

MAD 6206 - Combinatorics

Jay Pantone
University of Florida

Last Edited: September 1, 2013

Contents

1	Course Notes	1
1.1	Introduction	1
1.2	Chapter 3 - Subsets, Partitions, Permutations	2
1.2.1	Subsets	2
1.2.2	The Binomial Theorem	3
1.2.3	Permutations	3
1.2.4	Estimates for Factorials	4
1.2.5	Selections	6
1.2.6	Cayley's Theorem	6
1.2.7	Bell Numbers	7
1.2.8	Combinatorial Generation	8
1.3	Chapter 5 - The Principle of Inclusion-Exclusion	11
1.3.1	PIE	11
1.3.2	A Generalization	13
1.3.3	Stirling Numbers	15
1.3.4	Even & Odd Permutations	17
1.4	Chapter 6 - Latin Squares and SDRs	19
1.4.1	Latin Squares	19
1.4.2	SDRs	19
1.4.3	How Many Latin Squares?	21
1.4.4	Quasigroups and Groups	22
1.4.5	Orthogonal Latin Squares	24
1.4.6	Direct Products	25
1.5	Chapter 7 - Extremal Set Theory	27
1.5.1	Intersecting Family of Sets	27
1.5.2	Sperner Families (Antichains)	28
1.5.3	The de Bruijn-Erdős Theorem	29
1.6	Chapter 8 - Steiner Triple Systems & Design Theory	31
1.6.1	Steiner Systems	31
1.6.2	A Direct Construction	33
1.6.3	A Recursive Construction	35
1.7	Chapter 9 - Finite Geometry	38
1.7.1	Linear Algebra over Finite Fields	38
1.7.2	Gaussian Coefficients	38
1.7.3	Projective Geometry	41
1.8	Chapter 10 - Ramsey Theory	47
1.8.1	The Pigeonhole Principle	47
1.8.2	Ramsey's Theorem	48
1.8.3	Applications of Ramsey's Theorem	52
1.8.4	Infinite Ramsey's Theorem	53
1.9	Chapter 12 - Posets, Lattices, Matroids	55
1.9.1	Posets and Lattices	55

1.9.2	Linear Extensions of a Poset	55
1.9.3	Distributive Lattices	58
1.9.4	Dimension Posets	61
1.9.5	The Möbius Function of a Poset	63
1.10	Chapter 13 - More on Partitions and Permutations	68
1.10.1	Partitions, Diagrams, and Conjugacy Classes	68
1.10.2	Tableaux	70
1.11	Chapter 15 - Enumeration Under Group Action	72
1.11.1	Definition of a Group	72
1.11.2	Pölya Counting	73
	Index	78

This packet consists of notes, homework assignments, and exams, from MAD6206 Combinatorics taught during the Fall 2012 semester at the University of Florida. The course was taught by [Professor Vince Vatter](#). The notes for the course follow *Combinatorics*, by Peter Cameron. Numbering in these notes corresponds to the numbering in the text.

If you find any errors or you have any suggestions, please contact me at jay.pantone@gmail.com.

Chapter 1

Course Notes

1.1 Introduction

We present an example of a simple problem which has not been proved. This illustrates how combinatorial problems can be deceptively difficult.

Erdős-Szekeres Conjecture: (1935) Any collection of $2^{n-2} + 1$ points in the plane (in general position, i.e., no three are collinear) contains a convex n -gon.

In the case $n = 3$, the proof is obvious. For $n = 4$, we consider sets of 5 points. Let X be a set of 5 points in general position. Let H denote the convex hull of X (connect the points, fill in the middle). We have three subcases.

Case 1: 5 points of X lie on the boundary of H . In this case, pick any 4 points.

Case 2: 4 points of X lie on the boundary of H . Use these 4 points to form the convex 4-gon.

Case 3: 3 points of X lie on the boundary of H . Pick the two points inside. Draw the line between them, and then two boundary points (out of the three) will lie on one side of that line. Use these four points.

The $n = 5$ case was proved in 1970. The $n = 6$ case was proved in 2006 with a computer. Remaining cases are unsolved.

1.2 Chapter 3 - Subsets, Partitions, Permutations

1.2.1 Subsets

Notation: $[n] := \{1, 2, \dots, n\}$.

Question: How many subsets of $[n]$ are there?

Answer: 2^n

Question: How many subsets of $[n]$ have k elements?

Answer: $\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$

This quantity is described as “ n choose k ”.

To see this using the formula on the right, the numerator gives us the number of ways to pick k elements in which order matters, then we divide by $k!$ to not count the same set of elements with a different order multiple times.

Some Binomial Identities:

$$\binom{n}{k} = \binom{n}{n-k}$$

Choosing a k -subset is the same thing as choosing the complement $(n-k)$ -subset.

$$k \binom{n}{k} = n \binom{n-1}{k-1}$$

The left-hand side represents picking a k -subset and selecting one element. The right-hand side represents picking an element and then a $(k-1)$ -subset of the remaining elements.

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

The k -subsets of $[n+1]$ can be split into two groups: those which contain $n+1$ and those which don't. If a k -subset contains $n+1$, you need $k-1$ more elements (first summand). If it doesn't, you need k more elements (second summand).

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

Both sides count the number of subsets of $[n]$.

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$$

The left-hand side counts the number of ways for each k to pick an n -subset by picking a k -subset from n elements and a $(n-k)$ -subset for a different n elements. Summing these, we get the number of ways to pick n from $2n$, which is the right hand side.

1.2.2 The Binomial Theorem

Binomial Theorem: For integers n ,

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$$

Proof: Expand the left hand side:

$$\underbrace{(1+x)(1+x)\cdots(1+x)}_{n \text{ times}}$$

The coefficient of x^k here is $\binom{n}{k}$ because the only way to get an x^k is by picking k of the x 's out of the n possible, and the number of ways to do this is $\binom{n}{k}$. \square

Proposition: For $n > 0$, the number of subsets of $[n]$ of even and odd size are equal.

Proof: Set $x = -1$ in binomial theorem. \square

1.2.3 Permutations

Definition: A permutation of X is a bijection from X to itself. Usually we will use $X = [n]$.

Notation: There are three ways to write a permutation.

(1) "passive representation" or "one-line notation":

$$(\pi(1), \pi(2), \dots, \pi(n))$$

(2) "two-line notation":

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

(3) "cycle notation"

$$(x_1 \ x_2 \ \cdots \ x_m) \text{ means } x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_m \rightarrow x_1$$

Warning: In the textbook, permutations act on the right, i.e.,

$$x\pi := \pi(x)$$

and

$$\pi\sigma \text{ means apply } \pi \text{ first, then } \sigma.$$

Additionally, we have the associativity

$$x(\pi\sigma) = (x\pi)\sigma.$$

Proposition 3.5.1: The number of permutations of $[n]$ is $n!$.

Proposition 3.5.2: Every permutation can be written as the composition of cycles on pairwise disjoint subsets. This representation is unique up to the order of the cycles and the choice of starting points in each cycle.

Proof: To construct the cycle decomposition, use the following algorithm. Let π be a permutation of X . While there is a point of X not assigned to a cycle, choose any such point x . Let m be the least positive integer such that $x\pi^m = x$. Then, we have the cycle:

$$(x \ x\pi \ x\pi^2 \ \dots \ x\pi^{m-1}).$$

The final decomposition is the product of all such cycles.

Why can't we have repetition within a cycle? Say that $x\pi^i = x\pi^j$ for $0 \leq i < j < m$. Then, $x = x\pi^{j-i}$, which contradicts how we picked m .

Why can't there be an overlap between two different cycles? Say the overlapping cycles have x in only one cycle and y in only the other. Suppose $y\pi^m = y$ and we have the overlap $x\pi^i = y\pi^j$. Then, $x\pi^{i-j+m} = y$, which is a contradiction. \square

1.2.4 Estimates for Factorials

Big-O Notation: We say that $f(n) = O(g(n))$ if there exists c such that $|f(n)| \leq cg(n)$ for all n .

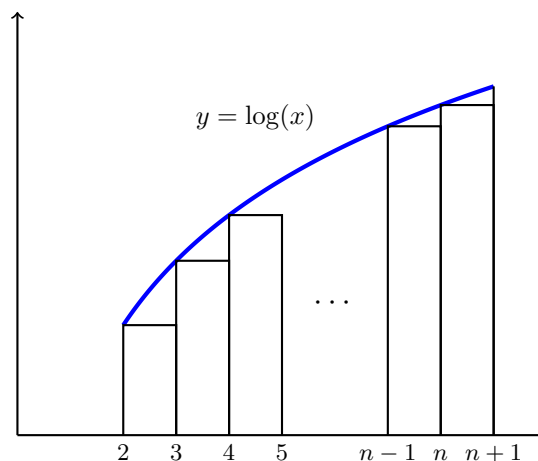
Stirling's Formula:

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(1 + O\left(\frac{1}{n}\right)\right)$$

Remark: Stirling's formula is tricky to prove, so we will prove an upper bound by using the fact that

$$\log(n!) = \sum_{k=2}^n \log(k)$$

and finding an estimate. We use the Calculus 1 trick of graphing $\log(x)$ from 1 to $n+1$ and drawing boxes below the graph of width :



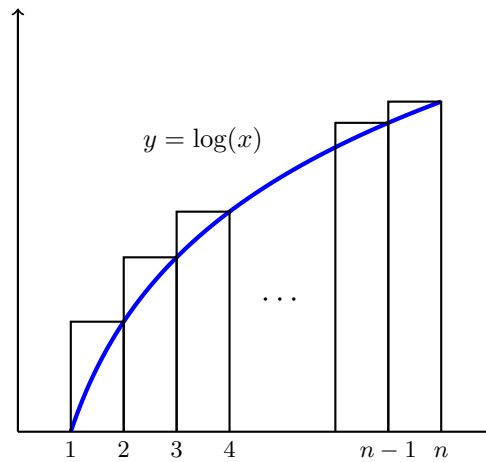
This yields us the estimate

$$\begin{aligned}\log(n!) &\leq \int_2^{n+1} \log(x) dx \\ &= [x \log(x) - x]_2^{n+1} \\ &\leq (n+1) \log(n+1) - (n+1) - 2 \log(2) + 2.\end{aligned}$$

Hence

$$\begin{aligned}n! &= e^{\log(n!)} \\ &\leq e^{(n+1) \log(n+1) - (n+1) - 2 \log(2) + 2} \\ &= \frac{(n+1)^{n+1} e^2}{e^{n+1} \cdot 4} \\ &= \left(\frac{n+1}{e}\right)^{n+1} \cdot \frac{e^2}{4}.\end{aligned}$$

We find a lower bound in the same way. This time we draw our bars above the $\log(x)$ line from $x = 1$ to $x = n$:



which gives us the bound

$$\begin{aligned}\log(n!) &\geq \int_1^n \log(x) dx \\ &= [x \log(x) - x]_1^n \\ &= n \log(n) - n + 1.\end{aligned}$$

Hence,

$$\begin{aligned}n! &= e^{\log(n!)} \\ &\geq \frac{n^n}{e^n} e \\ &= e \left(\frac{n}{e}\right)^n.\end{aligned}$$

Therefore, we have shown that:

$$e \left(\frac{n}{e}\right)^n \leq n! \leq \left(\frac{n+1}{e}\right)^{n+1} \cdot \frac{e^2}{4}.$$

1.2.5 Selections

There are four basic ways to select k things from n things:

—	order matters	order doesn't matter
with repetition	n^k	$\binom{n+k-1}{k}$
without repetition	$\frac{n!}{(n-k)!}$	$\binom{n}{k}$

Lemma 3.7.3: The number of k -tuples of nonnegative integers that sum to n is:

$$\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$$

Proof: “Balls and walls” technique. There is a bijection between these k -tuples and lists containing n balls and $k-1$ walls. For example:

$$(3, 0, 0, 2, 1) \mapsto \cdots ||| \cdot | \cdot$$

So, we take the $n+k-1$ balls and walls together and choose which $k-1$ will be walls (or analogously, which n will be balls). \square

1.2.6 Cayley’s Theorem

Definition: A graph consists of vertices with edges between them.

Note: Two labelled graphs are considered the same if they have the same vertex sets and the same edges.

Notation: If v_1 and v_2 are vertices, then, we say $v_1 \sim v_2$ if v_1 and v_2 are adjacent, or connected by an edge.

Definition: A path is a sequence v_1, v_2, \dots, v_k such that

$$v_i \sim v_{i+1}$$

for all $1 \leq i \leq k-1$, and there is no repetition of vertices.

Definition: A cycle is a path with $v_k \sim v_1$.

Definition: A tree is a connected graph without any cycles.

Definition: A rooted tree is a tree with a designated “root”.

Cayley's Theorem The number of labelled trees on n vertices is n^{n-2} .

Proof: We're going to “multiply by n^2 ” and find a bijection with something counted by n^n : functions from $[n]$ to $[n]$. For each labelled tree, choose two vertices. Call them the “head” and the “tail”. Call the path between them a “backbone” and call the resulting object a “vertebrate”. Note that the head and the tail can be equal.

Now, we can view each vertex on the tree as being part of a subtree whose root is on the backbone. We can specify a vertebrate with the following information.

- (1) A backbone: $K = \{v_1, \dots, v_k\} \subseteq [n]$.
- (2) A permutation of K (from head to tail).
- (3) A partition of $[n] \setminus K$ into sets T_1, T_2, \dots, T_k .
- (4) For each i , the structure of the subtree rooted at v_i on the vertices $T_i \cup \{v_i\}$.

Consider functions $f : [n] \rightarrow [n]$. Recall that a point m is f -periodic if $f^t(m) = m$ for some t . Note that if m is periodic, then $f(m), f^2(m), \dots$ are all periodic. It's clear that f acts as a permutation on its periodic points. If we take a nonperiodic point x there exists t big enough so that $f^t(x)$ is a periodic point.

The periodic points are equivalent to the backbone points v_i . Define

$$T_i := \{\text{nonperiodic } m \mid \text{the first periodic } f^t(m) \text{ is } v_i\}.$$

So, we specify a function $f : [n] \rightarrow [n]$ with the following information.

- (1) Periodic points: $K = \{v_1, \dots, v_k\} \subseteq [n]$.
- (2) Permutation on K : $f|_K$.
- (3) A partition of $[n] \setminus K$ into sets T_1, T_2, \dots, T_k .
- (4) For each i , a tree on $T_i \cup \{v_i\}$ representing the action of f on non-periodic points.

So it's clear that the functions from $[n]$ to $[n]$ are in bijection with the “vertebrates”. Since there are n^2 vertebrates per labelled tree, the number of labelled trees is

$$\frac{n^n}{n^2} = n^{n-2}. \quad \square$$

1.2.7 Bell Numbers

Definition: The n^{th} Bell number, denoted B_n , is the number of (set) partitions of $[n]$ (with nonempty parts).

Notation: Rather than writing the partition $\{\{1\}, \{2\}, \{3\}\}$, we abbreviate it to 1/2/3.

Example: We can find B_3 by listing the partitions of $[3]$:

$$1/2/3 \quad 12/3 \quad 13/2 \quad 23/1 \quad 123$$

So, $B_3 = 5$.

Theorem: We have the recurrence for B_n :

$$B_n = \sum_{k=1}^n \binom{n-1}{k-1} B_{n-k}$$

Proof: Let k denote the size of the block containing n . We choose the other $k-1$ elements in this block, then partition the other $n-k$ elements. \square

1.2.8 Combinatorial Generation

There are four aspects to combinatorial generation:

- (1) Listing
- (2) Ranking (Objects $\rightarrow \mathbb{N}$)
- (3) Unranking ($\mathbb{N} \rightarrow$ Objects)
- (4) Random Selection

There are two types: Recursive (`GenerateAll`) and Iterative (`NextSubset`).

Example: As an example, we will look at listing the power set of $[n]$, denoted by “ $2^{[n]}$ ” or “ $\mathcal{P}([n])$ ”.

```

GenerateAll(n):
  If n = 0:
    Return {}
  Else:
    Set S := GenerateAll(n - 1)
    Make a new copy of each subset in S and add n to this copy
    Return S

```

```

NextSubset(S):
  Find the greatest element not in S
  If i does not exist:
    S is the last subset
  Else:
    Return S \ {i + 1, ..., n} \cup {i}

```

If we use set $n = 3$ and iterate `NextSubset` starting with \emptyset , we get:

$\emptyset, \{3\}, \{2\}, \{2,3\}, \{1\}, \{1,3\}, \{1,2\}, \{1,2,3\}$.

If we make a indicator table and put a 1 in column 1, 2, or 3 based on what digits are in the set, we get

$n = 3$	1	2	3	Decimal Representation
\emptyset	0	0	0	0
$\{3\}$	0	0	1	1
$\{2\}$	0	1	0	2
$\{2,3\}$	0	1	1	3
$\{1\}$	1	0	0	4
$\{1,3\}$	1	0	1	5
$\{1,2\}$	1	1	0	6
$\{1,2,3\}$	1	1	1	7

So, to list these sets, we can use binary numbering.

Example: Next we will try to generate $\binom{[n]}{k}$.

```

GenerateAll( $n, k$ ):
  If  $k > n$  or  $k < 0$ :
    Return  $\emptyset$ 
  Elseif  $k = 0$ :
    Return  $\{\emptyset\}$ 
  Else:
    Set  $S = \text{GenerateAll}(n - 1, k - 1)$ 
    Adjoin  $n$  to all sets in  $S$ 
    Set  $T = \text{GenerateAll}(n - 1, k)$ 
    Return  $S \cup T$ 

```

A possible ordering for this listing is lexicographic (or dictionary) ordering.. For example

$$1\ 3\ 5\ 6 \prec_{\ell} 1\ 3\ 5\ 7.$$

More precisely,

$$a_1\ a_2\ \cdots\ a_k \prec_{\ell} b_1\ b_2\ \cdots\ b_k$$

if there is some index j with $1 \leq j \leq k$ such that

- (1) $a_j < b_j$,
- (2) $a_i = b_i$ for all $1 \leq i < j$.

Example: The lexicographical ordering of $\binom{[5]}{3}$ is:

$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 3, 4\}, \{2, 3, 5\}, \{2, 4, 5\}, \{3, 4, 5\}.$$

For an iterative algorithm, we need to figure out how to find the next subset in lexicographic order given a subset.

```

Next( $S$ ):
  Suppose  $S = \{s_1 < s_2 < \cdots < s_k\}$ 
  Find the greatest index  $i$  such that  $s_i + 1 \notin S$ 
  If  $i$  does not exist:
     $S$  is the last set
  Else:
    Let  $j$  denote the number of elements of  $S$  greater than  $s_i$  (so  $j = k - i$ )
    Return  $S \setminus \{s_i, s_{i+1}, \dots, s_k\} \cup \{s_i + 1, \underbrace{s_i + 2, \dots, s_i + j + 1}_{j \text{ elements}}\}$ 

```

Definition: We may also consider co-lexicographical order (or “co-lex” order). (Note: the textbook calls this “reverse order”, which is misleading. We define this order by:

$$a_1\ a_2\ \cdots\ a_k \prec_c b_1\ b_2\ \cdots\ b_k$$

if and only if

$$a_k\ a_{k-1}\ \cdots\ a_1 \prec_{\ell} b_k\ b_{k-1}\ \cdots\ b_1.$$

Example: In our example above, the co-lex order is:

$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 5\}, \{1, 3, 5\}, \{2, 3, 5\}, \{1, 4, 5\}, \{2, 4, 5\}, \{3, 4, 5\}$.

Now we demonstrate an iterative algorithm to find the next subset in co-lex order.

```

CLNext( $S$ ):
  Set  $S := \{s_1 < \dots < s_k\}$ 
  Find the least  $i$  such that  $s_i + 1 \notin S$ 
  If  $i$  does not exist:
     $S$  is the last set
  Else:
    Return  $S \setminus \{s_1, \dots, s_i\} \cup \{s_1 + 1, \underbrace{1, 2, \dots, i-1}_{i-1 \text{ elements}}\}$ 

```


1.3 Chapter 5 - The Principle of Inclusion-Exclusion

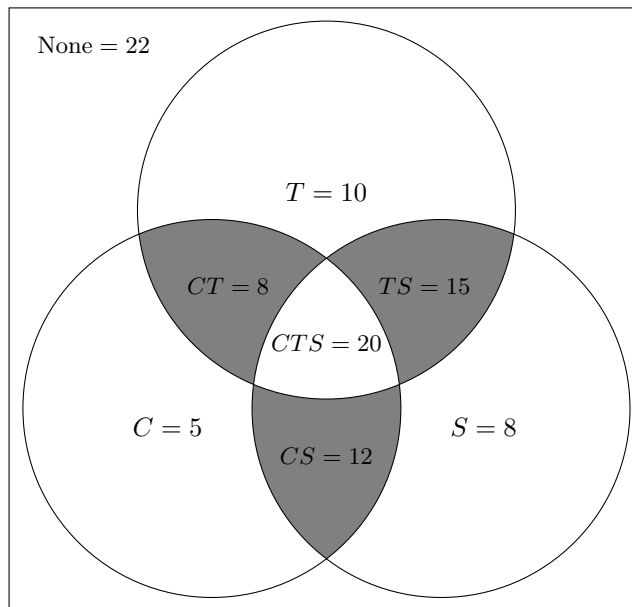
1.3.1 PIE

Suppose there are 100 pupils, and they play some combination of the sports: Cricket, Tiddlywinks, Space Invaders. We know that: (we abbreviate the fact that 45 people play cricket by “45 C”, etc.)

$$45C, 53T, 55S, 28CT, 32CS, 35TS, 20CTS.$$

How many people don't play any of these games?

We can solve this with a Venn Diagram. We start from the innermost part and work outward. At the last step we subtract everything in the diagram from 100 to find the number of students who play no sport.



The rigorous way to solve these problems is with the **Principle of Inclusion-Exclusion**, or **PIE**.

Theorem 5.1.1: (PIE) Let the universe be X with subsets $A_1, \dots, A_n \subseteq X$. If $I \subseteq [n]$, then define

$$A_I := \bigcap_{i \in I} A_i, \quad A_\emptyset = X.$$

Then, the number of elements of X which lie in none of the A_i is

$$\sum_{I \subseteq [n]} (-1)^{|I|} |A_I|.$$

Proof: Let $x \in X$. We count its contribution to the sum. We'd like it to contribute zero times if it lies in some A_i and contribute exactly once if it doesn't.

If x does not lie in any A_i , then the only contribution of X is as an element of A_\emptyset , and its contribution is 1.

Otherwise, x lies in at least one set A_i . Set $J = \{i \mid x \in A_i\}$ and let $j = |J|$. Notice that $x \in A_I$ if and only if $I \subseteq J$. So, the contribution of x is

$$\sum_{I \subseteq J} (-1)^{|I|} = \sum_{i=0}^j \binom{j}{i} (-1)^i = 0. \quad \square$$

Applying this example to the above problems tells us that the number of students who play no sports is

$$100 - 45 - 53 - 55 + 28 + 32 + 35 - 20 = 22.$$

Application: (Surjections) A surjection is a function $[n] \rightarrow [k]$ which is onto. The universe X is the set of all functions $[n] \rightarrow [k]$. Define $\overline{A_i}$ to be the set of all functions $[n] \rightarrow ([k] \setminus \{i\})$. Then, for $I \subseteq [k]$, it's clear that A_I is the set of functions $[n] \rightarrow ([k] \setminus I)$. Clearly,

$$|A_I| = (k - |I|)^n.$$

So, the number of surjections is

$$\sum_{I \subseteq [k]} (-1)^{|I|} |A_I| = \sum_{I \subseteq [k]} (-1)^{|I|} (k - |I|)^n = \sum_{i=0}^k (-1)^i \binom{k}{i} (k - i)^n.$$

Corollary: Set $k = n$. Then, the number of surjections (in this case, bijections) $[n] \rightarrow [n]$ is

$$\sum_{i=0}^n (-1)^i \binom{n}{i} (n - i)^n.$$

But, we know that a bijection is a permutation of n and so there are $n!$ of these. Hence,

$$n! = \sum_{i=0}^n (-1)^i \binom{n}{i} (n - i)^n.$$

This is an unexpected identity!

Application: (Derangements) A derangement is a permutation with no fixed points. Define the universe to be all permutations. Let A_i be the set of permutations which fix i and let A_I be the set of permutations which fix all of I . Then,

$$|A_I| = (n - |I|)!.$$

So, the number of derangements of $[n]$ is

$$\begin{aligned} \sum_{I \subseteq [n]} (-1)^{|I|} (n - |I|)! &= \sum_{i=0}^n \binom{n}{i} (-1)^i (n - i)! \\ &= \sum_{i=0}^n \frac{n!}{i!(n - i)!} (-1)^i (n - i)! \\ &= n! \sum_{i=0}^n \frac{(-1)^i}{i!} \end{aligned}$$

This sum is the truncated series for e^{-1} , and it converges very quickly. In fact, for $n \geq 2$, the number of derangements of $[n]$ is the nearest integer to $n!e^{-1}$. To see this, we want to find that

$$\begin{aligned} \left| n! \sum_{i=0}^{\infty} \frac{(-1)^i}{i!} - n! \sum_{i=0}^n \frac{(-1)^i}{i!} \right| &< \frac{1}{2} \\ n! \left| \sum_{i=n+1}^{\infty} \frac{(-1)^i}{i!} \right| &< \frac{1}{2} \\ \underbrace{\left| \sum_{i=n+1}^{\infty} \frac{(-1)^i}{i!} \right|}_{\leq 1/(n+1)!} &< \frac{1}{2n!} \end{aligned}$$

We want

$$\frac{1}{(n+1)!} < \frac{1}{2n!}$$

and so $2 < n+1$ which gives $n > 1$.

1.3.2 A Generalization

Proposition 5.2.1: Let $I \subseteq [n]$. The number of elements which lie in A_i precisely when $i \in I$ is

$$\sum_{J \supseteq I} (-1)^{|J \setminus I|} |A_J|.$$

Proof: Define for $k \in [n] \setminus I$ the set $B_k = A_{I \cup \{k\}}$. Then, by the **Principle of Inclusion-Exclusion**, the number of elements which are in no B_k is

$$\sum_{K \subseteq [n] \setminus I} (-1)^{|K|} |B_K|$$

where $B_K := \bigcap_{k \in K} B_k$ and $B_\emptyset := A_I$. \square

Remark: Suppose we have functions $f, g : 2^{[n]} \rightarrow \mathbb{R}$ (e.g. $J \mapsto |A_J|$) which satisfy

$$g(I) = \sum_{J \supseteq I} f(J).$$

In relation to the earlier problem, we would set

$$g(I) := \left| \bigcap_{i \in I} A_i \right| = |A_I| = [\text{the } \# \text{ of elements that lie in all } A_i \text{ for } i \in I]$$

and

$$f(J) := [\text{the } \# \text{ of elements that lie in } A_i \text{ precisely when } i \in J].$$

We would like to invert our earlier statement and ask if it's always true that

$$f(I) = \sum_{J \supseteq I} (-1)^{|J \setminus I|} g(J) \quad ?$$

Proposition 5.2.2: If $f, g : 2^{[n]} \rightarrow \mathbb{R}$ satisfy

$$g(I) = \sum_{J \supseteq I} f(J),$$

then

$$f(I) = \sum_{J \supseteq I} (-1)^{|J \setminus I|} g(J).$$

(This is a generalization of the Principle of Inclusion-Exclusion, but is also relevant to Möbius inversion for the set $2^{[n]}$.)

Proof: (This proof is different than the proof in the text.) Expand the right-hand side:

$$\begin{aligned}
\sum_{J:J\supseteq I} (-1)^{|J\setminus I|} g(J) &= \sum_{J:J\supseteq I} \left[(-1)^{|J\setminus I|} \sum_{K:K\supseteq J} f(K) \right] \\
&= \sum_{J,K:K\supseteq J\supseteq I} (-1)^{|J\setminus I|} f(K) \\
&= \sum_{K:K\supseteq I} \left[\sum_{J:K\supseteq J\supseteq I} (-1)^{|J\setminus I|} f(K) \right] \\
&= \sum_{K:K\supseteq I} \left[\sum_{j=0}^{|K\setminus I|} (-1)^j \binom{|K\setminus I|}{j} f(K) \right] \\
&= \sum_{K:K\supseteq I} \left[f(K) \underbrace{\sum_{j=0}^{|K\setminus I|} (-1)^j \binom{|K\setminus I|}{j}}_{= \begin{cases} 1, & |K\setminus I| = 0 \\ 0, & |K\setminus I| \neq 0 \end{cases}} \right] \\
&= f(I). \quad \square
\end{aligned}$$

Proposition 5.2.3: (replace “ \supseteq ” with “ \subseteq ” in **Proposition 5.2.2**) If $f, g : 2^{[n]} \rightarrow \mathbb{R}$ satisfy

$$g(I) = \sum_{J\subseteq I} f(J)$$

then

$$f(I) = \sum_{J\subseteq I} (-1)^{|I\setminus J|} g(J).$$

Proof: Define $\bar{f}(I) := f([n] \setminus I)$ and $\bar{g}(J) := g([n] \setminus J)$. Define $\bar{I} := [n] \setminus I$ and $\bar{J} := [n] \setminus J$. Now we see that

$$\bar{g}(I) = g(\bar{I}) = \sum_{\bar{J}\subseteq\bar{I}} f(\bar{J}) = \sum_{J\supseteq I} f(\bar{J}) = \sum_{J\supseteq I} \bar{f}(J).$$

So, by **Proposition 5.2.2**.

$$\bar{f}(I) = \sum_{J\supseteq I} (-1)^{|J\setminus I|} \bar{g}(J).$$

Hence,

$$f(\bar{I}) = \sum_{J\supseteq I} (-1)^{|J\setminus I|} g(\bar{J}).$$

Since $J \supseteq I$ is the same condition as $\bar{J} \subseteq \bar{I}$ and since $J \setminus I = \bar{I} \setminus \bar{J}$ we get

$$f(\bar{I}) = \sum_{\bar{J}\subseteq\bar{I}} (-1)^{|\bar{I}\setminus\bar{J}|} g(\bar{J})$$

which completes the proof. \square

Example: How many permutations of $[n]$ are there where at least one of the first two entries is even? We break this into two cases, either n is even or n is odd.

If n is even, then the number of permutations which start with two even numbers is

$$\binom{n}{2} \binom{n}{2} (n-2)!$$

and the number of permutations which start with an even then an odd is

$$\binom{n}{2} \binom{n}{2} (n-2)!$$

(and this is the same as the number of permutations which start with an odd then an even. Add these together to get the answer.

1.3.3 Stirling Numbers

Definition: The (signed) Stirling numbers of the first kind $s(n, k)$ are defined by

$$(-1)^{n-k} s(n, k) = [\# \text{ of permutations of } [n] \text{ with } k \text{ disjoint cycles}].$$

Definition: The Stirling numbers of the second kind $S(n, k)$ are defined by

$$S(n, k) = [\# \text{ of set partitions of } [n] \text{ into } k \text{ blocks}].$$

Proposition 5.3.1:

$$(a) \sum_{k=1}^n (-1)^{n-k} s(n, k) = n!.$$

$$(b) \sum_{k=1}^n S(n, k) = B_n.$$

Proposition 5.3.2:

$$(a) s(n, n) = S(n, n) = 1.$$

$$(b) s(n+1, k) = -ns(n, k) + s(n, k-1).$$

$$(c) S(n+1, k) = kS(n, k) + S(n, k-1).$$

Proof of (a): Trivial. \square

Proof of (c): Consider a set partition of $[n+1]$. There are $S(n, k-1)$ partitions where the element $n+1$ lies in its own block and $kS(n, k)$ partitions where $n+1$ is in a block with other elements. Adding these together gives all possibilities. \square

Proof of (b): First consider the unsigned version

$$|s(n+1, k)| = |ns(n, k)| + |s(n, k-1)|.$$

The $|s(n, k-1)|$ term counts the cases where $n+1$ is in its own cycle (i.e., is a fixed point). The $|ns(n, k)|$ term counts the number of ways to insert $n+1$ into one of the already existing k disjoint cycles. So, the unsigned version holds.

For the signed version, observe that either all terms are positive or all are negative, so we either have the unsigned version already or we can multiply by -1 to get it, which proves the theorem for the signed version. \square

Definition: $(x)_n := \underbrace{x(x-1)\cdots(x-n+1)}_{n \text{ terms}}$. This is called the falling factorial. We can either think of x as a number (and get a numerical result), or as a variable (and get a polynomial).

Proposition 5.3.3:

$$(a) \quad (x)_n = \sum_{k=1}^n s(n, k)x^k.$$

$$(b) \quad x^n = \sum_{k=1}^n S(n, k)(x)_k.$$

Remark: Stirling constructed the Stirling numbers of the first kind to prove **part (a)**, which is why they have the sign.

Proof: We proceed by induction on n . For $n = 1$, both are trivially true ($x = x$).

For **part (a)**, we assume true for n , i.e., we assume that

$$(x)_n = \sum_{k=1}^n s(n, k)x^k.$$

Now,

$$\begin{aligned} (x)_{n+1} &= (x)_n(x-n) \\ &= (x-n) \sum_{k=1}^n s(n, k)x^k \\ &= \sum_{k=1}^n s(n, k)x^{k+1} - \sum_{k=1}^n ns(n, k)x^k \\ &= \sum_{j=2}^{n+1} s(n, j-1)x^j - \sum_{k=1}^n ns(n, k)x^k && \text{(using } j := k+1) \\ &= \sum_{k=1}^{n+1} [s(n, k-1)x^k - ns(n, k)x^k] \\ &= \sum_{k=1}^{n+1} s(n+1, k)x^k. \quad \square && \text{(Proposition 5.3.2(b))} \end{aligned}$$

For **part (b)**, we assume true for n , i.e., we assume that

$$x^n = \sum_{k=1}^n S(n, k)(x)_k.$$

Now,

$$\begin{aligned}
x^{n+1} &= xx^n \\
&= x \sum_{k=1}^n S(n, k)(x)_k \\
&= \sum_{k=1}^n S(n, k)(x)_k((x - k) + k) \\
&= \sum_{k=1}^n S(n, k)(x)_k(x - k) + \sum_{k=1}^n S(n, k)(x)_k k \\
&= \sum_{k=1}^n S(n, k)(x)_{k+1} + \sum_{k=1}^n kS(n, k)(x)_k \\
&= \sum_{j=2}^{n+1} S(n, j - 1)(x)_k + \sum_{k=1}^{n+1} kS(n, k)(x)_k && \text{(using } j := k + 1\text{)} \\
&= \sum_{j=1}^{n+1} S(n, j - 1)(x)_k + \sum_{k=1}^{n+1} kS(n, k)(x)_k \\
&= \sum_{k=1}^{n+1} [S(n, k - 1)(x)_k + kS(n, k)(x)_k] \\
&= \sum_{k=1}^{n+1} S(n + 1, k). \quad \square && \text{(Proposition 5.3.2(b))}
\end{aligned}$$

Remark: We can find a formula for $S(n, k)$ which will help with calculations. Remember that the number of surjections $[n] \rightarrow [k]$ is:

$$\sum_{i=0}^k (-1)^i \binom{k}{i} (k - i)^n.$$

We can look at a surjection as a set of preimages of $[k]$, i.e., a partition of $[n]$ into k parts and then ordered to say which part is which preimage. This gives the following proposition.

Proposition 5.3.5:

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k - i)^n.$$

1.3.4 Even & Odd Permutations

Definition: The sign of a permutation π , denoted $\text{sign}(\pi)$ is defined by

$$\text{sign}(\pi) := (-1)^{n - [\# \text{ of disjoint cycles in } \pi]}.$$

We say that a permutation is even if $\text{sign}(\pi) = +1$ and that a permutation is odd if $\text{sign}(\pi) = -1$.

Remark: This definition is not the usual definition of an even/odd permutation taught in an algebra class, but the definition coincides.

Remark: The number of even permutations is equal to the number of odd permutations for all $n \geq 2$. To see this, recall

$$(x)_k = \sum_{k=1}^n s(n, k)x^k$$

$$(x)(x-1)\cdots(x-n+1) = \sum_{k=1}^n (-1)^{n-k} \cdot [\# \text{ of permutations with } k \text{ disjoint cycles}] \cdot x^k.$$

Now set $x = 1$ (remember $n \geq 2$) and see that

$$0 = \sum_{k=1}^n (-1)^{n-k} \cdot [\# \text{ of permutations with } k \text{ disjoint cycles}].$$

So, the cases where k is even and where k is odd must cancel out (from the -1 power) and thus the number of each is the same.

Definition: Define $c(\pi) := [\# \text{ of disjoint cycles of } \pi]$, so that $\text{sign}(\pi) = (-1)^{n-c(\pi)}$.

Proposition 5.5.2: If π is a permutation of $[n]$ and if τ is a transposition, then

$$c(\pi\tau) = c(\pi) \pm 1.$$

Proof: Let $\tau = (i j)$. If i, j are in different disjoint cycles of π , then switching them links two disjoint cycles together, which decreases the number of cycles by 1. If i, j are in the same disjoint cycle of π , then switching them breaks the cycle into two pieces. \square .

Remark: This proves that our definition of even/odd cycles coincides with the usual algebraic definition (once the trivial base case is verified).

1.4 Chapter 6 - Latin Squares and SDRs

1.4.1 Latin Squares

Definition: A Latin square is an $n \times n$ matrix with entries from $[n]$ such that each symbol occurs once in each row and column.

Example: Start with a permutation, for example $(3\ 5\ 2\ 1\ 4)$ and shift it for each row:

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

Question: How many Latin squares are there for a given n ? Well, we just showed that there are at least $n!$.

Definition: Two Latin squares S and T are orthogonal if

$$|\{(S_{i,j}, T_{i,j})\}| = n^2.$$

Remark: This is the start of a subject called “design theory” which is relevant throughout the book.

1.4.2 SDRs

Definition: A system of distinct representatives (or, SDR) for a family $A_1, \dots, A_n \subseteq X$ is an n -tuple (x_1, \dots, x_n) such that:

- (a) $x_i \in A_i$ for all i (representatives),
- (b) $x_i \neq x_j$ for $i \neq j$ (distinct).

Example: Let $A_1 := \{1, 2, 3\}$ and $A_2 := \{1, 3, 4\}$. The possible SDRs for this family are:

$$(1, 3), (1, 4), (2, 1), (2, 3), (2, 4), (3, 1), (3, 4).$$

There are $7 = 3^2 - 2$ possible SDRs, because there are 3^2 ordered pairs in total and two with $x_i = x_j$.

Notation: $A(J) := \bigcup_{j \in J} A_j$.

(Phillip) Hall’s Marriage Theorem: The family $A_1, \dots, A_n \subseteq X$ has an SDR if and only if

$$(HC): |A(J)| \geq |J| \text{ for all } J \subseteq [n].$$

The condition (HC) is called Hall’s Condition.

Proof:

(\implies) If there is an SDR (x_1, \dots, x_n) then for all $J \subseteq [n]$, we have $\{x_j \mid j \in J\} \subseteq A(J)$. Since all x_j are distinct, $|A(J)| \geq |\{x_j \mid j \in J\}| = |J|$.

(\Leftarrow) We proceed by (strong) induction on n . Clear for $n = 1$.

Definition: We call an index set J critical if $|A(J)| = |J|$.

We consider two cases.

Case 1: (There is no critical set except \emptyset and possibly $[n]$.) Choose $x_n \in A_n$ and define

$$A'_j := A_j \setminus \{x_n\}.$$

We claim that Hall's Condition still holds on the sets A'_1, \dots, A'_{n-1} . Let $J \subseteq [n-1]$. Then,

$$\begin{aligned} |A'(J)| &\geq |A(J)| - 1 \\ &> |J| - 1. \end{aligned}$$

Hence $|A'(J)| \geq |J|$ and so by induction, there exists an SDR for the family.

Case 2: (There is a critical set which is not \emptyset or $[n]$.) Take J to be a minimal (by cardinality) nonempty critical set. By induction $\{A_j \mid j \in J\}$ has an SDR which uses all of $A(J)$. For $i \notin J$ define

$$A_i^* := A_i \setminus A(J).$$

We claim that Hall's Condition still holds on the sets A_i^* for $i \notin J$. Pick some $K \subseteq [n] \setminus J$. Then,

$$A^*(K) = A(K \cup J) \setminus A(J).$$

So,

$$\begin{aligned} |A^*(K)| &= |A(K \cup J) \setminus A(J)| \\ &= |A(K \cup J)| - |A(J)| && \text{(since } A(J) \subseteq A(K \cup J)\text{)} \\ &\geq |K \cup J| - |A(J)| \\ &= |K \cup J| - |J| \\ &= |K|. && \text{(since } J \cap K = \emptyset\text{)} \end{aligned}$$

Hence the theorem is true in this case.

So, the inductive step holds. \square

(Marshall) Hall's Variant: Suppose $|A_i| \geq r$ for all i , and the sets A_1, \dots, A_n satisfy Hall's Condition. Then the number of SDRs for A_1, \dots, A_n is at least

$$\begin{cases} r!, & r \leq n \\ (r)_n, & r \geq n \end{cases}.$$

Proof: We adapt the proof of the previous theorem. The base case is clear.

Case 2: ($r \leq |J| < n$) By induction, the family $\{A_j \mid j \in J\}$ has $\geq r!$ SDRs.

Case 1: ($r > |J|$). In this case, we have $\geq r$ choices for x_n . Each A'_j has $\geq r-1$ elements. If $r \leq n$ then $r-1 \leq n-1$, so we have $\geq (r-1)!$ SDRs on $\{A'_j\}$, so there are $\geq r!$ SDRs in total. If $r > n$ then $r-1 > n-1$, so $\{A'_j\}$ has $\geq (r-1)_{n-1} = (r-1) \cdots (r-n+1)$ SDRs, so we have $\geq (r)_n$ SDRs in total. \square

Theorem 6.2.4: Suppose that $A_1, \dots, A_n \subseteq [n]$ and suppose there is some r such that:

- (a) $|A_i| = r$ for all i ,
- (b) each element of $[n]$ occurs in precisely r of the sets A_i .

Then, we have at least $r!$ SDRs.

Proof: Fix $J \subseteq [n]$. We want

$$|A(J)| = \left| \bigcup_{j \in J} A_j \right| \geq |J|.$$

We will double count the set

$$\{(j, x) \mid j \in J, x \in A_j\}.$$

Counting “ j first”, we get $|J|r$ elements. Counting “ x ” first we get $\leq |A(J)r$ elements. Well, then

$$|J|r \leq |A(J)r,$$

i.e., $|A(J)| \geq |J|$. \square

1.4.3 How Many Latin Squares?

Definition: Let $L(n)$ denote the number of Latin squares of size n .

Remark: We showed the lower bound $L(n) \geq n!$ because we take any permutation for the first row and then just shift it for any other row. Additionally, we have the obvious upper bound $L(n) \leq n^{n^2}$ because n^{n^2} is the number of ways to make any square of size n with entries from $[n]$. A better upper bound is $L(n) \leq (n!)^n$, which comes from the fact that each row must be a permutation (no duplicates within a row).

Theorem 6.3.2: $L(n) \geq \prod_{r=1}^n r!$

Proof: Build a Latin square row by row, at each state letting A_i denote the elements that haven't occurred yet in column i . Apply **Theorem 6.2.4**. \square

Remark: Let $n = 4$. Then $L(4) \geq 4!3!2! = 288$. However, the actual number is $L(4) = 576$, and we will prove this in a homework problem. To see some additional Latin squares of size 4, we have $4!$ possibilities for the first row, and without loss of generality (by reordering columns) we can assume that the first row is 1234. Then, the second row must be a *derangement*, or which there are

$$\left[\frac{4!}{e} \right] = 9$$

possibilities, and this number is bigger than the previous $3!$. Since each row must be a derangement, we have a better upper bound

$$L(n) \leq (n!) \left(\frac{n!}{e} \right)^{n-1} = \frac{(n!)^n}{e^{n-1}}.$$

Remark: We can evaluate our lower bound from **Theorem 6.3.2** using logarithms:

$$\begin{aligned} \log(L(n)) &\geq \sum_{r=1}^n \log(r!) \\ &\geq \sum_{r=1}^n [r \log(r) - r]. && \text{(using the integral trick)} \\ &\geq \frac{1}{2}n^2 \log(n) + O(n^2) \end{aligned}$$

So, $\log(L_n) \approx \frac{1}{2}n^2 \log(n)$.

Using the same trick with the (awful) upper bound $L(n) \leq n^{n^2}$, we see that

$$\log(L(n)) \leq n^2 \log(n).$$

The question is: which approximation is closer, the version with the $\frac{1}{2}$ or the version with the 1?

1.4.4 Quasigroups and Groups

Definition: Let M be an $n \times n$ matrix. Define the determinant by

$$\det(M) = \sum_{\pi \in S_n} (-1)^{\text{sign}(\pi)} \prod_{i=1}^n M_{i, i\pi}.$$

(Recall that $i\pi = \pi(i)$ using the notation of the book.)

Definition: Let M be an $n \times n$ matrix. Define the permanent by

$$\text{per}(M) = \sum_{\pi \in S_n} \prod_{i=1}^n M_{i, i\pi}.$$

Examples:

$$\text{per} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1.$$

$$\text{per} \begin{pmatrix} 1 & 0 & * \\ * & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1.$$

$$\text{per} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = 1 \cdot \text{per} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + 1 \cdot \text{per} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = 1 \cdot \text{per}(1) + 1 \cdot \text{per}(1) = 2.$$

Definition: A doubly stochastic matrix has nonnegative entries for which every row and column sums to 1.

Example: $\begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{pmatrix}$ is a doubly stochastic matrix. Also,

$$\text{per} \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \\ 1/3 & 1/3 & 1/3 \end{pmatrix} = 3! \left(\frac{1}{3}\right)^3 = \frac{2}{9}.$$

Example:

$$\begin{aligned} \text{per} \begin{pmatrix} 1/2 & 1/2 & 0 \\ 1/4 & 0 & 3/4 \\ 1/4 & 1/2 & 1/4 \end{pmatrix} &= \frac{1}{2} \text{per} \begin{pmatrix} 0 & 3/4 \\ 1/2 & 1/4 \end{pmatrix} + \frac{1}{2} \text{per} \begin{pmatrix} 1/4 & 3/4 \\ 1/4 & 1/4 \end{pmatrix} \\ &= \frac{1}{2} \left(0 + \frac{3}{8} \right) + \frac{1}{2} \left(\frac{1}{16} + \frac{3}{16} \right) \\ &= \frac{3}{16} + \frac{2}{16} \\ &= \frac{5}{16}. \end{aligned}$$

Remark: It seems that looking at permanents of doubly stochastic 3×3 matrices, the smallest we can get is $\frac{2}{9}$. This is described by the following.

van der Waerden Conjecture: Let M be a doubly stochastic $n \times n$ matrix. Then,

$$\text{per}(M) \geq \frac{n!}{n^n}$$

with equality if and only if every entry of M equals $\frac{1}{n}$.

Remark: This is a tricky proof. It was finally proved in 1979 after being open for over 80 years.

Remark: Suppose A_1, \dots, A_n are subsets of $[n]$. Define the matrix M by

$$M_{i,j} = \begin{cases} 1, & \text{if } i \in A_j \\ 0, & \text{otherwise} \end{cases}.$$

For example, define $A_1 := \{1, 2\}$, $A_2 := \{1, 3\}$, $A_3 := \{2, 3\}$. Then,

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Observe that

$$\text{per}(M) = 2,$$

which corresponds to the fact that the family $\{A_1, A_2, A_3\}$ has two SDRs.

Proposition 6.5.1: With A_1, \dots, A_n and M defined as above, we have that

$$\text{per}(M) = [\# \text{ of SDRs of the family } A_1, \dots, A_n].$$

Proof: Every nonzero term in $\text{per}(M)$ corresponds to a permutation such that $M_{i,i\pi} = 1$ for all i , so that $i \in A_{i\pi}$ for all i . Conversely, SDRs correspond to permutations. \square

Proposition 6.5.2: Let $A_1 \dots, A_r$ be a family of subsets of $[n]$, with r a positive integer. If

- (a) $|A_i| = r$,
- (b) every element lies in r sets,

then the number of SDRs is $\geq n! \left(\frac{r}{n}\right)^n$.

Proof: Form the matrix M as before. Then, $\frac{1}{r}M$ is doubly stochastic, and

$$\text{per} \left(\frac{1}{r}M \right) \geq \frac{n!}{n^n}.$$

Also,

$$\text{per} \left(\frac{1}{r}M \right) = \frac{1}{r^n} \text{per}(M)$$

and so

$$\text{per}(M) \geq n! \left(\frac{r}{n}\right)^n. \quad \square$$

Remark:

$$\begin{aligned} L(n) &\geq \prod_{r=1}^n n! \left(\frac{r}{n}\right)^n \\ &= \left(\frac{n!}{n^n}\right)^n \prod_{r=1}^n r^n \\ &= \frac{(n!)^{2n}}{n^{n^2}} \\ &\geq \frac{\left(\frac{n}{e}\right)^{2n^2}}{n^{n^2}}. \end{aligned}$$

So,

$$\begin{aligned} \log(L(n)) &\geq 2n^2 \log(n) - 2n^2 - n^2 \log(n) \\ &= n^2 \log(n) - 2n^2. \end{aligned}$$

Hence, our earlier question is answered and we can now see that the number of Latin squares is much closer to $n^2 \log(n)$ than to $\frac{1}{2}n^2 \log(n)$.

1.4.5 Orthogonal Latin Squares

Euler's 36 Officers Problem (1783): There are 36 officers which make up 6 regiments and 6 ranks. For every regiment, there is an officer of every rank. Can we put them in a 6×6 array so that in every row and every column, we see every rank? We are looking for two Latin squares of order 6 so that when we put them together, every pair of entries occurs. This is called an orthogonal Latin square. These are also sometimes called Graeco-Latin squares.

Euler conjectured that the answer was no. This was proved by Tarry in 1901.

Proposition 6.6.1: If $n > 2$ is a prime power, then there is a pair of orthogonal Latin squares of order n .

Proof: Because n is a prime power, there is a finite field \mathbb{F}_n with n elements. For nonzero $m \in \mathbb{F}_n$, define

$$(A_m)_{i,j} = im + j$$

where computation is being done over the field. For example, if $n = 5$ and $m = 3$, then,

$$A_3 = \begin{pmatrix} 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}.$$

First we show that in a row, no element appears twice. Assume that,

$$im + j_1 = im + j_2$$

(in the field). Then, $j_1 = j_2$. So, no element appears twice in a row. Now assume that

$$i_1m + j = i_2m + j$$

(in the field). Then, $i_1 = i_2$. So, no element appears twice in a column. So, each A_m is a Latin square.

Lastly, we need to check that each pair A_{m_1} and A_{m_2} for $m_1 \neq m_2$ is orthogonal. So, we need to show that every pair (a, b) occurs. We need to show that the system

$$\begin{cases} im_1 + j = a \\ im_2 + j = b \end{cases}$$

has a solution. But since we're in a field, a system with two equations and two unknowns (with $m_1 \neq m_2$) has a unique solution. \square

1.4.6 Direct Products

Example:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \left(\begin{array}{cc|cc|cc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ \hline 3 & 4 & 5 & 6 & 1 & 2 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ \hline 5 & 6 & 1 & 2 & 3 & 4 \\ 6 & 5 & 2 & 1 & 4 & 3 \end{array} \right).$$

The entry in position (i, j) of block (a, b) is equal to $(T_{(a,b)} - 1)m + S_{i,j}$ where S is the first component of the product (of size $m \times m$) and T is the second component of the product (of size $n \times n$).

Proposition 6.6.2: If S^1 and S^2 are orthogonal Latin squares of order m and T^1 and T^2 are orthogonal Latin squares of order n , then $S^1 \times T^1$ and $S^2 \times T^2$ are orthogonal Latin squares of order mn .

Proof: We want to show that (x, y) occurs. Let q_x, q_y, r_x, r_y be so that

$$x = q_x m + r_x$$

$$y = q_y m + r_y$$

for $r_x, r_y < m$. Use the division algorithm on each equation individually to find these.

Because T^1 and T^2 are orthogonal, there are indices a, b such that

$$T_{a,b}^1 = q_x,$$

and

$$T_{a,b}^2 = q_y.$$

Similarly, there exist i, j such that

$$S_{i,j}^1 = r_x,$$

and

$$S_{i,j}^2 = r_y. \quad \square$$

Remark: Write n as $2^{p_1}3^{p_2}5^{p_3}\dots$. With the above methods, as long as $p_1 \neq 1$, we can create a pair of orthogonal Latin squares of order n , i.e., we can create a pair of orthogonal Latin squares of order n as long as $n \not\equiv 2 \pmod{4}$.

Remark: Euler knew all of this, and he conjectured that there was *no* pair of orthogonal Latin squares in the case $n \equiv 2 \pmod{4}$. However, in 1959, Parker (with the help of his UNIVAC computer) found a pair for $n = 10$ (in less than an hour!). He later proved the theorem below.

Theorem: Orthogonal Latin squares exist unless $n = 2, 6$.

1.5 Chapter 7 - Extremal Set Theory

Remark: In this chapter, we will look at families of subsets of $[n]$ with some condition and ask how large they can be.

1.5.1 Intersecting Family of Sets

Definition: The family \mathcal{F} is intersecting if $A \cap B \neq \emptyset$ for all $A, B \in \mathcal{F}$.

Proposition 7.1.1: The largest intersecting family of subsets of $[n]$ has 2^{n-1} subsets.

Proof: We can attain 2^{n-1} by fixing an element in all sets. We can't have more than 2^{n-1} because we can only pick one element from each pair (A, A^C) . \square

Example 1: Fix some $i \in [n]$ and let

$$\mathcal{F} := \{A \subseteq [n] \mid i \in A\}.$$

Example 2: If n is odd, set $n = 2m + 1$ and observe that

$$2^{n-1} = \binom{2m+1}{m+1} + \binom{2m+1}{m+2} + \cdots + \binom{2m+1}{2m+1}.$$

Set

$$\mathcal{F} := \left\{ A \subseteq [n] \mid |A| \geq \left\lceil \frac{n}{2} \right\rceil \right\}.$$

This is equivalent to picking the sets from the right half of a row of Pascal's Triangle. Now, for $A, B \in \mathcal{F}$, we have

$$|A \cap B| = |A| + |B| - |A \cup B| > \frac{n}{2} + \frac{n}{2} - n = 0.$$

Example 3: If n is even, take all subsets of cardinality $> \frac{n}{2}$ and one set from each pair (A, A^C) with $|A| = \frac{n}{2}$.

Example 4: Consider the subset of $[7]$:

$$S := \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\}.$$

Define

$$\mathcal{F} := \{A \subseteq [7] \mid A \supseteq [\text{some set in } S]\}.$$

Then $|\mathcal{F}| = 2^{7-1} = 2^6 = 64$, and this is an intersecting family of sets. This is derived from a Steiner triple system, which we'll study further in the future.

Definition: The family \mathcal{F} is t -intersecting if $|A \cap B| \geq t$ for all $A, B \in \mathcal{F}$.

Theorem 7.1.2: (Erdős-Ko-Rado) Given k and t , there are n_1 and n_2 with $n_1 \leq n_2$ such that

- (1) If $n \geq n_1$, then the largest t -intersecting family in $\binom{[n]}{k}$ has $\binom{n-t}{k-t}$ sets.
- (2) If $n \geq n_2$, the only way to achieve this is by fixing a t element subset.

1.5.2 Sperner Families (Antichains)

Definition: \mathcal{F} is Sperner if $A \not\subseteq B$ and $B \not\subseteq A$ for all $A, B \in \mathcal{F}$.

Sperner's Theorem: [[*Could be on Qualls!*]] We have $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$ for all Sperner families $\mathcal{F} \subseteq 2^{[n]}$.
Moreover, equality holds only if

$$\mathcal{F} = \binom{[n]}{\lfloor n/2 \rfloor} \quad \text{or} \quad \mathcal{F} = \binom{[n]}{\lceil n/2 \rceil}.$$

Remark: The original proof was much more complicated. The one presented here is called the **LYM** proof (after Lubell Yamamoto Meshalkin) and is very well known.

Proof (LYM): A saturated chain (called just a “chain” for the remainder of the proof) in $2^{[n]}$ is a chain

$$\emptyset = A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n = [n].$$

There is a bijection between these and permutations:

$$A_i = \{\pi(1), \dots, \pi(i)\}, \quad \pi(i) = A_i \setminus A_{i-1}.$$

Note that \mathcal{F} contains at most one element of every chain. Suppose $|A| = k$. Then A is contained in $k!(n-k)!$ chains. So, as a proportion, A is contained in

$$\frac{k!(n-k)!}{n!} = \frac{1}{\binom{n}{k}}$$

of all chains. The number of chains which contain an element of \mathcal{F} is

$$\begin{aligned} \sum_{A \in \mathcal{F}} |A|!(n-|A|)! &= n! \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \\ &\leq n! = (\text{the total number of chains}). \end{aligned}$$

So,

$$\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1.$$

The summand is smallest when $|A| = \lfloor n/2 \rfloor$ or $|A| = \lceil n/2 \rceil$. Hence,

$$1 \geq \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \geq \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} = \frac{|\mathcal{F}|}{\binom{n}{\lfloor n/2 \rfloor}}.$$

Hence

$$|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$$

and the same is true for $\lceil n/2 \rceil$. This proves the first part of the theorem.

When n is even, to achieve equality, we must have $\mathcal{F} = \binom{[n]}{n/2}$.

When n is odd, we may worry about having $|A| = \lfloor n/2 \rfloor$ and $|B| = \lceil n/2 \rceil$. Suppose to the contrary that this situation happens for $A, B \in \mathcal{F}$. Then, we can remove elements of A and add elements of B one at a time:

$$A = A_0 \subsetneq B_0 \supsetneq A_1 \subsetneq B_1 \supsetneq \cdots \supsetneq A_k \subsetneq B.$$

This is a contradiction because if $A = A_0$ is in the Sperner family, then B_0 cannot be. Hence, A_1 is in the Sperner family, and so B_1 cannot be. Repeating this process, B is not in the Sperner family. \square

1.5.3 The de Bruijn-Erdős Theorem

Theorem: Let \mathcal{F} be a family of subsets of $[n]$ such that every two sets in \mathcal{F} intersect in exactly one element. Then $|\mathcal{F}| \leq n$. Moreover, equality holds if and only if (up to relabeling) $\mathcal{F} = \{A_1, \dots, A_n\}$ and :

- (a) $A_i = \{i, n\}$, or
- (b) $A_i = \{i, n\}$ for $i \leq n-1$ and $A_n = [n-1]$, or
- (c) $n = q^2 + q + 1$, $|A_i| = q + 1$, and every element lies in $q + 1$ sets.

Proof: We start with some notation:

- $\mathcal{F} := \{A_1, \dots, A_b\}$
- $r_i := [\# \text{ of sets containing } i]$ (the “replication number”)

We make the following assumptions:

- $b \geq n$ (otherwise there is nothing to prove),
- $[n] \notin \mathcal{F}$ (otherwise its impossible for the other sets to intersect each other if $n > 2$),
- no element lies in every set (otherwise we’re in **case (a)** above and we’re done).

We start by double counting three things:

- (1) Pairs (A_j, i) with $i \in A_j$. We can count these pairs by

$$\sum_{j=1}^b |A_j| = \sum_{i=1}^n r_i =: N.$$

- (2) Triples (A_j, A_k, i) such that $i \in A_j \cap A_k$ and $j \neq k$. We can count these triples by

$$b(b-1) = \sum_{i=1}^n r_i(r_i - 1).$$

This is true because any two sets intersect in a unique element, so we can pick from b sets to pick A_j and from $b-1$ sets to pick A_k . Alternatively, we can count by i , first picking one of the r_i sets that i is in, then picking one of the remaining sets that i is in.

- (3) Triples (A_j, i, i') with $\{i, i'\} \subseteq A_j$ and $i \neq i'$. We can count these triples by

$$n(n-1) \geq \sum_{j=1}^b |A_j|(|A_j| - 1).$$

The left hand side is the number of ways to pick any two elements where order matters, and the right hand side is the number of ways to pick any two elements where order matters which are in the same set, from all b sets.

We’ve assumed $b \geq n$, so focus on A_1, \dots, A_n . We now claim that the family $\{A_1^C, \dots, A_n^C\}$ satisfies Hall’s Condition, i.e.,

$$\left| \bigcup_{j \in J} A_j^C \right| \geq |J|$$

for all $J \subseteq [n]$. By **DeMorgan’s Law**, we’re claiming that

$$\left| \left(\bigcap_{j \in J} A_j \right)^C \right| \geq |J|.$$

We show this in three cases:

Case 1: ($|J| = 1$) Since $[n] \notin \mathcal{F}$, $|A_j^C| \geq 1 = |J|$.

Case 2: ($2 \leq |J| \leq n - 1$) By assumption the intersection of two or more sets has size at most 1, and so its complement has size at least $n - 1$, while $|J|$ is at most $n - 1$.

Case 3: ($|J| = n$) By assumption, no element is in all the sets. So, this intersection is empty and its complement is everything. So in this case we have equality.

Hence Hall's Condition is satisfied. So, (after relabeling) we have that $i \in A_i^C$, i.e., $i \notin A_i$, for all $i \in [n]$.

Now we claim that if $i \notin A_j$, then $r_i \leq |A_j|$. To see this, note that the sets containing i must intersect A_j in *different* points (otherwise, they would intersect each other in more than one point). This proves the claim.

Now, by our double-counting in (3), we have

$$\begin{aligned}
 n(n-1) &\geq \sum_{j=1}^b |A_j|(|A_j| - 1) \\
 &= \left[\sum_{j=1}^b |A_j|^2 \right] - N && \text{(double counting in (1))} \\
 &\geq \left[\sum_{j=1}^n r_j^2 \right] - N && \text{(claim above)} \\
 &= \sum_{i=1}^n r_i(r_i - 1) && \text{(double counting in (1))} \\
 &= b(b-1). && \text{(double counting in (2))}
 \end{aligned}$$

So, $b \leq n$, which shows the first part of the theorem.

It remains to show the equality cases. To have equality, we need:

- $r_i = |A_i|$ for all i , and
- $n(n-1) = \sum |A_j|(|A_j| - 1)$, i.e., every two elements lie in some set together, and
- if $i \notin A_j$, then $r_i = |A_j|$.

We handle two cases.

Case 1: ($r_x \neq r_y$ for some $x \neq y$) If $x, y \notin A_j$, then $r_x = |A_j| = r_y$, which is a contradiction. So, every set has either x or y in it (or both). Now choose z so that $r_z \neq r_x$ and by the above, every set has either x or z (or both). Since we said every two elements lie in a set together, there must be some set which contains y and z . Then, every other set must contain x . This case ends up being case (b) in the equality condition.

Case 2: ($r_x = r_y$ for all x, y) Let q be defined such that $r_x = q + 1$, i.e., $q := r_x - 1$. Well, $|A_j| = q + 1$ for all j . Now fix some x . Then, $q + 1$ sets contain x , and each has q other elements. So,

$$n = 1 + (q + 1)q = q^2 + q + 1.$$

This is case (c) in the equality condition.

The proof is now complete. \square

1.6 Chapter 8 - Steiner Triple Systems & Design Theory

1.6.1 Steiner Systems

Historical Note: In the “Lady’s and Gentleman’s Diary” in 1845, they asked: given integers ℓ, m, n with $\ell < m < n$ what is the largest family

$$\mathcal{B} \subseteq \binom{[n]}{m}$$

such that every $L \in \binom{[n]}{\ell}$ lies in at most one set in \mathcal{B} . The readers of the “Lady’s and Gentleman’s Diary” were not able to solve this. However, a guy named Kirkman (who was a vicar) became interested in mathematics upon seeing this problem and provided a solution for the $\ell = 2, m = 3$ case.

Proposition 7.1.1: Given the setup in the note above,

$$|\mathcal{B}| \leq \frac{\binom{n}{\ell}}{\binom{m}{\ell}}.$$

Proof: We double-count the pairs (L, B) where $L \in \binom{[n]}{\ell}$ and $B \in \mathcal{B}$ with $L \subseteq B$. Well, we can count this by

$$\# \text{ pairs} = |\mathcal{B}| \binom{m}{\ell}$$

and

$$\# \text{ pairs} \leq \binom{n}{\ell}.$$

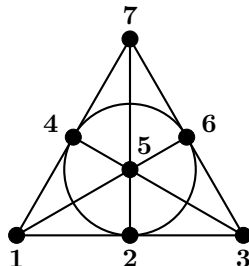
Solving this for $|\mathcal{B}|$ gives us the result. \square

Remark: This is a mostly naive and obvious bound, as is usual when working with families of sets. We care much more about when equality holds.

Definition: When we have equality, every ℓ -element set lies in precisely one set in \mathcal{B} . This is a Steiner system $S(\ell, m, n)$.

Definition: When $\ell = 2$ and $m = 3$ we call it a Steiner triple system and denote $STS(n) := S(2, 3, n)$.

Example: We can draw $STS(7)$ as:



Remark: We can ask: for what values of n do $STS(n)$ exist?

n	$STS(n)$
0	Yes
1	Yes
2	No
3	Yes
4	?
5	?
6	?
7	Yes

The $n = 0, 1, 2$ cases are vacuous. If $n = 0, 1$ there are no pairs and there are no triples. If $n = 2$, there is a pair, but no triple to put it in. We will return to the $n = 4, 5, 6$ case later.

Proposition: Let \mathcal{B} be an $STS(n)$. Then every element lies in $\frac{n-1}{2}$ triples (for $n > 0$).

Proof: Fix x . Count pairs (y, B) where $x, y \in B \in \mathcal{B}$. Well,

$$\# \text{ pairs} = n - 1.$$

Say that x lies in b triples, then,

$$\# \text{ pairs} = 2b.$$

$$\text{So, } b = \frac{n-1}{2}. \quad \square$$

Remark: This tells us that n must be odd (or zero) in order to have a Steiner triple system. This answers the question for $n = 4$ and $n = 6$ in the above table: there do not exist such systems.

Proposition: $|\mathcal{B}| = \frac{n(n-1)}{6}$.

Proof: We double-count the pairs (x, B) with $x \in B \in \mathcal{B}$. Well,

$$\# \text{ pairs} = \frac{n(n-1)}{2}$$

and

$$\# \text{ pairs} = |\mathcal{B}| \cdot 3.$$

So,

$$|\mathcal{B}| = \frac{n(n-1)}{6}. \quad \square$$

Remark: This rules out the case $n = 5$ in our table above.

Remark: Consider the cases $n \equiv 1, 3, 5 \pmod{6}$.

- If $n = 6k + 1$, then

$$\frac{n(n-1)}{6} = \frac{(6k+1)(6k)}{6} \text{ is an integer.}$$

- If $n = 6k + 3$, then

$$\frac{n(n-1)}{6} = \frac{(6k+3)(6k+2)}{6} \text{ is an integer.}$$

- If $n = 6k + 5$, then

$$\frac{n(n-1)}{6} = \frac{(6k+5)(6k+4)}{6} = \frac{(6k+5)(3k+2)}{3} \text{ is not an integer.}$$

This proves **Theorem 7.1.2**: if $STS(n)$ exists, then either $n \equiv 1 \pmod{6}$ or $n \equiv 3 \pmod{6}$. We next show that in either case we can build a Steiner triple system.

1.6.2 A Direct Construction

Construction of $STS(n)$ for $n \equiv 3 \pmod{6}$:

Set $n \equiv 3 \pmod{6}$. So, $n = 3m$ where m is odd. We label the elements with three copies of \mathbb{Z}_m , so that

$$X := \{a_i, b_i, c_i \mid i \in \mathbb{Z}_m\}.$$

We have two types of blocks of \mathcal{B} :

- (1) Diagonal blocks: $a_i b_i c_i$
- (2) Blocks of the form $a_i a_j b_k, b_i b_j c_k, c_i c_j a_k$, where $i \neq j$ and $i + j \equiv 2k \pmod{m}$.

Consider the case $i + j \equiv 2k \pmod{m}$. Given k, i (or k, j), we can solve for the remaining term (uniquely, modulo m): because m is odd, $\gcd(2, m) = 1$, and so 2 has multiplicative inverse $(m+1)/2$ modulo m , and thus given i, j we can also find k uniquely.

We need to check that every pair lies in a unique block. We have three cases (all calculations performed modulo m):

Case 1: If we have a_i, a_j with $i \neq j$ then this uniquely determines the block $a_i a_j b_{(i+j)/2}$.

Case 2: If we have b_i, b_j or c_i, c_j with $i \neq j$, then again this uniquely determines a block as in the previous case.

Case 3: Consider a_i, b_i . These are contained in $a_i b_i c_i$. If they were contained in another block, it would have to be $a_i a_j b_i$ which would force $i + j = 2i$ and so $i = j$, which we eliminated in our definition of blocks of this form.

Case 4: If we have b_i, c_i or a_i, c_i , then this is similar to the previous case.

Case 5: If we have a_i, b_k then this is in the block $a_i b_{2k-i} b_k$.

Case 6: If we have a_i, c_k or b_i, c_k , this is similar to the previous case.

This completes the proof. \square

Remark: The construction of a Steiner triple system for $n \equiv 1 \pmod{6}$ is recursive, and is complicated. Before we present it, we look at some less general constructions.

Proposition 8.5.2: Let $B_1, \dots, B_t \in \binom{\mathbb{Z}_n}{3}$ so that for every nonzero $u \in \mathbb{Z}_n$, there is a unique $i \in [t]$ and then a unique $x, y \in B_i$ so that $u = x - y$. Set

$$\mathcal{B} := \{B_i + z \mid i \in [t], z \in \mathbb{Z}_n\}$$

where

$$B_i + z := \{b + z \mid b \in B_i\}.$$

Then, $(\mathbb{Z}_n, \mathcal{B})$ is an STS. These are called Netto systems.

Proof: Take $x, y \in \mathbb{Z}_n$ with $x \neq y$. When are $x, y \in B_i + z$? Exactly when $x - z, y - z \in B_i$. Notice that

$$(x - z) - (y - z) \neq 0$$

and so there is a unique i and unique $x - z, y - z \in B_i$ such that

$$x - y = (x - z) - (y - z).$$

Every $x \neq y \in \mathbb{Z}_n$ this lies in a unique triple $B_i + z$. \square

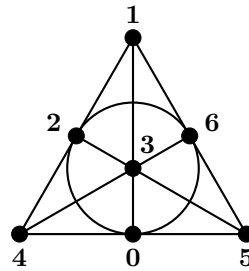
Example: Consider $n = 7$ and $B_1 = \{0, 1, 3\}$. Then, the differences (modulo 7) are

$$1 = 1 - 0 \quad 2 = 3 - 1 \quad 3 = 3 - 0 \quad 4 = 0 - 3 \quad 5 = 1 - 3 \quad 6 = 0 - 1$$

and these are unique. So, the construction gives us the triples:

$$(0, 1, 3) \quad (1, 2, 4) \quad (2, 3, 5) \quad (3, 4, 6) \quad (4, 5, 0) \quad (5, 6, 1) \quad (6, 0, 2).$$

Drawing this:



and we see that this is the same as our previous drawing of $STS(7)$.

Recall: Earlier, we double counted:

$$\# \text{ of triples} = \frac{n(n-1)}{6} = tn$$

where $t = \frac{n-1}{6}$. So, in this case we need $n \equiv 1 \pmod{6}$.

Construction:

Take $p \equiv 1 \pmod{6}$ to be prime. Then, \mathbb{Z}_p contains a primitive 6th root of unity. Recall that the multiplicative group \mathbb{Z}_p^* of \mathbb{Z}_p has order $p-1$ and is cyclic. Since $6 \mid p-1$ we have $6 \mid |\mathbb{Z}_p^*|$. There exists x such that $\mathbb{Z}_p^* = \{x, x^2, x^3, \dots, x^{p-1} = 1\}$. Define $z := x^{(p-1)/6}$ and observe that now z is a 6th root of unity in \mathbb{Z}_p . So, $z^6 = 1$, and

$$0 = z^6 - 1 = (z^3 - 1)(z + 1)(z^2 - z + 1).$$

Since z is a primitive 6th root of unity, we can't have $z^3 - 1 = 0$ or $z + 1 = 0$. Therefore, $z^2 - z + 1 = 0$, i.e., $z^2 = z - 1$.

Let $B_1 := \{0, 1, z\}$ and consider the following table.

u	$x - y$
1	1 - 0
z	$z - 0$
z^2	$z - 1$
z^3	$z^2 - z = 0 - 1$
z^4	$0 - z$
z^5	$0 - z^2 = 1 - z$

Let $t = (p-1)/6$. Let s_1, \dots, s_t be coset representatives for (z) in \mathbb{Z}_p^* . Each a can be written uniquely as

$$a = s_i z^j.$$

Each $s_i z^j$ can be written uniquely as

$$s_i z^j = s_i(x - y) = s_i x - s_i y$$

for $x, y \in \{0, 1, z\}$. Now set

$$B_i := \{0, s_i, s_i z\}.$$

For $n = 7$ we can pick $z = 3$ and we get $B_1 = \{0, 1, 3\}$.

For $n = 13$ we can pick $z = 4$ which generated $\langle 4 \rangle = \{4, 3, 12, 9, 10, 1\}$. Pick coset representatives 1 and 2. Then,

$$B_1 = \{0, 1, 4\}$$

and

$$B_2 = \{0, 2, 8\}.$$

Construct $STS(13)$ from the algorithm.

1.6.3 A Recursive Construction

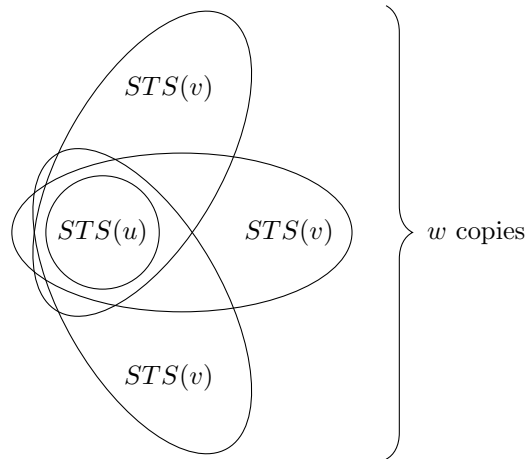
Definition: Suppose (X, \mathcal{B}) is a Steiner triple system. If $Y \subseteq X$ such that $\left(Y, \mathcal{B} \cap \binom{Y}{3}\right)$ is an STS, then Y is a subsystem of (X, \mathcal{B}) .

Proposition 8.3.1: If we have

- (1) an $STS(v)$ with an $STS(u)$ subsystem, and
- (2) an $STS(w)$,

then we can build an $STS(u + w(v - u))$. If $w > 0$, this Steiner triple system contains an $STS(v)$ subsystem. If $v > u > 0$ and $w > 0$, then this Steiner triple system contains an $STS(7)$ subsystem.

Proof: The picture below demonstrates the general idea of the construction:



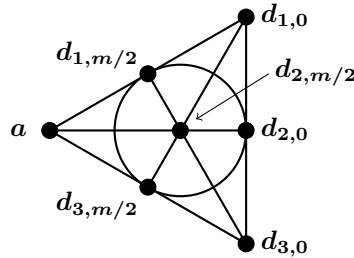
Let the $STS(v)$ be labeled as $\underbrace{\{a_1, \dots, a_u\}}_{STS(u)} \cup \{b_i \mid i \in \mathbb{Z}_m\}$ where $m := v - u$. Let the $STS(w)$ be labeled as $\{c_1, \dots, c_w\}$. Set $X := \{a_1, \dots, a_u\} \cup \{d_{p,i} \mid p \in [w], i \in \mathbb{Z}_m\}$.

The blocks are:

- (1) the blocks for each copy of $STS(v)$,
- (2) the blocks of the form $\{d_{p_1, i_1}, d_{p_2, i_2}, d_{p_3, i_3}\}$, where
 - (i) $c_{p_1}, c_{p_2}, c_{p_3}$ is a triple in the $STS(w)$
 - (ii) $i_1 + i_2 + i_3 \equiv 0 \pmod{m}$

Is each pair in a unique block? What about $(d_{p_1, i_1}, d_{p_2, i_2})$ where $p_1 \neq p_2$? The $STS(w)$ contains a unique triple $\{c_{p_1}, c_{p_2}, c_{p_3}\}$. Then, there is a unique i_3 such that $i_1 + i_2 + i_3 = 0$ in \mathbb{Z}_m . So, $\{d_{p_1, i_1}, d_{p_2, i_2}, d_{p_3, i_3}\}$ is this unique triple.

Now suppose $v > u > 0$ and $w > 0$. Then, $m = v - u$ is even (the only Steiner triple system of even size is the trivial one of size 0). Choose any point a in the $STS(u)$. Number the points of $STS(v) \setminus STS(u)$ so that $ab_0b_{m/2}$ is a triple of $STS(v)$. Suppose $c_1c_2c_3$ is a triple of $STS(w)$. Then we can construct triples $ad_{1, m/2}d_{1, 0}$, $ad_{2, m/2}d_{2, 0}$, and $ad_{3, m/2}d_{3, 0}$. Then, consider the subsystem:



The proof is complete. \square

Theorem: Let $A := \{n \mid STS(n) \text{ exists}\}$ and let $B := \{n \mid STS(n) \text{ exists with an } STS(7) \text{ subsystem}\}$. Then, A contains all integers congruent to 1 or 3 modulo 6, and $B = A \setminus \{0, 1, 3, 9, 13\}$.

Proof: We apply the above proposition with the following values:

Hypothesis	(u, v, w)	Conclusion
$n \in A$	$(0, n, 3)$	$3n \in A$
$n \in B$	$(0, n, 3)$	$3n \in B$
$n \in A, n > 1$	$(1, n, 3)$	$1 + 3(n - 1) = 3n - 2 \in B$
$n \in A, n > 3$	$(3, m, 3)$	$3n - 6 \in B$
$n \in B$	$(7, n, 3)$	$3n - 14 \in B$

Consider the residue classes $n \equiv 1, 3, 7, 9, 13, 15 \pmod{18}$. In the below table, we don't worry about $k = 1$ because we have already shown the existence of most of the base cases.

Need	Get
$6k + 1 \in A$	$18k + 1 = 3(6k + 1) - 2 \in B$
$6k + 3 \in A$	$18k + 3 = 3(6k + 3) - 6 \in B$
$6k + 3 \in A$	$18k + 7 = 3(6k + 3) - 2 \in B$
$6k + 3 \in B$	$18k + 9 = 3(6k + 3) \in B$
$6k + 9 \in B$	$18k + 13 = 3(6k + 9) - 14 \in B$
$6k + 7 \in A$	$18k + 15 = 3(6k + 7) - 7 \in B$

We now claim that every $n \equiv 1, 3 \pmod{6}$ with $n \geq 15$ lies in B , i.e., $B = A \setminus \{0, 1, 3, 9, 13\}$. Assume toward a contradiction that n is a minimal counterexample.

If $n = 18k + 1$ then $6k + 1 \notin A$ and so $6k + 1 < 15$. Thus $k < \frac{14}{6}$, which forces $18k + 1 < 43$. So $n = 19$ or $n = 37$. Well, $19 = 1 + 9(3 - 1)$ and $37 = 1 + 3(13 - 1)$ and the proposition applies in both

cases (we've previously built $STS(13)$, which is necessary here).

We don't need to check $18k + 3$ or $18k + 7$ because according to the table, those are always in A . It remains to check $18k + 9$, $18k + 13$, and $18k + 15$, but these follow the same argument. \square

1.7 Chapter 9 - Finite Geometry

1.7.1 Linear Algebra over Finite Fields

Theorem: There is a field of order q if and only if $q = p^m$ for some prime p and $m \in \mathbb{N}$. This field is unique and is denoted $\text{GF}(q)$.

Definition: The matrix A is in reduced echelon form if:

- (1) The first nonzero entry in every row is a 1.
- (2) If the i^{th} row is nonzero, so is the $(i-1)^{\text{st}}$ and the leading 1 in the $(i-1)^{\text{st}}$ row lies to the left of the leading 1 in the i^{th} row.
- (3) The leading 1's are the unique nonzero entries in their columns.

1.7.2 Gaussian Coefficients

Definition: $V(n, q)$ denotes the vector space of dimension n over $\text{GF}(q)$.

Proposition 9.2.1: The number of vectors in $V(n, q)$ is q^n .

Proof: There are n entries. For each, we have q choices. \square

Definition: $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k -dimensional subspaces of $V(n, q)$.

Definition: $[n]_q := \frac{q^n - 1}{q - 1}$.

Remark: $\lim_{q \rightarrow 1} [n]_q = \lim_{q \rightarrow 1} \frac{q^n - 1}{q - 1} = \lim_{q \rightarrow 1} 1 + q + q^2 + \dots + q^{n-1} = n$.

Definition: $[n]_q! := [n]_q [n-1]_q \dots [1]_q$. These are called " q -analogues".

Theorem 9.2.2:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q! [n-k]_q!} = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}.$$

Proof: Choose rows (vectors) in order to build a linearly independent set. For the first vector, there are $q^n - 1$ choices. For the second vector, there are $q^n - q$ choices. Proceeding this way, we see that the number of linearly independent sets of k vectors in $V(n, q)$ is

$$(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{k-1}) = (q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)q^{1+2+\dots+(k-1)}.$$

However, we wanted to count subspaces, not matrices. So, we have overcounted. Well,

$$\begin{aligned} \# \text{ of subspaces} &= \frac{\# \text{ of linearly independent sets of } k \text{ vectors in } V(n, q)}{\# \text{ of linearly independent sets of } k \text{ vectors in } V(k, q)} \\ &= \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)q^{\binom{k}{2}}}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)q^{\binom{k}{2}}} \\ &= \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \quad \square \end{aligned}$$

Example: $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$ = # of 2-dimensional subspaces of $V(4, q)$. To see this, we can construct matrices in reduced echelon form:

Form	# of matrices
$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}$	q^4
$\begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}$	q^3
$\begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	q^2
$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}$	q^2
$\begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	q
$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	1

So,

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1.$$

Mystery # 1: Why is this always a polynomial?

Mystery # 2: Why is the coefficient sequence always unimodal?

Remark: The first mystery is easy to show, the second mystery is complicated.

Theorem 9.2.3:
$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = q^k \begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n \\ k-1 \end{bmatrix}_q$$

Proof: The term on the left-hand side counts the $k \times (n+1)$ matrices over $\text{GF}(q)$ in reduced echelon form. The first term on the right-hand side counts the $k \times n$ matrices in reduced echelon form. The second term on the right-hand side counts the $(k-1) \times n$ matrices in reduced echelon form. We take a $k \times n$ matrix in reduced echelon form and add a column (which can have q^k different values), or we take a $(k-1) \times n$ matrix, add a row of all zeros, and then a column of all zeros with a 1 at the bottom. There is only one way to do this. Each way yields a $k \times (n+1)$ matrix in reduced echelon form. This is our bijection. \square

Proposition 9.2.4:
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$$

Proof: Map each subspace V to its orthogonal subspace V^\perp . This is a bijection. Of course $V = \{v \mid v \in V\}$ and $V^\perp = \{w \mid w \cdot v = 0 \forall v \in V\}$. Recall $\dim(V) + \dim(V^\perp) = n$. \square

Corollary:
$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{n+1-k} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q$$

Proof:

$$\begin{aligned} \begin{bmatrix} n+1 \\ k \end{bmatrix}_q &= \begin{bmatrix} n+1 \\ n+1-k \end{bmatrix}_q \\ &= q^{n+1-k} \begin{bmatrix} n \\ n-k+1 \end{bmatrix}_q + \begin{bmatrix} n \\ n-k \end{bmatrix}_q \\ &= q^{n+1-k} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q + \begin{bmatrix} n \\ k \end{bmatrix}_q. \end{aligned}$$

Lemma:
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q}{[k]_q} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$$

q -Binomial Theorem:

$$(1+x)(1+qx)(1+q^2x) \cdots (1+q^{n-1}x) = \sum_{k=0}^n q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k.$$

Note: If you take the limit at $q \rightarrow 1$, the original Binomial Theorem is recovered.

Proof: Proceed by induction on n . If $n = 1$, the right-hand side is

$$q^{\binom{0}{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix}_q x_0 + q^{\binom{1}{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}_q x_1 = 1 + x$$

which equals the left-hand side.

Now suppose the statement is true for n . So, we have that

$$\prod_{i=0}^{n-1} (1 + q^i x) = \sum_{k=0}^n q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k.$$

Multiply both sides by $1 + q^n x$ to get

$$\prod_{i=0}^n (1 + q^i x) = \left(\sum_{k=0}^n q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k \right) (1 + q^n x).$$

Consider the coefficient of x^k on the right-hand side of the above equation. It is:

$$q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q + q^n q^{\binom{k-1}{2}} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q.$$

Well,

$$\binom{k}{2} = \binom{k-1}{1} + \binom{k-1}{2}$$

and so

$$q^n q^{\binom{k-1}{2}} = q^{n+1-k} q^{\binom{k}{2}}.$$

Hence this coefficient is

$$q^{\binom{k}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{\binom{k}{2}} q^{n+1-k} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q = q^{\binom{k}{2}} \begin{bmatrix} n+1 \\ k \end{bmatrix}_q.$$

This completes the inductive step. So, the theorem is proved. \square

1.7.3 Projective Geometry

Definition: Let F be a field. Then, the projective geometry of dimension n over F , denoted $\text{PG}(n, F)$ is defined as the n -dimensional projective space of F defined in terms of $V := V(n+1, F)$, which is the vector space of dimension $n+1$ over F . The points of $\text{PG}(n, F)$ are the 1-dimensional subspaces of V , and the lines of $\text{PG}(n, F)$ are the 2-dimensional subspaces, etc. The textbook uses the notation that a “ k -flat” is $(k+1)$ -dimensional subspace, i.e. a 0-flat is a line, a 1-flat is a plane, etc.

Properties of Projective Geometries:

(a) Any two distinct points lie on a unique line.

Proof: Let P_1 and P_2 be two points. These are 1-dimensional subspaces of V . If $P_1 \neq P_2$, then $\dim(\text{span}_V(P_1, P_2)) = 2$. \square

(b) Any two distinct intersecting lines lie on a unique plane (for $n \geq 3$).

Proof: Let L_1 and L_2 be two distinct intersecting lines. Then, $\dim(L_1 \cap L_2) = 1$ and so $\dim(L_1 \cup L_2) = \dim(L_1) + \dim(L_2) - \dim(L_1 \cap L_2) = 2 + 2 - 1 = 3$. \square

(c) Any two coplanar lines intersect.

Proof: Use the formula from part (b). Since they’re coplanar, $\dim(L_1 \cup L_2) = 3$. This forces $\dim(L_1 \cap L_2) = 1$, i.e., the lines intersect. \square

(d) Let $F = \text{GF}(q)$ for a prime power q . Define $\text{PG}(n, q) := \text{PG}(n, \text{GF}(q))$. The number of points in $\text{PG}(n, q)$ is

$$\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = \frac{q^{n+1} - 1}{q - 1} = 1 + q + q^2 + \cdots + q^n.$$

The number of lines is

$$\begin{bmatrix} n+1 \\ 2 \end{bmatrix}_q.$$

The number of k -flats is

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q.$$

Remark: (de Bruijn-Erdős) The third option from the de Bruijn-Erdős theorem (which we did not know the existence of) is $\text{PG}(2, q)$ which as claimed has $1 + q + q^2$ points.

Proposition 9.5.1: In $\text{PG}(2, q)$ (also called the projective plane of order q), the following hold:

- (1) Every point lies on $q + 1$ lines.
- (2) Two lines meet in a unique point.
- (3) There are $q^2 + q + 1$ lines.

Proof: Take a point P . There are $q^2 + q = q(q + 1)$ other points. Every line through P contains q other points, with no overlaps. So, the number of lines through P is $q(q + 1)/q = q + 1$.

Let L_1 and L_2 be lines, where $P \in L_1$. Then $|L_2| = q + 1$, and each point of L_2 lies on a unique line with p . So, L_1 and L_2 intersect in a unique point.

Count (p, L) with $p \in L$. Then,

$$(\# \text{ of lines})(q + 1) = (q^2 + q + 1)(q + 1)$$

and so the number of lines is $q^2 + q + 1 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q$. \square

So, for a projective plane (X, \mathcal{L}) , where X is the set of points and \mathcal{L} is the set of lines, we can send it to its dual by interchanging points and lines, i.e. the map $(X, \mathcal{L}) \rightarrow (X^*, \mathcal{L}^*)$ is defined by $X^* := \mathcal{L}$ and

$$\mathcal{L}^* := \{\mathcal{B}_x \mid x \in X\}$$

where

$$\mathcal{B}_x := \{L \in \mathcal{L} \mid x \in L\}.$$

Veblen-Young Theorem: Let \mathcal{L} be a family of subsets of X . Suppose:

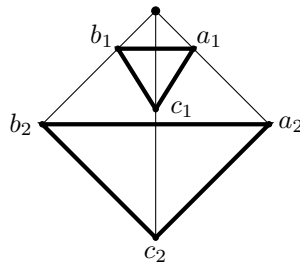
- (1) Every line has ≥ 3 points.
- (2) Every pair of points lies on a unique line.
- (3) There are at least two disjoint lines.
- (4) If a line meets two sides of a triangle not at their intersection, then it meets the third side.

(Note that condition (4) is not true in \mathbb{R}^2 ! However, it is true in projective spaces.) Then, \mathcal{L} can be identified with a projective space $\text{PG}(n, q)$ for $n \geq 3$ and q a prime power.

Bruck-Ryser Theorem: If a projective plane of order $n \equiv 1$ or $2 \pmod{4}$ exists, then n is the sum of squares. This shows us that there are no projective planes of order 6, for example.

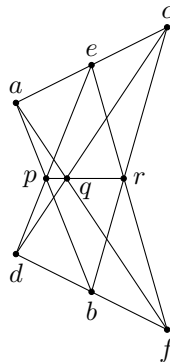
Remark: Next, we'd like to recognize the families of sets that correspond to $\text{PG}(2, q)$ for some q .

Desargue's Theorem: Let $a_1b_1c_1$ and $a_2b_2c_2$ be two triangles in the projective plane Π . Suppose that the lines a_1a_2 , b_1b_2 , and c_1c_2 are concurrent (i.e., all three intersect at a common point).



Then, if $p := b_1c_1 \cap b_2c_2$ and $q := c_1a_1 \cap c_2a_2$ and $r := a_1b_1 \cap a_2b_2$, we have that p, q, r are collinear.

Pappus' Theorem: Let a, b, c, d, e, f be points of a projective plane Π . Suppose a, c, e are collinear and that b, d, f are collinear. Let $p := ab \cap de$, $q := bc \cap ef$, $r := cd \cap fa$. Then, p, q, r are collinear.



Definition: Define the affine plane $AP(2, q)$ such that

- there are q^2 points,
- every two points are on a unique line.

Example: $STS(9) = AP(2, 3)$. We call this the affine plane of order 3.

Remark: Two lines have at most 1 point in common, by the second property above.

Definition: Two lines are said to be parallel if they are either equal or disjoint.

Proposition 9.5.6: In $AP(2, q)$,

- (1) Each point lies in $q + 1$ lines.
- (2) There are $q(q + 1)$ lines.
- (3) Euclid's parallel postulate holds: Given a point P and a line L there is a unique L' with $P \in L'$ and $L' \parallel L$.
- (4) Parallelism is an equivalence relation.

Proof of (1): $\frac{q^2 - 1 \text{ other points}}{q - 1 \text{ other points per line, without overlap}} = q + 1 \text{ lines. } \square$

Proof of (2): We double-count (p, L) with $p \in L$:

$$q^2(q+1) = |\{\text{Lines}\}|q$$

and so $|\{\text{Lines}\}| = q(q+1)$. \square

Proof of (3): Take a point P and a line L . If $P \in L$, we're done. If $P \notin L$, then of the $q+1$ lines containing P , one of them must be disjoint from L . Set this line to be L' . \square

Proof of (4): The reflexive and symmetric properties are obvious. Let $L \parallel J$ and $J \parallel K$. We want to show $L \parallel K$. This is trivially true if any two of L, J, K are equal. So assume now that no two are equal. Suppose toward a contradiction that $P \in L \cap K$. By the parallel postulate, there is a unique line through P which is parallel to J . Since both L and K have this property, we must have $L = K$, a contradiction. \square

Remark: Each parallel class contains q lines: By Euclid's parallel postulate, each parallel class covers the point set. No two lines in a parallel class intersect, and they all have q points. So, the size of the parallel class is $\frac{q^2}{q} = q$.

Remark: There are $q+1$ parallel classes. There is one class for every line through some point P . Any point P lies on $q+1$ lines.

Theorem 9.5.7: $\text{PG}(2, q)$ exists if and only if $\text{AP}(2, q)$ exists.

Proof: Suppose (X, \mathcal{B}) is a $\text{PG}(2, q)$. Fix $L \in \mathcal{B}$. Remove it and its points. Define

$$X' := X \setminus L$$

and

$$\mathcal{B}' := \{L' \setminus L \mid L' \in \mathcal{B}, L' \neq L\}.$$

Each of these new lines has q points. So,

$$|X'| = (q^2 + q + 1) - (q + 1) = q^2$$

and

$$|\mathcal{B}'| = (q^2 + q + 1) - 1 = q(q + 1).$$

Additionally, we need that two points lie on a unique line. Since we started with a projective plane any two points do lie on a unique line (any points that lie on the line we removed were also removed). So, (X', \mathcal{B}') is an $\text{AP}(2, q)$.

Conversely, suppose (X, \mathcal{B}) is an $\text{AP}(2, q)$. We need to add in $q+1$ elements and 1 line. Let \mathcal{P} be the set of parallel classes. Define

$$X^* := X \cup \mathcal{P}$$

(for now, we are thinking of each parallel class as simply an object). For $L \in \mathcal{B}$, define $L^* := L \cup \{C\}$ where $L \in C \in \mathcal{P}$. Define

$$\mathcal{B}^* := \{L^* \mid L \in \mathcal{B}\} \cup \{\mathcal{P}\}.$$

Are two points in a unique line? We handle three cases:

- (1) If $x, y \in X$, then they were on a unique line L and so now they're on a unique line L^* .
- (2) If $x \in X$ and $C \in \mathcal{P}$, then by Euclid's parallel postulate, there is a unique line through x parallel to the lines of C , say L . Then, $L^* \ni x, C$.

- (3) If $C_1, C_2 \in \mathcal{P}$, then they can only be in the line \mathcal{P} since the other new lines contain only one parallel class each.

(This operation is known as “adding a line at infinity”.) So, (X^*, \mathcal{B}^*) is a $\text{PG}(2, q)$. \square

Definition: A set of Latin squares is mutually orthogonal if each pair is orthogonal. We call this a set of MOLS.

Question: How many $n \times n$ MOLS can we have?

Theorem 9.5.8: There exist $n - 1$ MOLS of order n if and only if $\text{AP}(2, n)$ exists.

Proof: Let $\{A_1, \dots, A_r\}$ be a set of MOLS of order n . Build a geometry (X, \mathcal{B}) where

$$X := \{(i, j) \mid i, j \in [n]\}.$$

The set \mathcal{B} of lines consists of:

- (1) Horizontal Lines: $\{(i, x) \mid x \in [n]\}$, where i is fixed.
- (2) Vertical Lines: $\{(x, j) \mid x \in [n]\}$, where j is fixed.
- (3) Other nr lines: for each A_m and fixed k , $L_{m,k} := \{(i, j) \mid (A_m)_{i,j} = k\}$.

Now, the number of points is n^2 . The number of lines is $n(r + 2)$ which is $n(n + 1)$ if $r = n - 1$. Is it true that two points are on at most one line. Take two points (i, j) and (i', j') .

- (1) If $i = i'$ then these points lie on a vertical line together, but they don't lie on another line because they're not together on a horizontal line (or they'd be the same point) and because $(A_m)_{i,j} \neq (A_m)_{i,j'}$, otherwise A_m would not be a Latin square.
- (2) If $j = j'$ then these points lie on a horizontal line together, but they don't lie on another line because they're not together on a vertical line (or they'd be the same point) and because $(A_m)_{i,j} \neq (A_m)_{i',j}$, otherwise A_m would not be a Latin square.
- (3) If $i \neq i'$ and $j \neq j'$, then the two points are not together on any vertical or horizontal lines. Suppose these points were in two lines of type 3, say $L_{m,k}$ and $L_{m',k'}$. Then,

$$(A_m)_{i,j} = (A_m)_{i',j'} = k \quad \text{and} \quad (A_{m'})_{i,j} = (A_{m'})_{i',j'} = k'.$$

This breaks the orthogonality condition. So, this is impossible.

This shows one direction of the proof, because if $r = n - 1$, then by a simple counting argument, every two points would be on *exactly* one line.

Conversely, suppose $\text{AP}(2, n)$ exists. Take two parallel classes:

$$\mathcal{H} = \{H_1, \dots, H_n\}, \quad \text{and} \quad \mathcal{V} = \{V_1, \dots, V_n\}.$$

Label the point set so that

$$H_i \cap V_j = \{(i, j)\}.$$

There are $n - 1$ other parallel classes. Take one:

$$\mathcal{L} = \{L_1, \dots, L_n\}.$$

Make $A^{\mathcal{L}}$ by:

$$(A^{\mathcal{L}})_{i,j} = k \text{ if } (i, j) \in L_k.$$

Are these Latin squares? If $(A^{\mathcal{L}})_{i,h} = (A^{\mathcal{L}})_{i,j'}$, then $(i, h), (i, j') \in L_k$. But, we know $(i, j), (i, j') \in H_i$, so $H_i = L_k$, which is a contradiction. So, no value appears twice in a row. Similarly, no value appears twice in a column. Thus, each $A^{\mathcal{L}}$ is in fact a Latin square. It remains to check mutual orthogonality.

Suppose that we have two ordered pairs

$$((A^{\mathcal{L}})_{i,j}, (A^{\mathcal{J}})_{i,j}), \quad ((A^{\mathcal{L}})_{i',j'}, (A^{\mathcal{J}})_{i',j'})$$

which are equal. Then,

$$(i, j), (i', j') \in L_a$$

and

$$(i, j), (i', j') \in J_b$$

which is a contradiction because L_a and J_b were in two different parallel classes. So, mutual orthogonality holds. \square

1.8 Chapter 10 - Ramsey Theory

1.8.1 The Pigeonhole Principle

Historical Note: In 1834, Dirichlet used a theorem which came to be called “Dirichletscher Schubfachprinzip”. Thankfully, in 1956, Erdős and Rado renamed it the “pigeonhole principle”. He used it to prove the following theorem.

Proposition 10.1.2: (Dirichlet, 1834) Let α be irrational. There are infinitely many rationals $\frac{p}{q}$ such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Proof: Define $\{x\}$ to be the fractional part of x . We claim that for every $n \in \mathbb{N}$, there is a rational $\frac{p}{q}$ such that $q \leq n$ and $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$.

This claim proves the proposition because:

- (1) If $\frac{p}{q}$ satisfies the claim, then $\frac{1}{q^n} \leq \frac{1}{q^2}$, so, $\frac{p}{q}$ satisfies the proposition.
- (2) There are infinitely many such $\frac{p}{q}$ because if we start with $n_1 := \frac{p_1}{q_1}$, then we can take n_2 so that $\left| \alpha - \frac{p_1}{q_1} \right| > \frac{1}{n_2}$ and take $\frac{p_2}{q_2}$ so that $\left| \alpha - \frac{p_2}{q_2} \right| < \frac{1}{q_2^2}$, then take n_3 so that $\left| \alpha - \frac{p_2}{q_2} \right| < \frac{1}{n_3}$, etc. This would prove the theorem.

Now we prove the claim. Consider the $n + 1$ numbers $\{i\alpha\}$ for $i \in [n + 1]$. Put these $\{i\alpha\}$ into n intervals $\left(\frac{j}{n}, \frac{j+1}{n} \right)$ for $j = 0, 1, \dots, n - 1$. By the pigeonhole principle, there is some interval with two, say $\{i_1\alpha\}$ and $\{i_2\alpha\}$. Set $q = |i_1 - i_2|$. We want a p such that $|q\alpha - p| < \frac{1}{n}$. This exists because $\{i_1\alpha - i_2\alpha\} < \frac{1}{n}$, so we pick p to be the nearest integer.

Therefore, $\left| \alpha - \frac{p}{q} \right| < \frac{1}{nq}$ and so the claim is proved. \square

Example: There is a number of the form $\underbrace{77 \dots 7}_{n \geq 1 \text{ digits}}$ which is divisible by 2003.

Proof: Take the first 2004 of these. Divide them into groups based on their remainders modulo 2003. Two have the same remainder, say:

$$\underbrace{77 \dots 7}_i \equiv \underbrace{77 \dots 7}_j \pmod{2003}.$$

Suppose $j > i$. Then, subtracting them, we get

$$2003 \mid \underbrace{77 \dots 7}_{j-i} \underbrace{00 \dots 0}_i.$$

Dividing this number by 10^i , we still get a number divisible by 2003 because 2003 and 10 have no common factors. \square

1.8.2 Ramsey's Theorem

Remark: Ramsey Theory is often associated with the quote “complete disorder is impossible”. The idea is encapsulated in the statement as “Among any 6 people, you can find 3 who either know each other or 3 who don't know each other.

Ramsey's Theorem: There is a number $R(k, \ell)$ such that if the edges of $K_{R(k, \ell)}$ (the “complete graph” of $R(k, \ell)$ vertices) are colored red and blue, then there is a red K_k or a blue K_ℓ .

Proof: Pick a vertex x . Each edge from x to another point is either red or blue. Group the other vertices by the color of the edge that joins them with x . If the blue set has a blue $K_{\ell-1}$ or a red K_k , then we're done. If the red set has a red K_{k-1} or a blue K_ℓ , then we're also done. So, we see that its possible to have $R(k, \ell)$ at least as small as:

$$R(k, \ell) \leq 1 + R(k, \ell - 1) + R(k - 1, \ell).$$

In fact, we can remove the 1, as well. So,

$$R(k, \ell) \leq R(k, \ell - 1) + R(k - 1, \ell). \quad \square$$

Remark: The above proof was given in the way you would derive it. Now knowing the result, we prove it in a more straight-forward way.

Proof: (Base case) $R(1, \ell) = R(k, 1) = 1$ because any graph has a K_1 of any color. Now set $n := R(k, \ell - 1) + R(k - 1, \ell)$. Color the edges of K_n red and blue. Consider a vertex v which has

$$R(k, \ell - 1) + R(k - 1, \ell) - 1$$

neighbors. If v has $R(k - 1, \ell)$ red neighbors, we're done. Otherwise v has $R(k, \ell - 1)$ blue neighbors, in which case we're also done. \square

Computations: Note that

$$R(k, 2) \leq R(k, 1) + R(k - 1, 2) = 1 + R(k - 1, 2).$$

Iterating this,

$$R(k, 2) \leq k.$$

Additionally, we can see that $R(k, 2) \geq k$ since K_{k-1} can be two-colored to avoid a red K_k or a blue K_2 (make everything red). So we have equality:

$$R(k, 2) = k.$$

Additionally,

$$R(3, 3) \leq R(3, 2) + R(2, 3) = 6.$$

Equality can be shown by construction.

Theorem: $R(k, \ell) \leq \binom{k + \ell - 2}{k - 1}$

Proof: True for $k = 1$ or $\ell = 1$. By induction and the previous theorem,

$$\begin{aligned} R(k, \ell) &\leq R(k, \ell - 1) + R(k - 1, \ell) \\ &\leq \binom{k + \ell - 3}{k - 1} + \binom{k + \ell - 3}{k - 2} \\ &= \binom{k + \ell - 2}{k - 1}. \quad \square \end{aligned}$$

Definition: The diagonal Ramsey numbers are the numbers $R(k, k)$.

Remark: Observe that

$$\begin{aligned} R(k, k) &\leq \binom{2k-2}{k-1} \\ &= \frac{(2k-2)(2k-3)\cdots 1}{(k-1)\cdots 1 \cdot (k-1)\cdots 1} \\ &\approx 2^{2k-2} \\ &= 4^{k-1}. \end{aligned}$$

So,

$$\lim_{k \rightarrow \infty} \sqrt[k]{R(k, k)} \leq 4,$$

if the limit exists. The limit is conjectured to exist, but this is unknown.

Remark: Can we find a lower bound? To do this, we would just need to be able to color a K_n . No one has been able to color with n exponential in k without a red or blue K_k .

Theorem: (Erdős) $R(k, k) > n - \binom{n}{k} 2^{1-\binom{k}{2}}$ for all n .

Proof: Take K_n and flip a coin for each edge. How many monochromatic K_k 's do we get? Suppose R is a k -subset of the vertices. Define

$$X_R := \begin{cases} 1, & \text{if } R \text{ is a monochromatic } K_k \\ 0, & \text{otherwise} \end{cases}.$$

Well, we see that

$$\mathbb{P}[X_R = 1] = 2 \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}} = 2^{1-\binom{k}{2}}.$$

The expected value $\mathbb{E}[X_R]$ is just

$$\mathbb{E}[X_R] = 2^{1-\binom{k}{2}}$$

since it's a 0-1 random variable and R is fixed. By linearity of expectation

$$\mathbb{E}[\# \text{ of monochromatic } K_k \text{'s}] = \sum_{k\text{-subsets}} \mathbb{E}[X_R] = \binom{n}{k} 2^{1-\binom{k}{2}}.$$

So, there exists some coloring which has $\binom{n}{k} 2^{1-\binom{k}{2}}$ monochromatic K_k 's or fewer. In fact, there must be some with fewer because there are some with more (for example, color everything red).

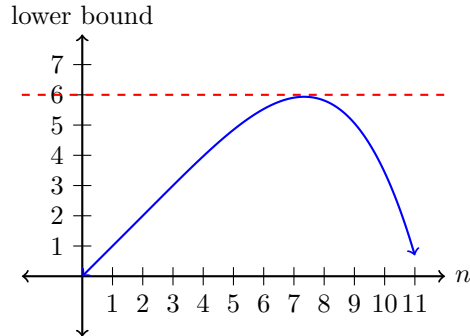
Delete one vertex from each of the monochromatic K_k 's. We will delete at most $\binom{n}{k} 2^{1-\binom{k}{2}} - 1$ vertices and be left with no monochromatic K_k 's. Hence,

$$R(k, k) > n - \binom{n}{k} 2^{1-\binom{k}{2}}. \quad \square$$

We need to justify the strict inequality.

Remark: Set $k = 4$ in the above theorem. Then,

$$R(4, 4) > n - \binom{n}{4} 2^{-5} = n - \frac{1}{32} \binom{n}{4}.$$



Hence, $R(4, 4) \geq 6$. Note that this is not really a good bound since $R(3, 3) = 6$ and we'd expect that $R(4, 4) \geq R(3, 3)$.

Remark: How can we find the best n ? Well, (using the approximation $\binom{n}{k} \approx \left(\frac{n}{k}\right)^k$),

$$\begin{aligned} \text{Bound} &= n - \binom{n}{k} 2^{1-\binom{k}{2}} \\ &\approx n - \left(\frac{n}{k}\right)^k 2^{1-\binom{k}{2}} \end{aligned}$$

Taking the derivative with respect to n :

$$1 - \left(\frac{n}{k}\right)^{k-1} 2^{1-\binom{k}{2}}.$$

Solving for where the derivative is zero:

$$\left(\frac{n}{k}\right)^{k-1} 2^{1-\binom{k}{2}} = 1$$

and so using the guess $n \approx k2^{k/2}$, we have

$$(2^{k/2})^{k-1} 2^{1-\binom{k}{2}} = 2^{\binom{k}{2}} 2^{1-\binom{k}{2}} = 2.$$

and $2 \approx 1$ so our guess for n was alright. Using more rigorous methods, we get

$$n \sim \frac{k}{e} 2^{k/2}.$$

Thus,

$$R(k, k) \text{ is approximately greater than } 2^{k/2} = \sqrt{2}^k.$$

We see

$$\sqrt{2} \leq \lim_{k \rightarrow \infty} \sqrt[k]{R(k, k)} \leq 4.$$

Remark: By the previous theorem, $R(4, 3) \leq R(4, 2) + R(3, 3) = 10$. In fact we will show that $R(4, 3) = 9$.

Theorem: $R(4, 3) = 9$,

First we show that all two-colorings of K_9 result in a red K_4 or a blue K_3 . Pick a vertex v of an arbitrary K_9 . If v has 6 red neighbors, then we're done. (This is because $R(3, 3) = 6$, so these 6 red neighbors have either a red K_3 (which combined with v makes a red K_4) or a blue K_3 .) If v has 4 blue neighbors, then we've got a blue K_3 or a red K_4 . (This is because if there is a blue edge between any of the 4 neighbors, we have a blue K_3 . If there is no blue edge between them, the neighbors form a red K_4 .) The only case remaining to check is the case where v has 5 red neighbors and 3 blue neighbors. Since v was arbitrary, in this case we can consider that all vertices simultaneously have 5 red neighbors and 3 blue neighbors. We claim that this cannot occur. For the sake of contradiction, assume that our K_9 has this property. We will double count (v, e) where v is a vertex of the red edge e . On one hand, each red edge has two vertices, so this is equal to $2(\# \text{ of red edges})$. On the other hand, there are 9 vertices and each has 5 red edges, so,

$$2(\# \text{ of red edges}) = 45,$$

which is a contradiction. Hence, we've shown that every K_9 has a red K_4 or a blue K_3 , i.e., $R(4, 3) \geq 9$.

To show $R(4, 3)$, we will construct a two-coloring of K_8 that has no red K_4 and no blue K_3 . The vertices will be elements of $[8]$. The edge between i and j (with $i < j$) is blue if $j - i \in \{1, 4, 7\}$ and red otherwise. Assume we have a blue K_3 . Let i be the smallest vertex in the blue K_3 . The blue neighbors of i are $i + 1, i + 4, i + 7$, but the edges between each of these three are red, so this is impossible. Assume we have a red K_4 . Let i be the smallest vertex in the red K_4 . The red neighbors of i are $i + 2, i + 3, i + 5, i + 6$. The edges between $(i + 2, i + 3), (i + 2, i + 6),$ and $(i + 5, i + 6)$ are all blue. The rest are red. By inspection, there can be no red K_4 .

So, $R(4, 3) = 9$. \square

Theorem: $R(4, 4) \geq 18$. (In fact we have equality, though we will only prove the given inequality.)

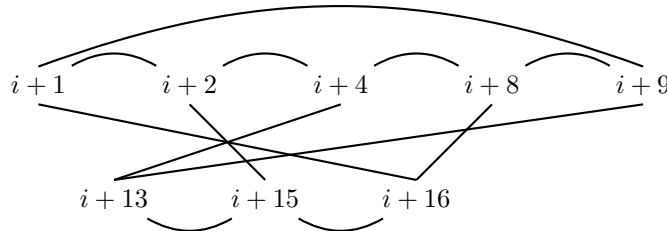
We start by two-coloring a K_{17} graph without a monochromatic K_4 . For $i < j$, the edge between i and j (with $i < j$) is red if

$$j - i \in \{1, 2, 4, 8, 9, 13, 15, 16\}$$

and is blue otherwise. Note that the set of red edge numbers is the set of quadratic residues modulo 17. Suppose toward a contradiction that this K_{17} has a red K_4 with smallest vertex i . The red neighbors of i are:

$$i + 1, i + 2, i + 4, i + 8, i + 9, i + 13, i + 15, i + 16.$$

We will draw the red edges between these and show that there is no triangle, hence no red K_4 .



We see by inspection that there is no triangle. Do the same thing for the blues. \square .

1.8.3 Applications of Ramsey's Theorem

Theorem: (Erdős-Szekeres) There exists a function $f(k, \ell)$ such that every permutation of $[f(k, \ell)]$ contains an increasing subsequence of length k or a decreasing subsequence of length ℓ .

Historical Note: This fact was used by Erdős and Szekeres in their work on the problem posed in the introduction to these notes.

Proof: Define $n := f(k, \ell) := R(k, \ell)$. Given $\pi \in S_n$, color $K_{[n]}$ by the rule that if $i < j$, we color the edge red if $\pi(i) < \pi(j)$ and blue if $\pi(i) > \pi(j)$. By Ramsey's Theorem (which guarantees the existence of such an $R(k, \ell)$) there exists either a red K_k or a blue K_ℓ . If we have a red K_k , then there is a sequence $i_1 < i_2 < \dots < i_k$ such that $\pi(i_1) < \pi(i_2) < \dots < \pi(i_k)$. Similarly, if there is a blue K_ℓ , then there is a sequence $j_1 < j_2 < \dots < j_\ell$ such that $\pi(j_1) > \pi(j_2) > \dots > \pi(j_\ell)$. \square

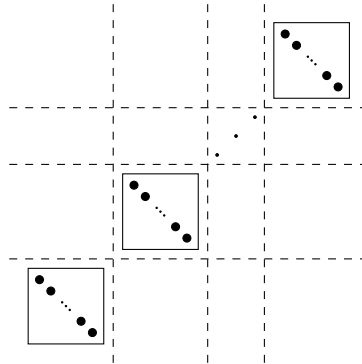
Remark: This gives us the inequality

$$f(k, \ell) \leq \binom{k + \ell - 2}{k - 1}$$

using the theorem regarding Ramsey numbers in the previous section.

Theorem: [*Could be on Qualls!*] $f(k, \ell) = (k - 1)(\ell - 1) + 1$

Proof: First we show that $f(k, \ell) \geq (k - 1)(\ell - 1) + 1$ by constructing a permutation of length $(k - 1)(\ell - 1)$ that contains neither an increasing subsequence of length k nor a decreasing subsequence of length ℓ . We arrange the permutation into $k - 1$ blocks, each which has $\ell - 1$ consecutive decreasing entries.



It's clear that this permutation has neither an increasing subsequence of length k nor a decreasing subsequence of length ℓ .

Now we show the reverse inequality. Set $n := (k - 1)(\ell - 1) + 1$. Let $\pi \in S_n$. Suppose there is no increasing subsequence of length k . For $a \in [k - 1]$, set

$$I_a := \{i \mid \text{the largest increasing subsequence ending at } \pi(i) \text{ has length } a\}.$$

By the Pigeonhole Principle, there exists some a such that $|I_a| \geq \ell$. Let I_a contain the sequence of indices:

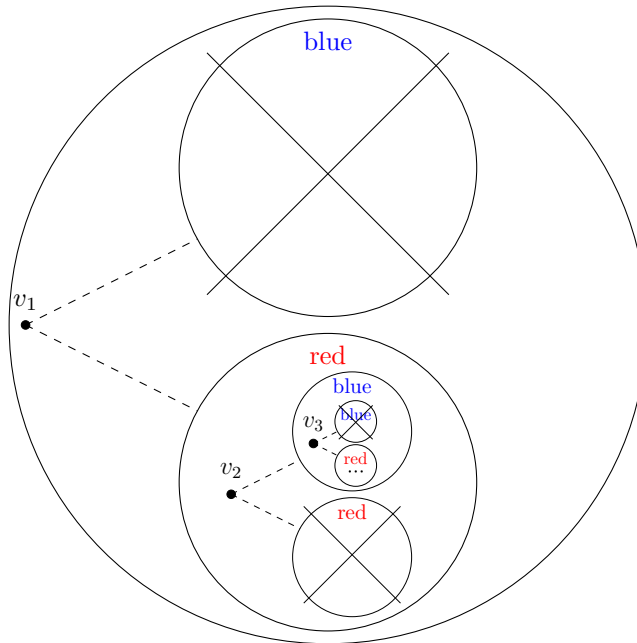
$$I_a \supseteq \{i_1 < i_2 < \dots < i_\ell\}.$$

By construction, we must have that $\pi(i_1) > \pi(i_2) > \dots > \pi(i_\ell)$, and so we have found a decreasing subsequence of length ℓ . \square

1.8.4 Infinite Ramsey's Theorem

Theorem: If we two-color the edges of an infinite complete graph, then we will get a monochromatic infinite complete graph of some color.

Proof: The idea of the proof is that we start with a vertex v_1 and consider the set of its blue neighbors and the set of its red neighbors. One of these sets must be infinite, so we pick that set, call it X_1 , and ignore the other one. Then, we pick v_2 in that set, consider its sets of neighbors *within* X_1 and repeat the process. Consider the picture:



Formally, define X_1 to be the set of all vertices and pick $v_1 \in X_1$. Define c_1 to be a color such that v_1 has infinitely many c_1 -neighbors in X_1 . Then, define X_2 to be the set of c_1 -neighbors of v_1 in X_1 , pick $v_2 \in X_2$, and define c_2 to be a color such that v_2 has infinitely many c_2 -neighbors. Observe that $X_1 \supseteq X_2 \supseteq \dots$ and that $|X_i| = \infty$ for all i . Repeat this process, and look at the c_i sequence. Necessarily, there is an infinite constant sequence

$$c_{i_1} = c_{i_2} = \dots$$

Set $Y = \{v_{i_1}, v_{i_2}, \dots\}$. We claim that this is the infinite monochromatic complete graph. To see this, consider the indices $i_a < i_b$. Then,

$$v_{i_b} \in X_{i_b} \subseteq X_{i_{a+1}} = \{c_{i_a}\text{-neighbors of } v_{i_a}\}. \quad \square$$

Many logicians are working in the field of "Reverse Mathematics". They try to prove statements like

$$[\text{Infinite Ramsey Theorem}] \implies [\text{Finite Ramsey Theorem}].$$

Of course, since both are true, looking at this statement from a basic logic point-of-view, it is a tautology. However, the real question is whether we can prove one directly from the other. In fact the statement above is true:

Proof: Suppose that the Finite Ramsey Theorem is false. Then, $R(k, \ell)$ does not exist for some k, ℓ . Say that a "good-coloring" is one which has neither a red K_k nor a blue K_ℓ . Set G_n to be the set of good-colorings of K_n . By assumption, $|G_n| \geq 1$ for all n .

Define G_n^j to be the set of restrictions of good-colorings of $[n+j]$ to $[n]$. Observe that

$$G_n = G_n^0 \supseteq G_n^1 \supseteq G_n^2 \supseteq \dots$$

Therefore

$$\bigcap_{i=0}^{\infty} G_n^i \neq \emptyset$$

because each G_n^i is finite and nonempty.

Define $H_n := \bigcap_{i=0}^{\infty} G_n^i$. Now take any coloring in H_n . We can extend it to an infinite good-coloring, which is a contradiction to the Infinite Ramsey Theorem, which proves the contrapositive.

We can also ask if the converse is true. Does the Finite Ramsey Theorem imply the Infinite Ramsey Theorem? In Peano Arithmetic, the answer is no. The following related theorem has a strange property.

Paris-Harrington Theorem: There exists a function $f(k)$ such that if we two-color the edges of $K_{[f(x)]}$, then there exists a monochromatic complete graph X such that $|X| \geq k$ and $|X| \geq \min(X)$.

This theorem is true, but is not provable in Peano Arithmetic.

Proof: Using Peano Arithmetic and the **Paris-Harrington Theorem**, we can prove the consistency of Peano Arithmetic. One of Gödel's Theorems says that no sufficiently rich set of axioms can prove its own consistency. This shows that the **Paris-Harrington Theorem** cannot be provable by Peano Arithmetic.

1.9 Chapter 12 - Posets, Lattices, Matroids

1.9.1 Posets and Lattices

Definition: A partial order on X is a relation R on X which is:

- (1) reflexive ($(x, x) \in R$),
- (2) antisymmetric (if $(x, y) \in R$ and $(y, x) \in R$, then $x = y$),
- (3) transitive (if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$).

Definition: The pair (X, R) is called a partially ordered set, or a poset.

Definition: A Hasse diagram is a graph where y covers x if $y \geq x$ and $y \neq x$ and there is no $z \neq x, y$ with $x \leq z \leq y$. We connect x, y with a line if y covers x .

Definition: A maximal element in (X, \leq) is an element x such that

$$[x \leq y] \implies [y = x].$$

[Note: this does not imply that $x \geq y$ for all $y \in X$.]

Proposition: Every finite poset has a maximal element.

Proof: Take $x_1 \in X$. If x_1 is not maximal, we can find $x_2 > x_1$ (i.e., $x_2 \geq x_1$ and $x_2 \neq x_1$). Continue this process until we stop at a maximal element. Because X is finite, the only way we wouldn't stop is if we have a chain

$$x_1 < x_2 < \cdots < x_j < \cdots < x_k < x_j$$

for some $j < k$. But by transitivity, $x_j < x_k < x_j$, which is a contradiction to antisymmetry. \square

1.9.2 Linear Extensions of a Poset

Definition: Given a poset (X, \leq) , the relation L is a linear extension if it is a total order on X (i.e., xLy or yLx for all $x, y \in X$) and L is a partial order, and $[x \leq y] \implies xLy$.

Proposition: Every finite poset has a linear extension.

Proof: We proceed by induction on $|X|$. We remove a maximal element, use induction, then put the maximal element back, appropriately redefining L . \square

Definition: A chain is a set $\{x_1 < x_2 < \cdots < x_m\}$. An antichain is a set $\{x_1, x_2, \cdots, x_m\}$ such that $x_i \not\leq x_j$ for all $i, j \in [m]$.

Example: In $(2^{[n]}, \subseteq)$, the largest chain has length $n + 1$ (build up from \emptyset to $2^{[n]}$). The largest antichain has

$$\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$$

elements (see **Sperner's Theorem**).

Dilworth's Theorem: (1950) Let (X, \leq) be a finite poset. The minimum number, say r , of disjoint chains which together cover X is equal to the size, say s of the largest antichain.

Proof: Trivially, $r \geq s$. We proceed by induction on $|X|$. The base case is trivial.

Suppose $|X| > 1$. Let C be a maximal chain in (X, \leq) (a chain which has the most possible elements of X).

If every chain in $(X \setminus C, \leq)$ has size at most $s - 1$, then we're done by induction.

So, suppose that $\{a_1, \dots, a_s\}$ is a maximal antichain in $(X \setminus C, \leq)$. We make the following clever definitions:

$$\begin{aligned} X^+ &:= \{x \in X \mid x \geq a_i \text{ for some } i\}, \\ X^- &:= \{x \in X \mid x \leq a_i \text{ for some } i\}. \end{aligned}$$

We claim that

$$X^- \cap X^+ = \{a_1, \dots, a_s\},$$

because clearly each $a_i \in X^- \cap X^+$, and if $x \in X^- \cap X^+$, then

$$[a_i \leq x \leq a_j] \implies [a_i \leq a_j] \implies [a_i = x = a_j].$$

Now we claim that $|X^-| < |X|$. This is obvious, because by the definition of C , the maximal element of C is not in X^- , since it's not an a_i and so if it were in X^- , we could extend c by some a_i . By symmetry, we also have $|X^+| < |X|$.

By induction, (X^-, \leq) can be covered by s chains

$$C_1^-, C_2^-, \dots, C_s^-$$

where $a_i \in C_i^-$. Similarly, (X^+, \leq) can be covered by s chains

$$C_1^+, C_2^+, \dots, C_s^+$$

where $a_i \in C_i^+$.

Then, (X, \leq) can be covered by

$$(C_1^- \cup C_1^+), \dots, (C_s^- \cup C_s^+)$$

and these are indeed chains. \square

Corollary: Dilworth's Theorem proves Hall's Marriage Theorem.

Proof: Let $X := \bigcup_{j \in [n]} A_j = A([n])$. The poset elements are the elements of X together with the elements $\{A_1, \dots, A_n\}$. The ordering on this poset is set inclusion. So, we have the antichains

$$\{A_1, A_2, \dots, A_n\}$$

and

$$\{\text{the elements of the sets}\}$$

and we see that the Hasse diagram has only two layers. X is an antichain, and there can be no bigger antichain. If there were, say Y , then set

$$J = \{j \mid A_j \in Y\}.$$

Well, $A(J) \cap Y = \emptyset$, and $|Y| \leq |J| + |X| - |A(J)|$. By Hall's Condition, $|Y| \leq |X|$, which confirms that there can be no bigger antichain than X . By **Dilworth's Theorem**, we have a chain cover of size $|X|$. No two elements of $|X|$ line in the same chain. So, there is chain for every element of X , and each A_i is in some chain with an element of X , which is its representative. Thus this yields an SDR. \square

Definition: A lattice is a poset P in which each pair $x, y \in P$ has a unique greatest lower bound (glb) and least upper bound (lub).

Example: The poset $(2^{[n]}, \subseteq)$ is a lattice, with $\text{glb}(A, B) = A \cap B$ and $\text{lub}(A, B) = A \cup B$.

Notation: This motivates the notation,

$$\text{glb}(A, B) =: A \wedge B$$

and

$$\text{lub}(A, B) =: A \vee B.$$

(\wedge is called the “meet” and \vee is called the “join”.)

Lemma: Every finite lattice has a unique maximal element and a unique minimal element. The maximal element is the join of all the elements and the minimal element is the meet of all the elements. We call the maximal and minimal elements 1 and 0, respectively.

Proposition: $(X, \wedge, \vee, 0, 1)$ is a lattice if and only if it satisfies:

- (1) associativity: $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$,
- (2) commutativity: $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$,
- (3) idempotency: $x \wedge x = x \vee x = x$,
- (4) $x \wedge (x \vee y) = x = x \vee (x \wedge y)$,
- (5) $x \wedge 0 = 0$ and $x \vee 1 = 1$.

Proof: It’s clear that a lattice satisfies these axioms. We now show the converse. From the axioms, we need to construct a partial order. To this end, we define \leq by:

if $x \wedge y = x$ then we say $x \leq y$, or

if $x \vee y = x$ then we say $x \geq y$.

We need to show the following.

- (a) The definition is consistent.
- (b) The definition induces a partial order.
- (c) \wedge and \vee are the glb and lub.
- (d) 1 and 0 are the maximal and minimal elements.

To see (a), observe that

$$x \wedge y = x \iff y \vee (x \wedge y) = y \iff x \vee y = y.$$

So, the relation \leq is well-defined.

To prove (b), we start by showing reflexivity. By idempotency, $x \wedge x = x \vee x = x$, and so $x \leq x$. Next we prove antisymmetry. Suppose $x \leq y$ and $y \leq x$. Then, $x = x \wedge y = y \wedge x = y$. To see transitivity, suppose $x \leq y$ and $y \leq z$. Then, $x \wedge y = x$ and $y \wedge z = y$. So,

$$\begin{aligned} x \wedge z &= (x \wedge y) \wedge z \\ &= x \wedge (y \wedge z) \\ &= x \wedge y \\ &= x. \end{aligned}$$

Hence $x \leq z$. We have now shown that \leq is a partial order.

To prove (c), we start by showing that \wedge is the glb, i.e., that $x \wedge y \leq x, y$. Well,

$$\begin{aligned} x \wedge y &= x \wedge (y \wedge y) \\ &= (x \wedge y) \wedge y. \end{aligned}$$

Therefore, $x \wedge y \leq y$. Repeat with $y \wedge x$. This shows that $x \wedge y$ is a lower bound. To see that it's the greatest lower bound, suppose $z \leq x, y$. Then,

$$\begin{aligned} z \wedge (x \wedge y) &= (z \wedge x) \wedge y \\ &= z \wedge y \\ &= z. \end{aligned}$$

So, indeed, $z \leq x \wedge y$. Repeat for \vee to show lub.

Lastly, property (d) follows from property (5). \square

Definition: Let $P = (X, \leq)$ be a poset. The set $D \subseteq X$ is a downset if for all $y \in D$ and $x \leq y$, we have $x \in D$. These are sometimes called ideals or order ideals.

Remark: To specify a downset, we usually describe the minimal elements which are not in the downset. This is sometimes called the basis.

Example: Consider the divisor lattice and the downset $D = \{n \mid 5 \nmid n\}$. There are no maximal elements, but the minimal element not in it is 5, so we can call this the downset with basis $\{5\}$.

Tangent: We can create maximal elements in the divisor lattice by associating natural numbers with vectors of infinite length by

$$2^{a_1} 3^{a_2} 5^{a_3} \dots \iff (a_1, a_2, a_3, \dots).$$

With this notation, we can write

$$D = \{v \mid v \leq (\infty, \infty, 0, \infty, \dots)\}.$$

This technique is called Fraisse's Ages.

1.9.3 Distributive Lattices

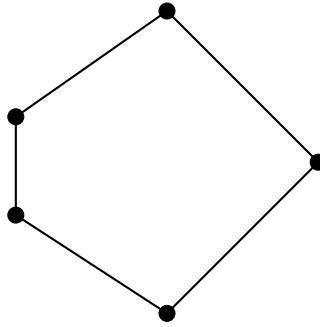
Definition: A lattice is distributive if:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$

and

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Example: An example of a non-distributive lattice is:



Example: $(2^{[n]}, \subseteq)$ is distributive because union and intersection distribute. The divisor lattice is distributive.

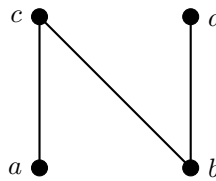
Remark: Any sublattice of a distributive lattice is distributive.

Definition: Let P be a poset (not necessarily finite). Define

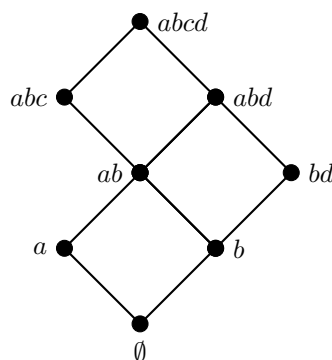
$$L(P) = (\{\text{downsets of } P\}, \subseteq)$$

to be another poset.

Example: Consider the poset P below.



The associated poset $L(P)$ is



The join is union and the meet is intersection. We see that $L(P)$ is a lattice, and in fact $L(P)$ is distributive. The key observation is that the nodes \emptyset , a , b , bd , and abc are the only nodes which are not the join of any two nodes. This corresponds to the fact that each of these nodes (other than \emptyset) introduces a new element. Additionally the relationships between these nodes (which is in the downset of another) correspond to their relationship in the original poset.

Fundamental Theorem of Finite Distributive Lattices: Let L be a finite distributive lattice. There is a poset P such that $L \cong L(P)$.

Proof: We want to “find” P inside of L . Consider the principal downsets

$$D_y := \{x \mid x \leq y\}.$$

An element $a \neq 0$ in L is called join irreducible, or **JI**, if

$$[a = b \vee c] \iff [a = b \text{ or } a = c].$$

Now observe that the JI elements are the principle downsets in $L(P)$.

Consider the following construction. Define our poset by

$$P := (\{\text{JI elements of } L\}, [\text{the order inherited from } L]).$$

We want to show that $L \cong L(P)$. We proceed by the following steps.

- (1) Every nonzero element of L is a join of JI elements.

Proof: Proceed by induction. This is true for the JI elements. For other elements, express them as $a = b \vee c$ with $a \neq b$ and $a \neq c$, then use induction.

- (2) Every nonzero element of L is the join of all JI elements beneath it (in L).

Proof: Take $a \in L$. Set

$$J := \{\text{JI elements } x \in L \mid x \leq a\}.$$

Observe that

$$\bigvee J \leq a.$$

On the other hand, a is the join of JI elements, and so we have equality.

- (3) Define the map $s : L \rightarrow \{\text{downsets of } P\} = L(P)$ by

$$s : a \mapsto \{\text{JI elements } x \mid x \leq a\}.$$

We claim that s is a bijection.

Proof: First we show s is one-to-one. For every a , we showed that

$$a = \bigvee s(a).$$

So, if $a \neq b$, we must have that $s(a) \neq s(b)$.

Next we show that s is onto. Let D be a downset of P . Set $a := \bigvee D$. Note that if $y \in D$ then, $y \leq a$. We want to show that $s(a) = D$. Clearly, $D \subseteq s(a)$. Suppose toward a contradiction that $x \in s(a) \setminus D$. Label $D = \{y_1, \dots, y_m\}$. Well, $x \leq a = y_1 \vee \dots \vee y_m$ and so

$$x \wedge (y_1 \vee \dots \vee y_m) = x.$$

Thus,

$$x = (x \wedge y_1) \vee (x \wedge y_2) \vee \dots \vee (x \wedge y_m).$$

x is JI, so for some u , we have $x = x \wedge y_i$. This shows that $x \leq y_i$, and hence $x \in D$, a contradiction. Therefore, $s(a) \setminus D$ is empty, i.e., $s(a) = D$. This shows that s is onto.

(4) We have now shown that s is a bijection. It remains to show that it is an isomorphism.

Proof: We need to show that meet and join are respected under s , i.e., that

$$s(a \wedge b) = s(a) \cap s(b),$$

$$s(a \vee b) = s(a) \cup s(b).$$

To see the first equality, take $x \in P$ with $x \leq a \wedge b$. Then, $x \leq a, b$, and so $x \in s(a) \cap s(b)$. Conversely, suppose $x \in s(a) \cap s(b)$. Then, $x \leq a, b$ and so $x \leq a \wedge b$. So, $x \in s(a \wedge b)$. Hence we have shown the first equality. The second equality follows similarly.

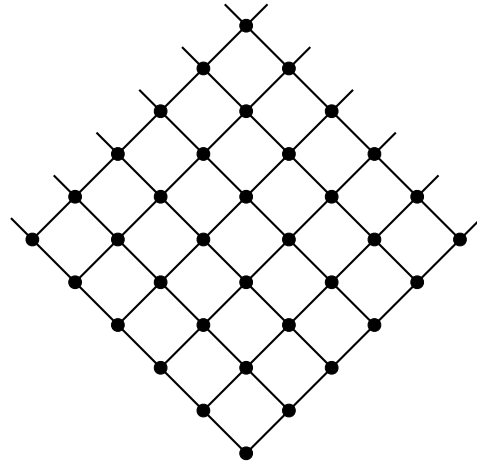
This completes the theorem. \square

1.9.4 Dimension Posets

Consider the following posets, which we say are of dimension 1 and dimension 2.



Dimension 1, or (\mathbb{N}, \leq)



Dimension 2, or (\mathbb{N}^2, \leq) or $(\mathbb{N}, \leq) \times (\mathbb{N}, \leq)$

Consider the product $P \times Q$ of such posets. $P \times Q$ contains elements of the form (x, y) such that $x \in P$ and $y \in Q$. We say that $(x_1, y_1) \leq (x_2, y_2)$ if $x_1 \leq_P x_2$ and $y_1 \leq_Q y_2$.

Definition: Define $\text{dim}(P)$ to be the minimum of all d such that P can be embedded into a product of d chains. Without loss of generality, we say that P is embedded into \mathbb{N}^d .

Question: The question we'd like to ask now is: Does every finite poset have a finite dimension?

Theorem: Every finite P has finite dimension.

Proof: A linear extension \leq_L is a total order on P such that if $x \leq_P y$ then $x \leq_L y$. Let R_1, \dots, R_ℓ be all of the linear extensions of $P = (X, \leq)$ (note that there are necessarily only finitely many linear extensions). We claim that P embeds into

$$(X, R_1) \times \dots \times (X, R_\ell)$$

under the map

$$x \mapsto (x, x, \dots, x).$$

Well, if $x \leq_P y$, then $x R_i y$ for all y , and so

$$(x, x, \dots, x) \leq (y, y, \dots, y)$$

in the product. If $x \not\leq_P y$, then is $x R_i y$ for some i ?

If $x \parallel y$ (meaning $x \not\leq y$ and $y \not\leq x$), then we want

$$(x, x, \dots, x) \parallel (y, y, \dots, y).$$

Consider the following theorem.

Theorem 12.2.1: Let $P = (X, \leq)$ be a poset with $a \parallel b$. There is a partial order R extending \leq (so as sets of ordered pairs, $R \supseteq \leq$) in which $a R b$. (Note that this proves the theorem.)

Proof: Think of relations as sets of ordered pairs:

$$[\downarrow a] := \{x \mid x \leq a\},$$

$$[\uparrow b] := \{x \mid x \geq b\}.$$

Note that

$$[\downarrow a] \cap [\uparrow b] = \emptyset$$

because if not there would be an x with $x \leq a$ and $x \geq b$ which would imply

$$b \leq x \leq a.$$

Set $R = \leq \cup ([\downarrow a] \times [\uparrow b])$. We claim that (X, R) is a poset.

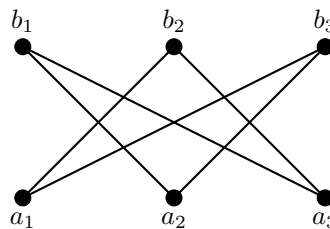
Is it reflexive? Well, $x \leq x$, so $x R x$. ✓

Is it antisymmetric? Suppose $x R y$ and $y R x$. If $x \leq y$ and $y \leq x$, then we're done. If $(x, y), (y, x) \in ([\downarrow a] \times [\uparrow b])$, then this contradicts the fact that $[\downarrow a] \cap [\uparrow b] = \emptyset$. Lastly, suppose $x \leq y$ and $(y, x) \in [\downarrow a] \times [\uparrow b]$. Then, $y \leq a$ and $x \geq b$, and so $b \leq x \leq y \leq a$, which is a contradiction. ✓

Is it transitive? If $x \leq y$ and $y \leq z$, we're done. If $(x, y), (y, z) \in [\downarrow a] \times [\uparrow b]$, then $y \in [\downarrow a] \cap [\uparrow b]$, a contradiction. If $x \leq y$ and $(y, z) \in [\downarrow a] \times [\uparrow b]$, then $y \leq a$ and so $x \leq y \leq a$ and $(x, z) \in [\downarrow a] \times [\uparrow b]$, hence $x R z$. Lastly, if $(x, y) \in [\downarrow a] \cap [\uparrow b]$ and $Y \leq z$, then $z \geq y \geq b$ and so $(x, z) \in [\downarrow a] \times [\uparrow b]$. □

The above theorem completes this theorem. □

Example: Consider the “standard poset” S_n :



In this poset, $a_i < b_j$ for all $i \neq j$.

Proposition: $\dim(S_n) = n$.

Proof: First we show $\dim(S_n) \leq n$. Consider the embedding

$$S_n \subseteq (\{0, 1\}, \leq)^n$$

by the map

$$a_i \mapsto (0, \dots, 0, 1, 0, \dots, 0)$$

following

$$b_i \mapsto (1, \dots, 1, 0, 1, \dots, 1)$$

where the i^{th} coordinate is different from the rest.

Now we show $\dim(S_n) \geq n$. Suppose $S_n \subseteq (\mathbb{N}, \leq)^m$ for $m < n$. We claim that for each i , there exists a j such that the j^{th} coordinate of b_i is smaller than the j^{th} coordinate of any other b_k . To see this, note that a_i lies below all b_k for $k \neq i$. So, if there were no such j , then all coordinates of a_i would lie under the corresponding coordinate of b_i , which is a contradiction. So, this requires n coordinates. \square

Example: Note that $(2^{[n]}, \leq) \cong (\{0, 1\}, \leq)^n$ and so $(2^{[n]}, \leq) \supseteq S_n$. So, $\dim((2^{[n]}, \leq)) = n$.

Example: Consider the poset of divisors of $n = p_1^{a_1} \cdots p_d^{a_d}$. The p_i 's are distinct and $a_i \geq 1$ for all i . Then,

$$(\text{divisors of } n, |) \cong \prod_{i=1}^d (\{0, 1, \dots, a_i\}, \leq).$$

This tells us that the dimension is at most d . But each poset in the product has 0 and 1 so it contains a copy of S_d . Hence,

$$\dim(\text{divisors of } n) = d.$$

1.9.5 The Möbius Function of a Poset

Recall the Principle of Inclusion-Exclusion. Say that we have 45 students: 14 play (S)occer, 17 play (B)asketball, 18 play (H)ockey, 4 play S&B, 3 play S&H, 5 play B&H, 1 plays S&B&H. From this, we can construct the Venn Diagram to see how many students play no sports or we can use the PIE formula.

Define $g : 2^{\{S,B,H\}} \rightarrow \mathbb{N}$ so that $g(X)$ is defined to be the number of students who play all sports in X (and maybe more). Define $f(X)$ to be the number of students who play precisely the sports in X . We see that

$$g(X) = \sum_{Y \supseteq X} f(Y).$$

By PIE,

$$f(\emptyset) = \sum_{Y \supseteq \emptyset} (-1)^{|Y|} g(Y).$$

Our goal is to take the given function g and “invert” it. In general, we have f and g defined from a poset to a ring and the relationship

$$g(X) = \sum_{Y \supseteq X} f(Y)$$

and we want to find a formula for f .

Consider the above example again. We will choose a linear extension of $2^{\{S,B,H\}}$:

$$\{\emptyset, S, B, H, SB, SH, BH, SBH\}.$$

Using linear algebra, we create

$$\underbrace{\begin{bmatrix} 45 \\ 14 \\ 17 \\ 18 \\ 4 \\ 3 \\ 5 \\ 1 \end{bmatrix}}_{\vec{g}} = \begin{matrix} \emptyset \\ S \\ B \\ H \\ SB \\ SH \\ BH \\ SBH \end{matrix} \underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}}_{\zeta} \cdot \underbrace{\begin{bmatrix} 7 \\ 8 \\ 9 \\ 11 \\ 3 \\ 2 \\ 4 \\ 1 \end{bmatrix}}_{\vec{f}}.$$

So, we have $\vec{g} = \zeta \vec{f}$ and we want to solve for \vec{f} .

Definition: For any poset P , the incidence algebra of P , denoted $I(P)$, is the set of matrices M indexed by elements of P such that

$$M(x, y) = 0 \text{ if and only if } x \not\leq y$$

(Per convention, we use function notation $M(x, y)$.)

We want $\mu\zeta = \text{Id}$, and μ will be our Möbius function. To find μ , look at the (x, y) entry of $\mu\zeta$, this equals

$$\sum_{z \in P} \mu(x, z)\zeta(z, y) = \sum_{z \leq y} \mu(x, z) = \sum_{x \leq z \leq y} \mu(x, z) = \begin{cases} 1, & x = y \\ 0, & \text{otherwise} \end{cases}.$$

We can compute μ inductively with $\mu(x, x) = 1$ and $\mu(x, y) = 0$ if $x \not\leq y$. Otherwise, $x < y$, and

$$\begin{aligned} 0 &< \sum_{x \leq z \leq y} \mu(x, z) \\ &= \left(\sum_{x \leq z < y} \mu(x, z) \right) + \mu(x, y) \end{aligned}$$

So,

$$\mu(x, y) = - \sum_{x \leq z < y} \mu(x, z).$$

The Principle of Möbius Inversion: Suppose f and g are functions from a poset to a ring, which satisfy

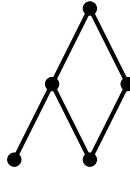
$$g(X) = \sum_{Y \supseteq X} f(Y)$$

for all $X \in P$. Then,

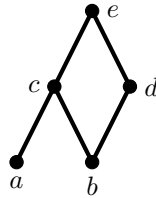
$$f(X) = \sum_{Y \supseteq X} \mu(X, Y)g(Y).$$

Proof: $\vec{g} = \zeta \vec{f}$, and so $\vec{f} = \mu \vec{g}$. \square

Example: Compute μ for the poset



First we pick a linear extension:



So, we construct

$$\begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} \begin{bmatrix} 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We used the facts that

$$\begin{aligned} \mu(a, c) &= - \sum_{a \leq z < c} \mu(a, z) = -\mu(a, a), \\ \mu(a, e) &= -[\mu(a, a) + \mu(a, c)] = -[1 - 1] = 0, \\ \mu(b, e) &= -[\mu(b, b) + \mu(b, c) + \mu(b, d)] = -[1 - 1 - 1] = 1. \end{aligned}$$

Example: Consider the poset of compositions

$$\mathbb{P}^* := \{w_1 \dots w_m \mid w_i \in \mathbb{P}\}$$

where

$$u_1 \dots u_j \leq w_1 \dots w_m$$

if there is some sequence

$$1 \leq i_1 < i_2 < \dots < i_j \leq m$$

such that

$$u_k \leq w_{i_k}$$

for all k . For example

$$3 \ 2 \leq 1 \ 5 \ 1 \ 1 \ 1 \ 1 \ 3 \ 1 \ 1 \ 1.$$

Remark: Möbius Inversion works in the other direction as well. If

$$g(x) = \sum_{y \leq x} f(y)$$

then

$$f(x) = \sum_{y \leq x} \mu(x, y)g(y).$$

Example: Let $P = (\mathbb{N}, \leq)$, then we can see easily that

$$\mu(x, y) = \begin{cases} 1, & y = x \\ -1, & y = x + 1 \\ 0, & \text{otherwise} \end{cases}$$

For this example, we have that if

$$g(n) = \sum_{i \leq n} f(i),$$

then

$$f(n) = \sum_{i \leq n} \mu(i, n)g(i)$$

and so applying the above findings

$$f(n) = g(n) - g(n-1).$$

Example: Let $P = (2^{[n]}, \subseteq)$. Then,

$$\mu(S, T) = \begin{cases} (-1)^{|T \setminus S|}, & S \subseteq T \\ 0, & \text{otherwise} \end{cases}$$

Proof: It suffices to show the following.

- (1) $\mu(S, S) = 1$. This is clear by definition.
- (2) $\mu(S, T) = 0$ if $S \not\subseteq T$. This is clear by definition.
- (3) $\sum_{S \subseteq Z \subseteq T} \mu(S, Z) = 0$ if $S \subsetneq T$.

We now prove (3). Note that

$$\begin{aligned} \sum_{S \subseteq Z \subseteq T} \mu(S, Z) &= \sum_{i=0}^{|T \setminus S|} (-1)^i \binom{|T \setminus S|}{i} \\ &= (1-1)^{|T \setminus S|} \\ &= 0. \end{aligned} \quad (\text{Binomial Theorem})$$

Example: Let $P = (\mathbb{N}, |)$ be the divisor lattice. Then,

$$\mu(x, y) = \begin{cases} (-1)^t, & \text{if } y/x \text{ is the product of } t \text{ distinct primes} \\ 0, & \text{otherwise} \end{cases}$$

Proof: It suffices to show the following.

- (1) $\mu(x, x) = 1$. This is clear by definition.
- (2) $\mu(x, y) = 0$ if $x \nmid y$. This is clear by definition.
- (3) $\sum_{x \leq z \leq y} \mu(x, z) = 0$ if $x \mid y$ and $x \neq y$.

We now prove (3). Note that “ \leq ” is the poset inequality, so what we need to show is:

$$\sum_{z: x|z|y} \mu(x, z) = \sum_{\substack{z: x|z|y \\ \frac{z}{x} \text{ is squarefree}}} \mu(x, z).$$

Suppose

$$\frac{y}{x} = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

for distinct primes p_1, \dots, p_t and nonzero a_1, \dots, a_t . So,

$$\sum_{\substack{z: x|z|y \\ \frac{z}{x} \text{ is squarefree}}} \mu(x, z) = \sum_{i=0}^t (-1)^i \binom{t}{i} = 0.$$

Extra Credit Homework Problem: (aka, unsolved problem) Define

$$M(n) = \sum_{1 \leq i \leq n} \mu(1, i).$$

Prove that for every $\epsilon > 0$, there exists c such that

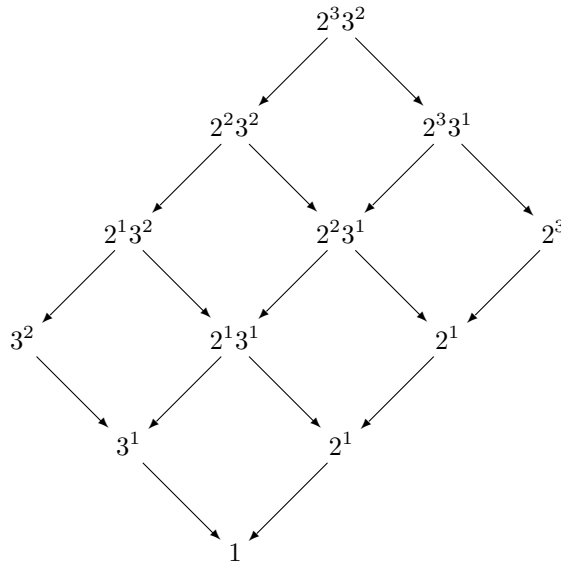
$$M(n) < cn^{1/2+\epsilon}.$$

This is equivalent to the Riemann Hypothesis. The function $M(n)$ is called Merten's function.

Recall: Let P_1 and P_2 be posets. Then, $P_1 \times P_2$ is defined on the elements (x, y) where $x \in P_1$ and $y \in P_2$. We say $(x_1, y_1) \leq (x_2, y_2)$ if $x_1 \leq x_2$ in P_1 and $y_1 \leq y_2$ in P_2 .

Definition: We say that the posets P_1 and P_2 are isomorphic if there exists a bijection $\phi : P_1 \rightarrow P_2$ such that $x \leq y$ in P_1 if and only if $\phi(x) \leq \phi(y)$ in P_2 .

Example: Consider the divisors of 72:



This is isomorphic to

$$(\{0, 1, 2, 3\}, \leq) \times (\{0, 1, 2\}, \leq),$$

(each of the first is a top-right to bottom-left chain, and there are three of them).

Example: Consider the boolean lattice on 3 elements and note that it is isomorphic to $(\{0, 1\}, \leq)^3$.

Remark: These examples lead us to believe the following theorem.

Theorem: $\mu_{P_1 \times P_2}((x_1, x_2), (y_1, y_2)) = \mu_{P_1}(x_1, y_1) \cdot \mu_{P_2}(x_2, y_2)$.

Proof: Check the three conditions as we did before. The first two are trivial. \square

1.10 Chapter 13 - More on Partitions and Permutations

1.10.1 Partitions, Diagrams, and Conjugacy Classes

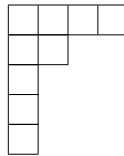
Definition: A partition of n is a list of numbers (called parts) that sum to n . Order does not matter. By convention, we list the parts in decreasing order.

Notation: For the partition $3 + 2 + 1 + 1 = 7$, we write $7 = 3^1 2^1 1^2$.

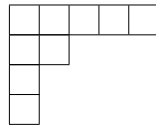
Notation: $p(n)$ denotes the number of partitions of n . The notation $\lambda \vdash n$ means λ is a partition of n .

Definition: The Ferrers diagram $D(\lambda)$ is drawn as an arrangement of boxes where, if $\lambda = n_1 + \cdots + n_k$ (in decreasing order), then the i^{th} row of $D(\lambda)$ contains n_i cells.

Example: Consider the partition $4 + 2 + 1 + 1 + 1$. This has the Ferrers diagram:



We find the conjugate partition $(4 + 2 + 1 + 1 + 1)^* = 5 + 2 + 1 + 1$ by flipping the Ferrers diagram:



Theorem: $\sum_{n \geq 0} p(n)x^n = \prod_{i \geq 1} \frac{1}{1 - x^i}$.

Proof: Look at the coefficient of x^n on the right-hand side.

$$\prod_{i \geq 1} \frac{1}{1 - x^i} = \prod_{i=1}^{\infty} (1 + x^i + x^{2i} + \cdots).$$

A term corresponding to x^n on the right-hand side comes from

$$x^{a_1} x^{2a_2} x^{3a_3} \cdots = x^n.$$

So,

$$a_1 + 2a_2 + 3a_3 + \cdots = n.$$

Therefore, this term came from

$$1^{a_1} 2^{a_2} 3^{a_3} \cdots \vdash n. \quad \square$$

Theorem: Let $d(n)$ be the number of partitions of n into distinct parts and let $o(n)$ be the number of partitions of n into odd parts. Then, $d(n) = o(n)$ for all n .

Proof: The generating function for the number of partitions into distinct parts is

$$\sum_{n=0}^{\infty} d(n)x^n = \prod_{i=1}^{\infty} (1 + x^i)$$

and the generating function for the number of partitions into odd parts is

$$\sum_{n=0}^{\infty} o(n)x^n = \prod_{i=1}^{\infty} \frac{1}{1-x^{2i-1}}.$$

Observe that

$$\begin{aligned} \sum_{n=0}^{\infty} o(n)x^n &= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots} \\ &= \frac{(1-x^2)(1-x^4)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots} \\ &= \frac{(1+x)(1-x)(1+x^2)(1-x^2)\cdots}{(1-x)(1-x^2)(1-x^3)(1-x^4)\cdots} \\ &= (1+x)(1+x^2)(1+x^3)\cdots \\ &= \sum_{n=0}^{\infty} d(n)x^n. \quad \square \end{aligned}$$

Orders on Partitions:

- (1) Containment of Ferrers diagrams. The poset lattice derived from this order is **Young's Lattice**.
- (2) (lex) Compare two partitions of the same number. For example,

$$5 + 1 + 1 \text{ comes after } 3 + 2 + 2$$

and

$$4 \text{ comes after } 2 + 1 + 1.$$

This is a total order (on each n ; we only talk about one n at a time).

Formally, if

$$\begin{aligned} \lambda &= n_1 + \cdots \vdash n, \text{ and} \\ \mu &= m_1 + \cdots \vdash n, \end{aligned}$$

then we say that λ comes after μ if there is some j such that $n_i = m_i$ for $i < j$ and $n_j > m_j$. (Normally, we don't use any symbol for this relationship. We just say " λ comes after μ ".)

- (3) (natural partial order / Dominance order) Suppose

$$\begin{aligned} \lambda &= n_1 + \cdots \vdash n, \text{ and} \\ \mu &= m_1 + \cdots \vdash n. \end{aligned}$$

We say $\lambda \trianglelefteq \mu$ if

$$n_1 + \cdots + n_i \leq m_1 + \cdots + m_i$$

for all i . As in (2), we only consider partitions of fixed n .

Proposition: If $\lambda \trianglelefteq \mu$, then λ precedes μ in lex order. (In other words, lex is a linear extension of dominance.)

Proof: Consider

$$\begin{aligned} \lambda &= n_1 + \cdots \vdash n, \text{ and} \\ \mu &= m_1 + \cdots \vdash n, \end{aligned}$$

such that $\lambda \trianglelefteq \mu$. Choose j to be minimal such that $n_j \neq m_j$. Since $n_1 + \cdots + n_j < m_1 + \cdots + m_j$, we have $n_j < m_j$. \square

1.10.2 Tableaux

Take $\lambda \vdash n$. Draw its Ferrers diagram, and then fill the cells with the numbers in $[n]$ so that

- (1) the rows increase left to right,
- (2) the columns increase top to bottom.

Example: $n = 3$. There are three partitions of 3: 3 , $2 + 1$, $1 + 1 + 1$. The tableaux are

$$\boxed{1\ 2\ 3}, \quad \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array}, \quad \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline \end{array}.$$

Example: $n = 4$. There are five partitions of 4: 4 , $3 + 1$, $2 + 2$, $2 + 1 + 1$, $1 + 1 + 1 + 1$. The tableaux are

$$\boxed{1\ 2\ 3\ 4}, \quad \begin{array}{|c|c|c|} \hline 1 & 3 & 4 \\ \hline 2 & & \\ \hline \end{array}, \quad \begin{array}{|c|c|c|} \hline 1 & 2 & 4 \\ \hline 3 & & \\ \hline \end{array}, \quad \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & & \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & 3 \\ \hline \end{array}, \quad \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline \end{array}.$$

Definition: Define f_λ to be the number of tableaux of shape λ .

Definition: For a cell c in a tableaux, define the hook of c to be the number of cells to the right of c (in the same row) and below c (in the same column), including c itself.

Theorem: $f_\lambda = \frac{n!}{\prod_c h_c}$.

Theorem: $\sum_{\lambda \vdash n} (f_\lambda)^2 = n!$.

Remark: We could prove this with a bijection from the permutations of n to the pairs (P, Q) of tableaux of the same shape. This was found by Robinson-Schensted-Knuth, and is called the RSK Correspondence.

We demonstrate the bijection $\pi \leftrightarrow (P, Q)$.

Algorithm: Subroutine INSERT(entry a , row j):

- (-) If a is greater than every entry in row j , append a to the end of the row
- (-) Otherwise, choose the smallest $b > a$ in this row, replace b by a , and run INSERT(b , $j + 1$).

Run RSK:

- (-) Start with P, Q empty.
- (-) For i from 1 to n do:
 - (-) Call INSERT($\pi(i)$, 1)
 - (-) This causes a cascade of bumps, eventually creating a new cell in P
 - (-) Create a new cell in Q in this position and write i in it

Example: If $\pi = 123456$ then we end up with

$$P = \boxed{1\ 2\ 3\ 4\ 5\ 6} \quad \text{and} \quad Q = \boxed{1\ 2\ 3\ 4\ 5\ 6}.$$

Example: If $\pi = 654321$ then we end up with

$$P = \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline 5 \\ \hline 6 \\ \hline \end{array} \quad \text{and} \quad Q = \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline 4 \\ \hline 5 \\ \hline 6 \\ \hline \end{array}.$$

Example: If $\pi = 4725136$ then we end up with

$$P = \begin{array}{|c|c|c|} \hline 1 & 3 & 6 \\ \hline 2 & 5 & \\ \hline 4 & 7 & \\ \hline \end{array} \quad \text{and} \quad Q = \begin{array}{|c|c|c|} \hline 1 & 2 & 7 \\ \hline 3 & 4 & \\ \hline 5 & 6 & \\ \hline \end{array}.$$

Proof:

(1) P and Q are tableaux.

- Q is clearly a tableau because we're always inserting a new maximum.

- The rows of P increase because that's how INSERT works.

- The columns of P increase because otherwise we would have $\begin{array}{|c|} \hline y \\ \hline x \\ \hline \end{array}$ with $y > x$. Consider the first time this happens in the evolution of P and Q . Which one was bumped here last? Neither is possible.

(2) Inverse Map. This is messy, check Bona's book.

□

Example: Consider

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 5 & 1 & 3 & 6 \end{pmatrix} = 4725136.$$

Then,

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 6 & 1 & 4 & 7 & 2 \end{pmatrix} = 5361472.$$

Applying RSK, we get

$$P = \begin{array}{|c|c|c|} \hline 1 & 2 & 7 \\ \hline 3 & 4 & \\ \hline 5 & 6 & \\ \hline \end{array} \quad \text{and} \quad Q = \begin{array}{|c|c|c|} \hline 1 & 3 & 6 \\ \hline 2 & 5 & \\ \hline 4 & 7 & \\ \hline \end{array}.$$

So, we have the nice property that if $\pi \leftrightarrow (P, Q)$ then $\pi^{-1} \leftrightarrow (Q, P)$.

1.11 Chapter 15 - Enumeration Under Group Action

1.11.1 Definition of a Group

Definition: Originally, groups were defined as “all symmetries of an object”, where an object was a pair (X, S) where X is a set (called the ground set) and S is a “structure” defined on X . S , for example, could be a graph on X or a (set) partition of X or a permutation of X , etc.

Given any permutation of X , there is a natural way to apply this permutation to an object.

The permutation π of X is an automorphism of (X, S) if $\pi(S) = S$. So,

$$\text{Aut}(X, S) = \{\pi \mid \pi(S) = S\}.$$

Historically, this is how groups were defined.

Remark: Every automorphism group satisfies:

- (1) contains the identity,
- (2) if $\pi(S) = S$ then $S = \pi^{-1}(S)$, i.e. it contains inverses,
- (3) if $\pi(S) = S$ and $\sigma(S) = S$ then $\pi(\sigma(S)) = S$, i.e., it contains compositions.

Definition: A permutation group is a set of permutations satisfying the above conditions.

Question: Is this definition more general? Or are all permutation groups automorphism groups?

Proposition: Every finite permutation group is an automorphism group.

Proof: Let G be a permutation group on the set $X := \{x_1, \dots, x_n\}$. Define

$$S = \{(\pi(x_1), \dots, \pi(x_n)) \mid \pi \in G\}.$$

So, S is a bunch of n -tuples. We claim that $G = \text{Aut}(X, S)$.

Let $\pi \in G$. Then,

$$\begin{aligned} \pi(S) &= \{(\pi(\sigma(x_1)), \dots, \pi(\sigma(x_n))) \mid \sigma \in G\} \\ &= \{(\tau(x_1), \dots, \tau(x_n)) \mid \tau \in G\} && \text{(by (2) and (3))} \\ &= S. \end{aligned}$$

So, $\pi \in \text{Aut}(X, S)$.

Now let $\pi \in \text{Aut}(X, S)$. By (1), G contains the identity. So, S contains (x_1, \dots, x_n) . Hence, if $\pi(S) = S$, then

$$S \ni \pi((x_1, \dots, x_n)) = (\pi(x_1), \dots, \pi(x_n)).$$

Therefore, $\pi \in G$.

Hence, $G = \text{Aut}(X, S)$. \square

Definition: In the late 1800s, Dyck defined an abstract group as a set G with a binary operation \cdot which satisfies:

- (a) associativity $(g \cdot (h \cdot k) = (g \cdot h) \cdot k)$,
- (b) identity $(\exists e \in G \forall g \in G : e \cdot g = g \cdot e = g)$,
- (c) inverses $(\forall g \in G \exists h \in G : g \cdot h = h \cdot g = e)$.

Historical Note: Many people hated this definition. Klein said: “The disadvantage of the abstract method is that it fails to encourage thought.”

Question: Are abstract groups any more general? No.

Theorem: (Cayley) Every abstract group is a permutation group.

Theorem: (Frucht) Every abstract group is the automorphism group of a graph.

Historical Note: From 1861-1873, Mathieu found the sporadic simple groups M_{11} , M_{12} , M_{22} , M_{23} , M_{24} . No other sporadic simple groups were found for 90 years. In 1967, we found the Higman-Sims group (HS) of order 44,352,000. Existence was shown as the automorphism group of a graph with 100 vertices, 1100 edges, which is 22-regular (every vertex has degree 22).

1.11.2 Pölya Counting

Example: Consider a coin with two sides, each is painted red or blue. How many coins are there? 3: RB, BB, RR. We think about \mathbb{Z}_2 acting on the coin to see that RB and BR are identified as the same coin.

Example: Suppose we color the corners of a square with red and blue and we allow the square to be moved around. How many different squares are there? The group acting on these is D_4 , generated by a flip along the diagonal τ and a 90 degree rotation ρ . If we have the square

$$\begin{array}{cc} 2 & - & 1 \\ | & & | \\ 3 & - & 4 \end{array}$$

then we can consider, for example

$$\rho \cdot \begin{array}{cc} 2 & - & 1 \\ | & & | \\ 3 & - & 4 \end{array} = \begin{array}{cc} 1 & - & 4 \\ | & & | \\ 2 & - & 3 \end{array} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

and

$$\tau \cdot \begin{array}{cc} 2 & - & 1 \\ | & & | \\ 3 & - & 4 \end{array} = \begin{array}{cc} 4 & - & 1 \\ | & & | \\ 3 & - & 2 \end{array} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Formally, let X be the set of all colorings of the square. For all $x \in X$ and all $g \in D_4$, we say that x is equivalent to gx . We want to count inequivalent elements, i.e., the number of equivalence classes. We want to count the orbits, where

$$\text{orb}(x) = \{gx \mid g \in G\}.$$

Orbit-Counting Lemma / Burnside's Lemma: Suppose the group G acts on the set X . Then,

$$\# \text{ of orbits} = \text{the average number of fixed points} = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

where

$$\text{fix}(g) = \{x \mid gx = x\}.$$

Example: Consider the square problem.

$g \in G = D_4$	$g \cdot \begin{array}{cc} 2 & - & 1 \\ & & \\ 3 & - & 4 \end{array}$	$ \text{fix}(g) $
e	$\begin{array}{cc} 2 & - & 1 \\ & & \\ 3 & - & 4 \end{array}$	16
ρ	$\begin{array}{cc} 1 & - & 4 \\ & & \\ 2 & - & 3 \end{array}$	2
ρ^2	$\begin{array}{cc} 4 & - & 3 \\ & & \\ 1 & - & 2 \end{array}$	4
ρ^3	$\begin{array}{cc} 3 & - & 2 \\ & & \\ 4 & - & 1 \end{array}$	2
τ	$\begin{array}{cc} 4 & - & 1 \\ & & \\ 3 & - & 2 \end{array}$	8
$\tau\rho$	$\begin{array}{cc} 3 & - & 4 \\ & & \\ 2 & - & 1 \end{array}$	4
$\tau\rho^2$	$\begin{array}{cc} 2 & - & 3 \\ & & \\ 1 & - & 4 \end{array}$	8
$\tau\rho^3$	$\begin{array}{cc} 1 & - & 2 \\ & & \\ 4 & - & 3 \end{array}$	4

Summing these, we get 48, which divided by $|G| = 8$ is 6. So there are six different squares.

Definition: Suppose G acts on the set X . Then, the stabilizer of x is

$$\text{stab}(x) = \{g \in G \mid gx = x\}.$$

Orbit-Stabilizer Theorem: The map $g \text{stab}(x) \mapsto gx$ is a bijection between $G/\text{stab}(x) = \text{orb}(x)$. In particular,

$$|G| = |\text{stab}(x)| |\text{orb}(x)|.$$

Proof: Is the map well-defined? Suppose that $g \text{stab}(x) = h \text{stab}(x)$. Then, $g = hs$ for some $s \in \text{stab}(x)$. Then,

$$gx = hsx = hx.$$

Is the map surjective? Take $y \in \text{orb}(x)$. Then, $y = gx$ for some $g \in G$. So, y is the image of $g \text{stab}(x)$.

Is the map injective? Suppose $gx = hx$. So, $g^{-1}hx = x$ and thus $g^{-1}h \in \text{stab}(x)$. Therefore, $g \text{stab}(x) = h \text{stab}(x)$. \square

Proof of Orbit-Counting Lemma:

Observe that

$$\begin{aligned} \sum_{g \in G} |\text{fix}(g)| &= |\{(g, x) \mid gx = x\}| \\ &= \sum_{x \in X} |\text{stab}(x)|. \end{aligned}$$

By the Orbit-Stabilizer Theorem,

$$\frac{|G|}{|\text{orb}(x)|} = |\text{stab}(x)|.$$

Hence,

$$\sum_{g \in G} |\text{fix}(g)| = |G| \sum_{x \in X} \frac{1}{|\text{orb}(x)|}.$$

For any orbit, the right-hand sum gets counted once for each element in the orbit, i.e.

$$\sum_{x \in X} \frac{1}{|\text{orb}(x)|} = \# \text{ of orbits.}$$

This proves the theorem. \square

Definition: The cycle index monomial of a permutation π is

$$\text{cim}(\pi) = x_1^{c_1} x_2^{c_2} \cdots x_k^{c_k}$$

where c_i is the number of cycles of π which have length i .

Definition: The cycle index of a group G is

$$\text{ci}(G) = \frac{1}{|G|} \sum_{g \in G} \text{cim}(g).$$

Remark: The number of equivalence classes of 2-colored squares is

$$\text{ci}(D_4) \Big|_{x_1=x_2=x_3=x_4=2}.$$

Example: (Graphs on 4 vertices) Our group is $G = S_4$. If x and y are graphs, then $gx = y$ when they have the same edges. A slight complication is that the group acts on vertices, but what we really care about is the action of the edges.

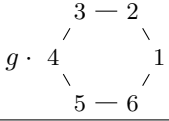
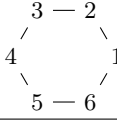
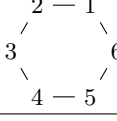
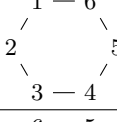
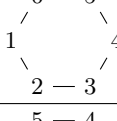
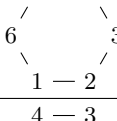
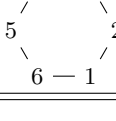
$\pi \in S_4$	# of them	action on edges	cim
id	1	id	x_1^6
2-cycle	6	(2,2)-cycle	$x_1^2 x_2^2$
(2,2)-cycle	3	(2,2)-cycle	$x_1^2 x_2^2$
3-cycle	8	(3,3)-cycle	x_3^2
4-cycle	6	(2,4)-cycle	$x_2^1 x_4^1$

Hence

$$\text{ci}(S_4) = \frac{1}{24} (x_1^6 + 9x_1^2 x_2^2 + 8x_3^2 + 6x_2 x_4).$$

Substituting $x_i = 2$ for all i , we find that there are 11 equivalence classes of squares.

Example: We will now count necklaces which are colored red/blue on 6 vertices. How many inequivalent necklaces are there? Equivalent necklaces are found via rotation only, not flipping. The group acting on necklaces is $\mathbb{Z}/6\mathbb{Z}$ (over addition).

group element	$g \cdot$ 	action	cycle index
0		1	x_1^6
1		(1 2 3 4 5 6)	x_6^1
2		(1 3 5)(2 4 6)	x_3^2
3		(1 4)(2 5)(3 6)	x_2^3
4		(1 5 3)(2 6 4)	x_3^2
5		(1 6 5 4 3 2)	x_6^1

So,

$$\text{ci}(\mathbb{Z}/6\mathbb{Z}) = \frac{1}{6} (x_1^6 + 2x_6^1 + 2x_3^2 + x_2^3).$$

Setting $x_i = 2$, we get 14.

Example: (The action of $\mathbb{Z}/n\mathbb{Z}$ on necklaces of n beads.) Take $m \in \mathbb{Z}/n\mathbb{Z}$. Its order is the least x such that $xm = yn$, which equals 0 in $\mathbb{Z}/n\mathbb{Z}$, for some y . Divide both sides by $\text{gcd}(m, n)$ to get

$$x \frac{m}{\text{gcd}(m, n)} = y \frac{n}{\text{gcd}(m, n)}.$$

We get the solution that the order of m in $\mathbb{Z}/n\mathbb{Z}$ is $\frac{n}{\text{gcd}(m, n)}$.

Take any $d \mid n$. How many m satisfy

$$d = \frac{n}{\text{gcd}(n, m)} = \text{order}(m)?$$

For each such m ,

$$m = \text{gcd}(m, n)y$$

with

$$\text{gcd}(y, d) = 1.$$

The number of elements of order $d \mid n$ is the number of elements which are coprime to d . Recall Euler's totient function

$$\phi(d) = |\{y \in \mathbb{Z}/d\mathbb{Z} \mid \gcd(y, d) = 1\}|.$$

Each element of order d consists of n/d cycles of length d . So,

$$\text{ci}(\mathbb{Z}/n\mathbb{Z}) = \frac{1}{n} \sum_{d \mid n} \phi(d) x_d^{n/d}.$$

Example: If we allow flipping, then our group is D_n . Well,

$$\text{ci}(D_n) = \frac{1}{2}(\text{ci}(\mathbb{Z}/n\mathbb{Z}) + R_n)$$

where R_n is the set of reflections (not a group on its own).

If n is odd, then each reflection is a $(2, 2, \dots, 2, 1)$ -cycle. If n is even, then each reflection is either a $(2, 2, \dots, 2, 1, 1)$ -cycle or a $(2, 2, \dots, 2)$ -cycle. So, if n is odd, then

$$R_n = \frac{1}{n}(nx_1x_2^{(n-1)/2}),$$

and if n is even, then

$$R_n = \frac{1}{n} \left(\frac{n}{2}x_2^{n/2} + \frac{n}{2}x_1^2x_2^{(n/2)-1} \right).$$

Example: Returning to $n = 6$, now allowing flipping:

$$\text{ci}(D_6) = \frac{1}{12} (x_1^6 + x_2^3 + 2x_3^2 + 2x_6^1 + 3x_1^2x_2^2 + 3x_2^3).$$

Plugging in $x_i = 2$,

$$\text{ci}(D_6) = 13.$$

Index

- abstract group, 73
- adjacent, 6
- affine plane, 43
- antichain, 55
- automorphism, 72

- B_n , 7
- Bell numbers, 7
- Binomial Theorem, 3
- Burnside's Lemma, 74

- Cayley's Theorem, 7, 73
- chain, 55
 - antichain, 55
- co-lexicographical order, 9
- complete graph, 48
- cycle, 6
- cycle index, 75
- cycle index monomial, 75

- de Bruijn-Erdős Theorem, 29, 42
- derangement, 12
- Desargue's Theorem, 43
- determinant, 22
- diagonal Ramsey numbers, 49
- dictionary ordering, 9
- Dilworth's Theorem, 56
- dimension of a poset, 61
- Dirichlet, 47
- distributive lattice, 58
 - fundamental theorem, 60
- Dominance order, 69
- doubly stochastic matrix, 22
- downset, 58

- Erdős-Ko-Rado Theorem, 27
- Erdős-Szekeres, 52
- even permutation, 17

- f_λ , 70
- falling factorial, 16
- Ferrers diagram, 68
- Fraisse's Ages, 58
- Frucht's Theorem, 73
- Fundamental Theorem of Finite Distributive Lattices, 60

- Gödel, 54
- Graeco-Latin square, 24
- graph, 6
- group, 72
 - abstract, 73

- h_c , 70
- Hall's Condition, 19
- Hall's Marriage Theorem, 19, 56
- Hasse diagram, 55
- hook, 70

- ideal, 58
- incidence algebra, 64
- intersecting, 27
- intersecting family of subsets, 27
- irreducible
 - join irreducible, 60
- isomorphism
 - of posets, 67

- join irreducible, 60

- k -flat, 41

- $L(n)$, 21
- Latin square, 19, 45
 - orthogonal, 24
- lattice, 57
- lexicographic ordering, 9
- linear extension, 55
- linearity of expectation, 49
- LYM Proof, 28

- Möbius function, 64
- Mertan's function, 67
- mutually orthogonal, 45

- natural partial order, 69
- Netto systems, 33

- odd permutation, 17
- Orbit-Counting Lemma, 74
- Orbit-Stabilizer Theorem, 74
- order ideal, 58
- orthogonal, 19
- orthogonal Latin square, 24

- $p(n)$, 68
- Pappus' Theorem, 43
- parallel, 43
- Paris-Harrington Theorem, 54
- part, 68
- partial order, 55
- partition, 68
- path, 6
- periodic, 7
- permanent, 22
- permutation, 3
 - even/odd, 17
 - sign, 17
- permutation group, 72
- Pigeonhole Principle, 47
- poset, 55
 - dimension, 61
 - standard, 62
- poset isomorphism, 67
- principal downsets, 60
- projective geometry, 41

- q -analogues, 38

- Ramsey numbers
 - diagonal, 49
- Ramsey's Theorem, 48
 - infinite version, 53
- reduced echelon form, 38
- reverse mathematics, 53
- Riemann Hypothesis, 67
- rooted tree, 6
- RSK Correspondence, 70

- saturated chain, 28
- SDR, 19
- sign of a permutation, 17
- Sperner, 28
- Sperner's Theorem, 28
- stabilizer, 74
- standard poset, 62
- Steiner system, 31
- Steiner triple system, 31
- Stirling numbers
 - first kind, 15
 - second kind, 15
- Stirling's Formula, 4
- subsystem, 35
- surjections, 12
- system of distinct representatives, 19

- t -intersecting, 27
- tableaux, 70
- tree, 6
 - rooted, 6
- van der Waerden Conjecture, 23
- Veblen-Young Theorem, 42
- Young's Lattice, 69