma_1), \text{ the polar of } \Sigma_1.$$

Then by theorem 3.3.a $Q_n \cap \tau(\Sigma_1) \cap \Sigma_{n-2}$ is Q_{n-4}, a nondegenerate quadric in PG(n-4,s) and $Q_n \quad \tau(\Sigma_1)$ is a cone of order 2 with Σ_1 as the vestex and $Q_n \quad \tau(\Sigma_1) \quad \Sigma_{n-2}$ as the base. It follows easily that the number of points $Q_n \quad \tau(\Sigma_1)$ is

$$(s+1) + s^2N(0,n-4).$$

Then the lemma follows from the fact that both P_1 and P_2 are points of $Q_n \cap \tau(\Sigma_1)$.

Theorem 3.1

Let B be the class of generators of Q_n, a nondegenerate quadric in PG(n,s) and V be the class of points of Q_n, each point being regarded as a point set. Then D(B,V) is a PBIB design with two associate classes with the following parameters.

$$
\begin{aligned}
v &= N(0,n), \\
b &= N(1,n), \\
k &= s+1, \\
r &= N(0,n-2), \\
\lambda_1 &= 1, \\
\lambda_2 &= 0, \\
n_1 &= s\,N(0,n-2), \\
p'_{11} &= (s-1) + s^2 N(0,n-4), \\
p^2_{11} &= N(0,n-2).
\end{aligned}
$$

The other parameters are easily obtained from the relations (2.1) between the parameters. In the above expressions N(p,n) denotes the number of p-flats contained in a nondegenerate quadric of the type of Q_n(elliptic or hybolic).

Proof. We shall apply corollary 2.1 to prove the theorem. It is easy to see the following:

b = Number of generators of Q_n,

= N(1,n).

k = Number of points on a generator,

= (s+1).

v = Number of points of Q_n,

= N(0,n).

r = Number of generators passing through a point,

= N(0,n-2) by theorem 5.2 of Chapter I.

The association scheme is defined as follows. Two points P_1 and P_2 of Q_n are first associates of each other if the line P_1P_2 is a generator and are second associates of each other if the line P_1P_2 is not a generator. Since there can be at most one generator passing through two points of Q_n, we have

$$\lambda_1 = 1$$

$$\lambda_2 = 0.$$

Let P_1 be a particular point of Q_n. The number of points P which are first associates to P_1 is equal to the number of points P such that PP_1 is a generator and hence equal to the number of points lying on the generators passing through P_1. From the above argument, we have

$$n_1 = sN(0,n-2).$$

Let P_1 and P_2 be two first associate points. Then P_1P_2 is a generator of Q_n. The number of points P which are first associates of both

P_1 and P_2 is equal to the number of points P other than P_1 and P_2 such that both PP_1 and PP_2 are generators. By lemma 3.3.2 this number is equal to

$$(s-1) + s^2 N(0,n-4).$$

From the above argument it follows that

$$P_{11}^1 = (s-1) + s^2 N(0,n-4).$$

Let P_1 and P_2 be two second associate points. Then the line P_1P_2 is not a generator. The number of points P which are first associates to both P_1 and P_2 is equal to the number of points P which are such that both PP_1 and PP_2 are generators. By lemma 3.3.1 this number does not depend on the particular pair of second associate points and is equal to N(0,n-2). From the above argument it follows that

$$P_{11}^2 = N(0,n-2).$$

Corollary 3.1.1

Taking n=2t, we get the series of PBIB designs with two associate classes with the following parameters

$$v = \frac{s^{2t}-1}{s-1},$$

$$r = \frac{s^{2t-2}-1}{s-1},$$

$$k = s+1,$$

$$b = \frac{(s^{2t}-1)(s^{2t-2}-1)}{(s-1)^2\,(s+1)},$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = \frac{s(s^{2t-2}-1)}{s-1},$$

$$p_{11}^1 = (s-1) + s^2\,\frac{(s^{2t-4}-1)}{(s-1)},$$

$$p_{11}^2 = \frac{s^{2t-2}-1}{s-1}.$$

Putting t=2, we get the following symmetric series.

$$v = b = s^3+s^2+s+1,$$

$$r = k = s+1,$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = s^2 + s,$$

$$p_{11}^1 = (s-1),$$

$$p_{11}^2 = s+1.$$

This series was obtained by Clatworthy [13] by a different method.

Corollary 3.1.2

Taking $n=2t-1$, $t \geq 3$, and Q_n elliptic we get the series of PBIB designs with two associate classes with the following parameters.

$$v = \frac{s^{2t-1}-s^t+s^{t-1}-1}{s-1},$$

$$r = \frac{s^{2t-3}-s^{t-1}+s^{t-2}-1}{s-1},$$

$$k = s+1,$$

$$b = \frac{(s^{2t-1}-s^t+s^{t-1}-1)(s^{2t-3}-s^{t-1}+s^{t-2}-1)}{(s-1)^2(s+1)},$$

$$\lambda_1 = 1,\ \lambda_2 = 0,$$

$$n_1 = \frac{s(s^{2t-3}-s^{t-1}+s^{t-2}-1)}{s-1},$$

$$p_{11}^1 = (s-1) + \frac{s^2(s^{2t-5}-s^{t-2}+s^{t-3}-1)}{s-1},$$

$$p_{11}^2 = \frac{s^{2t-3}-s^{t-1}+s^{t-2}-1}{s-1}.$$

Putting $t=3$, we get the following series.

$$v = (s^3+1)(s+1)$$

$$r = s^2+1$$

$$k = s+1$$

$$b = (s^3+1)(s^2+1)$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = s(s^2+1),$$

$$p_{11}^{1} = (s-1),$$

$$p_{11}^{2} = (s^2+1).$$

This series contains the following two designs with r and k not greater than 10.

Design Number	v	r	k	b	λ_1	λ_2	n_1	p_{11}^{1}	p_{11}^{2}
D_1	27	5	3	45	1	0	10	1	5
D_2	112	10	4	280	1	0	30	2	10

The design D_1 is included in BCS (Bose, Clatworthy and Shrikhande) catalogue [6]. The design D_2 is new.

Corollary 3.1.3

Taking $n = 2t-1, t \geq 2$, and Q_n hyperbolic, we get the series of PBIB designs with two associate classes with the following parameters.

$$v = \frac{s^{2t-1}+s^{t}-s^{t-1}-1}{s-1},$$

$$r = \frac{s^{2t-3}+s^{t-1}-s^{t-2}-1}{s-1},$$

$$k = s+1,$$

$$b = \frac{(s^{2t-1}+s^{t}-s^{t-1}-1)(s^{2t-3}+s^{t-1}-s^{t-2}-1)}{(s-1)^2(s+1)},$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = \frac{s(s^{2t-3}+s^{t-1}-s^{t-2}-1)}{(s-1)}$$

$$p_{11}^1 = (s-1) + \frac{s^2(s^{2t-5}+s^{t-2}-s^{t-3}-1)}{(s-1)}$$

$$p_{11}^2 = \frac{s^{2t-3}+s^{t-1}-s^{t-2}-1}{(s-1)}$$

Putting t = 2, we get the following one parameter family with the parameters.

$$v = (s+1)^2,$$

$$k = (s+1),$$

$$r = 2,$$

$$b = 2(s+1),$$

$$\lambda_1 = 1$$

$$\lambda_2 = 0$$

$$n_1 = 2s,$$

$$p_{11}^1 = (s-1),$$

$$p_{11}^2 = 2.$$

This family is same as the simple lattice family.

Putting t = 3, we get the following series.

$$v = (s^2+1)(s^2+s+1),$$

$$r = (s+1)^2$$

$$k = (s+1),$$

$$b = (s+1)(s^2+1)(s^2+s+1),$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$
$$n_1 = s(s+1)^2,$$
$$p_{11}^1 = (s-1)+2s^2,$$
$$p_{11}^2 = (s+1)^2.$$

This family contains only one design with r and k not greater than 10 with the following parameters.

$$v = 35, \quad r = 9, \quad k = 3, \quad b = 105, \quad \lambda_1 = 1, \quad \lambda_2 = 0$$
$$n_1 = 18, \; p_{11}^1 = 9, \; p_{11}^2 = 9.$$

This design is new.

Example.

The actual method of writing down the blocks is illustrated in the following example. Consider the design D_1 of the series given in corollary 3.1.1. The parameters are

$$v = b = 15, \; r = k = 3, \; \lambda_1 = 1, \; \lambda_2 = 0, \; n_1 = 6, \; p_{11}^1 = 1, \; p_{11}^2 = 3.$$

This design is obtained by taking generators of Q_4, a nondegenerate quadric in PG(4,2), as blocks and points of Q_4 as treatments. The equation of Q_4 can be taken as

$$x_0^2 + x_1x_2 + x_3x_4 = 0.$$

The 15 points of Q_4 are

$P_1 = (00001)$, $P_9 = (11101)$,

$P_2 = (00010)$, $P_{10} = (00110)$,

$P_3 = (10011)$, $P_{11} = (01010)$,

$P_4 = (00100)$, $P_{12} = (11110)$,

$P_5 = (01000)$, $P_{13} = (10111)$,

$P_6 = (11100)$, $P_{14} = (11011)$,

$P_7 = (00101)$, $P_{15} = (01111)$.

$P_8 = (01001)$,

To write down the blocks systematically we can proceed as follows. Consider the treatment 1. The blocks which contain treatmentl correspond to the generators containing the point P_1. So find out the generators passing through P_1, we find out $Q_4 \cap \tau(P_1)$ where $\tau(P_1)$ is the tangent space at P_1. For any point P of $Q_4 \cap \tau(P_1)$, PP_1 is a generator. In this way we can exhaust all the blocks containing treatment 1. Next we proceed to treatment 2 and by a similar procedure can find out the blocks containing treatment 2 which are not already included. We continue in this manner until all the blocks are obtained.

In our example the 15 generators are P_1P_4, P_1P_5, P_1P_6, P_2P_4, P_2P_5, P_2P_6, P_3P_4, P_3P_5, P_3P_6, P_7P_{11}, P_7P_{12}, P_8P_{10}, P_8P_{12}, P_9P_{10}, and P_9P_{11}. So the 15 blocks of the designs are

(1,4,7), (1,5,8), (1,6,9),

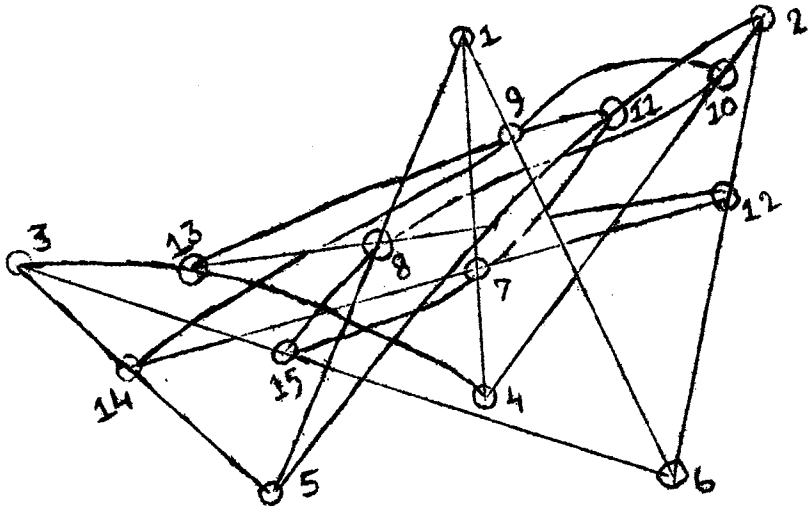
(2,4,10), (2,5,11), (2,6,12),

(3,4,13), (3,5,14), (3,6,15),

(7,11,15), (7,12,14), (8,10,15),

(8,12,13), (9,10,14) and (9,11,13).

The quadric Q_4 can be represented by the following diagram where points of Q_4 are represented by small circles and three points on a generator are joined together by a straight line or a continuous curve.



4. PBIB designs from the configuration of points of a quadric for blocks and generators of a quadric for treatments.

Let Q_n be a nondegenerate quadric in PG(n,s) which contains lines but does not contain planes. Thus Q_n can be a nondegenerate quadric in PG(4,s) or an elliptic quadric in PG(5,s) or a hyperbolic nondegenerate quadric in PG(3,s).

Lemma 4.1.1

Let ℓ be a generator of Q_n. The number of generators intersecting ℓ (other than ℓ) is

$$N(0,n-2)-1 \quad (s+1).$$

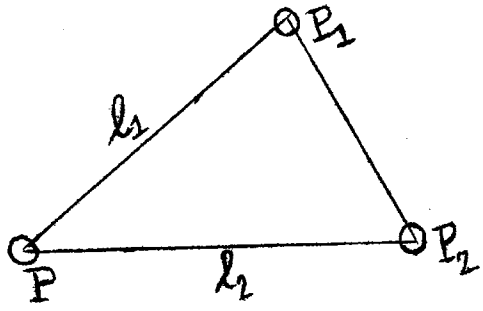
Proof. The line ℓ contains (s+1) points. By theorem 5.2 of Chapter I, the number of generators through every point of ℓ is $N(0,n-2)$ of which ℓ is one. Hence the lemma follows.

Lemma 4.1.2

Let ℓ_1 and ℓ_2 be two intersecting generators of Q_n. Then the number of generators other than ℓ_1 and ℓ_2 which intersect both ℓ_1 and ℓ_2 is

$$N(0,n-2)-2$$

Proof. Suppose the two generators in ℓ_1 and ℓ_2 intersect at the point P.



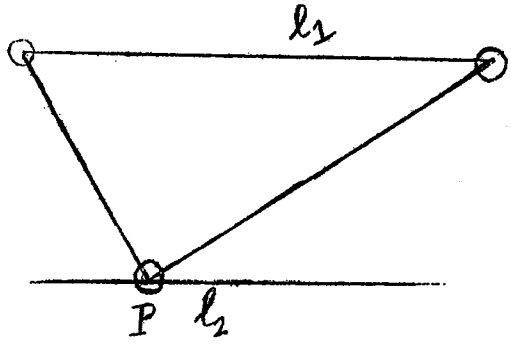
Then there cannot be any generator which intersects both ℓ_1 and ℓ_2 at points other than P. If possible, suppose there exists a generator which intersects ℓ_1 at P_1 and ℓ_2 at P_2. Then the three points P, P_1 and P_2 are mutually conjugate and are points of Q_n. So by theorem 3.2

of Chapter I, the plane determined by them is contained in Q_n. This contradicts the assumption that Q_n does not contain any planes. So it follows that the required generators are those which intersect both ℓ_1 and ℓ_2 at the point P. By theorem 5.2 of Chapter I the number of generators passing through P is N(0,n-2) of which ℓ_1 and ℓ_2 are two generators. Hence the lemma follows

Lemma 4.1.3

Let ℓ_1 and ℓ_2 be two nonintersecting generators of Q_n. Then the number of generators which intersect both ℓ_1 and ℓ_2 is (s+1).

Proof.



Let P be a point of the generator ℓ_2. Consider the generators which intersect ℓ_2 at P and also intersect ℓ_1. Any such generator will lie in the plane Σ_2 determined by ℓ_1 and the point P. The plane Σ_2 is not contained in Q_n and contains a generator ℓ_1 of Q_n and a point P of Q_n not lying on ℓ_1. From these facts it follows easily that Σ_2 intersects Q_n in a pair of lines. Hence there exists one and only one line passing through P and intersecting ℓ_1. This is true for every point of ℓ_2 and the number of points of ℓ_2 is (s+1). Hence the lemma follows.

Theorem 4.1

Let B be the class of points of Q_n a nondegenerate quadric in PG(n,s) which does not contain planes.

Let V be the class of generators of Q_n. Then D(B,V) is a PBIB design with two associate classes with the following parameters.

$$v = N(1,n),$$
$$r = s+1,$$
$$k = N(0,n-2),$$
$$b = N(0,n),$$
$$\lambda_1 = 1,$$
$$\lambda_2 = 0,$$
$$n_1 = \lfloor \overline{N}(0,n-2)-1 \rfloor (s+1),$$
$$p_{11}^1 = N(0,n-2)-2,$$
$$p_{11}^2 = (s+1).$$

The other parameters can be obtained from the relations (2.1) between the parameters of PBIB design.

Proof. We shall apply corollary 2.1 to prove this theorem. The following results can be obtaned easily.

v = Number of generators of Q_n

= N(1,n).

r = Number of points of Q_n intersecting a generator,

= (s+1).

k = Number of generators of Q_n intersecting a point,

= N(0,n-2).

b = Number of points of Q_n

= N(0,n).

The association scheme is defined as follows. Two generators ℓ_1 and ℓ_2 of Q_n are first associates if they intersect and are second associates if they do not intersect. Since two generators of Q_n can intersect at most one point, we have $\lambda_1=1$, $\lambda_2=0$.

Let ℓ_1 be a given generator. The number of generators which are first associates to ℓ_1 is equal to the number of generators which intersect ℓ_1. Hence we have from lemma 4.1.1

$$n_1 = \left[N(0,n-2) - 1 \right] (s+1)$$

The constancy of the parameters p_{11}^1 and p_{11}^2 and their expressions follow from lemma 4.1.2 and 4.1.3 by using an argument exactly similar to that used in the proof of theorem 2.1.

Corollary 4.1.1

Taking n = 5 and Q_5 an elliptic nondegenerate quadric in PG(5,s) we get the following series of PBIB designs with two associate classes.

$$v = (s^3+1)(s^2+1),$$

$$r = (s+1),$$

$$k = (s^2+1),$$

$$b = (s^3+1)(s+1),$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = s^2(s+1),$$

$$p_{11}^1 = s^2-1,$$

$$p_{11}^2 = s+1.$$

This series contains the following two designs with r and k not greater than 4.

Design Number	v	r	k	b	λ_1	λ_2	n_1	p_{11}^1	p_{11}^2
D_1	45	3	5	27	1	0	12	3	3
D_2	280	4	10	112	1	0	36	8	4

The design D_1 is included in the BCS catalogue. The design D_2 is new.

Corollary 4.1.2

Taking n = 3 and Q_3 an hyperbolic nondegenrate quadric in PG(3,s) we get the following series of PBIB designs with two associate classes.

$$v = 2(s+1),$$
$$r = s+1,$$
$$k = 2,$$
$$b = (s+1)^2,$$
$$\lambda_1 = 1,$$
$$\lambda_2 = 0,$$
$$n_1 = s+1,$$
$$p_{11}^1 = 0,$$
$$p_{11}^2 = s+1.$$

This series is given by Clatworthy [14].

5. PBIB designs from the configuration of generators on generators.

Theorem 5.1.

Let B be the class of generators of a nondegenerate quadric Q_n which contains lines but does not contain planes. If two coincident generators are regarded as nonintersecting, D(B,B) is a PBIB design with two associate classes with the following parameters.

$$v = b = N(1,n),$$
$$r = k = [N(0,n-2)-1](s+1),$$
$$\lambda_1 = N(0,n-2)-2,$$
$$\lambda_2 = (s+1),$$
$$n_1 = N(0,n-2)-1 \quad (s+1),$$
$$p_{11}^1 = N(0,n-2)-2,$$
$$p_{11}^2 = (s+1).$$

Proof. We shall apply corollary 2.1 to prove this theorem. The following results can be easily obtained.

$v = b$ = Number of generators of Q_n,

$= N(1,n)$.

$r = k$ = Number of generators intersecting a given generator excluding the given generator

$= \lceil N(0,n-2)-1 \rceil \ (s+1)$ by lemma 4.1.1.

The association scheme is defined as follows. If two generators intersect, they are first associates. If two generators do not intersect, they are second associates.

Let ℓ_1 and ℓ_2 be two generators which intersect each other. By lemma 4.1.2 the number of generators other than ℓ_1 and ℓ_2 which intersect both ℓ_1 and ℓ_2 is $N(0,n-2)-2$. Hence we have

λ_1 = Number of generators otherthan ℓ_1 and ℓ_2 which intersect both ℓ_1 and ℓ_2,

$= N(0,n-2)-2$.

Similarly by lemma 4.1.3

$$\lambda_2 = (s+1).$$

The constancy of p_{11}^1 and p_{11}^2 and their expressions also follow from lemma 4.1.2 and 4.1.3.

Corollary 5.1.1.

Taking Q_n a nondegenerate quadric in PG(4,s) we get the following series of PBIB designs with two associate classes.

$$v = b = s^3+s^2+s+1,$$

$$r = k = s(s+1),$$

$$\lambda_1 = (s-1),$$

$$\lambda_2 = (s+1),$$

$$n_1 = s(s+1),$$

$$p_{11}^1 = (s-1),$$

$$p_{11}^2 = (s+1).$$

This series contains only one design with r and k not greater than 10. This design is new. The parameters are

$$v = b = 15,\ r = k = 6,\ \lambda_1 = 1,\ \lambda_2 = 3,\ n_1 = 6,\ p_{11}^1 = 1,\ p_{11}^2 = 3.$$

Theorem 5.2.

Let B be the class of generators of a nondegenrate quadric Q_n in PG(n,s) which contains lines but does not contain planes. If two coincident generators are considered as intersecting, the D(B,B) is a PBIB design with two associate classes with the following parameters.

$$v = b = N(1,n),$$

$$r = k = (s+1)N(0,n-2)-s,$$

$$\lambda_1 = N(0,n-2),$$

$$\lambda_2 = (s+1),$$

$$n_1 = \lfloor N(0,n-2)-1 \rfloor\ (s+1),$$

$$p_{11}^1 = N(0,n-2)-2,$$

$$p_{11}^2 = (s+1).$$

Proof. The association scheme is defined as in theorem 5.1. If two generators of Q_n intersect, they are first associates. If they do not intersect, they are second associates. The paramters of the association scheme are obtained by the same argument as used in the proof of theorem 5.1. The expressions for v and b are obvious. Also, we have

$r = k$ = Number of generators which intersect a given generator including the given generator,

= $\lfloor N(0,n-2)-1 \rfloor\ (s+1)+1$ by lemma 4.1.1.

λ_1 = Number of generators which intersect two given mutually intersecting generators including the two given generators,

= $N(0,n-2)$ by lemma 4.1.2.

λ_2 = Number of generators which intersect two mutually non-intersecting generators,

= $(s+1)$ by lemma 4.1.3.

This completes the proof of the theorem.

Corollary 5.2.1.

Taking Q_n as a hyperbolic nondegenerate quadric in PG(3,s) we get the following series.

$$v = b = 2(s+1), \quad r = k = (s+2), \quad \lambda_1 = 2, \quad \lambda_2 = (s+1),$$

$$n_1 = b = 2(s+1), \quad p_{11}^1 = 0, \quad p_{11}^2 = (s+1).$$

This series is given by Clatworthy [12].

6. PBIB designs obtained from the configuration of lines and points of PG(3,s) truncated by a quadric.

Let $Q_1, Q_2, \ldots, Q_{s+1}$ be (s+1) points on a nondegenerate quadric on a plane Σ_2 in PG(3,s), $s=2^m$. Let Q_o be the nucleus of polarity of the quadric.

Lemma 6.1.1

Let P_1 be a point of PG(3,s) not lying on Σ_2. The number of points P other than P_1 not lying on Σ_2 such that PP_1 is a line passing through one of the points $Q_o, Q_1, \ldots, Q_{s+1}$ is

$$(s+2)(s-1)$$

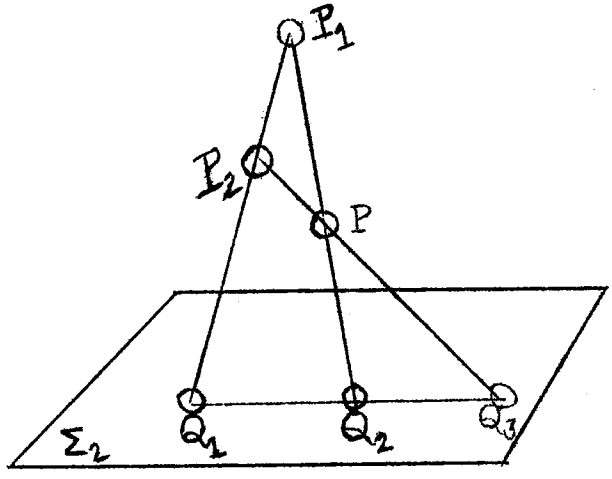
Proof is simple and hence omitted.

Lemma 6.1.2

Let P_1 and P_2 be two points which do not lie on Σ_2 and which are such that the line P_1P_2 passes through one of the points $Q_o, Q_1, \ldots, Q_{s+1}$. The number of points P other than P_1 and P_2 not lying on Σ_2 such that

both the lines PP_1 and PP_2 pass through one of the points $Q_0, Q_1, \ldots, Q_{s+1}$ is (s-2).

Proof.



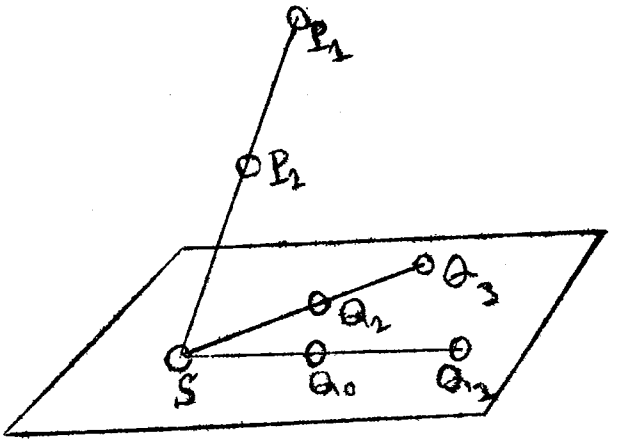
The points on the line P_1P_2 other than P_1, P_2 and Q_1, the point of intersection of P_1P_2 and Σ_2, possess the required property. So the line P_1P_2 contributes (s-1) points. If possible suppose there exists a point P not lying on the line P_1P_2 which possesses the required property. Let Q_2 and Q_3 be respectively the intersections of the lines PP_1 and PP_2 with Σ_2. Obviously the three points Q_1, Q_2 and Q_3 are collinear. Bose [3] has shown that the (s+2) points $Q_0, Q_1, \ldots, Q_{s+1}$ are such that no three of these points are collinear. Hence our assumption that there exists a point P outside the line P_1P_2 satisfying the required conditions leads to a contrdiction. This completes the proof of the lemma.

Lemma 6.1.3

Let P_1 and P_2 be two points not lying on the plane Σ_2 such that the line P_1P_2 does not pass through one of the points $Q_0, Q_1, \ldots, Q_{s+1}$. Then the number of points P other than P_1 and P_2 not lying on Σ_2 such

that both the lines PP_1 and PP_2 pass through one of the points $Q_o, Q_1, \ldots, Q_{s+1}$ is $(s+2)$.

Proof. Let S be the point of intersection of P_1P_2 and Σ_2.

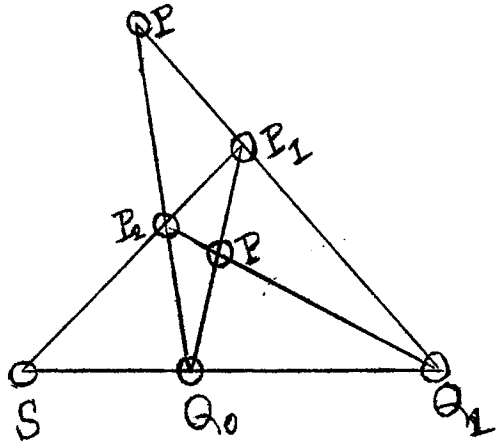


Since Q_o is the nucleus of polarity of the quadric containing the points $Q_1, Q_2, \ldots, Q_{s+1}$ in Σ_2, by theorem 7.1 of Chapter I, the line SQ_o will intersect the quadric in a single point Q_1(say). Consider the line SQ_2.

Since the line SQ_o intersects the quadric in a single point, by theorem 7.2 of Chapter I S and Q_o are mutually conjugate and SQ_o is the polar of S with respect to the quadric. Since Q_2 is not on the line SQ_o, S and Q_2 are not mutually conjugate and the line SQ_2 will be a secant. So the line SQ_2 contains another point Q, say Q_3. Similarly, any line through S containing one of the points of $Q_o, Q_1, \ldots, Q_{s+1}$ will contain a second point Q. Suppose the $(s+2)$ points Q lie on the $\frac{s+2}{2}$ lines, SQ_oQ_1, SQ_2Q_3, $\ldots$, SQ_sQ_{s+1}.

Any point P satisfying the required property must lie on one of the planes $P_2Q_oQ_1$, $P_2Q_2Q_3$, $\ldots$ $P_2Q_sQ_{s+1}$.

From the diagram given below we can easily see that any such plane contributes two points P.



Hence the total number of points P is (s+2).

Theorem 6.1

Let B be the class of lines in PG(3,s) not lying in Σ_2 and passing through one of the points $Q_0, Q_1, \ldots Q_{s+1}$. Let V be the class of points of PG(3,s) not lying on Σ_2. Then D(B,V) is a PBIB design with two associate classes with the following parameters.

$$v = s^3, \quad s=2^m,$$

$$r = s+2,$$

$$k = s,$$

$$b = s^2(s+2),$$

$$\lambda_1 = 1,$$

$$\lambda_2 = 0,$$

$$n_1 = (s+2)(s-1),$$

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

$$p_{11}^2 = (s+2).$$

Proof. The association scheme is defined as follows. Two points P_1 and P_2 are first associates if the line P_1P_2 passes through one of the points $Q_0, Q_1, \ldots, Q_{s+1}$ and second associates otherwise. Then the proof of the theorem follows easily from lemmas 6.1.1, 6.1.2, and 6.1.3.

This series contains the following 3 designs with r and k not greater than 10.

Design Number	v	r	k	b	λ_1	λ_2	n_1	p_{11}^1	p_{11}^2
D_1	8	4	2	16	1	0	4	0	4
D_2	64	6	4	96	1	0	18	2	6
D_3	512	10	8	640	1	0	70	6	10

The design D_1 is given in Clatworthy [14]. The designs D_2 and D_3 are new.

7. Concluding remarks.

The method of constructing PBIB designs developed in this chapter is very general. It is possible to obtain many series of PBIB designs with two associate classes from the configuration of linear spaces of higher dimensionality contained in the quadric. These series are not included since they do not contain new designs with r and k not greater than 10. However, these designs may be useful in experiments other than varietal trial, for instance in asymmetrical factorial experiments.

CHAPTER III

SOME CLASSES OF PBIB DESIGNS WITH THREE ASSOCIATE CLASSES

1. Summary.

In this chapter a theorem is proved about PBIB designs with three associate classes which in effect gives a much less demanding definition of PBIB design with three associate classes. This theorem is applied to construct PBIB designs with three associate classes. A series of PBIB designs with three associate classes is obtained from the configuration of generator and points of cone with a point vertex. Another series of PBIB designs with three associate classes is obtained from the configuration of secants and external points of a nondegenerate quadric in finite projective plane. These two series contain the following designs with r and k not greater than 10. The following table gives the parameters v, r, k, b, λ_1, λ_2, λ_3, n_1, n_2, p_{11}^i, p_{12}^i, p_{22}^i for i = 1, 2, 3. The other parameters can be obtained from the well known relations between the parameters of a PBIB design.

All these designs are new.

Design number	v	r	k	b	λ_1	λ_2	λ_3	n_1	n_2	p_{11}^1	p_{12}^1	p_{22}^1	p_{11}^2	p_{12}^2	p_{22}^2	p_{11}^3	p_{12}^3	p_{22}^3
D_1	15	2	3	10	1	0	0	4	2	1	0	0	0	0	1	1	1	0
D_2	18	4	3	24	1	0	0	8	1	2	1	0	8	0	0	4	0	0
D_3	30	6	3	60	1	0	0	12	1	2	1	0	12	0	0	6	0	0
D_4	48	6	4	72	1	0	0	18	2	6	2	0	18	0	1	6	0	0
D_5	54	10	3	180	1	0	0	20	1	2	1	0	20	0	0	10	0	0
D_6	63	4	7	36	1	0	0	24	6	9	2	0	8	0	5	9	3	0
D_7	100	8	5	160	1	0	0	32	3	12	3	0	32	0	2	8	0	0
D_8	180	10	6	300	1	0	0	50	4	20	4	0	50	0	3	10	0	0

2. A theorem on three associate PBIB designs.

In this section a theorem on three associate PBIB designs is proved which actually is an extension of a theorem of Bose and Clatworthy [5] for PBIB designs with two associate classes. Before proving this theorem we shall prove a lemma.

Lemma 2.1.1.

Let $p_{jk}^i(\theta,\phi)$ denote the number of treatments which are j-th associates of θ and k-th associates of ϕ where (θ,ϕ) is a pair of i-th associate treatments, i,j,k = 1,2,3.

Let there exist a relationship of association between every pair among v treatments satisfying the following:

(a) Any two treatments are either first associates or second associates or third associates.

(b) Each treatment has n_1 first associates, n_2 second associates and n_3 third associates.

(c) The numbers $p_{11}^i(\theta,\phi)$, $p_{12}^i(\theta,\phi)$ and $p_{22}^i(\theta,\phi)$ are independent of the particular pair of i-th associates (θ,ϕ) and $p_{12}^i(\theta,\phi) = p_{21}^i(\theta,\phi)$, $i = 1,2,3$.

Then the numbers $p_{13}^i(\theta,\phi)$, $p_{31}^i(\theta,\phi)$, $p_{23}^i(\theta,\phi)$, $p_{32}^i(\theta,\phi)$ and $p_{33}^i(\theta,\phi)$ are independent of the particular pair of i-th associates (θ,ϕ) and $p_{13}^i(\theta,\phi) = p_{31}^i(\theta,\phi)$, $p_{23}^i(\theta,\phi) = p_{32}^i(\theta,\phi)$, $i = 1,2,3$.

Proof. Consider the pair of treatments (θ,ϕ) which are first associates. The n_1 first associates of θ are made up ϕ, $p_{11}^1(\theta,\phi)$ treatments which are first associates of both θ and ϕ, $p_{12}^1(\theta,\phi)$ treatments which are first associates of θ and second associates of ϕ and $p_{13}^1(\theta,\phi)$ treatments which are first associates of θ and third associates of ϕ. So we have the identity

$$(2.1) \qquad \ldots\ldots \quad 1 + p_{11}^1(\theta,\phi) + p_{12}^1(\theta,\phi) + p_{13}^1(\theta,\phi) = n_1 .$$

Similarly considering the first associates of ϕ, we get

$$(2.2) \qquad \ldots\ldots \quad 1 + p_{11}^1(\theta,\phi) + p_{21}^1(\theta,\phi) + p_{31}^1(\theta,\phi) = n_1 .$$

Applying similar considerations to the second associates of θ and the second associates of ϕ and remembering that θ and ϕ are first associates we get

$$(2.3) \qquad \ldots\ldots \quad p_{21}^1(\theta,\phi) + p_{22}^1(\theta,\phi) + p_{23}^1(\theta,\phi) = n_2 ,$$

$$(2.4) \qquad \ldots\ldots \; p_{12}^{1}(\theta,\phi) + p_{22}^{1}(\theta,\phi) + p_{32}^{1}(\theta,\phi) = n_2 \; .$$

Similarly considering the third associates we get

$$(2.5) \qquad \ldots\ldots \; p_{31}^{1}(\theta,\phi) + p_{32}^{1}(\theta,\phi) + p_{33}^{1}(\theta,\phi) = n_3 \; ,$$

$$(2.6) \qquad \ldots\ldots \; p_{13}^{1}(\theta,\phi) + p_{23}^{1}(\theta,\phi) + p_{33}^{1}(\theta,\phi) = n_3 \; .$$

Solving these equalities we get

$$(2.7) \quad \ldots\ldots \begin{aligned} p_{13}^{1}(\theta,\phi) = p_{31}^{1}(\theta,\phi) &= n_1 - p_{11}^{1}(\theta,\phi) - p_{12}^{1}(\theta,\phi) - 1 \\ p_{23}^{1}(\theta,\phi) = p_{32}^{1}(\theta,\phi) &= n_2 - p_{12}^{1}(\theta,\phi) - p_{22}^{1}(\theta,\phi) \\ p_{33}^{1}(\theta,\phi) &= n_3 - n_1 - n_2 + p_{11}^{1}(\theta,\phi) + 2p_{12}^{1}(\theta,\phi) + p_{22}^{1}(\theta,\phi) + 1 \; . \end{aligned}$$

By assumption $p_{11}^{1}(\theta,\phi)$, $p_{12}^{1}(\theta,\phi)$ and $p_{22}^{1}(\theta,\phi)$ are independent of the particular pair of first associates (θ,ϕ). Hence from (2.7) it follows that $p_{13}^{1}(\theta,\phi)$, $p_{23}^{1}(\theta,\phi)$ and $p_{33}^{1}(\theta,\phi)$ are independent of the particular pair of first associates (θ,ϕ). This completes the proof of the lemma for i = 1. Similarly the lemma can be proved for i = 2 and 3.

Theorem 2.1.

If an arrangement of v treatments in b blocks is such that the following conditions are satisfied:

(i) Each of the v treatments is replicated r times in b blocks each of size k and no treatment occurs more than once in any block.

(ii) There exists a relationship of association between every pair of the v treatments satisfying the following conditions:

(a) Any two treatments are either first or second or third associates.

(b) Each treatment has n_1 first associates, n_2 second associates and n_3 third associates.

(c) Given any two treatments which are i-th associates, the numbers p_{11}^i, p_{12}^i and p_{22}^i are independent of the pair of i-th associates with which we start, i = 1,2,3 and $p_{12}^i = p_{21}^i$, i = 1,2,3.

(iii) Any pair of treatments which are i-th associates occur together in λ_i blocks for i = 1,2,3,

then this arrangement is a PBIB design with three associate classes with the following parameters.

$$v,\ b,\ r,\ k,\ \lambda_1, \lambda_2, \lambda_3,\ n_1, n_2, n_3,\ p_{11}^1, p_{12}^1,$$

$$p_{13}^1 = n_1 - p_{11}^1 - p_{12}^1 - 1,\quad p_{21}^1 = p_{12}^1, p_{22}^1, p_{23}^1 = n_2 - p_{22}^1 - p_{12}^1,$$

$$p_{31}^1 = p_{13}^1,\ p_{32}^1 = p_{23}^1,\ p_{33}^1 = n_3 - n_1 - n_2 + 2p_{12}^1 + p_{22}^1 + p_{11}^1 + 1,$$

$$p_{11}^2, p_{12}^2, p_{13}^2 = n_1 - p_{11}^2 - p_{12}^2,\ p_{21}^2 = p_{12}^2, p_{22}^2,$$

$$p_{23}^2 = n_2 - p_{22}^2 - p_{12}^2 - 1,\ p_{31}^2 = p_{13}^2,\ p_{32}^2 = p_{23}^2,$$

$$p_{33}^2 = n_3 - n_1 - n_2 + 2p_{12}^2 + p_{11}^2 + p_{22}^2 + 1,\ p_{11}^3, p_{12}^3,$$

$$p_{13}^3 = n_1 - p_{11}^3 - p_{12}^3, p_{21}^3 = p_{12}^3, p_{22}^3, p_{23}^3 = n_2 - p_{12}^3 - p_{22}^3,$$

$$p_{31}^3 = p_{13}^3, p_{32}^3 = p_{23}^3, p_{33}^3 = n_3 - n_1 - n_2 - 1 + 2p_{12}^3 + p_{11}^3 + p_{22}^3 .$$

Proof follows easily from lemma 2.1.1.

Theorem 2.1 provides a very useful way of checking whether a given arrangement is a PBIB design with 3 associate classes or not. The usual definition of PBIB designs with three associate classes requires the constancy of 27 parameters of the second kind p_{jk}^i,

$i,j,k = 1,2,3$ whereas due to theorem (2.1) we need to check the constancy of 9 parameters of the second kind namely p_{11}^i, p_{12}^i and p_{13}^i, $i = 1,2,3$. Also the usual definition requires 9 symmetry conditions of the type $p_{jk}^i = p_{kj}^i$, $i,j,k = 1,2,3$. In theorem 2.1 we need to check only 3 symmetry conditions.

Corollary 2.1.1.

Let B and V be two classes of sets in PG(n,s) and D(B,V) be the design as defined in section 2 of Chapter II. Let r_i, k_j and $\lambda_{ii'}$ have the same meaning as in section 2 of Chapter II. Then D(B,V) is a PBIB design with three associate classes if the following are true.

(i) r_i and k_j are constants for $i = 1,2,\ldots,v$ and $j = 1,2,\ldots,b$.

(ii) Any pair of sets are either first associates or second associates or third associates.

(iii) Each set V_i has n_1 first associates, n_2 second associates and n_3 third associates, $i = 1,2,\ldots,v$.

(iv) Given a pair of sets $(V_i,V_{i'})$ which are t-th associates the numbers $p_{11}^t(V_i,V_{i'})$, $p_{12}^t(V_i,V_{i'})$ and $p_{22}^t(V_i,V_{i'})$ are independent of the particular pair of t-th associates $(V_i,V_{i'})$ and $p_{12}^t = p_{21}^t$, $t = 1,2,3$.

(v) For any pair of t-th associates $(V_i,V_{i'})$, $\lambda_{ii'} = \lambda_t$, $t = 1,2,3$.

3. Some PBIB designs with three associate classes obtained from the configuration of generators and points of a cone.

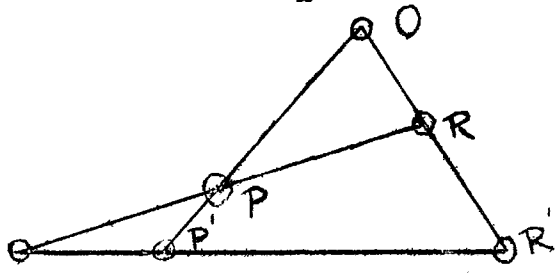
Let Q_{n-1} be a nondegenerate quadric on an (n-1)-flat Σ_{n-1} in PG(n,s) and Q_n be the cone with Q_{n-1} as the base and a point O outside

Σ_{n-1} as the vertex. As in Chapter II we shall use N(p, n-1-2t) to denote the number of p-flats contained in a nondegenerate quadric of the type of Q_{n-1} (hyperbolic or elliptic) in PG(n-1-2t). Now we shall prove some lemmas which will be used later.

Lemma 3.1.1.

Let P be any point of Q_n other than O. Then the number of generators which pass through P but do not pass through O is sN(O, n-3).

Proof. Let PR be a generator of Q_n not passing through O.



Then the three points O, P and R are points of Q_n and mutually conjugate. So by theorem 3.2 of Chapter I, the plane OPR is contained in Q_n. Let P'R' be the intersection of OPR and Σ_{n-1}. Then P'R' is a generator of Q_{n-1}. Hence any such generator PR is contained in a plane OP'R' where P' is the intersection of OP and Σ_{n-1} and P'R' is a generator of Q_{n-1}. The number of such planes OP'R' is equal to the number of generators of Q_{n-1} passing through P' and hence by theorem 5.2 is equal to N(O, n-3). Every plane OP'R' contains s generators passing through P but not through O. Hence the lemma follows.

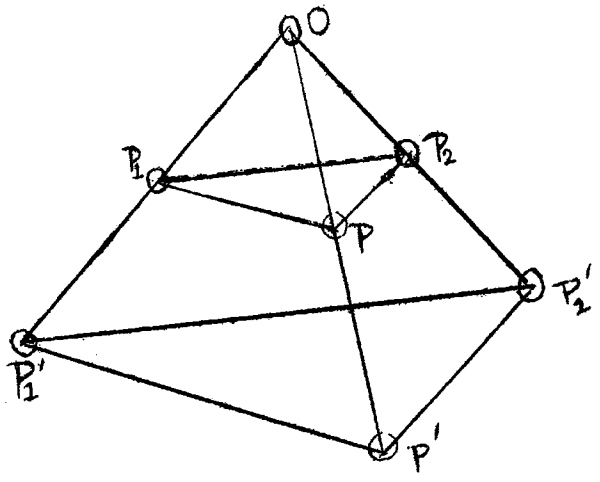
Lemma 3.1.2.

Let P_1 and P_2 be two points of Q_n other than O such that P_1P_2 is a generator not passing through O. Then the number of points P such

that both PP_1 and PP_2 are generators not passing through O is

$$s^2 - s + s^3 N(0, n-5) .$$

Proof.



By theorem 3.2 of Chapter I the plane OP_1P_2 is contained in Q_n. Hence the points of the plane other than those lying on the line OP_1 and OP_2 possess the required property. So the plane OP_1P_2 contributes $(s^2+s+1) - (2s+1)$ points P. Let P be a point not lying on the plane OP_1P_2 which possesses the required property. By theorem 3.2 of Chapter I it will follow that the 3-flat OPP_1P_2 is contained in Q_n. Let the plane $P_1'P_2'P'$ be the intersection of the 3-flat OPP_1P_2 and Σ_{n-1} where P_1' and P_2' are respectively the intersections of OP_1 and OP_2 with Σ_{n-1}.

Hence we have shown that every such point P lies in a 3-flat $OP_1'P_2'P'$ where $P_1'P_2'P'$ is a plane of Q_{n-1} passing through $P_1'P_2'$. The number of planes contained in Q_{n-1} passing through $P_1'P_2'$ is by theorem 5.2 of Chapter I equal to $N(0, n-5)$. Hence the number of 3-spaces of the type $OP_1'P_2'P'$ is also $N(0, n-5)$. Any point P of the 3-flat $OP_1'P_2'P'$ not lying on the plane OP_1P_2 contributes s^3 points. Hence it follows that

the total number of points P is

$$(s^2+s+1) - (2s+1) + s^3N(0, n-5) = s^2-s+s^3N(0,n-5) .$$

Lemma 3.1.3.

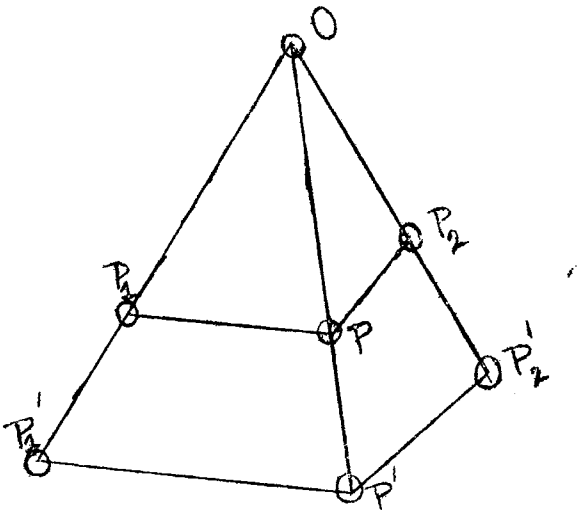
Let P_1 and P_2 be two points of Q_n such that P_1P_2 is a generator passing through 0. Then the number of points P such that both PP_1 and PP_2 are generators not passing through 0 is $s^2N(0, n-3)$.

Proof. Let P_1' be the intersection of the line OP_1P_2 and Σ_{n-1}. Let P be a point such that both PP_1 and PP_2 are generators not passing through 0. By theorem 3.2 of Chapter I it can be easily seen that the plane PP_1P_2 is contained in Q_n. Let $P_1'P'$ be the intersection of the plane PP_1P_2 and Σ_{n-1}. Obviously $P_1'P'$ is contained in Q_{n-1}, the base of the cone Q_n. Hence we have obtained that every such point P lies in a plane $OP_1'P'$ where $P_1'P'$ is a generator of Q_{n-1} passing through P_1'. The number of planes $OP_1'P'$ is equal to the number of generators $P_1'P'$ of Q_{n-1} passing through P_1' and hence is equal to $N(0, n-3)$ by theorem 5.2 of Chapter I. Every plane $OP_1'P'$ obviously contributes s^2 points P such that both PP_1 and PP_2' are generators not passing through 0. Hence the lemma follows.

Lemma 3.1.4.

Let P_1 and P_2 be two points of Q_n such that P_1P_2 is not a generator. Then the number of points P such that both PP_1 and PP_2 are generators not passing through 0 is $sN(0, n-3)$.

Proof.



Let P_1' and P_2' be respectively the intersection of OP_1 and OP_2 with Σ_{n-1}. Let P be a point such that both PP_1 and PP_2 are generators. Let P' be the intersection of OP and Σ_{n-1}. Then it can be easily seen that $P'P_1'$ and $P'P_2'$ is a pair of intersecting generators of Q_{n-1} and also $P_1'P_2'$ is not a generator of Q_{n-1}. Hence every point P such that both PP_1 and PP_2 are generators not passing through O lies on a line OP' where P' is a point of Q_{n-1} such that both $P'P_1'$ and $P_1'P_2'$ are generators of Q_{n-1}. The points P_1' and P_2' are points of Q_{n-1} and are not mutually conjugate. Hence by lemma 3.1.1 the number of points P' such that both $P'P_1'$ and $P'P_2'$ are generators of Q_{n-1} is N(O, n-3). Every line OP' contributes s points P possessing the required property. Hence the lemma follows.

Lemma 3.1.5.

Let P_1 and P_2 be two points of Q_{n-1} such that P_1P_2 is a generator not passing through O. Then the number of points P other than P_1 and P_2 such that PP_1 is a generator not passing through O and PP_2 is a

generator passing through 0 is (s-1).

Proof. Since P_1P_2 is a generator not passing through 0, by theorem 3.2 of Chapter I we can easily see that the plane OP_1P_2 is contained in Q_n. Let P be a point possessing the required property. Then PP_2 is a generator passing through 0. So P must be a point of OP_2. Since the plane OP_1P_2 is contained in Q_n, every point P of OP_2 is such that PP_1 is a generator of Q_n. Hence the required points P are the points of the line OP_2 other than 0 and P_2. Hence the lemma follows.

Lemma 3.1.6.

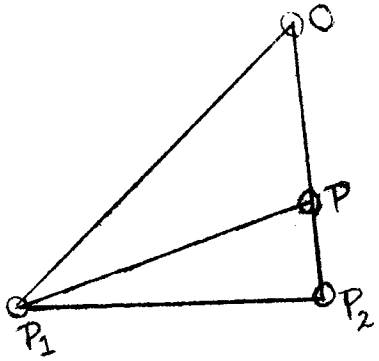
Let P_1 and P_2 be two points of Q_n such that P_1P_2 is a generator passing through 0. Then the number of points P such that PP_1 is a generator not passing through 0 and PP_2 is a generator passing through 0 is 0.

Proof is obvious and hence omitted.

Lemma 3.1.7.

Let P_1 and P_2 be two points of Q_n such that P_1P_2 is not a generator. Then the number of points P such that PP_1 is a generator not passing through 0 and PP_2 is a generator passing through 0 is 0.

Proof. Since PP_2 is a generator passing through 0, P must be a point of OP_2. If possible, suppose there is a point P on the line OP_2 such that PP_1 is a generator. Then the three points 0, P and P_1 are mutually conjugate and are points of Q_n. Hence by theorem 3.2 of Chapter I the plane OPP_1 is contained in Q_n. Obviously P_1P_2 is a line of the plane OPP_1.



We have shown that the plane OP_1P is contained in Q_n. So it follows that P_1P_2 is a generator of Q_n which is a contradiction. Hence the lemma follows.

Lemma 3.1.8.

Let P_1 and P_2 be two points of Q_n such that P_1P_2 is a generator not passing 0. Then the number of points P other than 0 such that both PP_1 and PP_2 are generators passing through 0 is 0.

Proof is simple and hence omitted.

Lemma 3.1.9.

Let P_1 and P_2 be two points of Q_n such that P_1P_2 is a generator passing through 0. Then the number of points P other than P_1 and P_2 and 0 such that both PP_1 and PP_2 are generators passing through 0 is $(s-2)$.

Proof is simple and hence omitted.

Lemma 3.1.10.

Let P_1 and P_2 be two points of Q_n such that P_1P_2 is not a generator. Then the number of points P other than 0, P_1 and P_2 such that both PP_1 and PP_2 are generators passing through 0 is 0.

Proof is simple and hence omitted.

Theorem 3.1.

Let B be the class of generators of Q_n not passing through 0 and V be the class of points of Q_n other than 0. Then D(B,V) is a PBIB design with three associate classes with the following parameters.

$$v = sN(0, n-1), \quad b = s^2N(1, n-1),$$

$$k = s + 1, \quad r = sN(0, n-3),$$

$$\lambda_1 = 1, \quad \lambda_2 = \lambda_3 = 0, \quad n_1 = s^2N(0, n-3), \quad n_2 = s - 1,$$

$$p_{11}^1 = s^2 - s + s^3N(0, n-5), \quad p_{12}^1 = (s-1),$$

$$p_{22}^1 = 0, \quad p_{11}^2 = s^2N(0, n-3),$$

$$p_{12}^2 = 0, \quad p_{22}^2 = (s-2),$$

$$p_{11}^3 = sN(0, n-3), \quad p_{12}^3 = p_{22}^3 = 0.$$

The other parameters can be obtained from the relations between the parameters of a PBIB design.

Proof. We shall apply corollary 2.1.1 to prove the theorem. The following results can be seen easily.

v = Number of points of the cone Q_n other than 0,

= $sN(0, n-1)$.

b = Number of generators of the cone Q_n not passing through 0,

= $s^2N(1, n-1)$.

k = Number of points on a generator,

= (s+1).

r = Number of generators passing through a point other than 0,

= sN(0, n-3) by lemma 3.1.1.

The association scheme is defined as follows. Two points P_1 and P_2 are first associates if P_1P_2 is a generator not passing through 0, second associates if P_1P_2 is a generator passing through 0 and third associates if P_1P_2 is not a generator. Obviously $\lambda_1 = 1$ and $\lambda_2 = \lambda_3 = 0$. The expressions for the parameters of the association scheme follow from lemmas 3.1.2 to 3.1.10.

Corollary 3.1.1.

Taking n = 4 and ω_3 a nondegenerate elliptic quadric in PG(3,s) we get the following series:

$$v = s(s+1)^2, \quad b = 2s^2(s+1),$$
$$r = 2s, \quad k = s + 1,$$
$$\lambda_1 = 1, \quad \lambda_2 = \lambda_3 = 0,$$
$$n_1 = 2s^2, \quad n_2 = (s-1),$$
$$p_{11}^1 = s^2 - s, \quad p_{12}^1 = (s-1),$$
$$p_{11}^2 = 2s^2, \quad p_{22}^2 = (s-2),$$
$$p_{11}^3 = 2s, \quad p_{12}^2 = p_{22}^1 = p_{12}^3 = p_{22}^3 = 0.$$

This series contains the following four designs with r and k not greater than 10. Some of the nonzero parameters are given below.

Design Number	v	r	k	b	λ_1	n_1	n_2	p_{11}^1	p_{12}^1	p_{11}^2	p_{22}^2	p_{11}^3
D_1	18	4	3	24	1	8	1	2	1	8	0	4
D_2	48	6	4	72	1	18	2	6	2	18	1	6
D_3	100	8	5	160	1	32	3	12	3	32	2	8
D_4	180	10	6	300	1	50	4	20	4	50	3	10

Corollary 3.1.2.

Taking n=5 and Q_4 a nondegenerate quadric we get the following series of PBIB designs with three associate classes.

$$v = s(s^3+s^2+s+1), \quad b = s^2(s^3+s^2+s+1),$$
$$k = (s+1), \quad r = s(s+1),$$
$$\lambda_1 = 1, \quad \lambda_2 = \lambda_3 = 0,$$
$$n_1 = s^2(s+1), \quad n_2 = (s-1),$$
$$p_{11}^1 = s^2 - s, \quad p_{12}^1 = (s-1),$$
$$p_{11}^2 = s^2(s+1), \quad p_{22}^2 = (s-2),$$
$$p_{11}^3 = s(s+1), \quad p_{22}^1 = p_{12}^2 = p_{12}^3 = p_{22}^3 = 0.$$

This series contains the following design with r and k not greater than 10.

$v = 30$, $b = 60$, $k = 3$, $r = 6$, $n_1 = 12$, $n_2 = 1$, $p_{11}^1 = 2$, $p_{12}^1 = 1$, $p_{11}^2 = 12$, $p_{11}^3 = 6$, $p_{22}^1 = p_{12}^2 = p_{22}^2 = p_{12}^3 = 0$, $p_{22}^3 = 0$.

Corollary 3.1.3.

Taking n = 6 and Q_5 a nondegenerate elliptic quadric in PG(5,s) we get the following series:

$$v = s(s^3+1)(s+1), \quad b = s^2(s^3+1)(s^2+1), \quad k = (s+1),$$
$$r = s(s^2+1), \quad \lambda_1 = 1, \quad \lambda_2 = \lambda_3 = 0, \quad n_1 = s^2(s^2+1),$$
$$n_2 = (s-1), \quad p_{11}^1 = s^2-s, \quad p_{12}^1 = (s-1), \quad p_{11}^2 = s^2(s^2+1),$$
$$p_{22}^2 = (s-2), \quad p_{11}^3 = s(s^2+1), \quad p_{22}^1 = p_{12}^2 = p_{12}^3 = p_{22}^3 = 0.$$

This series gives the following design with r and k not greater than 10.

$$v = 54, \quad b = 180, \quad k = 3, \quad r = 10, \quad n_1 = 20, \quad n_2 = 1, \quad \lambda_1 = 1,$$
$$\lambda_2 = \lambda_3 = 0, \quad p_{11}^1 = 2, \quad p_{12}^1 = 1, \quad p_{11}^2 = 20, \quad p_{11}^3 = 10,$$
$$p_{22}^1 = p_{12}^2 = p_{22}^2 = p_{12}^3 = p_{22}^3 = 0.$$

4. Some PBIB designs with three associate classes obtained from the configuration of secants and an external point of a quadric.

Let Q_2 be a nondegenerate quadric in PG(2,s), $s = 2^m$. Any line of PG(2,s) which intersects the quadric in two points is called a secant. We shall now prove a few lemmas which will be useful later.

Lemma 4.1.1.

Let P be a point other than the nucleus of polarity of Q_2 in PG(2,s), $s = 2^m$, which do not lie on Q_2. The number of secants passing through P is $\frac{s}{2}$.

Proof. We shall assume that $m > 1$. Let $\tau(P)$ denote the polar of P with respect to Q_2. $\tau(P)$ is a line. It is known that a line can be either completely contained in a quadric or can intersect the quadric in two points or can intersect the quadric in one point or can intersect

the quadric in no points. Since P is an external point and $\tau(P)$ contains P, $\tau(P)$ is not contained in Q_2. Hence it follows that $\tau(P)$ contains another external point P_1 (say). Then the points P and P_1 are external points of Q_2 and are mutually conjugate. So by theorem 7.2 of Chapter I the line PP_1, i.e. $\tau(P)$, contains only one point of the quadric Q_2. Let R_1 be any point of the quadric not lying on $\tau(P)$. Then P and R_1 are mutually not conjugate. Hence by theorem 7.3 of Chapter I the line PR_1 contains another point of the quadric. So PR_1 is a secant of the quadric. Hence for every point R of the quadric not lying on $\tau(P)$ PR is a secant. The number of points of the quadric not lying on $\tau(P)$ is s and every secant contains two points of the quadric. Hence the lemma follows.

Lemma 4.1.2.

Let S denote the nucleus of polarity of Q_2. Let P be any point of PG(2,s) not lying on Q_2. Then $\tau(P)$ contains S.

Proof. By lemma 4.1.1 $\tau(P)$ contains a single point R_0 of Q_2. Then the points P and R_0 are mutually conjugate. So the polar of R_0 contains P. Hence it follows that the polar of R_0 or the tangent line at R_0 is the line PR_0. Hence $\tau(R_0)$, the tangent line at R_0, is the same as $\tau(P)$. Then the lemma follows from theorem 7.1 of Chapter I.

Lemma 4.1.3.

Let P_1 be a point other than S, the nucleus of polarity of Q_2, which do not lie on Q_2. Then the number of external points P other than P_1 such that PP_1 is a secant is

$$\frac{s(s-2)}{2} .$$

Proof. Obviously the required points are those which lie on a secant passing through P_1 but do not lie on Q_2. The number of secants passing through P_1 is $\frac{s}{2}$ by lemma 4.1.1 and every secant contains two points of Q_2. Hence the lemma follows.

Lemma 4.1.4.

Let P_1 be an external point of Q_2 other than S. Then the number of external points P other than S and P_1 such that PP_1 intersects the quadric in a single point is (s-2).

Proof. Obviously the required points P lie on $\tau(P_1)$. By lemma 4.1.2 $\tau(P_1)$ contains S and one point of Q_2. Hence the lemma follows.

Lemma 4.1.5.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is a secant. Then the number of external points P other than S, P_1 and P_2 such that both PP_1 and PP_2 are secants is

$$(\tfrac{s}{2} - 2)^2 + (s-3) .$$

Proof. By theorem 7.2 of Chapter I, P_1 and P_2 are mutually non-conjugate. Let R_1 and R_2 be respectively the points at which $\tau(P_1)$ and $\tau(P_2)$ intersects the quadric. Then P_1R_2 must be a secant. If possible, suppose P_1R_2 is a tangent line intersecting Q_2 in a single point R_2. Then P_1 and R_2 are mutually conjugate. Then R_2 occurs in $\tau(P_1)$, the polar of P_1. So $\tau(P_1)$ intersects the quadric at two points R_1 and R_2 which contradicts theorem 7.2 of Chapter I since $\tau(P_1)$ is a line.

So it follows that P_1R_2 is a secant. Similarly P_2R_1 is a secant. Let $t = \frac{s}{2}$. Let the t secants passing through P_1 and P_2 respectively be

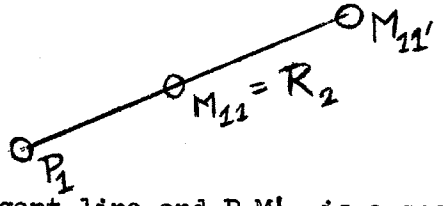
$$P_1M_{11},\ P_1P_2M_{12},\ \ldots,\ P_1M_{1t}$$

and

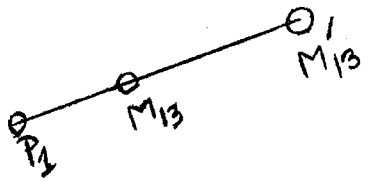
$$P_2M_{21},\ P_1P_2M_{22},\ldots,\ P_2M_{2t}$$

where $M_{11} = R_2,\ M_{21} = R_1,\ M_{12} = M_{22}$.

Obviously the required points P must lie on one of the secants P_1M_{11}, $P_1P_2M_{12}$, $\ldots$, P_1M_{1t}. Let us count the required number of points P lying on each of the secants. Consider the common secant $P_1P_2M_{12}$ which contains two points of Q_2, the points P_1 and P_2. Hence the common secant contains (s-3) points P satisfying the required conditions. Next we consider P_1M_{11}. The external points lying on P_1M_{11} which are points of intersection of P_1M_{11} and a secant passing through P_2 will possess the required property. P_1M_{11} contains two points M_{11} and M'_{11} of Q_2.



The line P_2R_2 is a tangent line and $P_2M'_{11}$ is a secant. Also $P_1P_2M_{22}$ intersects P_1M_{11} at P_1. Hence it follows that (t-2) of the secants passing through P intersect P_1M_{11} at external points other than P_1, P_2 and S. So the secant P_1M_{11} contributes (t-2) points P possessing the required property. Next we consider the secant P_1M_{13} which contains two points M_{13} and M'_{13} of Q_2.



Both the line P_2M_{13} and $P_2M'_{13}$ are secants. $P_1P_2M_{22}$ intersects P_1M_{13} at P_1. So (t-3) of the secants passing through P intersects P_1M_{13} at external points other than P_1, P_2 and S. So P_1M_{13} contributes (t-3) points P possessing the required property. Similarly each of the remaining secants contributes (t-3) points P. Counting together the points, we get the total number of points P as given in the lemma.

Lemma 4.1.6.

Let P_1 and P_2 be two external points other than S such that P_1P_2 is a tangent line intersecting the quadric in a single point. Then the number of external points P other than P_1, P_2 and S such that both PP_1 and PP_2 are secants is

$$\frac{s}{2}\left(\frac{s}{2} - 2\right) .$$

Proof. Let R_0 be the point at which P_1P_2 intersects Q_2. If R is any other point of Q_2, both P_1R and P_2R are secants by theorem 7.3 of Chapter I. Let the $\frac{s}{2}$ secants passing through P_1 and P_2 respectively be

$$P_1R_{11},\ P_1R_{12},\ \ldots,\ P_1R_{1t}$$

and $P_2R_{21},\ P_2R_{21},\ \ldots,\ P_2R_{2t}$ where $t = \frac{s}{2}$.

Any required point P must lie on one of the secants P_1R_{11}, P_1R_{12}, $\ldots$, P_1R_{1t}. Let us consider the points P which lie on P_1R_{11} and possess the required property. The secant P_1R_{11} contains two points R_{11} and R'_{11}

of Q_2. Both the lines P_2R_{11} and $P_2R'_{11}$ are secants. So $(\frac{s}{2} - 2)$ of the secants passing through P_2 intersect P_1R_{11} at external points other than P_1, P_2 and S (note that S, the nucleus of polarity, cannot lie on any secant). So the line P_1R_{11} contributes $(\frac{s}{2} - 2)$ required points P. This is true for all the secants passing through P_1. Hence the lemma follows.

Lemma 4.1.7.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is an external line intersecting the quadric in no point. Then the number of external points P other than P_1, P_2 and S such that both PP_1 and PP_2 are secants is

$$(\frac{s}{2} - 1)^2 .$$

Proof. Let R_1 and R_2 respectively be the points at which $\tau(P_1)$ and $\tau(P_2)$ intersect Q_2. Since P_1 and P_2 are mutually nonconjugate, by theorem 7.2 of Chapter I, it follows that P_1R_2 and P_2R_1 are secants. Let the secants passing through P_1 and P_2 be respectively

$$P_1M_{11},\ P_1M_{12},\ \ldots,\ P_1M_{1t}$$

and

$$P_2M_{21},\ P_2M_{22},\ \ldots,\ P_2M_{2t}$$

where $M_{11} = R_2$ and $M_{21} = R_1$.

By an argument exactly similar to that used in lemma 4.1.5 and 4.1.6, we can easily see that P_1M_{11} will contribute $(\frac{s}{2} - 1)$ points P possessing the required property and the remaining secants passing through P_1 will contribute $(\frac{s}{2} - 2)$ points each. Hence the lemma follows.

Lemma 4.1.8.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is a secant. Then the number of points P other than P_1, P_2 and S such that PP_1 is a tangent line and PP_2 is a secant is

$$(\tfrac{s}{2} - 2) .$$

Proof. Let P_1R_1 be the polar of P_1. Then obviously the required points P must lie on the line P_1R_1. Since P_1 and P_2 are nonconjugate, it can be easily seen that P_2R_1 will be a secant where R_1 is the point of intersection of the polar of P_1 and Q_2. So if the $\frac{s}{2}$ secants passing through P_2, $(\frac{s}{2} - 2)$ secants, namely the secants other than P_2P_1 and P_2R_1 intersects P_1R_1 in an external point other than P_1. Hence the lemma follows.

Lemma 4.1.9.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is a tangent line. Then the number of external points P other than P_1, P_2 and S such that PP_1 is a tangent line and PP_2 is a secant is 0.

Proof is simple and hence omitted.

Lemma 4.1.10.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is an external line. Then the number of external points P other than S, P_1 and P_2 such that PP_1 is a tangent line and PP_2 is a secant is

$$(\tfrac{s}{2} - 1) .$$

Proof. Let P_1R_1 be the polar of P_1, R_1 being the point at which the polar of P_1 intersects Q_2. Arguing as in lemma 4.1.8, we can see

that P_2R_1 is a secant. Hence out of the $\frac{s}{2}$ secants passing through P_2, $(\frac{s}{2} - 1)$ secants, namely the secants other than P_2R_1 intersects P_1R_1 in an external point. Hence the lemma follows.

Lemma 4.1.11.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is a secant. Then the number of external points P other than P_1, P_2 and S such that both PP_1 and PP_2 are tangent lines is 0.

Proof. Let P_1R_1 be the polar of P_1 and P_2R_2 be the polar of P_2. It can be easily seen that every point P satisfying the required conditions lie on both the lines P_1R_1 and P_2R_2. Hence the lemma follows from the fact P_1R_1 and P_2R_2 intersects at the points, the nucleus of polarity of Q_2.

Lemma 4.1.12.

Let P_1 and P_2 be two external points of Q_2 other than S such that P_1P_2 is a tangent line. Then the number of external points P other than P_1,P_2 and S such that both PP_1 and PP_2 are tangent lines is (s-3).

Proof follows easily from the fact that every point P satisfying the required condition must lie on the line P_1P_2 and the line P_1P_2 contains all the three points P_1, P_2 and S and a point of Q_2.

Lemma 4.1.13.

Let P_1 and P_2 be two external points of Q_2 such that P_1P_2 is an external line. Then the number of external points P other than P_1, P_2 and S such that both PP_1 and PP_2 are tangent lines is 0.

Proof is exactly similar to that of lemma 4.1.11.

Theorem 4.1.

Let B be the class of lines of PG(2,s) which are secants of Q_2 and V be the class of external points of Q_2 other than S, the nucleus of polarity of Q_2. Then D(B,V) is a PBIB design with three associate classes with the following parameters:

$$v = s^2 - 1, \quad r = \frac{s}{2},$$

$$b = (s+1)\frac{s}{2}, \quad k = (s-1),$$

$$\lambda_1 = 1, \quad \lambda_2 = \lambda_3 = 0, \quad n_1 = \frac{s}{2}(s-2), \quad n_2 = (s-2),$$

$$p_{11}^1 = (s-3) + (\tfrac{s}{2} - 2)^2, \quad p_{12}^1 = (\tfrac{s}{2} - 2),$$

$$p_{22}^1 = 0, \quad p_{11}^2 = \frac{s}{2}(\tfrac{s}{2} - 2),$$

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

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

The other parameters can be obtained from the relation between the parameters of a PBIB design.

Proof. We shall apply corollary 2.1 to prove the theorem. The following results can be obtained easily.

v = Number of points of PG(2,s) other than S which do not lie on Q_2,

$= s^2 - 1$.

r = Number of secants passing through a given external point other than S,

$= \frac{s}{2}$ by lemma 4.1.1.

k = Number of external points lying on a secant,

= (s-1).

The association scheme is defined as follows. Two external points P_1 and P_2 are first associates if the line P_1P_2 is a secant, second associates if the line P_1P_2 is a tangent line and third associates if the line P_1P_2 is an external line. Since there can be at most one secant passing through two external points, we have

$$\lambda_1 = 1 \qquad \text{and} \qquad \lambda_2 = \lambda_3 = 0.$$

The constancy of the parameters p_{11}^i, p_{12}^i, p_{22}^i (i = 1,2,3) and their expressions follow from lemmas 4.1.5 to 4.1.13. The expressions for n_1 and n_2 follow from lemmas 4.1.3 and 4.1.4.

Corollary 4.1.1.

The series given in theorem 4.1.1 contains the following two designs with r and k not greater than 10. The values of some of the non-zero parameters of these designs are given below.

Design Number	v	r	k	b	λ_1	n_1	n_2	p_{11}^1	p_{12}^1	p_{11}^2	p_{22}^2	p_{11}^3	p_{12}^3
D_1	15	2	3	10	1	4	2	1	0	0	1	1	1
D_2	63	4	7	36	1	24	6	9	2	8	5	9	3

CHAPTER IV

A CLASS OF TWO ERROR CORRECTING CODES WITH RATE OF TRANSMISSION ARBITRARILY CLOSE TO UNITY AND FRACTIONAL REPLICATIONS PRESERVING MAIN EFFECTS AND TWO FACTOR INTERACTIONS

1. Summary.

A set of points in PG(m,2) is defined to be a R_t-set if no t points of the set lie in a(t-2)-flat. Let $N_t(m)$ denote the number of points in a maximal R_t-set in PG(m,2). It is proved that there exists a t-error correcting binary (n,k)-group codes with n places and k information places if and only if $N_{2t}(n-k-1) \geq n$. It is shown there exists a $\frac{1}{2^k}$ fraction of a 2^n experiment, an experiment with n factors each at two levels, which preserves all main effects and c-factor interactions for $c \leq t$ if and only if there exists a t-error correcting (n,k) binary group code. We have proved that

$$N_4(2m-1) \geq 2^m - 1$$
$$N_4(2m) \geq 2^m + N_4(m-1) \quad .$$

Actual method of construction of R_4-sets containing 2^m-1 points in PG(2m-1, 2) and $2^m+N_4'(m-1)$ points in PG(2m, 2) are given where $N_4'(m-1)$ denote the number of points in the R_4-set in PG(m-1, 2) constructed by our method. These R_4-sets give two error correcting codes with

$$\text{(a)} \quad n = 2^m-1-c, \; k = 2^m-1-2m-c$$
$$\text{(b)} \quad n = 2^m+N_4'(m-1)-c, \; k = 2^m+N_4'(m-1)-2m-1-c \qquad (1.1)$$

where c is any non-negative interger or zero.

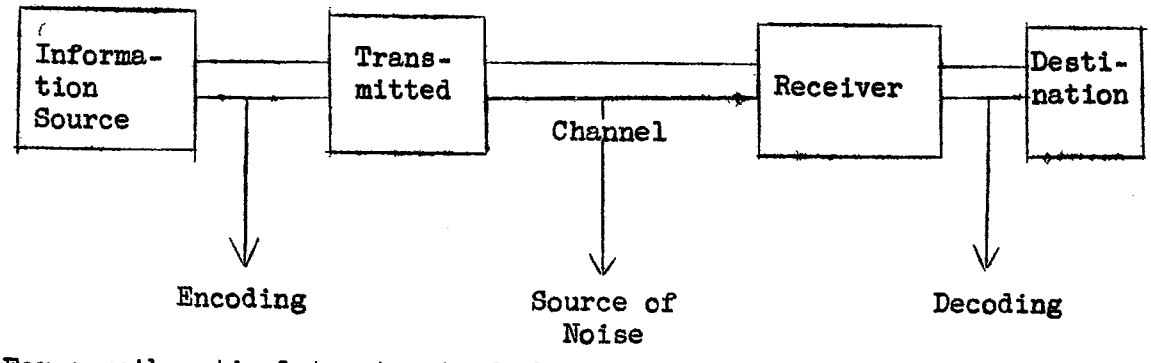
So two-error correcting codes can be obtained with rate of transmission k/n arbitrarily close to unity. Also these R_4-sets give a $\frac{1}{2^k}$ fraction of a 2^n experiment for preserving all main effects and two factor interactions for values of n and k given in (1.1). The following table gives the values of n and k for some of the two error correcting codes that have been obtained. For the same values of n and k we can also have a $\frac{1}{2^k}$ fraction of a 2^n experiment preserving main effects and two factor interactions.

n	k	Rate of transmission of the group code, bits per symbol
11	4	.36
15	7	.47
21	12	.57
31	21	.68
37	26	.70
63	51	.81
74	61	.82
127	113	.89
148	133	.90

2. General problem of information theory.

Information theory deals with the problem of sending information from one place to another through a channel subject to random disturbances in such a way that the probability of correct transmission of the

information is very close to unity and yet economic utilization of the channel is made. There is a source which is generating pieces of informations or messages one after another in a sequence. The messages of the source are encoded into symbols which are transmitted through the channel and the received symbols at the other end are decoded into the original message. The channel is subject to disturbances or noise as a result of which it is not always possible to obtain the transmitted information correctly from the received signal. The entire system can be described by the following diagram.



For a mathematical treatment of the subject it is assumed that the output of the source can be described by a stochastic process. Also for any given sequence of informations transmitted through the channel, the output at the receiving end can be described by a stochastic process. Mathematically encoding is a function which assigns a unique sequence of symbols of the transmitter to any sequence of messages of the source and decoding is a function which assigns a unique sequence of messages of the output to every sequence of symbols of the receiver.

Shannon in his fundamental paper [23] first introduced the basic concepts of information theory. Entropy H of a source is a measure of uncertainty about the information generated by a source, rate of transmission R is a measure of information transmitted per symbol of the transmitter and capacity C of a channel is the maximum rate of transmission for the given channel. Shannon [23] first proved that whenever the entropy of the source is less than the capacity of the given channel, it is possible to find a method of encoding and decoding such that the probability of correct transmission of information is arbitrarily close to unity and yet the rate of transmission is arbitrarily close to C provided certain conditions about the stochastic processes describing the source and the channel are satisfied. Macmillan [20] gave rigorous proofs of some of the Shannon results. Feinstein [16], Khinchin [18], Wolfowitz [27] and Blackwell, Breiman and Thomasian [1] extended Shannon's results in various directions. However the works of all these authors only prove the existence of codes with the required optimum properties but no method is available for actual construction of such codes. Khinchin [18] in page 116 comments, "From the purely practical point of view, we must note again that in both the Feinstein and Shannon methods the construction of codes with the required properties is not given; the existence of such a code is proved but no indication is given of how to actually find it." In the present chapter we shall be concerned with the construction of codes with some optimum property for a binary channel.

3. Binary channel.

A binary channel is one which can transmit two symbols denoted by 0 and 1. Each piece of information is encoded into a sequence of n binary digits which are transmitted through the channel one after another. A binary channel is called symmetrical if the probability of receiving 0 when 1 is transmitted is equal to the probability of receiving 1 when 0 is transmitted. For a symmetric binary channel in which the noise operates independently on every symbol transmitted, the capacity C of the channel is given by [23]

$$C = 1 + p \log_2 p + (1-p) \log_2 (1-p) \text{ bits/symbol},$$

bits meaning binary digits, where p denotes the probability of receiving 1 when 0 is transmitted.

Suppose the source can generate one of v possible messages or letters at a time. The collection of the v letters is called the output alphabet of the source. If $v = 2^k$, it is possible to transmit the messages by k-place binary sequences. In this case the probability of receiving a transmitted letter correctly is $(1-p)^k$ which may not be close enough to unity to be acceptable in actual practice. So the principal of redundancy is introduced. Instead of sending k-place binary sequences, n-place binary sequences are used to transmit the information. Roughly speaking, out of the n-places of the binary sequence, k-places are used as information positions and (n-k)-places are used as check positions as a result of which the probability of correct transmission of a letter is increased. The 2^k messages or letters of the alphabet

of the source are identified with 2^k n-place binary sequences chosen out of 2^n n-place binary sequences. This identification is called encoding. Also a rule of decoding is given which assigns a unique letter or message to every one of the 2^n possible received binary sequences. The basic problem is that of finding a method of encoding and decoding such that the probability of correct transmission of a letter is close to unity and yet the price paid by way of redundancy is not very high.

Since we are using n digits to transmit information that could be basically sent by k digits, it is reasonable to define the rate of information transmitted for such a binary code as

$$C_1 = k/n \text{ bits per symbol.}$$

The basic existence theorem of Shannon [23] for the case of a binary symmetric channel reduces to the following statement [25]. Given any fixed $C_1 = C - \delta$ $(\delta > 0)$ and any fixed $\epsilon > 0$, there exists a code which will transmit information at the rate C_1 bits per symbol and will decode it with an error probability per block of n symbols $Q_1(n,k,p) < \epsilon$. If $C_1 > C$, no such N exists.

However as already noted in section 1, the actual construction of such binary codes is also not known. The problem of construction of error correcting binary codes was first considered by Hamming [17]. Hamming solved the problem of construction of (n,k) binary codes which can transmit the information correctly if there is at most one error in the n binary digits transmitted. Slepian [25] considers (n,k) binary group codes and gives a maximum likelihood decoder which maximizes the

probability of correct transmission of a letter for a given method of encoding. Slepian poses the problem of finding the (n,k) binary group code which maximizes the probability of correct transmission for given n and k. He solves this problem for small values of n and k. Kuebler [19] solves Slepian's problem for k = 3,4 and general n. However the codes obtained by Slepian and Kuebler have poor rate of information transmittal and hence is not of much practical use. For instance the highest rate of information transmittal among the two error correcting codes given by Slepian is .36 bits per symbol which is attained by the code with n = 11 and k = 4. In this chapter we have considered the problem of finding two error correcting group codes with rate of information transmittal arbitrarily close to unity. In the following section we shall give a formal mathematical statement of the problem under investigation.

4. Statement of the problem.

Before stating the problem under investigation in formal mathematical terms, we shall need a few definitions. An n-place binary sequence is denoted by $\alpha = (a_1, a_2, \ldots, a_n)$ where each a_i is 0 or 1.

Weight of a sequence. The weight of an n place binary sequence α is defined to be the number of places in which the binary sequence has the number 1 and is denoted by $w(\alpha)$.

Hamming distance. The Hamming distance $d(\alpha,\beta)$ between two sequences α and β is defined to be the number of places in which the sequence α has 1 and β has 0 or vice versa.

Let B_n denote the set of 2^n n-place binary sequences. It is known that B_n is a group with respect to vector addition modulo 2 of the sequences.

Binary encoder. A v letter n-place binary encoder E is a subset of B_n consisting of v n-place sequences $\alpha_1, \alpha_2, \ldots, \alpha_v$.

Binary decoder. A v-letter n-place binary decoder D is a correspondence between the v sequences $\alpha_1, \alpha_2, \ldots, \alpha_v$ and v mutually disjoint sets $S_1, S_2, \ldots, S_v$ of n-place binary sequences such that $S_1 \cup S_2 \cup \ldots \cup S_v = B_n$.

Binary code. A v-letter n-place binary code C is the combination (E,D) of a v-letter n-place binary encoder E and a v-letter n-place decoder D.

Suppose the source alphabet consists of the v letters (or messages) $A_1, A_2, \ldots, A_v$. When the binary code C is used to transmit through a binary channel, the sequence α_i will be transmitted if A_i is the letter to be sent, $i = 1,2,\ldots,v$, and at the receiver the letter transmitted will be taken as A_j if the received n-place binary sequence is a member of the set S_j, $j = 1,2,\ldots,v$.

Minimum distance decoder. A binary decoder D is said to be a minimum distance decoder if for any sequence β of the set S_i

$$d(\alpha_i, \beta) \leq d(\alpha_j, \beta) \text{ for } i,j = 1,2,\ldots,v.$$

It is known that Slepian's [25] maximum likelihood decoder is a minimum distance decoder.

A t-error correcting binary code. A v-letter n-place binary code C is said to be a t-error correcting code if the decoder is a minimum distance

decoder and for any n-place sequence β,

$$d(\alpha_i,\beta) \leq t \Longrightarrow \beta \in S_i, \quad i = 1,2,\ldots,v.$$

Suppose the sequence α_i is transmitted through a binary channel and there is a disturbance in t or less of the places of α_i. Then the received sequence will be

$$\alpha_i + \gamma = \beta \quad \text{where } \gamma \text{ is an n-place}$$

sequence of weight not greater than t and addition is vector addition of the two sequences modulo 2. So the sequence β will differ from α_i in at most t places. Hence it follows that $d(\alpha_i,\beta) \leq t$ and consequently β is an element of S_i. Therefore the received signal will be read as α_i and the transmission will be correct.

Rate of information transmittal. For an n-place, v-letter, binary code C the rate of information transmittal is defined as

$$R = \frac{\log_2 v}{n} \quad \text{bits per symbol.}$$

R will also be referred to as rate of transmission.

R_t-set and $N_t(m)$. A set of points in PG(m,2) is defined to be a R_t-set if no t points of the set lie on a (t-2)-flat. The number of points in a maximal R_t-set in PG(m,2) is denoted by $N_t(m)$.

Sequence of t-error correcting codes with asymptotic rate of transmission equal to unity. Consider a sequence $\{C_m\}$ of binary codes such that the m-th code of the sequence is a t-error correcting code with n_m places and k_m information places. The sequence of binary codes C_m is said to have asymptotic rate of transmission equal to 1 if

$$\lim_{m \to \infty} R_m = 1$$

where R_m denotes the rate of transmission for the code C_m. In this chapter we have constructed such sequences of codes for t = 2 and in the course of this study certain bounds on $N_4(m)$ are obtained.

5. Some preliminary results on group codes.

A v-letter n-place binary code is said to be a group code if the sequences $\alpha_1, \alpha_2, \ldots, \alpha_v$ of the encoder form a group with respect to vector addition modulo 2.

For a group code, v is of the form 2^k. A 2^k-letter n-place group code is also referred to as an (n,k) group code.

Theorem 5.1.

There exists a t-error correcting (n,k) group code if and only if there exists a R_{2t}-set in PG(r-1, 2) containing n points and hence if and only if $N_{2t}(r-1) \geq n$ where r = n-k. This theorem is proved by Bose [3] in a different form. The proof given here is new and simpler.

Proof. Necessity. Let $\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1}$ be the elements of the encoder and let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be k independent generators of the encoder. Consider every n-place sequence as a vector with elements in GF(2). Let V_k denote the vector space determined by the k independent vectors $\alpha_1, \alpha_2, \ldots, \alpha_k$. Obviously the dimensionality of V_k is k. Hence the dimensionality of the orthogonal vector space V_r is r where r = n-k. Let $\beta_1, \beta_2, \ldots, \beta_r$ be r independent vectors in V_r. Let

$$\beta_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{rn}) \qquad i = 1,2,\ldots,r.$$

Let

$$C_j = \begin{bmatrix} \beta_{1j} \\ \beta_{2j} \\ \vdots \\ \beta_{rj} \end{bmatrix} \qquad j = 1,2,\ldots,r.$$

Then C_j can be regarded as a point in PG(r-1, 2). Consider the set $\lceil \rceil$ consisting of the points C_1, C_2, ..., C_n. We shall show that $\lceil \rceil$ is a R_{2t}-set. Kuebler [19] has shown that an (n,k) group code with a minimum distance decoder is a t-error correcting code if and only if

$$w(\alpha_j) \geq 2t + 1$$

for any nonnull element α_j of the encoder. Hence we have $w(\alpha_j) \geq 2t+1$, $j = 1,2,\ldots,v$, $v = 2^k-1$. If possible, suppose the set $\lceil \rceil$ is not a R_{2t}-set. Then there exists points C_1, C_2, ..., C_{2t} of $\lceil \rceil$ which lie on a (2t-2)-flat. Hence at least one of the points $C_1,\ldots,C_{2t}$ will lie on the linear space determined by the remaining points. Let us assume that C_1 lies on the linear space determined by $C_2,\ldots,C_{2t}$. Then there exists constants $\lambda_2,\ldots,\lambda_{2t}$ where λ's are elements of GF(2) and all λ's are not 0 such that

$$C_1 = \lambda_2 C_2 + \lambda_3 C_3 + \ldots + \lambda_{2t} C_{2t}.$$

Then we have

$$\lambda_1\beta_{i1} + \lambda_2\beta_{i2} + \ldots + \lambda_{2t}\beta_{i2t} = 0$$

for $i = 1,2,\ldots,r$, where $\lambda_1 = 1$.

Let $\underset{(1xn)}{\underline{\lambda}} = (\lambda_1,\lambda_2,\ldots,\lambda_{2t}, 0,0,\ldots,0)$. It can be easily seen that for any vector β of V_r, we have

$$\underset{(1xn)}{\underline{\lambda}} \quad \underset{(nx1)}{\underline{\beta}'} = 0$$

So the vector $\underline{\lambda}$ is orthogonal to the vector space V_r. Hence $\underline{\lambda}$ is a vector of V_k and hence $\underline{\lambda}$ is a sequence of the encoder. This is a contradiction since $w(\underline{\lambda}) \leq 2t$ whereas the code is a t-error correcting code and hence $w(\underline{\lambda}) \geq 2t+1$.

Sufficiency. Assume that there exists a R_{2t}-set $(\overline{\ })$ in PG(r-1, 2) containing n points. Suppose $(\overline{\ })$ consists of the points C_j, $j = 1,2,\ldots, n$ where $C_j = \begin{bmatrix} \beta_{1j} \\ \beta_{2j} \\ \vdots \\ \beta_{rj} \end{bmatrix}$. Let V_r be the vector space determined by the r n-vectors $\beta_1, \beta_2, \ldots, \beta_r$ where $\beta_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{in})$, $i = 1,2,\ldots,r$. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be k n-vectors orthogonal to the vector space V_r where $k = n-r$. Let $\alpha_0 = (0,0,\ldots,0)$ be the null vector. Let V_k denote the vector space determined by $\alpha_1, \alpha_2, \ldots, \alpha_k$. Let $\alpha_0, \alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_{v-1}$ be the 2^k n-vectors lying on the vector space V_k. Let C be the (n,k) group code whose encoder consists of the v sequences $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ and whose decoder is a minimum distance decoder. The code C will be said to be the code induced by the set $(\overline{\ })$ and denoted by $C((\overline{\ }))$ also. We shall show that C is a t-error correcting group code. Obviously the sequences $\alpha_0, \alpha_1, \ldots, \alpha_{v-1}$ form a group with vector addition modulo 2 as the group operation. If possible, suppose C is not a t-error correcting code. Then by Kuebler's result there exists an element of the encoder whose weight is less than (2t+1). So there exists an n-vector $\underline{\lambda} = (0\ 0\ \ldots\ \lambda_{i_1}\ 0\ \lambda_{i_2}\ 0\ \ldots\ \lambda_{i_{2t}}\ 0\ \ldots\ 0)$ with at most 2t non-zero elements which is a sequence of the encoder. So $\underline{\lambda}$ belongs to

the vector space V_k. Without any loss of generality let us take $\underline{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_{2t}, 0, 0, \ldots, 0)$. Since $\underline{\lambda}$ is an element of V_k, $\underline{\lambda}$ must be orthogonal to all the vectors of V_r. Hence we have

$$\lambda_1\beta_{i1} + \lambda_2\beta_{i2} + \ldots + \lambda_{2t}\beta_{i2t} = 0 \quad \text{for } i = 1,2,\ldots,r.$$

Now it follows easily that the points C_1, C_2, ..., C_{2t} of $\underline{(\bar{\ })}$ lie on a (2t-2)-flat which contradicts the fact that $\underline{(\bar{\ })}$ is a R_{2t}-set.

Corollary 5.1.

If there exists an (n,k) t-error correcting group code, then there exists an (n-1, k-1) t-error correcting group code.

6. Relationship between error-correcting binary group codes and fractional replications of factorial experiments at two levels.

The problem of finding $\frac{1}{2^k}$ fraction of a 2^n experiment, an experiment with n factors each at two levels, which preserves all main effects and interactions up to (t-1)-th order unaliassed with main effects and interactions up to (t-1)-th order is closely related to the problem of finding error correcting (n,k)-group code. Suppose the treatment combinations $x = (x_1, x_2, \ldots, x_n)$ of the n factors are represented by points in EG(n,2), the finite Euclidean geometry of n dimensions based on GF(2). Let

$$\ell = \ell_1 x_1 + \ell_2 x_2 + \ldots + \ell_n x_n = \text{constant}$$

denote a pencil of (n-1)-flats in EG(n,2). It is known that the contrasts corresponding to the pencil ℓ belong to a main effect or a t-factor or (t-1)-th order interaction according as the number of 1's among $\ell_1, \ell_2, \ldots, \ell_n$ is 1 or t.

Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be k independent linear forms where $\alpha_i = \alpha_{i1}x_1 + \alpha_{i2}x_2 + \ldots + \alpha_{in}x_n$, $i = 1,2,\ldots,k$. Consider the (n-k)-flat determined by the equations

$$\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0 . \tag{6.1}$$

Consider the $\frac{1}{2^k}$ fraction of the 2^n experiment which contains only the 2^{n-k} treatments corresponding to the 2^{n-k} points lying on the (n-k)-flat (6.1). If a fractional experiment is conducted containing only these 2^{n-k} treatments, it is known that a contrast belonging to the pencil ℓ will be aliassed (or confounded) with the corresponding contrasts of all the pencils $\ell + \lambda_1\alpha_1 + \ldots + \lambda_k\alpha_k$ = constant where λ's are elements in GF(2) and $(\lambda_1,\lambda_2,\ldots,\lambda_k) \neq (0,0,\ldots,0)$.

Theorem 6.1.

There exists a $\frac{1}{2^k}$ fraction of a 2^n experiment which preserves all main effects and interactions up to (t-1)-th order unaliassed with main effects and interactions up to (t-1)-th order if and only if there exists a t-error correcting (n,k) group code.

Proof. Sufficiency. Assume there exists an (n,k) t-error correcting group code. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be k independent generators of the encoder where $\alpha_i = (\alpha_{i1},\alpha_{i2},\ldots,\alpha_{in})$, $i = 1,2,\ldots,k$.

Let $\tilde{\alpha}_i$ denote the linear form $\alpha_{i1}x_1 + \alpha_{i2}x_2 + \ldots + \alpha_{in}x_n$. Let Σ_{n-k} denote the (n-k)-flat in EG(n,2) determined by the equations $\tilde{\alpha}_1 = \tilde{\alpha}_2 = \ldots \tilde{\alpha}_k = 0$.

Consider the fractional replication containing the 2^{n-k} treatments corresponding to the 2^{n-k} points of Σ_{n-k}. We shall show that this

fraction preserves all main effects and interactions up to (t-1)-th order unaliassed with main effects and interactions up to (t-1)-th order. In this fraction the contrasts belonging to a pencil

$$\ell = \ell_1 x_1 + \ell_2 x_2 + \ldots + \ell_n x_n = \text{constant}$$

will be aliassed with the corresponding contrasts of all the pencils

$$\ell + \lambda_1 \tilde{\alpha}_1 + \lambda_2 \tilde{\alpha}_2 + \ldots + \lambda_k \tilde{\alpha}_k = \text{constant}$$

where λ's are elements of GF(2) and $(\lambda_1, \lambda_2, \ldots, \lambda_k) \neq (0,0,\ldots,0)$. Hence to prove that the fraction corresponding to Σ_{n-k} possesses the required property it will be sufficient to show that none of the linear forms $\ell + \lambda_1 \tilde{\alpha}_1 + \ldots + \lambda_k \tilde{\alpha}_k$ has less than (t+1) non-zero coefficients whenever ℓ has at most t non-zero coefficients.

Since C is an (n,k) t-error correcting group code, by Kuebler's result any of the 2^k-1 non-zero sequences $\lambda_1 \alpha_1 + \ldots + \lambda_k \alpha_k$ has weight at least equal to (2t+1). Hence any one of the linear forms $\lambda_1 \tilde{\alpha}_1 + \ldots + \lambda_k \tilde{\alpha}_k$, $(\lambda_1, \ldots, \lambda_k) \neq (0,\ldots,0)$, has at least (2t+1) non-zero coefficients. Also ℓ has at most t non-zero coefficients. Hence it follows that the linear form $\ell + \lambda_1 \tilde{\alpha}_1 + \ldots + \lambda_k \tilde{\alpha}_k$ has at least (t+1) non-zero coefficients.

Necessity. Assume there exists a $\frac{1}{2^k}$ fraction of a 2^n experiment which preserves all main effects and interactions up to (t-1)-th order unaliassed with main effects and interactions up to (t-1)-th order. Let this fraction be determined by an (n-k)-flat Σ_{n-k} of EG(n,2) whose equations are

$$\tilde{\alpha}_1 = \tilde{\alpha}_2 = \ldots = \tilde{\alpha}_k = 0 \text{ where } \tilde{\alpha}_i = (\alpha_{i1} x_1 + \ldots + \alpha_{in} x_n),\ i=1,2,\ldots,k.$$

Let α_i denote the n-place sequence $(\alpha_{i1},\alpha_{i2},\ldots,\alpha_{in})$, i = 1,2,...,k. Let C denote the (n,k) group code whose encoder consists of the sequences $\lambda_1\alpha_1 + \ldots + \lambda_k\alpha_k$ where λ's are elements in GF(2) and addition is vector addition modulo 2 and whose decoder is a minimum distance decoder.

Since the fraction corresponding to Σ_{n-k} preserves main effects and interactions up to (t-1)-th order, it can be easily seen that any of the linear forms $\lambda_1\tilde{\alpha}_1 + \ldots + \lambda_k\tilde{\alpha}_k$ for $(\lambda_1,\ldots,\lambda_k) \neq (0,\ldots,0)$, has at least (2t+1) non-zero coefficients. Hence every sequence $\lambda_1\alpha_1 + \ldots + \lambda_k\alpha_k$ has weight at least equal to (2t+1) for $(\lambda_1,\ldots,\lambda_k) \neq (0,\ldots,0)$. Now it follows from Kuebler's result that C is a t-error correcting code.

7. A correspondence between the points of PG(n,2) and the elements of PG(2^{n+1}).

We shall set up a correspondence between the points of PG(n,2) and the elements of GF(2^{n+1}). Let

$a = (a_0,a_1,\ldots,a_n)$ be a point of PG(n,2).

We shall make a correspond to the element α of GF(2^{n+1}) where

$$\alpha = a_0 + a_1x + \ldots + a_nx^n$$

and vice versa and x is an undetermined element of GF(2). Obviously the correspondence is unique.

G_t-set. A set of elements of GF(2^{n+1}) is said to be a G_t-set if the sum of no c elements of the set is 0 for $c \leq t$.

Theorem 7.1.

Let $\{\bar{\ }\}$ be a set of points in PG(n,2) and A be the corresponding set of elements of $GF(2^{n+1})$. The set $\{\bar{\ }\}$ is an R_t-set if and only if the set A is a G_t-set provided $\{\bar{\ }\}$ contains at least t independent points.

Proof. Sufficiency. Assume that the set A of the elements of $GF(2^{n+1})$ is a G_t-set. If possible, suppose $\{\bar{\ }\}$ is not an R_t-set. Then there exists t points $a_1, a_2, \ldots, a_t$ of $\{\bar{\ }\}$ which lie on a (t-2)-flat. Then at least one of the points will lie on the linear space determined by the other points. Without any loss of generality we can assume that a_1 lies in the linear space determined by $a_2, a_3, \ldots, a_t$. Then we have

$$a_1 = \lambda_2 a_2 + \lambda_3 a_3 + \ldots + \lambda_t a_t \tag{7.1}$$

where λ's are elements in GF(2) and not all λ's are 0. Suppose (c-1) of the λ's are non-zero. Without any loss of generality, we can assume that

$$\lambda_2 = \lambda_3 = \ldots = \lambda_c = 1, \quad c \leq t.$$

Then it follows easily from (7.1) that the sum of the elements $\alpha_1, \alpha_2, \ldots, \alpha_c$ of A is 0 where α_i is the element of $GF(2^{n+1})$ corresponding to a_i, i = 1,2,...,t. But this contradicts the assumption that A is a G_t-set.

Necessity. Assume $\{\bar{\ }\}$ is an R_t-set. If possible, suppose A is not a G_t-set. Then there exists elements $\alpha_1, \alpha_2, \ldots, \alpha_c$ of A such that

$$\alpha_1 + \alpha_2 + \ldots + \alpha_c = 0, \quad c \leq t, \tag{7.2}$$

and the sum of the d's of these elements is non-zero for $d < c$. Let a_i denote the point of $\{\bar{\ }\}$ corresponding to the element α_i of A,

$i = 1,2,\ldots,t$. Then it follows easily from (7.2) that

$$a_1 = a_2 + a_3 + \ldots + a_c. \tag{7.3}$$

From (7.3) we can see that the points $a_1, a_2, \ldots, a_c$ determine a (c-2)-flat. Let $a_{c+1}, a_{c+2}, \ldots, a_t$ be (t-c) mutually independent points lying in $\bar{[}$ which are independent of the points $a_1, a_2, \ldots, a_c$. Then it is easy to see that the points $a_1, a_2, \ldots, a_t$ of $\bar{[}$ lie on a (t-2)-flat which contradicts the assumption that $\bar{[}$ is an R_t-set.

8. An R_4-set in PG(2m-1, 2) containig (2^m-1) points and a sequence of two error correcting codes with asymptotic rate of transmission equal to unity.

In this section we shall obtain a sequence of two error correcting codes with asymptotic rate of transmission equal to unity. First we shall prove a few lemmas.

Lemma 8.1.1.

Let α be a primitive element of $GF(s^2)$, the Galois field containing s^2 elements where s is a prime power. Consider the set of elements

$$0,\ \alpha^{s+1},\ \alpha^{2(s+1)},\ \ldots,\ \alpha^{(s+1)(s-1)}.$$

This set of elements constitute a subfield of $GF(s^2)$ with the operations of addition and multiplication as in $GF(s^2)$.

This lemma is a standard result in the theory of Galois field and hence the proof is omitted.

Lemma 8.1.2.

Let x, y, z be three non-zero elements of GF(s) such that

$$x + y + z = 0, \quad s = p^m, \quad p \neq 3 .$$

Then $$x^3 + y^3 + z^3 \neq 0.$$

This lemma is a result in elementary algebra which holds for any field and hence the proof is omitted.

Lemma 8.1.3.

Let x, y, z and w be four non-zero distinct elements of GF(s), $s = 2^q$, such that

$$x + y + z + w = 0.$$

Then $$x^3 + y^3 + z^3 + w^3 \neq 0.$$

Proof. Since the characteristic of the field is 2, we have from the assumption of the lemma

$$x + y + z = 0.$$

Combining both sides and expanding by binomial theorem for positive index which obviously holds for a Galois field, we get

(8.1) $$x^3 + y^3 + z^3 + 3(x+y)(y+z)(z+x) = w^3.$$

The lemma follows from (8.1) using the fact that the characteristic of the field is 2 and the addition inverse of any element in such a field is the element itself.

Theorem 8.1.

Let α be a primitive element of $GF(s^2)$, $s = 2^m$. Let A be the set consisting of the elements

$$\theta + \alpha\,\theta^3,\ \theta^2 + \alpha\,\theta^6,\ \ldots,\ \theta^{(s-1)} + \alpha\,\theta^{3(s-1)}$$

where $$\theta = \alpha^{(s+1)}.$$

Then A is a G_4-set consisting of (2^m-1) elements.

Proof. We have to show that the sum of no c elements of A is 0 for $c \leq 4$.

Let us consider two elements $\theta^i + \alpha\,\theta^{3i}$ and $\theta^j + \alpha\,\theta^{3j}$, $i \neq j$, $i,j = 1,2,\ldots,(s-1)$. The sum of these two elements is

$$\theta^i + \theta^j + \alpha(\theta^{3i} + \theta^{3j}) .$$

The sum is zero if and only if either (8.2) or (8.3) given below is true.

$$\begin{cases} \theta^i + \theta^j = 0 , \\ \theta^{3i} + \theta^{3j} = 0 . \end{cases} \tag{8.2}$$

$$\theta^i + \theta^j = \alpha(\theta^{3i} + \theta^{3j}) . \tag{8.3}$$

Since $i \neq j$ and in a field of characteristic 2, the addition inverse of any element is the element itself, (8.2) cannot be true.

By lemma (8.1.1) the set of elements $0, \theta, \theta^2, \ldots, \theta^{(s-1)}$ constitute a subfield of $GF(s^2)$ with respect to the operations of addition and multiplication as in $GF(s^2)$. So both $(\theta^i+\theta^j)$ and $\theta^{3i}+\theta^{3j}$ are elements of the subfield. Since α is not an element of the subfield, it follows that $\alpha(\theta^{3i}+\theta^{3j})$ is not an element of the subfield. Since $\theta^i + \theta^j$ is an element of the subfield and $\alpha(\theta^{3i}+\theta^{3j})$ is not an element of the subfield, (8.3) cannot be true. This proves that the sum of no two elements of A can be zero.

Now let us consider three elements $\theta^i + \alpha\,\theta^{3i}$, $\theta^j + \alpha\,\theta^{3j}$ and $\theta^k + \alpha\,\theta^{3k}$, $i \neq j \neq k$, $i,j,k = 1,2,\ldots,s-1$. The sum of these three elements can be zero if and only if either (8.4) or (8.5) given below is true.

$$\begin{cases} \theta^i + \theta^j + \theta^k = 0, \\ \theta^{3i} + \theta^{3j} + \theta^{3k} = 0, \end{cases} \tag{8.4}$$

$$\theta^i + \theta^j + \theta^k = \alpha(\theta^{3i}+\theta^{3j}+\theta^{3k}). \tag{8.5}$$

By lemma 8.1.2, (8.4) cannot be true. Using the fact that the set of elements 0, θ, θ^2, ..., θ^{s-1} constitute a subfield of GF(s^2) and α is not an element of this subfield, we can show that (8.5) is not true. This proves that the sum of no three elements is 0. Using lemma 8.1.3 and an exactly similar argument, we can show that the sum of no four elements is 0.

Corollary 8.1.1.

$$N_4(2m-1) \geq 2^m-1.$$

The existence of a G_4-set A in GF(2^{2m}) containing (2^m-1) elements implies the existence of an R_4-set in PG(2n-1, 2) containing (2^m-1) points. Hence the corollary follows from the fact $N_4(2m-1)$ denotes the number of points in a maximal R_4-set in PG(2m-1, 2).

Corollary 8.1.2.

Let A_m denote the G_4-set in GF(2^{2m}) containing (2^m-1) elements. Let $\underline{(\ )}_m$ denote the corresponding R_4-set in PG(2m-1, 2). Let C_m denote the (n,k) group code induced by the set $\underline{(\ )}_m$ with $n = 2^m-1$, and $k = 2^m-1-2m$ as used in the sufficiency part of theorem 5.1. Then $\{C_m\}$ is a sequence of two error correcting group codes with asymptotic rate of transmission equal to unity.

The corollary follows from theorem 5.1 and the fact that the rate of transmission of the code C_m is

$$R_m = \frac{2^m-1-2m}{2^m-1}$$

which tends to unity as m goes to infinity.

9. An R_4-set in PG(2m,2) containing $2^m+N_4(m-1)$ points and a sequence of two error correcting codes with asymptotic rate of transmission equal to unity.

Definitions.

Sum of points. Let $P_1, P_2, \ldots, P_k$ be k points in PG(n,2). Let

$$P_i = (a_{i0}, a_{i1}, \ldots, a_{in}), \quad i = 1,2,\ldots,k.$$

The sum of these k points is the point

$$\left(\sum_{i=1}^{k} a_{i0}, \sum_{i=1}^{k} a_{i1}, \ldots, \sum_{i=1}^{k} a_{in}\right)$$

where addition is in GF(2) and the sum is denoted by $P_1 + P_2 + \ldots + P_k$.

Null point. The vector $0 = (0,0,\ldots,0)$ containing all zero elements is called the null point. 0 is not a point of PG(n,2). For k points $P_1, P_2, \ldots, P_k$, if we have

$$P_2 = P_1 + \ldots + P_{i-1} + P_{i+1} + \ldots + P_k, \quad i = 1,2,\ldots,k,$$

we shall say that the sum of the k points is 0. Thus the sum of three distinct collinear points in PG(n,2) is 0. The sum of four distinct points of PG(n,2) which are coplanar is 0 if no three of the points are collinear.

Image of a set. Let $\{\ \}$ be a set of points in PG(n,2) and P be a point outside the set $\{\ \}$. Then the image of the set $\{\ \}$ with respect to P is

defined to be the set of all points P + X where X is a point of $\underline{\ }$ and is denoted by $P + \underline{\ }$.

Linear envelope of a set. The linear envelope of a set $\underline{\ }$ of points in PG(n,2) is defined to be the set of all points in PG(n,2) which lie on a line determined by two points of $\underline{\ }$ and is denoted by $L(\underline{\ })$. It is easily seen that $L(\underline{\ })$ consists of the points of $\underline{\ }$ and points which are sums of two points of $\underline{\ }$.

Lemma 9.1.1.

Let $\underline{\ }$ be an R_4-set in PG(n,2) lying on an (n-1)-flat Σ_{n-1}. Then the set

$$\underline{\ }^* = \{P\} \cup P + \underline{\ }$$

is an R_4-set where P is a point not lying on Σ_{n-1}.

Proof. It will be sufficient to show that the sum of no three points of $\underline{\ }^*$ is 0 and the sum of no three points occurs in $\underline{\ }^*$. Every point of $\underline{\ }^*$ can be represented as P + X where X is the null point or a point of $\underline{\ }$. When X is the null point, P + X is the point P. Consider three points $P+X_1$, $P+X_2$, $P+X_3$ of $\underline{\ }^*$. The sum of the three points is $P + X_1 + X_2 + X_3$. Since each X_i, i = 1,2,3, is either the null point or a point of Σ_{n-1}, it follows that $X_1 + X_2 + X_3$ is a point of Σ_{n-1}. Also P is a point outside Σ_{n-1}. Hence $P + X_1 + X_2 + X_3$ cannot be 0. The sum can occur in $\underline{\ }^*$ if and only if $X_1 + X_2 + X_3$ is 0 or is a point of $\underline{\ }$. Since $\underline{\ }$ is an R_4-set, $X_1 + X_2 + X_3$ cannot be 0 or a point of $\underline{\ }$. This completes the proof of the lemma.

Lemma 9.1.2.

Let Γ_1 be an R_4-set in PG(n,2) lying on an (n-1)-flat Σ_{n-1} and Γ_2 be another R_4-set in PG(n,2) such that no point of Γ_2 lies in Σ_{n-1}. Let

$$\Gamma = \Gamma_1 \cup \Gamma_2.$$

Then Γ is an R_4-set if $L(\Gamma_1) \cap L(\Gamma_2) = \phi$, the null set.

Proof. It will be sufficient to show that the sum of no 3 points of Γ is 0 or occurs in Γ. We shall use X and Y as generic notations for the points of Γ_1 and Γ_2 respectively. The triplets of the points of Γ can be of the following four kinds:

(i) (X_1, X_2, X_3),

(ii) (Y_1, Y_2, Y_3),

(iii) (X_1, Y_2, Y_3),

(iv) (X_1, X_2, Y_3).

Consider a triplet of the kind (i). Since all the three points are points of Γ_1, which is an R_4-set, the sum $X_1 + X_2 + X_3$ cannot be 0 and the sum does not belong to Γ_1. Also since Γ_1 is contained in Σ_{n-1}, the sum of three points of Γ_1 is a point of Σ_{n-1}. Γ_2 does not contain any point of Σ_{n-1}. So $X_1 + X_2 + X_3$ cannot be a point of Γ_2. Therefore $X_1 + X_2 + X_3$ is not a point of Γ.

Consider a triplet of the kind (ii). The sum is $Y_1 + Y_2 + Y_3$. Since all the three points are points of Γ_2 which is an R_4-set, the sum is not 0 and does not belong to Γ_2. Also as all the three points are points lying outside Σ_{n-1}, it follows easily that $Y_1 + Y_2 + Y_3$ is a

point outside Σ_{n-1}. $\sqsubset_1$ is completely contained in Σ_{n-1}. So $Y_1 + Y_2 + Y_3$ cannot be a point of $\sqsubset_1$. Hence $Y_1 + Y_2 + Y_3$ cannot be a point of $\sqsubset$.

Consider a triplet of the kind (iii). The sum is $X_1 + Y_2 + Y_3$. If possible, suppose

(9.1) $$X_1 + Y_2 + Y_3 = 0 .$$

X_1 is a point of $L(\sqsubset_1)$ and $Y_2 + Y_3$ is a point of $L(\sqsubset_2)$. The equation (9.1) implies that $L(\sqsubset_1)$ and $L(\sqsubset_2)$ have a common point which contradicts the assumption that

$$L(\sqsubset_1) \cap L(\sqsubset_2) = \emptyset, \text{ the null set.}$$

So $X_1 + Y_2 + Y_3$ cannot be 0. By similar arguments we will show that $X_1 + Y_2 + Y_3$ cannot be a point of $\sqsubset$. If possible, suppose $X_1 + Y_2 + Y_3$ is a point of $\sqsubset$. Then either (9.2) or (9.3) is true.

(9.2) $$X_1 + Y_2 + Y_3 = Y_4 .$$

(9.3) $$X_1 + Y_2 + Y_3 = X_2 .$$

From (9.2), we have

(9.4) $$X_1 = Y_2 + Y_3 + Y_4 .$$

Since Y_2, Y_3 and Y_4 are points of $\sqsubset_2$ and hence points outside Σ_{n-1}, $Y_2 + Y_3 + Y_4$ is a point outside Σ_{n-1}. Also X_1 is a point of Σ_{n-1}. So it follows that (9.4) is a contradiction.

From (9.3) we have

(9.5) $$X_1 + X_2 = Y_2 + Y_3 .$$

Since $X_1 + X_2$ is a point of $L(\sqsubset_1)$ and $(Y_2 + Y_3)$ is a point of $L(\sqsubset_2)$, (9.5) is a contradiction. So $X_1 + Y_2 + Y_3$ cannot be a point of $\sqsubset$.

Similarly we can show that the sum of three points of the kind (iv) cannot be 0 or a point of Γ.

This completes the proof of the lemma.

Let Σ_{2m-1} be a (2m-1)-flat in PG(2m,2). Let the points of Σ_{2m-1} be made to correspond to the elements of $GF(2^{2m})$ as in section 7. Let α be a primitive element of $GF(2^{2m})$. Let A_1 denote the set of elements

$$\theta + \alpha\theta^3,\ \theta^2 + \alpha\theta^6,\ \ldots,\ \theta^{(s-1)} + \alpha\theta^{3(s-1)} \text{ where } \theta = \alpha^{(s+1)},\ s = 2^m.$$

Let F_1 denote the set of elements

$$\theta,\ \theta^2,\ \theta^3,\ \ldots,\ \theta^{(s-1)}$$

which form the non-zero elements of GF(s).

Let A_2 be a G_4-set in $GF(2^{2m})$ which is a subset of F_1 containing $N_4'(m-1)$ points. Let Γ_1 and Γ_2 respectively denote the set of points of Σ_{2m-1} corresponding to the sets A_1 and A_2 of elements of $GF(2^{2m})$. Let

$$\Gamma_2^* = \{P\} \cup P + \Gamma_2 \quad ,$$
$$\Gamma = \Gamma_1 \cup \Gamma_2^*$$

where P is a point outside Σ_{2m-1}.

Theorem 9.1.

The set Γ in PG(2m,2) is an R_4-set containing $2^m + N_4'(m-1)$ points where $N_4'(m-1)$ denotes the number of points in Γ_2.

Proof. By theorem 8.1 A_1 is a G_4-set in $GF(2^{2m})$. By assumption A_2 is a G_4-set. So by theorem 7.1, both Γ_1 and Γ_2 are R_4-sets in Σ_{2m-1}. By lemma 9.1.1, Γ_2^* is an R_4-set. So the theorem will form lemma 9.1.2 if we can show that

$$L(\Gamma_1) \cap L(\Gamma_2^*) = \emptyset, \text{ the null set.}$$

Let X and Y be generic notations for points of Γ_1 and Γ_2 respectively. Since Γ_1 is a subset of Σ_{2m-1}, the points of $L(\Gamma_1)$ are points of Σ_{2m-1}. The points of $L(\Gamma_2^*)$ which lie in Σ_{2m-1} are either of the form (i) Y_1 or (ii) $Y_1 + Y_2$. Hence if $L(\Gamma_1)$ and $L(\Gamma_2^*)$ have a common point one of the following four equations must be true.

$$X_1 = Y_1 . \tag{9.6}$$

$$X_1 = Y_1 + Y_2 . \tag{9.7}$$

$$X_1 + X_2 = Y_1 . \tag{9.8}$$

$$X_1 + X_2 = Y_1 + Y_2 . \tag{9.9}$$

Suppose (9.6) is true. Let the element of A_1 corresponding to X_1 be $(\theta^i + \alpha\, \theta^{3i})$ and the element of A_2 corresponding to Y_1 be θ^j, $i,j = 1,2,\ldots,s-1$. Then (9.6) implies

$$\theta^i + \alpha\, \theta^{3i} = \theta^j \tag{9.10}$$

which is a contradiction by lemma 8.1.1.

Suppose (9.7) is true. Let the elements of A_2 corresponding to Y_1 and Y_2 be respectively $\theta^{\alpha k}$ and θ^k. Let the element of A_1 corresponding to X_1 be $\theta^i + \alpha\, \theta^{3i}$. Then (9.7) implies

$$\theta^i + \theta^j + \theta^k = \alpha\, \theta^{3i} \tag{9.11}$$

which is a contradiction by lemma 8.1.1. Similarly we can show that each of (9.8) and (9.9) leads to contradiction.

Corollary 9.1.1.

$$N_4(2m) \geq 2^m + N_4(m-1).$$

Proof. By theorem 7.1 there exists a G_4-set in $GF(2^m)$ containing $N_4(m-1)$ points where $N_4(m-1)$ denotes the number of points in a maximal

R_4-set in PG(m-1,2). Also by lemma 8.1.1 the set F_1 of elements

$$0, \theta, \theta^2, \ldots, \theta^{(s-1)}$$

constitute a subfield which actually is isomorphic with $GF(2^m)$, $s=2^m$. Hence there is a subset of F_1 which is a G_4-set and contains $N_4(m-1)$ points. So in theorem 9.1 we can take $N_4'(m-1) = N_4(m-1)$. Hence the corollary follows from the fact that theorem 9.1 provides an R_4-set $\underline{\ }$ containing $2^m + N_4(m-1)$ points.

Corollary 9.1.2.

Let $\underline{\ }_m$ be the R_4-set in PG(2m,2) containing $2^m + N_4'(m-1)$ points. Let C_m be the (n,k) group code induced by the R_4-set $\underline{\ }_m$ as introduced in the sufficiency part of theorem 5.1 with $n = 2^m + N_4'(m-1)$ and $k = 2^m + N_4'(m-1) - 2m-1$. Then $\{C_m\}$ is a sequence of two error correcting codes with asymptotic rate of transmission equal to unity.

Proof follows from theorem 5.1 and the fact that the rate of transmission of the code C_m is R_m where

$$R_m = \frac{2^m + N_4'(m-1) - 2m-1}{2^m + N_4'(m-1)} .$$

10. Examples illustrating the method of constructing R_4-sets.

Example I. R_4-set in PG(3,2) by the method of theorem 8.1.

The minimum function for $GF(2^4)$ according to Carmichel [11] is

$$f(x) = x^4 + x + 1 .$$

Let x denote a primitive root. Then we have

$$\theta = x^{s+1} = x^5, \quad s = 2^2 .$$

Using the minimum function we obtain the following polynomial representations for the powers of θ

$$\theta = x^2 + x, \quad \theta^2 = x^2 + x + 1, \quad \theta^3 = 1.$$

The G_4-set A in $GF(2^4)$ consists of the following three elements.

$$\alpha_1 = \theta + x\,\theta^3 = x^2, \qquad \alpha_2 = \theta^2 + x\,\theta^6 = x^2 + 1,$$
$$\alpha_3 = \theta^3 + x\,\theta^9 = 1 + x.$$

So the corresponding R_4-set consists of the following three points.

$$(0\ 0\ 1\ 0), \quad (1\ 0\ 1\ 0), \quad (1\ 1\ 0\ 0).$$

Example II. R_4-sets in PG(5,2) by the method of theorem 8.1.

The minimum function in $GF(2^6)$ as given by Carmichel [11] is

$$f(x) = x^6 + x + 1 .$$

Let x denote a primitive root. Then we have

$$\theta = x^{s+1} = x^9, \quad s = 2^3 .$$

Using the minimum function, we obtain the following polynomial expressions for the powers of θ.

$$\theta = x^4 + x^3, \quad \theta^2 = x^3 + x^2 + x + 1, \quad \theta^3 = x^3 + x^2 + x,$$
$$\theta^4 = x^4 + x^2 + x, \quad \theta^5 = x^4 + x^3 + 1, \quad \theta^6 = x^4 + x^2 + x + 1$$
$$\theta^7 = 1.$$

Hence the G_4-set A in $GF(2^6)$ consists of the following 7 elements.

$$\alpha_1 = \theta + x\,\theta^3 = x^2, \quad \alpha_2 = \theta^2 + x\,\theta^6 = x^5 + 1,$$
$$\alpha_3 = \theta^3 + x\,\theta^9 = x^4, \quad \alpha_4 = \theta^4 + x\,\theta^{12} = x^5 + x^2,$$

$$\alpha_5 = \theta^5 + x\theta^{15} = x^5 + x^3 + 1, \quad \alpha_6 = \theta^6 + x\theta^{18} = x^5 + x^4 + x^3 + x + 1,$$

$$\alpha_7 = \theta^7 + x\theta^{21} = 1 + x.$$

The corresponding R_4-set in PG(5,2) consists of the following 7 points.

(001000), (100001), (000010), (001001),

(100101), (110111), (11000).

BIBLIOGRAPHY

1. Blackwell, David, Leo Breiman and A. J. Thomasian, "Proof of Shannon's transmission theorem for finite-state indecomposable channel," Ann. Math. Stat., vol. 29 (1958), 1209-1220.

2. Bose, R. C., "On the construction of balanced incomplete block designs," Annals of Eugenics, vol. 9 (1939), 358-399.

3. --------"Mathematical theory of the symmetrical factorial designs," Sankhyā, vol. 8 (1947), 107-166.

4. --------"Partially balanced incomplete block designs with two associate classes involving only two replications," Calcutta Statistical Association Bulletin, vol. 3 (1951), 120-125.

5. --------and W. H. Clatworthy, "Some classes of partially balanced designs," Ann. Math. Stat., vol. 26 (1955), 212-232.

6. --------and S. S. Shrikhande, "Tables of partially balanced designs with two associate classes," North Carolina Agricultural Exp. Stat., Tech. Bull. No. 107 (1954) (Inst. of Stat. Mimeograph Series No. 50).

7. Bose, R. C., and K. R. Nair, "Partially balanced incomplete block designs," Sankhyā , vol. 4 (1939), 337-372.

8. --------"On complete sets of latin squares," Sankhyā, vol. 5 (1941), 361-382.

9. Bose, R. C., and T. Shimamato, "Classification and analysis of partially balanced incomplete block designs with two associate classes," Jour. Am. Stat. Assn., vol. 47 (1952), 151-184.

10. Bose, R. C., S. S. Shrikhande, and K. N. Bhatlacharya, "On the construction of group divisible designs," Ann. Math. Stat., vol. 24 (1953), 167-195.

11. Carmichael, R. D., Introduction to the theory of groups of finite order, Ginn and Co., 1937, 262.

12. Clatworthy, W. H.,"Contributions on partially balanced incomplete block designs with two associate classes," National Bureau of Standards, Applied Mathematical Series, 47, 1956.

13. --------"A geometrical configuration which is a partially balanced incomplete block design," Proceedings of the American Mathematical Society, vol. 5 (1954), 47-55.

14. Clatworthy, W. H., "Partially balanced incomplete block designs with two associate classes and two treatments per block," Journal of Research of the National Bureau of Standards, vol. 54 (1955).

15. Dickson, L. E., Linear groups, Teubner (1901), 197-198.

16. Feinstein, A., "A new basic theorem of information theory," Trans. I.R.E. PGIT, September 1954, 2-22.

17. Hamming, R. W., "Error detecting and error correcting codes," Bell System Technical Journal, vol. 29 (1950), 147-160.

18. Khinchin, A. I., Mathematical foundations of information theory, Dover Publications Inc. (1957).

19. Kuebler, R., On the Construction of a Class of Error-Correcting Binary Signalling Codes. Ph.D. thesis, University of North Carolina, Chapel Hill, 1958.

20. McMillan, B., "The basic theorems of information theory," Ann. Math. Stat., vol. 24 (1953), 196-219.

21. Primrose, E.J.F., "Quadrics in finite geometries," Cambridge Philosophical Society Proceedings, vol. 47 (1951), 299-304.

22. Roy, J., and R. G. Laha, "Two associate partially balanced designs involving three replications," Sankhyā, vol. 17 (1956), 175-184.

23. Shannon, C. E., "A mathematical theory of communication," Bell System Technical Journal, vol. 27 (1948), 379-423, 623-656.

24. Shrikhande, S. S., "On the dual of some balanced incomplete block designs," Biometrics, vol. 8 (1952), 66-72.

25. Slepian, D., "A class of binary signalling alphabets," Bell System Technical Journal, vol. 35 (1956), 203-234.

26. Tallini, Giuseppe, 'Sulle k-callote degli spazi lineari finiti," Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat., vol. 20 (1956), 311-317.

27. Wolfowitz, J., "The coding of messages subject to chance error," Illinois Journal of Mathematics, vol. 1 (1957), 591-606.