THE UNIVERSITY OF MANITOBA

COMBINATORIAL PROBLEMS IN CONFOUNDED, FACTORIAL DESIGNS

by

Douglas W. Mallenby

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF ARTS IN STATISTICS

DEPARTMENT OF STATISTICS

WINNIPEG, MANITOBA

May 1972

ACKNOWLEDGEMENTS

This study was supported initially by a graduate assistantship and was completed while holding a sessional lectureship in the Department of Statistics, University of Manitoba, for which I thank the Head of this Department, Dr. B. K. Kale.

I wish to express my sincere appreciation to Dr. J. G. Kalbfleisch, Department of Statistics, University of Waterloo, for his guidance in the selection of the thesis topic and in the structural design of the thesis, and also for his sponsorship over the past few years.

I am extremely grateful to Dr. J. F. Lawless, Department of Statistics, University of Manitoba, for his excellent suggestions and assistance in bringing the thesis to its final form, especially for urging me on to the general result of Chapter VII.

I am thankful to Mrs. A. Loewen, the most able secretary of the Department of Statistics, University of Manitoba, for her excellent rendition of my illegible scrawl into clarid typescript.
(I am also most grateful for Miss D. H.)

ABSTRACT

This is essentially a survey of all results pertaining to the existence of certain symmetrical, confounded, factorial designs when lower order interactions remain unconfounded. This survey is preceded by the preliminary topics of finite fields, finite geometries and their use in the construction of such designs.

All combinations of r factors, each at t levels, yield t^r distinct treatments. A single replication of a symmetrical, confounded factorial design consists of t^n experimental blocks each receiving a different set of t^{r-n} treatments (so that each treatment appears exactly once). The effects of some of the factor interactions are then confounded with the block effects. In practice, the most important interactions are the main effects and lower order interactions leading to the following problem: What is the maximum number of factors possible in a (t^r,t^n) design so that all interactions of up to f factors remain unconfounded?

The case of f = 2 was solved initially by Sir R. A. Fisher (1942, 1945) using an algebraic approach. Subsequently, Dr. R. C. Bose developed a powerful approach using finite Euclidean geometries, which led to an easy proof of Fisher's result, as well as some others (1947). However, the problem has proven to be difficult and not much more has been accomplished; for example, the complete solution for f = 3 is not yet known.

TABLE OF CONTENTS

CHAPTER I. FINITE FIELDS

This chapter defines the finite fields, characterizes them, gives a representation by Galois Fields and presents some examples.

I. Definition of a Finite Field

Definition I.1: A GROUP is a set, G, of elements and a rule of combination, "$\cdot$", satisfying the following properties:

a) CLOSURE: $\forall a, b \in G, (a \cdot b) \in G$.

b) ASSOCIATIVITY: $\forall a, b \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ where operations in parentheses are performed first.

c) IDENTITY: $\forall a \in G, \exists$ unique $e \in G \ni e \cdot a = a$.

d) INVERSE: $\forall a \in G, \exists$ unique $a' \in G \ni a \cdot a' = e$.

Definition I.2: An ABELIAN GROUP is a group with the cummutative property.

e) COMMUTATIVITY: $\forall a, b \in G, a \cdot b = b \cdot a$.

Definition I.3: A FIELD, F, is a set of elements such that:

i) the elements form an abelian group under addition, the rule of addition is denoted by "+", the identity by "$\bar{0}$" and the inverse of "a" by "-a";

ii) the non-zero elements form an abelian group under multiplication, the rule of multiplication is denoted by "$\times$", the identity by "$\bar{1}$", and the inverse of "a" by "a^{-1}";

iii) the DISTRIBUTIVE law of multiplication over addition holds:

$\forall a, b, c \in F : a \times (b + c) = (a \times b) + (a \times c)$.

Note: 1) $(b + c) \times a = a \times (b + c)$ by commutativity

$= (a \times b) + (a \times c)$ by distributive law

$= (b \times a) + (c \times a)$ by commutativity.

2) Commutativity of addition follows from the other properties in the definition of a field [Segre, p.21].

3) In a finite field the commutativity with respect to multiplication follows from the group properties [Segre, p.94].

Definition I.4: FINITE FIELD is a field with a finite number of elements.

II. Characterization of Finite Fields

Let the finite field, F, have t elements, $F = \{a_0, a_1, \ldots, a_{t-1}\}$. The integers of F are: $b_0 \equiv \bar{0}$, $b_1 \equiv \bar{1}$, $b_j = b_{j-1} + \bar{1}$ for $j = 2, 3, 4, \ldots$. Since t is finite, the series of b's must repeat. Let k be the smallest integer such that $k = m - n$ where $b_m = b_n$, $m > n$.

THEOREM II.1: k is a prime number (called the CHARACTERISTIC of the field)

Proof: $b_m = (\bar{1} + \bar{1} + \ldots + \bar{1}) = (\bar{1} + \ldots + \bar{1}) + (\bar{1} + \ldots + \bar{1})$ by associativity; $= b_n + b_{m-n}$ by definition

(m terms; n terms; (m-n) terms)

So $b_m = b_n$ implies $b_{m-n} = \bar{0}$ by uniqueness of additive identity

and $k = m - n$ implies $b_k = \bar{0}$.

Suppose $k = c \cdot d$ with $1 < c < k$, $1 < d < k$. Then

$\bar{0} = b_k = b_{c \cdot d} = (\bar{1} + \ldots + \bar{1}) + (\bar{1} + \ldots + \bar{1}) + \ldots + (\bar{1} + \ldots + \bar{1})$ (here there are c sums of d terms each by associativity)

$= b_d + b_d + \ldots + b_d$ by definition of b_d

$= b_d(\bar{1} + \ldots + \bar{1})$ by distributive

$= b_d \cdot b_c$ by definition b_c

$= \bar{0}$.

But $F - \{\bar{0}\}$ is an abelian group under multiplication and closed. Therefore, $b_d \cdot b_c \in F - \{\bar{0}\}$, a contradiction. Therefore, k must be prime. Then we may write $F = \{b_0, b_1, \ldots, b_{k-1}, a_k, \ldots, a_{t-1}\}$.

THEOREM II.2: The number of elements in F is $t = k^\ell$ where k is a prime and ℓ is some positive integer.

Proof: Define $\bar{0} \times \alpha \equiv \bar{0}$; $\forall \alpha \in F$.

We know $\{b_0, b_1, \ldots, b_{k-1}\} \subseteq F$. If there are no others, then the number is $t = k$. If there is another element, α_2 say, then the elements in the set

$\{b_i \times \bar{1} + b_j \times \alpha_2 | i, j = 0, 1, \ldots, k-1\} \subseteq F$ and are all distinct. If there are no others, than $t = k^2$. If there is another element, α_3 say, then the elements of the set

$\{b_i \times \bar{1} + b_j \times \alpha_2 + b_g \times \alpha_3 | i, j, g = 0, 1, \ldots, k-1\} \subseteq F$ and are all distinct. If there are no others, then $t = k^3$.

Since t is finite, this process must terminate after adding some final element, say α_ℓ, and the number of elements is $t = k^\ell$.

THEOREM II.3: The multiplicative group of the finite field is cyclic.

Proof: There are $(t-1) = (k^\ell - 1)$ elements in $F - \{\bar{0}\}$. Let $\alpha \in F - \{\bar{0}\}$, since the elements form a multiplicative group $(\alpha \times b_1)$, $(\alpha \times b_2), \ldots, (\alpha \times a_{t-1})$ are all the elements of $F - \{\bar{0}\}$ in some order. Therefore,

$$(\alpha \times b_1) \times (\alpha \times b_2) \times \ldots \times (\alpha \times a_{t-1}) = b_1 \times b_2 \times \ldots \times a_{t-1}$$

and $\alpha^{t-1} \times (b_1 \times \ldots \times a_{t-1}) = (b_1 \times \ldots \times a_{t-1})$ (commutativity).

So $\alpha^{t-1} = \bar{1}$ by uniqueness of multiplicative identity.

For $\alpha \in F - \{\bar{0}\}$, consider $\{\alpha, \alpha^2, \alpha^3, \ldots\}$. Since F is finite, there exists a smallest power, j, for which $\alpha^j = \bar{1}$; j is called the order of α.

Suppose $\alpha^r = \bar{1}$ with $r = nj + f$, $0 \leq f < j$: Then $\alpha^r = \alpha^{aj+f} = \alpha^{aj} \cdot \alpha^f =$ $= \alpha^f = \bar{1}$ implies $f = 0$.

$$\text{Since } \alpha^{t-1} = \bar{1} \qquad \forall \alpha \in F - \{0\}$$

$$\text{then } j \mid (t-1) \qquad \forall \alpha \in F - \{0\}.$$

Now let α_1 have order i_1, α_2 have order i_2 with L.C.M. $(i_1, i_2) = i$; then $(\alpha_1\alpha_2)^i = \bar{1}$ since $i_1 \mid i$ and $i_2 \mid i$ by definition of L.C.M. On the other hand $(\alpha_1\alpha_2)^r = \bar{1}$ implies $(\alpha_1^r)(\alpha_2^r) = \bar{1}$ implies $i_1 \mid r$ and $i_2 \mid r$.

Since i is the minimum possible value, then i is the order of $(\alpha_1\alpha_2)$.

Let b_j have order i_j, $j = 1,\ldots,k-1$; let a_j have order i_j, $j = k,\ldots,t-1$. Let m = Least Common Multiple of $\{i_1, i_2,\ldots,i_{t-1}\}$. Then m is the smallest number for which $i_1 \mid m$, $i_2 \mid m,\ldots,i_{t-1} \mid m$ are all true. Then m is the order of the element $(b_1 \times b_2 \times \ldots. \times a_{t-1})$ and it is the largest order and

$$\alpha^m = 1 \qquad \forall \alpha \in F - \{\bar{0}\}.$$

By fundamental theorem of algebra, any equation of degree m has at most m distinct roots. We know all (t-1) values in $F - \{\bar{0}\}$ are roots.

$$\therefore m \geq (t-1).$$

But $i_j \mid (t-1) \qquad \forall_j = 1, 2,\ldots,t-1.$

$$\therefore m = (t-1) = (k^{\ell}-1).$$

$\therefore$ there exists an element, b, with order (t-1). It is called a <u>primitive element</u>.

$\therefore$ $F - \{0\}$ is cyclic.

We may now write $F = \{\bar{0}, \bar{1}, b, b^2,\ldots,b^{t-2}\}$.

THEOREM II.4: The finite field, F, contains a sub-field, J, isomorphic to the field, J', of integers modulo k.

Proof: $J = \{b_0, b_1, \ldots, b_{k-1}\}$ contains the identities $b_0 \equiv \bar{0}$, $b_1 \equiv \bar{1}$. The obvious isomorphism $b_i \overset{1\text{-}1}{\longleftrightarrow} i$, $i = 0, 1, \ldots, k-1$, holds between this subset of F and the field of the integers modulo k.

$$\text{e.g. } b_i = \underbrace{(b_1 + b_1 + \ldots + b_1)}_{i \text{ terms}} \equiv \underbrace{(\bar{1} + \bar{1} + \ldots + \bar{1})}_{i \text{ terms}} \overset{1\text{-}1}{\longleftrightarrow} i.$$

It is easily checked that $(b_i + b_j) \overset{1\text{-}1}{\longleftrightarrow} (i+k) \bmod k$

$$(b_i \times b_j) \overset{1\text{-}1}{\longleftrightarrow} (i \cdot j) \bmod k.$$

The set $J = \{b_0, b_1, \ldots, b_{k-1}\} \overset{1\text{-}1}{\longleftrightarrow} \{0, 1, \ldots, k-1\} = J'$ and b_i has the same properties and characteristics as the integer i, so J "acts like" J'. It is convenient to use J' instead of J when working with the finite field.

THEOREM II.5: The finite fields of order k^ℓ are isomorphic to each other, k prime and ℓ a positive integer.

Proof: [Carmichael, p.250].

III. Representation by Galois Fields

Definition III.1: A POLYNOMIAL of degree ℓ over a finite field, $J' = \{0, 1, \ldots, k-1\}$, of k elements with k prime is a sum of the form

$$P(x) = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \ldots + c_1 x + c_0 \text{ where } c_i \in J', \; i = 0, \ldots, \ell.$$

Definition III.2: An IRREDUCIBLE polynomial is one with no factors except possibly constants or whole multiples of itself.

Definition III.3: $GF(k^\ell)$ denotes the set of residue classes of polynomials over the finite field $J' = \{0, 1, \ldots, k-1\}$ of order a prime k, modulo an irreducible polynomial of degree ℓ over J'.

It follows that $GF(k^\ell)$ = {all polynomials over J' of degree < ℓ}. The number of such polynomials is k^ℓ since there are ℓ coefficients, $c_0, c_1, \ldots, c_{\ell-1}$ each being able to assume any of the k values in J'.

THEOREM III.1: There exists at least one irreducible polynomial of degree ℓ over any finite field of order k, a prime.

Proof: [Carmichael, p.248]. [Mann, p.99].

Corollary: A set $GF(k^\ell)$ exists for all primes k, and all positive integers ℓ.

THEOREM III.2: $GF(k^\ell)$ is a finite field of order k^ℓ. (The GALOIS FIELD).

Proof: [Carmichael, p.255]. [Mann, p.97].

By virtue of Theorems II.5, III.1, and III.2 we have finite fields $GF(k^\ell)$ existing for all primes k and positive integers ℓ, all finite fields of the same order k being isomorphic. So we may take a $GF(k^\ell)$ as the representative of the finite fields of order k^ℓ.

IV. Examples

We use J' = {0, 1,...,k-1} instead of J = $\{\bar{0}, \bar{1}, \ldots, \overline{(k-1)}\}$ as notation.

IV.1: GF(k) = set of polynomials of degree < ℓ = 1 over finite fields of k elements

= {0, 1,...,k-1}.

Addition and multiplication is modulo k.

IV.2: $GF(2^2)$ = set of polynomials of degree < ℓ = 2 over field of 2 elements

= {0, 1, x, x+1}.

Addition: (mod 2)

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Addition is simply modulo k, independent of any irreducible polynomial.

Multiplication is determined by an irreducible polynomial f(x). A general procedure for finding all possible irreducible f(x) of degree ℓ is to consider all polynomials of degree ℓ and remove those which can be obtained by multiplying members of the Galois Field.

In this case: all possible polynomials of degree $\ell = 2$ over finite field of 2 are $\{x^2, x^2+1, x^2+x, x^2+x+1\}$. Those obtained by multiplication from $GF(2^2)$ are

$$\{x \cdot x = x^2,\ (x+1)^2 = x^2 + 1,\ x(x+1) = x^2 + x\}$$

This leaves $f(x) = x^2 + x + 1$ as the only irreducible choice. Equivalently $f(x) \equiv 0$ implies $(x^2 \equiv x+1)$.

Multiplication:

"x"	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

Since GF is cyclic, we may present the multiplication using a primitive element.

x	x^2	x^3
x	x+1	1

(x+1)	$(x+1)^2$	$(x+1)^3$
x+1	x	1

One primitive element is found using trial and error and any others are then easily found. In this case x, (x+1) both generate GF(2).

IV.3: $GF(2^3)$ = set of polynomials of degree $< \ell = 3$ over field of size 2

$$= \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}.$$

Addition is modulo 2.

Multiplication is determined by an irreducible f(x) of degree 3. Using the method of IV.2 we find exactly two possiblities.

1. $f(x) = x^3 + x + 1 = 0$ implies $x^3 \equiv (x+1)$. By trial and error we find generator x and by inspection of table below we see all elements except 1 are generators.

x	x^2	x^3	x^4	x^5	x^6	x^7
x	x^2	x+1	x^2+x	x^2+x+1	x^2+1	1

2. $f(x) = x^3 + x^2 + 1 = 0$ implies $x^3 \equiv (x^2+1)$. As above we find all elements but 1 are generators.

x	x^2	x^3	x^4	x^5	x^6	x^7
x	x^2	x^2+1	x^2+x+1	x+1	x^2+x	1

IV.4: $GF(3^2)$ = set of polynomials of degree $< \ell = 2$ over field of size 3

$$= \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}.$$

Addition is modulo 3.

Multiplication is determined by irreducible f(x) of degree 2. Using the method of IV.2, we find exactly three possibilities.

1. $f(x) = x^2+1 = 0$ implies $x^2 \equiv 2$. Generator (x+1) by trial and error and others 2x, 2x+2, x by inspection of table.

(x+1)	$(x+1)^2$	$(x+1)^3$	$(x+1)^4$	$(x+1)^5$	$(x+1)^6$	$(x+1)^7$	$(x+1)^8$
x+1	2x	2x+1	2	2x+2	x	x+2	1

2. $f(x) = x^2 + x + 2 = 0$ implies $x^2 \equiv 2(x+2) \equiv 2x + 1$. Generator (x+1) by trial and error and others x, 2x, 2x+2 by inspection.

(x+1)	$(x+1)^2$	$(x+1)^3$	$(x+1)^4$	$(x+1)^5$	$(x+1)^6$	$(x+1)^7$	$(x+1)^8$
x+1	x+2	2x	2	2x+2	2x+1	x	1

3. $f(x) = x^2 + 2x + 2 = 0$ implies $x^2 \equiv 2(2x+2) \equiv (x+1)$. Generator x by trial and error and others, 2x, x+2, 2x+1, by inspection.

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8
x	x+1	2x+1	2	2x	2x+2	x+2	1

[For Galois Fields of orders up to $k^{\ell} \leq 1000$, see Bussey (1909).]

Remark: Theorem II.5, page 5, also implies that these fields $GF(3^2)$ obtained by using different irreducible polynomials are isomorphic.

CHAPTER I. REFERENCES

1. BUSSEY, W. H. (1906), Galois Field Tables for $p^n \leq 169$, Bulletin, American Mathematical Society (12), p.22-39.

2. BUSSEY, W. H. (1909), Galois Field Tables of Order Less Than 1000, Bulletin, American Mathematical Society (16), p.188-206.

3. CARMICHAEL, R. D. (1937), Groups of Finite Order, Ginn and Company, Boston.

4. MANN, H. B. (1949), Analysis and Design of Experiments, Dover Publications, New York.

5. SEGRE, B. (1961), Lectures on Modern Geometry, Edizioni Cremonese, Roma.

CHAPTER II. FINITE PROJECTIVE AND EUCLIDEAN GEOMETRIES

Introduction:

Any synthetic geometry is a system based on primitive concepts, axioms and deductive logic. The primitive concepts are point, line and incidence. A point is a 0-space; a line is a 1-space and higher spaces are defined recursively. For example, a plane is a 2-space consisting of {all points on the lines through a specified point and any point of a specified line}, and in general an n-space consists of {all points on the line through a specified point and any point of a specified (n-1)-space}.

An analytic model for a finite synthetic geometry gives geometric names to certain sets of numbers in such a way that each geometric theorem is reduced to an algebraic theorem. The axioms and primitive concepts are replaced by definitions using elements of a finite field. [Coxeter, p.111].

In this section the properties of finite projective and Euclidean geometries are discussed, analytic models PG(r,t) and EG(r,t) are defined which are unique up to isomorphisms, counting results are obtained and examples included.

I. Finite Synthetic Projective Geometries

These geometries have properties which are maintained under central projection. Certain Axioms of Incidence belong to all synthetic projective geometry systems.

In the plane: -any two points lie on a unique line

-any two lines contain a unique point.

In a 3-space: -any 2 points lie on a unique line

-any 3 non-collinear points lie on a unique plane

-any line and point not lying in the line lie on a unique plane

-any 2 planes contain a unique line

-any 3 planes contain a unique point.

And so on for spaces of any dimension.

A certain property of incidence holds also:

-if sub-spaces of dimension m and n of an r-space intersect in a space of dimension p and have as union a space of dimension q then $m + n = p + q$. [Segre, p.122].

The Principle of Duality is a consequence of the axioms. Any axiom or theorem about points, lines, planes,...,(r-1)-spaces in a space of dimension r remain valid if these are interchanged with (r-1)-spaces,...,points respectively and the words "lie in" and "contain" are interchanged. So, for example, the axiom above "any line and point, not lying in the line, lie in a unique plane" with the interchanges would give the valid statement "any line and plane, not containing the line, contain a unique point".

For a finite, r-dimensional ($r > 2$) synthetic projective geometry, both Desargues' and Pappus' Theorem are consequences of the axioms of incidence. It has been shown that this implies the uniqueness of the geometry and that all such geometries are Desarguesian. For a finite,

plane (2-dimensional) synthetic projective geometry, neither of these results from the axioms of incidence. So, if one of these theorems is taken as an axiom, the resultant geometry is unique. Thus there exists only one such Desarguesian plane geometry (there do exist finite non-Desarguesian projective plane geometries). [Veblen and Bussey, p.244, p.247].

For $r \geq 2$, if Desargue's Theorem holds and if each line contains at least three points, then the points of the geometry form a finite linear space and all the results or ordinary linear algebra hold in the analytic models below. [Segre, p.176, #122].

II. Analytic Model, PG(r,t), for Finite Projective Geometries

Let GF(t) be the finite field of order $t = k^{\ell}$, with k prime and ℓ a positive integer. The non-negative integer r is the dimension of the space. The points of PG(r,t) are the equivalence classes of non-trivial (r+1)-tuples with co-ordinates in GF(t), where whole multiples are identified. Thus a given $(x_0, x_1, \ldots, x_r)$ would be a representation of the points $\{p \cdot (x_0, \ldots, x_r) \mid p \in (GF(t) - \{0\})\}$. The sub-spaces of dimension (r-1) of PG(r,t) are the sets of solutions to linear equations of the form $a_0x_0 + a_1x_1 + \ldots + a_rx_r = 0$ with coefficients in GF(t), not all zero. The sub-spaces of dimension (r-2) of PG(r,t) are the points satisfying pairs of independent linear equations of the form

$$a_0x_0 + \ldots + a_rx_r = 0 \text{ and } b_0x_0 + \ldots + b_rx_r = 0.$$

In general, the sub-spaces of dimension (r-m) of PG(r,t) are the points satisfying sets of m independent linear equations. Subspaces of PG(r,t) of dimension p are again PG(p,t)'s.

If we take as axioms those of incidence, along with Desargues

Theorem for r = 2, then finite projective geometries exist $\forall r \geq 2$, $\forall t = k^{\ell}$, a prime power. Geometries with the same (r,t) are isomorphic (because the finite fields of order t are isomorphic) and PG(r,t) is a representation for these geometries. The Principle of Duality is valid.

In PG(r,t) two points P_1, P_2 determine a line, ℓ, consisting of all points which are linear combinations of these, $\ell = \{\lambda_1 P_1 + \lambda_2 P_2 | \lambda_1, \lambda_2 \in GF(t)$, both not zero$\}$. Number of choices for $(\lambda_1, \lambda_2) = t^2 - 1$, since both cannot be zero. But each point has (t-1) representations. Therefore, the number of points on a line $= (t^2-1)/(t-1) = t + 1 \geq 3$ (V(r,t)). Since each line has at least three points, then the points of PG(r,t) form a finite linear space and all the results of ordinary linear algebra hold. In particular k points are linearly independent iff the matrix of their co-ordinates has rank k.

This provides a convenient, equivalent representation for finite projective geometries. All linear combinations, except the trivial one, of a set of (r+1) linearly independent points form a PG(r,t). Each such set of (r+1) points in a PG(r,t) will generate that PG(r,t) and is called a "basis" set. The "standard basis" is $B = \{B_0, B_1, \ldots, B_r\}$ where $B_i = (\varepsilon_{i0}, \ldots, \varepsilon_{ir})$, $\varepsilon_{ii} = 1$, $\varepsilon_{ij} = 0$ for $j \neq i$. Any (k+1) points of a basis is itself a basis for a $PG(k,t) \subset PG(r,t)$.

Carmichael (p.358) shows that any set of (r+2) points in PG(r,t) containing a basis set may be transformed linearly into the set $\{B_0, B_1, \ldots, B_r, U\}$ where the (r+1)-tuple U = (1, 1,...,1).

III. Counting Results in PG(r,t).

III.1: # points = # equivalence classes of (r+1)-tuples over GF(t), whole multiples identified.

(r+1)-tuples = $t^{r+1} - 1$ since each of (r+1) co-ordinates is chosen from GF(t), but all zeroes are not allowed.

representatives in each class = (t-1) since there are (t-1) multipliers in (GF(t) - {0}).

Therefore, # points = $(t^{r+1} - 1)/(t-1) = 1 + t + \ldots + t^r$.

By duality: # (r-1)-spaces = # 0-spaces = $1 + t + \ldots + t^r$.

III.2: We have seen that the number of points lying on a line equals t + 1. By duality, the number of (r-2)-spaces contained in an (r-1)-space equals (t+1).

III.3: # lines in PG(r,t): line determined by any two points

- two points may be selected in $(\frac{t^{r+1}-1}{t-1})\cdot(\frac{t^{r+1}-1}{t-1} - 1)$ ways;
- each line has (t+1) points.

Therefore, the number of different pairs determining the same line is $\binom{t+1}{2} = \frac{(t+1)(t)}{2}$. The number of different lines = $\frac{(t^{r+1}-1)(t^{r+1}-t)}{(t^2-1)(t^2-t)}$.

III.4: # different m-spaces in a PG(r,t):

Let N(r) = # ways of selecting (m+1) independent points PG(r,t). After j points have been selected, we select the $(j+1)^{st}$ from the points outside of the (j-1) space generated by the chosen j points.

choices= (# points in PG(r,t)) - (# points in PG(j-1,t))

$$= (\frac{t^{r+1}-1}{t-1}) - (\frac{t^j-1}{t-1}) = (\frac{t^{r+1}-t^j}{t-1}).$$

Therefore, $N(r) = \prod_{j=0}^{m} (\frac{t^{r+1}-t^j}{t-1})$.

But each m space will be counted here as many times as it is possible to select (m+1) independent points in PG(m,t), namely $N(m) = \prod_{j=0}^{m} (t^{m+1}-t^j)/(t-1)$. Therefore the number of different m-spaces

in $PG(r,t) = \frac{N(r)}{N(m)} = \prod_{j=0}^{m} \left(\frac{t^{r+1}-t^j}{t^{m+1}-t^j}\right)$.

m = 0: # 0-spaces in PG(r,t) = # points = $\left(\frac{t^{r+1}-1}{t-1}\right)$.

m = 1: # 1-spaces in PG(r,t) = # lines = $\left(\frac{t^{r+1}-1}{t^2-1}\right)\left(\frac{t^{r+1}-t}{t^2-t}\right)$.

m = r-1: # PG(r-1,t) in PG(r,t) = $\left(\frac{t^{r+1}-1}{t-1}\right)$.

III.5: The number of m-spaces containing a given q-space in a PG(r,t).

Start with a PG(q,t); we add (m-q) independent points to give a PG(m,t). We have (q+1) independent points generating PG(q,t). We may choose from the (points in PG(r,t)) - (points in PG(q,t)) equals

$\left(\frac{t^{r+1} - t^{q+1}}{t - 1}\right)$ points.

$\therefore$ # ways = $\prod_{j=q+1}^{m} \left(\frac{t^{r+1}-t^j}{t-1}\right)$.

But in PG(m,t), the number of ways to choose (m-q) independent points not in a given q space is

$$\prod_{j=q}^{m} \left(\frac{t^{r+1}-t^j}{t-1}\right).$$

$\therefore$ each m space has been counted this many times

$\therefore$ # ways = $\prod_{j=q+1}^{m} \left(\frac{t^{r+1}-t^j}{t^{m+1}-t^j}\right)$.

Remark : This equals the number of (r-m-1) spaces contained in a given (r-q-1) space by DUALITY.

Corollary: # lines through a point = # 1-spaces containing a 0-space

$$= \prod_{j=q+1}^{m} \left(\frac{t^{r+1}-t^j}{t^{m+1}-t^j}\right)$$

$$= \prod_{j=1}^{1} \left(\frac{t^{r+1}-t^j}{t^{m}-t^j}\right) = \left(\frac{t^{r+1}-t}{t^2-t}\right) = \left(\frac{t^{r}-1}{t-1}\right) = (1 + t + \ldots + t^{r-1}).$$

Corollary: # (q+1)-spaces containing a given q-space in a PG(r,t)

$$= (t^{r+1} - t^{q+1})/(t^{q+2} - t^{q+1}) = (t^{(r+1)-(q+1)}-1)/(t-1)$$

$$= (1 + t + \ldots + t^{r-q-1})$$

IV. Finite Synthetic Euclidean Geometries

Properties are maintained by parallel projection and perpendicularity is defined. A finite synthetic Euclidean geometry of dimension r may be obtained from a finite synthetic projective geometry of dimension r in the following manner: A subspace of dimension (r-1) of the projective geometry is singled out and called the "space at infinity". The Euclidean geometry consists of those points in the original projective geometry minus those in the space at infinity. Parallelism is defined as "incident in the space at infinity". Perpendicularity is defined by choosing an elliptic polarity in the space at infinity. [Coxeter, p.110]. The Euclidean spaces retain all their properties as subsets of the projective geometry.

V. Analytic Model, EG(r,t), for Finite Euclidean Geometries

Without loss of generality we take the space at infinity PG(r,t) to be PG(r-1, t) with basis = $\{B_1, B_2, \ldots, B_r\}$, from now on called $PG^{\infty}(r-1, t)$. All points in $PG^{\infty}(r-1, t)$ have first co-ordinates 0, and the number of points of PG(r,t) - $PG^{\infty}(r-1, t) = (\frac{t^{r+1}-1}{t-1}) - (\frac{t^r-1}{t-1}) = t^r$. [Bose and Kishen, p.24]. But the number of points in PG(r,t) with first co-ordinates $\neq 0 = t^r$ so all points of EG(r,t) are all the points of PG(r,t) with first co-ordinates $\neq 0$. Subspaces of EG(r,t) are "parallel" if they are incident in $PG^{\infty}(r-1, t)$, i.e., if their intersection has all points with first co-ordinates 0.

Without loss of generality we select the representative of the equivalence class for a points in EG(r,t), to be the one with first co-ordinate of 1. (When using Euclidean geometries one usually considers EG(r,t) to consist simply of all t^r r-tuples over GF(t).)

Finally EG(r,t) is defined by selecting among all ellipses centered at the origin the one given by $x_1^2 + x_2^2 + \ldots + x_r^2 = 1$, and calling it the "unit circle". This provides units of measurement in all direction and allows perpendicularity to be defined as "inner product = 0".

There exists a 1-1 correspondence between subsets of t^p points of EG(r,t) and subspaces $PG^{\infty}(p,t)$ of $PG^{\infty}(r-1, t)$. In fact, these t^p points are those with non-zero co-ordinates of some PG(p,t) < PG(r,t). And, the t^p points form an EG(p,t); so the relationship is $PG(p,t) = PG^{\infty}(p-1, t) \cup EG(p,t)$. This is also true for r: $PG(r,t) = PG^{\infty}(r-1, t) \cup EG(r,t)$. The points at infinity have all points with first co-ordinates zero, the Euclidean geometries have all points with first co-ordinates non-zero.

So points in EG(r,t) are

$$\{\{s(1, x_1,\ldots,x_r) \mid s \in (GF(t)-\{0\})\} \mid (x_1,\ldots,x_r) \in GF(t)\}.$$

For example, EG(2,k) consists of

$$\{\{s(1, x_1, x_2) \mid s \in (GF(k)-\{0\})\} \mid x_1, x_2 \in GF(k)\}.$$

This is ordinary Cartesian/Euclidean geometry with a finite number, k^2, of points which are those with integral co-ordinates from {0, 1, 2,...,(k-1)}. They could be plotted in a plane with (1, 0, 0) as the origin, and (1, 1, 0) and (1, 0, 1) as the axis directions.

VI. Examples

Example VI.1: PG(2,t): # points = $t^2 + t + 1$

lines = $t^2 + t + 1$ (duality)

points in a line = (t+1)

lines through a point = (t+1) (duality)

EG(2,t): # points = t^2 = all triples with first entry = 1

$$(1, x_1, x_2)$$

Points at ∞ = all points with first entry = 0

$$(0, x_1, x_2)$$

points = $\frac{t^2-1}{t-1} = (t+1)$ = # points in PG(1,t)

Example VI.2: PG(3,t): # points = $\frac{t^4-1}{t-1} = 1 + t + t^2 + t^3$ (duality)

planes = $1 + t + t^2 + t^3$

lines = $(t^2+1)(1+t+t^2)$

points on a line = $(t+1)$ = # planes through a line (duality)

lines through a point = $1 + t + t^2$ = # lines in a plane (duality)

= # points in a plane (duality in a plane)

Example VI.3: PG(4,t):

points = $\frac{t^5-1}{t-1} = 1 + t + t^2 + t^3 + t^4$ = # 3-spaces (duality)

lines = $(t^2+1)(1 + t + t^2 + t^3 + t^4)$ = # planes (duality)

points on a line = $(t+1)$ = # 3-spaces through a plane (duality)

lines through a point = $1 + t + t^2 + t^3$ = # planes in 3-space (duality)

points in a plane = $1 + t + t^2$ = # 3 spaces containing line (duality)

points in 3 space = $1 + t + t^2 + t^3$ = # 3 spaces through a point (duality)

lines in a plane = $1 + t + t^2$ = # planes through a line (duality)

lines in 3 space = $(t^2+1)(1 + t + t^2)$ = # planes through a point (duality)

Example VI.4: PG(2,2): GF(2) = {0, 1}

points = 7 = # lines

points on a line = 3 = # lines through a point

(1,0,0) (0,1,0) (0,0,1) (1,1,0) (1,0,1) (0,1,1) (1,1,1)

EG(2,2): # points = 4

(1,0,0) (1,0,1) (0,1,0) (1,1,1)

Example VI.5: PG(r,2): GF(2) = {0, 1}

points = $2^{r+1}-1$, # lines = $(2^{r+1}-1)(2^r-1)/3$

points on a line = 3, # lines through a point = (2^r-1)

(r+1) tuples

(1,0,....,0)

(0,1,0,..,0)

(0,....,0,1)

(1,1,0,..,0)

⋮

(1,1,....,1)

$$\binom{r+1}{1} + \binom{r+1}{2} + \ldots + \binom{r+1}{r+1} = (1+1)^{r+1} - 1 = (2^{r+1}-1)$$

EG(r,2): # points = 2^r = those with first co-ordinate = 1

(1,0,....,1)

(1,1,....,0)

(1,0,1,..,0)

(1,0,..,0,1)

(1,1,1,0,..,0)

⋮

(1,1,1,..,1)

$$2^r = \binom{r}{0} + \binom{r}{1} + \binom{r}{2} + \ldots + \binom{r}{r} = (1+1)^r \text{ points}$$

Example VI.6: PG(3,3): GF(3) = {0, 1, 2}

points = 40 = # planes, # lines = 130

points on a line = 4 = # planes containing a line (duality)

lines through a point = 13 = # lines in a plane

Each point has (t-1) = 2 representatives.

EG(3,3): remove $PG^{\infty}(2,3)$ with basis {(0,1,0,0),(0,0,1,0), (0,0,0,1)}

points = t^r = 27

We can list points cyclically.

(1,0,0,0)	(1,1,2,1)	(0,1,0,0)
(1,0,0,1)	(1,1,2,2)	(0,1,0,1)
(1,0,0,2)	(1,2,0,0)	(0,1,0,2)
(1,0,1,0)	(1,2,0,1)	(0,1,1,0)
(1,0,1,1)	(1,2,0,2)	(0,1,1,1)
(1,0,1,2)	(1,2,1,0)	(0,1,1,2)
(1,0,2,0)	(1,2,1,1)	(0,1,2,0)
(1,0,2,1)	(1,2,1,2)	(0,1,2,1)
(1,0,2,2)	(1,2,2,0)	(0,1,2,2)
(1,1,0,0)	(1,2,2,1)	(0,2,1,0)
(1,1,0,1)	(1,2,2,2)	(0,0,1,1)
(1,1,0,2)	These 27 points	(0,0,1,2)
(1,1,1,0)	have first co-	(0,0,0,1)
(1,1,1,1)	ordinate of 1.	Last 13 points have first
(1,1,1,2)	These are points	co-ordinate of zero.
(1,1,2,0)	of EG(3,3).	These are points of
		$PG^{\infty}(2,3)$.

CHAPTER II. REFERENCES

1. CARMICHAEL, R. D. (1937), Introduction to Theory of Groups of Finite Order, Ginn and Company, Boston.

2. COXETER, H. S. M. (1964), Projective Geometry, Blaisdell, Toronto.

3. BOSE, R. C. and KISHEN, K. (1940), On the Problem of Confounding in the General Symmetrical Factorial Design, Sankhya (5), p.21-36.

4. SEGRE, B. (1961), Lectures on Modern Geometry, Cremonese, Rome.

5. VEBLEN, O. and BUSSEY, W. H. (1906), Finite Projective Geometries Transactions, American Mathematical Society (7), p.241-259.

CHAPTER III. CONSTRUCTION OF CONFOUNDED SYMMETRICAL FACTORIAL DESIGNS VIA EUCLIDEAN GEOMETRIES

Introduction: Each of r factors at t different levels gives t^r different treatment combinations. Forming all t^r combinations gives a factorial experiment, which is symmetrical because each factor appears at the same number, t, of levels. If, in such an experiment, these are assigned in groups of t^{r-n} to t^n different blocks, we get a confounded design. This is called a confounded, symmetrical factorial design, (t^r, t^n).

If the number of levels $t = k^\ell$, with k prime and ℓ a positive integer, then we may use the elements of

$$GF(k^\ell) = \{b_0, b_1, \ldots, b_{t-1}\} \overset{1\text{-}1}{\longleftrightarrow} \{0, 1, \lambda, \lambda^2, \ldots, \lambda^{t-2}\},$$

where λ is a primitive element, to index the factor levels. Then each of the t^r distinct treatments is an r-tuple, $T(x_1, x_2, \ldots, x_r)$, with $x_i \in GF(t)$, $i = 1, 2, \ldots, r$, and there exists an obvious 1-1 correspondence with the t^r points of EG(r,t) of the form $(x_1, x_2, \ldots, x_r)$, $x_i \in GF(t)$, $i = 1, \ldots, r$. [Bose, 1938, 1940.]

I. Construction

DEFINITION I.1: A PENCIL, $P(a_1, a_2, \ldots, a_r)$ with $a_i \in GF(t)$, is a partition of EG(r,t) into t parallel hyperplanes called the subspaces of P. These are defined by

$$P_i: b_i + a_1x_1 + \ldots + a_rx_r = 0, \quad i = 0, 1, \ldots, (t-1).$$

There are (r-1) variables which may be assigned before the last is completely determined. Each of these takes any of the t values in GF(t) so the number of points in P_i is t^{r-1}. The subspaces are mutually exclu-

sive since the t equations are obviously linearly independnet. So there are $t(t^{r-1}) = t^r$ points, accounting for all the points of EG(r,t).

$P_k \cap P_j = \emptyset$ and $\bigcup_{k=0}^{t-1} P_k = EG(r,t)$, hence $\{P_0, P_1, \ldots, P_{t-1}\}$ is a partition of EG(r,t).

A set of n pencils $P^1, P^2, \ldots, P^n$ are linearly independent if the matrix of co-ordinates below has rank n.

$$\begin{pmatrix} a_1^1 & a_2^1 & \cdots & a_r^1 \\ a_1^2 & a_2^2 & \cdots & a_r^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^n & a_2^n & \cdots & a_r^n \end{pmatrix}$$

THEOREM I.1: Taking intersections of subspaces of n linearly independent pencils yields t^n sets of t^{r-n} combinations each.

Proof: This is clear for n = 1 from the definition above. For n = 2: Let $P(a_1,\ldots,a_r)$, $P'(a_1',\ldots,a_r')$ be linearly independent. Taking the intersection gives

$$P(a_1,\ldots,a_r) \cap P'(a_1',\ldots,a_r') = \{P_i \cap P_j' \mid i, j \in GF(t)\cdot GF(t)\}$$

consisting of t^2 sets. Points in $P_i \cap P_j'$ satisfy

$$b_i + a_1x_1 + \ldots + a_rx_r = 0 \quad \underline{\text{and}} \quad b_j + a_1'x_1 + \ldots + a_r'x_r = 0.$$

These are linearly independent with (r-2) variables free to take values in GF(t). Thus $P_i \cap P_j'$ has t^{r-2} points, and the points in all t^2 sets are counted as $t^2(t^{r-2}) = t^r$, accounting for all points of EG(r,t). So the intersection partitions EG(r,t) into t^2 sets of t^{r-2} points each.

For general n: Let $P^1, P^2, \ldots, P^n$ be linearly independent. Taking the intersection gives

$$\bigcap_{i=1}^{n} P^i = \{(P^1_{j_1} \cap P^2_{j_2} \cap \ldots \cap P^n_{j_n}) \mid (j_1, j_2, \ldots, j_n) \in \overset{n}{\underset{1}{X}} GF(t)\}$$

consisting of t^n sets.

Points in each intersection satisfy n linearly independent equations, and contain t^{r-n} points. The number of points in all the intersections is $t^n(t^{r-n}) = t^r$. So these partition the points of EG(r,t).

This completes the proof of Theorem I.1.

II. Properties of the (t^r,t^n) Design as Constructed. [Bose, 1947]

The t^r different combinations are denoted by

$\{T(x_1,\ldots,x_r) | x_i \in GF(t),\ i = 1, 2,\ldots,r\}$.

Definition II.1: A linear function, L, of the treatments may be written as $L = \sum_{(\text{all points})} c(x_1,\ldots,x_r)\cdot T(x_1,\ldots,x_r)$.

Definition II.2: Two linear functions, $L = \Sigma c(x_1,\ldots,x_r)\cdot T(x_1,\ldots,x_r)$ and $L' = \Sigma c'(x_1,\ldots,x_r)\cdot T(x_1,\ldots,x_r)$, are orthogonal if and only if $\Sigma c(x_1,\ldots,x_r)\cdot c'(x_1,\ldots,x_r) = 0$.

Definition II.3: The m linear functions, $L^{(k)} = \Sigma c^{(k)}(x_1,\ldots,x_r)\cdot T(x_1,\ldots,x_r)$, $k = 1, 2,\ldots,m$, are linearly dependent if there exist constants $\lambda_1, \lambda_2,\ldots,\lambda_m$ not all zero such that $\lambda_1 L^{(1)} + \lambda_2 L^{(2)} + \ldots + \lambda_m L^{(m)} \equiv 0$. Equivalently, $\Sigma_k \lambda_k c^{(k)}(x_1,\ldots,x_r) = 0$, for all points. Otherwise, they are said to be independent.

Definition II.4: A linear function is a contrast if it is orthogonal to the linear function $G = \Sigma T(x_1,\ldots,x_r)$ where $c(x_1,\ldots,x_r) \equiv 1$. So the necessary and sufficient condition for a linear function to be a contrast is $\Sigma c(x_1,\ldots,x_r) = 0$.

Definition II.5: The contrast between two sets of ℓ treatments $\{T^{(1)}, T^{(2)},\ldots,T^{(\ell)}\}$ and $\{T^{(1')}, T^{(2')},\ldots,T^{(\ell')}\}$ is the linear function $T^{(1)} + T^{(2)} + \ldots + T^{(\ell)} - T^{(1')} - T^{(2')} - \ldots - T^{(\ell')}$.

There are only (t^r-1) independent contrasts among the t^r treatments; each one possesses a degree of freedom. The degrees of freedom belonging

to two contrasts are defined to be orthogonal if the contrasts are orthogonal. In any set of contrasts, if just p are independent, then the set of contrasts possesses p degrees of freedom, which may be considered to belong to any p independent contrasts of the set.

When the t^r treatments are partitioned into t sets of t^{r-1} treatments each by the subspaces of a pencil, P, then there are only (t-1) independent contrasts between these sets, for example, between any fixed set and each of the remaining (t-1) sets. Thus the contrasts between these sets possess just (t-1) degrees of freedom. The pencil P may be said to carry (t-1) degrees of freedom.

THEOREM II.1: Contrasts among subspaces of a pencil, P, are orthogonal to contrasts among subspaces of another pencil, P'.

Proof: $L = \sum_{i=0}^{t-1} c_i P_i, \ \sum_{i=0}^{t-1} c_i = 0; \ L' = \sum_{i=0}^{t-1} c_i' P_i', \ \sum_{i=0}^{t-1} c_i' = 0.$

We must show $\sum_{\text{(all points)}}$ (product of coefficients) = 0. Consider $P_k \cap P_j'$, the set of t^{r-2} points satisfying $b_k + \Sigma a_i x_i = 0$, $b_j + \Sigma a_i' x_i = 0$. Points in this intersection receive c_k in L and c_j' in L'. Therefore,

$$\therefore \sum_{P_k \cap P_j'} \text{(product coefficient)} = \sum_{P_k \cap P_j'} c_k c_j' = (t^{r-2}) \cdot c_k \cdot c_j'.$$

Now sum over all points by summing over all intersections.

$$\sum_{\text{(all points)}} \text{(product coefficient)} = \sum_{k=0}^{t-1} \sum_{j=0}^{t-1} \left(\sum_{P_k \cap P_j'} \text{(product coefficient)} \right)$$

$$= \sum_{k=0}^{t-1} \sum_{j=0}^{t-1} (t^{r-2} \cdot c_k \cdot c_j')$$

$$= \sum_{k=0}^{t-1} \left(t^{r-2} \cdot c_k \left(\sum_{j=0}^{t-1} c_j' \right)\right)$$

$$= 0 \text{ since } \sum_{j=0}^{t-1} c_j' = 0.$$

An equivalent formulation of this result is that the (t-1) degrees of freedom belonging to contrasts among subspaces of P are orthogonal to those (t-1) which belong to contrasts among subspaces of P'.

This completes the proof of Theorem II.1.

Definition II.6: The confounded contrasts in the (t^r,t^2) design are those between the t^2 sets of the design. There are only (t^2-1) independent such contrasts, so there are (t^2-1) confounded contrasts in this design. These degrees of freedom are said to be confounded.

Lemma II.1: In a (t^r,t^2) design constructed by taking intersections of subspaces of two independent pencils, the (t^2-1) confounded d.f. are precisely those carried by the generating pencils and all linear combinations of them.

Proof: Let the subspaces of P be $P_0, P_1,\ldots,P_{t-1}$ where P_i is given by $b_i + \sum_1^r a_k X_k = 0$. Let the subspaces of P be $P'_0, P'_1,\ldots,P'_{t-1}$ where P'_j is given by $b_j + \sum_1^r a'_\ell X_\ell = 0$. The matrix $\begin{pmatrix} a_1, & a_2,\ldots,a_r \\ a'_1, & a'_2,\ldots,a'_r \end{pmatrix}$ has rank 2, and P,P' are linearly independent. P_k contains t^{r-1} points, $(P_k \cap P'_j)$ contains t^{r-2} points, k, j = 0, .,...,(t-1).

$P_k = (P_k \cap P'_0) \cup (P_k \cap P'_1) \cup \ldots \cup (P_k \cap P'_{t-1})$, k = 0, 1,...,(t-1). So the t^{r-1} points of P_k are distributed evenly over t sets of the design.

So any contrast between subspaces of P is also a contrast between sets in the design and is accordingly a confounded contrast. Thus all (t-1) degrees of freedom carried by P are confounded in this design. Similarly, the degrees of freedom carried by P' are confounded.

Consider the linear combination $P'' = \lambda_1 P + \lambda_2 P'$ with subspaces

$P''_0, P''_1, \ldots, P''_{t-1}$ for $\lambda_1, \lambda_2 \in GF(t)$, not both zero. P''_k is determined by $b_k + (\lambda_1 a_1 + \lambda_2 a'_1)x_1 + \ldots + (\lambda_1 a_r + \lambda_2 a'_r)x_r = 0$.

For each $b_i \in GF(t)$, $(\lambda_1 b_i) \in GF(t)$ and there exists a unique $b_j \in GF(t)$ such that $b_k = \lambda_1 b_i + \lambda_2 b_j$; in fact, $(\lambda_2 b_j) = -(\lambda_1 b_i - b_k)$, the additive inverse.

Thus some points of P''_k satisfy: $(\lambda_1 b_i + \lambda_2 b_j) + (\lambda_1 a_1 + \lambda_2 a'_1) + \ldots + a'_r x_r = 0$; so $(P_i \cap P'_j) \subset P''_k$.

This is true for all t choices of $b_i \in GF(t)$ accounting for $t(t^{r-2}) = t^{r-1}$ = all points of P''_k. So the points of P''_k are spread evenly over t of the sets in the design, for $k = 0, 1, \ldots, t-1$. Then any contrast between subspaces of $P'' = \lambda_1 P + \lambda_2 P'$ is a contrast between sets in the design and is accordingly confounded.

The number of such independent linear combinations, excluding the trivial case, is $(t^2-1)/(t-1)$ since each pencil has $(t-1)$ representations by whole multiples. Each of these pencils confounds $(t-1)$ degrees of freedom which are orthogonal by Theorem II.1. We have in total (t^2-1) confounded degrees of freedom which are all accounted for.

This completes the proof of Lemma II.1.

Definition II.7: The confounded contrasts in the (t^r, t^n) design are those between the t^n sets in the design. There are only (t^n-1) such independent contrasts, so there are (t^n-1) confounded contrasts in this design. These degrees of freedom are said to be confounded.

THEOREM II.2: In a (t^r, t^n) design constructed by taking intersections of subspaces of n independent pencils, the (t^n-1) confounded degrees of freedom are precisely those carried by the generating pencils and all linear combinations of them.

Proof: We have n linearly independent pencils $P^{(1)}, P^{(2)},\ldots,P^{(n)}$ with the matrix

$$\begin{pmatrix} a_1^{(1)} & a_2^{(1)} & \cdots & a_r^{(1)} \\ a_1^{(2)} & a_2^{(2)} & & a_r^{(2)} \\ \vdots & \vdots & & \vdots \\ a_1^{(n)} & a_2^{(n)} & & a_r^{(n)} \end{pmatrix}$$

of rank n. $P^{(k)}$ has subspaces $P_0^{(k)}, P_1^{(k)},\ldots,P_{t-1}^{(k)}$; k = 1, 2,...,n, with the subspace $P_i^{(k)}$ given by $b_i + \sum_{j=1}^{r} a_j^{(k)} X_j = 0$; i = 1,...,(t-1).

Each subspace $P_i^{(k)}$ has t^{r-1} points which are distributed evenly over t^{n-1} sets in the design, i = 0, 1,...,t-1. So any contrast between subspaces of $P^{(k)}$ is also a contrast between sets in the design, and is accordingly a confounded contrast. Then all (t-1) degrees of freedom carried by $P^{(k)}$ are confounded in this design, k = 1, 2,...,n.

Consider the linear combination $P = \lambda_1 P^{(1)} + \lambda_2 P^{(2)} + \ldots + \lambda_n P^{(n)}$ with $\lambda_i \varepsilon GF(t)$, i = 1, 2,...,n, not all zero.

Subspaces of P are $P_0, P_1,\ldots,P_{t-1}$. P_v is determined by:

$$\begin{aligned} b_v &+ (\lambda_1 a_1^{(1)} + \lambda_2 a_1^{(2)} + \ldots + \lambda_n a_1^{(n)}) x_1 \\ &+ (\lambda_1 a_2^{(1)} + \lambda_2 a_2^{(2)} + \ldots + \lambda_n a_2^{(n)}) x_2 \\ &\vdots \\ &+ (\lambda_1 a_r^{(1)} + \ldots + \lambda_n a_r^{(n)}) x_r = 0. \end{aligned}$$

For each set $\{b_{i_1}^{(1)}, b_{i_2}^{(2)},\ldots,b_{i_{n-1}}^{(n-1)}\}$ there exists a unique $b_{i_n}^{(n)}$ so that $b_v = \lambda_1 b_{i_1}^{(1)} + \lambda_2 b_{i_2}^{(2)} + \ldots + \lambda_n b_{i_n}^{(n)}$. So points of P_v satisfy

$$\begin{aligned} (\lambda_1 b_{i_1}^{(1)} + \lambda_2 b_{i_2}^{(2)} + \ldots + \lambda_n b_{i_n}^{(n)}) &+ (\lambda_1 a_1^{(1)} + \lambda_2 a_1^{(2)} + \ldots + \lambda_n a_1^{(n)}) x_1 \\ &\vdots \\ &+ (\lambda_1 a_r^{(1)} + \lambda_2 a_r^{(2)} + \ldots + \lambda_n a_r^{(n)}) x_r = 0 \end{aligned}$$

or $\lambda_1(b_{i_1}^{(1)} + \Sigma a_j^{(1)}x_j) + \lambda_2(b_{i_2}^{(2)} + \Sigma a_j^{(2)}x_j) + \ldots + \lambda_n(b_{i_n}^{(n)} + \Sigma a_j^{(n)}x_j) = 0$,
then $(P_{i_1}^{(1)} \cap P_{i_2}^{(2)} \cap \ldots \cap P_{i_n}^{(n)}) \subset P_v$.

This is true for all t^{n-1} choices $\{b_{i_1}^{(1)},\ldots,b_{i_{n-1}}^{(n-1)}\}$ accounting for $(t^{n-1})(t^{r-n}) = t^{r-1}$ = all points of P_v. Thus the points of P_v are spread evenly over t of the sets in the design, v = 0, 1,...,t-1. Then any contrast between subspaces of $P = \sum_{k=1}^{n} \lambda_j P^{(i)}$ is a contrast between sets of the design and is accordingly a confounded contrast.

The number of such independent linear combinations, excluding the trivial case, is $(t^n-1)/(t-1)$ since each pencil has (t-1) representatives by whole multipliers. Each of these carries (t-1) confounded degrees of freedom which are orthogonal by Theorem II.1. We have in total (t^n-1) confounded degrees of freedom which are all accounted for.

This completes the proof of Theorem II.2.

Definition II.8: A contrast belongs to main effect of factor F_i, if the coefficients in the contrast depend only on the level of factor F_i. A contrast belongs to two factor interactions of F_i, F_j iff

(a) the coefficients are dependent only on levels of F_i, F_j;

(b) it is orthogonal to all contrasts belonging to main effects of F_i, F_j.

Contrasts belong to f-factor interaction of $F_{i_1}, F_{i_2},\ldots,F_{i_f}$ iff

(a) the coefficients are dependent only on levels of those factors

(b) it is orthogonal to all contrasts of interactions of all subsets of the f-factors.

THEOREM II.3: A confounded interaction involves exactly f-factors if and only if the confounded pencil has exactly f non-zero coefficients.

Proof: Let pencil $P \equiv P(0,\ldots,a_i, 0,\ldots,0)$ where a_i is the only non-zero co-ordinate. Then contrasts among subspaces of P belong to the main effect of F_i, since subspaces are determined from $a_i x_i = b_\ell$, $b_\ell \in \{0, 1,\ldots,t-1\} = GF(t)$.

$\therefore$ subspaces $\xleftrightarrow{1\text{-}1}$ x_i, the level of F_i

$\therefore$ coefficients in contrast between subspaces are 1-1 with level, x_i, of F_i.

Let pencil $P \equiv P(0, a_i,\ldots,a_j,\ldots,0)$; a_i, a_j are only non-zero co-ordinates. Then contrasts among subspaces of P belong to the 2-factor interaction of F_i, F_j. Since subspaces are determined from $a_i x_i + a_j x_j = b_\ell \in GF(t)$,

$\therefore$ subspaces 1-1 (x_i, x_j), levels of F_i, F_j

$\therefore$ coefficients in contrast depend only on levels of F_i, F_j.

Contrast is orthogonal to contrasts among subspaces of all other pencils.

$\therefore$ contrast is orthogonal to all main effect contrasts of F_i, F_j.

Let $P \equiv P(a_1, a_2,\ldots,a_r)$, where only non-zero coefficients are $a_{i_1}, a_{i_2},\ldots,a_{i_f}$. Then contrasts among subspaces of P belong to the f-factor interaction of $F_{i_1}, F_{i_2},\ldots,F_{i_f}$.

Since subspaces determined from $\sum_{j=1}^{u} a_{i_j} x_{i_j} = b_\ell \in GF(t)$.

$\therefore$ subspaces 1-1 $(x_{i_1}, x_{i_2},\ldots,x_{i_f})$, levels of factors $F_{i_1},\ldots,F_{i_f}$.

$\therefore$ coefficients in contrast depend only on levels of $F_{i_1},\ldots,F_{i_f}$.

Contrasts are orthogonal to contrasts among subspaces of all other pencils.

So the contrast is orthogonal to contrasts among subspaces of all other pencils involving only subsets of the factors $F_{i_1},\ldots,F_{i_f}$. (The 1-1 correspondence in the preceeding takes care of the "if and only".)

III. Degrees of Freedom

There are only (t^r-1) independent contrasts among the t^r treatments; each possesses a degree of freedom. These are carried in sets of $(t-1)$ by the $(t^r-1)/(t-1)$ independent pencils. The number of pencils with a non-zero coefficient at $a_{i_1}, a_{i_2},\ldots,a_{i_f}$ is $(t-1)^f/(t-1) = (t-1)^{f-1}$. Each of these carries $(t-1)$ degrees of freedom, so there are $(t-1)^f$ degrees of freedom belonging to the f-factors interaction of $F_{i_1}, F_{i_2},\ldots,F_{i_f}$, $f = 1, 2,\ldots,r$. There are $\binom{r}{f}$ different interactions involving exactly f-factors, and $\binom{r}{f}(t-1)^f$ degrees of freedom belonging to f-factor interactions. Thus the (t^r-1) degrees of freedom are partitioned:

$$t^r-1 = \binom{r}{1}(t-1) + \binom{r}{2}(t-1)^2 + \ldots. + \binom{r}{r}(t-1)^2.$$

IV. Examples

IV.1: $(2^3, 2)$ confounded factorial design with $r = 3$ factors each at $t = 2$ levels in $t^n = 2$ blocks of $t^{r-n} = 4$ treatments each. We identify the 2^3 treatments with the points of EG(3,2), namely {(0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)}. In the construction we form 2 sets of 4 treatments each by taking subspaces of the single generating pencil. This confounds $1 = (t^n-1)$ degree of freedom belonging to the confounded contrast between subspaces of the generating pencil. This involves a 3-factor interaction if and only if the pencil has exactly 3 non-zero coefficients.

Pencil, $P(a_1, a_2, a_3)$ with $a_i \in GF(2) = \{0, 1\}$.

P(1,1,1) has Subspaces	P_0: $x_1 + x_2 + x_3 = 0$	P_1: $1 + x_1 + x_2 + x_3 = 0$
Blocks	(0,0,0), (1,1,0),	(1,0,0), (0,1,0),
	(1,0,1), (0,1,1).	(0,0,1), (1,1,1).

IV.2: $(3^2, 3)$ confounded factorial design, r = 2 factors each at t = 3 levels, with $t^n = 3$ blocks of $t^{r-n} = 3$ treatments each. We identify the 3^2 treatments with the points of EG(2,3) namely {(1,0), (0,1), (2,0), (0,2), (2,1), (1,2), (1,1), (2,2), (0,0)}. In the construction we form 3 blocks of 3 treatments each by taking subspaces of the single generating pencil. This confounds 2 degrees of freedom belonging to the confounded contrasts between subspaces of the generating pencil. These involve a 2-factor interaction if and only if the pencil has exactly 2 non-zero coefficients.

Pencil, $P(a_1, a_2)$ with $a_i \in GF(3) = \{0, 1, 2\}$.

P(1,2) has Subspaces	P_0: $x_1+2x_2=0$	P_1: $1+x_1+2x_2=0$	P_2: $2+x_1+2x_2=0$
Blocks	{(2,2), (0,0)	{(2,0), (0,1)	{(1,0), (0,2)
	(1,1)}	(1,2)}	(2,1)}

IV.3: $(3^3, 3^2)$ confounded factorial design, r = 3 factors each at t = 3 levels, with $t^n = 3^2$ blocks of $t^{r-n} = 3$ treatments each. We identify the 3^3 treatments with the points of EG(3,3) namely {(0,0,0), (0,0,1), (0,0,2), (0,1,0), (0,1,1), (0,1,2), (0,2,0), (0,2,1), (0,2,2), (1,0,0), (1,0,1), (1,0,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2), (2,0,0), (2,0,1), (2,0,2), (2,1,0), (2,1,1), (2,1,2), (2,2,0), (2,2,1), (2,2,2)}.

In the construction we form 3^2 blocks of 3 treatments each by taking all intersections of subspaces of 2 independent pencils. This confounds $(t^n-1) = 8$ degrees of freedom carried by the 2 generating

pencils and the 2 independent linear combinations of them. Take:

P(1,1,1), P(1,1,2); each carries (t-1) = 2 degrees of freedom belonging to a 3-factor interaction;

P(1,1,1) + P(1,1,2) = P(2,2,0), carrying 2 degrees of freedom belonging to a 2-factor interaction;

2P(1,1,1) + P(1,1,2) = P(0,0,1), carrying 2 degrees of freedom for a main effect.

<u>P(1,1,1):</u>

P_0: $x_1 + x_2 + x_3 = 0$

P_1: $1 + x_1 + x_2 + x_3 = 0$

P_2: $2 + x_1 + x_2 + x_3 = 0$

<u>P(1,1,2):</u>

P'_0: $x_1 + x_2 + 2x_3 = 0$

P'_1: $1 + x_1 + x_2 + 2x_3 = 0$

P'_2: $2 + x_1 + x_2 + 2x_3 = 0$

P(1,1,1) \ P'(1,1,2)	P'_0	P'_1	P'_2
P_0	(0,0,0)	(0,1,2)	(0,2,1)
	(1,2,0)	(1,0,2)	(1,1,1)
	(2,1,0)	(2,2,2)	(2,0,1)
P_1	(0,1,1)	(0,2,0)	(0,0,2)
	(1,0,1)	(1,1,0)	(1,2,2)
	(2,2,1)	(2,0,0)	(2,1,2)
P_2	(0,2,2)	(0,0,1)	(0,1,0)
	(1,0,0)	(1,2,1)	(2,0,2)
	(1,1,2)	(2,1,1)	(2,2,0)

The intersections of subspaces $P_i \cap P'_j$; i, j = 1, 2, 3 give 9 blocks of 3 treatments each.

CHAPTER III. REFERENCES

1. BOSE, R. C. (1938), On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Graeco-Latin Squares, Sankhya (4), p.323-338.

2. BOSE, R. C. and KISHEN, K. (1940), On the Problem of Confounding in the General Symmetrical Factorial Design, Sankhya (5), p.21-36.

3. BOSE, R. C. (1947), Mathematical Theory of the Symmetrical Factorial Design, Sankhya (8), Part 2, p.107-166.

CHAPTER IV. COMBINATORIAL PROBLEM IN CONFOUNDING, $m_f(p,t)$, AND RELATION TO FACTORIAL DESIGNS

I. Statement of the Combinatorial Problem, $m_f(p,t)$.

What is the maximum number r of factors possible in a (t^r,t^n) symmetrical, confounded factorial design so that no interactions involving less than or equal to f-factors are confounded. Call this number $m_f(p,t)$, where $r = p+n$ and t^p is the number of treatments per block.

THEOREM I.1: $m_f(p,t)$ = the maximum number of columns that it is possible to have in a p-rowed matrix, with elements in GF(t), such that no f columns are dependent.

Corollary I.1: $m_f(p,t)$ = the maximum number of points possible in a finite projective geometry PG(p-1,t) so that no f of the points lie in a subspace PG(f-2,t).

Proof: Basis for PG(r,t) is $B = \{B_i = (\alpha_{i_1}, \alpha_{i_2},\ldots,\alpha_{i_r}) \; \alpha_{i_i} = 1, \alpha_{i_j} = 0;\ j \neq i,\ i = 0, 1,\ldots,r\}$. $EG(r,t) = PG(r,t) - PG^{\infty}(r-1,t)$, all t^r points of EG(r,t) have first co-ordinate equal 1 and $PG^{\infty}(r-1,t)$ is generated by $\{B_1, B_2,\ldots,B_r\}$. The equation defining $PG^{\infty}(r-1,t)$ is $x_0 = 0$.

i) We show first that there is a 1-1 correspondence between (t^r,t^n) designs and $PG^{\infty}(r-n-1,t)$. A pencil, $P(a_1, a_2,\ldots,a_r)$ partitions EG(r,t) with its subspaces P_i determined by $b_i + a_1x_1 + \ldots + a_rx_r = 0$, $i = 0, 1,\ldots,t-1$; $GF(t) = \{b_0, b_1,\ldots,b_{t-1}\}$.

There is a 1-1 correspondence between the t subspaces P_i of EG(r,t) and the t subspaces PG(r-1,t) of PG(r,t), namely P_i corresponds to the PG(r-1,t) determined by $b_ix_0 + a_1x_1 + \ldots + a_rx_r = 0$. -The equiva-

lence sets in this PG(r-1,t) with $x_0 \neq 0$ are the points of P_i in EG(r,t), the points of this PG(r-1,t) with $x_0 = 0$ belong to $PG^{\infty}(r-1,t)$ and form the $PG^{\infty}(r-2,t)$ determined by $x_0 = 0$ and $a_1x_1 + \ldots + a_rx_r = 0$. This $PG^{\infty}(r-2,t)$ is thus determined uniquely by $P(a_1,\ldots,a_r)$ and is called the vertex of the pencil P.

A set of n independent pencils $P^{(1)}, P^{(2)},\ldots,P^{(n)}$ partitions EG(r,t) with intersections of subspaces, $P_i^{(k)}$ determined by $b_i + a_1^{(k)}x_1 + \ldots + a_r^{(k)}x_r = 0$, $i = 0, 1,\ldots,t-1$; $k = 1, 2,\ldots,n$. There is a 1-1 correspondence between the t^n sets in this partition of EG(r,t) and the t^k subspaces PG(r-n,t) of PG(r,t), namely,

$(P_{i_1}^{(1)} \cap P_{i_2}^{(2)} \cap \ldots \cap P_{i_k}^{(k)})$ determined by $\{b_{i_k} + a_1^{(k)}x_1 + \ldots + a_r^{(k)}x_r = 0, k = 1, 2,\ldots,n\}$ corresponds to the PG(r-n,t) determined by $\{b_{i_k}x_0 + a_1^{(k)}x_1 + \ldots a_r^{(k)}x_r = 0, k = 1, 2,\ldots,n\}$.

The equivalence sets in this PG(r-n,t) with $x_0 \neq 0$ are the points of $\bigcap_{k=1}^{n} P_{i_k}^{(k)}$ in EG(r,t), the points of this PG(r-n,t) with $x_0 = 0$ belong to $PG^{\infty}(r-1,t)$ and form the $PG^{\infty}(r-n-1,t)$ determined by $x_0 = 0$ and $\{a_1^{(k)}x_1 + \ldots + a_r^{(k)}x_r = 0, k = 1,\ldots,n\}$. This $PG^{\infty}(r-n-1,t)$ is thus determined uniquely by the vertices of $\{P^{(1)}, P^{(2)},\ldots,P^{(n)}\}$ and is called the vertex of the parallel bundle of these vertices.

This shows that a (t^r,t^n) design which is 1-1 with its set of n generating pencils determines a unique $PG^{\infty}(r-n-1,t)$. Now we show the converse.

Through a $PG^{\infty}(r-2,t)$ of PG(r,t) pass exactly (1+t) - PG(r-1,t)'s. For such a PG(r-1,t) there are exactly t^{r-1} points in $(PG(r-1,t) - PG^{\infty}(r-2,t))$. Adding any of these t^{r-1} points to a basis

for $PG^{\infty}(r-2,t)$ will lead to the same $PG(r-1,t) \supset PG^{\infty}(r-2,t)$. If one of these t^{r-1} points has a non-zero x_0, then they all do. Thus the t^r points of $EG(r,t)$ are split into t sets of t^{r-1} which give t of the $PG(r-1,t) \supset PG^{\infty}(r-2,t)$. This leaves one other which must have all points at ∞, and in fact it is the $PG^{\infty}(r-1,t)$. This partitioning of $EG(r,t)$ determines a unique pencil, or the $PG^{\infty}(r-2,t)$ is the vertex of a uniquely determined pencil.

Through a $PG^{\infty}(r-n-1,t)$ of $PG(r,t)$ pass exactly $(1 + t + \ldots + t^n)$ $PG(r-n,t)$'s, [Chapter 2]. For such a $PG(r-n,t)$ there are exactly t^{r-n} points in $(PG(r-n,t) - PG^{\infty}(r-n-1,t))$. Adding any of these t^{r-n} to a basis for $PG^{\infty}(r-n-1,t)$ will generate a $PG(r-n,t) \supset PG^{\infty}(r-n-1,t)$. If one of these additional points has a non-zero x_0, then they all do. Thus the t^r points of $EG(r,t)$ are split into t^n sets of t^{r-n} which give t^n of the $PG(r-n,t) \supset PG^{\infty}(r-n-1,t)$. This leaves $(1 + t + \ldots + t^{n-1})$ others which must have all points at ∞. This partitioning of $EG(r,t)$ determines a unique set of pencils, or, the $PG^{\infty}(r-n-1,t)$ is the <u>vertex</u> of a parallel bundle of uniquely determined vertices. Then the $PG^{\infty}(r-n-1,t)$ determines a unique (t^r,t^n) design.

Summary: (t^r,t^n) designs $\xleftrightarrow{1\text{-}1}$ sets of n linearly independent pencils $\xleftrightarrow{1\text{-}1}$ $PG^{\infty}(r-n-1,t)$.

ii) We know that contrasts among subspaces of a pencil, P, belong to an f-factor interaction if and only if P has exactly f non-zero coefficients [Chapter 3]. Then the vertex of P is determined by

$$a_{i_1} x_{i_1} + \ldots + a_{i_f} x_{i_f} = 0, \; x_0 = 0$$

and this vertex contains all (r-f) points of the basis for PG (r-1,t), $\{B_1, B_2, \ldots, B_r\}$, except for $\{B_{i_1}, \ldots, B_{i_f}\}$.

If all interactions with $\leq$ f-factors are to be unconfounded, then

the $PG^{\infty}(r-n-1,t)$ corresponding to the (t^r,t^n) design must not be contained in a vertex of a pencil with $\leq$ f non-zero coefficients. Therefore, the $PG^{\infty}(r-n-1,t)$ must be contained only by $PG^{\infty}(r-2,t)$'s which contain at most (r-f-1) points of $\{B_1, B_2,\ldots,B_r\}$. Equivalently, the $PG^{\infty}(r-n-1,t)$ cannot be contained by a $PG^{\infty}(r-2,t)$ which passes through (r-f) of the points of $\{B_1, B_2,\ldots,B_r\}$.

iii) Let the $PG^{\infty}(r-n-1,t)$ be generated by the r-n = p points in the matrix

$$\begin{pmatrix} 0, d_{11}, d_{12},\ldots,d_{1r} \\ 0, d_{21},\ldots\ldots\ldots,d_{2r} \\ \vdots \\ 0, d_{p1},\ldots\ldots\ldots,d_{pr} \end{pmatrix}$$

Any $PG^{\infty}(r-2,t)$ containing only the points $\{B_{i_1},\ldots,B_{i_f}\}$ of the set $\{B_1,\ldots,B_r\}$ will be determined by $x_0 = 0$ and $a_{i_1} x_{i_1} + \ldots + a_{i_f} x_{i_f} = 0$.

The necessary and sufficient conditions for the $PG^{\infty}(r-2,t)$ to contain the $PG^{\infty}(r-n-1,t)$ are

$$\begin{aligned} &a_{i_1} d_{1,i_1} + \ldots. + a_{i_f} d_{1,i_f} = 0 \\ &\vdots \\ &a_{i_1} d_{r,i_1} + \ldots. + a_{i_f} d_{r,i_f} = 0. \end{aligned}$$

Equivalently, the columns numbered $i_1, i_2,\ldots,i_f$ of the matrix A are dependent.

$$A = \begin{pmatrix} d_{11}, & d_{12},\ldots,d_{1r} \\ d_{21},\ldots\ldots\ldots,d_{2r} \\ \vdots \\ d_{p1},\ldots\ldots\ldots,d_{pr} \end{pmatrix}$$

$\therefore$ $m_f(p,t)$ = the maximum number of columns possible in a p-rowed matrix over GF(t) such that no set of f columns are dependent.

If we regard columns as points in some PG(p-1,t), then f of them will be dependent if and only if they lie in a PG(f-2,t).

$\therefore$ $m_f(p,t)$ = the maximum number of points possible in a PG(p-1,t) so that no subset of f belong to a PG(f-2,t).

This completes the proof of Theorem I.1.

II. $m_2(p,t)$ = maximum number of points possible in a PG(p-1,t) so that no two of them lie in a PG(0,t).

= number of points in a PG(p-1,t), so that no two are the same

$= (t^p-1)/(t-1)$.

$m_2(p,t)$ = maximum number of columns possible in a p-rowed matrix over GF(t) having no two columns dependent.

Since two columns are dependent iff they are multiples, excluding the column of zeroes and identifying the whole multiples in sets of (t-1) we find

$m_2(p,t) = (t^p-1)/(t-1)$.

NOTE: This result for f = 2 was first obtained by Fisher (1942, 1945). Using an algebraic approach, he gave a procedure for construction, but did not give any proof that this procedure did give the maximum. Fisher's papers are rather difficult to follow; a proof of his general construction is given by Finney (p.80, 81).

CHAPTER IV. REFERENCES

1. BOSE, R. C. (1947), Mathematical Theory of Symmetrical Factorial Design, Sankhya (8), Part 2, p.107 - 166.

2. FINNEY, D. J. (1960), Theory of Experimental Design, University of Chicago, Chicago, Illinois.

3. FISHER, R. A. (1942), The Theory of Confounding in Factorial Experiments in Relation to the Theory of Groups, Annals of Eugenics, Vol. XI, Part IV, p.341 - 353.

4. FISHER, R. A. (1945), A System of Confounding for Factors with More Than Two Alternatives, Giving Completely Orthogonal Cubes and Higher Powers, Annals of Eugenics, Vol. XII, Part IV, p.283 - 290.

CHAPTER V. $m_3(p, t)$

The values for $m_3(3,t)$, $m_3(4,t)$ and $m_3(p,2)$ are known. Also $m_3(5,3) = 20$ and upper and lower bounds are available for all other values.

I. $m_3(3,t)$

THEOREM I.1: $m_3(3,t) = \begin{cases} t+1 & t \text{ odd} \\ t+2 & t \text{ even} \end{cases}$ (Bose 1947)

Proof: $m_3(3,t)$ = maximum number of points possible in a PG(2,t) with no three collinear. Let M be a maximal set with this property. Through any point $0 \in M$ pass (t+1) lines in a PG(2,t), which exhaust all the points of the PG(2,t). There can be at most one other point of M on each line.

$$m_3(3,t) \leq 1 + (t+1) = t + 2 \qquad (\forall t)$$

Case 1: t even.

The matrix, A, has 3 rows with elements over GF(t) = {0, 1, b, $b^2,\ldots,b^{t-2}$} and (t+2) columns, no three of which are dependent.

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 0 & 1 & b & b^2 & \ldots & b^{t-2} \\ 0 & 0 & 1 & 1 & b^2 & b^4 & \ldots & b^{2t-4} \end{pmatrix}$$

$\therefore m_3(3,t) = t + 2$, t even.

Case 2: t odd.

Suppose we have (t+2) points, no three collinear. Then any three of them form a basis for the plane, PG(2,t). There exists

a linear transformation which will take these into the basis set $\{(1,0,0), (0,1,0), (0,0,1)\}$. Let the columns of C below be the set of (t+2) points, without loss of generality,

$$C = \begin{pmatrix} 1 & 0 & 0 & c_{11} & c_{12} & \cdots & c_{1,t-1} \\ 0 & 1 & 0 & c_{21} & c_{22} & \cdots & c_{2,t-1} \\ 0 & 0 & 1 & c_{31} & c_{32} & \cdots & c_{3,t-1} \end{pmatrix}$$

Since no three columns are dependent, then the partial determinant formed from any three columns must be non-zero.

$$\begin{vmatrix} 1 & 0 & c_{1j} \\ 0 & 1 & c_{2j} \\ 0 & 0 & c_{3j} \end{vmatrix} = c_{3j}, \quad \begin{vmatrix} 1 & 0 & c_{1j} \\ 0 & 0 & c_{2j} \\ 0 & 1 & c_{3j} \end{vmatrix} = -c_{2j}, \quad \begin{vmatrix} 0 & 0 & c_{1j} \\ 1 & 0 & c_{2j} \\ 0 & 1 & c_{3j} \end{vmatrix} = c_{1j}$$

$$j = 1, 2, \ldots, t-1.$$

Then $c_{ij} \neq 0$, $i = 1, 2, 3$; $j = 1, 2, \ldots, t-1$.

Since each point has (t-1) representatives, we may take $c_{1j} = 1$, $j = 1, 2, \ldots, t-1$, giving the matrix

$$D = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & d_{21} & d_{22} & \cdots & d_{2,t-1} \\ 0 & 0 & 1 & d_{31} & d_{32} & \cdots & d_{3,t-1} \end{pmatrix}$$

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & d_{2j} & d_{2k} \\ 0 & d_{3j} & d_{3k} \end{vmatrix} = -(d_{3k}-d_{3j}); \quad \begin{vmatrix} 0 & 1 & 1 \\ 0 & d_{2j} & d_{2k} \\ 1 & d_{3j} & d_{3k} \end{vmatrix} = (d_{2k}-d_{2j}).$$

Then $d_{3k} \neq d_{3j}$, $d_{2k} \neq d_{2j}$ for $j \neq k$, $j = 1, 2, \ldots, t-1$.

So $\{d_{21}, \ldots, d_{2,t-1}\}$ and $\{d_{31}, \ldots, d_{3,t-1}\}$ are each the non-zero elements of GF(t) in some order.

We may take $d_{21} = 1$, $d_{22} = b, \ldots, d_{2,t-1} = b^{t-2}$

and $d_{31} = b^{i_0}$, $d_{32} = b^{i_1}, \ldots, d_{3,t-1} = b^{i_{t-2}}$.

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & d_{2j} & d_{2k} \\ 0 & d_{3j} & d_{3k} \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & b^{j-1} & b^{k-1} \\ 0 & b^{i_j-1} & b^{i_k-1} \end{vmatrix} = (b^{j-1})(b^{i_k-1})-(b^{k-1})(b^{i_j-1}) \neq 0$$

So

$$\frac{b^{j-1}}{b^{i_j-1}} \neq \frac{b^{k-1}}{b^{i_k-1}} \qquad j \neq k,\ j = 1, 2, \ldots, t-1.$$

Then this set of ratios contains the non-zero elements of GF(t) in some order.

Let $S_1 = \{i_0, i_1, \ldots, i_{t-1}\}$

and $S_2 = \{i_0, (i_1-1)|\mathrm{mod}(t-1), (i_2-2)|\mathrm{mod}(t-1), \ldots, (i_{t-2}-(t-2))|\mathrm{mod}(t-1)\}$.

Then S_1 and S_2 are two different permutations of $S = \{0, 1, 2, \ldots, t-2\}$.

Let $(\Sigma S) = 0 + 1 + 2 + \ldots + (t-2) = (t-2)(t-1)/2 = \frac{(t-1)^2}{2} - (\frac{t-1}{2})$.

Since t is odd, then (t-1) is even and $(\Sigma S) \equiv (\frac{t-1}{2})|\mathrm{mod}(t-1)$, an integer greater than 0 and less than (t-1).

$(\Sigma S_1) \equiv (\Sigma S_2) \mod(t-1)$ since $\Sigma S_1 = \Sigma S_2$. But

$(\Sigma S_2) \equiv (\Sigma S_1 + \Sigma S) \mod(t-1)$.

$\therefore (\Sigma S) \equiv 0|\mathrm{mod}(t-1)$. Contradiction.

$\therefore m_3(3,t) \leq (t+1)$, t odd.

The matrix A' has 3 rows with elements over GF(t) and (t+1) columns with no three dependent

$$A' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & b & b^2 & \ldots & b^{t-2} \\ 0 & 1 & 1 & b^2 & b^4 & \ldots & b^{2t-4} \end{pmatrix}$$

$\therefore m_3(3,t) = t + 1$, t odd.

II. $m_3(4,t)$

Definition II.1: A set of (t+1) points in a PG with no three collinear is a (t+1)-CURVE.

Definition II.2: A set of (t+2) points in a PG with no three collinear is a (t+2)-CURVE.

Lemma II.1: There is exactly one tangent to any point of a (t+1)-curve in a PG(2,t).

Proof: Let P be a point of a (t+1)-curve C in PG(2,t). There are t lines joining P to the other points of C. Since there are (t+1) lines through any point of a PG(2,t), there is exactly one line through P with no other points of C. This line is called the TANGENT to C at P. The other lines with exactly 2 points of C are called SECANTS to C.

Lemma II.2: There are no tangents to a (t+2)-curve in a PG(2,t), t even.

Proof: Let P be a point of a (t+2)-curve D in PG(2,t). There are (t+1) lines joining P to the other points of D accounting for all (t+1) lines through P in a PG(2,t). All these lines contain exactly 2 points of D and are secants to D. There are no tangents to D.

THEOREM II.1: If t is odd, and Q is a point of PG(2,t) not in the (t+1) curve C, then there are exactly 2 or 0 tangents from Q to C.

Proof: Suppose there exists a tangent from Q to a point P of C. Each of the t other lines through Q can contain at most 2 of the other t points of C. If each contained exactly 0 or 2 then an even number would be counted, which is a contradiction for t odd. So if there is one tangent from Q to C, then there are at least two tangents from Q

to C. The same reasoning applies to each of the t positions for Q on the tangent QP. So there is at least one tangent to each of the t points of C - {P} from the t positions on QP. Then there is exactly one from each position by Lemma II.1. Therefore, any $Q \notin C$ has either 0 or 2 tangents to C.

Lemma II.3: For t odd, $t > 5$, let C_1, C_2 be (t+1)-curves in PG(2,t). If C_1, C_2 have more than (t+1)/2 points in common, then they are identical.

Proof: [Qvist, p.9].

THEOREM II.2: For t even, the tangents to a (t+1)-curve, C, meet in a point.

Proof: Let P_1, $P_2 \in C$ and $X \notin C$, with X on the line through P_1, P_2. There are (t-1) points of $C - \{P_1, P_2\}$, and (t-1) is odd, so there is at least one tangent from X to C since secants take 2 points each. This applies to each of the (t-1) positions for X on P_1P_2. So there is exactly one tangent to C from every point X on the secant P_1P_2. Thus two tangents cannot meet on a secant, that is, one cannot draw a secant from the point of intersection of two tangents, then only tangents can be drawn from the point of intersection of two tangents. Thus there are (t+1) lines, all tangents, to the (t+1)-curve C from the point Q where two tangents meet.

Corollary: For t even, any (t+1)-curve can be embedded in a (t+2)-curve.

Proof: Add the point Q where the tangents meet.

THEOREM II.3: $m_3(4,t) = (t^2 + 1)$ for $t \neq 2$.

Proof: Case 1: t odd. (Bose, 1947).

Let M be a maximal set of points in PG(3,t) with no three collinear.

By Theorem I.1 no more than (t+1) of these can be in the same plane PG(2,t). Let P_1, $P_2 \in M$. The line P_1P_2 has no other points of M. In PG(3,t) there pass (t+1) planes through the line P_1P_2 which exhaust all the points of PG(3,t). Each such plane can have at most (t-1) points of $M - \{P_1, P_2\}$. Therefore, $m_3(4,t) \leq 2 + (t+1)(t-1) = t^2 + 1$.

In PG(3,t), on the surface $x^2 - ky^2 + Zu = 0$ with k a non-residue, there are (t^2+1) points, no three collinear. [Quist, p.24].

$\therefore m_3(4,t) = t^2 + 1$, t odd.

Case 2: t even, $t \neq 2$. (Quist, Seiden: $t = 4$).

Let P be a point of a maximal set M, with no three points collinear. There are (t^2+t+1) lines through P which exhaust all the points of PG(3,t). Each of these lines can have at most one other point, P_1, of M. Thus,

$$m_3(4,t) \leq 1 + (t^2 + t + 1) = t^2 + t + 2.$$

Suppose $m_3(4,t) = t^2 + t + 2$. Then all lines through P are secants and there are no tangents to M. Any plane meets M is 0 or (t+2) points since there are no tangents by Lemma II.2. The number of secants to M equal the number of ways of choosing 2 points which equals $(t^2 + t + 2)(t^2 + t + 1)/2$. The number of lines in PG(3,t) equals $(t^2+1)(t^2+t+1)$. For $t > 1$, there are more lines than secants, and there exists a line, ℓ, not meeting M. Each of the planes through ℓ meets M in 0 or exactly (t+2) points, so the number of points in M is a multiple of (t+2).

So $(t+2)|(t^2+t+2)$ implies $(t+2)|((t^2+t+2) + (t+2))$

and $(t^2+t+2) + (t+2) = t(t+2) + 4$.

Then $t+2|4$ implies $t = 2$

and $m_3(4,2) = t^2 + t + 2 = 8$ (see Theorem III.1).

For $t > 2$, even: Let M contain (t^2+a) points, $a < t + 2$. Suppose $a > 1$; take M maximal. There are (t^2+a-1) secants through $P \in M$, there are (t^2+t+1) lines through P. So

tangents through P = # lines - # secants = $(t-a+2)$.

Since $a < (t+2)$, we can pick a tangent, T, through P. Each of the $(t+1)$ planes through T in PG(3,t) meet M in at most t other points since $(t+2)$ curves have no tangents. At least one plane, μ, does contain t other points; otherwise there would be $\leq 1 + (t+1)(t-1) = t^2$ points, a contradiction to $a > 1$. The $(t+1)$ tangents to the $(t+1)$ set obtained from $(\mu \cap M)$ meet in some point Q since t is even by Theorem II.2. If $Q \notin (\mu \cap M)$, then $Q \notin M$; so consider joining Q to M. If all lines from Q were tangents to C, we would have (t^2+a+1) points with no three collinear and M maximal, a contradiction. Thus there is a secant, S, from Q to M. Consider the planes through S, determined by S and each of the tangents from Q. Each of these has a tangent to M lying in μ, so none of these intersects M in $(t+2)$ points and each of these has at most $(t-1)$ other points of $C - \{P_1, P_2\}$.

Thus the number of points in $M \leq 2 + (t+1)(t-1) = t^2 + 1$, a contradiction to $a > 1$. Thus

$m_3(4,t) \leq t^2 + 1$.

In PG(3,t), on the surface $x^2 + y^2 + kxy + Zu = 0$, with k such that $(x/y)^2 + k(x/y) + 1 = 0$ has no roots in GF(t), there are (t^2+1)

points with no three collinear. [Quist, p.25].

$\therefore m_3(4,t) = t^2 + 1$, t even, $t \neq 2$.

III. $m_3(p,2)$.

THEOREM III.1: $m_3(p,2) = 2^{p-1}$ $\forall p \geq 3$ (Bose, 1947)

Proof: Let M be a maximal set of points in PG(p-1,2) with no three collinear. Through any point $P \in M$ there pass $(2^{p-1}-1)$ lines which exhaust the points of PG(p-1,2). Each of the lines can have at most one other point of M. So

$$m_3(p,2) \leq 1 + (2^{p-1}-1) = 2^{p-1}.$$

Consider the p-rowed matrix with elements over GF(2) = {0, 1} with each column containing an odd number of ones. The number of such columns is the number of ways of choosing an odd number of positions out of

$$p = (\binom{p}{1} + \binom{p}{3} + \ldots + \binom{p}{Z}) \text{ where } Z = p \text{ if } p \text{ odd}$$

$$= p-1 \text{ if } p \text{ even.}$$

Since

$$(1-1)^p = 0 = \binom{p}{0} - \binom{p}{1} + \binom{p}{2} - \binom{p}{3} \ldots$$

then $(\binom{p}{1} + \binom{p}{3} + \ldots + \binom{p}{Z}) = (\binom{p}{0} + \binom{p}{2} + \ldots + \binom{p}{Z'})$ where

$Z' = p$ if p even

$= p-1$ if p odd

and $\binom{p}{1} + \binom{p}{3} + \ldots + \binom{p}{2} = \frac{1}{2}(2^p) = 2^{p-1}$.

A subset of 3 columns of this matrix are linearly dependent if and only if a linear combination with coefficients in GF(2) is zero.

Then the sum of the three columns must be zero. In such a sum there are only two cases, either three zeroes or two ones and a zero will add to zero. Then the total number of ones in the three columns is even, a contradiction since each column has an odd number giving an odd total.

Then no subset of three columns are linearly dependent and the upper bound is attained.

$m_3(p,2) = 2^{p-1} \qquad \forall p \geq 3$

IV. $m_3(5,3)$

$m_3(5,3)$ = the maximum number of factors, m, possible in a (t^m, t^{m-5}) symmetrical, confounded, factorial design so that no interactions involving less than or equal to three factors are confounded.

THEOREM IV.1: $m_3(5,3) = 20$

Proof: [Tallini (1961), p.23].

V. Upper Bounds: $m_3(p,t)$

THEOREM V.1: $m_3(p,t) \leq 1 + (t^p-1)/(t-1)$ t even
or $\leq 1 + t^{p-2}$ t odd (Bose, 1947).

(These bounds have been improved, see * below.)

Proof: t even: Let m be a maximal set of points in PG(p-1,t) with no three collinear. Through a point P ε M there pass $(t^{p-1}-1)/(t-1)$ lines which exhaust all the points of PG(p-1,t). Each of these lines can have at most one other point of M. So $m_3(p,t) \leq 1 + (t^{p-1} - 1)/(t - 1)$.

t odd: Through P_1, $P_2 \in M$ there pass $(t^{p-2}-1)/(t-1)$ planes which exhaust all the points of PG(p-1,t). Each of these planes can have at most (t-1) other points of M by Theorem I.1. So

$$m_3(p,t) \leq 2 + (t-1)((t^{p-2}-1)/(t-1)) < 1 + t^{p-2}$$

THEOREM V.2: $m_3(p,t) < t^{p-2} + 1$, $t > 2$, $p \geq 5$

Proof: [Tallini, 1956]. This bound has been improved. (See * below.)

THEOREM V.3: i) $m_3(5,t) \leq t^3$; t even

ii) $m_3(p,t) \leq t^{p-2} - t \sum_{i=0}^{p-6} t^i$; t even, $p \geq 6$

(These bounds have been improved, see * below.)

* The following bounds are the best known currently. *

iii) $m_3(5,5) \leq 124$

iv) $m_3(p,5) \leq 5^{p-2} - 10\left(\sum_{i=0}^{p-6} t^i\right) - 1$; $p \geq 6$, $t = 5$

p	5	6	7	8	9	10	...
$m_3(p,5) \leq$	124	614	3064	15,314	76,564	382,814	...

v) $m_3(p,t) \leq t^{p-2} - (t-5)\left(\sum_{i=0}^{p-5} t^i\right) + 1$; $p \geq 5$, $t \geq 7$, t odd

t \ p	5	6	7	8	....
7	342	2,286	15,994	116,850	....
9	726	6,522	58,786	528,162	
11	1326	14,570	160,254	⋮	
13	2190	28,450	⋮		
15	3366	⋮			
⋮	⋮				

Proof: [Barlotti, 1957].

THEOREM V.4: i) $m_3(p,3) \leq (3^p + 23)/10$, $p \geq 6$

p	6	7	8	9	10	
$m_3(p,3) \leq$	76	211	659	1971	5908	...

ii) $m_3(5,t) \leq t^3 - 1$; $t \geq 4$, t even

t	4	6	8	10	12	14	...
$m_3(5,t) \leq$	63	215	511	999	1727	2743	...

iii) $m_3(p,t) < [(t^2-2t-1) + ((t^p-1)/(t-1))(t-2)]/(t^2-t-1) + 1$

for $p \geq 6$, $t \geq 4$, t even

t \ p	6	7	8	...
4	< 250	< 995	< 3,974	...
6	<1289	< 7,725	< 46,336	...
8	<4088	<32,685	<152,375	...
.	.	.	.	
.	.	.	.	
.	.	.	.	

Proof: [Bose and Srivastava, 1965]. There are the best bounds known currently. The authors give a representation of the points in a PG(p-1,t) which completely specifies the structure of a maximal set. This result along with Theorems II.3 and I.1 are used to obtain the bounds.

VI. Lower Bounds: $m_3(p,t)$

i) $m_3(3h+2,t) \geq t^{2h} + (t^{2h+2} - 1)/(t^2 - 1)$; $h \geq 1$, $\forall$ t

$m_3(3h+2,t) \geq (t^{2h-2})(5t^2-2t+1)/2 + (t^{2h-2}-1)/(t^2-1)$;

$h \geq 1$, for $t = k^\ell$, $k \equiv 7 \pmod 8$ implies $t \equiv 3 \pmod 4$

ii) $m_3(3h+3,t) \geq (t^{2h+2}-1)/(t-1) - t(t^{2h}-1)/(t^2-1)$; t odd

$\geq t^{2h} + (t^{2h+2}-1)/(t-1) - t(t^{2h}-1)/(t^2-1)$; t even

$h \geq 1$

iii) $m_3(3h+4) \geq (t^{2h+4}-1)/(t^2-1)$; $h \geq 1$, $t > 2$

Proof: [Segre, 1957].

Examples: h = 1, 2,

(a) $m_3(5,t) \geq (5t^2 - 2t + 1)/2; \qquad t \equiv 3 \pmod 4$

$\geq t^2 + (t^4 - 1)/(t^2 - 1)$

t	2	3	4	5	6	7	8	9	10	11	...
$m_3(5,t) \geq$	9	20	33	51	73	116	129	163	201	342	...

(b) $m_3(6,t) \geq (t^4 - 1)/(t - 1) - t(t^2 - 1)/(t^2 - 1); \qquad t$ odd

$\geq t^2 + (t^4 - 1)/(t - 1) - t(t^2 - 1)/(t^2 - 1); \quad t$ even

t	2	3	4	5	6	7	8	9	10	...
$m_3(6,t) \geq$	17	37	97	151	289	393	641	811	1183	...

(c) $m_3(7,t) \geq (t^6 - 1)/(t^2 - 1); \quad t > 2$

t	3	4	5	6	7	8	9	10	...
$m_3(7,t) \geq$	91	273	651	133	2451	4161	6643	11,111	...

(d) $m_3(8,t) \geq t^2(5t^2 - 2t + 1)/2 + (t^2 - 1)/(t^2 - 1); \quad t \equiv 3 \pmod 4$

$\geq t^4 + (t^6 - 1)/(t^2 - 1); \qquad t$ otherwise

t	2	3	4	5	6	7	8	9	10	11	...
$m_3(8,t)$	37	181	529	1276	2629	5685	8257	13,204	12,111	41,383	...

(e) $m_3(9,t) \geq (t^6 - 1)/(t - 1) - t(t^4 - 1)/(t^2 - 1); \qquad t$ odd

$\geq t^4 + (t^6 - 1)/(t - 1) - t(t^4 - 1)/(t^2 - 1); \quad t$ even

t	2	3	4	5	6	7	8	9	...
$m_3(9,t) \geq$	69	334	1553	3776	9109	14,258	36,029	65,692	...

(f) $m_3(10,t) \geq (t^8 - 1)/(t^2 - 1); \quad t > 2$

t	3	4	5	6	...
$m_3(10,t) \geq$	820	4369	16,276	47,989	...

(g) $m_3(11,t) \geq t^4(5t^2 - 2t + 1)/2 + (t^4 - 1)/(t^2 - 1)$; $t \equiv 3 \pmod 4$

$\geq t^6 + (t^8 - 1)/(t^2 - 1)$; t otherwise

t	2	3	4	...
$m_3(11,t)$	149	1630	8465	...

Remark: The book of D. Ragavarao (1971), recently published, includes many of these results in Chapter 13.

CHAPTER V. REFERENCES

1. BARLOTTI, A. (1957), Una Limitazione Superiore Per K Numbero Di Punti Appartementi A Una K-Calotta, C(k,0) Di Uno Spazio Linere Finito, Unione Matematica Italiana, Bolletino, Ser 3, V. 12, p.67-70.

2. BOSE, R. C. (1947), Mathematical Theory of the Symmetrical Factorial Design, Sankhya, Vol. 8, Part 2, p.107-166.

3. BOSE, R. C. and SRIVASTAVA, J. N. (1964), On a Bound Useful in the Theory of Factorial Designs and Error Correcting Codes, Annals of Mathematical Statistics 35, p.408-414.

4. QVIST, B. (1952), Some Remarks concerning Curves of the Second Degree in a Finite Plane, Suomalaisen Tiedeakatemian Toimituksia, Annales Academiae Scientiarum Fennicae, Series A - Mathematica - Physica, 134, p.1-27.

5. RAGAVARAO, D. (1971), Constructions and Combinatorial Problems in Design of Experiments, J. Wiley and Sons, New York.

6. SEGRE, B. (1957), Le Geometrie Di Galois, Annali Di Matimatica, Vol. 48, p.1-96.

7. SEIDEN, E. (1950), A Theorem in Finite Projective Geometry and an Application to Statistics, Proceedings of the American Mathematical Society, Vol. 1, p.282-286.

8. TALLINI, G. (1956), Sulla K-Callota Di Uno Spazio Linere Finito, Annali Di Matimatica, Vol. 42, p.119-164.

9. TALLINI, G. (1961), On Caps of Kind S in a Galois r-Dimensional Space, Acta Arithmetica, Vol. VIII, p.2-28.

CHAPTER VI. $m_4(p, t)$

The values for $m_4(4,t)$ and some values of $m_4(p,2)$ are known. Also $m_4(5,3) = 11$ and upper bounds are known for all other values.

I. $m_4(4,t)$

Lemma I.1: $m_4(4,t) \leq t + 3 \quad \forall t$

Proof: Let M be a maximal set in PG(3,t) with no four points in a plane. Through any points P_1, $P_2 \in M$ there pass (t+1) planes which exhaust the points of PG(3,t). Each of these planes can have at most one other point of M. So

$$m_4(4,t) \leq 2 + (t + 1) = t + 3.$$

Corollary I.1: $m_4(4,2) = 5$ (Rao, Seiden, Bush).

Proof: By Lemma I.1 $m_4(4,2) \leq 5$. The 4-rowed matrix, A, with elements over GF(2) has five columns with no four dependent.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Thus $m_4(4,2) = 5$.

Lemma I.2: $m_4(4,t) \leq t + 2$, t odd

Proof: Let M be a maximal set in PG(3,t) no four on a plane. Suppose the maximum of (t+3) of Lemma I.1 is attained. Through P_1, $P_2 \in M$ there pass exactly (t+1) planes, each with one other point of M. Through $P_1 \in M$ there pass $(1+t+t^2)$ lines; at least one of these has no

other point of M, otherwise $((1+t+t^2)+1) > t+3$, a contradiction. Let P_1C be such a line, where there are t positions for C. Through P_1C there pass (t+1) planes; if one of these has a second point of M, then it has a third by the initial assumption. Then each has either 0 or 2 more points of M. If ℓ = # of planes with 2 more points, then the (t+3) points of M are counted as $(2\ell+1)$. So $\ell = \frac{t+2}{2}$ implies t even, a contradiction.

$\therefore m_4(4,t) \leq t + 2$, t odd.

Corollary I.2: $m_4(4,3) = 5$ (Bush, Gulati and Kounias).

Proof: By Lemma I.2, $m_4(4,3) \leq 5$. The 4-rowed matrix, A, with elements over GF(3) has five columns no four dependent.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$\therefore m_4(4,3) = 5$.

THEOREM I.1: $m_4(4,4) = 5$ (Bush, Gulati and Kounias).

Proof: The 4-rowed matrix, A above, with elements over $GF(2^2) = \{0, 1, b, b^2\}$ has five columns, no four dependent. So

$$m_4(4,4) \geq 5.$$

Suppose we have a maximal set of six columns. Without loss of generality we may take them to be those of the matrix A': (p. II-4, Chapter II).

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & d_1 \\ 0 & 1 & 0 & 0 & 1 & d_2 \\ 0 & 0 & 1 & 0 & 1 & d_3 \\ 0 & 0 & 0 & 1 & 1 & d_4 \end{pmatrix}$$

No subset of four columns can be dependent. Then the last column must be all non-zero, otherwise a linear combination with 3 of the first 4 columns would be zero. So we may take $d_1 = 1$. No pair of d's are the same, otherwise a linear combination with the fifth, sixth and two of the first four columns would be zero. So d_2, d_3, $d_4 \in \{b, b^2\}$, an impossibility, and $m_4(4,4) < 6$. Thus $m_4(4,4) = 5$.

Lemma I.3: For t odd. Every maximal set, M, of (t+1) points in PG(2,t) no three collinear is contained in a unique irreducible conic, whose (t+1) points are identical with those of M.

Proof: [Segre, 1955].

Definition I.1: An IRREDUCIBLE CONIC in PG(2,t) is of the form $\Sigma a_{ij} X_i X_j$, $i \leq j$, $i = 1, 2, 3$ with the coefficients not all zero. There are five unknown coefficients since any one of the coefficients may be taken to be 1. The conic may then be determined by five points or four points and a tangent.

THEOREM I.2: For t even, every set, M, of (t+2) points in PG(3,t) with no four dependent can be completed to form a set of (t+3) points with no four dependent. (Gulati and Kounias).

Proof: (1) Through any P_1, $P_2 \in M$ there pass (t+1) planes which exhaust all the points of PG(3,t). At least one of these has no other point of M, otherwise the points in M would be counted as $2 + (t+1) > t + 2$, a contradiction. So, through any pair P_1, $P_2 \in M$ there pass exactly t planes with exactly 1 other point of M, and exactly 1 plane with no further point of M.

(2) Let R_1, R_2, $R_3 \in M$ determine a plane $T_3 \subset PG(3,t)$. Through R_1 pass (t+1) lines in T_3; R_1P_2, R_1R_3, which have exactly 2 points of M, and (t-1) others, $\{R_1P_q | 4 \leq q \leq t+2\}$, which have only $R_1 \in M$.

(3) Let $R_4 \in M$, $R_4 \notin T_3$. Through R_1R_4 passes exactly one plane, T_4, with no other of M by (1). Since 2 planes meet in a line, then T_4 intersects T_3 in one of the lines R_1P_q. Since there are (t-1) choices for R_4 there are in total (t-1) distinct planes, $\{T_q | 4 \leq q \leq t+2\}$, intersecting T_3 in one of the (t-1) distinct lines through R_1 in T_3, $\{R_1P_q | 4 \leq q \leq t+2\}$.

(4) Suppose y planes through R_1P_q have exactly 2 other points of M and the remaining (t+1-y) planes through R_1P_q have no other points of M. The (t+2) points of M are counted as (2y+1) implying $t = 2y-1$, an odd number, and a contradiction. Thus R_1P_q has at least one plane through it with exactly 1 other point of M for each $4 \leq q \leq t+2$.

(5) Since there are only (t-1) planes to distribute over the (t-1) lines by (3), and each line must receive at least one line by (4), then there must be a 1-1 correspondence and each line R_1P_q is cut by exactly one plane T_q with no other points of M for $4 \leq q \leq (t+2)$.

(6) Let the unique plane of (1) with no other point of M through R_1R_3 be X, through R_1R_2 be Y, and through R_2R_3 be Z. There three planes meet in a point $Q \notin M$. Through R_1Q pass (t+1) planes; suppose one of these, T, has two other points of M, say R_i and R_j. Then R_1Q will be a line in a plane $R_1R_iR_j$ and there is only one plane through R_1Q with exactly one other point of M by (5). But X, Y both have exactly one other point of M, a contradiction. So no plane through R_1Q has 2 other points of M.

(7) Since the (t+1) planes through R_1Q exhaust the points of PG(3,t), all (t+1) other points of M must be distributed over these (t+1) planes. Since no plane can have 2 more points of M by (6), then each must have only 1 other point of M. The same reasoning holds for R_2 and R_3; so every plane through R_1Q, R_2Q and R_3Q has exactly one other point of M.

(8) Consider R_i, R_2, R_3. The unique planes with no other point of M through R_iR_2, R_iR_3 and R_2R_3 meet in the same point Q of (7). By the same reasoning as in (6) and (7) every plane through R_iQ has exactly one other point of M, for $4 \leq i \leq (t+2)$. So the planes R_iR_jQ, $i \neq j$, $i, j \in \{1, 2,\ldots,t+2\}$ have no other point of M.

(9) Add Q to the (t+2) points of M to form a set of (t+3) points in PG(3,t) with no 4 dependent. This set is maximal by Lemma I.1.

THEOREM I.3: $m_4(4,t) = t + 1$, $t \geq 5$ (Gulati and Kounias).

Proof: In the first part we consider three different cases and find an upper bound, in the second part we show this bound is attained.

Part I. Finding an upper bound.

Case (a): $t = k^{\ell}$, k odd.

(1) Suppose we have a set, S, of (t+2) points in PG(3,t) no four dependent. P_1, P_2, $P_3 \in S$ determine a plane, T. Let $P,Q \in S$. The (t+1) points of S - {P} when projected from P onto the plane T give a non-collinear set of (t+1)-points in the plane T. For if 3 of these were on the same line, ℓ, in T, then the plane determined by ℓ and P would contain 4 points of S, a contradiction. These (t+1) points in T

are the points of an irreducible conic, C, by Lemma I.3. Similarly, the (t+1) points in T obtained by projection of S - {Q} onto T are the points of an irreducible conic, C_2.

(2) Now C_1, C_2 have the 4 points P_1, P_2, P_3, R in common where R is the projection of P from Q (Q from P) onto T. The tangent to T at R of Lemma II.1, Chapter V, is common to C_1 and C_2; it is the intersection of T and the unique plane through PQ having no additional point of S (see Theorem I.2, part (1)). So C_1, C_2 coincide by definition I.1.

(3) Let P^* on the conic be the projection of L through P, and of M through Q. Then the plane determined by PQP^* contains the 4 points {P, Q, L, M}, a contradiction. Thus, such a set, S, of (t+2) points cannot exist. So $m_4(4,t) \leq t + 1$, t odd.

Case (b): $t = 2^{2h}$, t even.

(1) Let M be a maximal set of (t+3) points in PG(3,t), no four dependent. Using the same reasoning as in Lemma I.2 we find that through $A \in M$, $C \notin m$, there pass $(\frac{t+2}{2})$ planes with exactly 2 points of M - {A}, and $(t+1 - \frac{t+2}{2}) = \frac{t}{2}$ planes with no points of M - {A}.

(2) Let P_i, P_1, $P_2 \in M$; let Q be on the line P_1P_2 with $Q \notin M$. Through QP_i there pass $(\frac{t}{2} + 1)$ planes with exactly 2 points of M - $\{P_i\}$ by (1), namely $P_iP_1P_2$ and $\frac{t}{2}$ others. This is true for i = 3, 4,...,t+3. So the number of planes through QP_i, i = 3, 4,...,t+3 excepting $P_iP_1P_2$ is counted as $(\frac{t}{2})(t+1)$. But each of these is counted three times, once for each virtice. The number of such planes is counted as $\frac{t}{2} \cdot \frac{t+1}{3}$ which must be an integer.

(3) For $t = 2^{2h}$, then $2^{2h}(2^{2h}+1)/6$ is an integer

then $3 \mid (2^{2h-1})(2^{2h}+1)$.

Now $2^r = (3-1)^r = 3^r + \binom{r}{1}3^{r-1}(-1) + \ldots + \binom{r}{r}3^0(-1)^r$

$= 3\left[3^{r-1} + \ldots + \binom{r}{r-1}(-1)^{r-1}\right] + (-1)^r$

So $2^r \equiv 1 \pmod 3$ if r even;

$\equiv 2 \pmod 3$ if r odd.

So $(2^{2h-1})(2^{2h}+1) \equiv (2^{2h-1} \pmod 3)\cdot((2^{2h}+1) \pmod 3)$

$\equiv (2)(2) \pmod 3$

$\equiv 1 \pmod 3$, a contradiction.

So a maximal set of (t+3) cannot be attained.

(4) By Theorem I.2, any set of (t+2) in PG(3,t) with no four dependent can be completed to a set of (t+3). Since the latter does not exist, then the former does not exist. So $m_4(4,t) \leq t + 1$, $t = 2^{2h}$, even.

Case (c): $t = 2^{2h+1}$, t even

(1) Let M be a maximal set of (t+3) points in PG(3,t), no four dependent. There are $(1+t+t^2+t^3)$ points in PG(3,t). Through two points of M there pass $\binom{t+3}{2}$ lines; each has 2 points of M and (t-1) others not in M. The number of points in M plus the number of lines through 2 points of M is

$$(t+3) + (t-1)\left(\frac{t+3}{2}\right) = (t^3+5t^2+5t-6)/2 < (1+t+t^2+t^3).$$

So there exists a point $R \notin M$, and R is not on any line through 2 points of M.

(2) Let $\{P_i,\ i = 1, 2,\ldots,t+3\}$ be the points of M. As in case (b) (2), we find (t+2)/2 planes through the line P_iR with exactly 2 points of $M - \{P_i\}$, $i = 1, 2,\ldots,t+3$. Each of these is counted

three times, once for each vertice. The number of such planes is counted as $(\frac{t+2}{2})(\frac{t+3}{3})$ which must be an integer.

(3) For $t = 2^{2h+1}$, then $\frac{(2^{2h+1}+2)(2^{2h+1}+3)}{6}$ is an integer;

then $3 \mid (2^{2h}+1)(2^{2h+1}+3)$.

But $(2^{2h}+1)(2^{2h+1}+3) \equiv ((2^{2h}+1)(\text{mod } 3))((2^{2h+1}+3)(\text{mod } 3))$

$\equiv (2)(2)(\text{mod } 3)$

$\equiv 1 \text{ (mod } 3)$, a contradiction.

So a maximal set of (t+3) is not attainable.

(4) By Theorem I.2 if a set of (t+3) is impossible, then so is a set of (t+2). So $m_4(4,t) \leq (t+1)$, $t = 2^{2h+1}$, even.

Part II. The upper bound is attained.

The 4-rowed matrix, M, with elements in $GF(t) = \{0, 1, b, b^2, \ldots, b^{t-2}\}$ has (t+1) columns, no four of which are dependent.

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 0 & 1 & b & b^2 & \ldots & b^{t-2} \\ 0 & 0 & 1 & b^2 & b^4 & \ldots & b^{2t-4} \\ 0 & 1 & 1 & b^3 & b^6 & \ldots & b^{3t-6} \end{bmatrix}$$

Consider the possible sub-matrices of 4 columns.

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ b^{i_1} & b^{i_2} & b^{i_3} & b^{i_4} \\ (b^2)^{i_1} & (b^2)^{i_2} & (b^2)^{i_3} & (b^2)^{i_4} \\ (b^3)^{i_1} & (b^3)^{i_2} & (b^3)^{i_3} & (b^3)^{i_4} \end{bmatrix} \qquad |M_1| = \prod_{j<k} (b^{i_j} - b^{i_k}),$$

$$j, k = 0, 1, 2, 3, 4.$$

$$M_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & b^{i_1} & b^{i_2} & b^{i_3} \\ 0 & (b^2)^{i_1} & (b^2)^{i_2} & (b^2)^{i_3} \\ 1 & (b^3)^{i_1} & (b^3)^{i_2} & (b^3)^{i_3} \end{bmatrix} \qquad |M_2| = \prod_{j<k} (b^{i_j} - b^{i_k}),$$

$$j, k = 0, 1, 2, 3.$$

$$M_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & b^{i_1} & b^{i_2} & b^{i_3} \\ 0 & (b^2)^{i_1} & (b^2)^{i_2} & (b^2)^{i_3} \\ 0 & (b^3)^{i_1} & (b^3)^{i_2} & (b^3)^{i_3} \end{bmatrix} \qquad |M_3| = \prod_{j<k} (b^{i_j} - b^{i_k}),$$

$$j, k = 1, 2, 3, 4.$$

These determinants are all non-zero since b^{i_j}, b^{i_k} are distinct non-zero elements of GF(t). So no set of 4 columns are linearly dependent. So $m_4(4,t) = t + 1$, $t \geq 5$.

II. $m_4(5,t)$

THEOREM II.1: $m_4(5,3) = 11$ (Gulati and Kounias)

Proof: Let M be a maximal set in PG(4,t) with no four on a plane. For t odd, then Lemma I.2 gives at most (t+2) points of M in a PG(3,t). Through any 3 points P_1, P_2, $P_3 \in M$ there pass (t+1) PG(3,t)'s which exhaust all the points of PG(4,t). Each of these PG(3,t)'s can have at most (t+2)-3 = (t-1) other points of M. Then the number of points in $M \leq 3 + (t-1)(t+1) = t^2 + 2$, t odd. Thus $m_4(5,3) \leq 3^2 + 2 = 11$.

The 5-rowed matrix, A, with elements over GF(3) has 11 columns, no four of which are dependent. This may be checked by observation and simple enumeration. (Tallini, 1961).

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

Thus $m_4(5,3) = 11$.

THEOREM II.2: $m_4(5,t) \leq t(t-1)$, $t \geq 4$. (Gulati and Kounias).

Proof: (1) Let M be a maximal set of points in PG(4,t), no four dependent. Through P_1, P_2, $P_3 \in M$ there pass (t+1) PG(3,t)'s which exhaust all the points of PG(4,t). Since $m_4(4,t) = t+1$, each of these PG(3,t)'s can have at most $(t+1)-3 = t-2$ other points of M. Thus $m_4(5,t) \leq 3 + (t-2)(t+1) = t^2-t+1$.

(2) Suppose M attains the maximum of t^2-t+1. Through P_1, $P_2 \in M$ there pass (t^2+t+1) planes which exhaust all the points of PG(4,t). At least one of these planes, T, has no other point of M, otherwise the points in M would be counted as $\geq (t^2+t+1) + 2 \geq (t^2-t+1)$, a contradiction.

(3) Let $P \in T$, through P_1, P_2, P pass exactly (t+1)-PG(3,t)'s which exhaust all the points of PG(4,t). In order to attain a maximum of (t^2-t+1) every PG(3,t) which contains 3 points of M must contain (t-2) others by (1). Thus each PG(3,t) containing P_1, P_2, P has either (t-1) or 0 more points of M.

(4) Suppose there are S with (t-1) more points of M. Then the (t^2-t+1) points of M are counted as $S(t-2) + 2$. Then

$$S = (t^2-t-1)/t-1 = t - (\frac{1}{t} - 1)$$

must be an integer. This is a contradiction for $t \geq 4$, so $m_4(5,t) < t^2 - t + 1$. Thus $m_4(5,t) \leq t^2 - t = t(t-1)$, $t \geq 4$.

THEOREM II.3: $m_4(5,t) \leq ((t-3) + (8t^5+t^2-6t+1)^{1/2})/(2(t-1))$ for $t \geq 2$.

Proof: (Bose, Rao). See Corollary II.1, Chapter VIII.

A simple algebraic comparison shows that II.3 gives the better bound for $t \geq 5$.

t	4	5	6	7	8	.....
Gulati and Kounias Bound	12	20	30	42	56	....
Bose-Rao Bound	15	20	25	30	36	.....

III. $m_4(p,2)$

THEOREM III.1: $m_4(5,2) = 6$; $m_4(6,2) = 8$; $m_4(7,2) = 11$

(Rao, 1947; Seiden, 1964).

Proof: By enumeration, assuming without loss of generality that the p basis points $\{B_i = (a_1, a_2, \ldots, a_p)$, $a_i = 1$, $a_j = 0$, $j \neq i$ $i = 0, 1, \ldots, p-1\}$ belong to the maximal set of points in PG(p-1,2) no four on a plane. (See Corollary I.1, Chapter VII).

The following are examples of maximal sets:

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

$m_4(5,2) = 6$

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

$m_4(6,2) = 8$

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

$m_4(7,2) = 11$

THEOREM III.2: $m_4(8,2) = 17$; $m_4(9,2) \leq 29$; $m_4(p,2) \leq 3(2^{p-6}-1)+8$, $p \geq 10$.

Proof: (Seiden, 1964).

Let M be a maximal set in PG(p-1,2), no four on a plane. There are $(2^{p-6}-1)$-PG(6,2)'s containing any PG(5,2), which exhaust all the

points of PG(p-1,t). By Theorem III.1 $m_4(6,2) = 8$, $m_4(7,2) = 11$. Suppose our PG(5,2) has the maximum of 8 points of M. Then there are at most 11-8 = 3 more points of M in each of these. Thus $m_4(p,2) \leq 8 + 3(2^{p-6} - 1)$, $p \geq 8$.

For p = 8: $m_4(8,2) \leq 17$. The 8-rowed matrix, A, with elements in GF(2) has 17 columns with no four dependent.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Thus $m_4(8,2) = 17$.

For p = 9: $m_4(9,2) \leq 8 + 3(2^3 - 1) = 8 + 3(7) = 29$.

THEOREM III.3: $m_4(p,2) \leq m$ where $m(m+1) \leq 2^{p+1}-2$, $p \geq 5$.

Proof: (Bose, Rao). See Corollary II.1, Chapter VIII.

An algebraic comparison shows III.3 is better for $p \geq 10$.

p	8	9	10	11	12	...
$m \leq 8 + 3(2^{p-6}-1)$	17	29	53	101	197	...
$m(m+1) \leq 2^{p+1} - 2)$	22	31	44	63	90	...

IV. $m_4(p,t)$ = maximum number of points possible in a PG(p-1,t) with no four coplanar.

= maximum number of columns in a p-rowed matrix with elements of GF(t) with no four dependent

= maximum number of factors, m, in a (t^m, t^{m-p}) symmetrical,

confounded, factorial design so that no interactions involving less than or equal to four factors are confounded.

THEOREM IV.1: $m_4(p,t) \leq t^{p-3} - (t+1)\left[\sum_{j=1}^{p-5} t^j\right] + 1$ for $p \geq 6$, $t \geq 4$.

Proof: Let M be a maximal set of points, no four collinear in PG(p-1,t). Through any PG(3,t) pass exactly $(1+t+\ldots+t^{p-5})$-PG(4,t)'s. If we let PG(3,t) have its maximum of (t+1) points of M, then there are at most $t(t-1)-(t+1) = (t^2-2t-1)$ points of M in each of the PG(4,t)'s by Theorem II.2.

$$\therefore m_4(p,t) \leq (t+1) + (t^2-2t-1)(1+t+\ldots+t^{p-5})$$

$$= t + (t^2-t)\sum_{0}^{p-5} t^j - (t+1)\left[\sum_{0}^{p-5} t^j\right] + 1$$

$$= t + \sum_{2}^{p-3} t^j - \sum_{1}^{p-4} t^j - (t+1)\left[\sum_{0}^{p-1} t^j\right] + 1$$

$$\therefore m_4(p,t) \leq t^{p-3} - (t+1)\left[\sum_{0}^{p-5} t^j\right] + 1, \; p \geq 6, \; t \geq 4. \quad \text{(Gulati and Kounias).}$$

THEOREM IV.2: $m_4(p,t) \leq \dfrac{(t-3) + (8t^p+t^2-6t+1)^{1/2}}{2(t-1)}$, $p \geq 6$, $t \geq 4$.

Proof: (Bose, Rao). See Corollary II.1, Chapter VIII.

A simple algebraic comparison shows IV.2 gives the better bounds for $p \geq 6$, $t \geq 4$. For example:

t = 4, p =	6	7	8	9	....
Gulati and Kounias Bound	40	152	600	2392	....
Bose, Rao Bound	30	60	120	241	....

p = 6, t =	4	5	6	7	8	....
Gulati and Kounias Bound	40	90	168	280	432	...
Bose, Rao Bound	30	44	61	81	103	...

THEOREM IV.3: $m_4(p,3) \leq 2 + 3^{p-3}$, $p \geq 6$.

Proof: Let M be a maximal set of points, no four coplanar in PG(p-1,3). Through any PG(3,3) pass exactly $1+3+3^2+\ldots+3^{p-5}$ PG(4,3)'s. If we let PG(3,3) have its maximum of 5 points in M, then there are at most 11-(5) = 6 points of M in each of the PG(4,3)'s by Theorem II.1. Therefore, $m_4(p,3) \leq 5 + 6(1+3+3^2+\ldots+3^{p-5})$, $p \geq 6$. Let $X = 1 + 3 + \ldots + 3^{p-5}$. Then $3S = 3 + \ldots + 3^{p-5} + 3^{p-4}$,

$$2S = (3^{p-4} - 1).$$

Then $m_4(p,3) \leq 5 + 6\left(\frac{3^{p-4}-1}{2}\right) = 5 + 3(3^{p-4} - 1) = 3^{p-3} + 2.$

THEOREM IV.4: $m_4(p,3) \leq (\frac{1}{2}(3^p-1))^{1/2}$, $p \geq 4$.

Proof: (Bose, Rao). See Corollary II.1, Chapter VIII.

An algebraic comparison shows that IV.4 gives the better bound, $p \geq 5$.

p	4	5	6	7	8	9	...
$3^{p-3}+2$	5	11	29	83	245	731	...
$(\frac{1}{2}(3^p-1))^{1/2}$	6	11	19	33	56	99	...

Remark: The original upper bound on $m_4(p,t)$ obtained by Bose, Rao (1947) appears to remain as the best known for all but two of the values which are not yet completely determined.

Seiden's bound on $m_4(p,2)$, $p \geq 9$, is better only for p = 9, a reduction from 31 to 29. The bound on $m_4(5,t)$, $t \geq 4$, of Gulati and Kounias is better only for t = 4, an improvement from 15 to 12, and these same authors bound on $m_4(p,t)$, $t \geq 4$, $p \geq 6$ offers no improvements over the original (1947) bound. This author used the same technique on $m_4(p,3)$ only to meet a similar fate.

Gulati and Kounias (1970) are incorrect in asserting that Seiden's bound is the best known, and it is not clear if either the latter or the former realized that their bounds were, in fact, not improvements on a previous result.

CHAPTER VI. REFERENCES

1. BUSH, K. A. (1952). Orthogonal Arrays of Index Unity, Annals of Mathematical Statistics, Vol. 23, p.425-434.

2. GULATI, B. R. and KOUNIAS, E. G. (1970). On Bounds Useful in the Theory of Symmetrical Factorial Designs, Journal of the Royal Statistical Society, Series B, p.123-133.

3. RAO, C. R. (1947). Factorial Experiments Derivable from Combinatorial Arrangements of Arrays, Journal of the Royal Statistical Society, Supp. (9), p.128-139.

4. SEGRE, B. (1955). Curve Razionali E k-Archi Negli Spazi Finiti, Annali Matimatica Pure Applicata, (4)39, p.357,379.

5. SEIDEN, E. (1964). On the Maximum Number of Points no Four on One Plane in a Projective Space PG(r-1,2), Technical Report RM-117, Michigan State University.

6. TALLINI, G. (1961). On Caps of Kind S in Galois r-Dimensional Space, Acta Arithmetica, VII, p.19-28.

CHAPTER VII. $m_f(f+r,2)$

Introduction: A sequential procedure is developed which leads to all values of $m \equiv m_f(f+r,2)$ for which $m \leq 2f + r$, $f \geq 4$, $r \geq 0$, and assigns to all other cases a lower bound of $(2f+r+1)$, $f \geq 4$, $r \geq 0$. Gulati and Kounias (1969) state the Theorems 1, 2, 3 below, but give no proofs, so the author has supplied his own. The author is also responsible for the culmination of the procedure in its logical conclusion, namely, the proof of the general result.

THEOREM I: $m_f(f+r,2) \geq f+r+1$ for $f \geq 2$, $r \geq 0$.

Proof: Without loss of generality the maximal set may be taken to include the $(f+r)$ points each with exactly one 1, the standard basis for a $PG(f+r-1,t)$ and any other, Q_1. Thus, $m_f(f+r,t) = f+r+g$, $g \geq 1$. Let this maximal set be denoted by $\{B_1, B_2, B_3,\ldots,B_{f+r}, Q_1, Q_2,\ldots,Q_g\}$.

THEOREM II: The necessary and sufficient conditions for the existence of Q_i, $i = 1, 2,\ldots,g$, is that the sum of any j of the Q_i with $1 \leq j < \min\{g,f\}$ has at most $(r+j-1)$ zero co-ordinates.

Proof: (Necessity). The restriction on our points is that no set of f is linearly dependent. Since the elements come from GF(2), the only linear combination of points is their sum modulo 2. So any set of j points, $1 \leq j \leq f$ must have at least one 1 in the sum. Then any set of $1 \leq j \leq \min\{g,f\}$ of the $\{Q_1, Q_2,\ldots,Q_g\}$ must have at least ℓ ones in the sum where ℓ is such that adding up to $(f-j)$ members of $\{B_1, B_2,\ldots,B_{f+r}\}$ to these j will still leave at least

one 1 in the sum. Now the worst that could happen would be adding (f-j) points each with a 1 where the sum of the j points has a 1. Then all (f-j) positions would revert to 0 in the grand sum.

There are (f+r) positions in any sum, so $\ell \geq (f+j-1)$ and we need at least (f-j+1) ones in the sum of any $1 \leq j \leq \min\{g,f\}$ from $\{Q_1, Q_2, \ldots, Q_g\}$. So we can have at most $(f+r) - (f-j+1) = (r+j-1)$ zeroes in the sum of any set of $1 \leq j \leq \min\{g,f\}$ from $\{Q_1, Q_2, \ldots, Q_g\}$.

(Sufficiency). Clear from the construction involved above.

This completes the proof.

Now consider finding the condition on f in order that Q_2 exists. We know Q_1 exists by Theorem 1. Let $Q_1 = (a_1, a_2, \ldots, a_{f+r})$, $Q_2 = (b_1, b_2, \ldots, b_{f+r})$. Let

$$V_2 = \begin{array}{c} \begin{matrix} X_0 & X_1 & X_2 & X_3 \end{matrix} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \end{array};$$

define the variables X_0 = # indices with $a_h = b_h = 0$

X_1 = # indices with $a_h = 1$, $b_h = 0$

X_2 = # indices with $a_h = 0$, $b_h = 1$

X_3 = # indices with $a_h = b_h = 1$.

Then $\sum_{i=0}^{3} X_i = f + r$. By Theorem II, the following inequalities must hold for the existence of Q_2:

$$X_0 + X_1 \leq r \qquad \begin{pmatrix} Q_2 \\ Q_1 \\ Q_1+Q_2 \end{pmatrix}$$
$$X_0 + X_2 \leq r$$
$$X_0 + X_3 \leq (r+1)$$

Adding over these inequalities: $2X_0 + \sum_0^3 X_i \leq (3r+1)$. The maximum value of $\sum_0^3 X_i = (f+r)$ occurs for $X_0 \equiv 0$, and $\sum_0^3 X_i = f+r \leq 3r+1$ or $f \leq 2r + 1$.

Now $X_0 = 0$, $X_1 = X_2 = r$ and $X_3 = r+1$ satisfies all the restrictions so that $(2r+1)$ is the maximum value of f for which Q_2 exists. Thus $m_f(f+r,2) \geq f+r+2$ for $f \leq 2r + 1$.

But for $f > 2r + 1$, Q_2 does not exist and by Theorem I $m_f(f+r,2) \geq f+r+1$. Thus $m_f(f+1,2) = f+r+1$, $f \geq 2r + 2$, $f \geq 4$, $r \geq 0$.

For the cases with $g \geq 3$ we would follow this GENERAL PROCEDURE:

(1) Form 2^g-1 linear inequalities in 2^g unknowns by Theorem II.

(2) Add over these inequalities to obtain the following linear inequality in $\Sigma X_i = (f+r)$:

$$(2^g-1)X_0 + (2^{g-1}-1)\left(\sum_{j=0}^{2^g-1} X_j\right) \leq r(2^g-1) + ((g-2)2^{g-1} + 1)$$

(3) Add over the inequalities involving X_j to obtain the following linear inequalities for X_j, $j = 1, 2, \ldots, (2^g-1)$.

$$(2^{g-2})X_0 + 2^{g-2}X_j + (2^{g-2}-1)\left(\sum_{0\ \ j}^{2^g-1} X_j\right) \leq r(2^{g-1}-1) + ((g-3)2^{g-2} + 1)$$
$$\text{for } j = 1, 2, 2^2, \ldots, 2^{g-1}$$
$$\leq r(2^{g-1}-1) + ((g-2)2^{g-2} + 1)$$
$$\text{for } j \text{ otherwise.}$$

(4) The maximum value of $(f+r) = \Sigma X_i$ occurs for $X_0 = 0$. Try the maximum of Step 2 in Step 3. Lower the maximum for (f+r) from Step 2

until a value consistent with Step 3 is found. This involves $(2^{g-1}-1)$ cases, one for each possible value of $r \equiv j \pmod{(2^{g-1}-1)}$. (For proof of these inequalities and the general solution, see Theorems IV, V, VI.)

For example, we find the condition on f for the existence of Q_3. Let $Q_3 = (c_1, c_2, \ldots, c_{f+r})$. Let

$$V_3 = \begin{array}{c} \begin{matrix} X_0 & X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & X_7 \end{matrix} \\ \left[\begin{matrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}\right] \end{array} \begin{matrix} a_h \\ b_h \\ c_h \end{matrix} ;$$

define $\{X_0, X_1, \ldots, X_7\}$ as before. Then $\sum_{i=0}^{7} X_i = f+r$. From Step 1 we form $2^g-1 = 7$ linear inequalities.

$$\begin{array}{ll} X_0 + X_1 + X_4 + X_5 \leq r & Q_2 \\ X_0 + X_2 + X_4 + X_6 \leq r & Q_2 \\ X_0 + X_3 + X_4 + X_7 \leq r+1 & Q_1+Q_2 \\ X_0 + X_1 + X_6 + X_7 \leq r+1 & Q_2+Q_3 \\ X_0 + X_2 + X_5 + X_7 \leq r+1 & Q_1+Q_3 \\ X_0 + X_3 + X_5 + X_6 \leq r+2 & Q_1+Q_2+Q_3 \\ X_0 + X_1 + X_2 + X_3 \leq r & Q_3 \end{array}$$

From Step 2, adding over all inequalities yields $4X_0 + 3\sum_{0}^{7} X_i \leq 7r + 5$.

From Step 3: $2X_0 + 2X_j + \sum_{0}^{7} X_i \leq 3r + 1 \quad j = 1, 2, 4$

$\leq 3r + 3 \quad j = 3, 5, 6, 7.$

From Step 4, $X_0 = 0$ maximizes $(f+r) = \sum_{0}^{7} X_i \leq \frac{7r+5}{3}$.

Case 1: $r \equiv 0 \pmod 3$ implies $r = 3p$ and $f+r = \sum_{0}^{7} X_i \leq 7p + 1$. Now consider $2X_j \leq (3r+1) - (\Sigma X_i) \leq (9p+1) - (7p+1) = 2p$ so $X_j \leq p$, $j = 1, 2, 2^2$.

And $2X_j \leq (3r+3) - (\Sigma X_i) \leq (9p+3) - (9p+1) = 2p + 2$. Thus $X_j \leq (p+1)$, $j = 3, 5, 6, 7$. Then the maximum value of $(f+r) = \Sigma X_i = 2p + 1$ is attained.

Case 2: $r \equiv 1 \pmod 3$ implies $r = 3p+1$ and $f+r = \Sigma X_i \leq 7p + 4$. Now consider $2X_j \leq 3(3p+1) + 1 - (7p+4) = 2p$. Thus $X_j \leq p$, $j = 1, 2, 2^2$. And $2X_j \leq 3(3p+1) + 3 - (7p+4) = 2p + 2$. Thus $X_j \leq p + 1$, $j = 3, 5, 6, 7$. Then the maximum value of $f+r = \sum_0^7 X_i = 7p+4$ is attained.

Case 3: $r \equiv 2 \pmod 3$ implies $r = 3p+2$ and $f+r = \Sigma X_i \leq 7p+6$. Now consider $2X_j \leq 3(3p+2) + 1 - (7p+6) = 2p + 1$. Thus $X_j \leq p$, $j = 1, 2, 2^2$. And $2X_j \leq 3(3p+2) + 3 - (7p+6) = 2p + 3$. Thus $X_j \leq p + 1$, $j = 3, 5, 6, 7$. Then the maximum possible value of $\sum_0^7 X_i = 3p + 4(p+1) = 7p + 4 < 7p + 6$. So the maximum value of $(7p+6)$ is not attained. Now reduce by 1 and try the value of $(f+r) = 7p + 5$.

$2X_j \leq 3(3p+2) + 1 - (7p+5) = 2p + 2$; so $X_j \leq p + 1$, $j = 1, 2, 2^2$;

$2X_j \leq 3(3p+2) + 3 - (7p+5) = 2p + 4$; so $X_j \leq p + 2$, $j = 3, 5, 6, 7$.

Then the maximum value of $f+r = \sum_0^7 X_i = 7p + 5$ is attained. Let

$$f_3(r) = (r+1) + \left[\frac{r+2}{3}\right] \qquad r \equiv 0, 1 \pmod 3$$

$$= r + \left[\frac{r+2}{3}\right] \qquad r \equiv 2 \pmod 3.$$

Then $f_3(r)$ is the maximum value of f for which Q_3 exists. Thus $m_f(f+r,2) \geq f+r+3$ for $f \leq f_3(r)$. But $(f_3(r)+1) \leq f \leq (2r+1)$ means Q_2 exists and Q_3 does not; thus $m_f(f+r,2) = f+r+2$ for f in this range.

Definitions:

$$A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \bar{X} = \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix}, \quad I_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Then the system of inequalities at the top of page 3 may be written as $A_2\bar{X} \leq rI_2 + D_2$. We now prove this is true in general.

Define:

$$A_g = \begin{pmatrix} A_{g-1} & A_{g-1} \\ A_{g-1} & \bar{A}_{g-1} \\ \underline{1} & \underline{0} \end{pmatrix}, \quad I_g = \begin{pmatrix} I_{g-1} \\ I_{g-1} \\ 1 \end{pmatrix}, \quad D_g = \begin{pmatrix} D_{g-1} \\ D_{g-1}+I_{g-1} \\ 0 \end{pmatrix}$$

$$\bar{X} = \begin{pmatrix} X_0 \\ \vdots \\ X_{2^g-1} \end{pmatrix}, \quad V_g = \begin{pmatrix} V_{g-1} & V_{g-1} \\ \underline{0} & \underline{1} \end{pmatrix}$$

where $\bar{A}_{g-1}$ is A_{g-1} with the ones and zeroes interchanged.

THEOREM III: The system of linear inequalities for the existence of Q_g may be written as $A_g\bar{X} \leq rI_g + D_{g-1}$ where A_g is a $(2^g-1)X2^g$ matrix of zeroes and ones, each of its rows with 2^{g-1} zeroes and ones, and each of its columns having $(2^{g-1}-1)$ ones and (2^{g-1}) zeroes, except for the first column which is a column of (2^g-1) ones.

Proof: By induction. This is easily checked for g = 3. Assume true up to (g-1). Consider treating three cases as indicated.

$$\begin{array}{ll} a) & \begin{pmatrix} A_{g-1} & A_{g-1} \\ A_{g-1} & \bar{A}_{g-1} \\ \underline{1} & \underline{0} \end{pmatrix} \begin{pmatrix} \\ \bar{X} \\ \\ \end{pmatrix} \leq \begin{pmatrix} rI_{g-1} + D_{g-1} \\ rI_{g-1} + D_{g-1} + I_{g-1} \\ r + 0 \end{pmatrix} \\ b) & \\ c) & \end{array}$$

Case a) The upper part of the set of inequalities. By the definition of $\{X_0, X_1, \ldots, X_{2^g-1}\}$ and the relationship between V_g and V_{g-1}, each of these inequalities counts the zeroes in the sum of the same set of points as in the case (g-1). For example, the first row of $A_{g-1}\bar{X} \leq rI_{g-1} + D_{g-1}$ counted the zeroes in Q_2, now the first row of $(A_{g-1} \quad A_{g-1})(\bar{X}) \leq rI_{g-1} + D_{g-1}$ still counts the xeroes in Q_2. Before

the X_0 counted all places in which Q_2 and the points Q_1, $Q_3,\ldots,Q_{g-1}$ had zeroes. Now X_0 counts all the places in which Q_2 and the points Q_1, $Q_3,\ldots,Q_{g-1}$, Q_g have zeroes and $X_{2^{g-1}}$ counts all the places in which Q_2 and the points Q_1, $Q_3,\ldots,Q_{g-1}$ have zeroes and Q_g has a one. So (former X_0) = (new X_0) + $X_{2^{g-1}}$. In general:
(former X_j) = (new X_j) + $X_{(j+2^{g-1})}$ for all $j = 0, 1,\ldots,(2^{g-1}-1)$.

Case c) The bottom inequality is $X_0 + X_1 + \ldots + X_{2^{g-1}} \leq r$. This corresponds to the bottom row of V_g which indicates where the zeroes of Q_g are. This inequality is that of Theorem II for Q_g.

Case b) The lower portion of the set of inequalities. Here each inequality counts the number of zeroes in the sum of (Q_g + (the sum of the same set of points as the case (g-1)). Adding one more point to a set increases the upper bound of Theorem II by one, since j is increased by one. For example, the first of these inequalities counts the zeroes in the sum of (Q_g+Q_2). The X_0 formerly counted places which had zeroes in Q_2 and Q_1, $Q_3,\ldots,Q_{g-1}$, now X_0 counts places having zeroes in Q_g as well. So the total for such places over points counted by X_0 is still zero. But ($X_{2^{g-1}+1}$) counts places with Q_1, $Q_2,\ldots,Q_{g-1}$ a zero and Q_g a one, so the toal for such places over points counted by ($X_{2^{g-1}+1}$) is now 1, and we do not want to count ($X_{(2^{g-1}+1)}$).

In general: X_0, $X_1,\ldots,X_{2^{g-1}}$ have a zero in Q_g, so a sum of zeroes over a set remains a zero if Q_g is added. For $X_{2^{g-1}+1},\ldots,X_{2^{g}-1}$ which have a 1 in Q_g, a sum of zero over a set becomes a one if Q_g is added, and a sum of one over a set becomes a zero if Q_g is added. So interchanging the ones and zeroes in A_{g-1} will take this into account and $A_g\bar{X} \leq r1_g + D_g$ is correct.

What about the composition of A_g? Clearly A_2 and A_3 meet the statement of the theorem. It is an easy use of induction to establish the general case. Assume true up to (g-1). Consider

$$A_g = \begin{pmatrix} A_{g-1} & A_{g-1} \\ A_{g-1} & \bar{A}_{g-1} \\ \underline{1} & \underline{0} \end{pmatrix}.$$

The first column is all ones, since A_{g-1} has first column all ones. The number of rows in A_g = 2(# rows in A_{g-1})+1 = $2(2^{g-1}-1)+1 = 2^g-1$. The number of ones in each row of A_g is:

case a) 2(# ones in each row of A_{g-1}) = $2(2^{g-2}) = 2^{g-1}$

case b) (# ones in row of A_{g-1}) + (# ones each row of $\bar{A}_{g-1}$)
$= 2^{g-2} + 2^{g-2} = 2^{g-1}$.

case c) (# columns in A_{g-1}) = 2^{g-1}.

The number of columns in A_g = 2(# columns in A_{g-1}) = $2(2^{g-1}) = 2^g$.

The number of zeroes in each row of A_g = (# columns of A_g) - (# ones in each row A_g)
$= 2^g - 2^{g-1} = 2^{g-1}$.

The number of zeroes in each column of A_g is:

case 1) (first 2^{g-1}): 2(# zeroes in column of A_{g-1}) = $2(2^{g-2}) = 2^{g-1}$

case 2) (second 2^{g-1}): (# zeroes in column of A_{g-1}) + (# zeroes in column of $\bar{A}_{g-1}$) + 1 = $2^{g-2} + (2^{g-2}-1) + 1 = 2^{g-1}$.

The number of ones in each column of A_g = (# rows of A_g) - (# zeroes in each column) = $(2^g-1) - 2^{g-1} = (2^{g-1}-1)$.

The theorem is true for g = 3; and if (it is true for g - 1, then it is true for g) is true; thus it is true for all $g \geq 4$.

This completes the proof of Theorem III as stated by Gulati and Kounias.

The author is responsible for Theorems IV, V, VI which culminate in the general solution giving all values of $m \equiv m_f(f+r,2)$ for which $m \leq 2f+r$, $f \geq 2$, $r \geq 0$. (It is clear that Gulati and Kounias had not obtained the general solution since their conditions on existence of Q_g, for $g = 4, 5$, are incorrect.)

THEOREM IV: Adding over all (2^g-1) inequalities of Theorem II gives

$$(2^g-1)X_0 + (2^{g-1}-1)\sum_{0}^{2^g-1} X_j \leq r(2^g-1) + (g-2)2^{g-1} + 1.$$

Proof: First column has all ones, the number of rows is 2^{g-1} giving the term $(2^g-1)X_0$. The other columns have $(2^{g-1}-1)$ ones giving the term of $(2^{g-1}-1)X_j$ for $j = 1, 2, \ldots, (2^g-1)$.

In the right hand side Theorem II gives a bound of $(r+j-1)$ for each of the $\binom{g}{j}$ different subsets of size j, $j = 1, 2, \ldots, g$. The sum is $\binom{g}{1}(r) + \binom{g}{2}(r+1) + \binom{g}{3}(r+2) + \ldots + \binom{g}{g}(r+g-1)$

$$= r[\binom{g}{1} + \binom{g}{2} + \ldots + \binom{g}{g}] + [\binom{g}{2} + 2\binom{g}{3} + 3\binom{g}{4} + \ldots + (g-1)\binom{g}{g}]$$

$$= r[(1+1)^g - \binom{g}{0}] + [(2\binom{g}{2} + 3\binom{g}{3} + \ldots + g\binom{g}{g}) - (\binom{g}{2} + \binom{g}{3} + \ldots + \binom{g}{g})]$$

$$= r[2^g-1] + g[\binom{g-1}{1} + \binom{g-1}{2} + \ldots + \binom{g-1}{g-1}] - [(1+1)^g - g - 1]$$

$$= r[2^g-1] + g(2^{g-1}-1) - (2^g-g-1)$$

$$= r[2^g-1] + (g-2)2^{g-1} + 1.$$

THEOREM V: Summing only over inequalities which contain X_j gives

$$(2^{g-2})X_0 + 2^{g-2}X_j + (2^{g-2}-1)\sum_{i=0}^{2^g-1} X_i \leq r[2^{g-1}-1) + (g-3)2^{g-2} + 1$$

for $j = 1, 2, 2^2, \ldots, 2^{g-1}$

$$\leq r(2^{g-1}-1) + (g-2)2^{g-2} + 1$$

otherwise. _

Proof: By construction of A_g, each column has $(2^{g-1}-1)$ ones giving the left hand side as shown. For the right hand side by induction, this has been found true for g = 2, 3. Assume true up to (g-1).

Case 1: For X_j, j = 0, 1,...,$(2^{g-1}-1)$, the new bound is

[2(former bound) + $(2^{g-2}-1)$ + r]

For j a power of 2: $= 2[r(2^{g-2}-1) + (g-4)2^{g-3} + 1] + 2^{g-2} + r$

$= r(2^{g-1}-1) + (g-4)2^{g-2} + 2 + 2^{g-2} - 1$

$= r(2^{g-1}-1) + (g-3)2^{g-2} + 1.$

For j not a power of 2: $= 2[r(2^{g-2}-1) + (g-3)2^{g-3} + 1] + (2^{g-2}-1) + r$

$= r(2^{g-1}-1) + (g-3)2^{g-2} + 2 + 2^{g-2} - 1$

$= r(2^{g-1}-1) + (g-2)2^{g-2} + 1.$

Case 2: For X_j, j = $(2^{g-1}+1),\ldots,g^2-1$; the new bound is

[former bound - (former total of Corollary I - former bound)

+ $2^{g-2} - 1 + r$]

$= r(2^{g-1}-1) + (g-3)2^{g-2} + 1 + (2^{g-2}-1)$

$= r(2^{g-1}-1) + (g-2)2^{g-2} + 1.$

Case 3: For X_j, j = 2^{g-1}, the new bound is the former total of Corollary I by construction of A_g

$= r(2^{g-1}-1) + (g-3)2^{g-2} + 1.$

This completes the proof.

At this point we see that our results now leave us with only Step 4 to complete. We do this in Theorem VI.

THEOREM VI: $m_f(f+r,2) = f+r+g$ for $(f_{g+1}(r)+1) \leq f \leq f_g(r)$ and $f \geq 2$, $r \geq 0$, $g \geq 1$ where $f_1(r) = \infty$, $f_2(r) = 2r+1$ and for $g \geq 3$,

$$f_g(r) = \begin{cases} (r+g-2) + \left[\dfrac{r+g-1}{2^{g-1}-1}\right] & \text{for } r \equiv (2^{g-2}-(g-1)),\ldots,(2^{g-1}-2) \mid \mathrm{mod}(2^{g-1}-1) \\ (r+g-3) + \left[\dfrac{r+g-1}{2^{g-1}-1}\right] & \text{for } r \equiv 0, 1,\ldots,(2^{g-2}-g) \mid \mathrm{mod}(2^{g-1}-1) \\ & \text{and for } r \equiv (2^{g-1}-(g-1)),\ldots,(2^{g-1}-2) \mid \mathrm{mod}(2^{g-1}-1). \end{cases}$$

(This is equivalent to "Q_g exists iff $f \leq f_g(r)$".)

Proof: This complete Step 4 of the GENERAL PROCEDURE by showing that the upper bounds of Theorems IV, V are consistent for

$$r \equiv (2^{g-2}-(g-1)),\ldots,(2^{g-1}-g) \mid \mathrm{mod}(2^{g-1}-1).$$

For r otherwise, the upper bound of Theorem IV must be reduced by unity.

From Theorem IV:

$$(2^{g-1}-1)\sum_{0}^{2^g-1} X_j \leq r(2^g-1) + (g-2)2^{g-1} + 1 - (2^g-1)X_0.$$

The maximum of $\Sigma X_j = (f+r)$ will clearly occur only when $X_0 = 0$.

With $X_0 = 0$, then $(f+r) = \Sigma X_j \leq 2r + (g-2) + \left[\dfrac{r+g-1}{2^{g-1}-1}\right]$.

For $r \equiv k \mod(2^{g-1}-1)$: $\sum_{0}^{2^g-1} X_j \leq (2^g-1)p + 2k + (g-2) + \left[\dfrac{k+g-1}{2^{g-1}-1}\right]$. (1)

Now $k \leq (2^{g-1}-(g+1))$ implies $(k+g-1) \leq (2^{g-1}-2)$, so $\left[\dfrac{k+g-1}{2^{g-1}-1}\right] = 0$.

And $k \geq (2^{g-1}-g)$ implies $(k+g-1) \geq (2^{g-1}-1)$, so $\left[\dfrac{k+g-1}{2^{g-1}-1}\right] = 1$.

Thus the upper bound on $\Sigma X_j = (f+r)$ increases by 2 for each unit increase in k except for $k = (2^{g-1}-(g+1))$ to $k = (2^{g-1}-g)$ for which an increase of 3 occurs.

Next, sum over the upper bounds of Theorem V incorporating the upper bound above to find the maximum possible value of ΣX_j.

From Theorem V:

$$2^{g-2}X_j \leq r(2^{g-1}-1) + (g-3)2^{g-2} + 1 - (2^{g-2}-1)(\Sigma X_j)$$

for $j = 1, 2, 2^2, \ldots, 2^{g-1}$.

For $r \equiv k \bmod(2^{g-1}-1)$; $2^{g-2}X_j \leq p\cdot 2^{g-2} + (k+g-1) - 2^{g-2} - (2^{g-2}-1)[\frac{k+g-1}{2^{g-1}-1}]$.

$$\text{So } X_j \leq (p-1) + \left[\frac{(k+g-1) - (2^{g-2}-1)[\frac{k+g-1}{2^{g-1}-1}]}{2^{g-2}}\right] \qquad (2)$$

Call this bound B, so $X_j \leq B$ for $j = 1, 2, 2^2, \ldots, 2^{g-1}$.

A similar approach yields $X_j \leq B + 1$ for j otherwise.

Since there are g values in the set $\{1, 2, 2^2, \ldots, 2^{g-1}\}$, there are $((2^g-1) - g)$ other values so the maximum value of X_j will be

$$gB + ((2^g-1) - g)(B+1) = (2^g-1)(B+1) - g.$$

Let us consider four cases:

(a) $k \leq (2^{g-2}-g)$ implies $(k+g-1) \leq (2^{g-2}-1)$, so $[\frac{k+g-1}{2^{g-1}-1}] = [\frac{k+g-1}{2^{g-2}}] = 0$.

So ΣX_j attains $((2^g-1)p - g)$ from (2).

(b) For $(2^{g-2}-(g-1)) \leq k \leq (2^{g-1}-(g+1))$, $[\frac{k+g-1}{2^{g-1}-1}] = 0$, $[\frac{k+g-1}{2^{g-2}}] = 1$.

So ΣX_j attains $((2^g-1)(p+1) - g)$ from (2).

(c) When $k = (2^{g-1}-g)$, then $[\frac{k+g-1}{2^{g-1}-1}] = 1$, $[\frac{k+g}{2^{g-2}}] = 1$.

So ΣX_j attains $((2^g-1)(p+1) - g)$ from (2).

(d) For $k \geq (2^{g-1}-(g-1))$, $[\frac{k+g-1}{2^{g-1}-1}] = 1$, $[\frac{k+g}{2^{g-2}}] = 2$.

So ΣX_j attains $((2^g-1)(p+1) - g)$ from (2).

A simple comparison shows that the bound of (1) is consistent with the results of cases (b) and (c). Thus for

$$r \equiv (2^{g-2}-(g-1)),\ldots,(2^{g-1}-g) \mid \mathrm{mod}\ (2^{g-1}-1),$$

the maximum value of

$$(f+r) = \Sigma X_j \text{ is } 2r + (g-2) + [\frac{r+g-1}{2^{g-1}-1}].$$

Equivalently, a point Q_g exists for $f \leq (r+g-2) + [\frac{r+g-1}{2^{g-1}-1}]$ for r in this range.

Similarly, the results of cases (a) and (b) show that the upper bound of (1) is not attainable. However, it is easily shown that reducing the upper bound of (1) by unity yields a maximum value for ΣX_j which is compatible with Theorem V.

$$\Sigma X_j \leq (2^g-1)p + (2k+g-3) + [\frac{k+g-1}{2^{g-1}-1}] \qquad (1)'$$

$$\text{for } r \equiv 0, 1,\ldots,(2^{g-2}-g),\ (2^{g-1}-(g-1)),\ldots,(2^{g-1}-2) \mid \mathrm{mod}(2^{g-1}-1).$$

Putting this reduced bound in Theorem V, we obtain

$$2^{g-2}X_j \leq r(2^{g-1}-1) + (g-3)2^{g-2} + 1 - (2^{g-2}-1)(\text{old } \Sigma X_i - 1)$$

$$\text{for } j = 1, 2, 2^2,\ldots,2^{g-1}.$$

For $r \equiv k\ (\mathrm{mod}(2^{g-1}-1)$; $2^{g-2}X_j \leq p\cdot 2^{g-2} + (k+g-2) - (2^{g-1}-1)[\frac{k+g-1}{2^{g-1}-1}]$

$$X_j \leq p + \left[\frac{(k+g-2) - (2^{g-2}-1)[\frac{k+g-1}{2^{g-1}-1}]}{2^{g-2}}\right]. \qquad (2)'$$

Call this bound B' so $X_j \leq B'$ for $j = 1, 2, 2^2,\ldots,2^{g-1}$. Similarly, we obtain $X_j \leq B' + 1$ for j otherwise.

Let us consider the two remaining cases:

(a) For $k \leq (2^{g-2}-g)$; ΣX_j attains $((2^g-1)(p+1) - g)$ from (2)'.

(d) For $k \geq (2^{g-1}-(g-1))$; ΣX_j attains $((2^g-1)(p+2) - g)$ from (2)'.

In each case the reduced bound of (1)' is attained. Thus for

$$r \equiv 0, 1, \ldots, (2^{g-2}-g), (2^{g-1}-(g-1)), \ldots, (2^{g-1}-2) \mid \mathrm{mod}(2^{g-1}-1)$$

the maximum value of

$$(f+r) = \Sigma X_j \text{ is } (2r+g-3) + \left[\frac{r+g-1}{2^{g-1}-1}\right].$$

Equivalently, a point Q_g exists for $f \leq (r+g-3) + \left[\frac{r+g-1}{2^{g-1}-1}\right]$ for r in this range.

This complete the proof of Theorem VI.

The entries in the table are exact values or lower bounds for $m_f(p,2)$, $p = f+r$, $f \geq 5$, $r \geq 0$. This partial table indicates how the results are attained sequentially. Conditions for $g = 2$ yield more than half of all results in the lower left of the table. Conditions for $g = 3$ yield the ray from top left to bottom right, and conditions for $g = 4$ give the six other values which are specified. The other $m_f(f+r,2)$'s, which are determined by Theorem VI, have f and r both increasing as g increases. The remaining $m_f(f+r,2)$'s receive the lower bound of $(2f+r)$ as indicated.

f \ p	f	f+1	f+2	f+3	f+4	f+5	f+6	f+7	f+8	f+9	f+10
5	6	7	9	≥13	≥14	≥15	≥16	≥17	≥18	≥19	≥20
6	7	8	9	11	≥16	≥17	≥18	≥19	≥20	≥21	≥22
7	8	9	10	12	≥18	≥19	≥20	≥21	≥22	≥23	≥24
8	9	10	11	12	14	15	≥22	≥23	≥24	≥25	≥26
9	10	11	12	13	15	16	18	≥25	≥26	≥27	≥28
10	11	12	13	14	15	17	18	20	≥28	≥29	≥30
11	12	13	14	15	16	18	19	21	≥30	≥31	≥32
12	13	14	15	16	17	18	20	21	22	≥33	≥34
13	14	15	16	17	18	19	21	22	23	25	≥36
14	15	16	17	18	19	20	21	23	24	25	27
15	16	17	18	19	20	21	22	24	25	26	28
16	17	18	19	20	21	22	23	24	26	27	28
17	18	19	20	21	22	23	24	25	27	28	29
18	19	20	21	22	23	24	25	26	27	29	30
19	20	21	22	23	24	25	26	27	28	30	31
20	21	22	23	24	25	26	27	28	29	30	32

CHAPTER VII. REFERENCES

1. GULATI, B. R. and KOUNIAS, E. G. (1969). On Two Level Symmetrical Factorial Designs and Error Correcting Codes, unpublished seven page resume delivered at a conference. (Authors now at Eastern Connecticut State College and McGill University, respectively.)

CHAPTER VIII. FURTHER RESULTS

Introduction: Rao (1946) defines a hypercube of strength f as follows: If there are r factors each at t levels, then there are t^r combinations, a subset of t^p is called an (r,t,p) array. If all combinations of any f factors occur an equal number (t^{r-f}) of times in such an (r,t,p) array, it is said to be a hypercube of strength f.

Rao (1946) showed also that hypercubes for a maximum number of factors, r, lead to (t^r,t^{r-p}) symmetrical, confounded factorial designs with the number of factors at the maximum value of $m_f(p,t)$. The hypercube is in fact used to generate the corresponding design. It is taken as the "keyblock", and the others are found by taking all linear combinations of elements in this block.

By construction of the appropriate hypercubes of strength four with the maximum number of factors, Rao (1947) showed that $m_4(4,2) = 5$, $m_4(5,2) = 6$, $m_4(6,2) = 8$ and $m_4(7,2) = 11$.

Bush (1952) proves, by construction, certain inequalities about the maximum number of factors which may be accommodated in certain hypercubes. These may be translated directly into results for $m_f(f,t)$.

I. $\underline{m_f(f,t)}$

$m_f(f,t)$ = the maximum number of points in PG(f-1,t) such that no subset of f lie in a subspace PG(f-2,t);

= the maximum number of columns in an f-rowed matrix such that no f are dependent;

= the maximum number of factors in a (t^r, t^{r-f}) confounded, symmetrical, factorial design such that no interaction of up to f factors is confounded.

THEOREM I.1: $m_f(f,t) = t + 1$ for all $t \leq f$, $f \geq 4$.

THEOREM I.2: $t + 1 \leq m_f(f,t) \leq f + t - 1$, t odd, $t > f$

$t + 1 \leq m_f(f,t) \leq f + t - 2$, t even, $t > f$.

Proof: (Bush, 1952). See appendix for partial table.

II. A General Inequality

THEOREM II.1: Let $m_f(p,t) \equiv m$

$$t^p - 1 \geq \binom{m}{1}(t-1) + \ldots + \binom{m}{u}(t-1)^u \text{ for } f = 2u, \text{ even}$$

$$t^p - 1 \geq \binom{m}{1}(t-1) + \ldots + \binom{m}{u}(t-1)^u + \binom{m-1}{u}(t-1)^{u+1} \text{ for}$$

$f = 2u + 1$, odd.

Proof: Rao (1947) obtained this for hypercubes of strength f.

Bose (1947) took the viewpoint of finding bounds for $m_f(p,t)$. This solution assumes m points in PG(p-1,t) so that no f lie in a subspace PG(f-2,t).

We show that any set of $n < u$ of the m points must generate a PG(n-1,t). Any set of n points can generate at most a PG(n-1,t); this happens if all (n) are linearly independent. If a subspace of dimension < (n-1) were generated then the addition of any other (2u-n) of the m points would give f in a subspace of dimension < ((n-1) + (2u-n-1)) = (2u-2), a contradiction.

Case 1: $f = 2u$, even

Each of the $\binom{m}{2}$ different pairs determines a line with (t+1) points in PG(p-1,t). There are (t-1) points on each line excluding the two points of m.

Each of the $\binom{m}{3}$ different sets of three determines a plane with (t^2+t+1) points in PG(p-1,t). In each plane there are $(\binom{3}{2}(t-1) + 3) = 3t$ points on lines determined by the three points of m, which leaves $(1+t+t^2) - 3t = (t-1)^2$ points in the plane not belonging to any of these lines.

Each of the $\binom{m}{4}$ different sets of four determines a PG(3,t) with $(1+t+t^2+t^3)$ points in PG(p-1,t). In each PG(3,t) there are $(\binom{4}{3}(t-1)^2 + \binom{4}{2}(t-1) + 4)$ points in planes determined by the four points of m, which leaves $(1+t+t^2+t^3) - (4t^2-2t+8) = (t-1)^3$ points in PG(3,t) not belonging to any of these planes.

Following the same reasoning one could show that each of the $\binom{m}{n}$ sets of $n \leq 2u$ determines a PG(n-1,t) with $(1+t+\ldots+t^{n-1})$ points in PG(p-1,t). In each PG(n-1,t) there are $N = [\binom{n}{n-1}(t-1)^{n-2}+\binom{n}{n-2}(t-1)^{n-3}+ \ldots+\binom{n}{1}]$ points in the PG(n-2,t)'s determined by the n points of m. We need to show that this leaves $(t-1)^{n-1}$ points in PG(n-1,t) not belonging to any of these PG(n-2,t)'s.

We use mathematical induction: This is true for n = 2, our induction hypothesis is that it is true up to n-1, that is, we assume that $(t-1)^{n-2} = ((1+t+\ldots+t^{n-2}) - [\binom{n-1}{n-2}(t-1)^{n-3} + \ldots + \binom{n-1}{1}])$. Consider $\binom{p}{q} = \binom{p-1}{q} + \binom{p-1}{q-1}$, then

$$N = (\binom{n-1}{n-1}(t-1)^{n-2} + \binom{n-1}{n-2}(t-1)^{n-2}) + (\binom{n-1}{n-2}(t-1)^{n-3} + \binom{n-1}{n-3}(t-1)^{n-3}) + \ldots + (\binom{n-1}{2}(t-1) + \binom{n-1}{1}(t-1)) + (\binom{n-1}{1} + \binom{n-1}{0})$$

Also, $t^{n-1} = ((t-1) + 1)^{n-1} = (t-1)^{n-1} + \binom{n-1}{n-2}(t-1)^{n-2} + \ldots + \binom{n-1}{1}(t-1) + 1$. Thus the difference $= (1+t+ \ldots + t^{n-1}) - N = (t-1)^{n-1}$.

Further, the $\binom{m}{n}$ sets of $(t-1)^{n-1}$ points are disjoint for $n \leq u$, otherwise there would be $2u$ points in a PG(2u-2,t), since each set of n generates a PG(n-1,t). For it two of these sets of $(t-1)^{n-1}$ intersects there must be (n+1) points of m in one of the PG(n-1,t)'s which leads to the contradiction above.

So the number of distinct points obtained by counting up to $n = u$ cannot be greater than the number of points in PG(p-1,t).

$$\binom{m}{1} + \binom{m}{2}(t-1) + \ldots + \binom{m}{u}(t-1)^{u-1} \leq (t^p - 1)/(t-1).$$

Case 2: $f = 2u + 1$, odd

As in Case 1, we can count the points for $n = 1, w, \ldots, u$. Now fix a single point in the set, choose any u from the remaining (m-1).

Each of the $\binom{m-1}{u}$ sets plus this chosen point determines a PG(u,t) having $(t-1)^u$ points not in any PG(u-1,t) determined by u of these points. This gives the inequality as in Case 1 as:

$$\binom{m}{1} + \binom{m}{2}(t-1) + \ldots + \binom{m}{u}(t-1)^{u-1} + \binom{m-1}{u}(t-1)^u \leq (t^p - 1)/(t-1),$$

concluding the proof.

Corollary II.1: Let $m \equiv m_4(p,t)$, $f = 4 = 2u$ implies $u = 2$.

$$t^p \geq 1 + \binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2$$

$$m^2 \frac{(t-1)^2}{2} - m\left(\frac{(t-1)^2}{2} - (t-1)\right) - (t^p - 1) \leq 0$$

$$m^2 - m\left(\frac{t-3}{t-1}\right) - 2\frac{(t^p-1)}{(t-1)^2} \leq 0$$

$$m \leq \frac{(t-3) + (8t^p+t^2-6t+1)^{1/2}}{2(t-1)} \qquad p \geq 4,\ t \geq 2$$

t \ p	5	6	7	8	9	....
2	7	10	15	22	31	....
3	11	19	33	56	99	....
4	15	30	60	120	241	....
5	20	44	99	221	494	....
6	25	61	150	366	898	....
7	30	81	230	610	1613	....
8	36	103	357	827	2340	....
9	43	129	386	1160	3479	....
⋮	⋮	⋮	⋮	⋮	⋮	

Corollary II.2: Let $m \equiv m_5(p,t)$, $f = 5 = 2u + 1$ implies $u = 2$

$$t^p \geq 1 + \binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \binom{m-1}{2}(t-1)^3$$

t \ p	6	7	8	9	10	11	....
2	8	11	16	23	32	45	....
3	12	21	48	82	142	⋮	
4	16	32	61	121	171		
5	21	45	100	222	494		
6	26	62	149	⋮	⋮		
7	31	80	210				
⋮	⋮	⋮	⋮				

Corollary II.3: Let $m \equiv m_6(p,t)$, $f = 6 = 2u$ implies $u = 3$

$$t^p \geq 1 + \binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \binom{m}{3}(t-1)^3$$

t \ p	7	8	9	10	....
2	9	11	14	18	....
3	12	17	24	34	....
⋮	⋮	⋮	⋮	⋮	

Corollary II.4: Let $m \equiv m_7(p,t)$, $f = 7 = 2u + 1$ implies $u = 3$

$$t^p \geq 1 + \binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \binom{m}{3}(t-1)^3 + \binom{m-1}{3}(t-1)^4$$

t \ p	8	9	10	....
2	10	12	15	....
3	13	18	26	....
⋮	⋮	⋮	⋮	

Corollary II.5: Let $m \equiv m_8(p,t)$, $f = 8 = 2u$ implies $u = 4$

$$t^p \geq 1 + \binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \binom{m}{3}(t-1)^3 + \binom{m}{4}(t-1)^4$$

t \ p	9	10	11	....
2	10	12	15	
3	12	18	22	
⋮	⋮	⋮	⋮	

Corollary II.6: $m_5(6,3) = 12$ (Bose, 1961)

Proof: By Theorem II.1, with $m \equiv m_5(6,3)$

$$3^6 - 1 \geq \binom{m}{1}2 + \binom{m}{2}2^2 + \binom{m-1}{2}2^3$$

$$728 \geq 2m + 2m(m-1) + 4(m-1)(m-2)$$

$$0 \geq 1\ (m-12)(m+10)$$

$$-10 \leq m \leq 12$$

so $m_5(6,3) \leq 12$

The six rowed matrix A below with elements over GF(3) has 12 columns, no five of which are linearly dependent.

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}$$

We conclude with an alternative proof of Theorem II.1 (Bose, 1961). This takes the viewpoint of choosing the maximum number of columns in a p-rowed matrix over GF(t) so that no f are linearly dependent.

Case 1: $f = 2u$, even.

There exists a matrix, A, with no 2u columns dependent. Choose any $n \leq u$ columns of A; there are $(t-1)^n$ linear combinations with non-zero coefficients. Since n columns can be chosen in $\binom{m}{n}$ ways there are $[\binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \ldots + \binom{m}{u}(t-1)^2]$ such linear combinations. These must all be different, otherwise 2u of the columns of A would be dependent, since the appropriate combination of the $\{n_1 \cup n_2\}$ columns involved would be zero, a contradiction. Since this sum cannot exceed the number of all possible columns we have

$$\binom{m}{1}(t-1) + \binom{m}{2}(t-1)^2 + \ldots + \binom{m}{u}(t-1)^u \leq t^p - 1.$$

Case 2: $f = 2u + 1$, odd.

There exists a matrix, A, such that no (2u+1) columns are linearly dependent. Let c be any particular column; for each of the $\binom{m-1}{u}$ choices of u points there are $(t-1)^{u+1}$ linear combinations with non-zero coefficients of the u chosen plus c. Other combinations are counted as in Case 1 giving:

$$\binom{m}{1}(t-1) + \ldots + \binom{m}{u}(t-1)^u + \binom{m-1}{u}(t-1)^{u+1} \leq t^p - 1.$$

CHAPTER VIII. REFERENCES

1. BOSE, R. C. (1947). Mathematical Theory of the Symmetrical Factorial Design, Sankhya, Vol. 8, Part 2, p.107-166.

2. BOSE, R. C. (1961). On Some Connections Between the Design of Experiments and Information Theory, Bulletin de L'Institut Internationa de Statistique, Vol. 38, p.257-271.

3. BUSH, K. A. (1952). Orthogonal Arrays of Index Unity, Annals of Mathematical Statistics (23), p.426-434.

4. RAO, C. R. (1946). Hypercubes of Strength "d" Leading to Confounded Designs in Factorial Experiments, Calcutta Mathematical Society Bulletin, Vol. 38, p.67-77.

5. RAO, C. R. (1947). Factorial Experiments Derivable from Combinatorial Arrangements of Arrays, Journal of the Royal Statistical Society, Supplement 9, p.128-139.

APPENDIX

TABLE 1

Partial table of values for $m_2(p,t)$.

t \ p	2	3	4	5	6	7	8	9	...
2	3	7	15	31	63	127	255	1023	...
3	4	13	40	121	364	1093	3280	9841	...
4	5	21	83	341	1365	5461	21,845	87,381	...
5	6	31	156	781	3906	19,531	97,856	488,281	...
6	7	43	259	1555	9331	55,987	335,923	2,015,539	...
7	8	57	400	2801	19,608	137,257	960,800	6,725,601	...
8	9	73	585	4641	37,449	299,593	2,396,745	19,173,961	...
9	10	91	820	7381	66,430	597,871	5,380,840	48,427,561	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

f = 2 is the only value for which all values of $m_f(p,t)$ are known.

$$m_2(p,t) = (t^p - 1)/(t - 1), \quad \forall p \geq 2,\ t \geq 2.$$

(See Chapter IV, Theorem II.1).

TABLE 2

Partial table of values for $m_3(p,t)$.

t \ p	3	4	5	6	7	8	...
2	4	8	16	32	64	128	...
3	4	10	20	37/76	91/211	181/659	...
4	6	17	33/63	97/250	273/995	529/3974	...
5	6	26	51/124	151/614	651/3064	1276/15,314	...
6	8	37	73/215	289/1289	1333/7725	2629/46,336	...
7	8	50	99/342	393/2286	2451/15,994	5685/116,850	...
8	10	65	129/511	641/4088	4161/32,685	8257/152,375	...
9	10	82	163/726	811/6522	6643/58,786	13,204/528,162	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

(See Chapter V).

First column, $m_3(3,t) = t + 1$, t odd (Theorem I.1)

$= t + 2$, t even

Second column, $m_3(4,t) = t^2 + 1$ (Theorem II.3)

First row, $m_3(p,2) = 2^{p-1}$ (Theorem III.1)

$m_3(5,3) = 20$ is given by Theorem IV.1.

Upper and lower bounds for all other cases appear in Sections V, VI.

TABLE 3

Partial table of values for $m_4(p,t)$

t \ p	4	5	6	7	8	9	...
2	5	6	8	11	17	≤ 29	...
3	5	11	≤ 19	≤ 33	≤ 56	≤ 99	...
4	5	≤ 12	≤ 30	60	120	241	...
5	6	≤ 20	44	99	221	494	...
6	7	≤ 25	61	150	366	898	...
7	8	≤ 30	81	230	610	1613	...
8	9	≤ 36	103	357	827	2340	...
9	10	≤ 43	129	386	1160	3479	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	

(See Chapter VI).

First column, Section 1; $m_4(4,t) = t + 1$, $t \geq t$, Theorem I.3

Second column, $m_4(5,3) = 11$. Theorem II.1, Section 2

First row, $m_4(p,2)$ in Section 3.

Second row, $m_4(p,3) \leq 3^{p-3} + 2$, Lemma IV.1

Upper bounds on all other values from Corollary II.1, Chapter VIII.

TABLE 4

Partial table of values for $m_5(p,t)$.

t \ p	5	6	7	8	9	10	....
2	6	7	9	13/16	14/23	15/32	....
3	6	12	/21	/48	/82	/142	....
4	6	/16	/32	/61	/121	/171	....
5	6	/21	/45	/100	/222	/494	....
6	6/9	/26	/62	/149	⋮	⋮	
7	6/10	/31	/80	/210			
⋮	⋮	⋮	⋮	⋮			

First row ($t = 2$, $p \geq 5$) - see Chapter VII.

First column ($p = 5$, $t \geq 2$) - see Chapter VIII, Section 1.

The value of $m_5(6.3) = 12$ given by Chapter VIII, Corollary II.6.

For upper bounds on all other values see Chapter VIII, Corollary II.2.

Only seven values have been completely determined.

TABLE 5

Partial table of values for $m_f(f+r,2)$: $f \geq 5$, $r \geq 0$.

f \ f+r	f	f+1	f+2	f+3	f+4	f+5	f+6	f+7	f+8	f+9	f+10
5	6	7	9	13/16	14/23	15/32	16/45	17/	18/	19/	20/
6	7	8	9	11	16/18	17/	18/	19/	20/	21/	22/
7	8	9	10	12	18/	19/	20/	21/	22/	23/	24/
8	9	10	11	12	14	15	22/	23/	24/	25/	26/
9	10	11	12	13	15	16	18	25/	26/	27/	28/
10	11	12	13	14	15	17	18	20	28/	29/	30/
11	12	13	14	15	16	18	19	21	30/	31/	32/
12	13	14	15	16	17	18	20	21	22	33/	34/
13	14	15	16	17	18	19	21	22	23	25	36/
14	15	16	17	18	19	20	21	23	24	25	27
15	16	17	18	19	20	21	22	24	25	26	28
16	17	18	19	20	21	22	23	24	26	27	28
17	18	19	20	21	22	23	24	25	27	28	29
18	19	20	21	22	23	24	25	26	27	29	30
19	20	21	22	23	24	25	26	27	28	30	31
20	21	22	23	24	25	26	27	28	29	30	32

For exact values and lower bounds for $m_f(f+r,2)$, $f \geq 5$, $r \geq 0$, see Chapter VII.

Upper bounds may be determined by using Theorem II.1, Chapter VIII.

TABLE 6

Partial table of values for $m_f(f,t)$: $f \geq 5$.

t \ f	5	6	7	8	9	10	11	12	13	14	15
2	6	7	8	9	10	11	12	13	14	15	16
3	6	7	8	9	10	11	12	13	14	15	16
4	6	7	8	9	10	11	12	13	14	15	16
5	6	7	8	9	10	11	12	13	14	15	16
6	6/9	7	8	9	10	11	12	13	14	15	16
7	6/10	7/12	8	9	10	11	12	13	14	15	16
8	6/11	7/13	8/13	9	10	11	12	13	14	15	16
9	6/12	7/14	8/14	9/16	10	11	12	13	14	15	16
10	6/13	7/15	8/15	9/17	10/17	11	12	13	14	15	16
11	6/14	7/16	8/16	9/18	10/18	11/20	12	13	14	15	16
12	6/15	7/17	8/17	9/19	10/19	11/21	12/21	13	14	15	16
13	6/16	7/18	8/18	9/20	10/20	11/22	12/22	13/24	14	15	16
14	6/17	7/19	8/19	9/21	10/21	11/23	12/23	13/25	14/25	15	16
15	6/18	7/20	8/20	9/22	10/22	11/24	12/24	13/26	14/26	15/28	16
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

These values are obtained from Theorems I.1, I.2 in Chapter VIII.

$m_f(f,t) = t + 1$, $\forall t \leq f$, $f \geq 4$

$t + 1 < m_f(f,t) \leq f + t - 1$, t odd, $t > f$

$t + 2 \leq m_f(f,t) \leq f + t - 2$, t even, $t > f$