Block Designs

April 20, 21

The study of the incidence structures between finite sets is one of the most important topics in Combinatorial Theory. There are three basic directions : (1) Finite Geometry, (2) Block Design, and (3) Hypergraph. It is not easy to describe the difference between them. In general, "Finite Geometry" cares more about the property related to the geometry on a plane, "Block Design" emphsizes on numberical relationship and "Hypergraph" focuses on arbitraily given edges (finitesubsets).

Therefore, to study Block Design, we start with the construction of designs of small order. We also find the necessary conditions for the existence of the kind of designs we would like to obtain. Following that, we then put forth to prove the necessary conditions are also sufficient by constructing all such designs. In general, the part on necessary conditions is comparatively easier. As to construction part, some of the design does not exist even we know the necessary conditions. We shall see that in next section.

1. Notations and preliminaries

- $(X, \mathbb{B})$ is a design if X is a non-empty set and $\mathbb{B}$ is a collection of subsets of X. If all the subsets are of the same cardinality, then $(X, \mathbb{B})$ is called a block design. For convenienc all the sets in $\mathbb{B}$ are referred as a block in X.
- If all the subsets of a design $(X, \mathbb{B})$ are all distinct, then it is a simple design. Note that $\mathbb{B}$ can be a multi-set in a design, the blocks with repeated occurrence is known as repeated blocks.
- Let $X = \{x_1, x_2, \cdots, x_v\}$ be the set of "varieties" and $\mathbb{B} = \{B_1, B_2, \cdots, B_b\}$ be the set of blocks. Then, we can define a Variety-Block incidence matrix to represent the design, say $\underline{A}$ and also a bipartite graph to represent $(X, \mathbb{B})$, say $G_{X,\mathbb{B}}$.

(☆)

- $A = [a_{i,j}]_{v \times b}$ where $a_{i,j} = \begin{cases} 1, & \text{if } x_i \in B_j, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$

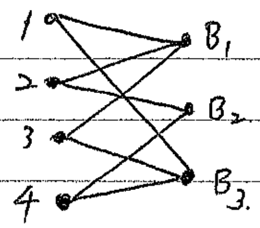
  Therefore, A is a $(0,1)$-matrix.

- $G_{\mathbb{X},\mathbb{B}} = (\mathbb{X}, \mathbb{B})$ is a bipartite graph such that $x_i \sim B_j$ if $x_i \in B_j$.

Example. $\mathbb{X} = \{1,2,3,4\}$, $\mathbb{B} = \{\overset{B_1}{\{1,2,3\}}, \overset{B_2}{\{2,4\}}, \overset{B_3}{\{1,3,4\}}\}$.

$$A: \begin{array}{c|ccc|} & B_1 & B_2 & B_3 \\ \hline 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 3 & 1 & 0 & 1 \\ 4 & 0 & 1 & 1 \\ \hline \end{array}_{4 \times 3}$$

$G_{\mathbb{X},\mathbb{B}}$:



Note: The relation of A and $G_{\mathbb{X},\mathbb{B}}$ is easy to see. In coding theory the elements in $\mathbb{B}$ can be referred as the set of codewords. In graph theory, they are "hyperedges".

- From the sense of Geometry, the incidence relation $x_i \in B_j$ can be "reversed". We can say "a point x_i is on a line B_j" or "a line B_j is passing x_i". Hence, we have the following

- $(\mathbb{B}, \mathbb{X})$ is a dual design of $(\mathbb{X}, \mathbb{B})$. The incidence matrix of $(\mathbb{B}, \mathbb{X})$ is A^T where A is the incidence matrix of $(\mathbb{X}, \mathbb{B})$.

- In an $(X,\mathbb{B})$, we let $r(x)$ or r_x denote the replication number of a variety x, i.e., the number of blocks containing x. We use K to denote $\{|B| \mid B \in \mathbb{B}\}$. If $K=\{k\}$, then we simply use k to denote K.

- (Definitions)

  A t-(v,k,λ) design is an $(X,\mathbb{B})$ such that $|X|=v$, $K=\{k\}$ and any t-subset of $\binom{X}{t}$ occurs together in exactly λ blocks of $\mathbb{B}$. In case that $\lambda=1$, then $(X,\mathbb{B})$ is also known as a Steiner t-design, denoted by $S(t,v,k)$.

- If $k<v$, a 2-(v,k,λ) design is called a balanced incomplete block design, BIBD in short. Notice that the term "balanced" comes from the fact that in a 2-(v,k,λ) design, for each $x \in X$, $r = r_x = \dfrac{\lambda(v-1)}{k-1}$ which is a constant. Another important fact is $bk = v \cdot r$.

- (Only two varieties are concerned!)

- An $(X, \mathbb{B})$ is called a pairwise balanced design (PBD in short), if any pair of elements in $\binom{X}{2}$, they occur together in exactly λ blocks of $\mathbb{B}$. Notice that in a PBD, the blocks are not necessarily be of the same size. So, it is denoted by $2-(v, K, \lambda)$ design where $|X| = v$.

Example, a $2-(6, \{2,5\}, 1)$ design.

$$X = \mathbb{Z}_6 \text{ and } \mathbb{B} = \{\{0,1\}, \{0,2\}, \{0,3\}, \{0,4\}, \{0,5\}, \{1,2,3,4,5\}\}.$$

- The following notions are not related to vector spaces. (与向量空间无关)

  An $(X, \mathbb{B})$ is called a partial linear space, if any two blocks of $\mathbb{B}$ contain at most one common element. If, indeed, any two elements (varieties) of a partial linear space occur together in a block of $\mathbb{B}$, then $(X, \mathbb{B})$ is a linear space with index 1.

- You may use "Geometry" to refer the above definitions:

  Partial L.S. : Any two lines intersect at most one point.

  L.S. : Any two points lie on a line (some line).

Special Designs

<u>Definition</u> (Projective plane and Affine plane) $B^{(1)}_{n^2+n+1,\,n+1}$

A Steiner 2-design $S(2, n+1, n^2+n+1) =_{def} PG(2,n)$ is called a projective plane of order n. A Steiner 2-design $S(2, n, n^2)$ is an affine plane of order n, denoted by $AG(2,n)$.

- (*) The existence of a $PG(2,n)$ is "equivalent" to the existence of an $AG(2,n)$.
- A $PG(2,n)$ does exist for each n when n is a prime power.
- No other kind of $PG(2,n)$ has been founded.
- A $PG(2,n)$ does not exist for $n = 1, 2, 6, 10$ and possibly others $\cdots$.
- We can extend $AG(2,n)$ and $PG(2,n)$ to $AG(d,n)$ and $PG(d,n)$ for $d \geq 3$ respectively. But, the constructions are getting harder.

<u>The proof of (*)</u>. More details will be given later.

$$PG(2,n) \xrightarrow[\text{Deleting a block (any)}]{} AG(2,n)$$

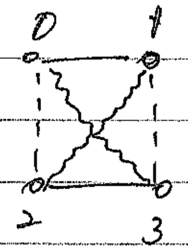
$AG(2,n) \Longrightarrow PG(2,n)$

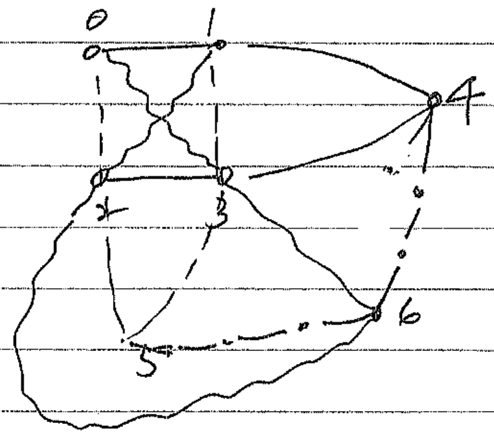
Adding a line at infinity

Examples

$n=2$, $AG(2,2)$: $X=\mathbb{Z}_4$, $\mathcal{B}=\{\underline{\{0,1\},\{2,3\}},\underline{\{1,2\},\{0,3\}},\underline{\{1,3\},\{0,2\}}\}$

parallel classes





$n=2$, $PG(2,2)$, $X=\mathbb{Z}_7$, $\mathcal{B}=\{\{0,1,4\},\{2,3,4\},\{0,2,5\},\{1,3,5\},\{0,3,6\},$
$\{1,2,6\},\{4,5,6\}\}$.

- A $PG(2,n)$ is a symmetric design, i.e., $|X|=|\mathcal{B}|$.
- An $AG(2,n)$ contains parallel classes each has n blocks.

  In fact, there are $n+1$ parallel classes.
- A parallel class of a design is a collection of blocks $B_1, B_2, \cdots, B_t$ such that $\bigcup_{i=1}^{t} B_i = X$.

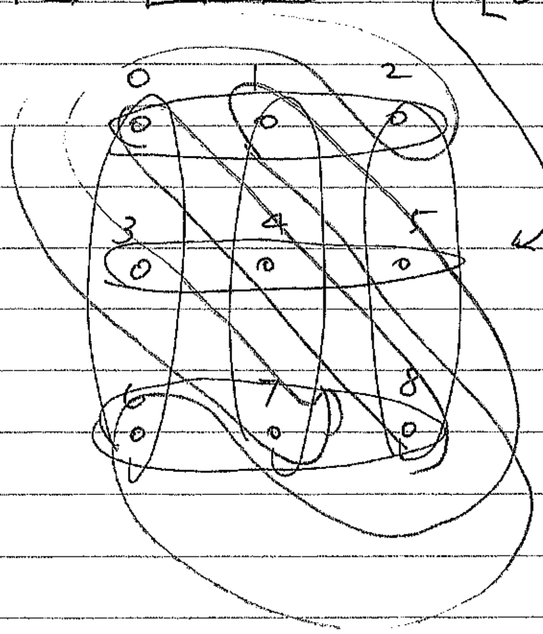
<u>Exercise 2-8.</u> (3 points) Construct a $2-(22, K, 1)$ design where $K = \{4, 7\}$.

<u>Exercise 2-9.</u> (3 points) Prove that for any prime power n, a $PG(2, n)$ (and $AG(2,n)$) exists.

<u>Hint.</u> Use the orthogonal array obtained by a complete family of orthogonal Latin squares of order n, i.e, $n-1$ mutually orthogonal Latin squares.

<u>Example.</u>

$$\begin{array}{|c|c|c|}\hline 0&1&2\\\hline 1&2&0\\\hline 2&0&1\\\hline\end{array} \perp \begin{array}{|c|c|c|}\hline 0&1&2\\\hline 2&0&1\\\hline 1&2&0\\\hline\end{array} \Rightarrow \begin{bmatrix} 0\,0\,0 & 1\,1\,1 & 2\,2\,2 \\ 0\,1\,2 & 0\,1\,2 & 0\,1\,2 \\ 0\,1\,2 & 1\,2\,0 & 2\,0\,1 \\ 0\,1\,2 & 2\,0\,1 & 1\,2\,0 \end{bmatrix}$$



...

$\therefore$ n: prime power. $\therefore$ $PG(2,n) \Leftrightarrow AG(2,n) \Leftrightarrow$ Complete family MDLS(n)

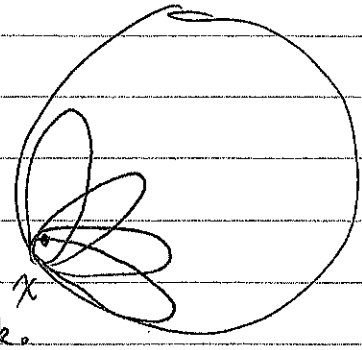
Basic properties of a design

1. If $(X, \mathbb{B})$ is a $2-(v,k,\lambda)$ design, then we have

   (a) for each $x \in X$, $r_x = r = \frac{\lambda(v-1)}{k-1}$ or $r\cdot(k-1) = \lambda(v-1)$.

   (b) $b = |\mathbb{B}| = \frac{\lambda v(v-1)}{k(k-1)}$ or $b \cdot k = r \cdot v$.

<u>Proof.</u> Since x occurs with (each of) all the other $v-1$ element exactly in λ blocks, r_x is equal to $\lambda(v-1)$ possible such pairs divided by the $k-1$ pairs which can be obtained from a block.



(The second equality is a consequence of the above idea by using two-way counting.) This concludes the proof of (a).

As to (b), it is a direct counting of the number of pairs occur in $\mathbb{B}$ via the number of pairs occur in a block. Therefore $|\mathbb{B}| = \lambda\binom{v}{2} / \binom{k}{2}$. The second identity comes from the occurrence of elements (total). ∎

2. If $(X, \mathbb{B})$ is a $2-(v,k,\lambda)$ design, then $|X| \leq |\mathbb{B}|$. (Fisher's inequality.)

Proof. Let A be the incidence matrix of $(X, \mathcal{B})$. Then

$AA^T = (r-\lambda)I + \lambda J$, i.e., AA^T is a $v \times v$ matrix such that each entry in the diagonal is r and each entry outside diagonal is λ.

$$AA^T : \begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ x_v \end{array} \overset{\;B_1 \, B_2 \, \cdots \, B_b}{\begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}}_{v \times b} \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}_{b \times v}$$

Note: $AA^T(i,j)$ is the inner product of the ith row and the jth row

So, if $i = j$, it is the occurrence of $\underset{(r_{x_i} = r)}{x_i}$ in the blocks of $\mathcal{B}$ and

if $i \neq j$, it is the the number of blocks in which x_i and x_j occur together in the blocks, λ.

Now, we can find $\underset{\text{(Gaussian elimination)}}{\underline{\det(AA^T) = kr(r-\lambda)^{v-1}}}$. Since $v > k$, $\lambda < r$. This concludes that AA^T is non-singular, i.e., $\text{rank}(AA^T) = v$

Furthermore, $\text{rank}(AA^T) \leq \text{rank}(A) \leq \min\{v, b\}$, hence $b \geq v$. ■

In fact, we have a stronger property on designs.

3. If $(X, \mathcal{B})$ is a linear space, then $|X| \leq |\mathcal{B}|$.

To find $\det(AA^T)$, we may also use the eigenvalues of AA^T. Since $AA^T = (r-\lambda)I + \lambda J$, a eigenvalue μ satisfies $(AA^T)\vec{x} = \mu\vec{x} = (r-\lambda)\vec{x} + \lambda J\vec{x} = (r-\lambda)\vec{x} + \lambda\mu'\vec{x}$

where μ' is an eigenvalue of J. By the fact that J is of rank 1, the set of eigenvalues of J are $\{v, \underbrace{0, 0, \cdots, 0}_{v-1}\}$.

Hence $\mu\vec{x} = ((r-\lambda)+\lambda\mu')\vec{x}$. This implies that

$\mu = r-\lambda$ ($v-1$ of them) and $\mu = r-\lambda+\lambda v = r+\lambda(v-1) =$

$r+(k-1)r = kr$. Thus, $\det(AA^T) = kr\cdot(r-\lambda)^{v-1}$.

Note here that using the spectrum of an adjacency matrix of a graph is one of the main subjects of <u>Algebraic Graph Theory</u>.

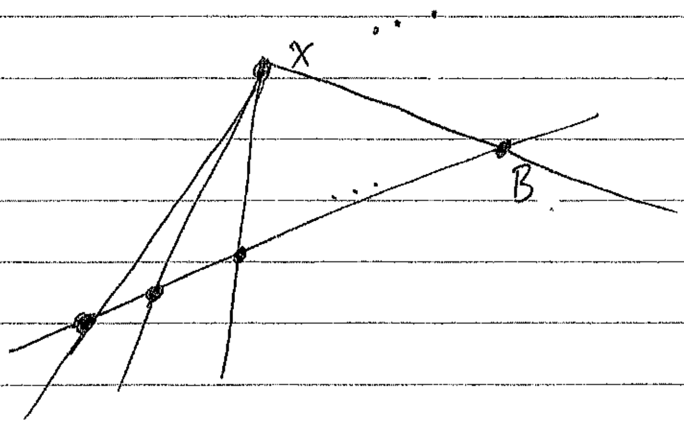
Proof. Again, let $X = \{x_1, x_2, \cdots, x_v\}$ and $\mathbb{B} = \{B_1, B_2, \cdots, B_b\}$. Since $(X, \mathbb{B})$ is a linear space, any two elements in X occur together in a block of $\mathbb{B}$. Assume that $b \le v$.

Here is an important observation: If $x \notin B_i$, then $r_x \ge |B_i|$ since each element of B_i is going to occur together with x in some other blocks in $\mathbb{B}$. Now, we are ready for the following statements.

$$1 = \sum_{B \in \mathbb{B}} 1/b = \sum_{B \in \mathbb{B}} \left(\sum_{x \notin B} \frac{1}{b(v - |B|)} \right) \quad \text{——— (a)}$$

$$\cancel{1} = \sum_{x \in X} 1/v = \sum_{x \in X} \left(\sum_{B \not\ni x} \frac{1}{v(b - r_x)} \right) \quad \text{——— (b)}$$

$v \cdot r_x \ge b \cdot |B|$ for each $x \notin B$. $(v \ge b)$ — (c)



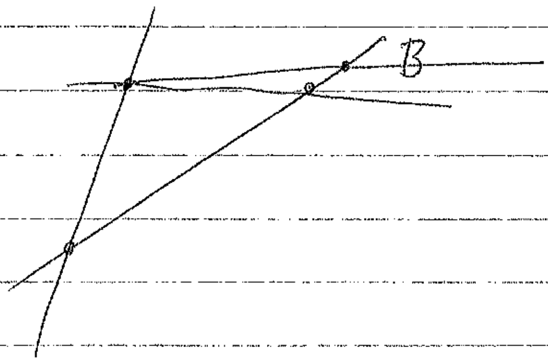
By (a), (b) and (c), $\displaystyle \underbrace{\sum_{B \in \mathbb{B}} \left(\sum_{x \notin B} \frac{1}{b(v - |B|)} \right)}_{= \frac{1}{b}} \le \underbrace{\sum_{x \in X} \left(\sum_{B \not\ni x} \frac{1}{v(b - r_x)} \right)}_{= \frac{1}{v}} \Rightarrow b \ge v.$ ∎

Hence, $b = v$.

More details

$\forall\ x \in X,\ x \notin B \in \mathcal{B},\ r_x \geq |B|$. (x 要和 B 中的点落在某條直線上)

①



$$\frac{1}{b} = \frac{1}{b} \sum_{x \notin B} \frac{1}{v-|B|}$$ (這樣的 x 有 $v-|B|$ 点)

$$= \sum_{x \notin B} \frac{1}{b(v-|B|)}$$

$$\frac{1}{v} = \frac{1}{v} \cdot \sum_{B \not\ni x} \frac{1}{\underbrace{b-r_x}_{\text{(不含x的線數)}}} = \sum_{x \notin B} \frac{1}{v(b-r_x)}$$

Since $v \geq b$, $v \cdot r_x \geq b \cdot |B|$. (From ①)

$$\frac{1}{v} = \sum_{x \notin B} \frac{1}{v(b-r_x)} \geq \sum_{x \notin B} \frac{1}{vb-b|B|} = \sum_{x \notin B} \frac{1}{b(v-|B|)} = \frac{1}{b}$$

$$\frac{1}{vb-大} \geq \frac{1}{vb-小}$$

$\therefore\ b \geq v$,

Hence, $b = v$ provided $v \geq b$. This implies that $b \geq v$ in general.

(*) The equality $v=b$ also shows that $r_x = |B|$ for each $x \in X$ and $B \in \mathbb{B}$. The implication of this fact is that any two blocks intersect at exactly one element, i.e., $|B_i \cap B_j| = 1$, $1 \le i \ne j \le b$.

(**) $(X, \mathbb{B})$ is a projective plane if $|X| = |\mathbb{B}|$ and $(X, \mathbb{B})$ is a linear space.

- A BIBD is a square BIBD, denoted by SBIBD if $v=b$.

The following Theorem is well-known, we state it and omitt the proof here. (It is a "necessary condition" for the existence of an SBIBD

Theorem (Bruck-Ryser-Chowla, 1949-1950)

If a $2-(v,k,\lambda)$ design is a square BIBD, then

(1) $k-\lambda$ is a square of an integer when v is even; and

(2) $z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda y^2$ has a nonzero integral solution when v is odd.

Note that (1) is easy to see, but the proof of (2) is quite complicate, we omit it.

(?)

$\det(AA^T) = (\det A)^2$

$= kr(r-\lambda)^{v-1} = k^2 (k-\lambda)^{v-1}$

$(r = k \Leftarrow v=b)$