Chapter 10

Combinatorial Designs

A ***combinatorial design*** (or alternatively, an ***incidence structure***) consists of a domain set X and another set B, commonly represented as subsets of that domain, analogous to the way in which the edges of a simple graph can be represented as pairs of vertices. This final chapter studies several kinds of combinatorial designs, each with additional axioms and/or mathematical structure on the domain and/or on the subsets.

10.1 LATIN SQUARES

A *Latin square* is a type of combinatorial design most easily described as an $n \times n$ array.

DEF: A ***Latin square*** on a set X of n objects is an $n \times n$ array such that each object in X occurs once in each row and once in each column.

Example 10.1.1: A Latin square on four graphic patterns is shown in Figure 10.1.1.

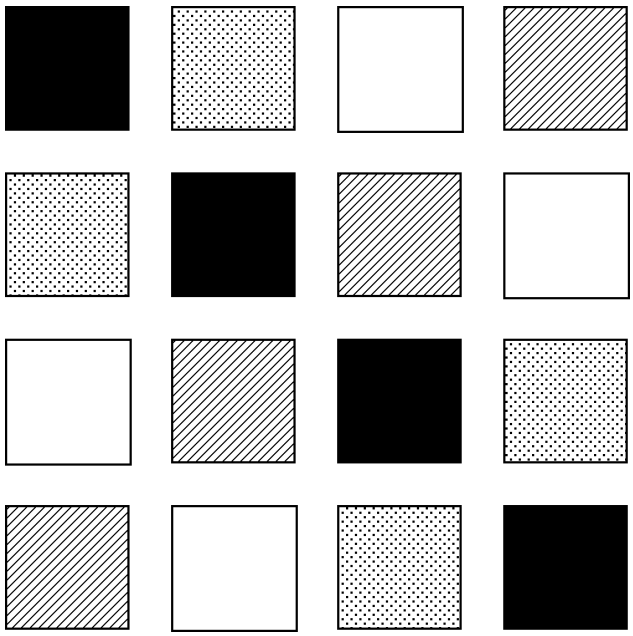

Fig 10.1.1 A 4×4 Latin square.

The standard symbols for an $n \times n$ Latin square are the integers modulo n. The rows and columns of a Latin square on $\mathbb{Z}_n$ are commonly indexed in $\mathbb{Z}_n$, so that there is a row

0 and a column 0. In particular, the following 4×4 Latin square on $\mathbb{Z}_4$ is obtainable from the Latin square of Figure 10.1.1 by a bijection of the symbol sets.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \tag{10.1.1}$$

Remark: A sudoku is a form of 9×9 Latin square on the numbers 1 to 9, with an additional requirement that each number occur exactly once in certain 3×3 sub-arrays.

It is easy enough to construct a Latin square of any given size.

Proposition 10.1.1. *For every positive integer n, there exists an $n \times n$ Latin square with $\mathbb{Z}_n$ as the set of objects.*

Proof: Let $L[i, j] = i + j$ modulo n. Thus,

$$L = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-2 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \\ 2 & 3 & 4 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ n-2 & n-1 & 0 & \cdots & n-4 & n-3 \\ n-1 & 0 & 1 & \cdots & n-3 & n-2 \end{pmatrix}$$

Clearly the array L is a Latin square. ♢

Example 10.1.2: For $n = 4$, the construction of Proposition 10.1.1 yields the following Latin square.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \tag{10.1.2}$$

A *Latin square* can be recognized as a type of combinatorial design $\langle X, B \rangle$ with additional structure. The set B is ordered, corresponding to the order of the rows in the array. Each member $B_j \in B$ contains every object of X, is construed to be ordered, corresponding to the order of the elements of a row. Moreover, the number of subsets in B equals the number of objects in X, and for each object x and each possible position within a row, there is a unique row in which x occupies that position.

Product of Latin Squares

The next definition indicates a method of construction of a new Latin square, starting from two given Latin squares.

DEF: Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares on $\mathbb{Z}_r$ and $\mathbb{Z}_s$, respectively. Then the ***product square*** $A \otimes B$ is the Latin square on $\mathbb{Z}_r \times \mathbb{Z}_s$

$$A \otimes B = \begin{pmatrix} a_{00} \times B & a_{01} \times B & \cdots & a_{0(r-1)} \times B \\ a_{10} \times B & a_{11} \times B & \cdots & a_{1(r-1)} \times B \\ \vdots & \vdots & \cdots & \vdots \\ a_{(r-1)0} \times B & a_{01} \times B & \cdots & a_{(r-1)(r-1)} \times B \end{pmatrix}$$

where the $s \times s$ submatrix $a_{ij} \times B$ is given by

$$a_{ij} \times B = \begin{pmatrix} (a_{ij}, b_{00}) & (a_{ij}, b_{01}) & \cdots & (a_{ij}, b_{0(s-1)}) \\ (a_{ij}, b_{10}) & (a_{ij}, b_{11}) & \cdots & (a_{ij}, b_{1(s-1)}) \\ \vdots & \vdots & \cdots & \vdots \\ (a_{ij}, b_{(s-1)0}) & (a_{ij}, b_{(s-1)1}) & \cdots & (a_{ij}, b_{(s-1)(s-1)}) \end{pmatrix}$$

Proposition 10.1.2. *Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares on $\mathbb{Z}_r$ and $\mathbb{Z}_s$, respectively. Their product $A \otimes B$ is a Latin square.*

Proof: Since each row of A contains each number in $\mathbb{Z}_r$ and each row of B contains each number in $\mathbb{Z}_s$, it follows that each row of $A \otimes B$ contains each pair in $\mathbb{Z}_r \times \mathbb{Z}_s$. The same fact holds for the columns. $\diamondsuit$

Example 10.1.3: If

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

then

$$A \otimes B = \begin{pmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \\ (0,1) & (0,2) & (0,0) & (1,1) & (1,2) & (1,0) \\ (0,2) & (0,0) & (0,1) & (1,2) & (1,0) & (1,1) \\ (1,0) & (1,1) & (1,2) & (0,0) & (0,1) & (0,2) \\ (1,1) & (1,2) & (1,0) & (0,1) & (0,2) & (0,0) \\ (1,2) & (1,0) & (1,1) & (0,2) & (0,0) & (0,1) \end{pmatrix}$$

which we observe is equivalent to the Latin square

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 & 3 \\ 2 & 0 & 1 & 5 & 3 & 4 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 3 & 1 & 2 & 0 \\ 5 & 3 & 4 & 2 & 0 & 1 \end{pmatrix}$$

under the bijection $\mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$ given by

$$\begin{array}{lll} (0,0) \mapsto 0 & (0,1) \mapsto 1 & (0,2) \mapsto 2 \\ (1,0) \mapsto 3 & (1,1) \mapsto 4 & (1,2) \mapsto 5 \end{array}$$

Orthogonal Latin Squares

DEF: Two $n \times n$ Latin squares $A = (a_{i,j})$ and $B = (b_{i,j})$ are ***orthogonal Latin squares*** if the n^2 ordered pairs $(a_{i,j}, b_{i,j})$ are mutually distinct.

Remark: By the pigeonhole principle, two $n \times n$ Latin squares are orthogonal if each possible ordered pair of domain elements occurs.

Example 10.1.4: It is easy enough to construct the pair of orthogonal 4×4 Latin squares in Figure 10.1.2 by ad hoc methods. One Latin square is represented pictorially by the outer pattern in an array location, and the other Latin square by the inner pattern.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

outer

$$\begin{pmatrix} 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 0 & 3 & 2 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

inner

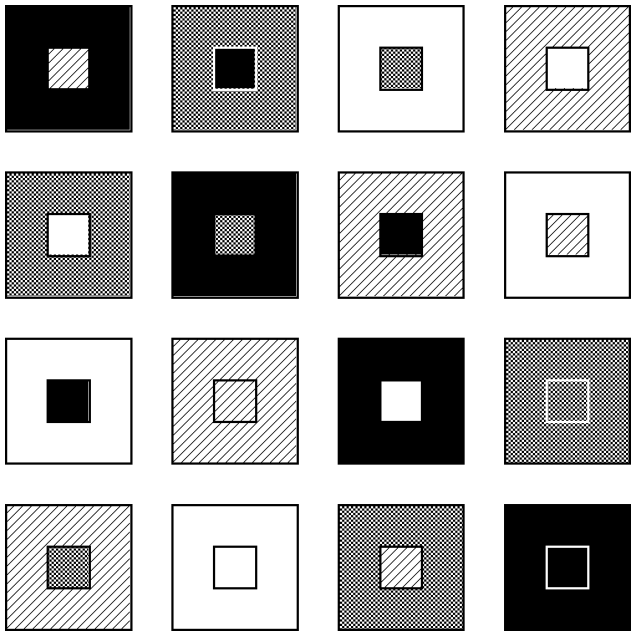

Fig 10.1.2 Two orthogonal Latin squares.

The next proposition indicates how to construct a family of mutually orthogonal Latin squares.

Proposition 10.1.3. *For $k = 1, \ldots, p-1$, where p is a prime number, let L_p^k be the $p \times p$ array such that*

$$L_p^k[i,j] \;=\; ki + j \bmod p \qquad 0 \le i, j \le p-1$$

Then the $p-1$ arrays

$$L_p^1, \quad L_p^2, \quad \ldots, \quad L_p^{p-1}$$

are mutually orthogonal Latin squares.

Proof: The entries in row i of the array L_p^k are

$$ki,\ ki+1,\ ki+2,\ \ldots,\ ki+(p-1)$$

which are clearly distinct. The entries in column j are

$$j,\ j+k,\ j+2k,\ \ldots,\ j+(p-1)k$$

Two of these entries differ by some number ck with $0 < c, k < p$. Since p is prime, $ck \not\equiv 0$ modulo p. Therefore, each of the arrays L_p^k is a Latin square.

Now suppose that the pairs of entries

$$\left(L_p^k[i,j],\ L_p^{k'}[i,j]\right) \quad \text{and} \quad \left(L_p^k[\hat{i},\hat{j}],\ L_p^{k'}[\hat{i},\hat{j}]\right)$$

are identical. Then

$$ki + j \ = \ k\hat{i} + \hat{j} \tag{10.1.3}$$

and

$$k'i + j \ = \ k'\hat{i} + \hat{j} \tag{10.1.4}$$

If $i \neq \hat{i}$, then $i - \hat{i}$ has a multiplicative inverse in $\mathbb{Z}_p$ (see Corollary 6.4.2). Hence,

$$k \ = \ \frac{\hat{j} - j}{i - \hat{i}} \qquad \text{from (10.1.3)}$$

and

$$k' \ = \ \frac{\hat{j} - j}{i - \hat{i}} \qquad \text{from (10.1.4)}$$

Therefore, $k = k'$. ♢

Example 10.1.5: The arrays L_5^2 and L_5^3 of Proposition 10.1.3 are orthogonal.

$$L_5^2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix} \quad L_5^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$$

Remark: If p is not a prime, then L_p^k might not be a Latin square. For instance, row 2 of the array L_6^3 is identical to row 0.

Theorem 10.1.4 [MacNeish, 1922]. *Let*

$$A^{(1)},\ A^{(2)},\ \ldots,\ A^{(r)}$$

be r mutually orthogonal $m \times m$ Latin squares, and let

$$B^{(1)},\ B^{(2)},\ \ldots,\ B^{(r)}$$

be r mutually orthogonal $n \times n$ Latin squares. Then the Latin squares

$$A^{(1)} \otimes B^{(1)},\ A^{(2)} \otimes B^{(2)},\ \cdots,\ A^{(r)} \otimes B^{(r)}$$

are mutually orthogonal.

Proof: Suppose that the pair of entries at location $ij \times k\ell$ of the Latin square $A^{(x)} \times B^{(x)}$ and of the Latin square $A^{(y)} \times B^{(y)}$, i.e.,

$$(a_{ij}^{(x)}, b_{k\ell}^{(x)}) \quad \text{and} \quad (a_{ij}^{(y)}, b_{k\ell}^{(y)})$$

is the same as the pair in location $pq \times uv$ of those two Latin squares, i.e., as the pair

$$(a_{pq}^{(x)}, b_{uv}^{(x)}) \quad \text{and} \quad (a_{pq}^{(y)}, b_{uv}^{(y)})$$

Then the pairs

$$(a_{ij}^{(x)}, a_{ij}^{(y)}) \quad \text{and} \quad (a_{pq}^{(x)}, a_{pq}^{(y)})$$

are identical, which implies, since $A^{(x)}$ and $A^{(y)}$ are orthogonal, that

$$i = p \quad \text{and} \quad j = q$$

Similarly,

$$k = u \quad \text{and} \quad \ell = v$$

Therefore, $A^{(x)} \times B^{(x)}$ and $A^{(y)} \times B^{(y)}$ are orthogonal. $\diamondsuit$

Proposition 10.1.5. *For every odd number $n > 1$, there is a pair of orthogonal $n \times n$ Latin squares.*

Proof: This follows from Proposition 10.1.3 and Theorem 10.1.4, since every odd number factors into a product of odd primes. $\diamondsuit$

Proposition 10.1.6. *Let $n = 2^k$ with $k \geq 2$. Then there is a pair of orthogonal $n \times n$ Latin squares.*

Proof: Example 10.1.4 gives a pair of orthogonal 4×4 Latin squares. The following is a pair of orthogonal 8×8

Latin squares.

$$\begin{pmatrix} 0&1&2&3&4&5&6&7\\ 1&0&3&2&5&4&7&6\\ 2&3&0&1&6&7&4&5\\ 3&2&1&0&7&6&5&4\\ 4&5&6&7&0&1&2&3\\ 5&4&7&6&1&0&3&2\\ 6&7&4&5&2&3&0&1\\ 7&6&5&4&3&2&1&0 \end{pmatrix} \qquad \begin{pmatrix} 0&1&2&3&4&5&6&7\\ 7&6&5&4&3&2&1&0\\ 3&2&1&0&7&6&5&4\\ 4&5&6&7&0&1&2&3\\ 6&7&4&5&2&3&0&1\\ 1&0&3&2&5&4&7&6\\ 5&4&7&6&1&0&3&2\\ 2&3&0&1&6&7&4&5 \end{pmatrix}$$

If k is even, then n is a power of 4, and if k is odd, then n is a product of 8 with a power of 4. It follows from the base cases 4×4 and 8×8 and Theorem 10.1.4 that there is a pair of orthogonal $n \times n$ Latin squares. ♢

There are only two possible 2×2 Latin squares in $\mathbb{Z}_2$, and they are not orthogonal. Euler conjectured in 1782 that for n odd, there is no orthogonal pair of $2n \times 2n$ Latin squares. In 1901, Gaston Tarry [Tarr1901] proved by exhaustion that there is no 6×6 pair. However, Ernest Parker [Park1959] produced a 10×10 pair in 1960, and then Bose, Shrikhande, and Parker [BSP1960] proved that there is a $2n \times 2n$ orthogonal pair except for $n = 1$ or 3.

Summary. *For every positive integer n except 1, 2, and 6, there is a pair of orthogonal $n \times n$ Latin squares.*

Isotopic Latin Squares

DEF: The Latin squares $L[i,j]$ and $L'[i,j]$ on $\mathbb{Z}_n$ are ***isotopic Latin squares*** if L' can be obtained from L by a sequence of transformations, each chosen from any of the following three types.

- A permutation of the rows.
- A permutation of the columns.
- Applying a permutation $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ to the symbols of the array.

Example 10.1.6: Swapping rows 0 and 1 of the Latin square

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \tag{10.1.2}$$

yields the Latin square

$$\begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

Example 10.1.7: Swapping the symbols 0 and 1 in the Latin square (10.1.2) yields this Latin square.

$$\begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 2 & 3 & 1 & 0 \\ 3 & 1 & 0 & 2 \end{pmatrix}$$

Remark: Clearly, isotopy on Latin squares is an equivalence relation.

DEF: A Latin square on $\mathbb{Z}_n$ is said to be ***normalized*** if its initial row is

$$0 \quad 1 \quad \cdots \quad n-1$$

and its initial column is

$$\begin{matrix} 0 \\ 1 \\ \vdots \\ n-1 \end{matrix}$$

Clearly, every Latin square is isotopic to a normalized Latin square.

Abstract Latin Squares

Isotopy allows three natural kinds of transformation on Latin squares that may be regarded as natural equivalences. The following alternative conceptualization of a Latin square allows some additional equivalences.

DEF: An ***abstract Latin square*** on $\mathbb{Z}_n$ is a set L of triples

$$(r,\ c,\ s)$$

in $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ such that

- For any $(i, j) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $i = r$ and $j = c$.
- For any $(i, k) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $i = r$ and $k = s$.
- For any $(j, k) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $j = c$ and $k = s$.

Proposition 10.1.7. *Every abstract Latin square corresponds to a unique concrete Latin square (i.e., the array form). Conversely, for every concrete Latin square, there is a unique abstract Latin square.* $\diamondsuit$

We observe that the operation of transposition on the array form of a Latin square has as its abstract counterpart the operation of swapping the first and second entry in each triple. Yet from the abstract perspective, we could equally well swap the first and third entry of each triple. Indeed, we equally apply any of the six possible permutations uniformly to all the triples. This motivates the following definition.

DEF: Let π be a permutation on the set $\{1,\ 2,\ 3\}$. The operation of transforming a Latin square by applying π to the coordinates of the triples is called a ***conjugacy operation***. The array resulting from applying π to a Latin square L is called the π***-conjugate*** of L. It may be denoted L^{π}.

Example 10.1.8: Consider the following Latin square in array and abstract form.

$$L = \begin{pmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} \qquad \begin{matrix} (0,0,0) & (0,1,3) & (0,2,1) & (0,3,2) \\ (1,0,1) & (1,1,2) & (1,2,0) & (1,3,3) \\ (2,0,3) & (2,1,0) & (2,2,2) & (2,3,1) \\ (3,0,2) & (3,1,1) & (3,2,3) & (3,3,0) \end{matrix}$$

Applying the permutation $(1,2)(3)$ to the set of triples means swapping the first and second coordinates of each triple, thereby obtaining

$$\begin{matrix} (0,0,0) & (1,0,3) & (2,0,1) & (3,0,2) \\ (0,1,1) & (1,1,2) & (2,1,0) & (3,1,3) \\ (0,2,3) & (1,2,0) & (2,2,2) & (3,2,1) \\ (0,3,2) & (1,3,1) & (2,3,3) & (3,3,0) \end{matrix}$$

which is the abstract form of the Latin square

$$L^{(1,2)(3)} = \begin{pmatrix} 0 & 1 & 3 & 2 \\ 3 & 2 & 0 & 1 \\ 1 & 0 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix}$$

Observing that $L^{(1,2)(3)}$ is simply the transpose of L, we recognize that the transformation $L \mapsto L^{(1,2)(3)}$ simply swaps the roles of rows and columns.

Alternatively, applying the permutation $(1,3)(2)$ to the set of triples means swapping the first and third coordinates of each triple, thereby obtaining

$$\begin{matrix} (0,0,0) & (3,1,0) & (1,2,0) & (2,3,0) \\ (1,0,1) & (2,1,1) & (0,2,1) & (3,3,1) \\ (3,0,2) & (0,1,2) & (2,2,2) & (1,3,2) \\ (2,0,3) & (1,1,3) & (3,2,3) & (0,3,3) \end{matrix}$$

which is the abstract form of the Latin square

$$L^{(1,3)(2)} = \begin{pmatrix} 0 & 2 & 1 & 3 \\ 1 & 3 & 0 & 2 \\ 3 & 1 & 2 & 0 \\ 2 & 0 & 3 & 1 \end{pmatrix}$$

Remark 1: We observe that conjugacy is an equivalence relation on the Latin squares. The possible class sizes are 1, 2, 3, and 6.

Remark 2: For $n \leq 5$, the conjugacy operations on a Latin square produce only Latin squares that could be obtained by isotopy operations. However, for $n \geq 6$, they produce additional Latin squares.

DEF: Two Latin squares L and L' are ***main class isotopic*** if L is isotopic to any conjugate of L'.

10.2 BLOCK DESIGNS

A generic *block design* can be regarded as a generalization of a graph, in which a *block* is a generalized edge.

DEF: A ***block design*** $\mathcal{B}$ has a non-empty domain

$$X = \{ x_1, x_2, \ldots, x_v \}$$

whose elements are sometimes called *varieties* and a non-empty collection

$$B = \{B_1, B_2, \ldots, B_b\}$$

of subsets of X called ***blocks***. It is a ***simple design*** if no two blocks are identical.

DEF: The number of blocks in which an element x appears is called the ***valence of that element of the design.***

DEF: The number of blocks in which a pair of elements x and y appears is called the ***covalence of that pair.***

Thus, a graph is a block design in which every block has size 2. The valence of an element within the block design would be its degree as a vertex of the graph. The covalence of a pair of elements of the design would be their multiplicity of adjacency as vertices of the graph. To allow self-loops in a graph, one would allow the blocks to be multisets of elements of the design and make suitable revisions in the definition of valence and covalence.

DEF: A block design is ***regular*** if the following two conditions hold:

- every block is the same size $k \geq 2$, which is called the ***blocksize***;
- each element x_j has the same valence; that is, each appears in the same number r of blocks, which is called the ***replication number***.

Thus, a d-regular graph is a regular block design with blocksize 2 and replication number d.

Balanced Designs

The idea of *balancing* a design with *incomplete blocks* arose with Sir Ronald Fisher (1890-1962) in his theoretical study of the design of experiments in agriculture.

DEF: A regular block design $\mathcal{B}$ with v varieties and b blocks is ***balanced*** and is called either a ***(v, b, r, k, λ)-design*** or a ***(v, k, λ)-design*** if each pair of elements x_i and x_j has the same covalence, that is, if each pair appears in the same number λ of blocks, which is called the ***index of the design***.

A balanced design is ***complete*** if $k = v$, so that each block contains all of X. If $k < v$, then it is ***incomplete***.

TERMINOLOGY: A balanced incomplete block design is commonly called a ***BIBD***.

Example 10.2.1: For $X = \{0, 1, 2, 3\}$, the blocks

$$B_1 : 012 \quad B_2 : 013 \quad B_3 : 023 \quad B_4 : 123$$

form a $(4, 4, 3, 3, 2)$-design.

Example 10.2.2: For $X = \{0, 1, \ldots, 8, 9, A\}$, the blocks

$$\begin{array}{cccccc} 02348 & 13459 & 2456A & 35670 & 46781 & 57892 \\ 689A3 & 79A04 & 8A015 & 90126 & A1237 & \end{array}$$

form a $(v = 11, b = 11, r = 5, k = 5, \lambda = 2)$-design. In this design, the initial block generates all of the others, if we regard the elements of X as integers modulo 11, with a standing for 10 modulo 11. Then each other block is obtained by adding 1 modulo 11 to each of the elements of the previous block.

Example 10.2.3: For every $n \geq 2$, setting $X = [1 : n]$ and $B_1 = X$ yields a complete design with $v = n$, $b = 1$, $r = 1$, $k = n$, and $\lambda = 1$.

Example 10.2.4: For every $n \geq 2$, setting $X = [1 : n]$ and having the pairs of elements from X as blocks yields a balanced design with

$$v = n, \quad b = \binom{n}{2}, \quad r = n - 1, \quad k = 2, \quad \lambda = 1$$

Thus, the complete graph K_n is representable as a BIBD.

Example 10.2.5: When a simple graph is drawn on an arbitrary surface without crossings, each edge lies on exactly two faces. If the graph is K_n, and if all faces are k-sided, then this drawing may be regarded as a BIBD with $v = n$, blocksize k, and $\lambda = 2$, in which a block is the set of corners of a face.

Necessary Conditions

The examples above establish that BIBD's exist for certain combinations of the parameters v, b, r, k, and λ. However, there are no BIBD's for various other combinations. Our immediate concern is to derive some necessary conditions for the existence of a (v, b, r, k, λ)-design.

Prop 10.2.1. *For every non-empty* (v, b, r, k, λ)*-BIBD*

$$(a)\ \lambda \geq 1 \quad \text{and} \quad (b)\ k < v$$

Proof: Since there is at least one block, and since it has at least two elements, some pair has at least once occurrence. Since all pairs occur equally often, it follows that $\lambda \geq 1$.

Since a block is a subset of the domain, its size cannot exceed the size of the domain. Thus, $k \leq v$. Since a BIBD is *incomplete*, it follows that $k < v$. ♢

Proposition 10.2.2. *The parameters of a* (v, b, r, k, λ)*-design on*

$$X = \{ x_1, x_2, \ldots, x_v \}$$

satisfy the following two conditions:

$$(a) \qquad bk \;=\; vr$$

$$(b) \qquad r\,(k-1) \;=\; \lambda\,(v-1)$$

Proof: First consider the $v \times b$ incidence matrix

$$I \;=\; \begin{array}{c|ccc} & B_1 & \cdots & B_b \\ \hline x_1 & \iota_{1,1} & \cdots & \iota_{1,b} \\ \vdots & \vdots & \vdots & \vdots \\ x_v & \iota_{v,1} & \cdots & \iota_{v,b} \end{array} \qquad \iota_{i,j} \;=\; \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{otherwise} \end{cases}$$

There are v rows, each with row-sum r, and there are b columns, each with column-sum k. Therefore, $bk = vr$.

Next consider the $\binom{v}{2} \times b$ pair-incidence matrix

$$I' \;=\; \begin{array}{c|ccc} & B_1 & \cdots & B_b \\ \hline x_1x_2 & \iota'_{12,1} & \cdots & \iota'_{12,b} \\ \vdots & \vdots & \vdots & \vdots \\ x_{v-1}x_v & \iota'_{(v-1)v,1} & \cdots & \iota'_{(v-1)v,b} \end{array}$$

with

$$\iota'_{ij,\ell} \;=\; \begin{cases} 1 & \text{if } x_ix_j \in B_\ell \\ 0 & \text{otherwise} \end{cases}$$

There are $\binom{v}{2}$ rows, each with row-sum λ, and there are b columns, each with column-sum $\binom{k}{2}$. Therefore,

$$\lambda\binom{v}{2} \;=\; b\binom{k}{2}$$

Accordingly,

$$\begin{aligned} \lambda v\,(v-1) &= bk\,(k-1) \\ \Rightarrow \lambda v\,(v-1) &= vr\,(k-1) \quad \text{since } bk = vr \\ \Rightarrow \lambda\,(v-1) &= r\,(k-1) \end{aligned}$$ ♢

TERMINOLOGY NOTE: The inferrability (from Prop 10.2.2) of values of b and r from values of v, k, and λ justifies optionally calling a (v, b, r, k, λ)-design a (v, k, λ)-design.

Corollary 10.2.3. *For every non-empty BIBD,*

$$\lambda < r$$

Proof: Since $\lambda\,(v-1) = r\,(k-1)$ (from Thm 10.2.2) and $k < v$ (from Prop 10.2.1), it follows that $\lambda < r$. ♢

REVIEW FROM LINEAR ALGEBRA:

- If AB is the product of the matrices A and B then

$$rank(AB) \;\leq\; \min\{rank(A),\, rank(B)\}$$

NOTATION: The *transpose* of a matrix M is denoted M^T.

Thm 10.2.4 [Fisher's Ineq]. *In any BIBD, $b \geq v$.*

Proof: Let I be the incidence matrix of the BIBD. Then

$$I\,I^T = \begin{pmatrix} r & \lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \lambda & \cdots & r \end{pmatrix}$$

Subtracting the first column of a matrix from the other columns does not change the determinant. Hence,

$$det(I\,I^T) \;=\; \begin{vmatrix} r & \lambda - r & \lambda - r & \lambda - r & \cdots & \lambda - r \\ \lambda & r - \lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & 0 & \cdots & r - \lambda \end{vmatrix}$$

Adding the other rows of a matrix to the first row does not change the determinant. Hence,

$$det(I\,I^T) \;=\; \begin{vmatrix} r + (v-1)\lambda & 0 & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & 0 & \cdots & r - \lambda \end{vmatrix}$$

Since the upper triangle of this matrix is all zeroes, the determinant is the product of the diagonal entries. Thus,

$$det(I\,I^T) \;=\; [r + (v-1)\lambda](r - \lambda)^{v-1}$$

By Corollary 10.2.3, $r - \lambda > 0$. Moreover, $r + (v-1)\lambda$ is positive. Thus, $det(I\,I^T)$ is non-zero. Accordingly, the rank of the $v \times v$-matrix $I\,I^T$ is v. Since the rank of the $v \times b$ incidence matrix I is at most b, and since the rank, v, of the product matrix $I\,I^T$ cannot exceed the rank of the matrix I, it follows that $v \leq b$. $\diamondsuit$

Steiner Triple Systems

DEF: A $(v, 3, 1)$-design is also called a ***Steiner triple system.***

Example 10.2.6: The complete balanced block design

$$\mathcal{A} = \begin{cases} \text{domain} & X = \{0,\ 1,\ 2\} \\ \text{1 block} & B = \{012\} \end{cases} \tag{10.2.1}$$

is a Steiner triple system. (A Steiner triple system on a domain with more than three elements is a BIBD.)

Example 10.2.7: The BIBD

$$\mathcal{B} = \begin{cases} \text{domain} & Y = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\} \\ \text{7 blocks} & C = \{013,\ 124,\ 235,\ 346,\ 450,\ 561,\ 602\} \end{cases}$$

is a $(7, 3, 1)$-design. As in Example 10.2.2, the first block generates the others.

Proposition 10.2.5. *In a $(v, 3, 1)$-design,*

$$(a)\ r = \frac{v-1}{2} \quad \text{and} \quad (b)\ b = \frac{v(v-1)}{6}$$

Proof: Part (a) follows from Proposition 10.2.2(b):

$$r\,(k-1) = \lambda\,(v-1)$$

Simply substitute $k = 3$ and $\lambda = 1$.

For part (b), start with the equation

$$bk = rv$$

from Proposition 10.2.2(a). Then substitute 3 for k and $(v-1)/2$ for r to obtain

$$3b = v\,\frac{v-1}{2}$$

which leads immediately to the desired formula. ♢

Corollary 10.2.6. *In a* $(v, 3, 1)$*-design,*

$$v \equiv 1 \text{ or } 3 \text{ modulo } 6$$

Proof: Prop 10.2.5(a) implies that v is odd. Thus,

$$v \equiv 1, 3 \text{ or } 5 \text{ modulo } 6$$

However, if $v \equiv 5$ modulo 6, then $v(v-1) \equiv 2$ modulo 6, contradicting Prop 10.2.5(b). ♢

Constructing Designs

Jakob Steiner (1796-1893) asked in 1853 whether for every positive v such that $v \equiv 1$ or 3 modulo 6, there exists a $(v, 3, 1)$-design. He was unaware that in 1847, the Rev. Thomas P. Kirkman (1806-1895) had proved they always exist. Kirkman's methods are beyond the present

scope. We presently offer some elementary methods that can also be used for constructing BIBD's with larger block-size. The first such method generalizes Example 10.2.7.

DEF: A set of numbers

$$S = \{a_1,\ a_2,\ \ldots,\ a_k\}$$

in $\mathbb{Z}_n$ is a ***perfect difference set*** of index λ for $\mathbb{Z}_n$ if each non-zero number in $\mathbb{Z}_n$ occurs exactly λ times in the list

$$\langle x_{ij} = a_i - a_j \mid a_i, a_j \in S;\ i \neq j \rangle$$

It is simply called a ***perfect difference set*** if $\lambda = 1$.

Proposition 10.2.7. *A perfect difference set B of cardinality k and index λ for $\mathbb{Z}_v$ generates a (v, k, λ)-design.*

Proof: For $j = 0, \ldots, v-1$, let $B_j = \{j + b \mid b \in B\}$. By the definition of a perfect difference set, these blocks form a (v, k, λ)-design. ♢

Example 10.2.7, cont.: The set $\{0, 1, 3\} \subset \mathbb{Z}_7$ is a perfect difference set of index 1, since

$$\begin{array}{lll} 1 = 1-0 & 2 = 3-1 & 3 = 3-0 \\ 4 = 0-3 & 5 = 1-3 & 6 = 0-1 \end{array}$$

DEF: A family $\mathcal{S}$ of sets $S_1, \ldots, S_f \subset Z_n$ is a ***perfect difference family*** of index λ if each non-zero number in $\mathbb{Z}_n$ occurs exactly λ times in the list

$$\langle x_{ijk} = a_i - a_j \mid a_i, a_j \in S_k;\ i \neq j;\ 1 \leq k \leq f \rangle$$

It is called a ***perfect difference family*** if $\lambda = 1$.

Proposition 10.2.8. *If the sets of a perfect difference family of index λ for $\mathbb{Z}_v$ are all of the same size k, then they generate a (v, k, λ)-design.* ♢

Example 10.2.8: We construct a perfect difference family for $\mathbb{Z}_{13}$

$\{0,\ 1,\ 4\}$ with differences $\{1,\ 3,\ 4,\ 9,\ 10,\ 12\}$
$\{0,\ 2,\ 8\}$ with differences $\{2,\ 5,\ 6,\ 7,\ 8,\ 11\}$

These two blocks together generate the following $(13, 3, 1)$-design.

$$X = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C\}$$

$$B = \left\{ \begin{array}{ccccccccc} 014 & 125 & 236 & 347 & 458 & 569 & 67A & 78B & 89C \\ & 9A0 & AB1 & BC2 & C03 & & & & \\ 028 & 139 & 24A & 35B & 46C & 570 & 681 & 792 & 8A3 \\ & 9B4 & AC5 & B06 & C17 & & & & \end{array} \right\}$$

Example 10.2.9: The set $\{0, 1, 4, 6\}$ is a perfect difference set for $\mathbb{Z}_{13}$. Thus, with the domain

$$X = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C\}$$

the set of blocks

$$B = \left\{ \begin{array}{ccccccc} 0146 & 1257 & 2368 & 3479 & 458A & 569B & 67AC \\ 78B0 & 89C1 & 9A02 & AB13 & BC24 & C035 & \end{array} \right\}$$

forms a (13, 4, 1)-design.

The next example offers a way to construct a new Steiner triple system from two (possibly identical) smaller systems.

Example 10.2.10: The cartesian product of the domain of the $(3, 3, 1)$-design $\mathcal{A}$ of Example 10.2.6 and the domain of the $(7, 3, 1)$-design $\mathcal{B}$ of Example 10.2.7 is representable as the following array.

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 00 & 01 & 02 & 03 & 04 & 05 & 06 \\ 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 20 & 21 & 22 & 23 & 24 & 25 & 26 \end{pmatrix} \end{array}$$

To obtain a (21, 3, 1)-design $\mathcal{A} \times \mathcal{B}$ on the set of elements of that array, we choose as blocks

(i) every column;

(ii) from each row, each triple $\{ri,\ rj,\ rk\}$ such that $\{i,\ j,\ k\}$ is a block of $\mathcal{B}$;

(iii) each triple $\{0i,\ 1j,\ 2k\}$ such that $\{i,\ j,\ k\}$ is a block of $\mathcal{B}$.

Observe that the number of blocks we have chosen is

$$7 + 21 + 42 = 70$$

Two elements xy and $x'y'$ of $\mathcal{A} \times \mathcal{B}$ appear in one and only one block. There are three cases.

(i) $x \neq x'$ and $y = y'$: only in the block arising from column y.

(ii) $x = x'$ and $y \neq y'$: only in the block arising from row x and the unique block of $\mathcal{B}$ in which y and y' are paired.

(iii) $x \neq x'$ and $y \neq y'$: let x'' be the remaining row, and let y'' be the third entry in the unique block of $\mathcal{B}$ that contains both y and y'. Then $\{xy,\ x'y',\ x''y''\}$ is the unique block containing xy and $x'y'$.

DEF: The ***product of two Steiner triple systems*** $\mathcal{A}$ and $\mathcal{B}$ is the triple system whose domain is the product of the domains of $\mathcal{A}$ and $\mathcal{B}$, with blocks as follows:

(i) from each column of the product array $\mathcal{A} \times \mathcal{B}$, each triple $\{rc,\ sc,\ tc\}$ such that $\{r,\ s,\ t\}$ is a block of $\mathcal{A}$;

(ii) from each row of $\mathcal{A} \times \mathcal{B}$, each triple $\{ri,\ rj,\ rk\}$ such that $\{i,\ j,\ k\}$ is a block of $\mathcal{B}$;

(iii) each triple $\{ri,\ sj,\ tk\}$ such that $\{r,\ s,\ t\}$ is a block of $\mathcal{A}$ and $\{i,\ j,\ k\}$ is a block of $\mathcal{B}$.

Theorem 10.2.9. *Let $\mathcal{A}$ and $\mathcal{B}$ be Steiner triple systems with u and v varieties, respectively. Then their product is a Steiner triple system with uv varieties.*

Proof: The proof for the general case is essentially the same as for Example 10.2.10. ♢

Remark: The definition and theorem just above are generalizable to a product of BIBD's and a theorem that the result is a new BIBD.

Isomorphism of Designs

DEF: A bijection $f : X \to Y$ of the domains of two block designs

$$\mathcal{B} = \langle X, \{B_i\} \rangle \quad \text{and} \quad \mathcal{C} = \langle Y, \{C_j\} \rangle$$

is called an ***isomorphism of block designs*** if for every block C_j of design $\mathcal{C}$, there is a block B_i of design $\mathcal{B}$, such that the restriction $f : B_i \to C_j$ is onto.

Proposition 10.2.10. *Let $\mathcal{B} = \langle X, \{B_i\} \rangle$ be a $(7, 3, 1)$ Steiner system. Then $\mathcal{B}$ is isomorphic to the $(7, 3, 1)$ Steiner system with elements $0, 1, 2, 3, 4, 5, 6$ and blocks*

$$013 \quad 124 \quad 235 \quad 346 \quad 450 \quad 561 \quad 602$$

Proof: Choose an arbitrary element of X and call it x_0. Since each of the six other elements of X must appear with x_0 exactly once, there must be exactly three blocks of $\mathcal{B}$ that contain x_0. Call the other two elements in one of these blocks x_1 and x_3, and call the other two in a second of these blocks x_2 and x_6. Partially specify the bijection f by

$$x_0 \mapsto 0 \quad x_1 \mapsto 1 \quad x_2 \mapsto 2 \quad x_3 \mapsto 3 \quad x_6 \mapsto 6$$

which ensures some block preservation, namely,

$$x_0x_1x_3 \mapsto 013 \quad x_0x_2x_6 \mapsto 026 \quad x_0x_4x_5 \mapsto 045$$

The elements x_1 and x_2 appear together in a unique block of $\mathcal{B}$. Since the third element of that block cannot be x_0, x_3, or x_6, each of which appears in another block with x_1 or x_2, it can be called x_4, with the remaining element of X to be x_5.

Completing the bijection specification with

$$x_4 \mapsto 4 \quad x_5 \mapsto 5$$

immediately ensures further block preservation

$$x_1x_2x_4 \mapsto 124$$

Moreover, given that $x_0x_1x_3$ and $x_1x_2x_4$ are blocks, it follows that the third block containing x_1 must be $x_1x_5x_6$. Similarly, the third block containing x_2 must be $x_2x_3x_5$. Since the elements x_3, x_4, and x_6 have so far appeared in only two blocks each, the seventh block must be $x_3x_4x_6$. Thus all blocks are preserved by the bijection f. $\diamondsuit$

Remark: There is essentially only one (7, 3, 1)-design, as established by Prop 10.2.10, and also only one (9, 3, 1)-design. There are two non-isomorphic (13, 3, 1)-designs and 80 mutually non-isomorphic (15, 3, 1)-designs. See the table on p764 of [CoDi2000a].

10.3 CLASSICAL FINITE GEOMETRY

Many properties of the Euclidean spaces $\mathbb{R}^n$ can be derived purely from a short list of axioms about points and lines, without consideration of distance or angles, and without consideration that a line in $\mathbb{R}^n$ contains infinitely many points. In this spirit, various kinds of combinatorial designs on a finite set of elements have been called ***finite geometries***. The elements of their domains are traditionally called the ***points of the geometry***, and their distinguished subsets are called the ***lines of the geometry***. The following two general axioms are standard for geometries.

G1. Two distinct points are contained in at most one line.

G2. Two distinct lines intersect in at most one point.

NOTATION: In view of Axiom G1, we may denote the line containing two distinct points u and v by uv.

TERMINOLOGY: Two disjoint lines of a geometry are often said to be ***parallel lines***.

DEF: The ***incidence matrix of a geometry*** $\langle X, L \rangle$ with p points

$$X = \{x_1, \ldots, x_p\}$$

and ℓ lines

$$L = \{L_1, \ldots, L_\ell\}$$

is the $p \times \ell$ matrix

$$M_{\langle X,L\rangle}[i,j] \;=\; \begin{cases} 1 & \text{if } x_i \in L_j \\ 0 & \text{otherwise} \end{cases}$$

A geometry is commonly specified by its incidence matrix.

Example 10.3.1: Figure 10.3.1 illustrates a geometry with a drawing of its four points and its six lines.

$$\begin{array}{c} \\ x_0 \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cccccc} L_0 & L_1 & L_2 & L_3 & L_4 & L_5 \end{array} \\ \left(\begin{array}{cccccc} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array} \right) \end{array}$$

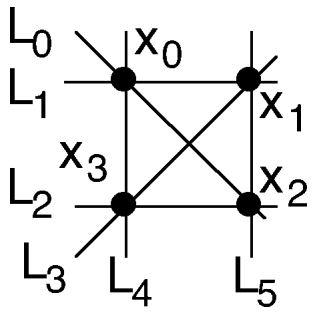

Fig 10.3.1 A geometry with 4 points and 6 lines.

DEF: The ***dual of a geometry*** $\langle X, L\rangle$ is the geometry $\langle X^*, L^*\rangle$ with

$$X^* \;=\; L \quad \text{and} \quad L^* \;=\; X$$

whose incidence matrix is the transpose of the incidence matrix of $\langle X, L\rangle$. (In view of the reciprocity of Axioms G1 and G2, the dual design satisfies both of them.)

Example 10.3.1, cont.: Figure 10.3.2 illustrates the dual of the geometry specified by Figure 10.3.1.

$$\begin{array}{c} \\ L_0^* \\ L_1^* \\ L_2^* \\ L_3^* \\ L_4^* \\ L_5^* \end{array} \begin{array}{c} \begin{array}{cccc} x_0^* & x_1^* & x_2^* & x_3^* \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

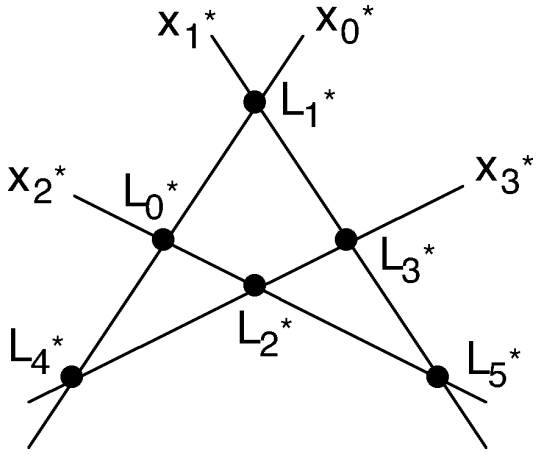

Fig 10.3.2 The dual geometry has 6 points and 4 lines.

The Fano Plane

A design named for the Italian geometer Gino Fano (1871-1952) is the first of three widely cited classical geometries that we now consider.

DEF: The ***Fano plane*** is defined by the incidence matrix

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

It is depicted in the diagram in Figure 10.3.3, in which the line L_0 is represented by a circle.

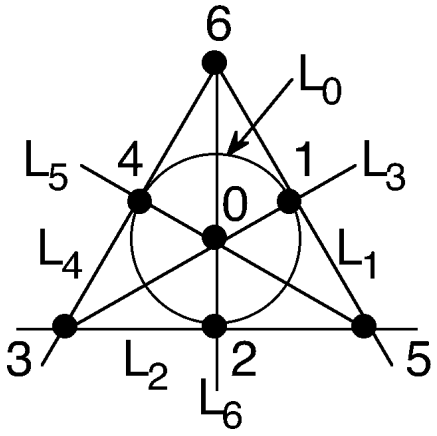

Fig 10.3.3 The Fano plane.

We observe that as a design, the Fano plane is precisely the Steiner triple system of Example 10.2.7.

The Pappus Geometry

A second classical geometry is named for Pappus of Alexandria (c. 300-350 C.E.), who proved the following theorem of Euclidean geometry.

Theorem of Pappus. *Let 0, 1, and 2 be three distinct points on a line L_1 and 3, 4, and 5 three distinct points on line $L_2 \neq L_1$, such that there are points of intersection*

$$6 = 04 \cap 13 \quad 7 = 05 \cap 23 \quad \text{and} \quad 8 = 15 \cap 24$$

Then the points 6, 7, and 8 are colinear. ♢

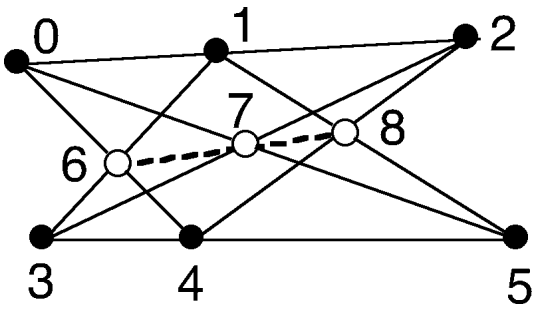

Fig 10.3.4 The geometry of Pappus.

DEF: The ***Pappus geometry*** is the following finite geometry

$$X = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}$$
$$L = \{012,\ 345,\ 064,\ 075,\ 163,\ 185,\ 273,\ 284,\ 678\}$$

or any other geometry of the same isomorphism type.

The Pappus geometry has uniform blocksize 3 and uniform replication number 3. As in Euclidean plane geometry, no pair of points occurs more than once in a line. However, in the Pappus geometry, and unlike Euclidean geometry, some pairs of points do not lie on any line. This implies that the Pappus geometry is not a Steiner triple system or a BIBD. The Pappus geometry shares the following property with Euclidean plane geometry.

Proposition 10.3.1. *Let L_i be any line of the Pappus geometry, and let p be a point that is not on that line. Then there is a unique line L_j containing the point p and parallel to the line L_i.*

Proof: The lines of the Pappus geometry are resolvable

into three classes of parallel lines.

$$\begin{aligned} C_1 &= \{\,012 \quad 345 \quad 678\,\} \\ C_2 &= \{\,064 \quad 185 \quad 273\,\} \\ C_3 &= \{\,075 \quad 163 \quad 284\,\} \end{aligned}$$

If the given line L_i lies in the class C_k, then choose line L_j to be the unique line in class C_k that contains point p. ♢

The Desargues Geometry

Another theorem of plane Euclidean geometry is due to Girard Desargues (1591-1661).

Theorem of Desargues. *Let 123 and 456 be triangles such that the lines 14, 25, and 36 meet at point 0. Let*

$$7 = 13 \cap 46 \quad 8 = 23 \cap 56 \quad \text{and} \quad 9 = 12 \cap 45$$

Then 7, 8, and 9 are colinear. ♢

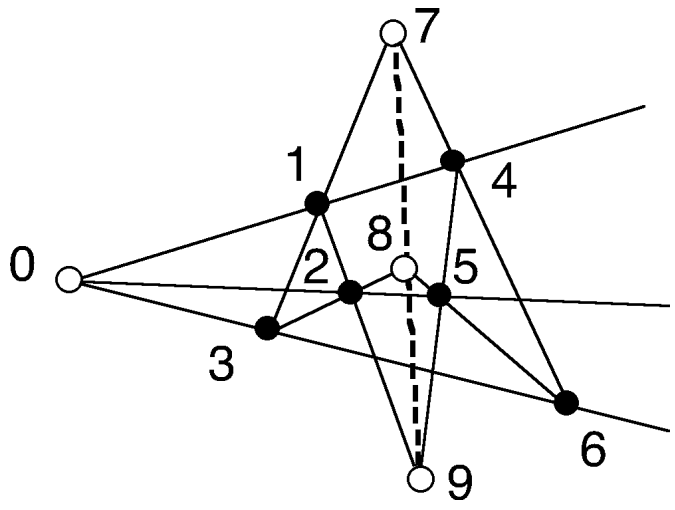

Fig 10.3.5 **The geometry of Desargues.**

DEF: The ***Desargues geometry*** is the following finite geometry

$$X = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9\}$$
$$L = \{014,\ 025,\ 036,\ 137,\ 129,\ 238,\ 467,\ 459,\ 568,\ 789\}$$

or any other geometry of the same isomorphism type.

In the Desargues geometry, as in the Pappus geometry, there is a uniform blocksize of 3 and a uniform replication number of 3. As in Euclidean geometry and the Pappus geometry, no pair of points occurs more than once in a block. As in the Pappus geometry, and unlike Euclidean geometry, some pairs do not occur on any line. Accordingly, it is not a Steiner triple system or a BIBD.

Remark 1: Observe that Proposition 10.3.1 does not apply to the Desargues geometry. In fact, for every line L_i in the Desargues geometry, there is a point p such that no line containing p intersects the line L_i. Such a point p is called a *pole* of the line L_i.

Example 10.3.2: In the Desargues geometry, the point 8 is a pole of the line 014, and the point 1 is a pole of the line 568.

Remark 2: Another interesting property in which Desargues geometry differs from Euclidean geometry is that in the Desargues geometry, two lines that are parallel to the same line are *not* parallel to each other.

Example 10.3.3: The lines that are parallel to the line 789 of the Desargues geometry are 014, 036, and 025. Observe that any pair of them intersects in the point 0.

Partially Balanced Designs

DEF: A $(v, b, r, k; \lambda_1, \lambda_2)$-***PBIBD*** (stands for ***partially balanced incomplete block design***) is a design with v elements and b blocks, in which

(i) each element lies in exactly r blocks;

(ii) each block contains exactly k elements;

(iii) each pair of distinct elements occurs either in λ_1 or λ_2 blocks.

Example 10.3.4: The Pappus geometry is a $(9, 9, 3, 3; 1, 0)$-PBIBD.

Example 10.3.5: The Desargues geometry is a $(10, 10, 3, 3; 1, 0)$-PBIBD.

10.4 PROJECTIVE PLANES

A *projective plane* is a type of finite geometry, and thus, a combinatorial design. Toward the end of this section, there is a method for constructing projective planes from 3-dimensional vector spaces. This construction is what motivates calling these designs *projective planes.*

DEF: A ***projective plane*** $\mathcal{P}$ has a domain X, whose elements are called *points*, and a collection of subsets of X that are called *lines*, such that the following axioms hold:

PP1. For each pair of distinct points, there is exactly one line containing them.

PP2. Each pair of distinct lines intersects in exactly one point.

PP3. There exist four points, no three of which lie on the same line.

These three simple axioms have many implications.

Some Basic Examples

Example 10.4.1: The Fano plane is a projective plane. This can be verified by checking its definition as a design.

Prop 10.4.1. *For $k \geq 3$, any $(v, k, 1)$-design $\mathcal{B}$ generated by a perfect difference set $S = \{a_1, \ldots, a_k\} \subseteq \mathbb{Z}_v$ is a projective plane. Moreover, $v = k^2 - k + 1$.*

Proof: Let $i, j \in \mathbb{Z}_v$ with $i \leq j$. To find a block in $\mathcal{B}$ that contains both i and j, let a_r and a_s be the unique pair in the difference set S such that $a_s - a_r = j - i$. Then the block $S + (i - a_r)$ contains

$$\begin{aligned} a_r + (i - a_r) &= i \quad \text{and} \\ a_s + (i - a_r) &= i + (a_s - a_r) = i + (j - i) = j \end{aligned}$$

No other pair from S has difference $j - i$, so no other pair can translate to i and j in the same block. Moreover, a_r and a_s translate to i and j only in the block $S + (i - a_r)$. This establishes Axiom PP1.

Next, consider two arbitrary blocks of $\mathcal{B}$, say

$$S + i = \{a_t + i \mid a_t \in S\} \quad \text{and} \quad S + j = \{a_t + j \mid a_t \in S\}$$

There is a unique pair a_r, a_s in the difference set S such that

$$j - i = a_r - a_s$$

It follows that the number $j + a_s = i + a_r$ is the unique point in the intersection

$$(S + i) \cap (S + j)$$

This establishes Axiom PP2.

To prove the third axiom, let B_1 and B_2 be any two blocks. By PP2, they intersect in a single point. Since $k \geq 3$, there are at least two points $x_1, x_2 \in B_1 - B_2$ and at least two points $x_3, x_4 \in B_2 - B_1$. The four points x_1, x_2, x_3, x_4 satisfy the condition of PP3.

The method of block generation yields v blocks. Thus, when $\mathcal{B}$ is represented as a (v, b, r, k, λ)-BIBD, we have $b = v$. Hence, the equation

$$bk \;=\; rv \qquad\qquad \text{Prop. 10.2.2(a)}$$

implies that $r = k$. Using that fact and the specification $\lambda = 1$, the equation

$$r\,(k-1) \;=\; \lambda\,(v-1) \qquad \text{Prop. 10.2.2(b)}$$

further implies that $v = k^2 - k + 1$. ♢

Example 10.4.2: The 9-point Pappus geometry is not a projective plane, since, for instance, the lines 012 and 345 do not meet. Some projective planes do satisfy the Theorem of Pappus, but some do not.

Example 10.4.3: The 10-point Desargues geometry is not a projective plane, since (as observed previously) there are pairs of points with no lines through them. Some non-Desarguesian projective planes exist, but most of the familiarly encountered projective planes do satisfy the Theorem of Desargues.

Duality Principle for Projective Planes

We observe that Axioms PP1 and PP2 are absolute duals of each other. The following proposition establishes a dual to Axiom PP3.

Prop 10.4.2. *In a projective plane $\mathcal{P}$, there exist four lines, no three of which contain the same point.*

Proof: By Axiom PP3, there exist four points 0, 1, 2, and 3, no three on the same line. By Axiom PP1, there exist lines 01, 12, 23, and 03, as shown in Figure 10.4.1.

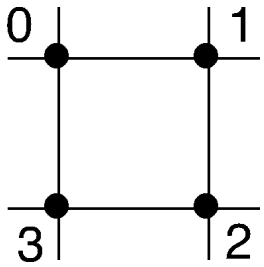

Fig 10.4.1 Proving the dual to Axiom PP3.

By Axiom PP2 none of these lines contains a third point from the set $\{0, 1, 2, 3\}$. Moreover, since among any three of these four lines, there are two with a common point in $\{0, 1, 2, 3\}$, it follows from Axiom PP2 that there cannot be some other point common to all three. ♢

Duality Principle. *The dual of a valid assertion about projective planes is also a valid statement about projective planes.*

Proof: Axioms PP1 and PP2 are dual to each other, and Proposition 10.4.2 is dual to Axiom PP3. ♢

Projective Planes as BIBD's

Lemma 10.4.3. *For any two distinct lines L and L' of a projective plane $\mathcal{P}$, there is a point x such that $x \notin L \cup L'$.*

Proof: Let y be the intersection of the lines L and L', let $0, 1 \in L - y$ and $2, 3 \in L' - y$, as shown in Figure 10.4.2.

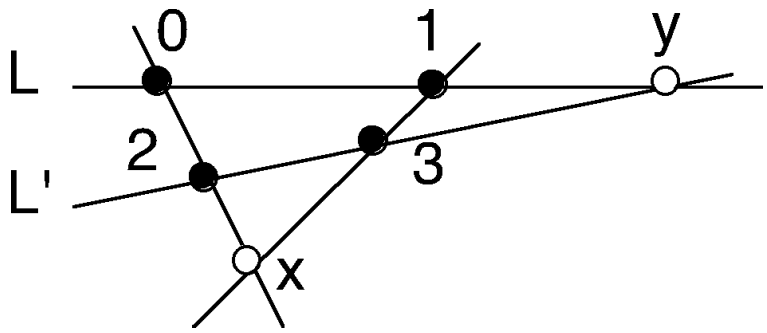

Fig 10.4.2 A point x not in the union of two lines.

Let x be the intersection of the lines 02 and 13. Since 0 is the unique interesction point of 02 and L, it follows that $x \notin L$. Since 3 is the unique interesection point of 13 and L', it follows that $x \notin L'$. ♢

Prop 10.4.4. *Any two lines of a projective plane $\mathcal{P}$ have the same number of points.*

Proof: Let L and L' be two distinct lines. By Lemma 10.4.3, there is a point $x \notin L \cup L'$. Now suppose that

$$L = \{y_0, \ldots, y_{k-1}\} \quad \text{with} \quad y_0 = L \cap L'$$

and that, for $j = 1, \ldots, k-1$, the intersection of the line xy_j with line L' is the point z_j, as in Figure 10.4.3.

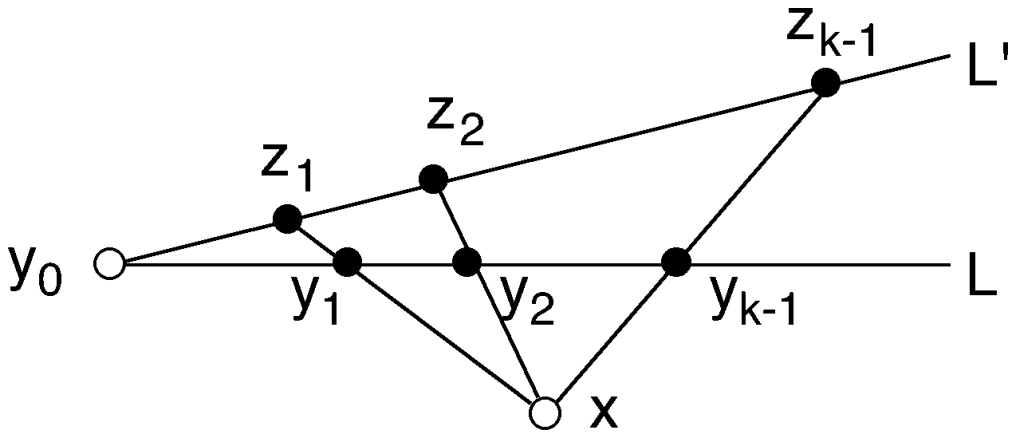

Fig 10.4.3 A bijection between two lines.

Then none of the points z_j, with $j = 1, \ldots, k-1$, coincides with y_0, because the lines L and xy_j meet only at y_j. If $z_j = y_0$, then line xy_j would also meet line L at y_0, which would be a second point in their intersection, since $y_j \neq y_0$. Moreover, if $i \neq j$, then the lines xy_i and xy_j are distinct, and then meet only at x. If $z_i = z_j$, then they would also meet there, contradicting Axiom PP2. Thus, the correspondence $y_i \mapsto z_i$ is a bijection of $L - y_0$ to $L' - y_0$. ♢

DEF: The ***order of a projective plane*** is defined to be one less than its blocksize as a design. (Significantly, the order is *not* defined to be the number of elements.)

Corollary 10.4.5. *In a projective plane of order n, every point lies on exactly $n+1$ lines.*

Proof: Using the definition of *order* just given, this assertion is simply the dual of Proposition 10.4.4. ♢

TERMINOLOGY: The set of all lines that meet at a point x of a projective plane is called the ***pencil of lines*** at x. (See Figure 10.4.4).

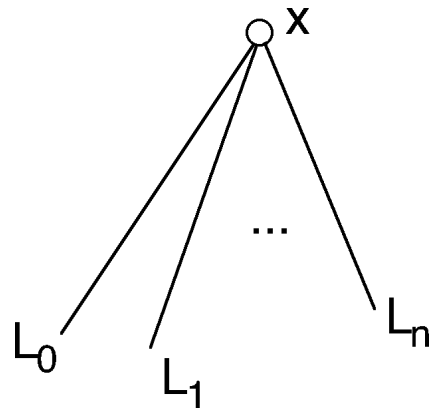

Fig 10.4.4 The pencil of lines at point x.

Proposition 10.4.6. *In a projective plane $\mathcal{P}$ of order n, the number of points is*

$$n^2 + n + 1$$

Proof: Let x be any point, and let

$$L_0, L_1, \ldots, L_n$$

be the pencil of lines that meets at x. Since every point of $\mathcal{P}$ lies on some line containing x, by Axiom PP1, the union of these lines is the entire domain of $\mathcal{P}$. Since no two of these lines intersect anywhere except x, by Axiom PP2, it follows that the number of points in $\mathcal{P}$ equals 1 for x plus n points on each of the $n+1$ lines unique to that line, that is,

$$1 + n(n+1) \;=\; n^2 + n + 1$$

points in all. ♢

Corollary 10.4.7. *In a projective plane $\mathcal{P}$ of order n, the number of lines is*

$$n^2 + n + 1$$

Proof: This is the dual of Proposition 10.4.6. ♢

Thm 10.4.8. *A projective plane of order n is a BIBD with parameters*

$$(v = n^2 + n + 1,\ b = n^2 + n + 1,\ r = n,\ k = n,\ \lambda = 1)$$

Proof: This summarizes the results above. ♢

Constructing Projective Planes

Much of the elementary theory of finite vector spaces is the same as for real vector spaces. The row-reduction algorithm is the key to establishing some additional facts to be used in the construction of some projective planes. After presenting some of the basics, we will use various such results from elementary linear algebra withour proof.

FROM APPENDIX A3:

- The *vector space* $\mathbb{Z}_p^3$, with p prime, is the set of triples (x_1, x_2, x_3) (called *points*) in $\mathbb{Z}_p$ under *vector addition*

  $$(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1+y_1, x_2+y_2, x_3+y_3)$$

  and *scalar multiplication*

  $$c(x_1, x_2, x_3) = (cx_1, cx_2, cx_3)$$

- A *line in the finite vector space* $\mathbb{Z}_p^3$ is the set of all scalar multiples of a non-zero point (x_1, x_2, x_3), i.e., the set

$$\{(0, 0, 0), (x_1, x_2, x_3), (2x_1, 2x_2, 2x_3), \ldots \\ \ldots, ((p-1)x_1, (p-1)x_2, (p-1)x_3)\}$$

Proposition 10.4.9. *Every non-zero point* (x_1, x_2, x_3) *of the vector space* $\mathbb{Z}_p^3$ *lies in a unique line of* $\mathbb{Z}_p^3$.

Proof: Certainly, (x_1, x_2, x_3) lies in the line comprising all of its own scalar multiples. Since the modulus p is prime, every non-zero scalar in $\mathbb{Z}_p$ is a multiple modulo p of any other scalar. It follows that any line containing (x_1, x_2, x_3) must be that same line. ♢

Corollary 10.4.10. *The number of lines in the vector space* $\mathbb{Z}_p^3$ *is* $p^2 + p + 1$.

Proof: Clearly, the number of non-zero points in $\mathbb{Z}_p^3$ is $p^3 - 1$. Since each line contains $p-1$ non-zero points, and since two distinct lines meet only at $(0, 0, 0)$, it follows from the Rule of Quotient (§0.3) that the number of lines is

$$\frac{p^3 - 1}{p - 1} = p^2 + p + 1$$ ♢

A *plane in the finite vector space* $\mathbb{Z}_p^3$ is the set of sums of the scalar multiples of two points not on the same line.

DEF: The ***projective geometry*** $PG(2,p)$ has for points the set of all lines of the vector space $\mathbb{Z}_p^3$ and for lines the set of all planes of $\mathbb{Z}_p^3$.

Example 10.4.4: In Fig 10.4.5, the seven points of the projective geometry $PG(2,2)$ are shown as lines through the origin 000 in Z_2^3.

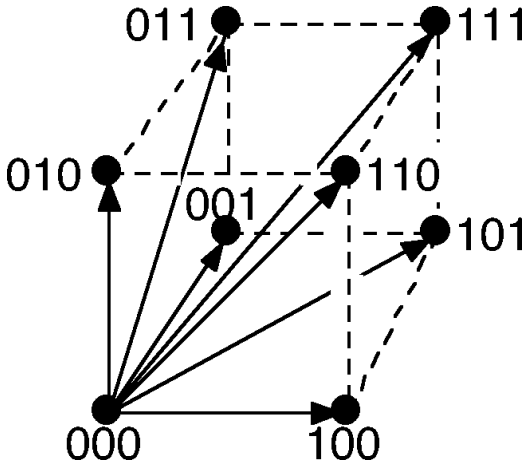

Fig 10.4.5 The projective geometry $PG(2,2)$.

Proposition 10.4.11. *The projective geometry $PG(2,p)$ is a projective plane of order p.*

Proof: Axiom PP1 holds because two distinct lines in the vector space $\mathbb{Z}_p^3$ determine a unique plane. Axiom PP2 holds because two distinct planes in $\mathbb{Z}_p^3$ meet in a line. Axiom PP3 holds because each combination of three of the following four vectors

$$(1,\,0,\,0)\quad(0,\,1,\,0)\quad(0,\,0,\,1)\quad(1,\,1,\,1)$$

lies on a line of $\mathbb{Z}_p^3$, is a linearly independent set, from which it follows that they and the lines they generate cannot all lie in the same plane of $\mathbb{Z}_p^3$. Hence, $PG(2,p)$ is a projective plane. Since a plane in $\mathbb{Z}_p^3$ has p^2-1 non-zero points and a line has $p-1$ non-zero points, it follows that the number of points in a line of $PG(2,p)$ is

$$\frac{p^2-1}{p-1} = p+1$$

Thus, its order as a projective plane is p. $\diamondsuit$

10.5 AFFINE PLANES

An *affine plane* is another kind of finite geometry. There is a close correspondence between affine planes and projective planes.

DEF: An ***affine plane*** $\mathcal{A}$ has a domain X, whose elements are called *points*, and a collection of subsets of X that are called *lines*, such that the following axioms hold:

AP1. For each pair of distinct points, there is exactly one line containing them.

AP2. For any given line L_i and any point x not on L_i there is a line through x that is parallel to L_i.

AP3. There exist four points, no three of which lie on the same line.

Example 10.5.1: The following geometry, seen previously in §10.3, is an affine plane called $AG(2,2)$. The name is explained later in this section.

	L_0	L_1	L_2	L_3	L_4	L_5
x_0	1	1	0	0	1	0
x_1	0	1	0	1	0	1
x_2	1	0	1	0	0	1
x_3	0	0	1	1	1	0

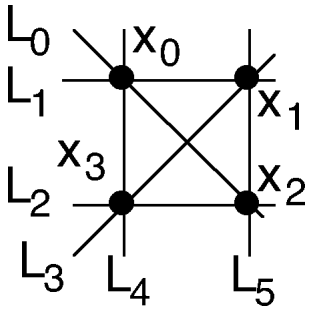

Fig 10.5.1 The affine plane AG(2,2).

Axioms AP1 and AP3 are easily verified for $AG(2,2)$ either from the incidence matrix or from the diagram. To verify Axiom AP2 from the drawing, one recognizes that lines L_0 and L_3 are parallel, in the sense of finite geometry, even though they cross each other in the drawing.

Example 10.5.2: The Fano plane is not an affine plane. In general, a projective plane has no pair of parallel lines. Thus, it cannot satisfy Axiom AP2.

Example 10.5.3: We observe that lines of the Pappus geometry can be partitioned into three cells of three lines each, as represented by the three columns to the left of Figure 10.5.2, such that within each cell, each point of the geometry occurs exactly once.

$$L = \left\{ \begin{array}{lll} 012, & 046, & 057 \\ 345, & 158, & 136 \\ 678, & 237, & 248 \end{array} \right\}$$

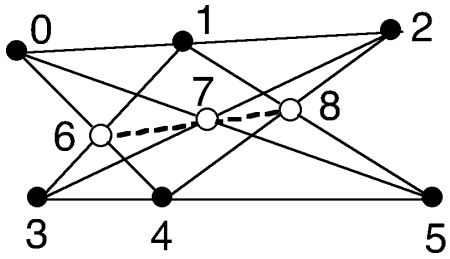

Fig 10.5.2 Resolving the geometry of Pappus.

If a point of the Pappus geometry does not lie on a given line, then it lies on another line in the same column as the given line, which is parallel to the given line. Thus, Axiom AP2 holds. However, the Pappus geometry does not satisfy AP1, so it is not an affine plane.

DEF: A ***resolvable geometry*** is a geometry whose lines can be partitioned into cells such that the lines within each cell partition the domain.

Prop 10.5.1. *A finite geometry satisfies Axiom AP2 if and only if it is resolvable.* ♢

The Affine Plane AG(2,p)

DEF: An ***affine line*** in the finite vector space $\mathbb{Z}_p^2$ is the set of p points produced by adding a fixed pair (c_1, c_2) to every point on a line of $\mathbb{Z}_p^2$,

$$K = \{(0,0),\ (x_1, x_2),\ (2x_1, 2x_2),\ \ldots,\ ((p-1)x_1, (p-1)x_2)\}$$

thereby obtaining a set of the form

$$L = \{(c_1, c_2),\ (x_1 + c_1, x_2 + c_2),\ (2x_1 + c_1, 2x_2 + c_2),\ \ldots \\ \ldots,\ ((p-1)x_1 + c_1, (p-1)x_2 + c_2)\}$$

This is conceptualized like adding a fixed vector to every point on a line through the origin in the real plane $\mathbb{R}^2$, thereby translating the line to a parallel line, as illustrated in Figure 10.5.3.

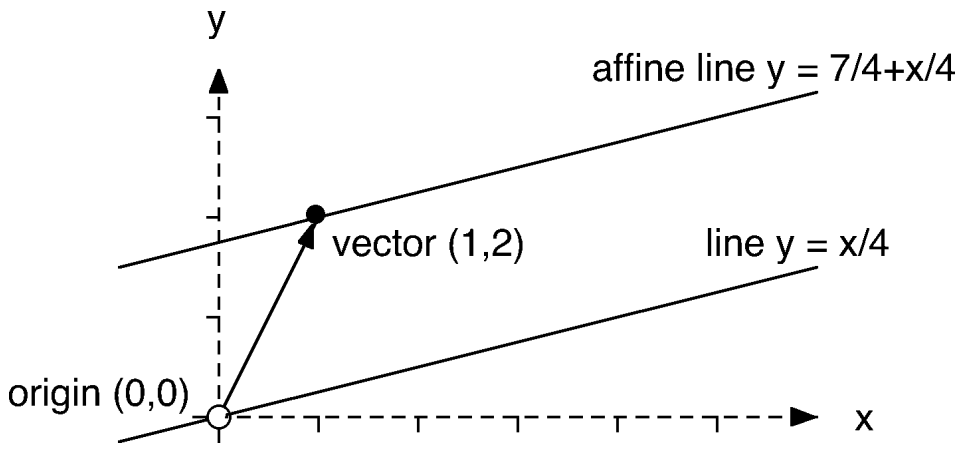

Fig 10.5.3 An affine line in the plane $\mathbb{R}^2$.

An alternative perspective is to choose numbers $a, b \in Z_p$ such that $ax_1 + bx_2 = 0$, so that the vector (a, b) is normal to the line K. Then the affine line L is the line normal to (a, b) that contains the point (c_1, c_2), i.e.,

$$L = \{(y_1, y_2) \mid ay_1 + by_2 = ac_1 + bc_2\}$$

Example 10.5.4: Adding the fixed pair $(1, 2)$ in $\mathbb{Z}_5^2$ to the line

$$K = \{(0, 0),\ (1, 3),\ (2, 1),\ (3, 4),\ (4, 2)\}$$

yields the affine line

$$L = \{(1, 2),\ (2, 0),\ (3, 3),\ (4, 1),\ (0, 4)\}$$

We observe that $3 \cdot 1 + 4 \cdot 3 = 0$ and that $3 \cdot 1 + 4 \cdot 2 = 1$, so the affine line L is also specifiable as the set of pairs (y_1, y_2) such that $3y_1 + 4y_2 = 1$.

DEF: The ***affine geometry*** $AG(2, p)$ is the geometry that has the points of the vector space $\mathbb{Z}_p^2$ and whose lines are the affine lines of $\mathbb{Z}_p^2$.

Example 10.5.5: In Fig 10.5.4, each of the four classes of parallel lines is represented by a different graphic – thin solid curve, thin dashed line, bold solid curve, and bold dashed line.

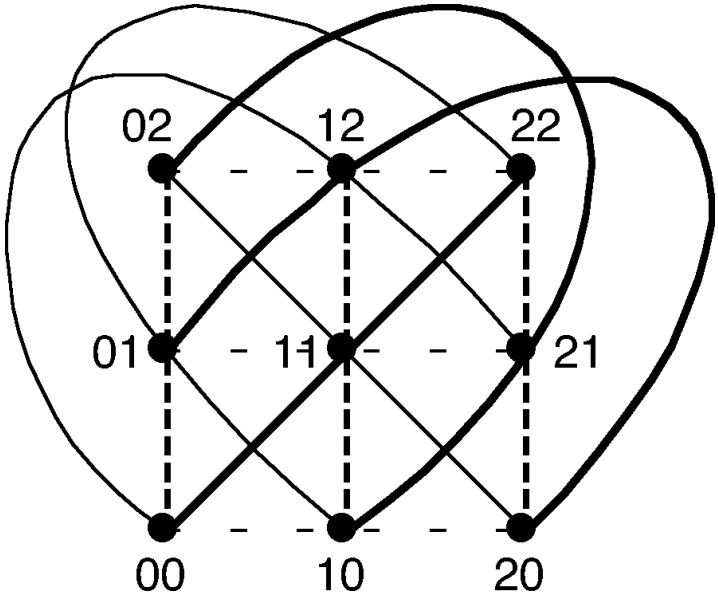

Fig 10.5.4 The affine geometry $AG(2,3)$.

It may be observed in Figure 10.5.4 that every affine line in $AG(2,3)$ has the same number of points – representing a common blocksize of $k = 3$ as a design, and that each pair of points occurs in exactly one affine line – representing a common index of $\lambda = 1$ as a design. These properties are verified shortly for every affine geometry $AG(2,p)$.

Proposition 10.5.2. *The affine geometry $AG(2,p)$ is an affine plane.*

Proof: (Axiom AP1): Given any two points (x_1, x_2) and (y_1, y_2) in $AG(2,p)$, the affine line

$$\{(x_1, x_2) + j\,(y_1 - x_1, y_2 - x_2) \mid j = 0, \ldots, p-1\}$$

contains both (x_1, x_2) (when $j = 0$) and (y_1, y_2) (when $j = 1$), and it is the only such affine line.

(Axiom AP2): Suppose that the affine line

$$L = \{(c_1, c_2) + j(x_1, x_2) \mid j \in Z_p\}$$

does not contain the point (y_1, y_2). Then the affine line

$$\{(y_1, y_2) + j(x_1, x_2) \mid j \in Z_p\}$$

is parallel to L and contains (y_1, y_2).

(Axiom AP3): No three of the points

$$(0,0), \quad (0,1), \quad (1,0), \quad \text{and} \quad (1,1)$$

lie on the same affine line in Z_p^2. ♢

Prop 10.5.3. *The affine plane $AG(2,p)$ is a $(p^2, p, 1)$-design, and, thus, a $(p^2, p^2+p, p+1, p, 1)$-BIBD.*

Proof: The number of points in $\mathbb{Z}_p^2$ is p^2, and thus the number of points in $AG(2,p)$ is p^2. Moreover, the number of points in every affine line in $\mathbb{Z}_p^2$, and, thus, in every line of $AG(2,p)$ is p. Since $AG(2,p)$ satisfies Axiom AP1, every pair of points of $AG(2,p)$ lies in exactly one line, so $\lambda = 1$. ♢

Affine Planes from Projective Planes

Suppose that a particular block B is deleted from a combinatorial design $\mathcal{B}$, and that each point of B is deleted from the domain. This is called a *restriction of*

the design $\mathcal{B}$ to the complement of block B. Then the incidence matrix of the resulting design can be obtained from the incidence matrix for design $\mathcal{B}$ by deleting column B and also deleting each row corresponding to an element of B.

Example 10.5.6: If we delete column L_0 and rows 1, 2, and 4 from the incidence matrix for the Fano plane

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 \end{array} \\ \left(\begin{array}{ccccccc} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \end{array}$$

then the resulting incidence matrix is

$$\begin{array}{c} \\ 0 \\ 3 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} L_1 & L_2 & L_3 & L_4 & L_5 & L_6 \end{array} \\ \left(\begin{array}{cccccc} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{array} \right) \end{array}$$

Referring back to Example 10.5.1, we recognize that the corresponding design is isom to the affine plane $AG(2,2)$.

Thm 10.5.4. *The geometry $\mathcal{G}$ resulting from restricting a projective plane $PG(2,p)$ to the complement of any given line L is an affine plane.*

Proof: By Axiom PP2, the line L intersects every other line of $PG(2,p)$ exactly once. Since every line of $PG(2,p)$ has $p+1$ points, it follows that every line of $\mathcal{G}$ has p points.

(Axiom AP1): Each pair of points of $PG(2,p)$ not on line L lies on exactly one line of $PG(2,p)$, by Axiom PP1. This implies that each pair of points of $\mathcal{G}$ lies on exactly one line.

(Axiom AP2): For each of the points $x_0, \ldots, x_p \in L$, the pencil of lines of $PG(2,p)$ meeting at x_j partitions $PG(2,p) - x_j$, by Axiom PP1. By Axiom PP2, none of the points on line L is on any line of this pencil other than line L. Thus, after x is deleted from the remaining lines of that pencil, the resulting subsets partition the set $PG(2,p) - L$, which is precisely the domain of the geometry $\mathcal{G}$. Thus, the lines of $\mathcal{G}$ can be partitioned into $p+1$ sets of p points each. In other words, $\mathcal{G}$ is a resolvable geometry, from which it follows (by Proposition 10.5.1) that it satisfies Axiom AP2.

(Axiom AP3): Choose the first two points w and x of the needed four from any line of $\mathcal{G}$. Then choose two other points y and z from any parallel line. Any subset of three points from this foursome must include either the pair w and x or the pair y and z. Since there is only one line through either pair, it follows from Axiom AP1 that no line can go through three of these points. $\diamondsuit$

Projective Planes from Affine Planes

Now suppose that the $p+1$ classes of parallel lines in $AG(2,p)$ are

$$C_0,\ C_1,\ \ldots,\ C_p$$

Suppose further that $p+1$ distinct new points

$$\infty_0,\ \infty_1,\ \ldots,\ \infty_p$$

are added to the domain of $AG(2,p)$, that the point ∞_j is added to each of the lines in class C_j, and that a new line

$$L_\infty\ =\ \{\infty_0,\ \infty_1,\ \ldots,\ \infty_p\}$$

is added.

TERMINOLOGY: We adopt the name *projective extension* for each artifact of the construction just described.

Theorem 10.5.5. *The geometry $\mathcal{G}$ resulting from projective extension of the affine plane $AG(2,p)$ is a projective plane.*

Proof: Since $AG(2,p)$ has p^2 points and p^2+p lines of p points each, the geometry $\mathcal{G}$ has p^2+p+1 points and p^2+p+1 lines of $p+1$ points each.

(Axiom PP1): If two points of the geometry $\mathcal{G}$ are already in $AG(2,p)$, then they are on some line of $AG(2,p)$, and accordingly, they lie on the extension of that line in $\mathcal{G}$. If the two points are ∞_i and ∞_j, then they lie on the line L_∞. If one point x is from $AG(2,p)$ and the other is ∞_j, then since each of class C_j partitions $AG(2,p)$, the point

x lies on some line of class C_j, and thus on the extension of that line in geometry $\mathcal{G}$.

(Axiom PP2): The line L_∞ evidently meets every other line of $\mathcal{G}$. Moreover, the intersection of two lines not in the same parallel class of $AG(2,p)$ is a single point, by Axiom $AP1$, from which it follows that their extensions meet only at that same point. If two lines of $AG(2,p)$ are in the same parallel class C_j, then their extensions meet only at ∞_j.

(Axiom PP3): If 4 points satisfy Axiom AP3 in $AP(2,p)$, then those same 4 points satisfy Axiom PP3 in $\mathcal{G}$. ♢

Example 10.5.7: Figure 10.5.5 shows how the projective plane $PG(2,3)$ with 13 points can be constructed by extending the 9-point affine plane $AG(2,3)$.

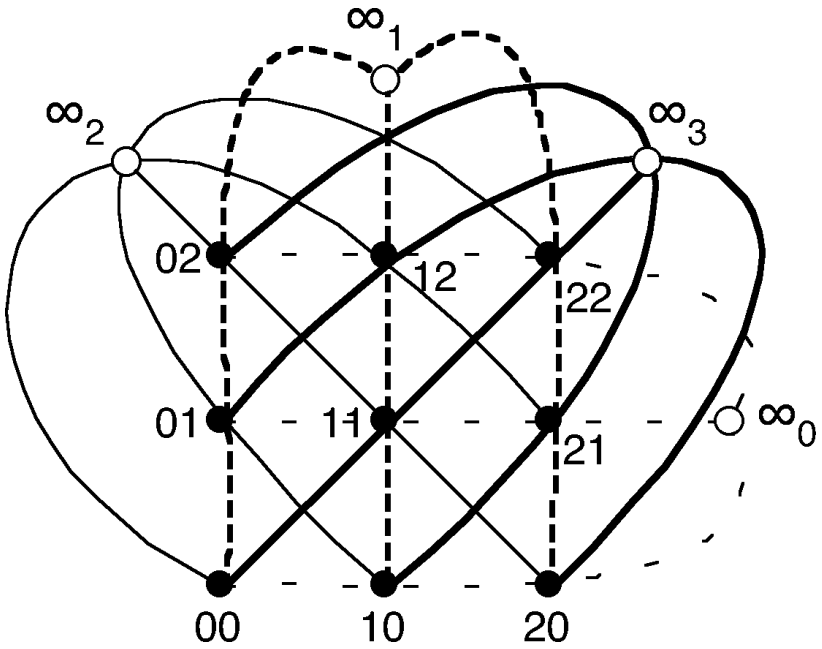

Fig 10.5.5 Extending $AG(2,3)$ to $PG(2,3)$.