t-Designs

Definitions

We will now consider a generalization of the concept of a BIBD, called a t-Design. Since t-designs are not as tied to statistical applications as BIBD's are, the terminology used is closer to mainstream mathematics.

A ***t-(v,k,λ) design*** is an ordered pair (S,B), where S is a set of cardinality v, and B is a family of k-subsets (called blocks) of S with the property that each t-subset of S is contained in precisely λ blocks of B. For nondegeneracy, we shall always assume that $0 < t < k < v$. Clearly, a BIBD is a 2-(v,k,λ) design. While not much is known about general t-designs much work has been done in certain special cases.

Definitions

For each triple satisfying 0< t < k < v there are many t designs that may be obtained trivially as follows. Let S be any v-set. Form $\mathscr{C}$, the set of all possible k-subsets of S. The result (S,$\mathscr{C}$) is a t-design that we call the ***full combinatorial design***. In this design λ equals the binomial coefficient

$$\binom{v-t}{k-t}$$

Let $\mathscr{B}$ be the family of k-subsets of S that includes each member of $\mathscr{C}$ exactly n times. (S,$\mathscr{B}$) is a t-(v,k,nλ) design. In fact, given any t-(v,k,λ) design we can obtain a t-(v,k,nλ) design by replicating each block n times.

Hadamard 3-designs

An example of a 3-(8,4,1) design on the set S = {1,2,...,8} is given by the blocks:
{1,2,5,6} {3,4,7,8} {1,3,5,7} {2,4,6,8} {1,4,5,8} {2,3,6,7} {1,2,3,4} {5,6,7,8} {1,2,7,8} {3,4,5,6} {1,3,6,8} {2,4,5,7} {1,4,6,7} {2,3,5,8}.

This is a particular example of an ***Hadamard 3-design***. Let H be an Hadamard matrix of order > 4 which is standardized. Identify the set S with the columns of H and form the blocks in the following way: For each row of H other than the first form a block consisting of all the columns containing a +1 in this row and also form a block consisting of all the columns which contain a -1. If H is order n, the design formed will be a 3-(n, ½n, ¼n - 1) design.

Smaller t's

Theorem; Every t-(v,k,λ) design is a (t-1)-(v,k,λ^*) design where $\lambda^* = \lambda(v - t + 1)/(k - t + 1)$

Proof: Let $D = (S,\mathcal{B})$ be a t-(v,k,λ) design. Let X be any (t-1)-subset of S, and ℓ_x the number of blocks of $\mathcal{B}$ that contain X. X is contained in v-t+1 t-subsets of S. Each of these t-subsets occurs in λ blocks of $\mathcal{B}$. Now count ordered pairs (z,B) with B a block containing X and z a point of B\X in two ways to obtain $(k-t+1)\ell_x = (v-t+1)\lambda$. Since ℓ_x does not depend on the particular (t-1)-subset chosen, the result follows with $\lambda^* = \ell_x$.

Thus, our example of a 3-(8,4,1) design is also a 2-(8,4,3) design.

Some Corollaries

Corollary: Let $\lambda_0 = b$ the number of blocks and $\lambda_1 = r$ the number of blocks containing a given element, and λ_i the number of blocks containing a given i-subset, $0 \le i \le t$. Then,

$$\lambda_i \binom{k-i}{t-i} = \lambda_t \binom{v-i}{t-i}.$$

Proof: This follows from repeated application of the Theorem.

Corollary: A t-design is also an s-design for $0 \le s \le t$.

And a few more

Corollary: If a t-(v,k,λ) design exists, then for $0 \le s \le t-1$,

$$\binom{k-s}{t-s} \text{ divides } \lambda_t \binom{v-s}{t-s}.$$

Corollary: The complement of a t-design is a t-design.

Proof: A straightforward application of the principle of inclusion-exclusion shows that the complementary design of a t-(v,k,λ) design is a t-(v,v-k, λ*) design, where

$$\lambda^* = \frac{\lambda_t \binom{v-k}{t}}{\binom{k}{t}}.$$

Lower t's

Theorem:The existence of a t-(v,k,λ) design implies the existence of a (t-i) - (v-i, k-i, λ) design, 0 < i < t.

Proof: Let C(x) be the set of blocks of D = (S,$\mathcal{B}$) that contain a given element x of S. Every (t-1)-subset of S\{x} occurs with x in exactly λ blocks of D, these blocks being those of C(x)). Thus, (S - {x},$\mathcal{B}'$), where $\mathcal{B}'$ is obtained from the blocks of C(x) by removing x, is the required design for i = 1. Repeated application establishes the required result.

A different reduction

Corollary: The existence of a t-(v,k,λ_t) design implies the existence of a (t-1)-$(v-1,k,\lambda^*)$ design, where $\lambda^* = \lambda_{t-1} - \lambda_t$.

Proof: Let $(X,\mathcal{B})$ be a t-(v,k,λ_t)-design and let z be an element of X. Let $\mathcal{B}'$ be the set of all the blocks of $\mathcal{B}$ which do not contain z. Consider any (t-1)-subset T of $X\backslash\{z\}$. This subset is contained in λ_{t-1} blocks of $\mathcal{B}$. Some of these blocks will also contain z. In fact, there are exactly λ_t blocks containing the t-set T U {z}, and so, λ^* will contain T and not z. $(X\backslash\{z\}, \mathcal{B}')$ is thus a (t-1)-$(v-1,k,\lambda^*)$-design.

An Existence Result

Theorem: For all positive integers t, k and v such that

$$t < k < v-t$$

there exists a non-trivial t-(v,k,λ) design for some λ.

Pf: Let X be a v-set and $N = \binom{v}{t}$.

Consider the N-dimensional vector space $\mathbb{Q}^N$ in which the coordinates are indexed by the t-subsets of X. For each k-subset $A \subseteq X$, define a vector s_A in $\mathbb{Q}^N$ in which the entry in the coordinate corresponding to a t-subset Y of X is 1 if $Y \subseteq A$ and 0 otherwise. Since t < k < v-t, there are more of these vectors than the dimension of the space they are in, so, there exists a linear dependence amongst them. In other words,

An Existence Result

Theorem: For all positive integers t, k and v such that

$$t < k < v-t$$

there exists a non-trivial t-(v,k,λ) design for some λ.

Pf: (cont) there exist rational numbers α_A such that

$$\sum_{A \subseteq X, |A|=k} \alpha_A s_A = (0, \cdots, 0) .$$

By multiplying by the gcd of the denominators, we can assume that the α_A's are all integers. Let M be the minimum α_A (M must be negative). Define $\mathcal{A}$ to be the collection of blocks where for every k-set A of X, A appears exactly α_A – M times in $\mathcal{A}$.

We can now show that (X,$\mathcal{A}$) is a t-(v,k,λ)-design.

An Existence Result

Theorem: For all positive integers t, k and v such that

$$t < k < v-t$$

there exists a non-trivial t-(v,k,λ) design for some λ.

Pf: (cont) First observe that

$$\sum_{A \subseteq X, |A|=k} s_A = \left(\binom{v-t}{k-t}, \ldots, \binom{v-t}{k-t} \right);$$

since the full combinatorial design is a

$$t-\left(v, k, \binom{v-t}{k-t} \right) \quad \text{design.}$$

Now we have,

$$\sum_{A \subseteq X, |A|=k} (\alpha_A - M) s_A = \left(-M \binom{v-t}{k-t}, \ldots, -M \binom{v-t}{k-t} \right).$$

An Existence Result

Theorem: For all positive integers t, k and v such that

$$t < k < v-t$$

there exists a non-trivial t-(v,k,λ) design for some λ.

Pf: (cont) This means that every t-set appears in the same number of blocks, namely

$$\lambda = -M\binom{v-t}{k-t}.$$

The design is not a full combinatorial design since we have $\alpha_A - M = 0$ for at least one A.

1-designs

1-designs are simple structures where the only requirement other than constant block size is that each point appears in the same number of blocks. Generalized Quadrangles are examples of 1-designs.

Theorem: There exists a1-(v,k,λ)-design if and only if
$v\lambda \equiv 0 \bmod k$.

Pf: If a 1-(v,k,λ)-design exists, then the number of blocks $b = v\lambda/k$ must be an integer. Now, suppose that $v\lambda \equiv 0 \bmod k$ and let $u = \gcd(k,\lambda)$. Then $\lambda = u\lambda'$ and $k = uk'$ with $(\lambda',k')=1$. Now $b = v\lambda/k = v\lambda'/k'$ so $v \equiv 0 \bmod k'$ and we can let $v = sk'$ and thus have $b = s\lambda'$.

1-designs

Theorem: There exists a1-(v,k,λ)-design if and only if $v\lambda \equiv 0 \bmod k$.

Pf: (cont.) Let X be a set of cardinality k' and define $Y = X \times \mathbb{Z}_s$. Then $|Y| = v$. Let $A_1, \ldots, A_{\lambda'}$ be λ' arbitrary u-subsets of $\mathbb{Z}_s$. For $1 \le i \le \lambda'$, define $B_i = X \times A_i$. Each B_i is a k-subset of Y. Now develop each B_i through $\mathbb{Z}_s$, obtaining a set of b blocks that contain every point of Y exactly λ times. This is a 1-(v,k,λ) design.

1-design example

Let $v = 15$, $k = 9$ and $\lambda = 6$. Then $b = 10$, $s = 5$, $k' = 3$ and $\lambda' = 2$. Let $X = \{x,y,z\}$ and $A_1 = \{0,1,2\}$ and $A_2 = \{1,2,4\}$, then

$B_1 = \{x_0, y_0, z_0, x_1, y_1, z_1, x_2, y_2, z_2\}$ and

$B_2 = \{x_1, y_1, z_1, x_2, y_2, z_2, x_4, y_4, z_4\}$.

Develop each block by changing the subscripts mod 5.

for instance, $B_1 \rightarrow \{x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3\}$,

and we will obtain 10 blocks of size 9 with each element appearing 6 times.

Some 3-designs

Theorem: A resolvable BIBD with v = 2k is a 3-design.

Pf: Suppose that $(X, \mathcal{A})$ is a resolvable $(2k,k,\lambda)$-BIBD. Let Π_i be the parallel classes for $1 \le i \le r$. Each Π_i consists of two blocks $A_i^{(1)}$ and $A_i^{(2)}$.

Let $\{x,y,z\} \subset X$ and define a, b, c, d as follows:

$a = |\{i: \{x,y,z\} \subseteq A_i^{(j)}$, where j = 1 or 2$\}|$

$b = |\{i: \{x,y\} \subseteq A_i^{(j)}$ and $z \notin A_i^{(j)}$, where j = 1,2$\}|$

$c = |\{i: \{x,z\} \subseteq A_i^{(j)}$ and $y \notin A_i^{(j)}$, where j = 1,2$\}|$

$d = |\{i: \{z,y\} \subseteq A_i^{(j)}$ and $x \notin A_i^{(j)}$, where j = 1,2$\}|$.

Since each parallel class falls into exactly of these cases,

$$a + b + c + d = r.$$

Consider a pair of elements from {x,y,z}, we have;

$$a + b = a + c = a + d = \lambda.$$

Some 3-designs

Theorem: A resolvable BIBD with v = 2k is a 3-design.

Pf:(cont) Solving for a from these equations gives

$$a = (3\lambda - r)/2.$$

The constancy of this value shows that $(X, \mathcal{A})$ is a

$$3 - (2k, k, (3\lambda - r)/2) \text{ -design.}$$

Corollary: If there exists a Hadamard matrix of order 4m, then there exists a 3-(4m,2m,m-1)-design.

Pf: If there exists a Hadamard matrix of order 4m then there exists a resolvable (4m,2m,m-1)-BIBD and we can then apply the previous theorem.

Some 3-designs

Theorem: For all even integers $v \geq 6$, there exists a 3-$(v,4,3)$-design.

Pf: Every $(v,2,1)$-BIBD with v even is resolvable [1-factorizations of complete graphs]. Let $(X,\mathcal{A})$ be one such. Suppose $v \geq 6$ and let Π_i be the parallel classes, $1 \leq i \leq v-1$. Define

$$\mathcal{B} = \{A_1 \cup A_2 \mid A_1, A_2 \text{ in } \Pi_i,\ A_1 \neq A_2,\ 1 \leq i \leq v-1\}.$$

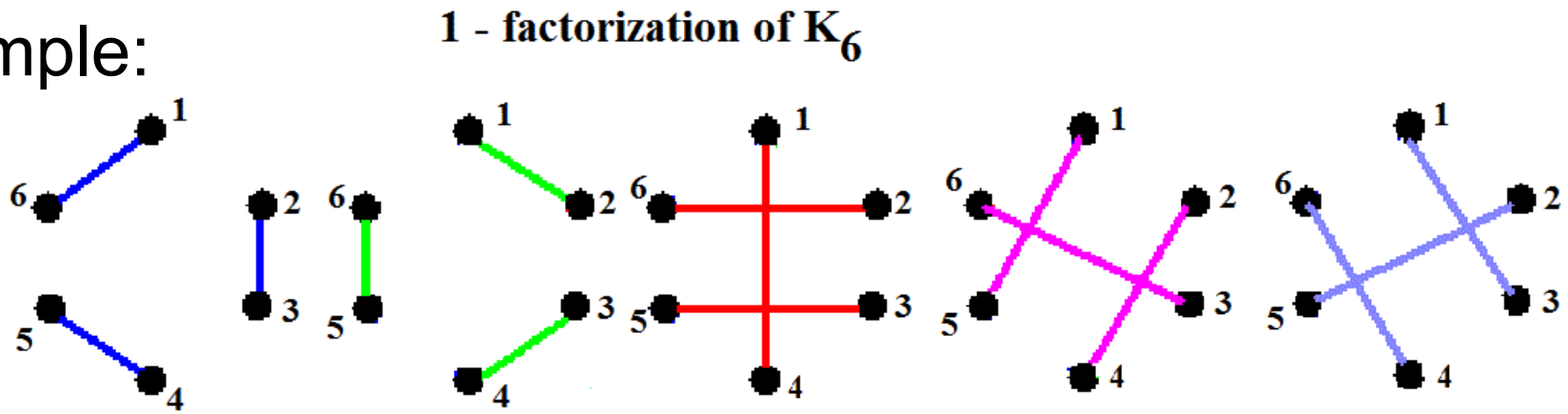
Consider 3 points x_1,x_2,x_3. Let $1 \leq i \leq 3$. There is a unique block A_i in $\mathcal{A}$ that contains the pair $\{x_1,x_2,x_3\}\backslash\{x_i\}$. The block A_i is in a unique parallel class (must be different for each i) and that parallel class contains a unique block A_i' containing x_i. Then $\{x_1,x_2,x_3\} \subseteq A_i \cup A_i'$ for $1 \leq i \leq 3$.

Some 3-designs

Theorem: For all even integers v ≥ 6, there exists a 3-(v,4,3)-design.

Pf: (cont). We have thus found 3 blocks that contain this triple, and no other block can contain them. Thus we have constructed a 3-(v,4,3)-design.

Example:



{1,6,2,3}	{1,2,3,4}	{1,4,2,6}	{1,5,2,4}	{1,3,2,5}
{1,6,4,5}	{1,2,5,6}	{1,4,3,5}	{1,5,3,6}	{1,3,4,6}
{2,3,4,5}	{3,4,5,6}	{2,6,3,5}	{2,4,3,6}	{2,5,4,6}

Steiner Systems

There are two definitions of Steiner Systems – the currently fashionable one is that a Steiner System is a t-design with $\lambda = 1$.

However, the classical definition is that a Steiner System is a $t-(v, t+1, 1)$-design. Thus we would only have

$1-(v,2,1)$ designs (a graph which is a 1-factor)

$2-(v,3,1)$ designs : Steiner Triple Systems

$3-(v,4,1)$ designs : Steiner Quadruple Systems

etc.

Steiner Quadruple Systems

The necessary condition for the existence of an SQS(v) [Steiner Quadruple System on v points] is $v \equiv 2, 4 \bmod 6$.

Theorem: If there exists an SQS(v), then there exists an SQS(2v).

Pf: Since an SQS(v) exists, $v \equiv 2,4 \bmod 6$ and so is even. Take two disjoint sets of size v, X and Y. Let $(X,\mathcal{A})$ and $(Y,\mathcal{B})$ be resolvable (v,2,1)-BIBDs with parallel classes Π_i and Ψ_i with $1 \le i \le v-1$ respectively. Also, let $(X,\mathcal{C})$ and $(Y,\mathcal{D})$ be SQS(v)'s. Define

$$\mathcal{E} = \{A \cup B \mid A \text{ in } \Pi_i,\ B \text{ in } \Psi_i,\ 1 \le i \le v-1\}.$$

We show that $(X \cup Y, \mathcal{C} \cup \mathcal{D} \cup \mathcal{E})$ is an SQS(2v).

Steiner Quadruple Systems

Theorem: If there exists an SQS(v), then there exists an SQS(2v).

Pf: (cont) Suppose that $\{z_1,z_2,z_3\} \subseteq X \cup Y$.

a) If $|\{z_1,z_2,z_3\} \cap X| = 3$ then $\{z_1,z_2,z_3\}$ is in a block of $\mathcal{C}$.

b) If $|\{z_1,z_2,z_3\} \cap Y| = 3$ then $\{z_1,z_2,z_3\}$ is in a block of $\mathcal{D}$.

c) If $|\{z_1,z_2,z_3\} \cap X| = 2$, suppose z_3 in Y. There is a unique parallel class Π_j with $\{z_1,z_2\} \in \Pi_j$. There is also a unique block of the form $\{z_3,z_4\}$ in Ψ_j. Thus, $\{z_1,z_2,z_3\} \subseteq \{z_1,z_2,z_3,z_4\}$ and can not be contained in $\mathcal{C}$ or $\mathcal{D}$.

d) If $|\{z_1,z_2,z_3\} \cap Y| = 2$ we can argue as in the last case. Thus we must have an SQS(2v).

SQS(8)

The smallest SQS(v) will have $v = 8$, but we can not construct it from the last result since there is no SQS(4).
However, the following construction will produce one.

Let V be the 3-dimensional vector space over GF(2). For every three distinct vectors in V, define a fourth vector to be the sum of the three (in other words, the sum of all 4 is the zero vector, 000.
This gives:

{000,001,010,011} {000,001,100,101} {000,001,110,111} {000,010,100,110}
{000,010,101,111} {000,011,100,111} {000,011,101,110} {100,101,110,111}
{010,011,110,111} {010,011,100,101} {001,011,101,111} {001,011,100,110}
{001,010,101,110} {001,010,100,111}

SQS's

Theorem: There exists an SQS(2^n) for all integers $n \geq 3$.

Pf: Repeatedly apply the last theorem starting with the SQS(8) we just constructed.

1-Point Extensions

I am unhappy with the text's treatment of inversive planes, so I shall do it my way!

Let **D** = (X, **B**) be a t-(v,k,λ) design and p a point. The ***derived design*** $\mathbf{D}_p$ has point set X - {p} and as block set all the blocks of **D** which contain p with p removed. It is a (t-1)- (v-1, k-1, λ) design. Note that derived designs with respect to different points may not be isomorphic. A design **E** is called an ***extension*** of **D** if **E** has a point p such that $\mathbf{E}_p$ is isomorphic to **D**; we call **D** ***extendable*** if it has an extension.

Divisibility Condition

An extension of a t-(v,k,λ) design is a (t+1)-$(v+1,k+1,\lambda)$ design, so we have:

Proposition. If a t-(v,k,λ) design has an extension, then k+1 divides b(v+1).

Pf. Take s = 0 and t = 1 for the extension in

$$\binom{k-s}{t-s} \text{ divides } \lambda_t \binom{v-s}{t-s}.$$

giving k + 1 divides $\lambda_1(v+1)$ for the (t+1)-design. But λ_1 = r for the larger design is just b for the smaller design.

Extendable Projective Planes

Proposition . The only extendable projective planes are those of orders 2 and 4.

Proof. By the previous proposition, if a symmetric 2-$(n^2+n+1, n+1, 1)$ has an extension then $n+2$ must divide $(n^2+n+1)(n^2+n+2) = n^4 + 2n^3 + 4n^2 + 3n + 2$. The division gives a remainder of $12/(n+2)$, and since this must be an integer we have that $n + 2$ divides 12, i.e., $n = 2,4$ or 10. The non-existence of a projective plane of order 10 establishes the result.

Comment: As we shall see, both of these planes are in fact extendable.

A Generalization

Theorem . (Cameron) If a symmetric 2-(v,k,λ) design **D** is extendable, then one of the following holds:

(a) **D** is a Hadamard 2-design;

(b) $v = (\lambda+2)(\lambda^2 + 4\lambda + 2)$, $k = \lambda^2 + 3\lambda + 1$;

(c) $v = 495$, $k=39$, $\lambda = 3$.

We will not prove this result but only mention that the only known example of (b) is the projective plane of order 4 and the parameter set of (c) has no known solutions.

Inversive Planes

A design with the parameters of the extension of an affine plane, i.e., a 3-($n^2 + 1$, n+1,1) design, is called an ***inversive plane***, or a ***Möbius plane*** of order n.

Example: It is possible to give a geometric description of some inversive planes. An ***ovoid*** in PG(3,q) is a set of $q^2 + 1$ points, no three collinear. It can be shown that every plane (which is a hyperplane since dim = 3) of PG(3,q) meets an ovoid $\mathcal{O}$ in either 1 or q + 1 points. The plane sections of size q + 1 of $\mathcal{O}$ are the blocks of an inversive plane of order q. Any inversive plane arising this way is called ***egglike***. All known inversive planes are egglike.

Ovoids

An example of an ovoid is the *elliptic quadric*, the set of zeros of the quadratic form

$$x_1x_2 + f(x_3, x_4),$$

where f is an irreducible quadratic form in two variables over GF(q). [$f(x,y) = x^2 + xy + y^2$ for example].

If q is an odd power of 2, another type of ovoid is known - the *Suzuki-Tits* ovoid.

Theorem. (a) If q is odd, then any ovoid is projectively equivalent to the elliptic quadric; so there is a unique egglike inversive plane of order q (but maybe non-egglike ones exist).
(b) if q is even, then any inversive plane is egglike (but there maybe some unknown ovoids).

Hyperovals

A ***k-arc*** in a projective plane is a set of k points no three of which are incident with the same line. Axiomatically, every plane contains a 4-arc. On the other extreme, the maximum number of points in a k-arc in a projective plane of order n is n+2.

Suppose P is a point of the k-arc, then there can be at most one other point of the k-arc on each of the lines through P, and every point of the plane is on one of these lines, so the maximum number of other points of the k-arc is n+1.

An (n+1)-arc is called an ***oval***. Although many examples of ovals exist, there are projective planes of order 16 which contain no ovals. An (n+2)-arc is called an ***hyperoval***.

Hyperovals

Let K be a k-arc in the projective plane π of order n. The lines of π fall into three classes with respect to K. Lines which intersect K in two points are called ***secant lines***, those that meet K in only one point are called ***tangent lines*** and those that have no point in common with K are called ***exterior lines***. We can easily count the numbers of these types of lines. There is a secant line for each pair of points of K, so there are k(k-1)/2 secant lines altogether, k-1 passing through each point of K. A point of K will therefore have n+1 – (k-1) = n - k + 2 tangent lines through it, and so the total number of tangent lines is k(n-k+2). All other lines of π are then exterior lines so there are $n^2 + n + 1 - k(k-1)/2 - k(n-k+2)$ of them.

n is even

Theorem: If n is odd, no hyperoval can exist in a projective plane of order n. If n is even, every oval in a projective plane of order n can be extended to a hyperoval in a unique way.

Proof: Suppose n is odd and K is an (n+2)-arc. There are n+2-1 = n + 1 secants passing through each point of K, i.e., every line through a point of K is a secant line. Consider a point P which is not in K. The lines through P either intersect K, in which case they must contain two points of K or else they are exterior lines. Since all the points of K are joined to P in pairs, n + 2 must be even which is impossible if n is odd.

n is even

Theorem: If n is odd, no hyperoval can exist in a projective plane of order n. If n is even, every oval in a projective plane of order n can be extended to a hyperoval in a unique way.

Proof (cont): Assume n is even and let K be an oval. Since k = n+1, there is exactly one tangent line through each point of K and n+1 tangents in all. Let A and B be points of K, and let X be any other point on the secant they determine. Since K contains n-1 points other than A and B, and n is even, there must exist at least one tangent line which passes through X. There are at least n+1 distinct tangent lines, one through each point on this secant line, but that is the total number of tangent lines, so through each point on a secant line there passes exactly one tangent line. Consider the intersection of two tangent lines; through this point no secant line can pass and since it is connected to each of the points of K, its n+1 lines must all be tangent lines. This point is not on any secant line, so it can be joined to K to produce an hyperoval.

A 5-Design

Theorem: For all integers $n \geq 3$, there exists a $5\text{-}(2^n+2,6,15)$-design.

Proof: Let $\mathcal{O}$ be a hyperoval in a projective plane π of order 2^n. For each point x not on $\mathcal{O}$, define

$$P(x) = \{\text{lines through } x \text{ which are secant to } \mathcal{O}\}.$$

Each P(x) contains $2^{n-1} + 1$ lines. Also, define Π_x to be the set of pairs of points on $\mathcal{O}$ which are determined by the secant lines of P(x). For each x, Π_x is a partition of $\mathcal{O}$ into $2^{n-1}+1$ 2-sets. Furthermore, given any two disjoint 2-sets of points of $\mathcal{O}$, there is a unique point z so that Π_z contains them both (z is the intersection of the two secants).

A 5-Design

Theorem: For all integers $n \geq 3$, there exists a $5\text{-}(2^n+2,6,15)$-design.

Proof: (cont): Define

$\mathcal{B}$ = { U all triples of distinct 2-sets contained in any Π_x}.

The blocks of $\mathcal{B}$ consist of 6 points of $\mathcal{O}$. Let $\{x_1,x_2,\ldots,x_5\}$ be a set of five distinct points of $\mathcal{O}$. There are 15 ways to pick two disjoint 2-sets from this set. WLOG say $\{x_1,x_2\}$ and $\{x_3,x_4\}$. There is a unique Π_z which contains this pair, and it also contains $\{x_5,x_6\}$. Thus, there are 15 blocks which will contain $\{x_1,x_2,\ldots,x_5\}$, showing that $(\mathcal{O},\mathcal{B})$ is a $5\text{-}(2^n+2,6,15)$-design.

The only thing that remains is to prove that there always exists an hyperoval in some plane of order 2^n.

Coordinates

The points of a projective plane $PG(2,q)$ are the 1-dimensional subspaces of a 3-dimensional vector space over $GF(q)$. Any non-zero vector in a 1-dimensional subspace can be used to represent the point (as all other vectors are just scalar multiples of the representative). These representatives are called homogeneous (or projective) coordinates. If (x,y,z) are homogeneous coordinates of a point, and $z \neq 0$, then we may take a representative in which $z = 1$.

The coordinates of the points on a line satisfies a linear equation, i.e., $ax + by + cz = 0$. If $b = 0$, the point $(0,1,0)$ satisfies the equation which now has the form $ax + cz = 0$. If the line is not $z = 0$, then $a \neq 0$ and $x = (c/a)z$. The points other than $(0,1,0)$ will have $z = 1$, so the line is $x = c/a$, a vertical line passing through $(0,1,0)$.

Equations in Characteristic 2

A quadratic equation $ax^2 + bx + c = 0$ defined over a field of characteristic 2 has at most two solutions, but we can not use the usual quadratic formula to find them since $2 = 0$.

We may assume $a \neq 0$ (otherwise this is not a quadratic) and substitute $x = (b/a)y$ in the equation to get:

$$a(b/a)^2y^2 + b(b/a)y + c = 0$$

$$b^2/a\, y^2 + b^2/a\, y + c = 0$$

If $b \neq 0$ we may rewrite this as:

$$y^2 + y + (ac)/b^2 = 0.$$

A solution of this equation gives a solution of the original. Note that $(y+1)^2 + (y+1) = y^2 + 1 + y + 1 = y^2 + y$, so if y is a solution then so is $y+1$. Thus, if $b \neq 0$, there are either 2 or 0 solutions to the quadratic equation.

Existence

Theorem: The projective plane PG(2,2^n) contains an hyperoval.

Pf: In terms of homogeneous coordinates, we shall show that the point set,

$$\Omega = \{(x,y,z) \mid y^2 + xz = 0\} \cup \{(0,1,0)\},$$

is a hyperoval in PG(2,2^n) [this is an hyperconic].

We need to show that Ω consists of 2^n+2 points, no three of which are collinear. Consider the points of Ω which lie on the line $z = 0$. There are only two such points, (0,1,0) and (1,0,0). All other points of Ω have coordinates of the form (x,y,1) where $x = y^2$. That is, points of the form (y^2,y,1) as y runs through GF(2^n). So Ω has in total $2^n + 2$ points.

Existence

Theorem: The projective plane PG(2,2^n) contains an hyperoval.

Pf: (cont) We have seen that the line z = 0 contains 2 points, so we can restrict ourselves to points with z = 1 and the affine equations of lines. Lines not through the point (0,1,0) have (affine) equations of the form y = mx+k. So points of Ω on these lines have coordinates that satisfy $(mx+k)^2 + x = 0 \rightarrow m^2x^2 + x + k^2 = 0$, which if $m \neq 0$ has either 0 or 2 solutions. If m = 0 then there is only one solution, but the line passes through (1,0,0) so these lines meet Ω in 2 points. The only other lines of the plane are the vertical lines through (0,1,0) which have equations of the form x = k, meeting Ω in points (k,y,1) where $y^2 = k$. Since squaring is an automorphism, it is a bijection and there is a unique solution for y for every k.