Lecture 9-12: Discrete Geometry

Main points:

- **counting intersections and regions**: combinatorial method helps solving geometric problems
- **Carathéodory theorem and Happy Ending Theorem**: convexity in geometry, emergence in geometry, combinatorial and linear algebra method helps solving geometric problems.
- **Finite geometry, Fano plane, Coding**: Geometry helps solving combinatorial problems and has important applications such as in error-correcting codes.

The main theme of these lectures is to illustrate how combinatorial (and other tools such as linear algbera) helps solve discrete geometry problems, and vice versa, and they have important computer science applications.

1 Combinatorics helps Geometry 1: counting intersections and regions

1.1 Intersections of diagonals in a convex polygon

Ref. LPV 11.1

Examples of how combinatorial method helps solve geometry problems.

Question: In a convex polygon with n vertices, how many *interior* intersection points of diagonals?

illustrate with $n = 4, 5, 6$, one gets $1, 5, 15$, by actually counting them from the figures.

A: $\binom{n}{4}$. key observation: every 4 vertices uniquely determines an intersection point inside the convex polygon.

1.2 Counting regions

Ref. LPV 11.2

Definition 1. *A set of lines in the plane is said to be* in general position*, if no two are parallel, and no three intersect at the same point.*

A set of random lines is in general position with high probability.

Question: how many regions does a set of n lines in general position form?

Two proofs.

Pf1: the n-th line generates $n-1$ intersection points, with n new regions, so,

$$1 + 1 + 2 + \cdots + n = 1 + \frac{n(n+1)}{2}.$$

Pf2: If we view the problem *suitably* (all regions in a slightly tilted rectangle), we see that every region corresponds uniquely to its lowest point. This can be done as follows: firstly, we add a giant box so that all lines intersect the bottom line of the box, and the box contains all intersection points of two lines. Next, imagine all the lines including the boundary form a rigid structure, and we rotate the whole structure *suitably*, such that every region has a **unique** lowest point. Such a rotation is possible, is because the number of regions is finite, but the choices of rotations are infinite (in fact, uncountable), hence, there exists such a desired rotation. The above operation changes the original problem of counting the number of regions to the problem of counting the number of lowest points, which are of two types: $n+1$ on the bottom line of the rectangle, and $\binom{n}{2}$ intersection points by n lines. Hence, $1+n+\binom{n}{2}$.

One may check that

$$1+\frac{n(n+1)}{2}=1+n+\binom{n}{2}.$$

2 Combinatorics helps Geometry 2: from Carathéodory to Erdös–Szekeres Theorem (Happy Ending Theorem)

Definition 2. *Let $X \subseteq \mathbb{R}^2$ be a set of points in the plane. The convex hull* $\operatorname{conv}(X)$ *denotes the set of all points $y \in \mathbb{R}^2$ that can be written as a convex combination of some points in X, i.e., there exist k points $x_1, \ldots, x_k \in X$, such that,*

$$y=\sum_{i=1}^{k} a_i x_i, \tag{1}$$

where $0 \le a_i \le 1$, and $\sum_{i=1}^{k} a_i = 1$. The equation (1) *means that the point y is a* convex combination *of points $x_1, \ldots, x_k$.*

2.1 Carathéodory Theorem

Theorem 3 (Carathéodory)**.** *Let $X \subseteq \mathbb{R}^n$, then every point $v \in \operatorname{conv}(X)$ is a convex combination of at most $n+1$ points from X.*

证明. Since $v \in \operatorname{conv}(X)$, by definition, we know there are k points $x_1, \ldots, x_k \in X$, such that v is a convex combination of these k points,

$$v=\sum_{i=1}^{k} a_i x_i,$$

where $\sum_i a_i = 1$ and $0 < a_i < 1$.

If $k \le n+1$, then there is nothing prove.

So, suppose $k \ge n+2$. We will show that v is a convex combination of $k-1$ points. If this is true, then we can repeat this process, each time reducing the number of points in the convex combination, and finally reach a set of $n+1$ points as desired.

So, now we show that, if $k \geq n+2$, then v is a convex combination of $k-1$ points. Consider the $k-1 \geq n+1$ vectors:

$$x_2 - x_1, \ldots, x_k - x_1.$$

These are at least $n+1$ vectors of dimension n. By linear algebra, we know these $k-1$ vectors must be linearly dependent, i.e.,

$$\sum_{j=2}^{k} b_j (x_j - x_1) = 0,$$

for some $b_2, \ldots, b_k \in \mathbb{R}$, and not all of $b_2, \ldots, b_k$ are 0. Rewriting this equation we get

$$\left(-\sum_{j=2}^{k} b_j \right) x_1 + \sum_{j=2}^{k} b_j x_j = 0.$$

If we let $\beta_1 = -\sum_{j=2}^{k} b_j$ and $\beta_j = b_j$ for $j \geq 2$, then,

$$\sum_{i=1}^{k} \beta_i x_i = 0.$$

Note that $\sum_{i=1}^{k} \beta_i = 0$, and not all β_i are 0. Hence, there must be some β_i that are strictly positive. Consider those β_i, and let

$$\gamma = \min\{\frac{a_i}{\beta_i} : \beta_i > 0\} > 0.$$

Without loss of generality, assume $\gamma = \frac{\alpha_k}{\beta_k}$. For every $1 \leq i \leq k$, we have

$$c_i = a_i - \gamma \beta_i \geq 0.$$

Indeed, since $\gamma > 0$, if $\beta_i \leq 0$, the above holds. Otherwise, if $\beta_i > 0$, the definition of γ ensures that the above inequality also holds. Furthermore, we have

$$c_k = a_k - \gamma \beta_k = 0.$$

Let's look at

$$v = v - \gamma \cdot 0 = \sum_{i}^{k} (a_i - \gamma \beta_i) x_i = \sum_{i}^{k-1} c_i x_i.$$

We already know $c_i \geq 0$. We continue to show that $\sum_{i=1}^{k-1} c_i = 1$. If this is true, then v is a convex combination of points $x_1, \ldots, x_{k-1}$, as we wanted.

To verify $\sum_{i=1}^{k-1} c_i = 1$, since $c_k = 0$, we compute

$$\sum_{i=1}^{k-1} c_i = \sum_{i=1}^{k} c_i = \sum_{i=1}^{k} a_i - \gamma \sum_{i=1}^{k} \beta_i = 1 - \gamma \cdot 0 = 1.$$

This finishes the proof. $\square$

If $n = 2$, Carathéodory's theorem implies that any point v in a convex hull of X is a convex combination of at most 3 points, in other words, v will lie inside some triangle whose 3 vertices are from X.

To appreciate Carathéodory's theorem, let us define the notion of *convex independence*.

Definition 4. *A set of points X in $\mathbb{R}^n$ is* convex independent *if no $v \in X$ lies in the convex hull of $X - \{v\}$. Otherwise, we say X is* convex dependent.

Geometrically, in the plane $\mathbb{R}^2$, a set of k convex independent points corresponds to the set of vertices of a convex k-gon. Clearly, we can have arbitrary large (finite) set of convex independent points in $\mathbb{R}^2$, for example, arrange them on the circle.

Question: Suppose there is a large set of m points (m being quite large, say 100) in $\mathbb{R}^2$, how to test whether these points are convex independent?

By definition, one can check this by checking, for every point x in the set, whether x can be written as a convex combination of other points. This requires solving linear equation (1) to find out whehter it has a solution. So, if $m = 100$, we need to solve 100 equations, each has 99 variables.

Carathéodory's theorem offers an alternative method.

Corollary 5. *Let $S \subseteq \mathbb{R}^n$ be a finite set of points. Then, S is convex independent iff every subset of $n + 2$ points of S is convex independent.*

In particular, for $n = 2$, a set S of points in the plane $\mathbb{R}^2$ is convex independent iff every 4 points of S is convex independent.

证明. $\Longrightarrow$: obvious.

$\Longleftarrow$: we prove by contradiction. Assume not, then S is convex dependent. So, there is $v \in S$, such that v is a convex combination of other points in S. By Carathéodory's theorem, v is a convex combination of at most $n + 1$ points from S. Hence, together these $n + 2$ points form a set of points that is convex dependent. But, the condition says that every subset of S of $n + 2$ points is convex independent, which is a contradiction. $\square$

Hence, to test 100 points in $\mathbb{R}^2$ whether they are convex independent, by Corollary 5, we would need to solve $\binom{100}{4}$ equations, each having 3 variables only. This means we have many more equations to solve, however, each equation is much easier to solve since it has only 3 variables!

In other words, Carathéodory's theorem implies that test whether a set of points is convex independent, is a **local property**: as long as we know that convex independence holds "locally" (i.e., subsets of 4 points are convex independent), we know the convex independence also holds "globally" (i.e., for the whole set of 100 points). This type of reduction of testing a global property to testing a local property is very useful in property-testing related tasks in computer science.

2.2 Erdös–Szekeres Theorem (Happy Ending Theorem)

Ref. LPV 11.3

Next, we discuss a famous so-called Happy Ending Theorem by Erdös–Szekeres, which can be viewed, similar to Ramsey theorem, as emergence phenomenon in geometry, in this case, that when a set of points is large enough, it must contain k points that are convex independent.

Theorem 6 (Erdös–Szekeres Theorem, Happy Ending Theorem)**.** *In $\mathbb{R}^2$, for every k, there is some number $ES(k)$, such that any set of at least $ES(k)$ points in general position, must contain k convex independent points, in other words, must contain k points that form a convex k-gon.*

For example, when $k = 3$, it is easy to see that 3 points in general position (so, the three points are not in the same line) must form a triangle.

Show (by case analysis): 5 points in the plane in general position must contain 4 points form a convex quadrilateral.

表 1: Erdös–Szekeres numbers for small k.

k	2	3	4	5	6	7
$ES(k)$	2	3	5	9	17	33?

Erdös–Szekeres [1] in 1935 showed that $2^{k-2} + 1 \le ES(k) \le \binom{2k-4}{k-2} + 1$. The upper bound was only improved very recently, firstly in a breakthrough paper in year 2017 by Suk [6] to $2^{k+O(k^{2/3}\log k)}$, and then in 2020 Holmsen et al [2] to $2^{k+O(\sqrt{k\log k})}$.

Open Problem 7. *Erdös–Szekeres Conjecture: $ES(k) = 2^{k-2} + 1$.*

Since the Happy ending theorem and Ramsey theory are in the same spirit, one cannot help but thinking they must have some connection. Indeed, below, we show how Carathéodory's theorem together with Ramsey theory can be combined to prove $ES(k)$ is finite.

We need the following "hypergraph Ramsey number".

Lemma 8. *For every natural number $p, q \in \mathbb{N}$, there exists a finite number $R_4(p, q) \in \mathbb{N}$ such that for any number $N \ge R_4(p, q)$, any coloring of 4-subsets of $\{1, 2, \ldots, N\}$ by two colors red and blue, the following is true:*

- *either there is a subset $S \subseteq \{1, 2, \ldots, N\}$ of size $|S| = p$, such that all 4-subsets of S are colored red,*
- *or, there is a subset $T \subseteq \{1, 2, \ldots, N\}$ of size $|T| = q$, such that all 4-subsets of T are colored blue.*

Proof of Theorem 6. We already know for $k = 4$ one has $ES(4) = 5$, so we assume $k > 4$, i.e., $k \ge 5$.

We show $ES(k) \le R_4(k, k)$, hence, $ES(k)$ is finite. Let $N = \max\{R_4(k, k), 5\} \ge 5$. Consider a set $X \subseteq \mathbb{R}^2$ of N points in general position. We number these N points by numbers $1, 2, \ldots, N$, hence, we can identify $X = \{1, 2, \ldots, N\}$.

Consider the following coloring of 4-subsets of $\{1, 2, \ldots, N\}$, let $A = \{a, b, c, d\} \subseteq X$ be a set of 4 points:

(1) if the 4 points a, b, c, d form a quadrilateral (or equivalently, are convex independent), color A by red;

(2) otherwise, color A by blue.

By Lemma 8, one of two cases will happen. We show the second case can not happen. Suppose the second case does happen, i.e., there is a set $T \subseteq X$ of size $|T| = k \geq 5$ such that all 4-subsets of T are colored blue. However, since $ES(4) = 5$, we know that T must contain 4 points that form a quadrilateral, hence, this 4-point-subset should be colored red, a contradiction.

Hence, the first case of Lemma 8 must happen. That is, there must be a set S of k points such that every 4-subset of S is colored red, i.e., every subset of 4 points of S is convex independent. By Corollary 5, this implie S itself must be convex independent. In other words, S is a set of k points that form a k-gon as desired. $\square$

3 Geometry helps combinatorics: Finite geometry and Error Correcting Codes

Ref: LPV-14.1, 14.6

3.1 Finite geometry: small exotic worlds

3.1.1 Fano plane

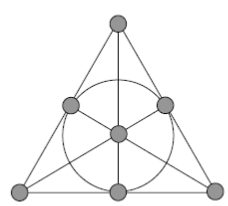


图 1: The Fano plane.

Fano plane property:

- 9 points; 7 lines
- every line consists of 3 points;
- any two points determine uniquely one line;
- every two lines intersect at one unique point;
- every point lies in exactly 3 lines.

3.1.2 Tictactoe plane

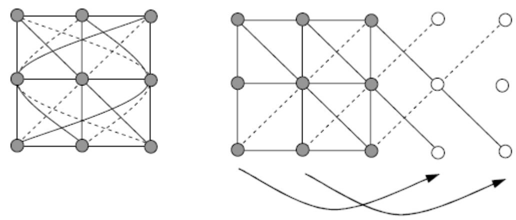


图 2: The Tictactoe plane.

Tictactoe plane: 9 points, every line consists of 3 points

- 9 points; 12 lines;
- every line consists of 3 points;
- any two points determine uniquely one line;
- two lines may intersect at one unique point, or may be parallel (non-intersecting)
- every point lies in exactly 4 lines.

3.1.3 Cube Space

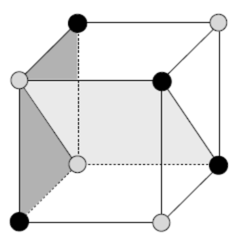


图 3: The Cube Space.

The cube space:

- 8 points;
- $\binom{8}{2} = 28$ lines: any 2 points determine a line, every line contains exactly two points
- 14 planes: (1) 4-tuples of points forming a face of the cube (there are 6 of them); (2) 4-tuples of points on two opoosite edges of the cube (6 of them); (3) the four black points; (4) the four light points
- any three lines determine uniquely a plane, hence $\binom{8}{3}/\binom{4}{3} = 56/4 = 14$ planes

- every plane consists of exactly 4 points, hence, contains exactly $\binom{4}{2} = 6$ lines
- every line lies in exactly 3 planes.

  For example, we can double count the (P, L) pairs, where P represents a plane and L is a line whose two points belong to the plane. How many such pairs?

  Counting by planes, since each plane contains 6 lines, we have $14 \times 6 = 84$.

  Counting by lines, suppose each line lies in x planes, then it is $x \times 28$.

  Hence, $x = 84/28 = 3$.
- every point belongs to 7 lines (again you can do double counting)
- every point lies in exactly 7 planes (by double counting, try it yourself).

  Exercise: Can you identify the 7 planes for the left bottom black point?

3.1.4 Summary

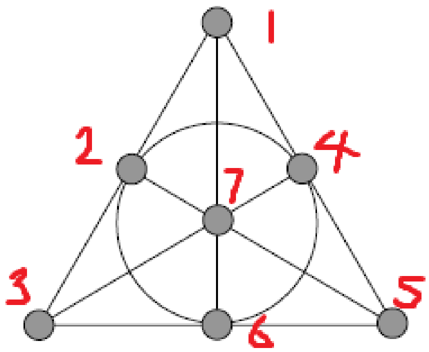
	#points, n	#lines/planes, b	line/plane contains #pts, k	point in #lines/planes, r	two points in #lines/planes, λ
Fano plane	7	7	3	3	1
Tictactoe plane	9	12	3	4	1
Cube Space	8	14	4	7	3

表 2: Summary of the finite geometry.

sanity check: column 1 $\times$ column 4 = column 2 $\times$ column 3, because of double counting

A helpful view of looking at these finite geometries is to view them as matrices. Consider Fano plane for an example, every line is a subset of 3 points, hence we can view a line as a vector in $\{0, 1\}^7$, where 1's correspond to the points in the line. We write each line as a row vector and put them together as a matrix, we get a 0/1 matrix of size 7×7, as shown in Figure 4. Such matrices are called *incidence matrices*, because they represent the incidence relation between points and lines(or planes). In general, for Tictactoe plane and Cube space, we get $b \times n$ matrices.

Observe that in the Fano incidence matrix, every row has exactly three 1's, and every column has exactly three 1's, as expected.

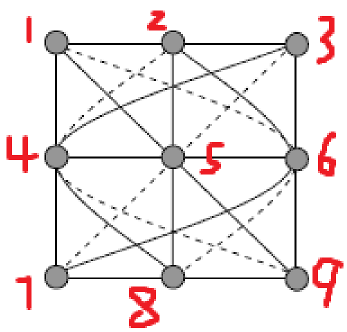


(a) The Fano plane with labels

$$A = \begin{array}{cc} & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{array}{c} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \end{array} & \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

(b) Incidence matrix

图 4: The Fano plane with labels, giving its incidence matrix.

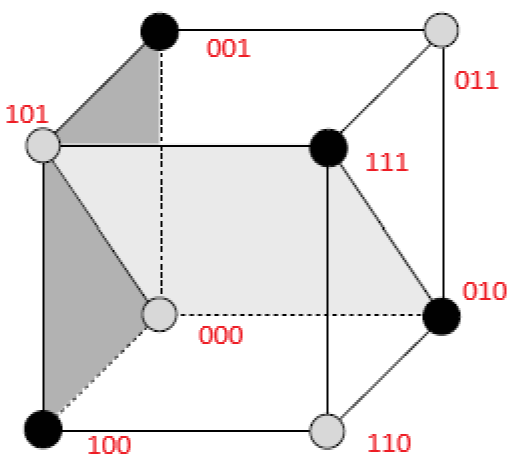


(a) The Tictacto plane with labels

$$A = \begin{array}{cc} & \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{array}{c} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \\ \ell_5 \\ \ell_6 \\ \ell_7 \\ \ell_8 \\ \ell_9 \\ \ell_{10} \\ \ell_{11} \\ \ell_{12} \end{array} & \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

(b) Incidence matrix

图 5: The Tictacto plane with labels, giving its incidence matrix.



(a) The Cube space with labels

	000	001	010	011	100	101	110	111
$x = 0$	1	1	1	1	0	0	0	0
$x = 1$	0	0	0	0	1	1	1	1
$y = 0$	1	1	0	0	1	1	0	0
$y = 1$	0	0	1	1	0	0	1	1
$z = 0$	1	0	1	0	1	0	1	0
$z = 1$	0	1	0	1	0	1	0	1
$x + y = 0$	1	1	0	0	0	0	1	1
$x + y = 1$	0	0	1	1	1	1	0	0
$x + z = 0$	1	0	1	0	0	1	0	1
$x + z = 1$	0	1	0	1	1	0	1	0
$y + z = 0$	1	0	0	1	1	0	0	1
$y + z = 1$	0	1	1	0	0	1	1	0
$x + y + z = 0$	1	0	0	1	0	1	1	0
$x + y + z = 1$	0	1	1	0	1	0	0	1

(b) Incidence matrix

图 6: The Cube space with labels, giving its incidence matrix. Note that the planes corresponds to solutions of the linear equations where the addition is modulo 2, i.e., $1 + 1 = 0$.

3.2 Application to block design

Example 9. *Suppose a society has n citizens, citizens can form clubs. In an ideal society with absolute equality, one would like the following:*

- *if some club has 10000 members, while all other clubs have at most 100 members, then the big club clearly also has larger influence to the society than the smaller club. Hence, every club should have equal size.*
- *Suppose there is one person X joining 100 clubs, but other people only join at most 10 clubs. Clearly, X will have much larger influence than other people. The society would like to avoid such situation, so, each citizen should appear in equal number of clubs;*
- *Similary, if there are two people X and Y who join together in 50 clubs, but all other pairs of two people join at most 7 clubs, then, again, X and Y as a group of two people will together have much more influence than any other pair of two people. Hence, every pair of citizens should appear jointly in equal number of clubs.*
- *and so on...*

Clearly, these will put constraints on how clubs can be formed.

Questions as above are called **block design**. In general, block design has the following parameters:

- a set of n elements, (e.g., the set of all citizens in the society)
- a family of k-element subsets, each subset is called a block (e.g., each club is a block)
- every element appears in exactly r blocks
- every pair of elements appears jointly in exactly λ blocks

Then, the block design question is: does there exist such family of k-subsets, and if so what is it?

Let b denote the number of k-element subsets in the block design satisfying the above conditions. Clearly, by double counting (k-subset, element) pairs, we must have

$$bk = nr. \tag{2}$$

By double counting (k-subset, x, y) where x and y jointly appears in the k-subset, we have

$$b\binom{k}{2} = \binom{n}{2}\lambda.$$

Expand it we have $bk(k-1) = n(n-1)\lambda$, using $bk = nr$ we obtain

$$r(k-1) = (n-1)\lambda. \tag{3}$$

What we have shown is that conditions (2) and (3) are *necessary* conditions for block design, but they are not *sufficient*.

Next, we prove one more necessary condition, called Fisher's inequality.

Proposition 10 (Fisher's inequality)**.** $b \geq n$.

证明. We will take the incidence matrix view and apply **linear algebra** (recall we have used linear algebra in proving Carathéodory theorem).

Here, we view each subset as a 0/1 vector as a row of the matrix, hence, we have b rows. Every column is labelled by an element from the ground set, so, we have n columns. Let $M_{b\times n}$ denote the incidence matrix (as we illustrated for finite geometries previously). Observe that,

- every column has exactly r many 1's,
- every row contains exactly k many 1's,
- every two different columns have exactly λ many common 1's.

This implies that

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

Note that $M^T M$ is an $n \times n$ matrix. Because we must have $r > \lambda$, hence, the matrix $M^T M$ has full rank, i.e., $\text{rank}(M^T M) = n$. However, we know that $\text{rank}(M^T M) \leq \text{rank}(M) \leq b$. Therefore, $b \geq n$. □

In Table 2, one can check that Fano plane, Tictactoe plane, and cube space all give some special cases of block design for the following parameters. In the Fano plane and Tictactoe plane, each line is a block. In the cube space, each plane is a block. The corresponding parameters are for column 1, 2, 3, 4, 5 are respectively: n, b, k, r, λ. It is easy to check that (2), (3), and Fisher's inequality all hold in Table 2.

3.2.1 Steiner systems

Block design with $\lambda = 1$ are called **Steiner systems**. We have seen that Fano plane and Tictactoe plane are both Steiner systems with $k = 3$, but cube space is not. In previous block design, there is in fact also a paramete t, namely we require every t-subset appears in exactly λ times in the k-subsets. In previous examples we always have $t = 2$. But, of course sometimes one needs to consider consider larger t.

In general, Steiner systems require every t-subset appears exactly once in the family of k-subsets (namely, $\lambda = 1$). Fano plane and Tictactoe plane shows that there are Steiner systems for $t = 2$. Scientists have found examples of Steiner systems for $t = 3, 4, 5$, however, it was a longstanding open problem about whether there exists Steiner system for $t \geq 6$. This was solved only in recent years by breakthrough work of Peter Keevash [3, 4].

Block design and Steiner systems have applications in coding theory (error-correcting codes), experimental design, software testing etc, where the combinatorial properties of the design provide optimal or near-optimal solutions to practical problems.

3.3 Application to error correcting codes

Ref: LPV 14.6

key points:

- the channels to send bits are often noisy (i.e., receiver can get different bits from sender's), hence, we need encoding, in other words, to send n bits we will in fact send $n + f(n)$ bits, using these extra $f(n)$ bits to help the receiver to detect, and hopefully even correct, errors in received string. Obviously, we would like $f(n)$ small compare to n.

- common examples: repetition code, parity check code.

- Error-detecting codes: a method of encoding such that if upto k errors happened during transmission, then the receiver can detect the received string is not the correct string, however, the receiver might not be able to recover the original bits.

  For example: parity check code ($f(n) = 1$) is 1 error-detecting.

- Error-correcting codes: a method of encoding such that if upto k' errors happened during transmission, then the receiver can detect and correct the errors, that is, the receiver can recover the original string of bits sent by the sender.

  For example: suppose we encode 0 by 00000000, and 1 by 11111111 (i.e., repeat 8 times, $n = 1$ and $f(n) = 7$). This code is 7 error-detecting, and is 3 error-correcting. For example, if we know the channal can cause at most 3 error bits, then, if the receiver received 0100110, then, we know the original bits is 00000000, i.e., the send is sending the bit 0.

- Fano plane: the code is of length 7, every line in the plane provides two codewords: one in which the 3 points of the line all get 1, the other being the 3 points of the line all get 0. Hence, there are $7 \times 2 = 14$ codewords (i.e., these are simply the rows of the Fano plane incidence matrix, and the rows obtained by flipping the 0 and 1 of the matrix). We also add the all 0 and all 1 strings, hence, we get a code with $14 + 2 = 16$ codewords, each of length 7.

  Fano plane code is 3 error-detecting, and 1 error-correcting.

- Cube space: the code is of length 8, each plane gives a codeword: the 4 points in the plane all get 1 and the rest get 0, this gives 14 codewords (i.e., these are the rows of the Cube space incidencec matrix), we also add all 0 and all 1 strings, hence in total we get a coding of $14+2 = 16$ codewords, each of length 8.

Cube space code is 3 error-detecting, and 1 error-correcting.

> The codes we derived from the Fano plane and the Cube space are special cases of a larger family of codes called *Reed–Müller codes*. These are very important in practice. For example, the NASA Mariner probes used them to send back images from the Mars. Just as the Cube Code was based on 2-dimensional subspaces of a 3-dimensional space, the code used by the Mariner probes were based on 3-dimensional subspaces of a 5-dimensional space. They worked with blocks of size 32 (instead of 8 as we did), and could correct up to 7 errors in each block. The price was, of course, pretty stiff: There were only 64 codewords used, so to safely transmit 6 bits, one had to package them in 32 bits. But of course, the channel (the space between Earth and Mars) was very noisy!
>
> Error-correcting codes are used all around us. Your CD player uses a more sophisticated error-correcting code (called the Reed–Solomon code) to produce a perfect sound even if the disk is scratched or dusty. Your Internet connection and digital phone use such codes to correct for noise on the line.

图 7: Citing from [5]: Important Application of Error Correcting Codes.

中国数学家的贡献

Constantin Carathéodory的一位女学生徐瑞云（1915年6月－1969年1月），是中国第一位女数学博士。在Carathéodory的指导下于德国获得博士学位后，徐瑞云回国工作，为中国的分析学做出了奠基性的贡献，并培养了许多杰出的数学家。

陆家羲（1935年6月10日—1983年10月31日）在施泰纳系(Steiner system)等问题中也做出了重要贡献。

参考文献

[1] Paul Erdös and George Szekeres. A combinatorial problem in geometry. *Compositio mathematica*, 2:463–470, 1935.

[2] Andreas F Holmsen, Hossein Nassajian Mojarrad, János Pach, and Gábor Tardos. Two extensions of the erdős–szekeres problem. *Journal of the European Mathematical Society (EMS Publishing)*, 22(12), 2020.

[3] Peter Keevash. The existence of designs. *arXiv preprint arXiv:1401.3665*, 2014.

[4] Peter Keevash. A short proof of the existence of designs. *arXiv preprint arXiv:2411.18291*, 2024.

[5] László Lovász, József Pelikán, and Katalin Vesztergombi. *Discrete mathematics: elementary and beyond*. Springer Science & Business Media, 2003.

[6] Andrew Suk. On the erdős-szekeres convex polygon problem. *Journal of the American Mathematical Society*, 30(4):1047–1053, 2017.