MAST30012 Discrete Mathematics

School of Mathematics and Statistics
The University of Melbourne

2021

Contents

1 Sets and Tuples

Sets and Tuples

Definition 1 (Sets and Tuples)**.**
- A **set** is a list of objects or elements.
- A **tuple** is an ordered list of objects or elements.

Notation 2 (Sets and Tuples)**.** Sets are denoted by enclosing the elements in braces. So $\{a, b, c, d\}$ is the set with elements a, b, c, and d. Tuples are denoted by enclosing the elements in parenthesis, e.g. (a, c, d).

Definition 3 (Cardinality)**.** Let X be a finite set. The cardinality or size of X, denoted by $|\,X\,|$ is the number of elements in X.

Note: The sets $\{a, b, c\}$ and $\{b, c, a\}$ are the same because they contain the same elements. However, the tuples (a, b, c) and (b, c, a) are distinct.

2 Probability by Enumeration

Probability by Enumeration

Axiom 4 (Probability by Enumeration)**.** Let T be the set of possible outcomes and F the set of favourable outcomes. Assuming each outcome is equally likely the probability of F is:

$$\Pr(F) = \frac{\text{number of favourable outcomes}}{\text{total number of outcomes}} = \frac{|\,F\,|}{|\,T\,|}$$

Note: This axiom provides the fundamental link between counting or enumeration of finite sets and probability theory.

Example:

1. 'Birthday' problem: In a room with r people how likely is it that two have the same birthday?
2. When two dice are thrown what is the probability that the total is 8?

Two Dice Problem

Example: Back to the two dice problem. Probability total is 8.

$$\begin{array}{rllllll}
T = \{ & (1,1), & (1,2), & (1,3), & (1,4), & (1,5), & (1,6), \\
 & (2,1), & (2,2), & (2,3), & (2,4), & (2,5), & (2,6), \\
 & (3,1), & (3,2), & (3,3), & (3,4), & (3,5), & (3,6), \\
 & (4,1), & (4,2), & (4,3), & (4,4), & (4,5), & (4,6), \\
 & (5,1), & (5,2), & (5,3), & (5,4), & (5,5), & (5,6), \\
 & (6,1), & (6,2), & (6,3), & (6,4), & (6,5), & (6,6)\ \}
\end{array}$$

There are six rows and six columns. So $|\,T\,| = 6 \times 6 = 36$.

The favourable outcomes are $F = \{(2,6),(3,5),(4,4),(5,3),(6,2)\}$. Hence

$$\Pr(\text{Total is } 8) = \frac{|F|}{|T|} = \frac{5}{36}.$$

Note: $(2,6)$ and $(6,2)$ etc. are distinct outcomes, i.e. we distinguish the dice. *We are counting tuples*!

3 Multiplication Principle

Multiplication Principle

Axiom 5 (Multiplication Principle)**.** Let A and B be finite sets and let

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$

Then

$$|A \times B| = |A| \cdot |B|.$$

Example: For the two dice problem: $A = B = \{1,2,3,4,5,6\}$ and $T = A \times B$. Then we have that $|T| = |A| \cdot |B| = 6^2 = 36$.

Example: How many number plates are there with 3 letters then 3 digits?

With $L = \{a,b,c,\ldots,y,z\}$ and $D = \{0,1,\ldots,9\}$ we have

$$|L \times L \times L \times D \times D \times D| = |L|^3 \cdot |D|^3 = 26^3 \cdot 10^3.$$

4 Addition Principle

Addition Principle

Axiom 6 (Addition Principle)**.** Let A and B be finite disjoint sets, i.e. $A \cap B = \emptyset$, then

$$|A \cup B| = |A| + |B|.$$

More generally, if $A_1, A_2, \ldots, A_n$ are finite pairwise disjoint sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Example: Identify 3 'natural' disjoint sets from this class of students.

$$\begin{aligned} L &= \{\text{Left-handed students inside this lecture theatre}\} \\ R &= \{\text{Right-handed students inside this lecture theatre}\} \\ A &= \{\text{Ambidextrous students inside this lecture theatre}\} \end{aligned}$$

Then

$$L \cap R = L \cap A = R \cap A = \emptyset$$

$$|L \cup R \cup A| = |L| + |R| + |A| = \#\text{ of students in this lecture theatre.}$$

Addition Principle – Example

Example: How many integers between 100 and 100,000 are there that use different odd digits?

We solve this by breaking the problem into subsets according to the number of digits in the integers. There are either three, four or five digits (the cases).

Addition Principle – Example

Case 1: Integers with three digits. There are five odd digits. We have to choose three different odd digits. There are 5 choices for the first odd digit, 4 for the second, 3 for the third. So all in all $5 \cdot 4 \cdot 3 = 60$ such integers.

Case 2: There are $5 \cdot 4 \cdot 3 \cdot 2 = 120$ integers with four distinct odd digits.

Case 3: Five distinct odd digits. There are $5! = 120$ such integers.

The three subsets or cases are clearly disjoint.

By the Addition Principle there are $60 + 120 + 120 = 300$ integers of the required type.

5 Complement Principle

Complement Principle

Theorem 7 (Complement Principle)**.** *Let A and B be finite sets with $B \subset A$. Then*

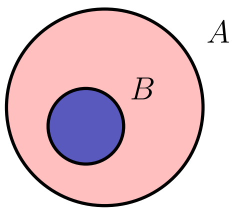
$$|A \backslash B| = |A| - |B|.$$

Proof: This is a simple consequence of the Addition Principle:

$$A = (A \backslash B) \cup B \quad \text{and} \quad (A \backslash B) \cap B = \emptyset$$

$$\Rightarrow \quad |A| = |A \backslash B| + |B| \qquad \text{(Addition Principle)}$$

$$\Rightarrow \quad |A \backslash B| = |A| - |B|.$$



Complement Principle

The complement principle is useful in counting sets with a restriction where we can embed the sought after set in a larger easy to count set and we can easily count the complementary set.

Complement Principle

Example: Count the integers from 0 to $999,999$ containing the digit '1'.

Solutions: View the integers as 6-tuples with entries from $\{0, 1, 2, \ldots, 9\}$.

By the multiplication principle there are 10^6 integers in total.

Consider the set of integers Y *not* containing the digit '1'.

These are 6-tuples with entries from $\{0, 2, \ldots, 9\}$, i.e.,

$$Y = \big\{(x_1, x_2, \ldots, x_6) \,|\, x_i \in \{0, 2, \ldots, 9\}\big\}$$

By the multiplication principle there are 9^6 such integers.

By the complement principle the number of integers containing the digit '1' is

$$10^6 - 9^6.$$

6 Birthday Problem

Birthday Problem

Example: Assuming that there are 365 days per year, and birthdays are uniformly spread among these days, what is the probability that in a group of r randomly chosen people, at least two have the same birthday?

Solution: Record birthdays by an integer from 1 to 365 starting from Jan 1, e.g., March $1^{st} = 31 + 28 + 1 = 60$.

Form a tuple of birthdays, $(b_1, b_2, \ldots, b_r)$, where b_r is the birthday of person r, and each $b_j \in \{1, 2, \ldots, 365\}$.

Use the basic probability formula:

$$\Pr(\text{2 or more birthdays coinciding}) = \frac{|\,F\,|}{|\,T\,|}$$

Here

$F = \{(b_1, b_2, \ldots, b_r) \,|\, b_j \in \{1, \ldots, 365\},\ \text{two or more } b_j\text{'s are the same}\}$

$$T = \{(b_1, b_2, \ldots, b_r) \,|\, b_j \in \{1, \ldots, 365\}$$

Birthday Problem (continued)

Immediately, by the multiplication principle, $|\,T\,| = 365^r$.

To evaluate $|\,F\,|$, we consider instead the complement of F:

$$C = \{(b_1, b_2, \ldots, b_r) \,|\, b_j \in \{1, \ldots, 365\} \text{ with all of the } b_j\text{'s different}\}.$$

We have by the complement principle: $|\,F\,| = |\,T\,| - |\,C\,|$.

To compute $|\,C\,|$, we have:

$$\begin{aligned}
&365 \text{ ways to choose } b_1\\
&364 \text{ ways to choose } b_2\\
&\quad\vdots\\
&365 - r + 1 \text{ ways to choose } b_r
\end{aligned}$$

Hence, by the multiplication principle,

$$|\,C\,| = 365 \cdot 364 \cdot \ldots \cdot (365 - r + 1)$$

Birthday Problem (continued)

Hence,

$$\begin{aligned}
|\,F\,| &= 365^r - 365 \cdot 364 \cdot \ldots \cdot (365 - r + 1)\\
&= 365^r \left(1 - 1 \cdot \frac{364}{365} \cdot \ldots \cdot \frac{(365 - r + 1)}{365}\right)
\end{aligned}$$

$$\Rightarrow \quad \Pr(\,\geq 2 \text{ birthdays coinciding}) = 1 - \frac{364}{365} \cdot \ldots \cdot \frac{(365 - r + 1)}{365}$$

In particular:

$$\begin{aligned}
r = 2,\quad &\Pr(\geq 2 \text{ birthdays coinciding}) = 1/365\\
r = 23,\ &\Pr(\geq 2 \text{ birthdays coinciding}) \approx 0.5072972\\
r = 116,\ &\Pr(\geq 2 \text{ birthdays coinciding}) \approx 0.999999998846
\end{aligned}$$

So in a group of just 23 people there is a better than even chance of two people having the same birthday.

In a class the size of this (enrolment as of July 25) it is almost certain there is at least one shared birthday.

7 Multisets

Multisets

Sometimes we want to repeat elements such as in $B = \{a, a, c, d, d\}$.

Problem is B is *not* a set. In a set all elements are distinct.

Solution: **Multisets** or "Sets with repetition".

A more formal definition of a multiset is

Definition 8 (Multiset)**.** Let A be a finite set and $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ then a multiset M is a map

$$M : A \to \mathbb{N}_0$$

where $M(a)$ is the number of repetitions of the element $a \in A$.

Example: If $A = \{a, b, c, d\}$ then for B above

$$M(a) = 2,\ M(b) = 0,\ M(c) = 1,\ M(d) = 2.$$

Multisets

Notation 9 (Multiset)**.**

1. **Conventional:** $B = \{a, a, c, d, d\}$. That is use set notation with repeated elements (though strictly speaking not a set).
2. **Exponents:** $B = \{a^2, b^0, c^1, d^2\}$.
3. **Map:** $B = (M(a), M(b), M(c), M(d))$.

Note: As with sets the order of the elements in a multiset is irrelevant.

Example: All the following multisets are identical (based on $A = \{a, b, c, d\}$)

$$\begin{array}{ccc} \{a, a, b, d, d, d\} & \{b, d, a, d, d, a\} & \{d, a, b, a, d, d\} \\ \{a^2, b^1, c^0, d^3\} & \{c^0, b^1, a^2, d^3\} & \{d^3, a^2, b^1, c^0\} \end{array}$$

Multisets

Definition 10 (Cardinality of Multiset)**.** The size or cardinality of a multiset $M = \{a_1^{n_1}, a_2^{n_2}, \cdots, a_m^{n_m}\}$ is

$$|\,M\,| = n_1 + n_2 + \cdots + n_m.$$

Example: $|\,\{b, d, a, a, d, a\}\,| = 6$. The size of the "set with repetitions".

Example: List all distinct 3-scoop icecreams with two flavours $F = \{a, b\}$.

3-scoop possibilities: $a, a, a \quad a, a, b \quad a, b, b \quad b, b, b$

Better to list as multisets: $\{a, a, a\}$, $\{a, a, b\}$, $\{a, b, b\}$, $\{b, b, b\}$.

$$\text{Scoop configurations} \quad \longleftrightarrow \quad \text{Multisets}$$

Note: If you care where scoops go use tuples, e.g.,

$$(b, b, a) \neq (b, a, b) \neq (a, b, b).$$

8 Words

Words

Definition 11 (Words)**.** A word in an alphabet $A = \{a_1, a_2, \ldots, a_k\}$ is a tuple $w = (x_1, x_2, \ldots, x_n) \in A^n$.

Words are often written by concatenating the entries $w = x_1 x_2 \cdots x_n$.

The elements of A are called ‘letters’ or ‘characters’ or ‘symbols’ etc.

The set of all words in A is denoted A^* – called the *Kleene closure* of A.

Note that A^* includes the empty word.

Words

Example:

1. $A = \{a, b, c\}$ Words: $abc, bbc, b, ca, ccbbac, \cdots$
2. $A = \{\triangle, \square\}$ Words: $\triangle\triangle, \square, \triangle\square\square, \square\triangle\square\square\triangle\triangle\square\square\square, \cdots$

Note: Using concatenation is convenient. But be careful that there is no ambiguity. If $A = \{0, 1, 01\}$ is ‘01’ a single letter or a two letter word?

Definition 12 (Unambiguous Alphabets)**.** If an alphabet does *not* have the above sort of ambiguity then it is called an *unambiguous alphabet.*

Words

Definition 13 (Properties of Words)**.**

- **Length** of a word w = number of letters in w, denoted $|w|$

- $|w|_{a_i}$ = number of times a_i occurs in w
- Two words $w_1 = x_1x_2\cdots x_n \in A^*$ and $w_2 = y_1y_2\cdots y_n \in A^*$ are **equal** iff $|w_1| = |w_2|$ and $x_i = y_i\ \forall i$

- **Product** of w_1 and w_2 is the concatenation of the two words:

$$w_1 \cdot w_2 = w_1w_2 = x_1x_2\cdots x_ny_1y_2\cdots y_m$$

- A **subword** of w is any non-empty sequence of *consecutive* letters.
- An **ordered alphabet** is an alphabet whose letters are “totally ordered”.

Words

Example:

- $|aca| = 3, \quad |abba|_b = 2, \quad |abba|_d = 0$
- $w = abbca; \quad a, ca, bbc, abb$ are subwords
- $A = \{a, b, c, e\}$ with $a < b < c < e$ is an ordered alphabet
- $B = \{\triangle, \square\}$ with $\triangle < \square$ is an ordered alphabet

Multisets and Words

A multiset M taken from an unambiguous set A can be represented by a unique word in the ordered alphabet A in which the order of the letters of the word have the same ordering as A.

Example: Let $A = \{a, b, c\} \qquad a < b < c.$

$$\begin{array}{lcl} \{a, a, b\} & \longrightarrow & aab \\ \{b, a, c, b\} & \longrightarrow & abbc \\ \{a, b, b, a\} & \longrightarrow & aabb \end{array}$$

Ordering of the letters is *required* since the order of the elements of a multiset is *not* important.

Problem

Example: Four different coloured cars are parked in a row. The red and blue cars are always next to each other and the yellow car must be next to a red car or a blue car. How many ways can the cars be parked?

Solution: Let $C = \{r, b, y, g\}$ be the set of cars:

$$r \to \text{red},\ b \to \text{blue},\ y \to \text{yellow},\ g \to \text{green}.$$

Let P = set of parking configurations. Then $P \subset C^*$ s.t. if $w \in P$ then

1. $|\,w\,| = 4$.
2. Each letter is used once.
3. rb or br is a subword.
4. yr or ry or yb or by is a subword.

Method: Use Addition Principle on a partition of P.

Problem (continued)

Claim: Restrictions 3 and 4 $\quad \Rightarrow \quad w$ must have a subword:

$$yrb,\ ybr,\ rby, \quad \text{or} \quad bry$$

(i) All words in P formed by adding g to the front or back of these subwords.

(ii) Easy to check (exercise) that this results in four disjoint subsets of size 2.

Hence, $\qquad |\,P\,| \;=\; 2 + 2 + 2 + 2 \;=\; 8.$

Note: Make sure that

(i) the partition into subsets produces the whole set

(ii) the subsets in the partition are mutually disjoint

is fulfilled for more complex problems is difficult!

It is **very** easy to miss cases!

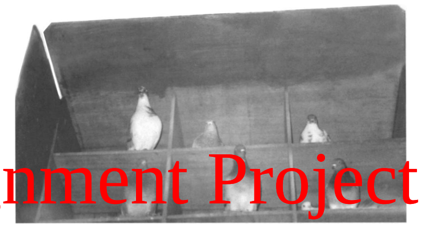
9 Pigeonhole Principle

Pigeonhole Principle (PHP)

Theorem 14 (Pigeonhole Principle)**.** *Let n be an integer. If $(n+1)$ pigeons occupy n pigeonholes, then at least one hole will house 2 or more pigeons.*

Proof Without Words:
The Pigeonhole Principle

RAN LIBESKIND-HADAS
Harvey Mudd College
Claremont, CA 91711



Seven pigeons in six boxes

Pigeonhole Principle (PHP)

Theorem 15 (Pigeonhole Principle)**.** *Let n be an integer. If $(n+1)$ pigeons occupy n pigeonholes, then at least one hole will house 2 or more pigeons.*

Note: This is *not* an enumeration principle, but an *existence* theorem. It states that under certain conditions (i.e. $(n+1)$ pigeons) a certain type of configuration *must* exist.

As an exercise in mathematical logic we will state the theorem more formally.

All possible pigeon hole occupancies correspond to the set of n-tuples:

$$P_n = \Big\{(p_1, p_2, \cdots, p_n) \in \mathbb{N}_0^n \;\Big|\; \sum_{i=1}^{n} p_i = n+1\Big\}$$

where $p_i = \#$ pigeons in box i.

Example: $n = 2:\quad P_2 = \{(0,3),(1,2),(2,1),(3,0)\}$

Pigeonhole Principle

Then the PHP can be stated (very) formally as

Theorem 16 (Pigeonhole Principle)**.**

$$\forall p \in \mathbb{N}_0^n \quad p \in P_n \to \exists p_i \in p \;\; s.t. \;\; p_i \geq 2.$$

Here we recall that $\forall$ means "for all", $\exists$ means "there exists", s.t. is just short-hand for "such that" and $\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \cdots\}$.

Also $p_i \in p$ means p_i is an entry in the n-tuple p.

Here we shall give two simple proofs of the PHP.

1. Prove the contrapositive statement

2. Proof using the bounded set theorem

Pigeonhole Principle: Proof 1

Proof by contrapositive:

- The logic statement $p \longrightarrow q$ is equivalent to the contrapositive:

$$\neg q \longrightarrow \neg p \qquad\qquad (\text{not } q \longrightarrow \text{not } p).$$

- The negation of: $\exists\, x \in S \;\; s.t. \;\; p(x)$ is $\forall x \in S \quad \neg p(x)$ or

$$\neg\,(\exists\, x \in S \;\; s.t. \;\; p(x)) \iff (\forall x \in S \quad \neg p(x))$$

Thus we first find the contrapositive.

$$\begin{array}{llcl} & p \in P_n & \longrightarrow & \exists\, p_i \in p \;\; s.t. \;\; p_i \geq 2 \\ \iff & \neg\,(\exists\, p_i \in p \;\; s.t. \;\; p_i \geq 2) & \longrightarrow & \neg\,(p \in P_n) \\ \iff & \forall p_i \in p \quad \neg(p_i \geq 2) & \longrightarrow & p \notin P_n \\ \iff & \forall p_i \in p \quad p_i < 2 & \longrightarrow & p \notin P_n \end{array}$$

Pigeonhole Principle: Proof 1

Proof by contrapositive continued:

$$\forall p_i \in p \quad p_i < 2 \quad \longrightarrow \quad p \notin P_n$$

$$\begin{array}{lll} & \forall p_i \in p \quad p_i \in \{0, 1\} & \text{(Premis)} \\ \Rightarrow & \displaystyle\sum_{i=1}^{n} p_i \;\leq\; \sum_{i=1}^{n} 1 \;=\; n & \text{(All the } p_i \text{ are 0 or 1)} \\ \Rightarrow & p \notin P_n & \text{(If } p \in P_n \text{ then } \displaystyle\sum_{i=1}^{n} p_i = n+1) \\ \Rightarrow & \forall p_i \in p \quad p_i < 2 \quad \longrightarrow \quad p \notin P_n & \end{array}$$

This completes the proof.

Bounded Set Theorem

Theorem 17 (Bounded Set)**.** *Given a bounded set of real numbers X then*

$$\sup(X) \geq \mathbb{E}(X).$$

Note: sup is the supremum or least upper bound. For a finite set this is equal to the value of the maximum element.

$\mathbb{E}$ denotes the expected value, which for a finite set is the average value.

So if X is a finite set $X = \{a_1, a_2, \ldots, a_n\}$, $a_i \in \mathbb{R}$, then the theorem above says

$$\max\{a_i\} \geq \frac{a_1 + a_2 + \ldots + a_n}{n}.$$

That is, in a finite set the element with the maximum value is at least as large as the average value of the elements in the set.

Pigeonhole Principle: Proof 2

Proof by bounded set: Need to prove:

$$p \in P_n \quad \longrightarrow \quad \exists p_i \in p \;\; s.t. \;\; p_i \geq 2$$

$$\begin{array}{rrcll} & p \in P_n & & & \text{(Premiss)} \\ \Rightarrow & \max\{p_i\} & \geq & \dfrac{p_1 + p_2 + \ldots + p_n}{n} & \text{(Bounded Set Theorem)} \\ & & = & \dfrac{n+1}{n} & (\text{Since } p \in P_n) \\ & & = & 1 + \dfrac{1}{n} & \\ \Rightarrow & \max\{p_i\} & \geq & 2 & (n \geq 1,\ \max\{p_i\} \text{ an integer}) \\ \Rightarrow & \exists p_i \in p \;\; s.t. \;\; p_i \geq 2 & & & \end{array}$$

Application of Pigeonhole Principle

Theorem 18. *Given any sequence of n positive integers there exists a subsequence of consecutive integers whose sum is divisible by n.*

Example:

- Take $n = 4$
- Consider the sequence $1, 5, 9$.
- Here 4 does not divide $1, 5, 9, 1 + 5 = 6, 5 + 9 = 14, 1 + 5 + 9 = 15$.

- The claim is that if we include one further positive integer, either the new integer is itself divisible by 4, or a sum of consecutive members from the sequence including the new integer is divisible by 4.
- Say we add 5 to the sequence to get $1, 5, 9, 5$.

  Here $1 + 5 + 9 + 5 = 20$, which is divisible by 4.
- Maybe check some further cases yourself.

Application of Pigeonhole Principle

Proof: Let the n positive integers be $(a_1, a_2, \ldots, a_n)$. Define

$$b_i = \Big(\sum_{p=1}^{i} a_p\Big) \mod n.$$

[From example $n = 4$, $(1, 5, 9, 5)$, $b_1 = 1$, $b_2 = 2$, $b_3 = 3$, $b_4 = 0$]

Case 1: For some i, $b_i = 0$. Then the statement is true.

Case 2 (remaining case): $1 \le b_i \le n - 1$.

Application of Pigeonhole Principle

Proof (continued): Apply the pigeonhole principle. The remainders $1, 2, \ldots, n-1$ are the pigeonholes, and $b_1, b_2, \ldots, b_n$ are the pigeons (b_i goes to hole j if $b_i = j$).

We then have that at least two of the b_i's have the same value.

Let these be b_p and b_q with $p \le q$, say.

Thus

$$b_q - b_p = 0 \quad \Rightarrow \quad (a_{p+1} + a_{p+2} + \ldots + a_q) \mod n = 0.$$

So the statement is again true.

Generalisation of Pigeonhole Principle

Theorem 19 (Generalised Pigeonhole Principle)**.** *Let $n, k \in \mathbb{N}$. If there are n identical objects and k boxes into which the objects are distributed then there exists a box containing at least $\left\lceil \frac{n}{k} \right\rceil$ objects.*

Notation 20 (Floor and Ceiling)**.** If $x \in \mathbb{R}$ then $\lceil x \rceil$, pronounced "ceiling of x", is the smallest integer greater than or equal to x

$$\lceil x \rceil = \min\, \{n \in \mathbb{Z} \,|\, n \ge x\}.$$

Similarly, $\lfloor x \rfloor$, pronounced "floor of x", is

$$\lfloor x \rfloor = \max\, \{n \in \mathbb{Z} \,|\, n \le x\}.$$

Generalisation of Pigeonhole Principle

Proof: We have k boxes and n objects so consider

$$P_k(n) = \Big\{(p_1, p_2, \cdots, p_k) \in \mathbb{N}_0^k \;\Big|\; \sum_{i=1}^{k} p_i = n\Big\}.$$

Take any $p \in P_k(n)$. Then by the bounded set theorem

$$\begin{aligned}
& \max\{p_i\} \geq \frac{\sum\limits_{p_i \in p} p_i}{|\,p\,|} = \frac{n}{k} \\
\Rightarrow\quad & \max\{p_i\} \geq \left\lceil \frac{n}{k} \right\rceil \qquad\qquad (\max\{p_i\} \in \mathbb{N}) \\
\Rightarrow\quad & \exists\, p_i \in p \;\; s.t. \;\; p_i \geq \left\lceil \frac{n}{k} \right\rceil.
\end{aligned}$$

Application of Pigeonhole Principle

Theorem 21 (Increasing or Decreasing Subsequences)**.** *Every sequence of n^2+1 distinct real numbers contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing.*

Proof: Let $x_1, x_2, \ldots, x_{n^2+1}$ be a sequence of n^2+1 distinct real numbers.

To each x_k associate an ordered pair (i_k, d_k) :

- i_k: length of longest increasing subsequence starting at x_k.

- d_k: length of longest decreasing subsequence starting at x_k.

Application of Pigeonhole Principle

Proof (continued):

Supposition: No increasing or decreasing subsequences of length $n+1$.

Now $1 \leq i_k, d_k \leq n$ so there are n^2 possible ordered pairs (i_k, d_k).

By the Pigeonhole Principle two of the pairs must be equal.

$\Rightarrow \exists\;\; x_s$ and x_t, with $s < t \quad s.t. \quad i_s = i_t$ and $d_s = d_t$.

The terms of the sequence are distinct so either $x_s < x_t$ or $x_s > x_t$.

Application of Pigeonhole Principle

Proof (continued):

If $x_s < x_t$ we can form an increasing subsequence of length $i_s + 1$.

Take x_s followed by the increasing subsequence starting at x_t of length $i_t = i_s$.

This contradicts $i_s = i_t$ (and i_s longest increasing subsequence).

A similar argument leads to a contradiction of $d_s = d_t$ when $x_s > x_t$.

Hence our original supposition, "No increasing or decreasing subsequences of length $n + 1$", must be false.

This completes the proof by contradiction.

10 Maps and Object Arrangements

Maps and Object Arrangements

Let $f : X \to A$ be a map or function (both X and A are finite sets).

We can interpret f combinatorially in two ways:

$\boxed{\text{I}}$ Arranging objects in boxes:

- X = set of objects to be sorted into
- A = set of boxes

Each way of sorting the objects is a map $f : X \to A$, e.g.,

$X = \{1, 2, 3, 4\}$, $A = \{a, b, c, d\}$, $f(1) = a$, $f(2) = d$, $f(3) = b$, $f(4) = a$

Box sorting:	1, 4	3		2
	a	b	c	d

Maps and Object Arrangements

$\boxed{\text{II}}$ Tuples or words:

- X = set of *positions* of letters (entries in tuple)
- A = alphabet (assumed unambiguous)

$X = \{1, 2, 3, 4\}$, $A = \{a, b, c, d\}$, $f(1) = a$, $f(2) = a$, $f(3) = c$, $f(4) = d$

$$w = aacd \qquad \text{Note: } |w| = |X|.$$

Duality of Object Arrangements and Words

Each objects-into-boxes arrangement corresponds to a *unique* word:

$$\begin{array}{rcl} \text{Objects} & \longleftrightarrow & \text{Positions} \\ \text{Boxes} & \longleftrightarrow & \text{Letters} \end{array}$$

This duality is often used to recast an enumeration into an easier form.

Duality of Object Arrangements and Words

1. Duality is a *bijection* (one-to-one onto map) between the set of n-object arrangements into boxes and words of length n defined by interchanging objects & positions and boxes & letters.

2. We can put constraints on the map f which in turn become constraints on box occupancy and by duality on word forms.

   (a) f injective : $\begin{cases} \longleftrightarrow & \text{at most one object per box} \\ \longleftrightarrow & \text{no repeated letters} \end{cases}$

   (b) f surjective : $\begin{cases} \longleftrightarrow & \text{no empty boxes} \\ \longleftrightarrow & \text{every letter used at least once} \end{cases}$

Example

Example: $X = \{1, 2, 3\} \quad A = \{a, b\}, \quad f$ surjective

Arrangements: $f : X \to \underset{a}{|\_\_\_|}\underset{b}{\_\_\_|}$ with no empty boxes.

$$\Rightarrow \quad |1\,2|\ 3\ | \quad |1\,3|\ 2\ | \quad |2\,3|\ 1\ |$$

$$|\ 1\ |2\,3| \quad |\ 2\ |1\,3| \quad |\ 3\ |1\,2|$$

Words: Each letter $\{a, b\}$ used at least once:

$$aab,\ aba,\ baa,\ abb,\ bab,\ bba$$

Duality map:

$$|1\,3|\ 2\ | \overset{\text{dual}}{\longrightarrow} \begin{matrix} a & b & a \\ 1 & 2 & 3 \end{matrix} \qquad |\ 3\ |1\,2| \overset{\text{dual}}{\longleftarrow} \begin{matrix} b & b & a \\ 1 & 2 & 3 \end{matrix}$$

11 Permutations

Permutations

- Different orderings of distinct objects are referred to as permutations.
- Let the distinct objects be denoted $a_1, a_2, \cdots, a_n$. From these objects form the set
  $$X = \{a_1, a_2, \cdots, a_n\}. \text{ (Note: } |X| = n)$$
- The task is to enumerate (count) all tuples $(x_1, x_2, \cdots, x_n)$ with each $x_j \in X$ and furthermore all the x_j's distinct.

More generally we have

Definition 22 (Permutation)**.** A **k-permutation** of a finite set X is a k-tuple

$$(x_1, x_2, \cdots, x_k) \qquad x_i \in X, \qquad x_i \neq x_j \ \forall i \neq j$$

If $k = |\,X\,|$ the tuple is called a **permutation** of X.

Permutations

Note:

1. $x_i \neq x_j$ means all entries are distinct and requires $k \leq |\,X\,|$.
2. If X is unambiguous k-permutations are often written as words.
3. A k-permutation is an injective map:

$$p: \text{ positions in the } k\text{-tuple } \longrightarrow X.$$

4. A permutation is a bijective map.

Example: $X = \{1, 2, 3, 4\}$

- 2-permutations: 12, 21, 13, 31, 14, ...
- 3-permutations: 123, 124, 213, 214, 132, ...
- 4-permutations: 1234, 2134, 2314, 2341, ...

Permutations

Theorem 23 (Number of k-permutations)**.** *The number of k-permutations of a finite set X with $|\,X\,| = n \geq k$ is*

$$(n)_k := \underbrace{n(n-1)(n-2)\cdots(n-k+1)}_{k \text{ factors}}.$$

Note: $(n)_k$ is called a *falling factorial.*

Corollary 24 (Number of Permutations)**.** *The number of permutations of X is $(n)_n = n!$, where $n = |\,X\,|$.*

Example: All permutations for $n = 3$:

$$\underbrace{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)}_{\text{6 permutations in total=3×2×1}}$$

Permutations

Proof: Let P_k be the set of all k-permutations of X.

$$\begin{array}{llll} \text{Let} & X_n & = X & \\ & X_{n-1} & = X_n \backslash \{x_1\}, & x_1 \in X_n \\ & X_{n-2} & = X_{n-1} \backslash \{x_2\}, & x_2 \in X_{n-1} \\ & \vdots & & \\ & X_{n-k+1} & = X_{n-k+2} \backslash \{x_{k-1}\}, & x_{k-1} \in X_{n-k+2} \end{array}$$

Then

$$
\begin{aligned}
P_k &= X_n \times X_{n-1} \times X_{n-2} \times \cdots \times X_{n-k+1} \\
\Rightarrow \quad |\,P_k\,| &= |\,X_n\,| \cdot |\,X_{n-1}\,| \cdot |\,X_{n-2}\,| \cdots |\,X_{n-k+1}\,| \\
&= n(n-1)(n-2)\cdots(n-k+1) \;=\; (n)_k
\end{aligned}
$$

Problem

Example: There are seven distinct red cars and 3 distinct blue cars. How many ways can they be parked (in a line) so that:

1. The blue cars form a block (no red cars between them)?
2. The cars at the ends are red and no blue cars are adjacent?

Solution 1: Treat the blue cars as a single object:

$$X = \{r_1, r_2, \ldots, r_7, B\},\ B = \{b_1, b_2, b_3\}$$

Parking configurations of X are permutations of X so $(7+1)!$ configurations.

Must also account for parking configurations within B $(= 3!)$.

So total number of parking configurations $= 8! \cdot 3!$

Problem continued

Solution 2: To solve this problem consider permutations of *positions* of cars.

The two constraints imply configurations are of the type:

$$R_1 \underset{1}{\underline{\quad}} R_2 \underset{2}{\underline{\quad}} R_3 \underset{3}{\underline{\quad}} R_4 \underset{4}{\underline{\quad}} R_5 \underset{5}{\underline{\quad}} R_6 \underset{6}{\underline{\quad}} R_7$$

Where: $\quad R_i \rightarrow$ red car, $\quad \underset{j}{\underline{\quad}} \rightarrow$ possible blue car position.

- Permutations of the seven positions $\{R_1, \ldots, R_7\}$ give the possible configurations of red cars.
- 3-permutations of the six positions $\{\underset{1}{\underline{\quad}}, \ldots, \underset{6}{\underline{\quad}}\}$ give the possible positions of the blue cars.
- Total number of parking configurations $= 7! \cdot (6)_3 = 7! \cdot 6 \cdot 5 \cdot 4.$

12 Combinations

Combinations

Definition 25 (Combinations)**.** A selection of r distinct elements from a set of size n *without* regard to order is called a **combination** of size r and the number of possible selections or combinations is denoted C^n_r.

Note: The order of elements is irrelevant so combinations are represented by sets (in fact a combination is just a subset).

There are many ways of thinking about combinations such as

- Given n elements and two boxes, count the number of ways of putting r elements in box 1, and $n-r$ elements in box 2 when the order of the elements within the boxes doesn't matter.
- Number of ways of choosing a subset of size r from a set of size n.
- Number of ways to colour n elements so that r elements are *red* and $n-r$ elements are *blue*.

Number of Combinations

Theorem 26 (Number of Combinations)**.** *The number of combinations of r elements from a set of size n is*

$$C^n_r = \frac{(n)_r}{r!} = \frac{n!}{r!\,(n-r)!} = \binom{n}{r};$$

that is, they are counted by the **binomial coefficients** $\binom{n}{r}$.

Proof: There are $(n)_r$ ways of forming r-permutations of the set. We can form any r-permutation by first choosing a combination of size r and then ordering the r elements chosen. There are $r!$ ways of ordering the chosen elements. This shows that

$$(n)_r = C^n_r \cdot r!$$

and the result follows.

Note: This explains why the binomial coefficient $\binom{n}{r}$ is often pronounced or referred to as 'n choose r'.

Basic Properties of Combinations

Corollary 27 ($C^n_r = C^n_{n-r}$)**.** *Let n and r be nonnegative integers with $r \le n$. Then $C^n_r = C^n_{n-r}$*

Proof: From previous theorem it follows that

$$C^n_{n-r} = \frac{n!}{(n-r)!\,(n-(n-r))!} = \frac{n!}{(n-r)!\,r!} = C^n_r.$$

Note: Combinatorially this makes perfect sense. In forming a combination choosing r elements that goes into the combination is equivalent to choosing $(n-r)$ elements that *does not* go into the combination.

Corollary 28 ($C_0^n = C_n^n = 1$)**.** *With the convention (or definition) that* $0! = 1$ *we have* $\binom{n}{0} = 1$ *and* $\binom{n}{n} = 1$.

Note: There is 1 way of selecting 0 or n elements from n elements. Even for $n = 0$ the result makes sense: There is 1 way of choosing no element from zero elements (or the empty set is the only subset of the empty set).

13 Interpreting Binomial Coefficients

Example

Example: List subsets of size 2 from $\{a, b, c, d\}$, and so determine $\binom{4}{2}$.

- The subsets are:

$$\begin{aligned} \{a,b\}, \{a,c\}, \{a,d\} \\ \{b,c\}, \{b,d\} \\ \{c,d\} \end{aligned}$$

- Hence: $\binom{4}{2} = 6$.

Note: We can put the elements from these subsets in the first box and the remaining elements from the set in the second box. This gives an interpretation or the problem in terms of boxes.

Combinations

Example: Calculate $\binom{n}{3}$ using the boxes interpretation.

- Procedure:

  - Choose any of the n elements to place in box 1 (n choices).
  - Choose any of the remaining $n - 1$ elements to also place in box 1.
  - Choose any of the remaining $n - 2$ elements to also place in box 1.
  - The remaining $n - 3$ elements are placed in box 2.

- Order is not important. So suppose we have chosen the elements a, d, g.

  - Then $\{a, d, g\} = \{a, g, d\} = \{d, a, g\} = \{d, g, a\} = \{g, a, d\} = \{g, d, a\}$.
  - There are $3!$ ways of arranging 3 objects on a line (permutations). Must divide out by this.

- Hence

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{3!}.$$

Interpreting $\binom{n}{r}$ - Example

Example: Number of ways to colour n elements so that r elements are coloured and $n - r$ elements are not.

- To see the equivalence of this viewpoint, list the elements in order.
- e.g. $n = 6$, $r = 2$

x_1	x_2	x_3	x_4	x_5	x_6
$\square$	$\square$	$\square$	$\square$	$\square$	$\square$

- Form a subset from the coloured elements e.g.
- $\{x_3, x_6\}$

x_1	x_2	x_3	x_4	x_5	x_6
$\square$	$\square$	$\blacksquare$	$\square$	$\square$	$\blacksquare$

Interpreting $\binom{n}{r}$

- Colouring: can think of placing n blocks in a row, $\binom{n}{r}$ is the number of ways of colouring r blocks red, $n - r$ blocks blue.
- Or, n_r red blocks, n_b blue blocks. Number of arrangements is

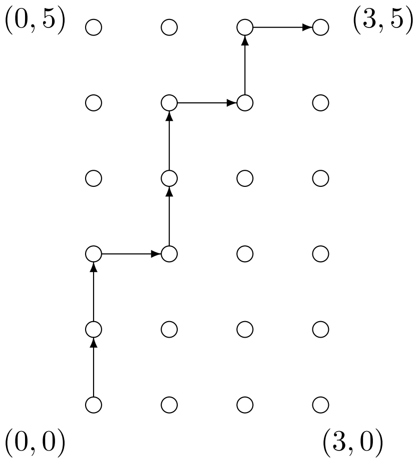
$$\binom{n_r + n_b}{n_r} = \frac{(n_r + n_b)!}{n_r!\, n_b!}$$

- $(n_r + n_b)!$ ways of arranging $(n_r + n_b)$ blocks, dividing out the number of ways of arranging the red blocks $(n_r!)$ and the blue blocks $(n_b!)$.
- Note that this is unchanged by $n_r \leftrightarrow n_b$.

14 Lattice Path Problem

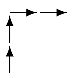
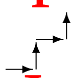
Lattice Path Problem

Example: Consider an integer grid. The number of lattice paths which go from $(0, 0)$ to (n, m) with each step either to the North or East is equal to $\binom{n+m}{n}$.



Lattice Path Problem

- Count the number of ways to go from $(0, 0)$ to (n, m), $n, m \geq 0$ according to the rule that paths consist of North and East steps only.
- There is an obvious one-to-one correspondence (or bijection) between the lattice path problem and words in the alphabet $\{N, E\}$, e.g.,

 $\iff$ $NNEE$  $\iff$ $ENEN$

  There are n east and m north steps so each path corresponds to a word of length $n + m$ with n letters E and m letters N.

- Also equivalent to arranging $\underbrace{n \text{ red blocks}}_{\text{east steps}}$ and $\underbrace{m \text{ blue blocks}}_{\text{north steps}}$ in a line.
- Hence the number of paths is $\binom{n+m}{n}$ or $\binom{n+m}{m}$.
- As these paths are counted by binomial coefficients they are called **binomial paths**.

15 Combinations: Ordering, Replacement and Repetition

Combinations: Ordering, Replacement and Repetition

Choosing r elements from a set of size n can be viewed as a sampling problem. In general sampling problems can be classified as follows.

1. **Order:** Is the sample (the chosen elements) ordered or not?
2. **Replacement:** Can an element be chosen more than once?

3. **Repetition:** Are the elements of the set distinct or not?

Thus far in forming combinations we have mostly considered cases with n distinct elements (no repetition) and the chosen elements were all different (no replacement).

The following example will demonstrate how to count with **replacement**.

Sample with Replacement

Example: Alice has a purse containing small change, i.e. 5, 10, 20, and 50 cent pieces. If the purse contains 12 coins how many possible combinations of coins are there?

Solution: A sample of size $r = 12$ is to be chosen from the set $\{5, 10, 20, 50\}$ so replacement is necessary and the sample is unordered.

Place the coins in order of their denomination. A typical sample may look like:

We need to count all such configurations. A nice trick does this. Place a separator between different denominations:

Sample with Replacement

Configurations can now be represented in a two-letter alphabet $\{C, L\}$:

$$CCCLCCCCCLCCLCC$$

Note: There is no need to specify the denomination of the coins. This is determined by the placement of the separators, i.e., every coin to the left of the first separator is a five cent piece etc.

The counting problem is now easy. There are $12 + 3$ positions 3 of which are separators and 12 of which are coins. So the answer is:

$$\#\text{ configurations} = \binom{15}{12} = \binom{15}{3} = 455.$$

Combinations: Ordering and Replacement

Theorem 29 (Unordered Sample with Replacement)**.** *The number of unordered samples of size r with replacement chosen from a set of size n is*

$$C_r^{n+r-1} = \binom{n+r-1}{r} = \binom{n+r-1}{n-1} = C_{n-1}^{n+r-1}$$

Proof: This is straightforward generalisation of the previous example.

We summarise our results on combinations in the following table:

Set Size	Sample Size	Replacement	Ordered	Number
n	r	No	Yes	$(n)_r$
n	r	No	No	C_r^n
n	r	Yes	Yes	n^r
n	r	Yes	No	C_r^{n+r-1}

At the Icecream Parlour

Example: An icecream parlour sells 3 scoop icecreams from 20 flavours.

1. How many combinations are possible if all scoops are different?
2. What if scoops with the same flavour are allowed?

Solution 1: $\binom{20}{3} = \frac{20 \times 19 \times 18}{3!} = 1140$

Solution 2: This a problem of selection with replacement.

Here $n = 20$, $r = 3$, giving

$$\binom{22}{3} = \frac{22 \times 21 \times 20}{3!} = 1540$$

At the Icecream Parlour (continued)

- Problem 2 can also be solved using "natural" disjoint sets:

$$S_1 = \{\text{all scoops are different}\}$$
$$S_2 = \{\text{two scoops are the same, the other different}\}$$
$$S_3 = \{\text{three scoops all the same}\}$$

- So

$$\# \text{ configurations} = |S_1| + |S_2| + |S_3| \qquad \text{by the addition principle}$$
$$= \binom{20}{3} + 20 \times 19 + 20$$
$$= \binom{20}{3} + 2\binom{20}{2} + \binom{20}{1} = 1140 + 380 + 20 = 1540 = \binom{22}{3}.$$

16 Combinatorial Identies

Combinatorial Identies

Theorem 30 (Sum of Binomial Coefficients)**.**

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = \sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

Proof: Count total number of subsets (from set of size n) in two ways.
LHS: Decomposition according to the subset size:

$$\{\text{subsets with 0 elements}\} \cup \{\text{subsets with 1 element}\} \cup \cdots$$
$$\cdots \cup \{\text{subsets with } n \text{ elements}\} = \{\text{all subsets}\}$$

Since the subsets are disjoint the Addition Principle gives the LHS.
Next we show that from n elements there are a total of 2^n subsets:
Think of the n elements as a tuple of size n. Record a 1 if the element is in the subset and a zero otherwise, e.g., for $n = 3$:

$$(0,0,0) \leftrightarrow \emptyset \qquad (0,1,0) \leftrightarrow \{x_2\} \qquad (1,1,0) \leftrightarrow \{x_1, x_2\}$$

The problem is reduced to counting tuples of size n with elements from $\{0,1\}$. $\Rightarrow$ Total number = RHS = 2^n, by the multiplication principle.

Combinatorial Identies

Theorem 31 (Recurrence for binomial coefficients)**.**

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Proof: The LHS is just the total number of subsets of size r from a set of size n, say, $\{1, 2, \cdots, n\}$.

Now partition these subsets into two disjoint sets: Those which *include* the element n and those which *don't*.

The first set can be identified with forming subsets of size $r-1$ (element n is already included) from a set of size $n-1$ (the remaining elements).

The second set entails forming subsets of size r from a set of size $n-1$.

Then by the Addition Principle we get the RHS.

Note: Pascal's triangle follows directly from this recursion relation.

Back to the Icecream Parlour

In the icecream parlour example we used two different methods to derive the number of ways to choose three scoops of icecream when scoops with the same flavour are allowed.

This way we found: $\binom{22}{3} = \binom{20}{3} + 2\binom{20}{2} + \binom{20}{1}$.
This is a special case of Vandermonde's identity.

Theorem 32 (Vandermonde's Identity)**.** *Let m, n and r be nonnegative integers with r not exceeding m or n. Then*

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}.$$

Note: The above special result follows by setting $n = 20, r = 3, m = r - 1 = 2$. Now this violates the restriction $r \leq m$. But we can use $\binom{2}{3} = 0$ and its OK.

In the general case, $m = r - 1$, the identity still holds if we use $\binom{r-1}{r} = 0$.

Vandermonde's Identity – Proof

Proof: We prove Vandermonde's identity by showing that the LHS and RHS count the same objects in two different ways:

Suppose we have two disjoint sets A and B with m and n elements.

We can pick r elements from the union of the two sets in $C_r^{m+n} =$ LHS ways.

Next pick elements from the union but keep track of where they came from.

We can pick $r - k$ elements from A and k elements from B. By the Multiplication Principle we know this can be done in $C_{r-k}^{m} C_k^n$ ways.

Clearly k can range from 0 to r and the resulting sets that we pick are disjoint so by the Addition Principle we get the RHS.

This proves Vandermonde's identity.

Vandermonde and Icecream

Is there a general r-scoop problem related to Vandermonde's identity?

Answer: Yes, but we need to engage in a bit of reverse engineering.

Look at the identity in the case $m = r - 1$:

$$\binom{n+r-1}{r} = \sum_{k=0}^{r} \binom{r-1}{r-k}\binom{n}{k}.$$

Now we have $n = \#$ of flavours and $r = \#$ of scoops.

From previous work we know that LHS = number of ways to choose r scoops with replacement from n flavours.

What about the RHS?

It would seem we are breaking the problem into 'partitions' according to k. So could k be the number of *distinct* flavours in our selection of scoops?

Vandermonde and Icecream

This makes sense since $\binom{n}{k}$ is "n choose k". But what about the factor $\binom{r-1}{r-k}$?

A concrete example should clarify things. Say $n = 20$, $r = 5$:

k	Factor	Flavours	Remaining Scoops	Comment
0	$\binom{4}{5}\binom{20}{0}$	None	None	Can't choose no flavours
1	$\binom{4}{4}\binom{20}{1}$	a	$aaaa$	All scoops the same
2	$\binom{4}{3}\binom{20}{2}$	ab	aaa, aab, abb, bbb	Choose 2 flavours then 3 scoops from 2 flavours
3	$\binom{4}{2}\binom{20}{3}$	abc	aa, ab, ac, bb, bc, cc	Choose 3 flavours then 2 scoops from 3 flavours
4	$\binom{4}{1}\binom{20}{4}$	$abcd$	a, b, c, d	Choose 4 flavours then 1 scoop from 4 flavours
5	$\binom{4}{0}\binom{20}{5}$	$abcde$	None	All scoops distinct

Vandermonde and Icecream

It should now be clear what is going on.

The term on the RHS comes about as:

We partition the problem on number of chosen flavours k.

First we choose k distinct flavours in $\binom{n}{k}$ ways.

Then we choose remaining $r-k$ scoops from k flavours with **replacement**.

This can be done in $\binom{k+(r-k)-1}{r-k} = \binom{r-1}{r-k}$ ways.

So we can choose r scoops, using k out of n flavours in $\binom{r-1}{r-k}\binom{n}{k}$ ways.

Then sum over $0 \le k \le r$ to get the RHS (scoop partitions are clearly disjoint).

17 Binomial Theorem

Binomial Theorem

Theorem 33 (Binomial Theorem)**.** *Let x and y be variables and $n \in \mathbb{N}$. Then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k\, y^{n-k}.$$

Proof: We shall give a combinatorial proof.

Now $$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ factors in total}}.$$

Think of each x as a white block and each y as a black block. Expanding out the factors then gives terms which correspond to arranging a total of n blocks (coloured white or black) in a line.

The term $x^k y^{n-k}$ corresponds to having k white blocks and $n-k$ black blocks, showing that its coefficient must be $\binom{n}{k}$.

Binomial expansion

Example: Illustration in the case $n = 3$:

$$
\begin{aligned}
&(x+y)(x+y)(x+y)\\
&= (\square + \blacksquare)(\square + \blacksquare)(\square + \blacksquare)\\
&= \square\square\square + (\blacksquare\square\square + \square\blacksquare\square + \square\square\blacksquare) + (\square\blacksquare\blacksquare + \blacksquare\square\blacksquare + \blacksquare\blacksquare\square) + \blacksquare\blacksquare\blacksquare\\
&= \text{All white} + \text{1 black, 2 white} + \text{2 black, 1 white} + \text{All black}\\
&= x^3 + 3x^2y + 3xy^2 + y^3\\
&= \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3
\end{aligned}
$$

Binomial expansion

Setting $y = 1$, we obtain

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

What do we find if we set $x = -1$? How can we interpret the identity?

LHS is 0. RHS is a sum of positive (k even) and negative (k odd) terms.

Theorem 34 (Even and Odd Subsets). *For any set the number of subsets with an even number of elements equals the number of subsets with an odd number of elements.*

Example: $X = \{1, 2, 3, 4\}$

- Even subsets: $\emptyset, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3,4\}$ – 8 subsets.
- Odd subsets: $\{1\}, \{2\}, \{3\}, \{4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}$ – 8 subsets.

Yet Another Identity

Theorem 35.

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

Proof: From a class with n students choose a committee of size k with a subcommittee of size m.

LHS: First choose a committee with k members in $\binom{n}{k}$ ways then from the k members choose a subcommittee with m members in $\binom{k}{m}$ ways.

RHS: First choose the m members of the subcommittee from the whole class then choose the remaining $k-m$ members from the remaining class.

A little more Number Theory

This last identity has an interesting application to Number Theory.

Theorem 36 (Erdös and Szekeres, 1978). *For integers $0 < m \le k < n$, $\binom{n}{m}$ and $\binom{n}{k}$ have a nontrivial common factor. That is,*

$$\gcd\left(\binom{n}{m}, \binom{n}{k}\right) > 1.$$

Proof: Suppose, to the contrary that $\binom{n}{m}$ and $\binom{n}{k}$ are relatively prime.

By the previous identity $\binom{n}{m}$ divides $\binom{n}{k}\binom{k}{m}$.

By supposition $\binom{n}{m}$ and $\binom{n}{k}$ have no common factors so $\binom{n}{m}$ must divide $\binom{k}{m}$.

This is impossible since clearly $\binom{n}{m} > \binom{k}{m}$.

18 Inclusion-Exclusion Principle

Inclusion-Exclusion Principle – Warm Up

The Addition Principle tells us how to find the size of a union of disjoint sets.

But what if the sets A and B aren't disjoint? What is $|A \cup B|$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

On the RHS, $|A \cap B|$ is subtracted since elements occurring in both A and B are counted twice in $|A| + |B|$.

Somewhat more formally we can argue as follows: Let $C = A \cap B$.

Now $A \backslash C$, $B \backslash C$ and C are disjoint sets and

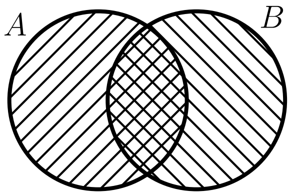
$$A \cup B = (A \backslash C) \cup (B \backslash C) \cup C$$

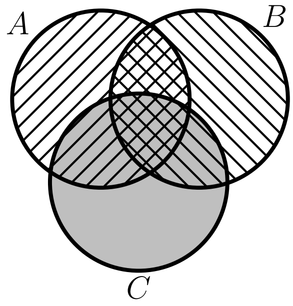
Hence by the Addition Principle and the Complement Principle

$$\begin{aligned} |A \cup B| &= |A \backslash C| + |B \backslash C| + |C| = (|A| - |C|) + (|B| - |C|) + |C| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

Inclusion-Exclusion Principle – Graphically

Graphically we have the following illustration:





And we get for the case with three sets:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Licence Plate Problem

Example: A license plate contains 3 letters followed by 3 digits. How many different plates can be produced if the plates cannot contain both the letter 'O' and the digit '0'.

Solution: We have $L = \{A, B, \dots, Z\}$ and $D = \{0, 1, \dots, 9\}$ and a valid licence plate is a word $w = l_1 l_2 l_3 d_1 d_2 d_3$ with $l_i \in L$ and $d_i \in D$ s.t. the letter 'O' and digit '0' don't *both* occur in w. Let N denote the set of valid license plates.

We previously looked at the unrestricted case T and found $|T| = 26^3 \cdot 10^3$.

Let S_1 = set of plates with no 'O' and S_2 = set of plates with no '0'.

Let $L_{\mathrm{O}} = L \setminus \{\mathrm{O}\}$ and $D_0 = D \setminus \{0\}$. Then $S_1 = L_{\mathrm{O}}^3 \times D^3$ and $S_2 = L^3 \times D_0^3$. Hence

$$|S_1| = |L_{\mathrm{O}}|^3 \cdot |D|^3 = 25^3 \cdot 10^3$$

$$|S_2| = |L|^3 \cdot |D_0|^3 = 26^3 \cdot 9^3$$

Both S_1 and S_2 satisfy the "no O-0" constraint $\quad \Rightarrow \quad N = S_1 \cup S_2$.

Licence Plate Problem (continued)

$$
\begin{aligned}
\Rightarrow \quad |\,N\,| \quad &= \quad |\,S_1\,| + |\,S_2\,| && \text{(Addition Principle)} \\
&= \quad 25^3 \cdot 10^3 + 26^3 \cdot 9^3 \\
&= \quad 26^3 \cdot 10^3 \cdot \underbrace{\left(\left(\frac{25}{26}\right)^3 + \left(\frac{9}{10}\right)^3\right)}_{=1.6\ldots} \\
\Rightarrow \quad |\,N\,| \quad &> \quad 26^3 \cdot 10^3 \\
\text{But} \quad |\,T\,| \quad &= \quad 26^3 \cdot 10^3 && \text{— \quad Ooops!!}
\end{aligned}
$$

What has gone wrong?

Actually: $\quad S_1 \cap S_2 \neq \emptyset \quad \Rightarrow \quad$ can't use Addition Principle!

e.g. $\quad$ AAA222 $\in S_1$ (no 'O') $\quad$ **and** $\quad$ AAA222 $\in S_2$ (no '0'.)

Licence Plate Problem (resolved)

We are over-counting words in

$$
S_1 \cap S_2 = L_{\mathrm{O}}^3 \times D_0^3 \quad \Rightarrow \quad |\,S_1 \cap S_2\,| = 25^3 \cdot 9^3.
$$

By the Inclusion-Exclusion Principle we then get:

$$
\begin{aligned}
|\,N\,| \quad &= \quad |\,S_1\,| + |\,S_2\,| - |\,S_1 \cap S_2\,| \\
&= \quad 25^3 \cdot 10^3 + 26^3 \cdot 9^3 - 25^3 \cdot 9^3 \\
&= \quad 26^3 \cdot 10^3 \cdot \underbrace{\left(\left(\frac{25}{26}\right)^3 + \left(\frac{9}{10}\right)^3 - \left(\frac{25}{26}\right)^3\left(\frac{9}{10}\right)^3\right)}_{=0.96\ldots}
\end{aligned}
$$

Inclusion-Exclusion Principle

Following on from the concrete examples we can state the general theorem.

Theorem 37 (Inclusion-Exclusion Principle).

$$
\begin{aligned}
|\, A_1 \cup A_2 \cup \cdots \cup A_n \,| &= |\, A_1 \,| + |\, A_2 \,| + \cdots + |\, A_n \,| \\
&- |\, A_1 \cap A_2 \,| - |\, A_1 \cap A_3 \,| - \cdots |\, A_{n-1} \cap A_n \,| \\
&+ |\, A_1 \cap A_2 \cap A_3 \,| + \cdots + |\, A_{n-2} \cap A_{n-1} \cap A_n \,| \\
&\quad \vdots \\
&+ (-1)^{n-1} |\, A_1 \cap A_2 \cap \cdots \cap A_n \,| \\
&= \sum_{k=1}^{n} (-1)^{k-1} \sum_{\{s_1,\ldots,s_k\} \subset \{1,2,\ldots,n\}} |\, A_{s_1} \cap A_{s_2} \cap \cdots \cap A_{s_k} \,| .
\end{aligned}
$$

Inclusion-Exclusion Principle – Interpreted in Words

Inclusion-Exclusion is intuitively simpler than the theorem looks.

So let us decipher it line-by-line:

On the LHS we ask for the number of elements in a union of n sets, which are not necessarily disjoint.

On the RHS we say this is the sum of the number of elements in each set.

Were the sets disjoint that would be it by the Addition Principle.

However, some elements occur in more than one set so we remove the count of these.

But we may have removed too much, namely elements occurring in more than two sets. So we add these back in and so on.

That is first we "include" all elements from all sets, then we "exclude" all the elements occurring in two or more sets, then we "include" elements occurring in three or more sets, and so on.

Example

Example: In a European languages class there are 25 students: 14 speak Spanish, 12 French, 6 French and Spanish, 5 German and Spanish, 2 Spanish, French and German.

The 6 that speak German all speak either French or Spanish as well.

How many students speak none of these languages?

Solution: The given information can be summarized as:

$$
\begin{aligned}
&|S| = \text{Number of Spanish speakers} = 14 \\
&|F| = \text{Number of French speakers} = 12 \\
&|G| = \text{Number of German speakers} = 6 \\
&|F \cap S| = 6 \\
&|G \cap S| = 5 \\
&|F \cap S \cap G| = 2
\end{aligned}
$$

Missing information is: $|F \cap G|$.

Example – Continued

We are given that $G \subset (F \cup S)$.

We also know that $|G \cap S| = 5$, $|F \cap S \cap G| = 2$ and $|G| = 6$.

Can therefore conclude that $|F \cap G| = 3$.

Applying the Inclusion-Exclusion principle, we have

$$\begin{aligned} |S \cup F \cup G| = \ & 14 + 12 + 6 \\ & - (6 + 5 + 3) \\ & + 2 \\ = \ & 20. \end{aligned}$$

Let $|T|$ denote the total number of students.

Given $|T| = 25$, we therefore have $|T| - |S \cup \ F \cup G| = 25 - 20 = 5$.

An Exercise

Example: Calculate the number of positive integers less than or equal to 1,000 divisible by 7, 10 or 15.

Solution: For $1 \leq k \leq 1000$, let A_k denote the set of integers divisible by k.

$$\begin{aligned} A_k &= \{k, 2k, 3k, \ldots, \left\lfloor \frac{1000}{k} \right\rfloor k\} \\ \Rightarrow \qquad |A_k| &= \left\lfloor \frac{1000}{k} \right\rfloor \end{aligned}$$

Also,

$$A_k \cap A_l = A_n$$

where $n =$ the lowest common multiple of k and l, e.g. $A_{10} \cap A_{15} = A_{30}$

Final answer $= 256$.

Inclusion-Exclusion Principle – Towards a Proof

For 4 sets the Inclusion-Exclusion formula read:

$$\begin{aligned} & |A \cup B \cup C \cup D| \\ = \ & |A| + |B| + |C| + |D| \\ & -(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|) \\ & +(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) \\ & -|A \cap B \cap C \cap D| \end{aligned}$$

- To check this formula, our task is to show that for an element x in some given sets, it is counted once on the RHS.
- e.g. suppose $x \in A, C, D$, $x \notin B$

- Then subsets containing x, formed by intersections, are

$$\begin{array}{lllr} \text{"size" } 1 & A, C, D & = & +3 \\ \text{"size" } 2 & A \cap C, A \cap D, C \cap D & = & -3 \\ \text{"size" } 3 & A \cap C \cap D & = & \underline{+1} \\ & & & +1 \end{array}$$

  as required.

Inclusion-Exclusion Principle – Proof

Proof: The proof follows by formalising the above example. We shall show that the elements in $A_1 \cup A_2 \cup \cdots \cup A_n$ are counted exactly once on the RHS:

$$\sum_{k=1}^{n} (-1)^{k-1} \sum_{\{s_1,\ldots,s_k\} \subset \{1,2,\ldots,n\}} |\, A_{s_1} \cap A_{s_2} \cap \cdots \cap A_{s_k} \,| \,.$$

Suppose x is an element in r of the sets $A_1, A_2, \ldots, A_n$ where $1 \le r \le n$. This element is counted C_1^r times by $\sum |\, A_i \,|$ and C_2^r times by $\sum |\, A_i \cap A_j \,|$.

In general, it is counted C_m^r times in the term involving the intersection of m distinct sets. Thus this element is counted

$$C_1^r - C_2^r + C_3^r - \cdots + (-1)^{r-1} C_r^r = \sum_{k=1}^{r} (-1)^{k-1} C_k^r$$

times on the RHS. From our work on the binomial theorem we know

$$\sum_{k=0}^{r} (-1)^k C_k^r = 0 \quad \Rightarrow \quad \sum_{k=1}^{r} (-1)^{k-1} C_k^r = C_0^r = 1.$$

This completes the proof of the inclusion-exclusion principle.

19 Bijection Principle

Bijection Principle

Bijections have already been mentioned several times. e.g., between object arrangements and words or binomial paths and words.

We have seen that it can be useful to count the same set in two different ways (e.g. in proving binomial identities) or to replace one counting problem with an "equivalent" problem (e.g. the small coins example).

These ideas are formalised in the following fundamental principle.

Bijection Principle

Axiom 38 (Bijection Principle (BP))**.** Let A and B be finite sets. If there is a bijection from A to B, then $|\, A \,| = |\, B \,|$.

1. The BP only tells us two sets have the same size. It only gives us a formula for $|\, A \,|$ if we *already* have one for $|\, B \,|$.

2. With different formulae for $|A|$ and $|B|$ the BP gives us an **identity**.

3. The BP is frequently used to replace the problem of finding $|A|$ by that of finding $|B|$. To do this we must know (or prove) that a bijection exists between A and B.

Bijection Principle - Example 1

Example: Bijective proof that $C^n_r = \dfrac{(n)_r}{r!}$.

Proof: We shall give a bijective proof that $(n)_r = r!\,C^n_r$.

Task: 'Find' two sets A and B enumerated by $(n)_r$ and $r!\,C^n_r$, respectively, and a bijection $T : A \to B$.

Let $N = \{1, 2, \ldots, n\}$

- A = the set of all r-permutations of N. By definition $|A| = (n)_r$.
- $B = \{(S, \pi) \mid S \subseteq N, |S| = r, \pi \text{ a permutation of } S\}$.

  There are C^n_r subsets of N of size r and $r!$ permutations of each subset.
- Hence $|B| = r!\,C^n_r$.

But what is T? Do a simple example to get idea for general case.

Bijection Principle - Example 1

Take $n = 3$, $r = 2$: $\quad r! = 2, \quad C^n_r = C^3_2 = 3, \quad (n)_r = 3 \cdot 2 = 6.$

$$A = \{12, 21, 13, 31, 23, 32\} \rightsquigarrow |A| = 6$$

Subsets: $\quad S \subseteq \{1, 2, 3\}$ s.t. $|S| = 2 \rightsquigarrow \{1, 2\}, \quad \{1, 3\}, \quad \{2, 3\}$

Permutations: $\quad 12 \quad 21 \quad 13 \quad 31 \quad 23 \quad 32$

$$\Rightarrow \quad B = \{(\{1, 2\}, 12), (\{1, 2\}, 21), (\{1, 3\}, 13), (\{1, 3\}, 31), (\{2, 3\}, 23), (\{2, 3\}, 32)\}$$

The bijection should be clear: $T(12) = (\{1, 2\}, 12)$, $\;T(21) = (\{1, 2\}, 21), \ldots$

General Case: If the permutation of r objects is $\pi = a_1 a_2 \cdots a_r$, then

$$T(\pi) = (\{a_1, a_2, \ldots, a_r\}, \pi).$$

Bijection Principle - Example 2

Example: Give a bijective proof of the statement:

Number of subsets of even size = Number of subsets of odd size.

Warm-up: $n = 3$, there are $2^3 = 8$ subsets in total.

subsets of even size		subsets of odd size
$\emptyset$		$\{x_1\}$
$\{x_1, x_2\}$	$\Longleftrightarrow$	$\{x_2\}$
$\{x_1, x_3\}$		$\{x_3\}$
$\{x_2, x_3\}$		$\{x_1, x_2, x_3\}$

Here, the rule is that the element x_1 is to be added to a subset if it wasn't already present, and removed if it was present.

This works for general n and establishes the result.

Bijection Principle - Example 3

Example: Binomial Paths to Binary Words

- A = set of binomial paths: $(0,0) \to (n,m)$.
- With $D = \{0,1\}$, $B = \{w \in D^* \mid |\,w\,| = n+m,\ |\,w\,|_0 = n,\ |\,w\,|_1 = m\}$.

The bijection maps east steps to the digit 0 and north steps to the digit 1.

Formally we can write this as:

$$\begin{aligned} p &= s_1 s_2 \cdots s_{n+m} \in A \qquad s_i = \text{ step } i \\ T(p) &= d_1 d_2 \cdots d_{n+m} \in B \end{aligned}$$

where

$$d_i = \begin{cases} 0 \text{ if } s_i = \text{ East step} \\ 1 \text{ if } s_i = \text{ North step} \end{cases}$$

Bijection Principle – General Notes

1. If $|\,A\,| = |\,B\,| = n$ then there *always* exists $n!$ bijections $T : A \to B$. How? Just list all elements in A and B. Then each permutation of B defines a T.

2. What we want is an "intrinsic" bijection. That is a map defined by the structure of the elements rather than just their position in a list.

3. In all the examples we have defined a map $T : A \to B$, but we have *not* explicitly proved that the map is a bijection (injective and surjective). In this course our bijections are sufficiently simple that we skip this step.

Bijection Principle – General Notes

4. The power of bijections goes well beyond the scope suggested by these simple examples. Say the objects in A can be partitioned into subsets A_i having property p_i. The bijection may then map to subsets of B_i with well-defined properties q_i so $|\,A_i\,| = |\,B_i\,|$.

- Proving theorems about the subsets A_i may be 'easy' and this then gives proofs for the subsets B_i.
- Objects in A can be partitioned into subsets with given properties in a natural way. In B what are the corresponding properties? This can give new and surprising insights into problem B.

20 Bijection Principle and Identities

Bijection Principle and Identities

Next we look at how to use bijections to prove identities such as

1. $$\binom{n}{r} = \binom{n}{n-r}$$

2. $$\sum_{r=0}^{n} \binom{n}{r} = 2^n$$

3. $$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

The general idea is to use that if LHS is $|A|$ and RHS is $|B|$ with $T : A \to B$ a bijection then invoking the BP gives a proof that $|A| = |B|$.

Note: We have already used this idea when proving binomial identities by counting the same set in different ways. Now we shall formally give bijections which were only implied by these proofs.

Identity : $\binom{n}{r} = \binom{n}{n-r}$

Bijective Proof:

- A= set of all r-subsets of an n-set.
- B= set of all $(n-r)$-subsets of an n-set.

Example: $N = \{a, b, c\}$, $r = 1$: $A = \{\{a\}, \{b\}, \{c\}\}$ and $B = \{\{a, b\}, \{a, c\}, \{b, c\}\}$.

We know $|A| = \binom{n}{r}$ and $|B| = \binom{n}{n-r}$. We need bijection $T : A \to B$.

Let $S \subseteq N$, $|S| = r$. Then

$$T(S) = N \backslash S$$

is a bijection and $S \subseteq N \Rightarrow |N \backslash S| = |N| - |S| = n - r$ by the complement principle so we have that $N \backslash S$ is a $(n-r)$-subset of N.

Thus by the BP we get $|A| = |B|$ as required.

Identity : $\displaystyle\sum_{r=0}^{n} \binom{n}{r} = 2^n$

Bijective Proof: The proof given in Week 2 (slide 25) is essentially bijective.

So we just need to formalise it a bit.

- A = set of all subsets of an n-set $N = \{1, 2, \ldots, n\}$.
- B = set of binary strings (words in $\{0, 1\}$) of length n.

LHS is obtained by partitioning A according to the size of the subsets.

RHS is the number of binary strings (or words) of length n.

The bijection is: Let $S = \{a_1, a_2, \ldots a_r\} \subseteq N$ with $|\,S\,| = r$. Then

$$T(S) = b_1 b_2 \cdots b_n, \quad b_i = \begin{cases} 1 \text{ if } i \in S \\ 0 \text{ if } i \notin S \end{cases}$$

Thus $|\,A\,| = |\,B\,| = 2^n$.

Binary Words, Binomial Paths and Subsets

Previously we found a bijection between binary words and binomial paths.

The above example gives a bijection between binary words and subsets.

This gives an (indirect) bijection between binomial paths and subsets.

First reexamine binary words and binomial paths. The bijection to subsets requires *all* binary words of length n. This is not quite what we had before.

Binary Words, Binomial Paths and Subsets

Bijection still maps east steps to the digit 0 and north steps to the digit 1, but

- A = set of binomial paths: $(0, 0) \to$???.
- B = set of binary words of length n.

A binomial path from $(0, 0) \to (x, y) \in \mathbb{N}_0^2$ has length $x + y$ so need $x + y = n$. Hence

A = set of binomial paths from $(0, 0)$ ending on the line $y = -x + n$.

The bijection from paths to subsets of $N = \{a_1, a_2, \cdots, a_n\}$ is: label the steps of the path so s_i labelled a_i then read of the labels of the North steps, e.g.,

$$\begin{array}{l} \underline{a_3}\,|\,a_4 \\ |\,a_2 \\ |\,a_1 \end{array} \quad \to \quad \{a_1, a_2, a_4\} \qquad\qquad \underline{a_1}\ \underline{a_2}\ \underline{a_3}\,|\,a_4 \quad \to \quad \{a_4\}$$

21 More on Multisets

Back to Multisets

Theorem 39 (Number of Multisets)**.** *The number of size k multisets with elements from a set of size n is*

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Proof: If this reminds you of sampling with replacement it should!

A multiset is essentially just a sample from a n-set with replacement.

More formally we note that a multiset is defined by the tuple

$$(a_1^{m_1}, a_2^{m_2}, \dots, a_n^{m_n}), \quad \text{with} \quad \sum_{i=1}^{n} m_i = k, \quad m_i \in \mathbb{N}_0.$$

If the alphabet is ordered we only need the exponents $m_1, m_2, \dots, m_n$ which we can view as (biject to) an arrangement of k identical objects into n boxes.

Note: The objects must be identical as we don't care which box they go to only how many go into a given box.

Multisets – Example

Example: 2 boxes containing 3 identical objects (represented by $\bullet$).

We have the following 'obvious' bijections (delete the first and last "wall" from the box):

$$\begin{array}{ccccc}
 & n_1 = 3, n_2 = 0 & n_1 = 2, n_2 = 1 & n_1 = 1, n_2 = 2 & n_1 = 0, n_2 = 3 \\
 & |\bullet\bullet\bullet|\quad| & |\bullet\bullet|\bullet| & |\bullet|\bullet\bullet| & |\quad|\bullet\bullet\bullet| \\
 & a \quad b & a \quad b & a \quad b & a \quad b \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\
 & \bullet\bullet\bullet\,| & \bullet\bullet\,|\,\bullet & \bullet\,|\,\bullet\bullet & |\,\bullet\bullet\bullet \\
 & 1\,2\,3\,4 & 1\,2\,3\,4 & 1\,2\,3\,4 & 1\,2\,3\,4 \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\
 & (a^3, b^0) & (a^2, b^1) & (a^1, b^2) & (a^0, b^3) \\
\text{or} & \{a, a, a\} & \{a, a, b\} & \{a, b, b\} & \{b, b, b\}
\end{array}$$

In the middle rows we have 4 positions and choose one position for the wall.

Dot–Wall Diagrams

Definition 40 (Dot–Wall Diagrams)**.** A word $w \in W^*$, where $W = \{\bullet, |\}$, is called a **dot-wall diagram**.

Theorem 41 (Number of Dot–Wall Diagrams)**.** *The number of dot-wall diagrams with m walls and k dots is* $\binom{m+k}{k}$.

Proof: Dot-wall diagrams clearly bijects to an object arrangement of black and white blocks on a line with (also recall Alice and her purse)

$$\#\,\text{positions} \;=\; \#\,\text{dots} \;+\; \#\,\text{walls}.$$

Now choose k walls from the $m+k$ possible positions.

Dot–Wall Diagrams and Multisets

Dot-wall diagrams with m walls and k dots bijects to multisets of size k chosen from a set of size $n = m+1$ (as per previous example):

$$T(\overbrace{\underbrace{\cdots}_{m_1}|\underbrace{\cdots}_{m_2}|\cdots\cdots|\underbrace{\cdots}_{m_n}}^{m=n-1 \text{ walls}}) \;=\; (a_1^{m_1}, a_2^{m_2}, \ldots, a_n^{m_n})$$

and from this we get

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k} = \binom{n+k-1}{n-1} \quad \text{with} \quad \sum_{i=1}^{n} m_i = k.$$

22 Multinomial Coefficients

Multinomial Coefficients

We can generalise the binomial coefficients by considering blocks of more than two colours:

1. n blocks (identical except for their colour).
2. k colours: $c_1, c_2 \cdots, c_k$.
3. n_i blocks of colour c_i with $n_1 + n_2 + \cdots + n_k = n$.

How many ways can the blocks be arranged?

Example: $n = 4, n_1 = n_2 = 1, n_3 = 2$, i.e., three colours r, g, b:

$rgbb, rbgb, rbbg \quad grbb, gbrb, gbbr \quad brgb, brbg, bbrg, \quad bgrb, bgbr, bbgr$

So 12 arrangements in total.

Multinomial Coefficients

If we use the (object arrangements) $\leftrightarrow$ (positions) duality or bijection we can state an equivalent box filling problem: the k colours are the k boxes

$$(\text{Colour } c_i \text{ occurs } n_i \text{ times}) \quad \rightsquigarrow \quad (n_i \text{ objects in box } c_i)$$

From previous example we have:

$$\begin{array}{llllll}
 & r\,g\,b\,b & r\,b\,g\,b & \cdots & g\,b\,r\,b & \cdots \\
\text{positions:} & 1\,2\,3\,4 & 1\,2\,3\,4 & & 1\,2\,3\,4 & \\
\big\downarrow \text{ duality} & \quad\downarrow & \quad\downarrow & & \quad\downarrow & \\
\text{boxes:} & \lfloor\, 1 \mid 2 \mid 3,4 \,\rfloor & \lfloor\, 1 \mid 3 \mid 2,4 \,\rfloor & & \lfloor\, 3 \mid 1 \mid 2,4 \,\rfloor & \\
 & \;\; r \;\; g \;\; b & \;\; r \;\; g \;\; b & & \;\; r \;\; g \;\; b &
\end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{n_r = 1,\ n_g = 1,\ n_b = 2}$$

Multinomial Coefficients

Theorem 42 (Multinomials)**.** *The number of ways of placing n distinct unordered objects into k distinct boxes with exactly n_i objects in box i is given by the* **multinomial coefficient**

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1!\, n_2! \cdots n_k!}$$

with $n_1 + n_2 + \cdots + n_k = n$.

Example: For the previous example $n = 4, n_1 = 1, n_2 = 1, n_3 = 2$ we get

$$\binom{4}{1, 1, 2} = \frac{4!}{1!\,1!\,2!} = 12.$$

Example: $k = 2 \ \rightsquigarrow \ \binom{n}{n_1, n_2} = \frac{n!}{n_1!\, n_2!} = \frac{n!}{n_1!\,(n - n_1)!} = \binom{n}{n_1}.$

So we recover the binomials.

Multinomial Coefficients – Proof

Proof: Similar to the proof that binomials count combinations. It is an exercise in the practice classes.

Note: Mathematically we can write arrangements of n objects into k boxes (order of boxes is significant while order of objects within boxes is not) as k-tuples of sets:

Ex. 3 boxes, 7 objects:

$$\lfloor\; 2,4,5 \mid 1,3 \mid 6,7 \;\rfloor$$
$$\downarrow$$
$$(\{2,4,5\},\ \{1,3\},\ \{6,7\})$$

If order within the boxes is significant then we can use k-tuples of tuples.

$$((2,4,5),\ (1,3),\ (6,7)) \neq ((2,4,5),\ (3,1),\ (6,7))$$

Multinomial Expansion

We have the following generalization of the binomial expansion:

Theorem 43 (Multinomial Expansion)**.** *For all $n, k \in \mathbb{N}$ with $m \geq 2$ and for commuting variables $x_1, \ldots, x_k$, we have*

$$(x_1 + \cdots + x_k)^n = \sum_{\substack{n_1,\ldots,n_k \geq 0 \\ n_1+\cdots+n_k=n}} \binom{n}{n_1, \cdots, n_k} x_1^{n_1} \cdots x_k^{n_k}$$

Proof: We will use a bijection to an "objects into boxes arrangement". On the LHS there are (n factors $\to$ n objects) and (k variables $\to$ k boxes).

Then n_i objects goes into box i $\rightsquigarrow$ n_i factors of x_i in product on RHS.

Hence the coefficient of $x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$ in the expansion of the LHS is exactly the multinomial coefficient $\binom{n}{n_1, n_2, \ldots, n_k}$ appearing on the RHS.

Multinomial Identities

Theorem 44 (Sum of Multinomial Coefficients)**.**

$$\sum_{\substack{n_1,\ldots,n_k \geq 0 \\ n_1+\cdots+n_k=n}} \binom{n}{n_1, \cdots, n_k} = k^n.$$

Proof: Set $x_1 = x_2 = \cdots = x_k = 1$ in the multinomial theorem.

Multinomial Identities

Theorem 45 (Multinomial Recursion)**.**

$$\binom{n+1}{n_1, n_2, \ldots, n_k} = \binom{n}{n_1-1, n_2, \ldots, n_k} + \binom{n}{n_1, n_2-1, \ldots, n_k} + \cdots + \binom{n}{n_1, n_2, \ldots, n_k-1}$$

Proof: LHS counts the number of to ways to distribute $n+1$ elements in k boxes with n_i elements in box i.

RHS counts the same thing by taking a given element a and placing it in box i.

Distribute remaining n elements in k boxes with n_j elements in box $j \neq i$ and $n_i - 1$ elements in box i. Sum over the box i in which we placed element a.

Note: This is a generalisation of Pascal's Triangle to multinomials.

23 Sampling with Repetition

Sampling with Repetition

Example: How many different strings can be made by reordering the letters of the word '*SUCCESS*' ?

Solution: Since the word has repeated letters the answer is *not* $7!$

We are looking for all **ordered** samples of size 7 **without replacement**.

Let $x =$ number of possible strings.

Label repeated letters, e.g., S_1, S_2, S_3 and C_1, C_2. Then there are $7!$ ways of ordering (permutations) the labelled *distinct* letters.

Now there are x ways of making the required string a letters. The letters S can be permuted (or labelled) in $3!$ ways and the C's can be labelled in $2!$ ways.

So

$$7! = x(3!)(2!) \quad \Rightarrow \quad x = \frac{7!}{3!\,2!} = \binom{7}{3,2,1,1} = 420.$$

Number of Samples with Repetition

Theorem 46 (Number of Samples with Repetition)**.** *If a set of k distinct objects has repetitions, say n_i repetitions of object a_i, with $n = \sum_i^k n_i$, then the number of* **ordered samples without replacement** *of size n is given by the multinomial coefficient*

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1!\,n_2! \cdots n_k!}$$

Proof: This is a straightforward generalisation of the previous example.

24 Graph Theory

Graph Theory

Definition 47 (Graphs, Vertices and Edges)**.** A **graph** G is an ordered pair $G = (V, E)$ consisting of a finite nonempty set V of objects called **vertices** and a (possibly empty) set E of 2-element subsets of V called **edges**. Vertices $u, v \in V$ are **adjacent** if $\{u, v\} \in E$.

Example: $G = (V, E)$, $V = \{a, b, c, d\}$, $E = \{\{a, b\}, \{a, c\}, \{b, d\}\}$

Graph Theory

Notation 48 (Vertices and Edges)**.** The set of vertices is often denoted $V(G)$ and is called the **vertex set** of G. Similarly the set of edges is denoted $E(G)$ and called the **edge set** of G.

If $u, v \in V(G)$ then an edge $\{u, v\} \in E(G)$ can be denoted uv (we have $vu = uv$).

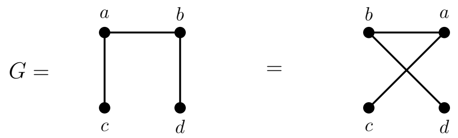
Definition 49 (Order and Size)**.** The number of vertices in G, that is $|\,V(G)\,|$, is called the **order** of G, while $|\,E(G)\,|$ (number of edges in G) is called the **size** of G.

Graph Theory

Definition 50 (Adjacent and Incident)**.** Let $u, v \in V(G)$ and $uv \in E(G)$. We say that u and v are **adjacent** and that the edge uv is **incident** on the vertex u (v).

It is customary to draw graphs with vertices represented as points or circles (open or filled) and edges represented by lines between adjacent vertices.

Example: $G = (V, E)$, $V = \{a, b, c, d\}$, $E = \{\{a, b\}, \{a, c\}, \{b, d\}\}$



Definition 51 (Degree of Vertices)**.** Let $u \in V(G)$. The number of edges incident on u (adjacent vertices) is called the **degree** of u and denoted $\deg(u)$.

Example: In the above graph $\deg(a) = \deg(b) = 2$ and $\deg(c) = \deg(d) = 1$.

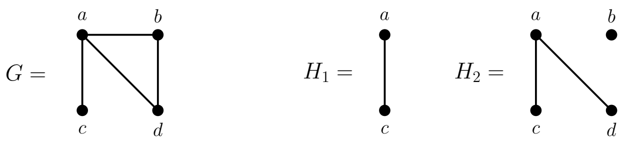
Graph Theory

Definition 52 (Complement)**.** The **complement** of a graph G, denoted G', has the same vertex set as G, $V(G') = V(G)$, but an edge $e \in E(G')$ if and only if $e \notin E(G)$.

Example:

Definition 53 (Subgraph)**.** A **subgraph** H of G has $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$ such that if $uv \in E(H)$ then $u, v \in V(H)$ (we can have $u, v \in V(H)$ but $uv \notin E(H)$).

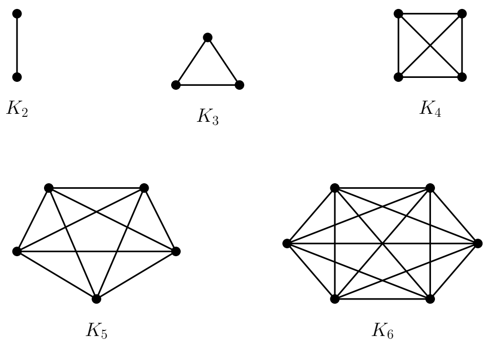
Example:



Complete Graph K_n

Definition 54 (Complete Graphs K_n)**.** The complete graph on n vertices, denoted K_n, is the graph where all vertices are mutually adjacent. Every vertex has degree $n - 1$ and there are $\binom{n}{2}$ edges.

Example:



Note: Any graph with n vertices is a subgraph of K_n. If we colour edges of K_n red if $e \in E(G)$ and blue if $e \notin E(G)$ then the blue edges are the edges of G'.

Walks, Trails, Paths and Cycles

Definition 55 (Walks, Trails, Paths and Cycles)**.** A **walk** in a graph is an alternating sequence

$$v_0, e_1, v_1, e_2, v_2, \ldots, e_k, v_k$$

of vertices and edges, where $k \geq 0$, $v_0, v_1, v_2, \ldots, v_k$ are vertices, and $e_i = v_{i-1}v_i$ for $i = 1, 2, \ldots, k$. This walk is called a (v_0, v_k)**-walk** of **length** k.

Note: A walk in a graph can also be specified by omitting the edges (but in a multigraph, where parallel edges can occur, the edges should be included).

A **trail** is a walk with no edge repeated.

A **path** is a walk in which no vertex is repeated.

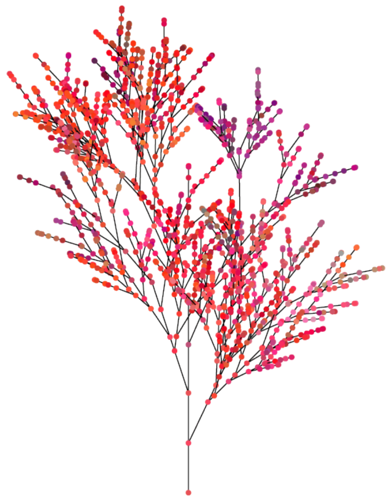
The **length** of a walk is the number of edges in it.

A **cycle** is a walk with distinct vertices $v_0, v_1, \ldots, v_n$ where $n \geq 3$ and $v_0 = v_n$.

A cycle of length n is called an n**-cycle**.

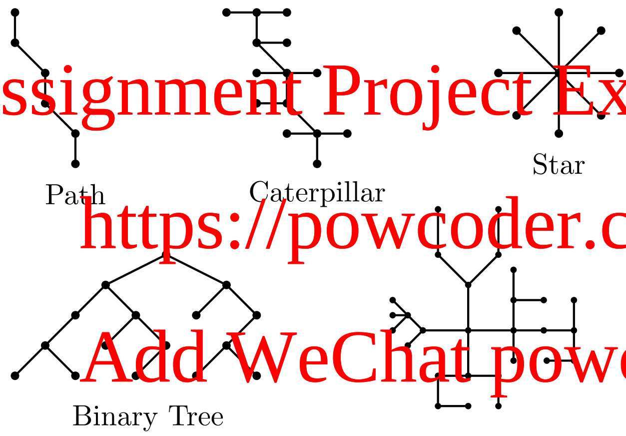
Trees

Definition 56 (Tree)**.** A **tree** is a connected graph with no cycles.



Trees – Examples

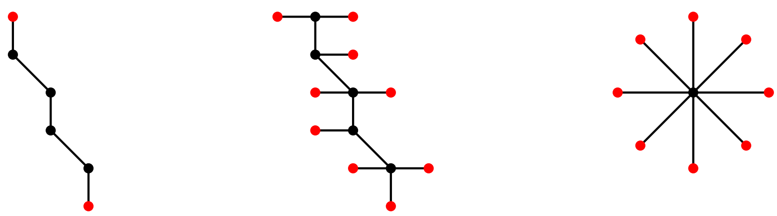
Example:



Leafs

Definition 57 (Leaf)**.** A **leaf** in a tree is a vertex of degree 1.

Example: Leafs are red.



Equivalent Definitions of Trees

Definition 58 (Tree)**.**

1. A connected graph with no cycles.
2. A connected graph G with $|E(G)| = |V(G)| - 1$.

3. A graph G with $|E(G)| = |V(G)| - 1$ and no cycles.

4. A graph in which every pair of vertices are joined by exactly one path.

Properties of Trees

A tree T with order n and size m has the following properties:

1. connected
2. no cycle
3. exactly one path between any two vertices
4. deleting an edge gives a graph with two components
5. deleting a non-leaf vertex v gives a graph with $\deg(v)$ components
6. $m = n - 1$
7. at least two leafs.

Forests

Definition 59 (Forest)**.** A graph is called a **forest** if it has no cycles.

Equivalently, a graph is a forest if each of its components is a tree.

A forest may or may not be connected. A forest is connected iff it is a tree.

Theorem 60. *A forest F of order n has exactly $n - k(F)$ edges, where $k(F)$ is the number of components of F.*

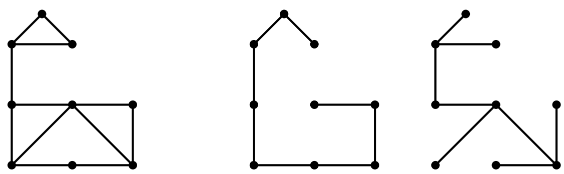
Proof: Let $k = k(F)$ and let $T_1, \ldots, T_k$ denote the components of F. Then each T_i is a tree and so $|E(T_i)| = |V(T_i)| - 1$. Hence

$$|E(F)| = \sum_{i=1}^{k} |E(T_i)| = \sum_{i=1}^{k} (|V(T_i)| - 1) = \left(\sum_{i=1}^{k} |V(T_i)| \right) - k = n - k$$

Spanning Trees

Definition 61 (Spanning Tree)**.** A **spanning tree** of a graph G is a spanning subgraph of G that is a tree.

Example:



G Spanning trees of G

Note: Construct spanning trees by repeatedly deleting an edge that lies on a cycle (edges that are not bridges).

25 Pigeonhole Principles

Back to Pigeonhole Principles

There are many different formulations of Pigeonhole Principles:

1. $n+1$ pigeons in n holes $\Rightarrow$ at least one hole has two pigeons.
2. When m balls go into n boxes at least one box contains at least $\lceil \frac{m}{n} \rceil$ balls.
3. $a_1 + a_2 - 1$ balls in 2 boxes $\Rightarrow$ either box 1 has at least a_1 balls or box 2 has at least a_2 balls.
4. More generally if $m = a_1 + \cdots + a_n - (n-1)$ balls are placed into n boxes then at least one box, say j, contains at least a_j balls.

Often easy to prove when proposition written in the contrapositive form. Consider the third statement: if there are less than a_1 balls in box 1 and less that a_2 balls in box 2, then there is not $a_1 + a_2 - 1$ balls in total.

Note: The values $n+1$ and a_1+a_2-1 are the smallest possible for which statements 1 and 3 are true.

Statement 1 is a special case of statement 4 with $a_i = 2$ for all i.

Examples

Example: 51 numbers from the integers $1 \leq n \leq 100$ are chosen. Show that at least two of them must be consecutive.

Solution: Form 50 pigeonholes labelled by $(2j-1, 2j)$ for $j = 1, 2, \ldots, 50$.

$$\begin{array}{cccc} \square & \square & \cdots & \square \\ \text{box}(1,2) & \text{box}(3,4) & & \text{box}(99,100) \end{array}$$

Place the number k from the set in box $(2j-1, 2j)$ if $k = 2j-1$ or $k = 2j$. There are 51 numbers in the range from 1 to 100 to be placed so at least one of the boxes contains two numbers. Thus these numbers are consecutive.

Examples

Example: There are 5 points in a square of side length 2. Show that there are 2 points having a distance less than or equal to $\sqrt{2}$.

Solution: Divide the square up into 4 sub-squares of side length 1.

The maximum separation of points in the unit square is $\sqrt{2}$ (= the length of the hypotenuse). Since 5 points are placed into 4 unit squares then two or more points must be placed into the same unit square. But points in a unit square are no more than $\sqrt{2}$ units apart.

Examples

Example: In an 11 week period, a chess player plays at least one game a day, but no more than 12 games in a week. Show that there is a succession of consecutive days in which exactly 21 games have been played.

Solution: Let a_i = the number of games played on day i, $1 \leq i \leq 77$ (= 11 weeks).

Let b_i = number of games played up to and including day i, i.e.,

$$b_i = a_1 + a_2 + \cdots + a_i$$

Since at least 1 game is played each day,

$$1 \leq b_1 < b_2 < b_3 < \cdots < b_{77}$$

Also, since no more than 12 games are played in a week,

$$b_{77} \leq 12 \times 11 = 132$$

Example Continued

Now introduce '21':

We know that

$$b_1 + 21 < b_2 + 21 < \cdots < b_{77} + 21 \leq 132 + 21 = 153$$

Now consider the 154 numbers

$$b_1, b_2, \ldots, b_{77}, b_1 + 21, b_2 + 21, \ldots, b_{77} + 21$$

These are between 1 and 153, so by the pigeonhole principle we can conclude that at least two must be the same.

But $b_1, b_2, \ldots, b_{77}$ are distinct, as are $b_1 + 21, b_2 + 21, \ldots, b_{77} + 21$.

Hence we must have $b_i = b_j + 21$ for some $i > j$

$$\Rightarrow 21 = b_i - b_j = \sum_{k=j+1}^{i} a_k$$

Thus on the consecutive days $j + 1, j + 2, \ldots, i$ exactly 21 games were played.

26 Ramsey Theory

Ramsey Theory

Introduction: Loosely speaking Ramsey Theory is concerned with finding the *smallest* size system of objects *certain* to satisfy some given property:

- **Every** size n configuration has property p.
- **At least one** size $n-1$ configuration does not have property p.

Ramsey Theory is thus concerned with existence theorems as was the Pigeon Hole Principle, and indeed Ramsey Theory can be viewed as an advanced generalisation of the PHP.

Example: Restate the pigeon hole problem in a Ramsey like fashion.

Question: What is the minimum number of balls, m, placed into n boxes such that there is certainly at least one box with 2 or more balls?

Answer: Clearly $m \geq n+1$ (if $m = n$ a '1 ball per box' configuration exists). The PHP tells us that $m \leq n+1 \quad \Rightarrow \quad m = n+1$.

Ramsey Theory

The metastatement of Ramsey theory is: "complete disorder is impossible".

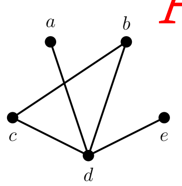
In other words, in a large system, however complicated, there is always a smaller subsystem which exhibits some sort of special structure.

Perhaps the oldest answered question of this type is the following.

Example: What is the smallest group of people such that

1. All pairs are either friends or strangers and
2. **Surely** there are at least 3 mutual friends or 3 mutual strangers.

We can represent this problem as a graph. People are vertices, friendships are indicated by an edge while there is no edge between strangers.



$\Rightarrow$ $\{b, c, d\}$ are mutual friends

$\{a, b, e\}$ and $\{a, c, e\}$ are mutual strangers

Ramsey Theory

We can now rephrase the problem in a more formal way. Let R_n be the set of all possible graphs of order n.

Question: What is the minimum value of n such that

$\boxed{\text{A}}$ **Every** $G \in R_n$ has the property

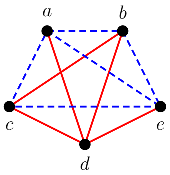
(a) G contains the subgraph K_3 (a triangle)

OR

(b) the complement of G contains the subgraph K_3.

$\boxed{\text{B}}$ **At least one** $G = R_{n-1}$ does not have the above property.

Rather than looking at the complement it is visually easier and equivalent to colour edges red (friends) or blue (strangers). Previous example then gives



$\Rightarrow$ $\{b, c, d\}$ are mutual friends $\rightarrow$ Red K_3

$\{a, b, e\}$ and $\{a, c, e\}$ are mutual strangers
$\rightarrow$ Blue K_3

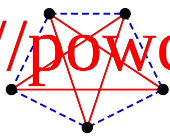
Ramsey Theory

Theorem 62 (3 Mutual Friends/Stangers)**.** *In* **any** *group of 6 or more people (all pairs either friends or strangers) there always exists at least 3 mutual friends or 3 mutual strangers. Moreover 6 is the smallest number of people in a group that guarantees this is true.*

The equivalent more formal graph theoretical theorem says

Theorem 63 (K_3 Subgraphs of a Bicoloured K_n)**.** *In any bicolouring of K_n with $n \geq 6$ there is a monochromatic K_3 and $n = 6$ is the smallest number for which this is true.*

Example: K_5 can be bicoloured with no monochromatic K_3:



Ramsey Theory

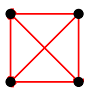
The general problem concerns edge-colourings of the complete graph K_n.

Definition 64 (Ramsey Numbers)**.** The **Ramsey number** $R(a, b)$ is the *smallest* value of n s.t. an edge-colouring of K_n using red and blue edges always contains either a subgraph K_a in red or a subgraph K_b in blue. By symmetry (interchange colours) we have $R(a, b) = R(b, a)$.

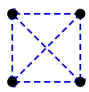
Example: The Ramsey number $R(3, 3)$ is the smallest value of n such that two colouring K_n always give a red triangle or a blue triangle.

The previous theorem tells us that $R(3, 3) = 6$.

Example: $R(4, 4)$ is the smallest number n such that any two colouring of K_n always contains a red K_4 or a blue K_4. It has been proved that $R(4, 4) = 18$.



Red K_4



Blue K_4

$R(2,n)$

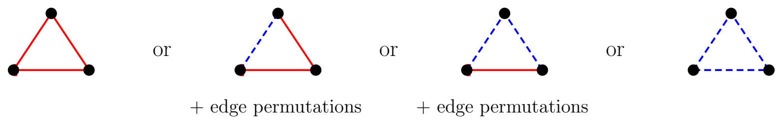
Theorem 65 ($R(2,n) = R(n,2) = n$)**.** *The Ramsey numbers* $R(2,n) = R(n,2) = n$.

Example: Consider the case $R(2,3)$.

$R(2,3)$ is the smallest value of n such that a two colouring of K_n always gives a red K_2 (an edge) or a blue K_3 (a triangle).

$R(2,3) > 2$ since by colouring K_2 blue we do not have the sought pattern.

Consider now the 2-colouring of K_3. We can have:



all of which satisfy the condition, $\Rightarrow$ $R(2,3) \leq 3$.

Combining with $R(2,3) > 2$ gives $R(2,3) = 3$.

Proof that $R(2,n) = n$

Proof: This is essentially a straightforward generalization of the $R(2,3)$ case.

We must have $R(2,n) > n-1$. By colouring K_{n-1} blue we do not have a subgraph K_n in blue or a subgraph K_2 in red.

Consider a 2-colouring of K_n: Using blue to colour all the edges gives K_n blue as a subgraph (as required).

All other colourings have at least one red edge.

Hence for all 2-colourings of K_n, there is either a red edge or a blue K_n.

This tells us that: $R(2,n) \leq n$.

Thus

$$R(2,n) = n \qquad (\text{as } R(2,n) > n-1).$$

Proof that $R(3,3) = 6$

Theorem 66 ($R(3,3) = 6$)**.** *The Ramsey number* $R(3,3) = 6$.

Proof: We already showed explicitly that we can bicolour K_5 so there isn't a red K_3 or a blue K_3. Thus, $R(3,3) > 5$.

Show via the pigeonhole principle that $R(3,3) \leq 6$. Key argument:

- Start with K_6 and single out one of the vertices.
- There are 5 edges to the other vertices and by the pigeonhole principle there must either be at least 3 red edges or 3 blue edges.

- Assume that at least 3 edges are red. If the adjacent vertices have **any** red edges between them we must have a red triangle; else **all** the edges between these vertices are blue, in which case we have a blue triangle.

- Hence, any two-coloured complete graph of 6 vertices must have either a blue or red triangle. Thus $R(3,3) \le 6$.

Combining results we get $R(3,3) = 6$.

27 Ramsey Numbers

Ramsey Numbers

Next we shall prove that $R(3,4) = 9$. After this it should be clear that calculating $R(a,b)$ is a very hard problem.

The general methods is as for $R(3,3)$.

1. First we establish a lower bound by explicitly finding a two-colouring of a K_n which has no red K_3 or blue K_4. For the $R(3,4)$ case this is K_8 showing that $R(3,4) > 8$.

2. Next we establish the upper bound $R(3,4) \le 9$.

   This entails proving the general results:

   (a) The general upper bound $R(a,b) \le R(a-1,b) + R(a,b-1)$, refined to

   (b) $R(a,b) \le R(a-1,b) + R(a,b-1) - 1$, when $R(a-1,b)$, $R(a,b-1)$ even.

   We shall also prove these general results.

3. The Ramsey number $R(a,b)$ is finite $\Rightarrow$ $R(a,b)$ is well-defined.

4. The general upper bound: $R(a,b) \le \binom{a+b-2}{a-1}$.

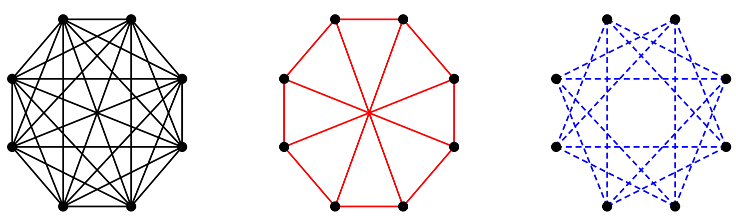
Lower Bound on $R(3,4)$

We show that we have the lower bound $R(3,4) > 8$ by presenting an explicit two-colouring of K_8 containing neither a red K_3 nor a blue K_4.

- K_8 has total number of edges equal to $\binom{8}{2} = 28$.

- Mark in the red edges (no K_3's allowed).

- Furthermore, the remaining edges don't permit any blue K_4.



K_8 $\qquad$ K_8 without red K_3 $\qquad$ K_8 without blue K_4

Handshaking Theorem – Graph Version

Theorem 67 (Handshaking Theorem)**.** *In any graph G the number of odd degree vertices is even.*

Proof: Let G be a graph with $|V(G)| = p$ and $|E(G)| = q$. Then

$$\sum_{v \in V(G)} \deg(v) = 2q,$$

since each edge is counted twice once for each incident vertex.

Let V_e denote the set of even degree vertices and V_o the set of odd degree vertices of G. Then

$$\sum_{v \in V(G)} \deg(v) = \sum_{v \in V_e} \deg(v) + \sum_{v \in V_o} \deg(v) = 2q,$$

so that

$$\sum_{v \in V_o} \deg(v) = 2q - \sum_{v \in V_e} \deg(v).$$

Every term on the RHS is even so the sum on the LHS is even. A sum of odd numbers is even if and only if it contains an even number of terms.

Upper Bound on Ramsey Numbers

Theorem 68 (Upper Bound)**.** *The Ramsey numbers satisfy the inequality*

$$R(a, b) \leq R(a-1, b) + R(a, b-1).$$

This can be sharpened to:

Theorem 69 (Upper Bound for $R(a-1, b)$ and $R(a, b-1)$ Even)**.** *The Ramsey numbers satisfy the inequality*

$$R(a, b) \leq R(a-1, b) + R(a, b-1) - 1$$

when $R(a-1, b)$ and $R(a, b-1)$ are even.

- The first bound implies that $R(3, 4) \leq R(2, 4) + R(3, 3) = 4 + 6 = 10$, which is then sharpened to $R(3, 4) \leq R(2, 4) + R(3, 3) - 1 = 9$.
- Combined with the lower bound $R(3, 4)$ is thus equal to 9.

Upper Bound – Proof

Proof: Argument similar (in structure) to proof of upper bound for $R(3, 3)$.

Form a graph with $R(a-1, b) + R(a, b-1)$ vertices.

Single out a particular vertex, say x, which is connected to the remaining $R(a-1, b) + R(a, b-1) - 1$ vertices by red and blue edges.

A version of the pigeonhole principle says that if we put $a_1 + a_2 - 1$ balls in two boxes, either box 1 contains at least a_1 balls or box 2 contains at least a_2 balls.

Therefore, there must be either $R(a-1, b)$ red edges or $R(a, b-1)$ blue edges.

Upper Bound – Proof

Say there are $R(a-1,b)$ red edges. They are incident to $R(a-1,b)$ vertices.

By definition of the Ramsey number, these vertices either have a red K_{a-1}, which together with the edges incident from x form K_a, or they have a blue K_b.

Similarly for the case when there are $R(a,b-1)$ blue edges.

Thus, any graph with $R(a-1,b)+R(a,b-1)$ vertices must either contain a red K_a or a blue K_b, and hence $R(a,b) \le R(a-1,b)+R(a,b-1)$.

Upper Bound – Proof – Even Case

If $R(a-1,b)$ and $R(a,b-1)$ are even, we can improve the bound to:

$$R(a,b) \le R(a-1,b)+R(a,b-1)-1.$$

Proof: Form a graph with $R(a-1,b)+R(a,b-1)-1$ vertices and single out a special vertex, x. There are now 2 cases to consider:

(a) At least $R(a-1,b)$ red edges or at least $R(a,b-1)$ blue edges.

(b) $R(a-1,b)-1$ red edges and $R(a,b-1)-1$ blue edges.

In case (a) we have subgraphs of the sought type as proved above.

For case (b) to be relevant **all** vertices must have the stated property $\Rightarrow$ all vertices have $R(a-1,b)-1$ red edges and $R(a,b-1)-1$ blue edges.

But this leads to a contradiction: The total number of red edges is

$$(R(a-1,b)+R(a,b-1)-1)(R(a-1,b)-1).$$

This is an odd number times an odd number.

This is **not** possible by the Handshaking Theorem.

Known Results

Small Ramsey Numbers, `http://www.combinatorics.org` under Surveys by Stanislaw P. Radziszowski. Values and bounds for $R(a,b)$.

a \ b	3	4	5	6	7	8	9	10	11	12
3	6	9	14	18	23	28	36	40 42	47 50	53 59
4		18	25	36 41	49 61	59 84	73 115	92 149	102 191	128 238
5			43 48	58 87	80 143	101 216	133 316	149 442	183 633	203 848
6				102 165	115 298	134 495	183 780	204 1171	256 1804	294 2566
7					205 540	217 1031	252 1713	292 2826	405 4553	417 6954
8						282 1870	329 3583	343 6090	10630	16944
9							565 6588	581 12677	22325	38832
10								798 23556	45881	81123

More Ramsey Theory

Theorem 70 ($R(a,b)$ is finite)**.** *The Ramsey number $R(a,b)$ is finite and $R(a,b)$ is a well-defined function.*

Proof: We showed that $R(a,b) \leq R(a-1,b) + R(a,b-1)$, valid for $a,b \geq 3$.

We also proved that $R(2,n) = R(n,2) = n$.

This guarantees that all Ramsey numbers are finite.

Apply inequality repeatedly to RHS:

$$\begin{aligned} R(a,b) &\leq R(a-1,b) + R(a,b-1) \\ &\leq R(a-2,b) + 2R(a-1,b-1) + R(a,b-2) \\ &\leq R(a-3,b) + 3R(a-2,b-1) + 3R(a-1,b-2) + R(a,b-3) \\ &\vdots \end{aligned}$$

Remind you of something?

The process stops once all terms are known.

Thus since a,b are finite we get a finite sum of integers.

Upper Bound: $R(a,b) \leq \binom{a+b-2}{a-1}$

Theorem 71 (Upper Bound)**.** *The Ramsey numbers*

$$R(a,b) \leq \binom{a+b-2}{a-1}$$

Proof: We will prove it by using induction on the value of $a+b$.

Base case: $a+b=4$, $R(2,2)=2$. RHS $= \binom{2+2-2}{2-1} = \binom{2}{1} = 2$, hence the result is true.

Suppose it is true for $a+b=p-1$. We need to prove that it is true for $a+b=p$:

$$\begin{aligned} \underbrace{R(a,b)}_{\substack{a+b=p \\ \text{case } p}} &\leq \underbrace{R(a-1,b)}_{\substack{a+b=p-1 \\ \text{case } p-1}} + \underbrace{R(a,b-1)}_{\substack{a+b=p-1 \\ \text{case } p-1}} \\ &\leq \binom{a+b-3}{a-2} + \binom{a+b-3}{a-1} = \binom{a+b-2}{a-1} \end{aligned}$$

Here we used that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Generalisations of Ramsey Problems

Example: Suppose in a group of 17 people, each pair are either friends, strangers or enemies. Show that there must always by either 3 mutual friends, 3 mutual strangers or 3 mutual enemies.

1. After singling out 1 person there are 16 persons left to put into 3 groups. By the PHP a group contains at least 6 people. Suppose this is group 1.

2. Group 1 are friends of person 1 so if there is a pair of mutual friends in group 1 this pair and person 1 form 3 mutual friends.

3. If there are no mutual friends in group 1 then they are either mutual strangers or enemies. Since $R(3,3) = 6$ we can conclude that there is at least 3 mutual strangers or 3 mutual enemies in group 1.

4. If there is less than 6 people in group 1 then either group 2 or group 3 has at least 6 people and similar arguments applies with 'friends' exchanged for 'strangers' or 'enemies' as appropriate.

Note: $R(3,3,3) = 17$ is the only non-trivial results for 3 colours. No results are known for more than 3 colours. So this ain't an easy problem.

28 Parity

Parity Arguments

Parity refers to the even/odd property of integers.

$$\begin{array}{ccc} \text{odd integer} & \longleftrightarrow & \text{odd parity} \\ \text{even integer} & \longleftrightarrow & \text{even parity} \end{array}$$

Notation 72 (Parity)**.** If $n \in \mathbb{Z}$, then parity(n) denotes the parity of n.

Like the pigeonhole principle it is an elementary idea and it can make apparently difficult problems simpler.

We already used a parity-type argument in a Ramsey Theory proof.

In the proof of the sharpened upper bound for Ramsey numbers we used that the product of two odd numbers is an odd number.

Parity arguments are not about counting but more about existence, proving whether a statement is true or not, demonstrating whether certain events can happen or not, etc..

Exercise

Example: On a table sits 5 drinking glasses all turned upside down. Turning over two glasses at a time can we make all glasses right way up? Turning over three glasses at a time can we make all glasses right way up?

Solution: Let $T = \#$ up glasses. When we flip two glasses, we could have

$$\begin{array}{cc} 2 \text{ up} \to 2 \text{ down}, & \delta T = -2; \\ 1 \text{ up, } 1 \text{ down} \to 1 \text{ down, } 1 \text{ up}, & \delta T = 0; \\ 2 \text{ down} \to 2 \text{ up}, & \delta T = 2. \end{array}$$

Starting with T even it must remain even.

Starting with $T = 0$ we can never reach $T = 5$.

Turning over 3 glasses at a time change T by $\pm 3, \pm 1$.

Answer is yes! Every move changes the parity of T.

Explicitly we have (glasses to be turned in boldface):

ddddd → u**uud**d → u**dd**u**d** → uuuuu

Example

Example: Let $(x, y, z) \in \mathbb{R}^3$ be a point with positive **integer** coordinates. Show that if we choose 9 such points then the midpoint of at least one pair of these points has integer coordinates.

Proof: Consider any two points (x_1, y_1, z_1) and (x_2, y_2, z_2) in $\mathbb{R}^3$ with integer coordinates. The midpoint of these is

$$((x_2 + x_1)/2, (y_2 + y_1)/2, (z_2 + z_1)/2).$$

The midpoint has integer coordinates if and only if x_1 and x_2 have the same parity, y_1 and y_2 have the same parity and z_1 and z_2 have the same parity.

(x, y, z) has 8 possible triples of parity (such as (even,odd,odd)).

By the PHP at least two of the nine points have the same triple of parities.

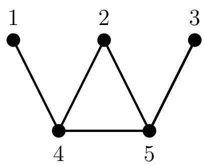
The midpoint of two such points has integer coordinates.

Handshaking Theorem

Theorem 73 (Handshaking Theorem)**.** *At a party the number of people who shake an odd number of hands is even.*

Example: Let there be 5 people indicate that any two have shaken hands by drawing an edge between them.

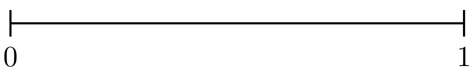
If $V = \{1, 2, 3, 4, 5\}$ and $E = \{\{1, 4\}, \{2, 4\}, \{2, 5\}, \{3, 5\}, \{4, 5\}\}$ then 1, 3, 4, 5 shook hands an odd number of times.



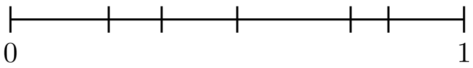
Parity and Subdivisions

Starting with the interval $[0, 1]$:

1. Subdivide into any finite number of subintervals

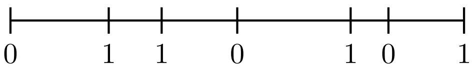


↓



Here five ticks gives us six intervals.

2. Label each new tick 0 or 1 (in any way):



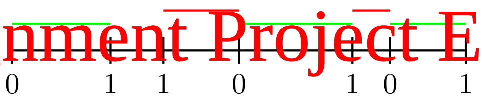
Parity and Subdivisions

Notation 74. $\#(a, b)$ denotes the number of intervals of type (a, b).

Note: There are no ticks between the labels a and b.

Question: What is the parity of $(\#(0, 1) + \#(1, 0))$?

- For our previous example we have:



- 3 (green) (0,1) intervals, 2 red (1,0) intervals. Note that green and red intervals alternate.

29 Sperner's Lemma for an Interval

Sperner's Lemma for an Interval

Lemma 75 (Sperner's Lemma for an Interval)**.** *The total number of* $(0, 1)$ *and* $(1, 0)$ *subintervals is odd.*

Proof: Suppose we have a given subdivision. Idea is to track the change in $(\#(0, 1) + \#(1, 0))$ as a single tick is added (an interval is divided). There are four types of intervals and two possible labels for the new tick:

$$\begin{array}{ll}
00 \to 000\ (+0) & 00 \to 010\ (+2) \\
01 \to 001\ (+0) & 01 \to 011\ (+0) \\
10 \to 100\ (+0) & 10 \to 110\ (+0) \\
11 \to 101\ (+2) & 11 \to 111\ (+0)
\end{array}$$

The number of (0,1) and (1,0) intervals always changes by an even number.

Given that the initial subdivision had exactly 1 such interval, any subdivision resulting from a sequence of insertions must also have an odd number of (0,1) and (1,0) intervals.

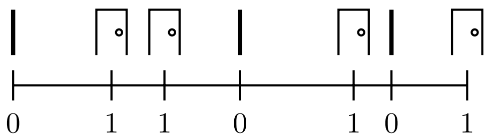
Sperner's Lemma for an Interval

Here is an alternative proof. It is more involved, but it will prepare us for the generalisation of Sperner's Lemma to two dimensions.

Alternative Proof: Idea: Map subdivisions to floor plans of 1D rooms.

Biject intervals to sequence of rooms and doors:

1. Interval $\longleftrightarrow$ Room
2. '1' tick $\longleftrightarrow$ Door
3. '0' tick $\longleftrightarrow$ Wall

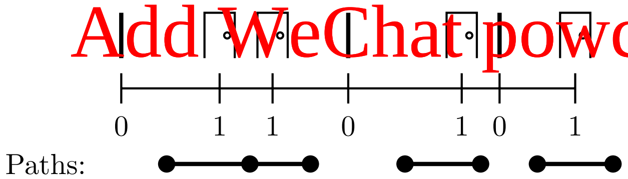


Note: Every room has *at most* two doors.

Sperner's Lemma for an Interval

Consider "room paths" defined such that:

1. Paths always start and end in one door rooms. The "outside" is considered a one-door room.
2. Paths traverses each door exactly once.



Sperner's Lemma for an Interval

There are two possible types of room path

1. Both ends are inside (an in-in path).
2. One end inside and the other end outside (in-out path).

We then have that

$$\#\,\text{rooms with one door} = 2(\#\,\text{in-in paths}) + (\#\,\text{in-out paths})$$

Clearly there is only one in-out path so the parity above is odd.

But $\#$ rooms with one door $= \#$ different labelled intervals

So the total number of $(0,1)$ and $(1,0)$ subintervals is odd.

30 Intermediate Value Theorem

Sperner's Lemma and Intermediate Value Theorem

We shall now make one of our few excursions into the continuum and relate Sperner's lemma to the intermediate value theorem for continuous functions.

Theorem 76 (Intermediate Value Theorem)**.** *Let $f : \mathbb{R} \mapsto \mathbb{R}$ be a continuous function, $a, b \in \mathbb{R}$, $a < b$ with $f(a) < f(b)$. For any $y \in \mathbb{R}$ with $f(a) < y < f(b)$ there exists $x \in (a, b)$ such that $f(x) = y$.*

The relation is easier to see if we look to the equivalent statement:

Theorem 77. *Let $f : [0, 1] \mapsto [-1, 1]$ be continuous and suppose that $f(0) < 0$, $f(1) > 0$.*

Then there exists $x \in (0, 1)$ such that $f(x) = 0$.

We show how Sperner's lemma for the interval implies the second theorem.

Intermediate Value Theorem – Proof

Proof: Let $f : [0, 1] \mapsto [-1, 1]$ be continuous with $f(0) < 0$, $f(1) > 0$.

Assume there is no $x \in (0, 1)$ such that $f(x) = 0$.

Divide the interval $[0, 1]$ at equidistant points and label the tick at position a in the subdivision by zero if $f(a) < 0$ and by 1 if $f(a) > 0$.

Sperner's lemma guarantees a $(0, 1)$ subinterval. Repeat this procedure on the $(0, 1)$ subinterval and so on.

Define two sequences $\{a_n\}$ and $\{b_n\}$ such that a_n is the position of the '0' tick and b_n the position of the '1' tick after n subdivisions.

We now appeal to the Bolzano-Weierstrass theorem to show that both $\{a_n\}$ and $\{b_n\}$ must contain convergent subsequences $\{a_{n_k}\}$ and $\{b_{n_k}\}$.

Since $|a_n - b_n| \leq 1/2^n$ these subsequences must have a common limit x.

By the continuity of f:

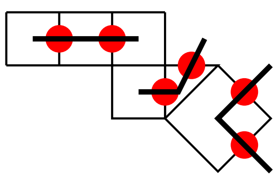
$$0 \geq \lim_{k \to \infty} f(a_{n_k}) = f(\lim_{k \to \infty} a_{n_k}) = f(x)$$
$$0 \leq \lim_{k \to \infty} f(b_{n_k}) = f(\lim_{k \to \infty} b_{n_k}) = f(x)$$

Note: Labels merge at x so can view x as labelled both 0 and 1.

Parity in two-dimensional floor plans

Setup: Two dimensional floor plans where each room has at most 2 doors. Why a max of 2 doors? Paths must enter via one door and exit (if possible) via another *unique* door.

Example: Indicate doors by a red circle:



Draw all possible paths on the floor plan above. Three kinds of paths:

1. Completely inside: Path joins 2 rooms with a single door at either end.
2. Inside to outside: Path from room with a single door exit via outside door.
3. Outside to outside: Path entering and exiting via outside doors.

Parity in two-dimensional floor plans

Theorem 78 (Floor Plan Lemma)**.** *# (rooms with one door) has the same parity as # (outside doors).*

Proof: Consider all possible paths.Three natural ways to categorize these:

1. Completely inside (one door room to one door room). Count p_{11}.
2. Inside to outside (one door room to outside). Count p_{10}.
3. Outside to outside. Count p_{00}.

The number of rooms with one door and the number of outside doors is:

$$\# \text{ of rooms with one door} = 2p_{11} + p_{10}$$
$$\# \text{ outside doors} = 2p_{00} + p_{10}$$

Numbers are expressed as (even number) + p_{10} and hence have same parity.

31 Sperner's Lemma

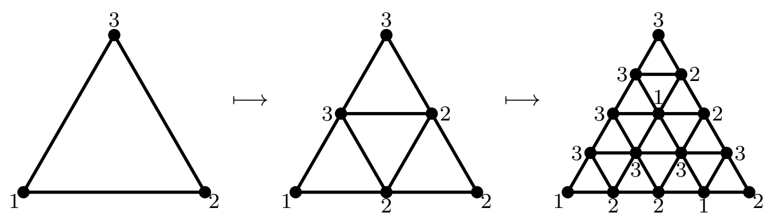
Sperner's Lemma – Setup

Suppose we are given a triangle whose main vertices are labelled 1, 2, and 3.

This triangle is then triangulated (subdivided into triangles) such that each vertex is labelled 1, 2, and 3 with the restrictions that:

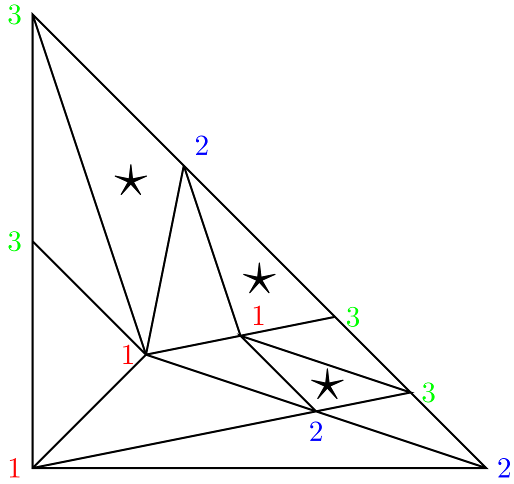
Definition 79 (Sperner Labelling)**.**

1. Vertices on the edge (a,b) of the large triangle are labelled a or b.
2. Interior vertices may be labelled arbitrarily



Sperner's Labelling – Example

Example:



Sperner's Lemma

Theorem 80 (Sperner's Lemma)**.** *Any Sperner labelled triangulation (of a triangle) contains an odd number of triangles possessing all the labels (1,2,3).*

Proof: Basic idea: *Bijection* between Sperner triangulations and floor plans.

Use FP lemma and Sperner's lemma for an interval to prove parity statement.

Map of triangulations to floor plans:

1. Triangles are rooms.
2. Edges labelled (1,2) have a door. All other edges are walls.

The only possible (1,2) triangles are: ${}_1\Delta_2^3$ ${}_1\Delta_2^2$ ${}_1\Delta_2^1$

$\Rightarrow$ all rooms have at most 2 doors and only (1,2,3)-triangles have one door.

Sperner's Lemma – Proof

Floor plan lemma $\Rightarrow$ parity of outside doors is the same as the parity of rooms with a single door.

All single doors must lie on the (1,2) edge: subdivision lemma $\Rightarrow$ there must be an odd number of (1,2) and (2,1) intervals.

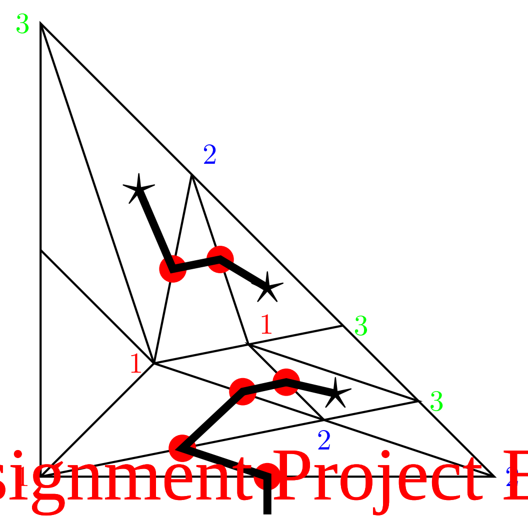
Number of outside doors is odd $\Rightarrow$ number of rooms with a single door is odd.

Thus the number of triangles labelled (1,2,3) must be odd, as required.

Aside: This argument can be generalized to higher dimensions, where one labels faces of simplices (tetrahedra, and generalizations). Note that we required that the theorem was true in one dimension, in order to prove the theorem in two dimensions. Can prove for all dimensions via induction.

Sperner's Lemma – Illustration

Doors marked by red circles:



32 Brouwer fixed point theorem

Brouwer Fixed Point Theorem in 1D

Theorem 81 (Brouwer Fixed Point Theorem in 1D). $f : [0, 1] \mapsto [0, 1]$ *continuous. Then f has a fixed point $x^* \in [0, 1]$, i.e., $f(x^*) = x^*$.*

Proof: Let $f : [0, 1] \mapsto [0, 1]$ continuous.

Define $g(x) = x - f(x)$.

From the intermediate value theorem we have that:

$g : [0, 1] \mapsto [-1, 1]$ continuous with $g(0) = -f(0) \leq 0$ and $g(1) = 1-f(1) \geq 0$

$$\Rightarrow \quad \exists\, x_0 \in [0, 1] \text{ for which } g(x_0) = 0 \quad \Rightarrow \quad f(x_0) = x_0.$$

Brouwer Fixed Point Theorem in 1D – Proof

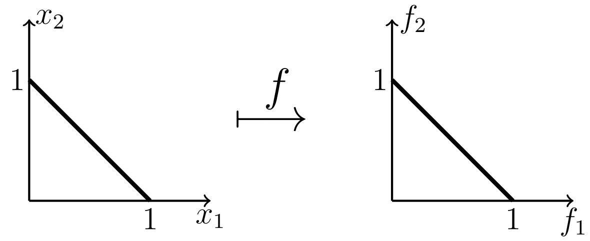
As a warm-up to the 2D case we give a proof for 1D using Sperner's Lemma in a different setting to the proof for the intermediate value theorem.

We shall embed a 1D interval in 2D and consider

$$I = \{(x_1, x_2) \in \mathbb{R}^2 \,|\, x_1 + x_2 = 1,\ x_1, x_2 \geq 0\}.$$

Let $f : I \mapsto I$ be a continuous function and let $\boldsymbol{x} = (x_1, x_2)$. Then

$$f(I) = \{(f_1, f_2) \in \mathbb{R}^2 \,|\, f_1(\boldsymbol{x}) + f_2(\boldsymbol{x}) = 1,\ f_1(\boldsymbol{x}),\ f_2(\boldsymbol{x}) \geq 0\}.$$



Brouwer Fixed Point Theorem in 1D – Proof

Now divide I into smaller segments by placing ticks (or vertices) along I.

Look at such a vertex at say $\boldsymbol{a} = (a_1, a_2) \in I$, then we can label this vertex '1' if $f_1(\boldsymbol{a}) \leq a_1$ and '2' if $f_2(\boldsymbol{a}) \leq a_2$.

Note that the restrictions $a_1 + a_2 = 1$ and $f_1(\boldsymbol{a}) + f_2(\boldsymbol{a}) = 1$ with all numbers positive guarantees that one or the other inequality from above must hold.

The vertex $(1, 0)$ can be labelled '1' since we can't have $f_2(1, 0) < 0$ and $(0, 1)$ can be labelled '2' since we can't have $f_1(0, 1) < 0$.

This then gives us a Sperner labelling of I and we can proceed along the lines of the proof of the intermediate value theorem to argue that there must exist a convergent sequence to $\boldsymbol{x}^*$ such that $f(\boldsymbol{x}^*) = \boldsymbol{x}^*$ (the point $\boldsymbol{x}^*$ is labelled both 1 and 2).

We naturally must ensure that the length of the sub-intervals vanish as the number of sub-divisions goes to ∞.

Brouwer Fixed Point Theorem

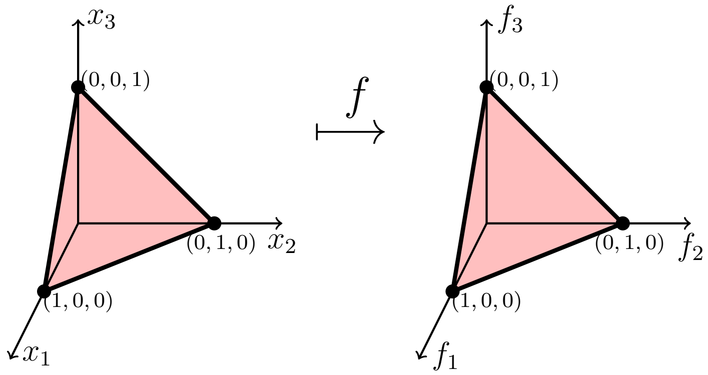
Theorem 82 (Brouwer Fixed Point Theorem for Triangles)**.** *Let Δ denote a triangle in the plane. Every continuous function $f : \Delta \mapsto \Delta$ has a fixed point in Δ.*

- Proved here in the case of a triangle, but this can be generalised to the unit disc or any other two-dimensional region (without a hole).
- Generalises the fact that every continuous mapping from the unit interval to the unit interval has a fixed point.
- Can be straightforwardly generalised to arbitrary dimension by using Sperner's lemma for simplices in arbitrary dimension.
- Important, fundamental result in topology.

Brouwer Fixed Point Theorem – Proof

Proof: Choose a triangular region, Δ, in three dimensional space, with vertices (1,0,0), (0,1,0), and (0,0,1), corresponding to a region in the plane defined by the equation $x_1 + x_2 + x_3 = 1$. This has the (slight) notational advantage that the vertices have extremal values of the coordinate directions.

Consider a continuous function f which maps this triangular region onto itself.



Brouwer Fixed Point Theorem – Proof

Let S_j be a sequence of triangulations of the triangle Δ, such that S_j is obtained from S_{j-1} via further subdivisions, i.e., the vertices in S_{j-1} form a proper subset of the vertices in S_j.

We impose the condition that all triangles in S_j approach size 0 as $j \to \infty$. In particular, we define $d(S_j)$ to be the maximum edge length in S_j and impose the condition $\lim_{j\to\infty} d(S_j) = 0$.

Assign labels to vertices in S_j as a value of i such that $f_i(\boldsymbol{x}) \le x_i$.

There is always such an i since $\sum_i x_i = \sum_i f_i(\boldsymbol{x}) = 1$.

Vertex (1,0,0) can be labelled 1 since we can't have $f_2(\boldsymbol{x}) < 0$ or $f_3(\boldsymbol{x}) < 0$.

Similarly the vertex (0,1,0) can be labelled 2 and (0,0,1) can be labelled 3.

Brouwer Fixed Point Theorem – Proof

Vertices on the edge between (1,0,0) and (0,1,0) can be labelled 1 or 2, vertices between (0,1,0) and (0,0,1) by 2 or 3, and vertices between (1,0,0) and (0,0,1) by 1 or 3. Interior vertices may have labels 1, 2 or 3.

Thus each triangulation S_j satisfies the conditions of Sperner's lemma; hence we are guaranteed that for each S_j there will be at least one triangle with vertices labelled 1, 2, and 3.

The vertices of these triangles labelled 1, 2, and 3 form an infinite sequence. Due to the compactness of Δ, we are guaranteed that there must be a subsequence of triangles whose vertices converge to a point $\boldsymbol{x}^* \in \Delta$ (in practice, we can consider this subsequence as arising from finer and finer subdivisions around $\boldsymbol{x}^*$).

The point $\boldsymbol{x}^*$ has all three labels. f is continuous so for $\boldsymbol{x}^{(j)} \in S_j$,

$$\lim_{j\to\infty} f(\boldsymbol{x}^{(j)}) = f(\lim_{j\to\infty} \boldsymbol{x}^{(j)}) = f(\boldsymbol{x}^*).$$

But if $\boldsymbol{x}^*$ has all three labels $f(\boldsymbol{x}^*) = \boldsymbol{x}^*$, which establishes the result.

A point of detail

- In 1-D, we always have a Sperner labelling for each subdivision - this gives our nesting.
- Compare to 2-D: A subtriangle is of the form ${}_1\triangle_3^2$. We can't be sure that this is a Sperner labelling - e.g. only 1, 3's along the bottom.
- To get around this, we subdivide by a half, say, at each step.
- According to Sperner's lemma in 2-D, there is at least one subtriangle $(1, 2, 3)$ for each such subdivision.
- We record the coordinates of one from each sequence member.
- Appeal to the Boltzano-Weierstrass theorem from real analysis guarantees a convergent sub-sequence that converges to a point, that furthermore involves nested subtriangles.

33 Lattice Paths

Lattice Paths

We shall confine ourselves to 2 dimensions and (largely) to paths on the integer grid $\mathbb{N}_0^2$ also known as the first quadrant of the square lattice. Most definitions can easily be generalised to higher dimensions and other lattices.

Definition 83 (Lattice Path)**.** A **lattice path** of length n is a sequence $v_0 v_1 \cdots v_n$ of vertices $v_i = (x_i, y_i) \in \mathbb{N}_0^2$ where $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, subject to the conditions:

1. $v_0 = (0, 0)$.
2. Steps, $s_i = v_i - v_{i-i} \in S$, where S is some step set.

Example: Binomial paths are lattice paths with $S = \{(0, 1), (1, 0)\}$.

The step set S is just: $(1, 0) \leftrightarrow$ East step and $(0, 1) \leftrightarrow$ North step.

Then a path, say, $ENEN \leftrightarrow \underbrace{(0,0)(1,0)}_{s_1=(1,0)}(1,1)\underbrace{(2,1)(2,2)}_{s_4=(0,1)}$.

Note: Vertex notation is good for definitions but otherwise cumbersome.

34 Ballot Paths

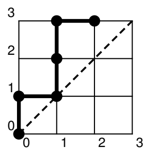
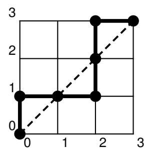
Ballot Paths

Definition 84 (Ballot Paths)**.** **Ballot paths** are lattice paths with the additional constraint:

3. If $v_i = (x_i, y_i)$ is a vertex in the paths then $x_i \leq y_i$ for all $i = 1, 2, \ldots, n$.

If $v_n = (m, m+h)$ denote set of all such ballot paths by B_m^h.

Note: All vertices in a ballot path lie on or above the line $y = x$.
Example: $b = NENNE \in B_2^1$, but $b' = NEENNE$ is not a ballot path:

Note: In a binomial ballot path $b = s_1 s_2 \ldots s_n$ with $s_j \in \{N, E\}$ in any subword $b' = s_1 s_2 \ldots s_k$ we have $|\,b'\,|_N \geq |\,b'\,|_E$, i.e., at any stage of the path the number of north steps cannot be less than the number of east steps.

General Lattice Paths

We shall generally only consider binomial ballot paths (ballot paths for short).

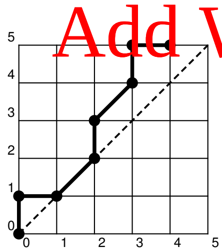
However, many interesting problems involve more involved step sets.

The only restriction on a step set is that any step must connect vertices in $\mathbb{N}_0^2$ and very often the path can only visit a vertex once (self-avoiding paths).

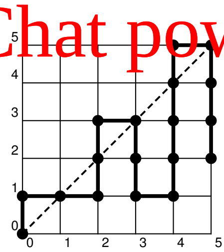
Example:

1. $S_1 = \{(0,1), (1,0), (1,1)\}$. Words in alphabet: $\{N, E, D\}$.

2. $S_2 = \{(0,1), (1,0), (0,-1)\}$. Words in alphabet: $\{N, E, S\}$.



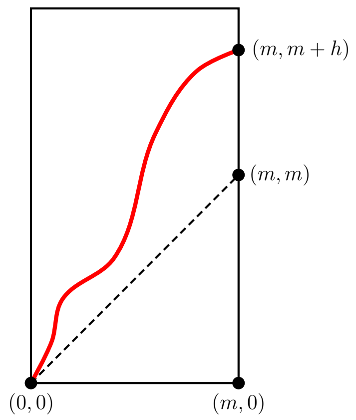
$w_1 = NEDNDNE$ (ballot path)



$w_2 = NEENNESSENNNNESSS$

Back to Ballot Paths

Geometrically we have:



B_m^h

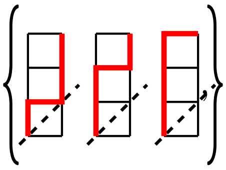
1. h = height above $y = x$.
2. $m + h$ = y-coor of last vertex.

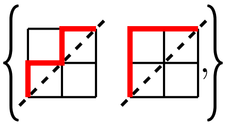
1. m = # east steps.
2. m = x-coor of last vertex.

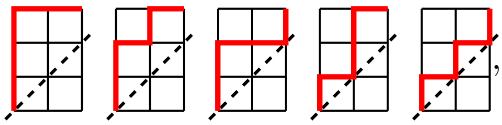
Number of Ballot Paths

How many ballot paths are there?

Example:

$B_1^2 = \{$  $\}$ $\quad \left| B_1^2 \right| = 3$

$B_2^0 = \{$  $\}$ $\quad \left| B_2^0 \right| = 2$

$B_2^1 = \{$  $\}$ $\quad \left| B_2^1 \right| = 5$

Ballot Number Recurrence

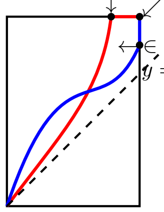
Theorem 85 (Ballot Number Recurrence)**.** *The number of ballot paths satisfy the recurrence*

$$\left| B_m^h \right| = \left| B_m^{h-1} \right| + \left| B_{m-1}^{h+1} \right|, \qquad h \geq 0$$

with $\left| B_m^h \right| = 0$ *for* $h < 0$ *and* $\left| B_0^h \right| = 1$.

Proof: Every $b \in B_m^h$ can be uniquely obtained by adding one (north) step to a $b' \in B_m^{h-1}$ $(h > 0)$ or one (east) step to a $b'' \in B_{m-1}^{h+1}$.

Note: This is a bijective proof. A $b \in B_m^h$ is mapped to a unique $b' \in B_m^{h-1} \cup B_{m-1}^{h+1}$. The map deletes the last step of b.



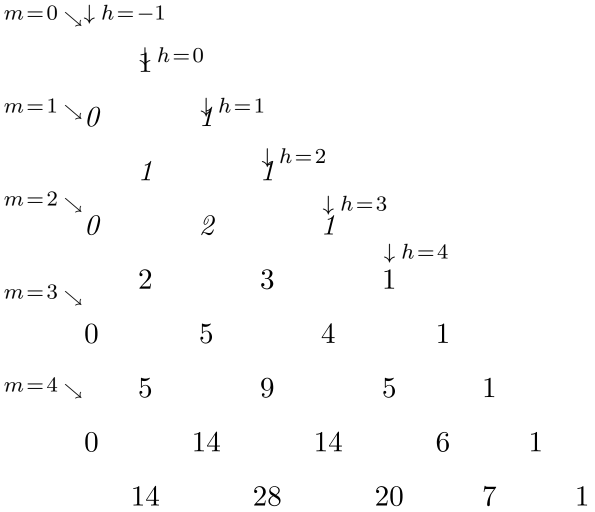
Ballot Triangle

Theorem gives the ballot triangle:

$$\begin{array}{ccc} \left| B_m^{h-1} \right| & + & \left| B_{m-1}^{h+1} \right| \\ \searrow & & \swarrow \\ & \left| B_m^h \right| & \end{array}$$

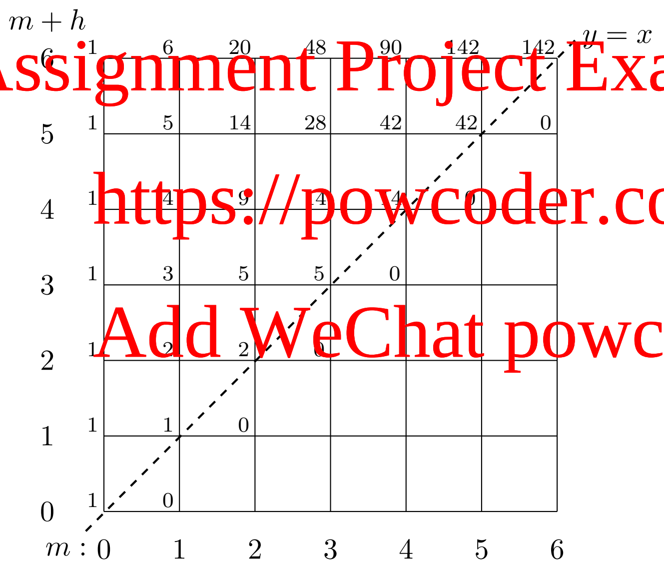
$$\left| B_m^h \right| = 0,\ h < 0$$

$$\left| B_0^h \right| = 1$$



Ballot Grid

Can also write counts on the $m \times (m+h)$ grid (above $y = x$):

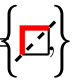
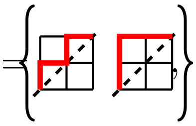


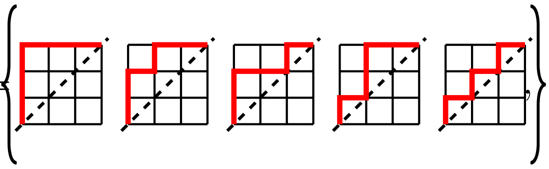
Dyck Paths and Catalan Numbers

Definition 86 (Dyck Paths)**.** Ballot paths with $h = 0$ are called **Dyck paths**. The numbers $\left| B_m^0 \right|$ are called **Catalan numbers**, denoted C_m.

Note: The number of steps n in a Dyck path is $n = 2m$.

Example:

$B_1^0 =$  $\left| B_1^0 \right| = 1$ $\quad B_2^0 =$  $\left| B_2^0 \right| = 2$

$B_3^0 =$  $\left| B_3^0 \right| = 5$

Number of Ballot Paths

Theorem 87 (Number of Ballot Paths)**.** *The number of ballot paths is*

$$\left| B_m^h \right| = \frac{h+1}{m+h+1}\binom{2m+h}{m+h}.$$

Proof (Algebraic): From the ballot number recurrence we have:

$$\left| B_m^h \right| = \left| B_m^{h-1} \right| + \left| B_{m-1}^{h+1} \right|, \quad h \geq 0$$

with $\left| B_m^h \right| = 0$ for $h < 0$ and $\left| B_0^h \right| = 1$.

First we just check the special cases:

$$\left| B_0^h \right| = \frac{h+1}{h+1}\binom{h}{h} = 1 \quad \text{and} \quad \left| B_m^{-1} \right| = \frac{0}{m}\binom{2m-1}{m-1} = 0.$$

Number of Ballot Paths – Proof

$$\begin{aligned}
\text{RHS} &= \left| B_m^{h-1} \right| + \left| B_{m-1}^{h+1} \right| \\
&= \frac{h}{m+h}\binom{2m+h-1}{m+h-1} + \frac{h+2}{m+h+1}\binom{2m+h-1}{m+h} \\
&= \frac{h\,(2m+h-1)!}{(m+h)\,(m+h-1)!\,m!} + \frac{(h+2)\,(2m+h-1)!}{(m+h+1)\,(m+h)!\,(m-1)!} \\
&= \frac{(2m+h-1)!}{(m+h)!\,m!}\left[h + \frac{m(h+2)}{(m+h+1)}\right] \\
&= \frac{(2m+h-1)!}{(m+h)!\,m!} \times \frac{(2m+h)(h+1)}{m+h+1} \\
&= \binom{2m+h}{m+h}\frac{h+1}{m+h+1} \quad = \quad \text{LHS.}
\end{aligned}$$

Number of Dyck Paths

Corollary 88 (Number of Dyck Paths)**.** *The number of Dyck paths is*

$$\left|B_m^0\right| = C_m = \frac{1}{m+1}\binom{2m}{m} = \frac{(2m)!}{m!\,(m+1)!}.$$

Note: Dyck paths is just one of more than a hundred known combinatorial problems which are counted by the Catalan numbers. A few others are

- Binary trees.
- Triangulations of polygons with n vertices.
- Perfectly balanced parenthesis.
- Non-crossing arcs on $2n$ nodes.
- etc. etc.

We shall explore some of these in week seven.

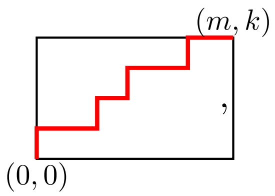
35 Lattice Paths

Ballot Numbers – Bijective Proof

Bijective Proof: We shall prove the formula for ballot numbers using a bijection and inclusion-exclusion.

The starting point is that it is easy to count *unconstrained* binomial paths.

$$B_{m,k} = \left\{ \quad , \right\} \qquad |B_{m,k}| = \binom{k+m}{m}$$



Not so easy if some constraint is imposed:

Ballot paths $\rightsquigarrow$ binomial paths with no vertex below $y = x$.

Ballot Numbers – Bijective Proof

Consider the binomial paths $B_{m,m+h}$. Partition $B_{m,m+h}$ into two disjoint subsets:

- G = binomial paths with **no** vertices below $y = x$, i.e., ballot paths.
- H = binomial paths with **at least one** vertex below $y = x$.

Then

$$|\, B_{m,m+h} \,| = |\, G \,| + |\, H \,|\,.$$

So

$$\begin{aligned} \left| B_m^h \right| &= |\, G \,| = |\, B_{m,m+h} \backslash H \,| \\ &= |\, B_{m,m+h} \,| - |\, H \,| \\ &= \binom{2m+h}{m+h} - |\, H \,|\,. \end{aligned}$$

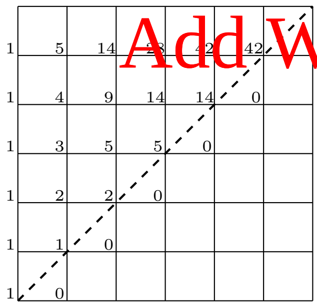
Ballot Numbers – Bijective Proof

How does this help?

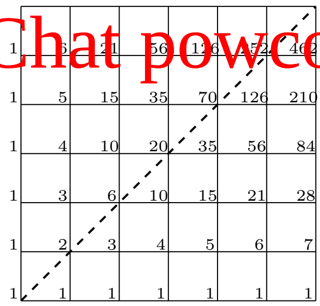
H is another constrained binomial path problem, so still not easy!

Idea: Biject the constrained problem H to an unconstrained binomial path problem so that $|\, H \,|$ = some binomial coefficient.

To see why and how this might work look at binomial and ballot grid counts:

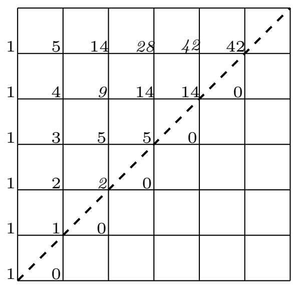


Ballot Numbers

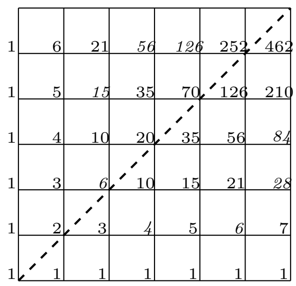


Binomial Numbers

Ballot Numbers – Bijective Proof



Ballot Numbers



Binomial Numbers

Now something amazing happens!

Every entry in position (i, j) in the ballot grid equals the entry at position (i, j) in the binomial grid minus another entry in the binomial grid. But which entry?

Pos (2,2) $\rightsquigarrow$ $2 = 6-4$ $\rightsquigarrow$ Pos (2,2) – Pos (3,1) Pos (2,4) $\rightsquigarrow$ $9 = 15-6$ $\rightsquigarrow$ Pos (2,4) – Pos (5,1) Pos (3,5) $\rightsquigarrow$ $28 = 56-28$ $\rightsquigarrow$ Pos (3,5) – Pos (6,2) Pos (4,5) $\rightsquigarrow$ $42 = 126-84$ $\rightsquigarrow$ Pos (4,5) – Pos (6,3)

Ballot Numbers – Bijective Proof

Now something amazing happens!

Every entry in position (i, j) in the ballot grid equals the entry at position (i, j) in the binomial grid minus another entry in the binomial grid. But which entry?

- Pos (2,2) $\rightsquigarrow$ $2 = 6-4$ $\rightsquigarrow$ Pos (2,2) – Pos (3,1)
- Pos (2,4) $\rightsquigarrow$ $9 = 15-6$ $\rightsquigarrow$ Pos (2,4) – Pos (5,1)
- Pos (3,5) $\rightsquigarrow$ $28 = 56-28$ $\rightsquigarrow$ Pos (3,5) – Pos (6,2)
- Pos (4,5) $\rightsquigarrow$ $42 = 126-84$ $\rightsquigarrow$ Pos (4,5) – Pos (6,3)

Notice: Sums of coordinates of the two entries are equal!

On closer inspection we see that we have: Pos (i, j) – Pos $(j+1, i-1)$

This corresponds to the position of the second entry being obtained from the first entry by **reflection in the line:** $y = x - 1$.

Ballot Numbers – Bijective Proof

In ballot 'notation' we have $i = m$ and $j = m + h$ so $i + j = 2m + h$ and we get if our observation is true:

$$\begin{aligned}
\left|B_m^h\right| &= \binom{i+j}{j} - \binom{i+j}{j+1} \\
&= \binom{2m+h}{m+h} - \binom{2m+h}{m+h+1} \\
&= \frac{(2m+h)!}{m!(m+h)!} - \frac{(2m+h)!}{(m-1)!(m+h+1)!} \\
&= \binom{2m+h}{m+h}\left(1 - \frac{m}{m+h+1}\right) \\
&= \frac{h+1}{m+h+1}\binom{2m+h}{m+h}.
\end{aligned}$$

So that is fine.

Ballot Numbers – Bijective Proof

Task: To complete bijective proof we must now 'find' the bijection between the set H and the set $B_{m+h+1,m-1}$.

Find a bijection between:

1. Binomial paths ending at $(m, m+h)$ with at least one vertex below $y = x$.
2. Binomial paths ending at $(m+h+1, m-1)$.

The hint was **reflection in the line** $y = x - 1$.

Bijection: $T : H \mapsto B_{m+h+1,m-1}$, where $b' = T(b) \in B_{m+h+1,m-1}$ is the path obtained from $b \in H$ by "reflecting" all steps after the **last** vertex on $y = x - 1$.

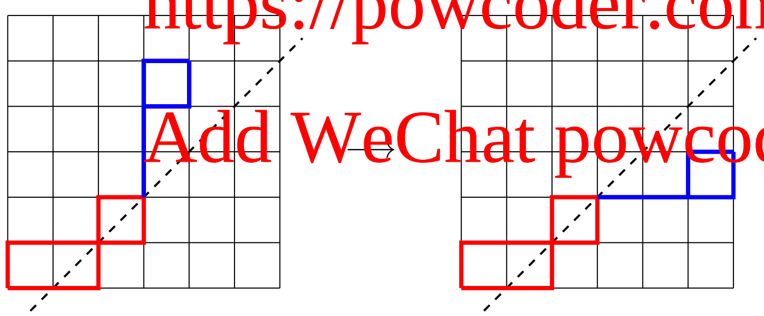
Note: Such a vertex **must** exist as every path in B has a vertex below $y = x$.

By "reflecting" the steps we mean that every north step after the "last" vertex becomes an east step and east steps become north steps.

I think we need to look at some examples.

Ballot Numbers – Bijective Proof

Example:



Ballot Numbers – Bijective Proof

Say "last" vertex occurs at $(i, i-1)$. Path continues to position $(m, m+h)$.

The "reflection" then takes

- Remaining $m-i$ East steps $\rightsquigarrow$ $m-i$ North steps.
- Remaining $m+h-i+1$ North steps $\rightsquigarrow$ $m+h-i+1$ East steps.

So the reflected path $b' = T(b)$ goes from $(i, i-1)$ to $(m+h+1, m-1)$, i.e.,

$$b' \in B_{m+h+1,m-1}.$$

Note: Every $b' \in B_{m+h+1,m-1}$ **must** cross $y = x - 1$ and so have at least one vertex on $y = x - 1$, i.e., b' is the image of some path in H.

This establishes the sought after bijection.

36 Generating Functions

Generating Functions – Definition

Generating functions are a way to encode information about sequences in an intuitive and powerful way.

Notation 89 (Sequences)**.** We denote sequences as $\{a_n\}$ or $a_0, a_1, a_2, \cdots$ where $n \in \mathbb{N}_0$.

Definition 90 (Generating Function)**.** The **generating function** $f(x)$ for a sequence $\{a_n\}$ is

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

Example: Given a sequence, say, $\{a_j\} = 1, 2, 3, 4, \cdots$ we could encode this information as a function

$$\begin{aligned} f(x) &= 1 + 2x + 3x^2 + 4x^3 + \cdots = \frac{\mathrm{d}}{\mathrm{d}x}(1 + x + x^2 + x^3 + \cdots) \\ &= \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2} \end{aligned}$$

Generating Functions

Notation 91 (Taylor Coefficient)**.** Let $f(x)$ be an analytic function. The coefficient a_n of x^n in the Taylor series of $f(x)$ about 0 is denoted $a_n = [x^n]\, f(x)$.

Thus if A_n is a set of objects of size n rather than calculating $a_n = |\,A_n\,|$ directly we could form the associated generating function $f(x)$ and obtain a_n from the Taylor expansion (provided it exists of course).

At first glance this does not seem to help does it? Why should it be better ('easier') to find $f(x)$ rather than $|\,A_n\,|$. Well I hope the next few weeks will convince you that often it is 'easier' to find the generating function $f(x)$.

Secondly if we have a generating function $f(x)$ we gain access to very powerful methods from real and complex analysis which we can use to study the function (and hence the problem). In particular we can use methods for analyzing the asymptotic behaviour of $|\,A_n\,|$.

Note: The generating function representation is *completely* equivalent to the original representation.

Generating Functions – Examples

Example: Binary numbers: $B_n = \{(b_1, b_2, \ldots, b_n)\,|\,b_j \in \{0,1\}\} \Rightarrow |\,B_n\,| = 2^n$.

The generating function is

$$f(x) = 1 + 2x + 4x^2 + 8x^3 + \cdots = \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (2x)^n = \frac{1}{1-2x}.$$

Example: Fibonacci numbers: ($F_n = F_{n-1} + F_{n-2}, F_1 = F_2 = 1$) have the generating function

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}.$$

We shall prove this next lecture.

Example: Number of Dyck paths of length $2n$ is $d_n = \frac{1}{n+1}\binom{2n}{n}$.
The generating function is

$$D(x) = \sum_{n=0}^{\infty} d_n x^n = \frac{1}{2x}\left(1 - \sqrt{1-4x}\right).$$

We shall prove this later on.

Multivariable Generating Functions

Natural generalisation is to have functions of more than one variable.

Example: Consider Dyck paths. It is natural to enumerate (count) these by the number of steps n and the number of times k the path touches the line $y = x$. Then

$$D(u, z) = \sum_{n,k} d_{n,k} u^k z^n,$$

where $d_{n,k}$ is the number of Dyck paths of length n with k returns to $y = x$.

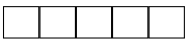
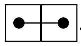
Physically we can view the path as a polymer (chain molecule) and $y = x$ as a surface. Then u represents an interaction energy between the monomers and the surface. This is a simple physical model for the attachment (adsorption) or detachment (desorption) of polymers that interact with a surface.

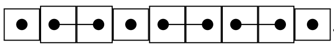
37 Binomial Expansion

Paving or Tiling

Definition 92 (Paving or Tiling)**.** An n**-board** is a line of n squares or cells. A **paving** or **tiling** is a covering of an n-board with a set of **pavers** or **tiles** such as:

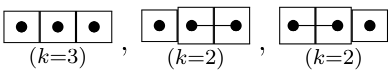
A **monomer** is a single square while a **dimer** is a pair of adjacent squares.

Notation: A 5-board  a monomer  and a dimer .

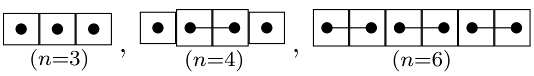
A paving of a 9-board: .

Questions:

1. How many pavings are there of an n-board (variable number of pavers)?

$n = 3$: 

2. How many pavings with k pavers (variable length boards)?

$k = 3$: 

Pavings and the Binomial Expansion

How to efficiently count the number of pavings? Use generating functions!

We have already seen the basic idea when proving the binomial theorem.

In expanding $(x+y)^n$ we had to choose a term x OR y from each factor.

Now think of the pavers as the variables. We fill the board from left to right by filling the next empty cell with a monomer OR a dimer (which takes up 2 cells).

Hence putting down k pavers gives us a term: $f_k(x) = (x+x^2)^k$.

This answers question 2.

The total number of pavings is $f_k(1) = 2^k$. But that is obvious!.

More interestingly the number of pavings of length $n \in [k, 2k]$ is the coefficient of x^n in the generating function $f_k(x)$, i.e., $[x^n]\, f_k(x) = \binom{k}{n-k}$.

Pavings and Generating Functions

What about question 1? Answer is not $(x+x^2)^n$.

Rather we look to the generation function formed by putting down any possible number of pavers:

$$F(x) = \sum_{k=0}^{\infty} (x+x^2)^k = \frac{1}{1-(x+x^2)} = \frac{1}{1-x-x^2}. \qquad \text{(Geometric series)}$$

The number a pavings of length n is: $[x^n]F(x)$.

What if we want to track the number of monomers or dimers? Easy!

Just add a factor y for a monomer so a k paving is $(xy+x^2)^k$ and hence:

$$F(x,y) = \sum_{k=0}^{\infty} (xy+x^2)^k = \frac{1}{1-(xy+x^2)} = \frac{1}{1-xy-x^2}.$$

In the expansion of this generating function the coefficient of $x^n y^m$ is the number of pavings of length n using m monomers!!

This is a hint that generating functions are objects of great beauty and power!

Algebra and Generating Functions

This example tells us something important about the relationship between algebra and the combinatorics of generating functions.

- **Algebra:**
  - **Multiplication** $\longleftrightarrow$ **Concatenation** of 'base' objects
  - **Addition** $\longleftrightarrow$ **'OR'**

    Where 'OR' means: **Choose** a 'replacement' for base object.

- **Paving:**
  - Base object $\longrightarrow \square$
  - $(x+x^2): \square \longrightarrow \underbrace{\boxed{\bullet} \;\text{OR}\; \boxed{\bullet \mid \bullet}}_{\text{pavers}}$

Binomial Expansion

Example: Consider a box with two balls, say red and purple. What are all the possible selections of balls we can take from the box?

$$f(r,p) = (1+r)(1+p) = 1 + r + p + rp$$

What if we don't care about the colour of the balls? Then we must change the labels (variables) $r \equiv$ red ball and $p \equiv$ purple ball to $b \equiv$ ball. We then obtain

$$g(b) = f(b,b) = (1+b)(1+b) = 1 + 2b + b^2.$$

So there is one way of choosing no balls, 2 ways of choosing 1 balls, and one way of choosing 2 balls.

But then we knew that already so what is the point?

Wait there is more.

Binomial Expansion

Example: Consider a box with four balls, say red, purple, green and yellow. What are all the possible selections of balls we can take from the box?

$$\begin{aligned} f(r,p,g,y) &= (1+r)(1+p)(1+g)(1+y) \\ &= 1 + r + p + g + y \\ &+ rp + rg + ry + pg + py + gy \\ &+ pgy + rgy + rpy + rpg \\ &+ rpgy \end{aligned}$$

Lets say we're interested in keeping track of whether the red ball has been chosen, but we don't care about the colours of the other balls. Then we set $p = b$, $g = b$, and $y = b$, and obtain:

$$\begin{aligned} f(r,b,b,b) &= (1+r)(1+b)(1+b)(1+b) = (1+r)(1+b)^3 \\ &= (1 + 3b + 3b^2 + b^3) + r(1 + 3b + 3b^2 + b^3). \end{aligned}$$

Thus, for example, the number of ways of choosing 3 balls, of which one of them must be red, is 3 (coefficient of rb^2).

Exercise

Example: How many ways are there to give k bananas to 3 people such that persons 1 and 2 get no more than 2 bananas, while person 3 gets at most 1 banana?

Solution via generating functions: For each banana given to a person there is a factor of x, first factor is for person 1, second factor for person 2, third factor for person 3.

$$
\begin{aligned}
f(x) &= (1+x+x^2)(1+x+x^2)(1+x) \\
&= 1+3x+5x^2+5x^3+3x^4+x^5
\end{aligned}
$$

We can read off, for example, that there are 5 ways to distribute 2 bananas according to this rule.

Note: The problem has no solution for $k \geq 6$ since all terms $[x^k]\, f(x) = 0$.

Why are Generating Functions Useful?

- **Recurrences:** Given a recurrence, we may be able to find an elegant, closed form solution.
- **Asymptotic formulae:** We may mostly be interested in how a sequence grows for large n. Generating functions encode this succinctly.

  Recall Stirling's formula for $n!$: $n! \simeq \sqrt{2\pi n}\, n^n e^{-n}$, valid for "large" n.

  We gain access to powerful methods from real and complex analysis.
- **Prove identities:** Given an identity, often the easiest way to prove it is to multiply each side by a power of x, and sum, to obtain expressions involving generating functions.
- **Relating combinatorial problems:** Basic manipulations (algebraic, change of variables, differentiation) have combinatorial interpretations and can be used to turn one combinatorial problem into another.

38 Fibonacci Numbers

Fibonacci Numbers – Introduction

- Study Fibonacci numbers and Fibonacci sequence.
- Apply generating function methods to the problem.
- Fibonacci numbers relate to the golden ratio with origin in classical geometry.

Motivation: Consider a population of rabbits, which reproduce according to the following rule. Each month,

1. Every baby female rabbit becomes an adult.

2. Female adult rabbits give birth to one female baby rabbit.

Denoting a for a baby rabbit, A for an adult rabbit, then this is equivalent to the **substitution rule**:

$$\begin{aligned} a &\mapsto A \\ A &\mapsto Aa \end{aligned}$$

Fibonacci Numbers

If we start with a single baby rabbit, a, then the population evolves as:

$$\begin{array}{ll} n=1 & a \\ n=2 & A \\ n=3 & Aa \\ n=4 & AaA \\ n=5 & AaAAa \\ n=6 & AaAAaAaA \\ n=7 & AaAAaAaAAaAAa \\ \vdots & \vdots \end{array}$$

Count the population as a function of time, with x_n being the number of baby rabbits, X_n adult rabbits, and $F_n = x_n + X_n$ total number of rabbits after n months.

We have the initial data $x_1 = 1$, $X_1 = 0$, and the substitution rules lead to the recurrence relations:

$$\begin{aligned} x_n &= X_{n-1} \\ X_n &= X_{n-1} + x_{n-1} \end{aligned}$$

Fibonacci Numbers

Thus,

$$\begin{aligned} F_n &= x_n + X_n \\ &= X_{n-1} + X_{n-1} + x_{n-1} \\ &= X_{n-2} + x_{n-2} + X_{n-1} + x_{n-1} \\ &= F_{n-2} + F_{n-1}. \end{aligned}$$

This is a 2-term linear recurrence relation with initial conditions $F_1 = 1$, $F_2 = 1$.

Questions:

1. Can we compute the generating function for $\{F_n\}$?

   i.e. $F(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \dots$

2. Is there a "simple" formula for F_n?

3. How fast does F_n grow with n? Is there a "simple" formula in that case?

Fibonacci Number Generating Function

Theorem 93 (Fibonacci Number Generating Function)**.** *The Fibonacci numbers (defined by $F_n = F_{n-1} + F_{n-2}, F_1 = F_2 = 1$) have the generating function*

$$F(x) = \sum_{n=1}^{\infty} F_n x^n = \frac{x}{1 - x - x^2}.$$

Proof: We prove the theorem using a general method that can be used to derive generating functions from some recurrence relations.

The starting point is

$$F_n = F_{n-1} + F_{n-2}$$

Multiply by x^n and sum from $n = 3$ (start from $n = 3$ so $F_{n-2} \to F_1$),

$$\sum_{n=3}^{\infty} F_n x^n = \sum_{n=3}^{\infty} F_{n-1} x^n \; + \; \sum_{n=3}^{\infty} F_{n-2} x^n$$

Fibonacci Number Generating Function

Shift the index so all sums explicitly involve F_n:

$$\begin{aligned} \sum_{n=3}^{\infty} F_n x^n &= \sum_{n=3}^{\infty} F_{n-1} x^n + \sum_{n=3}^{\infty} F_{n-2} x^n \\ &= \sum_{n=2}^{\infty} F_n x^{n+1} + \sum_{n=1}^{\infty} F_n x^{n+2} \\ &= x \sum_{n=2}^{\infty} F_n x^n \; + \; x^2 \sum_{n=1}^{\infty} F_n x^n \end{aligned}$$

Only last generating function equals $F(x)$. The others are missing some terms.

Fibonacci Number Generating Function

Add/Subtract missing terms to get $F(x)$ series:

$$\begin{aligned} \sum_{n=3}^{\infty} F_n x^n &= -xF_1 - x^2 F_2 + \sum_{n=1}^{\infty} F_n x^n &= -x - x^2 + F(x) \\ x \sum_{n=2}^{\infty} F_n x^n &= x \left(-xF_1 + \sum_{n=1}^{\infty} F_n x^n \right) &= -x^2 + xF(x) \end{aligned}$$

Solve for $F(x)$:

$$
\begin{aligned}
-x - x^2 + F(x) &= -x^2 + xF(x) + x^2F(x) \\
\Rightarrow \qquad (1 - x - x^2)F(x) &= x \\
\Rightarrow \qquad F(x) &= \frac{x}{1 - x - x^2}.
\end{aligned}
$$

39 Recursions and generating functions

Fibonacci Numbers – Asymptotics

Question: Can we extract useful information from the generating function?

Asymptotic behaviour of the Fibonacci numbers; an exact expression for F_n?

Answer: Yes. Use a partial fraction decomposition.

The zeroes of $1 - x - x^2$ are: $-\dfrac{1 \pm \sqrt{5}}{2}$.

Defining $\alpha_\pm = \frac{1 \pm \sqrt{5}}{2}$, we have $1 - x - x^2 = -(\alpha_+ + x)(\alpha_- + x)$. So

$$
\begin{aligned}
F(x) &= -\frac{x}{(\alpha_+ + x)(\alpha_- + x)} \\
&= -\frac{x}{\alpha_+\alpha_-(1 + x/\alpha_+)(1 + x/\alpha_-)}
\end{aligned}
$$

Since $\alpha_+\alpha_- = -1$, this finally leads to

$$
F(x) = \frac{x}{(1 - \alpha_- x)(1 - \alpha_+ x)}.
$$

Note: α_+ is the so-called "golden ratio".

Partial Fraction Decomposition

Now we are going to perform a partial fraction decomposition of $F(x)$:

$$
F(x) = \frac{x}{(1 - \alpha_- x)(1 - \alpha_+ x)} = \frac{A}{1 - \alpha_- x} + \frac{B}{1 - \alpha_+ x}
$$

Multiply each side of the equation by $(1 - \alpha_- x)(1 - \alpha_+ x)$ to obtain

$$
\begin{aligned}
x &= A(1 - \alpha_+ x) + B(1 - \alpha_- x) \\
&= (A + B) - (A\alpha_+ + B\alpha_-)x
\end{aligned}
$$

Equating terms on LHS and RHS and solving for A and B gives:

$$
A = -\frac{1}{\sqrt{5}} \quad \text{and} \quad B = \frac{1}{\sqrt{5}}
$$

and we find

$$
F(x) = \frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(-\frac{1}{1 - \alpha_- x} + \frac{1}{1 - \alpha_+ x} \right).
$$

Fibonacci Numbers – Exact Formula

We have now arrived at the moment of truth. We can immediately expand each of the terms on the RHS as they are simply geometric series. Thus

$$\begin{aligned} F(x) &= \frac{1}{\sqrt{5}} \sum_{n=1}^{\infty} \left(-(\alpha_- x)^n + (\alpha_+ x)^n\right) \\ &= \frac{1}{\sqrt{5}} \sum_{n=1}^{\infty} \left(\alpha_+^n - \alpha_-^n\right) x^n. \end{aligned}$$

Hence, by using the fact that the coefficient of x^n is, by definition, F_n, we obtain the *exact* closed form expression for the Fibonacci numbers.

Theorem 94 (Fibonacci Numbers I)**.** *The Fibonacci numbers are given by the formula*

$$F_n = \frac{1}{\sqrt{5}} \left(\alpha_+^n - \alpha_-^n\right), \quad \textit{where} \quad \alpha_\pm = \frac{1 \pm \sqrt{5}}{2}.$$

Fibonacci Numbers – Exact Simplified Formula

In this particular case we can simplify things a little bit further.

We have that $\alpha_- \approx -0.618$, and therefore

$$\left|\frac{\alpha_-^n}{\sqrt{5}}\right| \approx \frac{0.618^n}{2.21} < \frac{1}{2} \quad \forall n \geq 1$$

We know that F_n must be an integer. The α_- term contributes a value of less than 1/2.This means that F_n is the nearest integer to the remaining part.

We can write the "nearest integer" to a number x as $\left\lfloor x + \frac{1}{2} \right\rfloor$. Thus

Theorem 95 (Fibonacci Numbers II)**.** *The Fibonacci numbers are given by the formula*

$$F_n = \left\lfloor \frac{\alpha_+^n}{\sqrt{5}} + \frac{1}{2} \right\rfloor, \quad \textit{where} \quad \alpha_+ = \frac{1 + \sqrt{5}}{2}.$$

Fibonacci Numbers – Asymptotic

What is the asymptotic behaviour of F_n?

Frequently, this is the question we most want to answer about a sequence.

This follows immediately from the previous theorem:

Corollary 96 (Fibonacci Numbers Asymptotic)**.** *The asymptotic behaviour of the Fibonacci numbers is*

$$F_n \sim \frac{\alpha_+^n}{\sqrt{5}}, \quad \textit{where} \quad \alpha_+ = \frac{1 + \sqrt{5}}{2}.$$

Golden Ratio

In classical geometry, the Golden Ratio $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$ occurs in

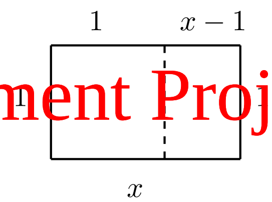
- A rectangle with a special subdivision property.
- Regular pentagons and pentagrams.
- Plus many other situations.

Rectangles can also be used to give a proof of the Fibonacci numbers identity

$$F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n F_{n+1}.$$

Golden Ratio and Rectangles

Question: Find $x > 1$ with property that the subdivided rectangle has the same proportions.



We require:

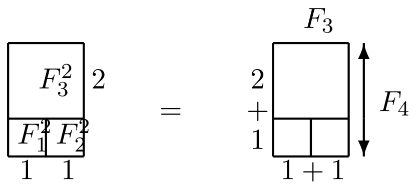
$$
\begin{aligned}
\frac{\text{long side}}{\text{short side}} &= \frac{x}{1} = \frac{1}{x-1} \\
\Rightarrow \quad x^2 - x - 1 &= 0 \\
\Rightarrow \quad x &= \frac{1}{2}\left(1 + \sqrt{5}\right) = \phi.
\end{aligned}
$$

Fibonacci Identity and Rectangles

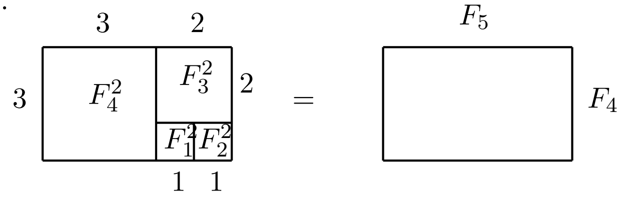
Fibonacci identity using rectangles,

$$F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n F_{n+1}.$$

$n = 3:$

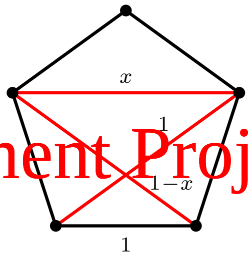


$n = 4:$



Golden Ratio and Pentagons

Regular unit pentagon



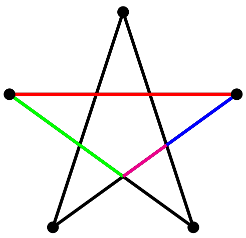
Similar triangles:

$$\frac{x}{1} = \frac{1}{x-1}$$

$$\Rightarrow \quad x = \frac{1}{2}\left(1+\sqrt{5}\right) = \phi$$

Golden Ratio and Pentagrams

Regular Pentagrams

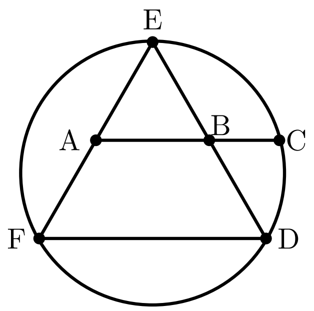


Here the ratio of the lengths of the coloured lines are ϕ:

$$\phi = \frac{|\text{red line}|}{|\text{green line}|} = \frac{|\text{green line}|}{|\text{blue line}|} = \frac{|\text{blue line}|}{|\text{magenta line}|}$$

Odom's Construction of the Golden Ratio

George Odom has given a construction for ϕ involving an equilateral triangle: if an equilateral triangle is inscribed in a circle and the line segment joining the midpoints of two sides is drawn so as to intersect the circle in either of two points, then these three points are in golden proportion:



$$\frac{|AB|}{|BC|} = \frac{|AC|}{|AB|} = \phi.$$

Fibonacci Numbers - Alternative Derivation

In the next few slides we give an alternative derivation for $F(x)$.

The Fibonacci recurrence can be represented in matrix form:

$$\begin{bmatrix} x_n \\ X_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ X_{n-1} \end{bmatrix}$$

subject to the initial condition

$$\begin{bmatrix} x_1 \\ X_1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

In physics a matrix like $T = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is known as a **Transfer Matrix**.

Fibonacci Numbers - Alternative Derivation

The solution of the above matrix recurrence is

$$\begin{bmatrix} x_2 \\ X_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} x_3 \\ X_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_2 \\ X_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^2 \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\vdots$$

$$\begin{bmatrix} x_n \\ X_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{n-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Question: How does one compute matrix powers? We write

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = QDQ^{-1}, \quad D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$$

Fibonacci Numbers - Alternative Derivation

Then

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{n-1} = QD^{n-1}Q^{-1} = Q \begin{bmatrix} \lambda_1^{n-1} & 0 \\ 0 & \lambda_2^{n-1} \end{bmatrix} Q^{-1}$$

Here λ_1 and λ_2 are the eigenvalues of the matrix T, obtained from the characteristic equation:

$$\det\,(T - \lambda I) = \det\left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) = 0$$

$$\Rightarrow \quad \lambda^2 - \lambda - 1 = 0 \quad \Rightarrow \quad \lambda_1 = \alpha_+,\ \lambda_2 = \alpha_-$$

With this we can then show that

$$Q = \frac{1}{5^{1/4}} \begin{bmatrix} 1 & -1 \\ \alpha_+ & -\alpha_- \end{bmatrix} \quad \text{and} \quad Q^{-1} = \frac{1}{5^{1/4}} \begin{bmatrix} -\alpha_- & 1 \\ -\alpha_+ & 1 \end{bmatrix}$$

Fibonacci Numbers - Alternative Derivation

Note that $F_n = X_n + x_n$ is the (2,2) entry in $QD^{n-1}Q^{-1}$. Now

$$QD^{n-1}Q^{-1} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -1 \\ \alpha_+ & -\alpha_- \end{bmatrix} \begin{bmatrix} \alpha_+^{n-1} & 0 \\ 0 & \alpha_-^{n-1} \end{bmatrix} \begin{bmatrix} -\alpha_- & 1 \\ -\alpha_+ & 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & -1 \\ \alpha_+ & -\alpha_- \end{bmatrix} \begin{bmatrix} -\alpha_-\alpha_+^{n-1} & \alpha_+^{n-1} \\ \alpha_+\alpha_-^{n-1} & \alpha_-^{n-1} \end{bmatrix}$$

which shows that:

$$F_n = \frac{1}{\sqrt{5}} \left(\alpha_+^n - \alpha_-^n \right)$$

Now to find the generating function $F(x)$ we simply have to reverse the steps used previously to go from $F(x)$ to the above result.

Walking on a Graph

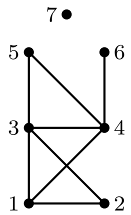
Question: How many walks of length n are there on a graph starting at a vertex v and ending at a vertex u or ending at any vertex?

This question can be answered using linear algebra. We need

Definition 97 (Adjacency Matrix)**.** Given a graph G with $V(G) = \{v_1, v_2, \dots, v_p\}$, the **adjacency matrix** of G is the $p \times p$ matrix $A = (a_{ij})$ where $a_{ij} = 1$ if $\{v_i, v_j\} \in E(G)$ and $a_{ij} = 0$ otherwise.

Note: The adjacency matrix relies on the given order of vertices, but is unique up to permutation of rows and permutation of columns.

Example:



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

Walking on a Graph

The adjacency matrix can be viewed as a transfer or transition matrix telling us which vertices can be reached from vertex v_i in a single step. We therefore get the following result

Theorem 98 (Random Walks on a Graph)**.** *Let A be the adjacency matrix of a graph G. The ij entry $a_{ij}^{(n)}$ in A^n equals the number of (random) walks of length n from vertex v_i to v_j.*

Proof: This is a direct consequence of the definition of matrix multiplication:

$$a_{ij}^{(n)} = (A^n)_{ij} = \sum a_{ii_1} a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_{n-1} j}$$

where the sum is over all sequences $(i_1, i_2, \dots, i_{n-1})$ with $i_k \in \{1, 2, \dots, p\}$. The summand is 1 if there is a walk along edges $\{v_{i_k}, v_{i_{k+1}}\}$ of G from vertex v_i to v_j and 0 otherwise ($a_{i_k i_{k+1}} = 0$ unless $\{v_{i_k}, v_{i_{k+1}}\} \in E(G)$). Hence the sum equals the number of walks from v_i to v_j.

Note: This concept is readily generalised to weighted graphs, directed graphs and/or pseudo graphs where loops are allowed.

Walking on a Graph

Theorem 99 (Rational Generating Functions)**.** *Define the generating function $F_{ij}(G, \lambda) = \sum a_{ij}^{(n)} \lambda^n$, then*

$$F_{ij}(G, \lambda) = \frac{(-1)^{i+j} \det (I - \lambda A : j, i)}{\det (I - \lambda A)},$$

where $(B : j, i)$ is the matrix obtained by removing row j and column i from B.

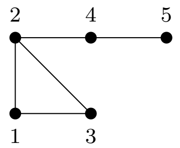
Thus in particular $F_{ij}(G, \lambda)$ is a rational function of λ.

Proof: Theorem 4.7.2 in "Enumerative Combinatorics, Vol 1" by R P Stanley.

Note: This fundamental result tells us that finite dimensional transfer matrices leads to rational generating functions. Thus only *infinite* dimensional transfer matrices can lead to generating functions that aren't rational.

Walking on a Graph

Example: Consider the graph



$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

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

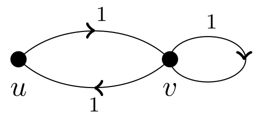
Walking on a Graph

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

$$A^5 = \begin{pmatrix} 12 & 18 & 13 & 7 & 5 \\ 18 & 14 & 18 & 16 & 2 \\ 13 & 18 & 12 & 7 & 5 \\ 7 & 16 & 7 & 2 & 6 \\ 5 & 2 & 5 & 6 & 0 \end{pmatrix}$$

Fibonacci as Walks on a Graph

Example: Consider the weighted pseudo di-graph



$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Walks on this graph generate the Fibonacci numbers. Theorem by Stanley gives expressions for the generating functions for the entries $a_{ij}^{(n)}$ of A^n.

$$\det(I - \lambda A) \;=\; \begin{vmatrix} 1 & -\lambda \\ -\lambda & 1-\lambda \end{vmatrix} \;=\; 1 - \lambda - \lambda^2.$$

We start at u so initial vector is $(1, 0)$. So we need the sum of the generating functions of the entries $a_{11}^{(n)}$ and $a_{21}^{(n)}$. These are

$$\frac{1-\lambda}{1-\lambda-\lambda^2} \qquad \text{and} \qquad \frac{\lambda}{1-\lambda-\lambda^2}.$$

The sought after generating function is

$$G(\lambda) \;=\; \frac{1}{1-\lambda-\lambda^2}.$$

A Checker Jumping Problem

Here is a problem in combinatorial logic which makes use of the golden ratio:

Consider the integer grid in the xy-plane.

Suppose that “checkers” are allowed to be placed on lattice points on or below the x-axis.

These checkers can jump over neighbouring checkers, with the checker being jumped over removed, according to the usual rule.

The problem is to determine the least number of checkers it takes to reach a prescribed height y above the x-axis.

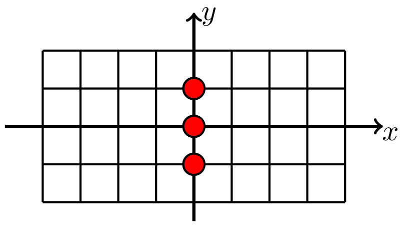
For $y = k$, $k = 1, 2, 3, 4$ the answer is $2, 4, 8, 20$.

However, amazingly, for $k \geq 5$ it is impossible.

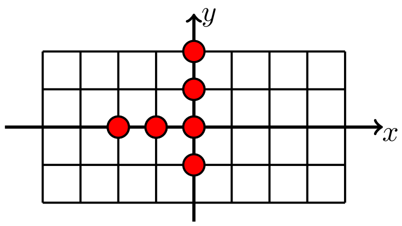
A Checker Jumping Problem

Initially, checkers must be on or below x-axis.

Height $y = 1$:



Height $y = 2$:



A Checker Jumping Problem

The aim is to get a checker to the point $(0, 5)$.

Associate with each lattice point a variable x^d. Define d to be the minimum number of steps along grid lines it takes to reach $(0, 5)$.

The *value* of a set of checkers is the sum of the corresponding variables.

We will show that by an appropriate choice of x, the value of a set of checkers can never increase.

On the other hand we will show that the value of the set of all checker in the region $y \leq 0$ is equal to 1, which is the same as the value of a checker at the point $(0, 5)$.

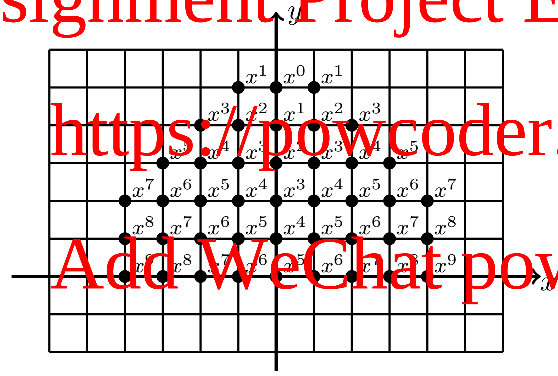
Hence no finite configuration of checkers can ever reach $(0, 5)$.

A Checker Jumping Problem

Step 1: Introduce a weighting to each lattice site.

Weigh the site we'd like to reach, $(0, 5)$ by $x^0 = 1$.

Weigh the other sites by x^d, where d is the shortest distance from the site to $(0, 5)$ as measured along the x and y axes, e.g.,



A Checker Jumping Problem

Step 2: Investigate change in weight associated with different moves:

- **Class 1** - Moves which carry a checker closer to the destination $(0, 5)$.

  Change in weight: $x^n - (x^{n+1} + x^{n+2}) = x^n(1 - x - x^2)$.

  That is $\bullet\bullet\circ \to \circ\circ\bullet$ with weights x^{n+2}, x^{n+1}, x^n, from left to right.

- **Class 2** - Moves taking a checker further away.

  Change in weight: $x^{n+2} - (x^{n+1} + x^n) = x^n(x^2 - x - 1)$.

- **Class 3** - Moves that leave the distance unchanged.

  Change in weight: $-x^n$ (central checker x^n ones next to it x^{n+1}).

- Choose $x > 0$ such that the change in weight of a 'closing' move is zero.

$$\Rightarrow x = \frac{1}{2}(-1 + \sqrt{5}) \;=\; \frac{1}{\phi}.$$

  Then change in weight of the other moves is negative!

A Checker Jumping Problem

The conclusion from the analysis above is that to be able to reach $(0, 5)$, the initial configuration of checkers must have weight ≥ 1, i.e. the weight at $(0, 5)$.

Step 3: Add up the weight of all the lattice sites on or below the x-axis.

Total initial weight of checkers on x-axis =

$$\begin{aligned} x^5 + 2x^6 + 2x^7 + \dots &= x^5 + 2x^6(1 + x + x^2 + x^3 + \dots) \\ &= x^5 + \frac{2x^6}{1-x} = x^5 \frac{1+x}{1-x}. \end{aligned}$$

Similarly total weight on line at $y = -1$ is $x^6 \dfrac{1+x}{1-x}$, at $y = -2$ it is $x^7 \dfrac{1+x}{1-x}$, etc. So total initial weight is:

$$x^5 \frac{1+x}{1-x} + x^6 \frac{1+x}{1-x} + x^7 \frac{1+x}{1-x} + \cdots = x^5 \frac{1+x}{(1-x)^2}.$$

Now insert $x = 1/\phi$ and we find that the total initial weight is at most 1.

So no **finite** configuration of checkers can ever reach $(0, 5)$.

Euclid's Algorithm

Euclid's Algorithm appears as a solution to Proposition VII.2 in the Elements:

- Given two numbers not prime to one another, to find their greatest common measure.

What Euclid called "common measure" is termed nowadays a common factor or a common divisor. Euclid VII.2 then offers an algorithm for finding the greatest common divisor (gcd) of two integers.

Not surprisingly, the algorithm bears Euclid's name.

Algorithm 100 (Euclid's Algorithm)**.** Let $a \geq b$ be integers then $\gcd(a, b) = \gcd(b, a \bmod b)$. Euclid's algorithm iterates this equation and stops once $a \bmod b = 0$ since $\gcd(b, 0) = b$.

Euclid's Algorithm

Example: Let $a = 2322, b = 654$

$$\begin{aligned} \gcd(2322, 654) &= \gcd(654, 2322 \mod 654) = \gcd(654, 360) \\ \gcd(654, 360) &= \gcd(360, 654 \mod 360) = \gcd(360, 294) \\ \gcd(360, 294) &= \gcd(294, 360 \mod 294) = \gcd(294, 66) \\ \gcd(294, 66) &= \gcd(66, 294 \mod 66) = \gcd(66, 30) \\ \gcd(66, 30) &= \gcd(30, 66 \mod 30) = \gcd(30, 6) \\ \gcd(30, 6) &= \gcd(6, 30 \mod 6) = \gcd(6, 0) = 6 \end{aligned}$$

Therefore, $\gcd(2322, 654) = 6$.

Question: Given a and b how many iterations are required to find $\gcd(a, b)$?

Lamé's Theorem

I used "Lamé's Theorem - the Very First Application of Fibonacci Numbers' at `http://www.cut-the-knot.org/blue/LamesTheorem.shtml`

Theorem 101 (Lamé's Theorem – Honsberger Version)**.** *The number of division steps in an application Euclid's algorithm never exceeds 5 times the number of digits in the lesser number.*

Theorem 102 (Lamé's Theorem – Knuth Version)**.** *For $n \geq 1$, let integers a and b, $a > b > 0$, be such that processing a and b by Euclid's algorithm takes exactly n division steps. Moreover, assume that a is the least possible number satisfying that requirement. Then $a = F_{n+2}$ and $b = F_{n+1}$, where $\{F_n\}$ is the Fibonacci sequence.*

Theorem 103 (Lamé's Theorem – Moll Version)**.** *Let $a > b$ be integers. The number of steps in Euclid's algorithm is about $\log_{10} b / \log_{10} \phi$. This is at most five times the number of digits of b.*

Proof – Honsberger Version

Here we define the Fibonacci numbers by $F_n = F_{n-1} + F_{n-2}$, $F_0 = 1$, $F_1 = 1$.

Lemma 104. *For all $n \geq 1$, $F_{n+5} > 10F_n$.*

Proof:

$$
\begin{aligned}
F_{n+5} &= F_{n+4} + F_{n+3} \\
&= 2F_{n+3} + F_{n+2} \\
&= 3F_{n+2} + 2F_{n+1} \\
&= 5F_{n+1} + 3F_n \\
&= 8F_n + 5F_{n-1} \\
&= 13F_{n-1} + 8F_{n-2} \\
&= 21F_{n-2} + 13F_{n-3} \\
&> 10(2F_{n-2} + F_{n-3}) \\
&= 10F_n
\end{aligned}
$$

Proof – Honsberger Version

Let d_n denote the number of digits in F_n.

From the above lemma it follows that F_{n+5} has at least one more digit than F_n.

By direct inspection, numbers F_n, for $1 \leq n \leq 5$ are single-digit. They have at least 2 digits for $5 < n \le 10$,

have at least 3 digits for $10 < n \le 15$,

have at least 4 digits for $15 < n \le 20$,

and, in general, have at least k digits for $5(k-1) < n \le 5k$.

Thus it is always the case that $d_n \ge n/5$.

Now back to Euclid's algorithm.

Proof – Honsberger Version

Given two integers, $a > b > 0$, we set $a = r_0$, $b = r_1$ and divide with remainder. Assuming Euclid's algorithm takes n steps,

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, \quad 0 < r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2 \\
&\cdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_n
\end{aligned}$$

Note that $q_n \ge 2$ (otherwise, we would have $r_{n-1} = r_n$). Proceed backwards, starting with $r_n \ge 1$, which implies $r_n \ge F_1$. Next, $r_{n-1} \ge 2r_n = F_2$. And further,

$$r_{n-2} = r_{n-1} q_{n-1} + r_n > r_{n-1} + r_n > F_2 + F_1 = F_3.$$

Proof – Honsberger Version

In general:

$$r_{n-k} = r_{n-k+1} q_{n-k_1} + r_{n-k+2} > r_{n-k+1} + r_{n-k+2} > F_k + F_{k-1} = F_{k+1},$$

such that at the end of the process (i.e., at the beginning of the algorithm) $b = r_1 > F_n$ and $a = r_0 > F_{n+1}$.

Therefore if Euclid's algorithm takes exactly n steps, then necessarily $b > F_n$ and has at least as many digits, which, as we found previously, is at least $n/5$. And this proves the Honsberger version.

40 Formal Power Series

Formal Power Series

It is very useful to view generating functions as "formal" mathematical objects.

Certain standard operations (such as term-by-term differentiation) can be given nice and useful combinatorial interpretations.

Term-by-term differentiation of the Taylor series of a function is only permitted when the series is uniformly convergent (the function is analytic).

However, the combinatorial interpretation is true irrespective of the analytic properties of the series. In combinatorics it is therefore very useful to always permit term-by-term differentiation (or other operations) regardless of their 'analytic' validity.

This view-point leads to the concept of **Formal Power Series**. But first

Definition 105 (Counting Function)**.** A **counting function** is a map $f : \mathbb{N}_0 \to \mathbb{C}$.

Note: We are mainly concerned with the case $f : \mathbb{N}_0 \to \mathbb{N}_0$.

Formal Power Series

Definition 106 (Formal Power Series)**.** Let $f : \mathbb{N}_0 \to \mathbb{C}$. We associate to f the **formal power series**

$$F(z) = \sum_{n \geq 0} f(n) z^n,$$

and say that $F(z)$ is the **generating function** of the counting function f.

Formal Power Series

- The adjective "formal" refers to the fact that we regard these series as *algebraic* objects to be added, multiplied or otherwise manipulated.
- The symbol z^n is just a mark for where $f(n)$ is placed.
- We do not need to consider $F(z)$ as a function is the usual sense; that is, we do not have to concern ourselves with its convergence etc.
- Two formal power series are equal if and only if they agree term by term.
- If we have manipulated two such series $F(z)$ and $G(z)$ algebraically and obtained $F(z) = G(z)$, we can read of $f(n) = g(n)$ for all n, and this proves a corresponding combinatorial identity.

Manipulation of Generating Functions

Operations such as addition, multiplication and differentiation are associated with certain operations on the coefficients of the generating functions.

These operations often have natural combinatorial interpretations.

Let

$$\begin{aligned} f(x) &= \sum_{k=0}^{\infty} f_k x^k \\ g(x) &= \sum_{k=0}^{\infty} g_k x^k \\ h(x) &= \sum_{k=0}^{\infty} h_k x^k \end{aligned}$$

Theorem 107 (Addition)**.** *If* $h(x) = f(x) + g(x)$ *then* $h_k = f_k + g_k$*.*

Proof: Trivial.

Manipulation of Generating Functions

Theorem 108 (Multiplication)**.** *If* $h(x) = f(x)\,g(x)$*, then*

$$h_k = \sum_{j=0}^{k} f_j\, g_{k-j} = \sum_{j=0}^{k} f_{k-j}\, g_j = \sum_{\substack{i+j=k \\ i,j\geq 0}} f_i\, g_j\,.$$

These sums are called the **convolution** *of the sequences* $\{f_k\}$ *and* $\{g_k\}$*.*

Proof:

$$\begin{aligned} h(x) &= f(x)g(x) = \left(\sum_{j=0}^{\infty} f_j x^j\right)\left(\sum_{i=0}^{\infty} g_i x^i\right) \\ &= \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} f_j\, g_i\, x^{i+j} \qquad (k = i + j,\ i = k - j) \\ &= \sum_{k=0}^{\infty}\sum_{j=0}^{k} f_j\, g_{k-j}\, x^k \quad \Rightarrow \quad [x^k]\,h(x) = \sum_{j=0}^{k} f_j\, g_{k-j} \end{aligned}$$

Manipulation of Generating Functions

There are two very important special cases of the multiplication theorem.

Corollary 109 (Shifting)**.** $f(x) = x^m$: $h_k = g_{k-m}$ *or* $[x^k]\,(x^m g(x)) = [x^{k-m}]g(x)$*.*

Note: Multiplication by x^m shifts backwards by m units.

Corollary 110 (Summing)**.** $f(x) = \dfrac{1}{1-x}$: $h_k = \sum_{j=0}^{k} g_j$ *or* $[x^k]\left(\dfrac{g(x)}{1-x}\right) = \sum_{j=0}^{k} g_j = \sum_{j=0}^{k}[x^j]g(x)\,.$

Proof: $f(x) = \dfrac{1}{1-x} = \sum_{k=0}^{\infty} x^k \ \Rightarrow \ f_k = 1 \ \forall k.$

Note: $h_k = \sum_{j=0}^{k} g_j$ are the **partial sums** of the sequence $\{g_k\}$.

Manipulation of Generating Functions

Theorem 111 (Differentiation)**.** *If* $h(x) = \left(x\dfrac{\mathrm{d}}{\mathrm{d}x}\right) f(x)$*, then* $h_k = k\, f_k$*.*

Proof: Differentiate term-by-term and use $x\dfrac{\mathrm{d}}{\mathrm{d}x}x^k = x\,k\,x^{k-1} = k\,x^k$.

Note: Why $x\frac{\mathrm{d}}{\mathrm{d}x}$? Here n is the 'size' of the combinational object.

Differentiating and then multiplying by x ensures that the placeholder x^n in the formal power series still refers to objects of size n.

Theorem 112 (Integration)**.** *If* $h(x) = \dfrac{1}{x}\displaystyle\int f(x)\,\mathrm{d}x$, *then* $h_k = \dfrac{1}{k+1}f_k$.

Note: Integration is rarely used in combinatorics.

Combinatorial Interpretations

1. **Addition:** Disjoint union of two sets of objects F and G so objects of same size are put together.
2. **Multiplication:**
   - Distribution of objects (balls into boxes etc.).
   - Convolution corresponds to concatenating (gluing) objects together. Form objects of size n by taking objects of size k from set F and 'glue' them to objects of size $n-k$ from G.
   - Particularly useful when $F = G$, then we are saying 'large' objects in F can be constructed be gluing together 'smaller' objects.
   - Very important when the objects in F have a recursive structure.
3. **Differentiation:** 'Marking' or singling out a component in an object.
4. **Integration:** No natural combinatorial interpretation.

Combinatorial Interpretations

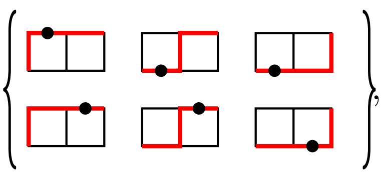
Definition 113 (Marking)**.** If an object consists of several indistinguishable parts then **marking** a part distinguishes this part in some way say by colouring an edge or vertex in a graph, putting a dot on an edge etc.

Example: Edge marked binomial paths.

Mark an edge by placing a dot on the edge, by different colour etc.

$$\overline{B}_{n,m} = \{b \,|\, b \in B_{n.m} \text{ with one } \textit{horizontal} \text{ step marked}\}$$

$\overline{B}_{2,1} =$



$\left|\overline{B}_{2,1}\right| = 6$

Edge Marked Binomial Paths

In general we have n horizontal steps gives a factor of n

$$|\,\overline{B}_{n,m}\,| = n\,|\,B_{n,m}\,| = n\binom{n+m}{n} = n\binom{p}{n} \qquad (p = n+m).$$

Thus

$$\begin{aligned}
\overline{B}(x) &= \sum_{n=0}^{p} |\,\overline{B}_{n,p-n}\,|\,x^n \qquad \text{(length } p \text{ is fixed)} \\
&= \sum_{n=0}^{p} n\binom{p}{n}x^n \quad = \quad \sum_{n=0}^{p}\binom{p}{n}\left[x\frac{\mathrm{d}}{\mathrm{d}x}x^n\right] \\
&= x\frac{\mathrm{d}}{\mathrm{d}x}\left[\sum_{n=0}^{p}\binom{p}{n}x^n\right] \quad = \quad x\frac{\mathrm{d}}{\mathrm{d}x}(1+x)^p \\
&= px(1+x)^{p-1}.
\end{aligned}$$

Proving an Identity

Example: Use generating functions to prove that

$$1 + 2 + 3 + \cdots + n = n(n+1)/2$$

Solution: Let $g(x) = 1 + 2x + 3x^2 + 4x^3 + \cdots = \sum_{n=0}^{\infty}(n+1)x^n = \dfrac{1}{(1-x)^2}$.

Coefficients are the numbers to be summed.

Define $h(x)$ as the product $h(x) = g(x)\dfrac{1}{1-x} = \dfrac{1}{(1-x)^3}$.

By the Summing Theorem $[x^{n-1}]h(x) \;=\; 1 + 2 + 3 + \cdots + n$.

Geometric series gives, for $|x| < 1$,

$$1 + x + x^2 + \ldots = \frac{1}{1-x}$$

Differentiating term-by-term we get (OK since series uniformly convergent)

$$0 + 1 + 2x + 3x^2 + 4x^3 + \ldots = \frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{1-x} = \frac{1}{(1-x)^2}$$

Proving an Identity

However, we also have

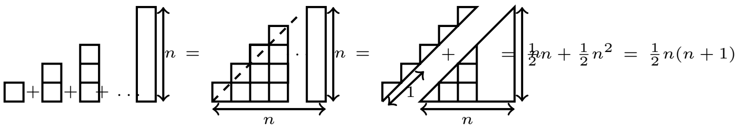
$$\begin{aligned}
h(x) = \frac{1}{(1-x)^3} \;&=\; \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{(1-x)^2} \\
= \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}x}\sum_{n=0}^{\infty}(n+1)x^n \;&=\; \frac{1}{2}\sum_{n=1}^{\infty}n(n+1)x^{n-1}
\end{aligned}$$

and hence the coefficient of x^{n-1} of $h(x)$ is $n(n+1)/2$.

The two expressions for $h(x)$ must be equal and we have proved the identity

$$1 + 2 + 3 + \cdots + n = n(n+1)/2.$$

Combinatorial interpretation as areas:



Derivatives and Averages

Example: Consider Dyck paths counted by length and number of contacts.

$$D(u, z) = \sum_{n,k} d_{n,k} u^k z^n,$$

where $d_{n,k}$ is the number of Dyck paths of length n with k returns to $y = x$.

First derivative w.r.t u gives an expansion for the average number of contacts:

$$D'(1, z) = \sum_n \left(\sum_k k d_{n,k} \right) z^n.$$

We first take the derivative and then set $u = 1$.

Second (and higher) derivatives give higher moments of the distribution of contacts., e.g., the fluctuation in the number of contacts is $\chi = \langle k^2 \rangle - \langle k \rangle^2$. Where the m'th moment given by

$$\langle k^m \rangle = \frac{\sum_k k^m d_{n,k}}{\sum_k d_{n,k}}.$$

Fluctuation quantities are particularly useful because they can give quite sensitive indications of phase-transitions.

41 Catalan Numbers

Catalan Numbers

Leonhard Euler, in the year 1751, introduced and found a closed formula for the Catalan numbers including the generating function. Euler was interested in the number of different ways of dividing a polygon into triangles. The proof of the result eluded him, until he was assisted by Christian Goldbach, and more substantially by Johann Segner. By 1759 a proof was completed.

The sequence is named after Eugène Charles Catalan, who discovered a connection to parenthesized expressions during his exploration of the Towers of Hanoi puzzle.

In 1988, it came to light that the Catalan number sequence had been used in China by the Mongolian mathematician Ming Antu by 1730. He wrote a book (completed by his student and not published until 1839) "Quick Methods for Accurate Values of Circle Segments" which included many trigonometric identities and power series, some involving Catalan numbers.

For more on the history of Catalan numbers see: Igor Pak Catalan Numbers Page at `http://www.math.ucla.edu/~pak/lectures/Cat/pakcat.htm` and check out his brief article under 'Historical articles'.

Dyck Paths – Application

Example: In a two candidate election with $2n+1$ voters, n voters cast their vote for candidate A and $n+1$ for B. What is the probability that A is always ahead of B (as the votes are counted) but loses at the last count?

Say $n = 3$ so there are 7 voters. The possible vote counting sequences are:

$$\left.\begin{array}{l} ABABAB\,B \\ ABAABB\,B \\ AABBAB\,B \\ AABABB\,B \\ AAABBB\,B \end{array}\right\} \quad A \text{ never losing except at last vote}$$

The vote count can be mapped (bijection) to a binomial path.

$$A \text{ vote} \mapsto \text{ North step} \qquad B \text{ vote} \mapsto \text{ East step}$$

The restriction A never losing except at last vote means that the path stays above $y = x$ except for the last step which must be an East step.

Dyck Paths – Application

So up until the last step the path is a Dyck path. Thus

$$\Pr(A \text{ ahead till last vote}) = \frac{|B^0_{2n}|}{|B_{n+1,n}|} = \frac{\frac{1}{n+1}\binom{2n}{n}}{\binom{2n+1}{n+1}}$$

$$= \frac{1}{n+1}\frac{(2n)!}{n!\,n!}\frac{n!\;(n+1)!}{(2n+1)!} = \frac{1}{2n+1}$$

$$= \frac{1}{v}, \quad v = \#\text{ voters.}$$

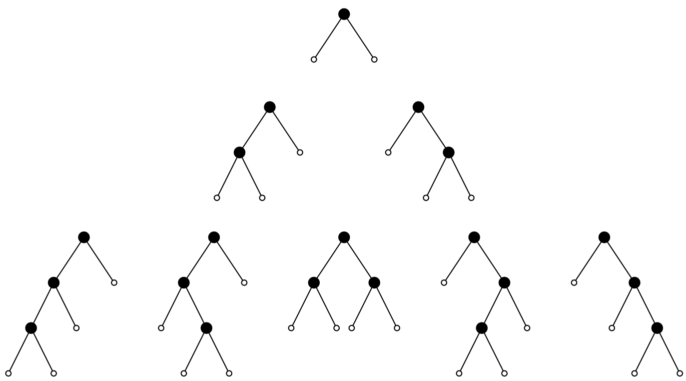
So with $v = 101$ the probability is about 1%.

42 Proper Binary trees

Proper Binary Trees

Definition 114 (Proper Binary Trees)**.** A proper binary tree is either a leaf or a node with a left and a right tree.

Example:



Generating Function for Proper Binary Trees

Theorem 115 (Generating Function for Proper Binary Trees)**.** *The generating function for proper binary trees has the functional equation*

$$T(x) = 1 + xT(x)^2$$

with exact closed form solution

$$T(x) = \frac{1}{2x}\left(1 - \sqrt{1-4x}\right).$$

The number of binary trees with n nodes t_n is given by the Catalan numbers

$$t_n = \frac{1}{n+1}\binom{2n}{n}$$

Proof: We have $t_0 = 1$. When constructing a tree of size n, we have a node at the root, and then we can have a tree on the LHS of size j and a tree on the RHS of size $n - j - 1$. Thus,

$$t_n = t_0 t_{n-1} + t_1 t_{n-2} + t_2 t_{n-3} + \cdots t_{n-1} t_0$$

Generating Function for Proper Binary Trees

$$t_n = t_0 t_{n-1} + t_1 t_{n-2} + t_2 t_{n-3} + \cdots t_{n-1} t_0$$

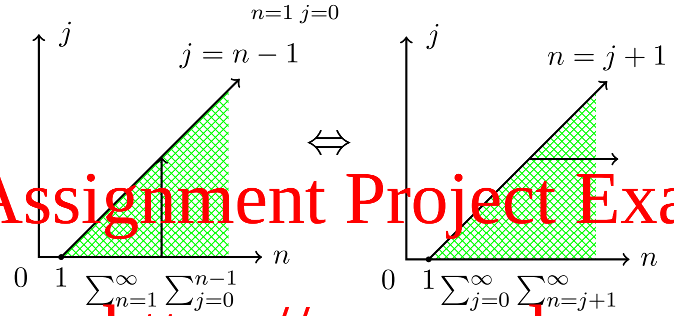
Note: The RHS is a *convolution* of $\{t_n\}$ with itself. It should look familiar - this kind of convolution occurs when multiplying generating functions. It suggests that the RHS involves $T(x)^2$.

Recipe: Let $T(x) = \sum_{n=0}^{\infty} t_n x^n$, multiply both sides of the recurrence by x^n, and sum over allowed values of n (t_{-1} is not a valid member of the sequence) so

$$
\begin{aligned}
t_n &= \sum_{j=0}^{n-1} t_j t_{n-1-j} \\
\Rightarrow \quad \sum_{n=1}^{\infty} x^n t_n &= \sum_{n=1}^{\infty} x^n \sum_{j=0}^{n-1} t_j t_{n-1-j} \\
\Rightarrow \quad T(x) - t_0 &= \sum_{n=1}^{\infty} x \sum_{j=0}^{n-1} \left(t_j x^j\right) \left(t_{n-1-j} x^{n-1-j}\right)
\end{aligned}
$$

Changing Summation Order

$$
T(x) - t_0 = x \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} \left(t_j x^j\right) \left(t_{n-1-j} x^{n-1-j}\right)
$$



Sum over n from 1 to ∞, for each fixed value of n, sum over j from 0 to $n-1$.

Sum over j from 0 to ∞, for each fixed value of j, sum over n from $j+1$ to ∞.

$$
T(x) - t_0 = x \sum_{j=0}^{\infty} \sum_{n=j+1}^{\infty} \left(t_j x^j\right) \left(t_{n-1-j} x^{n-1-j}\right)
$$

Functional Equation for $T(x)$

Note: "Convergence" of the infinite sums is not an issue as they are *formal* power series. We only need the two forms to be equal term-by-term.

Using that $t_0 = 1$, and substituting $k = n - 1 - j$, we have

$$
\begin{aligned}
T(x) - 1 &= x \sum_{j=0}^{\infty} \sum_{n=j+1}^{\infty} \left(t_j x^j\right) \left(t_{n-1-j} x^{n-1-j}\right) \\
&= x \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \left(t_j x^j\right) \left(t_k x^k\right) \\
&= x \left(\sum_{j=0}^{\infty} t_j x^j\right) \left(\sum_{k=0}^{\infty} t_k x^k\right) \\
\Rightarrow \quad T(x) &= 1 + x \left(T(x)\right)^2
\end{aligned}
$$

Solving the Functional Equation for $T(x)$

- It is also possible to simply *write down* the equation for the generating function directly from the recursive definition of the binary tree.
- Getting a functional equation for the generating function is enough to be able to extract useful information.
- Here we are "lucky" and find a simple closed form expression for $T(x)$.

$$
\begin{aligned}
& T(x) = 1 + x\,(T(x))^2 \\
\Downarrow \quad & \\
& x\,(T(x))^2 - T(x) + 1 = 0 \\
\Downarrow \quad & \\
& T(x) = \frac{1 \pm \sqrt{1-4x}}{2x} \\
\Downarrow \quad & \\
& T(x) = \frac{1}{2x}\left(1 - \sqrt{1-4x}\right),
\end{aligned}
$$

choosing the branch with $t_0 = 1$.

Taylor Expansion of $T(x)$

To extract a closed form expression for t_n we perform a Taylor expansion of $T(x)$ around $x = 0$. In general, the Taylor expansion of a function $f(x)$ is

$$f(x) \;=\; \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n,$$

and the expansion for $f(x) = (1+x)^\alpha$ is

$$(1+x)^\alpha \;=\; \sum_{n=0}^{\infty} \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!} x^n.$$

Let $f(x) = \sqrt{1-4x} = (1-4x)^{1/2}$. Then

$$T(x) \;=\; \frac{1}{2x}\left(1 - \sum_{n=0}^{\infty} \frac{\frac{1}{2}\cdot\left(-\frac{1}{2}\right)\cdot\left(-\frac{3}{2}\right)\cdots\left(\frac{1}{2}-n+1\right)}{n!}(-4x)^n\right).$$

Taylor Expansion of $T(x)$

$$T(x) = \frac{1}{2x}\left(1 - \sum_{n=0}^{\infty} \frac{\frac{1}{2}\cdot(-\frac{1}{2})\cdot(-\frac{3}{2})\cdots(\frac{1}{2}-n+1)}{n!}(-4x)^n\right)$$

Pull out the first two terms from the infinite sum.

$$= \frac{1}{2x}\left(1 - \left(1 - 2x + \sum_{n=2}^{\infty} \frac{\frac{1}{2}\cdot(-\frac{1}{2})\cdot(-\frac{3}{2})\cdots(\frac{1}{2}-n+1)}{n!}(-4x)^n\right)\right)$$

$$= 1 - \frac{1}{2x}\left(\sum_{n=2}^{\infty} \frac{\frac{1}{2}\cdot(-\frac{1}{2})\cdot(-\frac{3}{2})\cdots(\frac{1}{2}-n+1)}{n!}(-4x)^n\right)$$

Manipulate all the 'minus' signs. n terms, $n-1$ are negative.

$$= 1 - \frac{1}{2x}\left(\sum_{n=2}^{\infty} \frac{(-1)^{n-1}\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots(n-\frac{3}{2})}{n!}(-1)^n(4x)^n\right)$$

Taylor Expansion of $T(x)$

$$T(x) = 1 + \frac{1}{2x}\left(\sum_{n=2}^{\infty} \frac{\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots(n-\frac{3}{2})}{n!}2^{2n}x^n\right)$$

$$= 1 + \sum_{n=2}^{\infty} \frac{\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots(n-\frac{3}{2})}{n!}2^{2n-1}x^{n-1}$$

Make the substitution $r = n-1$.

$$= 1 + \sum_{r=1}^{\infty} \frac{\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdots(r-\frac{1}{2})}{(r+1)!}2^{2r+1}x^r$$

Multiply each factor in numerator by 2. There are $r+1$ factors.

$$= 1 + \sum_{r=1}^{\infty} \frac{1\cdot 3\cdots(2r-1)}{(r+1)!}2^r x^r$$

Taylor Expansion of $T(x)$

$$T(x) = 1 + \sum_{r=1}^{\infty} \frac{1 \cdot 3 \cdots (2r-1)}{(r+1)!} 2^r x^r$$

Make numerator equal $(2r)!$. The missing terms are $2^r r!$

$$= 1 + \sum_{r=1}^{\infty} \frac{(2r)!}{2^r r!(r+1)!} 2^r x^r$$

$$= 1 + \sum_{r=1}^{\infty} \frac{1}{r+1} \binom{2r}{r} x^r$$

$$= \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} x^n$$

$$\Rightarrow \quad [x^n]\, T(x) = t_n = \frac{1}{n+1} \binom{2n}{n} = C_n.$$

43 More Catalania

More Catalania

We explore several combinatorial problems counted by Catalan numbers.

1. Balanced parentheses

2. Two row standard Young tableaux
3. Non-itersecting arches on $2n$ points

4. Triangulations of $n+2$ sided polygons.

How does one prove that these are counted by Catalan numbers?

1. Direct construction
2. Show the counting problem satisfies the Catalan recurrence
3. Bijection to a problem known to be Catalan

Balanced Parentheses

Definition 116 (Balanced Parentheses)**. Balanced parentheses** consists of open '(' and closed ')' parentheses such that any open parentheses has a matching closed parentheses.

Example: $n{=}1:$ (), $n{=}2:$ ()() (()), $n{=}3:$ ()()() (())() ()(()) (()()) ((())).

Note: The matching (or balanced) condition means that as we scan the parentheses from left to right the number of (parentheses is never less than the number of) parentheses.

Claim: Balanced parentheses are counted by Catalan numbers.

Proof: We shall show that the number b_n of balanced parentheses of size n satisfies the Catalan recurrence (i.e., the same recurrence as binary trees).

Consider $n = 3$. Note that the balanced parentheses fall into two sets.

- Indecomposable parentheses, e.g., $(()())$ or $((()))$.
- Parentheses composed from smaller components, e.g., $()()()$ or $()(())$.

Balanced Parentheses

How do we then construct all possible parentheses of size n?

Break them into two parts. The first indecomposable component and the rest.

$$\underbrace{(()(()))}_{\text{1st comp}}\underbrace{(())()(()())\cdots}_{\text{The rest}}$$

Look at indecomposable components. Remove first (and last). What is left?

Balanced parentheses one size smaller, but not necessarily indecomposable.

Construct parentheses as: $(A)B$ where *both* A and B are parentheses.

Parentheses of size n are parentheses of size $0 \leq j \leq n-1$ placed inside ( ) with parentheses of size $n-1-j$ added on. This leads to the recurrence:

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-2} b_1 + b_{n-1} b_0.$$

This is exactly the same recurrence as for binary trees (also need that $b_0 = 1$).

Another Catalan Application

Example: Six people are all of different heights, with the tallest denoted 6 down to the smallest denoted 1. List all the ways the people can be arranged into two rows of length three such that the heights increase along each row, and each person in the second row is taller than the person in the first row.

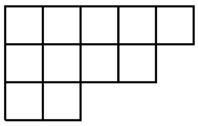
$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 4&5&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&3&4\\\hline 2&5&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&2&4\\\hline 3&5&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&3&5\\\hline 2&4&6\\\hline\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&2&5\\\hline 3&4&6\\\hline\end{array}$$

These are examples of *Standard Young Tableaux*

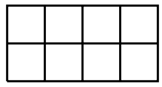
Young Diagrams – Integer Partitions

Definition 117 (Young Diagram)**.** A **Young diagram** is a finite collection of boxes, arranged in left-justified rows, with the row lengths weakly decreasing. The **shape** λ of a Young diagram is an ordered list of the lengths of the rows. The **size** of a Young diagram is the total number of boxes.

Example: Young diagrams:



Shape $\lambda = (5, 4, 2)$



Shape $\lambda = (4, 4)$

Note: A Young diagram of size n represents an **integer partition** of n, that is, n expressed as a sum of integers. The number of Young diagrams of size n equals the number of integer partitions of n. This is a fundamental problem in number theory.

Standard Young Tableux

Definition 118 (Standard Young Tableux)**.** A **Young tableau** is obtained by filling in the boxes of a Young diagram with symbols taken from some alphabet, which is usually required to be a totally ordered set, often just $\{1, 2, \dots, n\}$. In a **standard Young tableau** the entries are strictly increasing along both rows and columns.

Example:

$$\begin{array}{|c|c|c|c|c|}\hline a & c & d & f & h \\ \hline b & g & i & k & l \\ \hline e & j \\ \cline{1-2}\end{array} \qquad \begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 6 \\ \hline 2 & 5 & 7 & 8 \\ \hline\end{array}$$

Bijection to Parentheses

Claim: Two-row SYT of length n are in bijection to balanced parentheses.

Proof: Let $p_1 \dots p_{2n}$ denote a sequence of parentheses, i.e. $p_i \in \{(,)\}$.

Let $p_i =$ (, if i is in the first row, and let $p_i =$), if i is in the second row:

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & 6 \\ \hline\end{array} \mapsto ((())) \qquad \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 & 6 \\ \hline\end{array} \mapsto ()(()) \qquad \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 & 6 \\ \hline\end{array} \mapsto (()())$$

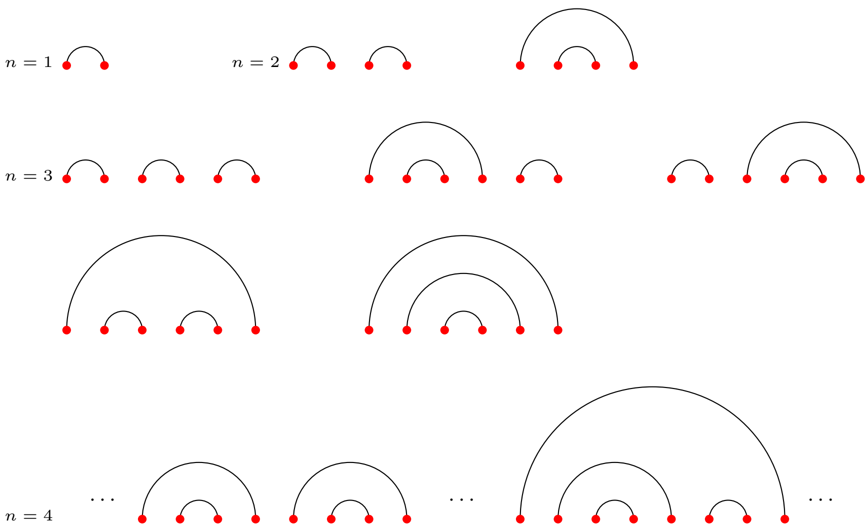
$$\begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 & 6 \\ \hline\end{array} \mapsto ()()() \qquad \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 & 6 \\ \hline\end{array} \mapsto (())()$$

Using the recurrence for parentheses one can now deduce (exercise!) the recurrence for the number T_n of two-row SYT's of length n:

$$T_n = T_0 T_{n-1} + T_1 T_{n-1} + \dots + T_{n-1} T_0.$$

Non-intersecting Arches Connecting $2n$ Points

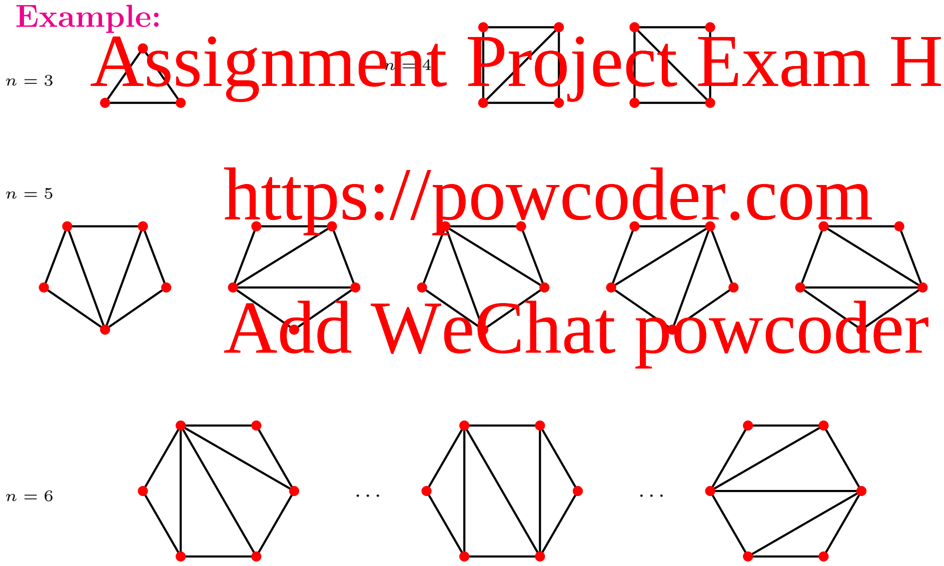
Example:



Bijection to parentheses is obvious.

Triangulations of $n+2$ Sided Polygons

Example:



Triangulations of $n+2$ Sided Polygons

Constructive Proof: Let $C_n = \#$ triangulations of $n{+}2$ sided polygons.

Note: At this stage we don't claim that C_n is a Catalan number.

Given a polygon P with $n+2$ sides. First mark one of its sides as the base. P is then triangulated. We can further choose and orient one of its $2n+1$ edges. There are $(4n+2)C_n$ such decorated triangulations.

Now given a polygon Q with $n+3$ sides. Again mark one of its sides as the base. If Q is triangulated, we can further mark one of the sides other than the base side. There are $(n+2)C_{n+1}$ such decorated triangulations.

There is a simple bijection between the two kinds of decorated triangulations: We can either collapse the triangle in Q whose side is marked, or in reverse expand the oriented edge in P to a triangle and mark its new side. Thus

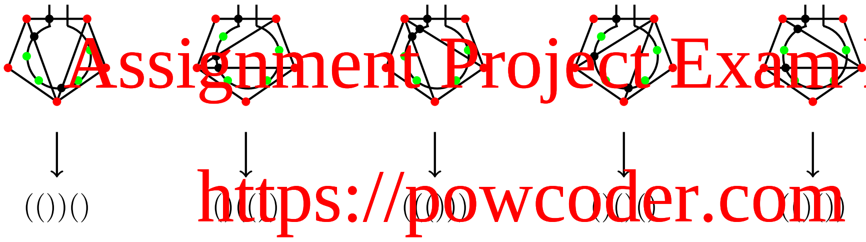
$$(4n+2)C_n = (n+2)C_{n+1}.$$

The formula for Catalan numbers follows from this relation and the initial condition $C_1 = 1$.

Triangulations of $n+2$ Sided Polygons

Bijective Proof: Bijection of polygons to parentheses:

1. Start at top edge of polygon. Step inside polygon and walk around the perimeter.
2. Each time an edge is **crossed** the first time record a '(' or $\bullet$.
3. Each time a polygon (outside) edge is **passed** record a ')' or $\bullet$.
4. Delete the last parentheses.



Geometric Series vs Catalan

We have seen that both the geometric series and Catalan generating function appears again and again as the solution to numerous combinatorial problems.

Why is this?

Let us look at the general structure of the combinatorial objects they count.

We are given a set of irreducible object A. Both the geometric series and Catalan series arise when we form large objects by concatenating objects from A, e.g., an objects could be:

$$a_1 a_2 a_3 \cdots a_{n-1} a_n$$

with each a_i chosen at random from A (including the empty object).

This explains the prevalence of these series. But why two cases?

- **Geometric:** This is the generating function in cases where $|\,A\,| = n$.
- **Catalan:** In this case $|\,A\,| = \infty$. To get the Catalan generating function the object in A need to have a 'nested or recursive inner structure'.

44 Asymptotic Results

Asymptotic Results

- The number of proper binary trees with n nodes is $t_n = \dfrac{1}{n+1}\dbinom{2n}{n}$.
- This is the n^{th} Catalan number.
- Is this a "good" answer?

  If you want to know the number of trees with 23 nodes, then yes.

  If you want to know whether, for example, $t_n > F_n^3$, then we would do better with an asymptotic formula.

  - $F_n = 0, 1, 1, 2, 3, 5, 8, \cdots$
  - $F_n^3 = 0, 1, 1, 8, 27, 125, 512, \cdots$
  - $t_n = 1, 1, 2, 5, 14, 42, 132, \cdots$

Asymptotic Results

We have

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

Using Stirling's formula for $n!$

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

we obtain

$$t_n \sim \frac{1}{n}\frac{\sqrt{2\pi 2n}\left(\frac{2n}{e}\right)^{2n}}{2\pi n\left(\frac{n}{e}\right)^{2n}} \sim \frac{4^n}{n^{3/2}\sqrt{\pi}}$$

- $t_n \sim \pi^{-1/2} n^{-3/2} 4^n$.
- We have $F_n \sim \phi^n \approx (1.618\cdots)^n$ which leads to $F_n^3 \sim (4.236\cdots)^n$.
- Thus, for sufficiently large n we see that F_n^3 is exponentially larger than t_n.

45 Asymptotics from Generating Functions

Asymptotics from Generating Functions

Recall the generating functions for Fibonacci and Catalan numbers:

$$F(x) \;=\; \sum_{n=0}^{\infty} F_n x^n \;=\; \frac{1}{1-x-x^2},$$

$$C(x) \;=\; \sum_{n=0}^{\infty} C_n x^n \;=\; \frac{1}{2x}\left(1-\sqrt{1-4x}\,\right).$$

In these expressions, x is a formal variable used for bookkeeping and the generating functions are to be interpreted as formal power series:

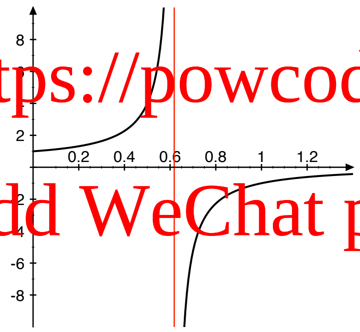
$$\frac{1}{1-x-x^2} \;=\; 1+x+2x^2+3x^3+5x^4+8x^5+\ldots$$

What if we were to interpret generating functions as real-valued functions? Or even complex valued functions?

Asymptotics from Generating Functions

If we interpret $\quad F(z) \;=\; \sum_{n=0}^{\infty} F_n z^n \;=\; \dfrac{1}{1-z-z^2},$

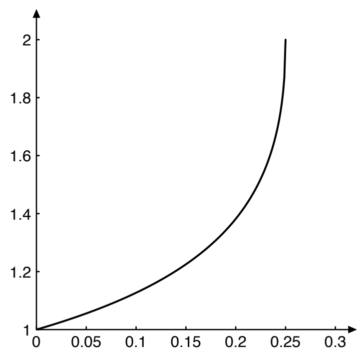
as a complex valued function, we have to worry about the convergence of the infinite series. Plot of the (real-valued) Fibonacci generating function:



This function has a pole at $x = 1/\phi = 0.618034\ldots$.

Asymptotics from Generating Functions

Plot of the (real-valued) Catalan generating function: $C(x) = \dfrac{1}{2x}\left(1-\sqrt{1-4x}\,\right)$



This function has a *singularity* (branch-point) at $x = 1/4$.

A complex function has a singularity at a point a if it is not analytic at a (i.e. if not all complex derivatives exist).

Asymptotics from Generating Functions

Recall that: $\quad F_n \sim \phi^n \quad$ and $\quad C_n \sim \pi^{-1/2} n^{-3/2} 4^n$.

The generating functions $F(x)$ and $C(x)$ have singularities at the inverse of the dominant asymptotic, i.e., at $x = 1/\phi$ and at $x = 1/4$, respectively.

More generally, if $G(x) = \sum_{n=0}^{\infty} g_n x^n$, the dominant asymptotics is determined by the singularity of $G(x)$ that is closest to the origin $x = 0$.

Asymptotics from Generating Functions

Many of the generating functions studied in combinatorics are believed to have algebraic singularities, though in many cases this has not been proved. That is to say, the generating function is believed to behave as

$$G(x) \sim A(1 - x/x_c)^{\theta} \text{ as } x \to x_c^-. \tag{1}$$

Hence it follows that

$$g_n = [x^n]G(x) \sim \frac{An^{-\theta-1}}{\Gamma(\theta) x_c^n}. \tag{2}$$

A is referred to as the *critical amplitude*, x_c as the *critical point* and θ as the *critical exponent*. It follows that the dominant asymptotic is μ^n where $\mu = 1/x_c$.

46 Functional Equations

Functional Equations

We have seen several examples that suggest that the best way to find a closed form solution for the generating functions of a sequence is to find a **functional equation** for the generating function.

Up till now we did this by finding a recurrence for the sequence and then solving this using generating functions.

Combinatorial Problems $\to$ Recurrences $\to$ Generating Functions $\to$ Functional Equations $\to$ Solutions

Here we wish to show that in many cases we can jump straight to the functional equation.

Combinatorial Problems $\to$ Functional Equations $\to$ Solutions

Definition 119 (Counting Variable)**.** By a **counting variable** we mean the variable, say z, used as a placeholder in a formal power series.

Functional Equation for Binomial Paths

Definition 120 (Binomial Paths)**. Binomial paths** are lattice paths in $\mathbb{N}_0^2$ with step set $S = \{(1,0),(0,1)\}$.

Let x be the counting variable for East steps and y for North steps.

Functional Equation for Binomial Paths:

$$B(x,y) = 1 + (x+y)B(x,y).$$

This equation 'reads': A binomial path is either an empty walk or it starts with a step along the x- or y-axis followed by any binomial path.

This functional equation is just a special case of the functional equation which arises by considering objects constructed entirely by concatenating elements from a finite set of basic units.

To get tilings with monomers and dimers set $x = z$, $y = z^2$, $B(x,y) = B(z)$.

To get tilings with tiles up to length k: $x+y \mapsto z+z^2+\cdots+z^k$, $B(x,y) = B(z)$.

Proper Binary Trees

Definition 121 (Proper Binary Trees)**.** A proper binary tree is either a leaf or a node with a left and a right tree.

Let x be the counting variable for the number of nodes in a binary tree.

The recursive definition then allows us to write down the functional equation:

$$T(x) = 1 + xT_L(x)T_R(x),$$

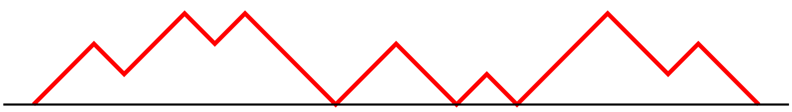
where '1' is the leaf, x is the node and attached to the node we have left and right trees. But the left and right trees are themselves just proper binary trees. So

$$T(x) = 1 + xT(x)^2.$$

Dyck Paths

Definition 122 (Dyck Path)**.** Consider **Dyck paths** as lattice paths in $\mathbb{N}_0^2$ with step set $S = \{(1,1),(1,-1)\}$ which start and end on the line $y = 0$.

Example:



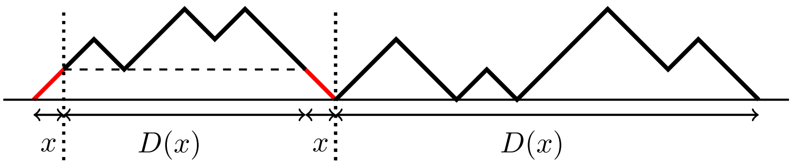
Theorem 123 (Dyck Path Generation Function)**.** *The number of Dyck paths of length $2n$ are the Catalan number C_n and hence the generating function $D(x)$ for Dyck paths is*

$$D(x) = \frac{1}{2x^2}\left(1 - \sqrt{1-4x^2}\right).$$

Dyck Paths

Proof: Partition (or factorise) a Dyck path at the **first** return to $y = 0$.

The left-most component is an **irreducible** Dyck path and the right-most component a Dyck path. Now, remove the first and last step of an irreducible Dyck path and the 'interior' is just another Dyck path. Pictorially we have:



Thus

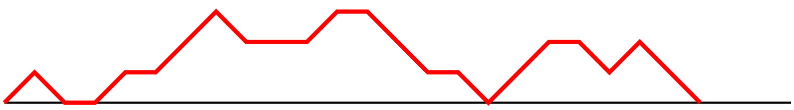
$$D(x) = 1 + x^2 D(x)^2 \implies D(x) = \frac{1}{2x^2}\left(1 - \sqrt{1-4x^2}\right).$$

Motzkin Paths

Definition 124 (Motzkin Path)**.** A **Motzkin path** is a lattice path in $\mathbb{N}_0^2$ with step set $S = \{(1,0),(1,1),(1,-1)\}$ which starts and ends on the line $y = 0$.

Note: The restriction to $\mathbb{N}_0^2$ means the path never goes below $y = 0$ (it is a ballot version of a more general path on $\mathbb{N}_0 \times \mathbb{Z}$).

Example:



Note: The associated Motzkin numbers also counts the number of ways of drawing any number of nonintersecting chords joining n (labeled) points on a circle; the number of standard Young tableaux of height ≤ 3, etc.

Motzkin Paths

Theorem 125 (Motzkin Path Generating Function)**.** *The generating function $M(x)$ for n-step Motzkin paths is*

$$M(x) \;=\; \frac{1}{2x^2}\left(1 - x - \sqrt{1-2x-3x^2}\right)$$

Proof by functional equation: 'Factorise' the path by first return to $y = 0$.

There are now two cases to consider:

Case 1: First step is $(1, 0)$. What follows is any Motzkin path so factor $xM(x)$.

Case 2: First step is $(1, 1)$. Akin to Dyck paths and gives factor $x^2M(x)^2$.

So we get:

$$M(x) = 1 + xM(x) + x^2M(x)^2.$$

Solve for $M(x)$ and choose the solution analytic at $x = 0$.

Motzkin Paths

Proof by Dyck paths (change of variable): We can also 'construct' Motzkin paths out of Dyck paths by a change of variable.

Consider the bijection from Dyck paths to parentheses. We get Motzkin paths by allowing **any** number of '$-$' to be inserted between the parentheses.

$$(()()()) \mapsto -(---()(---)---()-)--$$

The insertion of any number of '$-$' is given by a factor $1/(1-y)$. The change of variable $x \mapsto x/(1-y)$ takes care of every string of '$-$' except the first one . So

$$\begin{aligned} M(x, y) &= \frac{1}{1-y} D\left(\frac{x}{1-y}\right) \\ &= \frac{1}{1-y} \frac{(1-y)^2}{2x^2} \left(1 - \sqrt{1 - 4x^2/(1-y)^2}\right) \\ &= \frac{1}{2x^2} \left(1 - y - \sqrt{(1-y)^2 - 4x^2}\right). \end{aligned}$$

Motzkin Paths

But y was just a placeholder (or counting variable) for $(1, 0)$ steps.

If we don't want to distinguish steps we can set $y = x$ and elementary algebra gives us the result from the theorem.

But wait there is more!

x 'counts' the total number of steps.

For Motzkin paths we may ask a question such as 'what is the generating function when steps are weighted by their length'?

Now $(1, 0)$ steps have length 1 while $(1, 1)$ and $(1, -1)$ steps have length $\sqrt{2}$.

Thankfully, we kept track of the two types of step so we can easily answer the question. Just do $x \mapsto \sqrt{2}y$ and we get the generating function for Motzkin paths with length weighted steps:

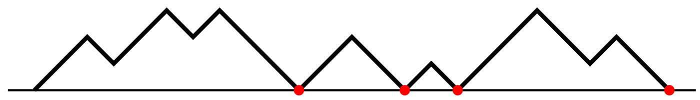
$$M(y) = \frac{1}{4y^2}\left(1 - y - \sqrt{1 - 2y - 7y^2}\right).$$

47 Dyck Paths

Dyck Paths by Returns to the Surface

Definition 126 (Dyck Paths at a Surface)**.** Consider **Dyck paths** as lattice paths in $\mathbb{N}_0^2$ with step set $S = \{(1,1),(1,-1)\}$ which start and end on the surface given by the line $y = 0$.

Example:



Theorem 127 (Dyck Path Generation Function)**.** *The generating function of Dyck paths of length n with k returns to $y = 0$ is*

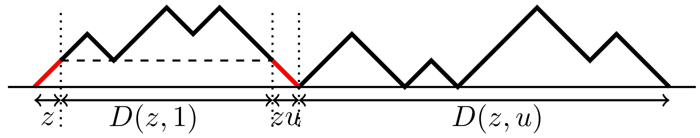
$$D(z,u) = \frac{2}{2 - u + u\sqrt{1 - 4z^2}}$$

where z 'counts' the number of steps and u the number of returns.

Dyck Paths by Returns to the Surface

Proof: Partition (or factorise) a Dyck path at the **first** return to $y = 0$.

Pictorially we have:



The left-most component is an **irreducible** Dyck path and the right-most component a Dyck path.

Now, remove the first and last step of an irreducible Dyck path and the 'interior' is a Dyck path. However, this path has no contacts with the surface.

The generating function for Dyck paths without contacts is $D(z,1) = D(z)$, where $D(z) = \frac{1}{2z^2}\left(1 - \sqrt{1 - 4z^2}\right)$.

Dyck Paths by Returns to the Surface

Thus

$$D(z,u) = 1 + uz^2 D(z,1) D(z,u) = 1 + uz^2 D(z) D(z,u)$$

$$\Downarrow$$

$$\begin{aligned} D(z,u) &= \frac{1}{1 - uz^2 D(z)} \\ &= \frac{1}{1 - u\frac{1}{2}\left(1 - \sqrt{1-4z^2}\right)} \\ &= \frac{2}{2 - u + u\sqrt{1-4z^2}} \\ &= 1 + uz^2 + (u+u^2)\,z^4 + (2u + 2u^2 + u^3)\,z^6 + \\ &\quad (5u + 5u^2 + 3u^3 + u^4)\,z^8 + \\ &\quad (14u + 14u^2 + 9u^3 + 4u^4 + u^5)\,z^{10} + \\ &\quad (42u + 42u^2 + 28u^3 + 14u^4 + 5u^5 + u^6)\,z^{12} + \cdots \end{aligned}$$

Singular Behaviour

Consider: $\quad D(z,u) = \dfrac{2}{2 - u + u\sqrt{1-4z^2}}$

The singularities (in z) of this function (may) depend on the parameter u.

Where is $D(z,u)$ singular?

Branch point from $\sqrt{1-4z^2}$ at $z = \frac{1}{2}$ or denominator is zero, i.e.,

$$2 - u + u\sqrt{1-4z^2} = 0 \quad \Rightarrow \quad \sqrt{1-4z^2} = \frac{u-2}{u}.$$

Since $\sqrt{1-4z^2} \geq 0$ we must have $u \geq 2$ for this to be relevant.

Solving for z gives $\quad z = \dfrac{\sqrt{u-1}}{u} < \dfrac{1}{2}, \quad u > 2.$

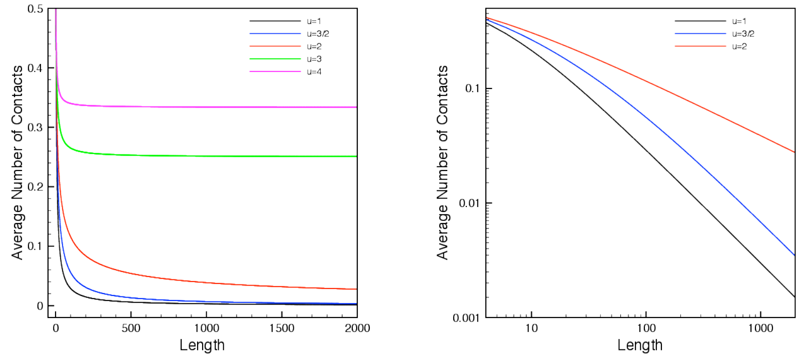
So the series for $D(z,u)$ (with u fixed) has dominant asymptotic

$$\mu = \begin{cases} 2 & u \leq 2 \\ \dfrac{u}{\sqrt{u-1}} & u > 2. \end{cases}$$

Average Number of Contacts

Let $D_m(z,u) = \left(u\frac{\mathrm{d}}{\mathrm{d}u}\right)^m D(z,u)$. A basic physical quantitiy of the model is the average number of contacts at a fixed length and fixed value $u = u_0$

$$\langle k \rangle = \frac{1}{n}\frac{[z^n]D_1(z,u_0)}{[z^n]D(z,u_0)}.$$

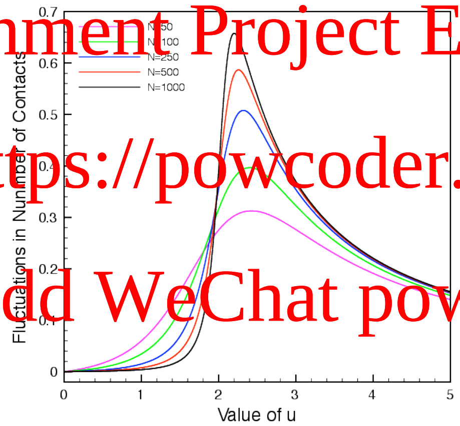


We see $\langle k \rangle \to 0$ for $u \leq 2$ and $\langle k \rangle \to$ constant > 0 when $u > 2$.
Furthermore, $\langle k \rangle \simeq 1/n,\ u < 2; \quad 1/n^{1/2},\ u = 2.$

Fluctuations of Number of Contacts

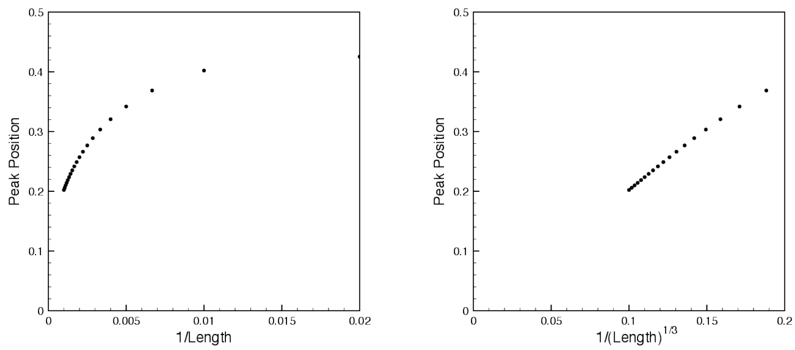
For fixed n a quantity of interest is the fluctuations in the number of contacts:

$$\chi(u) = \frac{1}{n}\left(\langle k^2 \rangle - \langle k \rangle^2\right)$$



Fluctuations of Number of Contacts – Peak Position

Expect position of peak u_p to approach the critical values $u = u_c = 2$.



Figures show $u_p - 2$ against $1/n$ and $1/n^{1/3}$.

48 Parenthesised Expressions

Parenthesised Expressions

Recall the 'construction' of Motzkin paths from Dyck paths by a change of variable. Consider the bijection from Dyck paths to parentheses.

We get the Motzkin path generating function by allowing *any* number of '•' to be inserted between the parentheses, e.g.,

$$(()())() \quad \to \quad \bullet(\bullet\bullet(\bullet)(\bullet\bullet\bullet)\bullet)\bullet\bullet(\bullet)\bullet\bullet$$

The insertion of any number of '•' is given by a factor $1/(1-b)$. The change of variable $z \mapsto z/(1-b)$ takes care of every string of '•' except the first one. So

$$M(z,b) \quad = \quad \frac{1}{1-b} D\left(\frac{z}{1-b}\right)$$

Now if we want 'properly' parenthesised expressions it is not 'natural' to allow symbols outside the parenthesis.

Can we fix this? Oh yes we can!

Parenthesised Expressions

The problem arises in terms such as

$$(\bullet(\bullet))\bullet\bullet()$$

that is where a '•' is inserted after the first set parenthesis was closed.

NOTE this is exactly when a Dyck path returns to the surface!

If we take our paths with returns, counted by generating function $D(z,u)$, then we can use u to fix the problem of counting 'illegal' configurations.

A factor of u occurs whenever the path returns to the surface OR (and this is the crucial observation) **when a set of parenthesis are properly closed**.

We can 'cancel' or 'delete' the offending strings of '•' by setting $u = (1-b)$ and $z = z/(1-b)$.

Here the change $z \mapsto z/(1-b)$ as before inserts a string of '•' after *every* parenthesis while $u \mapsto (1-b)$ deletes the ones we don't want.

Parenthesised Expressions

So

$$
\begin{aligned}
P(z) &= D\left(\frac{z}{1-z}, 1-z\right) \\
&= \frac{2}{2-(1-z)+(1-z)\sqrt{1-4z^2/(1-z)^2}} \\
&= \frac{2}{1+z+\sqrt{1-2z-3z^2}} \\
&= 1+z^2+z^3+3z^4+6z^5+15z^6+36z^7+91z^8+\cdots
\end{aligned}
$$

counts the number of parenthesised expressions where there is a factor z for each parenthesis and '•'.

Parenthesised Expressions

You may object that it is not natural to have empty parenthesis.

And you would be quite right! So let us try to fix that too.

We distinguish between opening and closing parenthesis.

In $D(z,u)$ we only have the factor z^2. This really represents an opening and closing parenthesis. We can replace the term z^2 by xy, where x counts opening parenthesis and y closing parenthesis.

We then have

$$
D(x,y,u) = \frac{2}{2-u+u\sqrt{1-4xy}}
$$

Two cases arise naturally: We count **both** parenthesis and '•' or **only** '•'.

Parenthesised Expressions

If we count both then we make the substitutions:

$$
x \mapsto \frac{xb}{1-b}, \quad y \mapsto \frac{y}{1-b}, \quad u \mapsto (1-b).
$$

If we don't care to distinguish between parenthesis and '•' then

$$
x \mapsto \frac{z^2}{1-z}, \quad y \mapsto \frac{z}{1-z}, \quad u \mapsto (1-z)
$$

so

$$
\begin{aligned}
P(z) &= D\left(\frac{z^2}{1-z}, \frac{z}{1-z}, 1-z\right) \\
&= \frac{2}{2-(1-z)+(1-z)\sqrt{1-4z^3/(1-z)^2}} \\
&= \frac{2}{1+z+\sqrt{1-2z+z^2-4z^3}} \\
&= 1+z^3+z^4+z^5+3z^6+6z^7+10z^8+\cdots
\end{aligned}
$$

Parenthesised Expressions

If we only count '•' then we make the substitutions:

$$x \mapsto \frac{b}{1-b}, \quad y \mapsto \frac{1}{1-b}, \quad u \mapsto (1-b)$$

and if we now set $b = z$ we get

$$
\begin{aligned}
P(z) &= D\left(\frac{z}{1-z}, \frac{1}{1-z}, 1-z\right) \\
&= \frac{2}{2-(1-z)+(1-z)\sqrt{1-4z/(1-z)^2}} \\
&= \frac{2}{1+z+\sqrt{1-6z+z^2}} \\
&= 1+z+3z^2+11z^3+45z^4+197z^5+903z^6 \\
&\quad +4279z^7+20793z^8+\cdots
\end{aligned}
$$

49 Penrose Tilings

Penrose Tilings

- The Fibonacci substitution sequence is generated by the rules $a \to A$ and $A \to Aa$, with initial string $S_1 = a$.
- Today we are going to study recursively defined geometric structures called *Penrose tilings* (tiles outside western entrance of Peter Hall).
- We derive a substitution rule to create a tiling of the plane which has five-fold symmetry (not possible for lattices to have five-fold symmetry).
- This forms a two-dimensional *quasicrystal*; with long range order, but no translational invariance. 3-dimensional quasicrystals are seen in nature.

Penrose Tilings

- There are various formulations, but one formulations has triangles A and B with dimensions and substitution rules derived below.
- Further reading: `http://en.wikipedia.org/wiki/Quasicrystal` `http://en.wikipedia.org/wiki/Penrose_tiling` `http://en.wikipedia.org/wiki/Pinwheel_tiling` (as seen at Federation square)

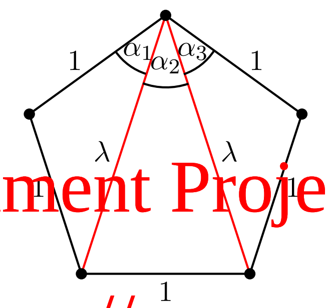
  Tilings Encyclopedia

  `http://tilings.math.uni-bielefeld.de`

  Well worth a visit if only for the beautiful pictures!

Some Geometry

Given the regular pentagon below, what is α_j and λ?

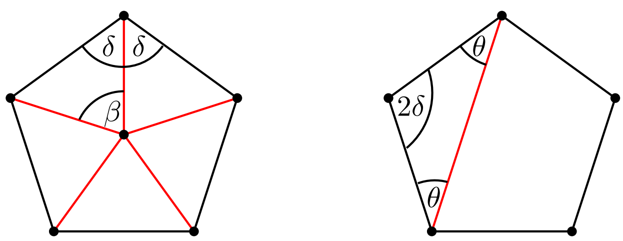


Theorem 128. *1.* $\alpha_1 = \alpha_2 = \alpha_3 = \pi/5$.

2. $\lambda = \frac{1}{2}(1+\sqrt{5}) = \phi$ *(The golden ratio)*

Some Geometry

Proof: $\boxed{1}$ By symmetry we have $\alpha_1 = \alpha_3 = \theta$. Now consider



We have from the left-most figure $5\beta = 2\pi$ and $2\delta + \beta = \pi \quad \Rightarrow \quad 2\delta = 3\pi/5$.

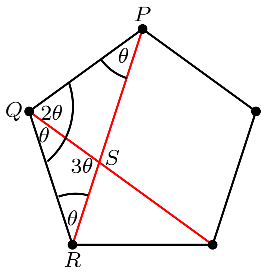
From the right-most figure we have $2\delta + 2\theta = \pi \quad \Rightarrow \quad \theta = \pi/5$.

Thus $\alpha_2 = 2\delta - 2\theta = 3\pi/5 - 2\pi/5 = \pi/5$ and hence

$$\alpha_1 = \alpha_2 = \alpha_3 = \pi/5.$$

Some Geometry

Proof: $\boxed{2}$ We use similar triangles and consider



$\triangle PQR \cong \triangle QSR$ (angles the same). $\triangle QPS$ is isosceles so $|PS| = 1$.
Let $|PR| = \lambda$ and $|RS| = \lambda'$, then (using $1 + \lambda' = \lambda$)

$$\frac{|QR|}{|RS|} = \frac{|PR|}{|QR|} \Rightarrow \frac{1}{\lambda'} = \lambda \Rightarrow \lambda\lambda' = 1 \Rightarrow \lambda(\lambda - 1) = 1 \Rightarrow \lambda = \frac{1}{2}\left(1 + \sqrt{5}\right).$$

Note: We have $\lambda^2 = \lambda + 1$.

Tiles and Tilings

Definition 129 (Tiles and Tilings)**.**

- A **tile** is the interior of some region in $\mathbb{R}^2$.
- A **tiling** of $\mathbb{R}^2$ is a (countable) set of tiles which is a **covering** (their union is $\mathbb{R}^2$) and a **packing** (the intersection of any pair of tiles is empty).

This definition is obviously very general. To be a little more concrete we shall create a tiling via the following procedure:

Algorithm 130 (Tiling)**.**

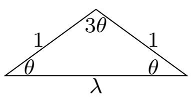
1. Start with an initial set of tiles $\{T_1, T_2, \cdots, T_n\}$.
2. Scale each tile: $\{T_1, T_2, \cdots, T_n\} \mapsto \{Q(T_1), Q(T_2), \cdots, Q(T_n)\}$
3. Subdivide scaled tiles: $Q(T_j) \mapsto \{T_{j_1}, T_{j_2}, \cdots, T_{j_k}\}$
4. Repeat 2 and 3 ad infinitum.

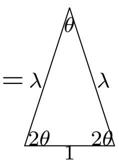
Note: The scaling must increase the size of the tiles.

Penrose Tiling

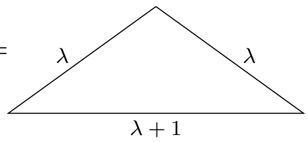
Back to the triangles of our pentagon:

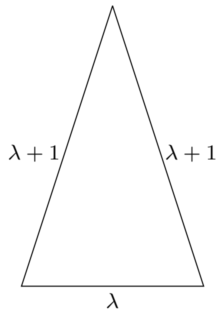
Initial tiles:

$A =$ 

$B =$ 

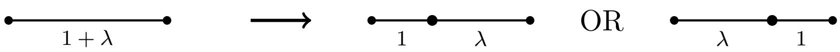
Q: Scale by λ (i.e. inflate as $\lambda > 1$) and use $\lambda^2 = \lambda + 1$:

$Q(A) =$ 

$Q(B) =$ 

Penrose Tiling

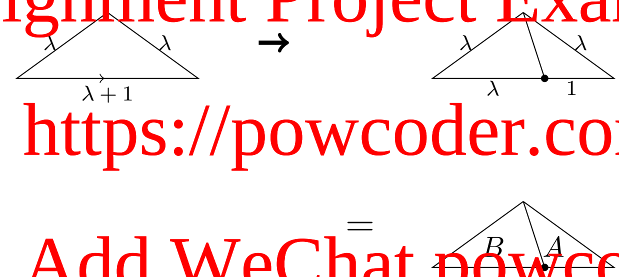
Subdivide the "$1 + \lambda$" side of the triangles:



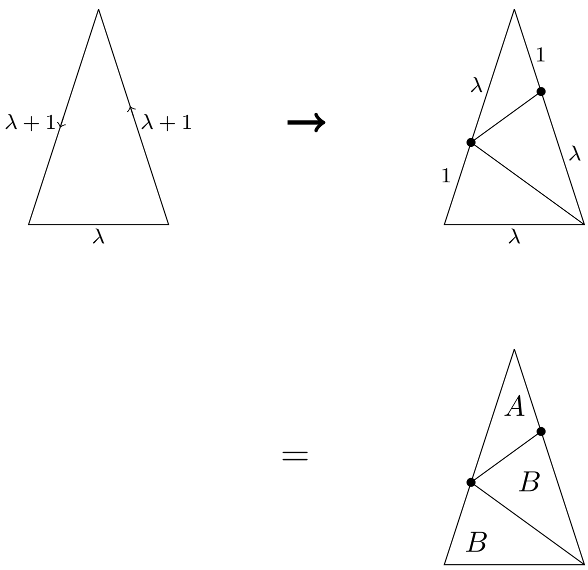
The choice of which way to subdivide leads to *many* different tilings of $\mathbb{R}^2$.

Use arrows to indicate which of the two subdivisions to choose.

Arrow points to the shorter length.

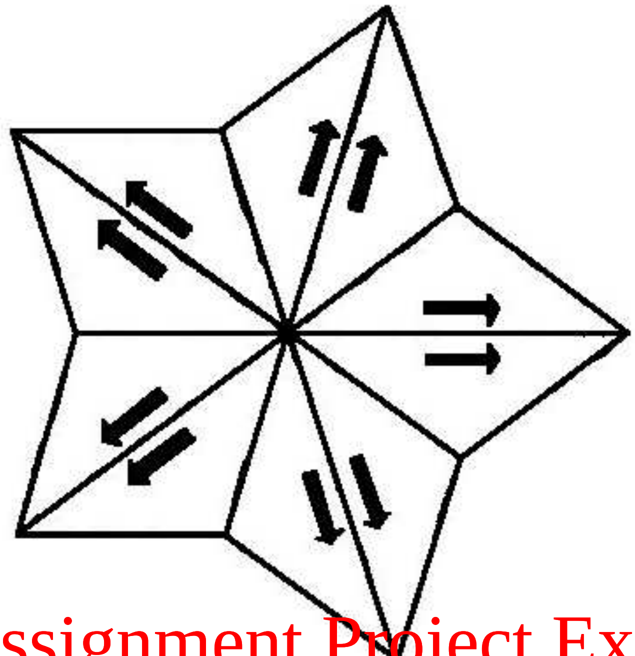
$Q(A)$: 

Penrose Tiling

$Q(B)$: 

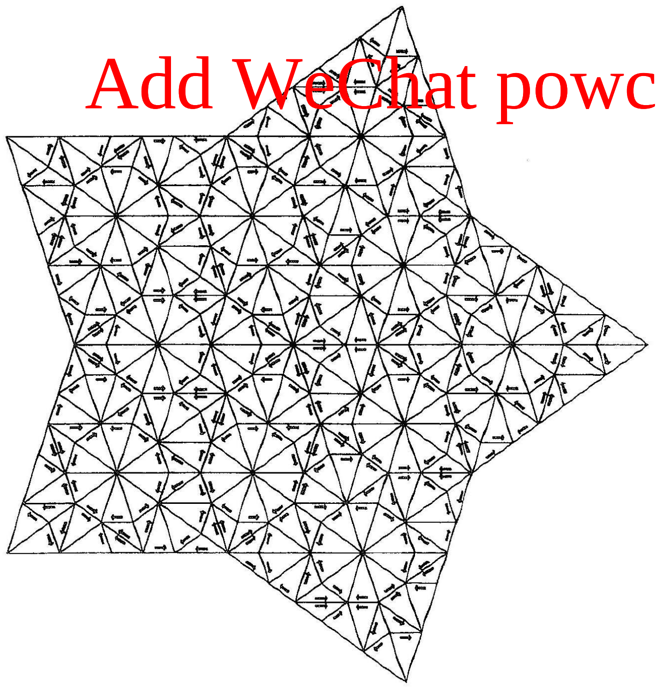
Penrose Tiling

We start with a five-fold symmetric configuration of type A triangles.



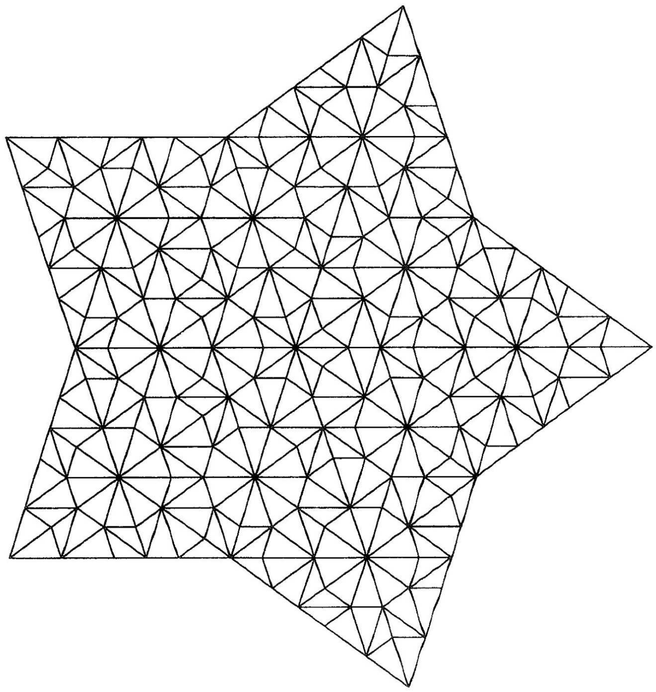
Penrose Tiling

And after successive substitutions we obtain:



Penrose Tiling

Dropping the arrows gives the aperiodic tiling:



Penrose Tiling

How many A and B triangles are there after n substitutions?

$A \to AB$, $B \to ABB$, and therefore

$$\begin{aligned} A_{n+1} &= A_n + B_n \\ B_{n+1} &= A_n + 2B_n. \end{aligned}$$

In matrix form

$$\begin{pmatrix} A_{n+1} \\ B_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} A_n \\ B_n \end{pmatrix}$$

We have initial conditions $A_0 = 10$, $B_0 = 0$, thus

$$\begin{pmatrix} A_n \\ B_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n \begin{pmatrix} 10 \\ 0 \end{pmatrix}$$

Penrose Tiling

What is $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n$? The first few iterates are

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \quad \begin{pmatrix} 5 & 8 \\ 8 & 13 \end{pmatrix} \quad \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix} \quad \cdots$$

Lets *guess* that

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n = \begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix}$$

This leads to

$$\begin{pmatrix} A_n \\ B_n \end{pmatrix} = \begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix} \begin{pmatrix} 10 \\ 0 \end{pmatrix} = 10 \begin{pmatrix} F_{2n-1} \\ F_{2n} \end{pmatrix}$$

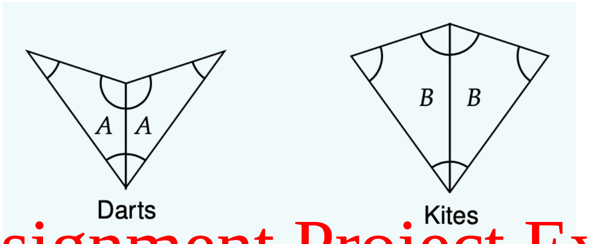
Thus as we perform more iterations

$$\lim_{n\to\infty} \frac{B_n}{A_n} = \lim_{n\to\infty} \frac{F_{2n}}{F_{2n-1}} = \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\phi^{2n}}{\frac{1}{\sqrt{5}}\phi^{2n-1}} = \phi.$$

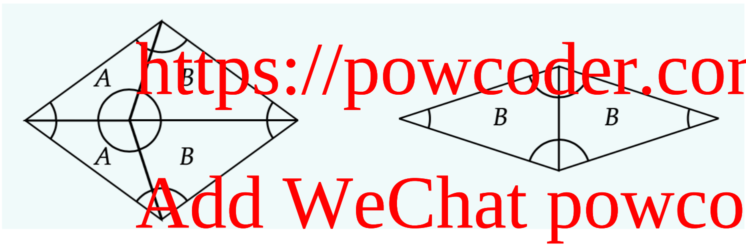
The ratio between the two types of triangles approaches the golden ratio.

Penrose Tiling

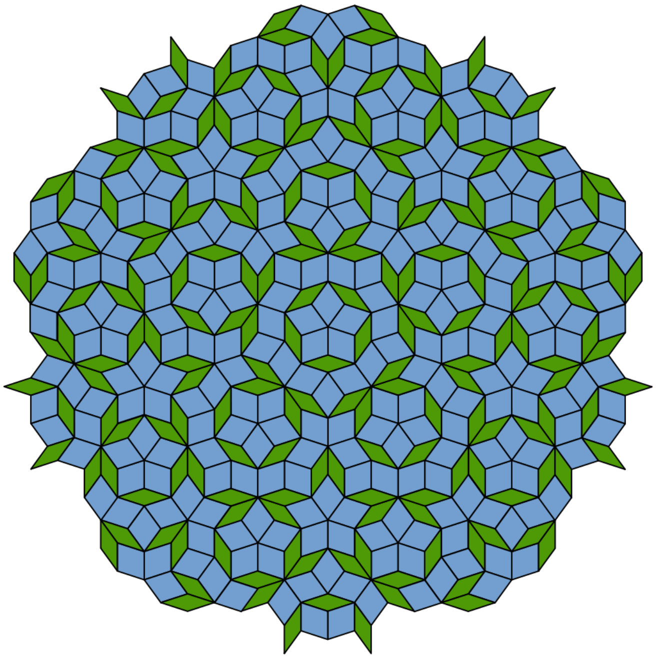
The elementary shapes in the original formulation of the Penrose tiling are



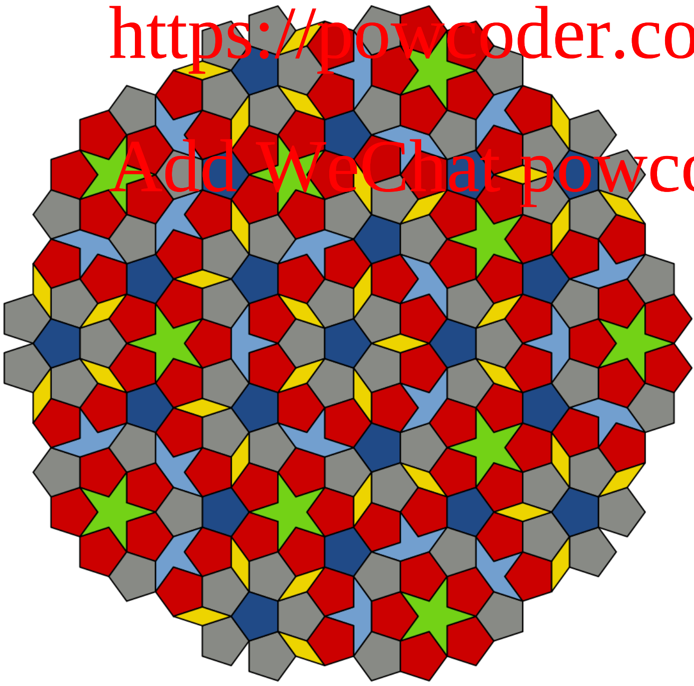
On the RMIT building the elementary shapes are rhombi



Penrose Tiling



Penrose Tiling
One final image



50 Permutations

Permutations and Bijective Maps

Definition 131 (Permutation)**.** A **permutation** of $N = \{1, 2, 3, \ldots, n\}$ is an arrangement or n-tuple

$$(\sigma_1, \sigma_2, \cdots, \sigma_n) \qquad \sigma_i \in N, \qquad \sigma_i \neq x_j \ \forall i \neq j$$

such that each $i \in N$ occurs exactly once.

Definition 132 (Permutations as Bijective Maps)**.** A permutation can be viewed as a bijective map on $N = \{1, 2, 3, \ldots, n\}$

$$\sigma : N \mapsto N, \qquad \sigma \text{ bijective, i.e., one-to-one onto.}$$

Notation: We write $\sigma : i \mapsto \sigma_i$ or $\sigma : i \mapsto \sigma(i)$.

Example: If σ maps: $1 \mapsto 2,\ 2 \mapsto 4,\ 3 \mapsto 1,\ 4 \mapsto 3$ then we may write

$$\sigma = (2, 4, 1, 3) \qquad \text{(or just 2413)}$$

Note: Recall that there are $n!$ permutations or arrangements of n objects.

51 Two-line Arrays

Permutations as Two-line Arrays

Notation 133 (Two-line Arrays)**.** A permutation can be encoded in a **two-line array**, telling us where elements in position j are mapped to

$$\begin{pmatrix} 1 & 2 & \cdots & j & \cdots & n \\ \sigma_1 & \sigma_2 & \cdots & \sigma_j & \cdots & \sigma_n \end{pmatrix} \quad \begin{array}{l} \leftarrow \text{ original positions, in order} \\ \leftarrow \text{ new positions} \end{array}$$

Example: For the above example we have

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

For our example there are $4!$ different two-line arrays, corresponding to permutations of $1, 2, 3, 4$ in the bottom line.

For n positions (objects) there are $n!$ possible orderings in the second line $\Rightarrow n!$ two-line arrays.

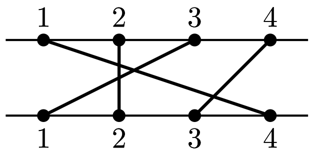
Permutations as Bipartite Graphs

Definition 134 (Bipartite Graph)**.** A graph G is **bipartite** if the vertices $V(G)$ can be partitioned into two subsets $V_1 \neq \emptyset$ and $V_2 \neq \emptyset$ such that for all edges, $e = v_1 v_2 \in E(G)$, $v_1 \in V_1$, $v_2 \in V_2$. That is, every edge joins a vertex of V_1 and a vertex of V_2.

Example: Permutations can be represented on bipartite graphs. Consider

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

This permutation can be depicted as



Note: The horizontal line is there as a 'guide to the eye'.

Exercises

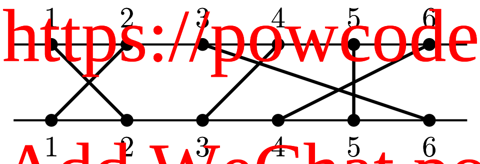
Example: Give in two-line notation the permutation σ with the action

$$\sigma : \ (a, b, c, d, e, f) \ \mapsto \ (b, a, f, c, e, d).$$

Solution:

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

Example: Give the above permutation as a bipartite graph:



52 Cycle Notation

Permutations in Cycle Notation

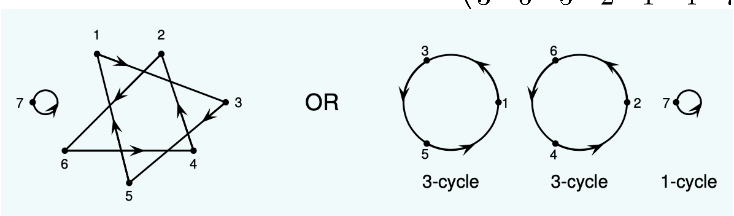
A notation which is often more convenient is so-called cycle notation.

To see where this comes from we represent permutations as directed graphs.

Definition 135 (Permutation as Directed Graph)**.** Draw a directed graph (edges have arrows on them) with n vertices and an arc (directed edge) from vertex i to vertex $j = \sigma_i$.

Example:

Consider the permutation: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 2 & 1 & 4 & 7 \end{pmatrix}$



Note: Every vertex has exactly one 'in' arc and one 'out' arc.

Cycle Notation

Definition 136 (k-cycle)**.** A k-cycle is a cyclic mapping of length k that takes an element back to itself:

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \mapsto a_1$$

Notation: The k-cycle is written as $(a_1 a_2 a_3 \cdots a_k)$.

Example: From the above example we have

$$1 \mapsto 3 \mapsto 5 \mapsto 1 = (135); \quad 2 \mapsto 6 \mapsto 4 \mapsto 2 = (264); \quad 7 \mapsto 7 = (7).$$

$$\Rightarrow \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 2 & 1 & 4 & 7 \end{pmatrix} = (135)(264)(7).$$

Note: We often express permutations as "products" of disjoint cycles. Here are some more examples:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1243) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 4 & 1 \end{pmatrix} = (15436)(2)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24) \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix} = (135)(264)$$

Cycle Notation

- The start of a cycle is *not* important.

  $(2314), (4231), (1423)$ and (3142) are all the same cycle.

  So a k-cycle can be written in k ways (all cyclic permutations).

- If a permutation contains several cycles it is written as a 'product' of disjoint cycles, e.g., $\sigma = 21435 = (12)(34)(5)$

- Cycles are disjoint $\Rightarrow$ each $i \in N$ occurs in *exactly one* cycle.

- Since there are k ways to write any k-cycle and $r!$ ways to arrange or order the cycles in any product of r cycles it is convenient to have a standard way for writing down a cycle form.

Definition 137 (Fixed Points and Transpositions)**.**

1. 1-cycles are called **fixed points**.
2. 2-cycles are called **transpositions**.
3. If 2-cycle is $(i\, i{+}1)$ it is called an **elementary** or **simple** transposition.

Standard Cycle Form

Definition 138 (Standard Cycle Form)**.**

1. Of the k ways to write a k-cycle choose the one which starts with the smallest member.

2. Order the product so the cycle starting with lowest number is to the left, then write down the cycle involving the next lowest number and so on until all elements are exhausted.

3. Omit any 1-cycles.

This "prescription" makes cycle notation unique ($\star$ is standard form):

$$\begin{aligned}
&(123)(456)\star = (456)(123)\\
&(1)(25)(3)(46) = (25)(46)\star = (52)(1)(64)(3)\\
&(456123) = (123456)\star
\end{aligned}$$

Note: In standard form omitted 1-cycles may mean n has to be specified.

$$\sigma = (12)(34) = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} \quad (n=4) \quad \text{but} \quad \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 4 & 3 & 5\end{pmatrix} \quad (n=5)$$

53 Composition of Permutations

Composition of Permutations

Since permutations can be considered to be maps we can form compositions.

Definition 139 (Composition of Permutations)**.** Let τ and σ be permutations of $N = \{1, 2, \ldots, n\}$. The **composition** of τ and σ, $\alpha = \tau \circ \sigma$, is a permutation of N defined as

$$\alpha : i \mapsto \alpha(i) \;=\; \tau(\sigma(i)).$$

Note: σ is applied first, then τ. Often we drop the '$\circ$' and talk of "products".

Given σ and τ we can compute $\alpha = \tau \circ \sigma$ using any representation.

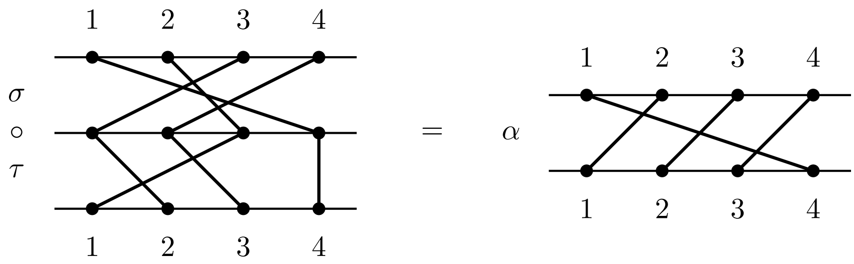
Example: Let $\sigma = (4, 3, 1, 2)$ and $\tau = (2, 3, 1, 4)$ then

$$\begin{aligned}
\alpha : 1 &\mapsto \tau(\sigma(1)) = \tau(4) = 4\\
\alpha : 2 &\mapsto \tau(\sigma(2)) = \tau(3) = 1\\
\alpha : 3 &\mapsto \tau(\sigma(3)) = \tau(1) = 2\\
\alpha : 4 &\mapsto \tau(\sigma(4)) = \tau(2) = 3\\
&\Rightarrow \alpha = (4, 1, 2, 3)
\end{aligned}$$

Composition or Multiplication of Bipartite Graphs

Multiplication in graph notation is easily done by top to bottom concatenation:

With $\sigma = (4, 3, 1, 2)$ and $\tau = (2, 3, 1, 4)$ we have:



Composition or Multiplication of Two-line Arrays

We can multiply (compose) two-line arrays, e.g.

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

When acting on arrangement of objects, the rightmost "permutation" acts first.

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

For this example we have $1 \to 4 \to 4$, $\quad 2 \to 3 \to 1$, $\quad 3 \to 1 \to 2$, $4 \to 2 \to 3$.

We can express the resulting permutation in a two-line array:

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

Composition or Multiplication in Cycle Notation

In standard cycle notation we have

$$\sigma = (4, 3, 1, 2) = (1423) \qquad \tau = (2, 3, 1, 4) = (123)$$

For the multiplication put back in the (4) in τ so

$$\alpha = (123)(4) \circ (1423) = (1432)$$

We read of the action: $1 \mapsto 4 \mapsto 4, 4 \mapsto 2 \mapsto 3, 3 \mapsto 1 \mapsto 2, 2 \mapsto 3 \mapsto 1$.

Example: What is $\sigma \circ \tau = (1423) \circ (123)(4)$?

54 Inverse permutations

Identity and Inverse Permutations

Definition 140 (Identity and Inverse Permutations)**.** The **identity** permutation, denoted σ_{I} or "id", is:

$$\sigma_{\mathrm{I}} \;=\; (1,2,3,\ldots,n) \;=\; \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}, \cdots$$

Since σ is a bijection it has an **inverse** σ^{-1} defined by

$$\sigma \circ \sigma^{-1} \;=\; \sigma^{-1} \circ \sigma \;=\; \sigma_{\mathrm{I}}$$

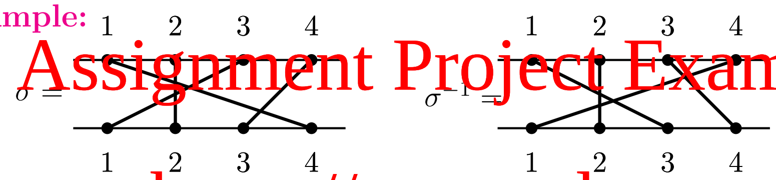
Next we consider:

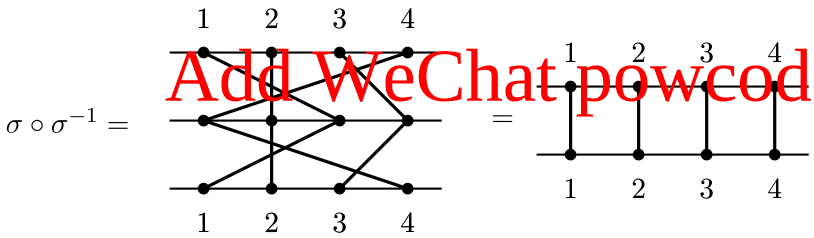
- Given σ in various representations; compute σ^{-1}.
- For each representation there is a simple way to compute σ^{-1}.

Inverse Permutations from Bipartite Graphs

Procedure 141 (Inverse Permutation from Bipartite Graph)**.** Given a bipartite graph of a permutation σ we get the inverse permutation σ^{-1} by "reading" the graph backwards.

Example:





Inverse Permutations from Two-line Arrays

Procedure 142 (Inverse Permutation from Two-line Array)**.** Given a two-line array of a permutation σ we get the inverse permutation σ^{-1} by "reading" the two-line array from bottom to top.

Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 5 & 4 \end{pmatrix} \quad \Rightarrow \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$$

Exercise: Check that $\sigma \circ \sigma^{-1} \;=\; \sigma^{-1} \circ \sigma \;=\; \sigma_{\mathrm{I}}$

Inverse Permutations from Cycles

Procedure 143 (Inverse Permutation from Cycles)**.** Given a permutation σ in standard cycle form we get the inverse permutation σ^{-1} by "reading" each cycle backwards, i.e., from right to left.

Example: σ^{-1} is obtained by 'reversing the arrows' in cycle notation.

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_k \mapsto a_1$$

becomes

$$a_1 \mapsto a_k \mapsto a_{k-1} \mapsto \cdots \mapsto a_2 \mapsto a_1$$

So

$$\sigma = (1357)(24) \quad \Rightarrow \quad \sigma^{-1} \;=\; (7531)(42) \;=\; (1753)(24)$$

Note: The inverse of a 2-cycle is the same 2-cycle.

55 Involutions

Involutions

Definition 144 (Involution)**.** A permutation σ which contains only 1-cycles and 2-cycles is an **involution**.

Theorem 145 (Basic Involution Property)**.** *If σ is an involution then $\sigma^2 = \sigma_{\mathrm{I}}$ and $\sigma = \sigma^{-1}$.*

Proof: A 1-cycle is already the identity.

We showed above that the inverse of a 2-cycle is the same 2-cycle.

Now σ is a product of 1- and 2-cycles so each factor in $\sigma \circ \sigma = \sigma^2$ becomes the identity on these 1 or 2-cycles.

So σ^2 leaves every element in place and hence is the identity.

Fixed Point Free Involutions

Theorem 146 (Fixed Point Free Involutions)**.** *The number of fixed point free involutions of $N = \{1, 2, 3, \ldots, n\}$ is*

$$(n-1)!! := (n-1)(n-3)(n-5)\cdots 3 \cdot 1$$

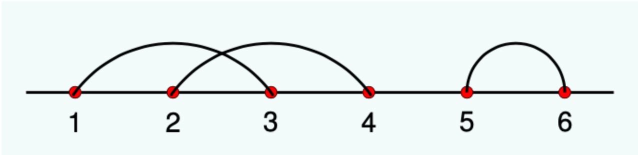
Note: n must be even.

Proof (outline): Since σ is fixed point free (it has no 1-cycles) all $i \in N$ are part of some 2-cycle $(i\,\sigma_i)$.

Represent σ by a "dot-link" diagram (which is a line with n dots where the dots are connected by "arcs" or edges above the line).

Link set $= \{\, (i\,\sigma_i) \mid i \in N,\ i < \sigma_i\}$.

Example: $\sigma = (13)(24)(56)$



Fixed Point Free Involutions

We calculate the number of such link-dot diagrams as:

- First link dot at position 1 to any of the remaining $n-1$ dots.
- Among the remaining $n-2$ dots take the one in the left-most position and link to any of the remaining $n-3$ dots.
- Next from the remaining $n-4$ dots take the one in the left-most position and link to any of the remaining $n-5$ dots.
- etc. etc.

$$\Rightarrow |\text{Link set}| = (n-1)(n-3)(n-5)\cdots 3\cdot 1 = (n-1)!! \quad (n \text{ even})$$

(Use induction to do a proper proof.)

56 Stirling numbers

Counting Cycles

Definition 147 (S_n)**.** Let S_n be the set of all permutations of $N = \{1, 2, 3, \ldots, n\}$.

Definition 148 (Stirling Numbers)**. Stirling numbers** of the first kind, $S_1(n,k)$ are defined as the number of permutations $\sigma \in S_n$ with exactly k disjoint cycles (in standard form).

Example: $n = 4,\ k = 2:\quad S_1(4,2) = 11.$

(123)(4), (132)(4), (124)(3), (142)(3), (134)(2), (143)(2), (1)(234), (1)(243),

(12)(34), (13)(24), (14)(23).

Example: List all permutations of S_4 which consist of a single cycle.

$$\begin{array}{ccc} (1234) & (1243) & (1324) \\ (1342) & (1423) & (1432) \end{array}$$

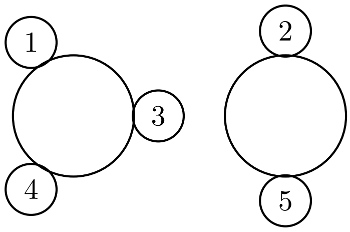
i.e. fix 1, and then consider all possible orderings of $2, 3, 4$.

Seating Arrangements

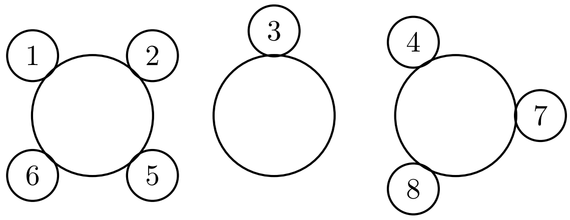
An equivalent representation is that $S_1(n,k)$ counts the number of ways of seating n people at k round tables, where the tables are indistinguishable, no table is empty, and we only care about the order of people around the table.

Example:

$(134)(25)\ =$



$(1256)(3)(478)\ =$



Special Values of Stirling Numbers

1. $S_1(n,k) = 0,\ k > n$ or $k < 0$.

   By convention, but obvious combinatorially.

2. $S_1(0,0) = 1,$ otherwise $S_1(n,0) = 0,\ n > 0$.

   By convention to give correct boundary conditions for recurrence.

3. $S_1(n,1) = (n-1)!$

   There is one cycle which in standard form starts with 1. There are $(n-1)!$ permutations of the remaining elements.

4. $S_1(n,n) = 1$.

   Only one way to seat n people at n tables.

5. $S_1(n,n-1) = \binom{n}{2}$.

   There are $n-1$ tables and exactly one table has 2 people. We can choose these two people in $\binom{n}{2}$ ways. After that there is only one way to seat the remaining people.

Basic Properties of Stirling Numbers

Theorem 149 (Basic Properties of Stirling Numbers). *1.* **Summation formula:** $\displaystyle\sum_{k=1}^{n} S_1(n,k)\ =\ n!$

2. **Recurrence relation:** $S_1(n,k) = S_1(n-1,k-1)+(n-1)S_1(n-1,k)$.

3. **Generating function:** $\displaystyle\sum_{k=1}^{n} S_1(n,k)x^k \;=\; x(x+1)(x+2)\cdots(x+n-1).$

Proof: $\boxed{1}$ Obvious from the definition.

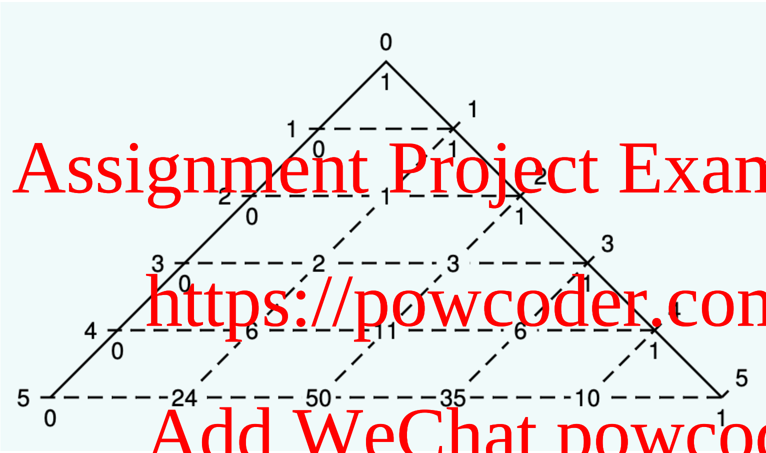
$\boxed{2}$ On the RHS we have $S_1(n-1,k-1)$ from 'add the 1-cycle (n)' **and** $(n-1)S_1(n-1,k)$ from 'insert 'n' into standard form of a $\sigma \in S_{n-1}$ with k cycles.' 'n' can be inserted in any position in a cycle except before the first number. Now check there are $n-1$ such positions, e.g., $\sigma = (15)(243)$ 5 positions for 6.

$\boxed{3}$ **Q5** from Practice Class 9.

Sterling Triangle

Recurrence relation and the boundary conditions leads to a Sterling triangle resembling Pascal's triangle for binomial coefficients:

n increases down rows while k is constant along 'right to left diagonals'.



57 Symmetric group

Symmetric Group

The fact that permutations can be multiplied to form other permutations, and have inverses, tells us that the set of all permutations from a group.

This group is called the symmetric group, and denoted S_n where n is the size of the permutation.

Example: The six elements of S_3 are

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = (1)(2)(3), \qquad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12)(3),$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (1)(23), \qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123),$$

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132), \qquad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13)(2).$$

58 Group theory

Groups

Definition 150 (Group)**.** A group, G, is a collection of elements with a multiplication relation satisfying:

Closed under multiplication:
$$a, b \in G \Rightarrow a \cdot b \in G$$
Associativity:
$$a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
Existence of unique identity element:
$$\exists\, e \in G \text{ s.t. } e \cdot a = a \cdot e = a \;\forall\, a \in G$$
Existence of inverse:
$$\forall\, a \in G,\ \exists\, b \in G \text{ s.t. } a \cdot b = b \cdot a = e$$

Note: Group multiplication need *not* be commutative: can have $a \cdot b \neq b \cdot a$.

Permutations – Exercise

Exercise: multiplying permutations.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} =?$$

Solution:

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} =?$$

Solution:

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

Permutations form a Group

Let $S_n =$ set of all permutations of n elements $\{1, 2, 3 \ldots, n\}$. With composition of permutations as multiplication S_n is a group called the **symmetric group**.

Definition 151 (Symmetric Group)**.** Let $\sigma, \tau, \alpha \in S_n$.

1. S_n is closed under multiplication: $\sigma \circ \tau \in S_n$.

2. Multiplication is associative: $(\sigma \circ \tau) \circ \alpha = \sigma \circ (\tau \circ \alpha)$. Which follows since composition of maps is associative.

3. Unique identity element: $\sigma_{\mathrm{I}} = (1, 2, 3, \cdots, n)$.
4. Every $\sigma \in S_n$ has a unique inverse (property of bijections).

Note: Multiplication in S_n is not commutative: in general $\sigma \circ \tau \neq \tau \circ \sigma$.

As we saw in previous example $(2314)(1342) = (2143) \neq (1342)(2314) = (3412)$.

Transpositions

Definition 152 (Transpositions)**.** If $\sigma \in S_n$ and $\sigma = (i\,j)$ (i.e. σ is a single 2-cycle and $n-2$ 1-cycles) then σ is called a **transposition**. If $j = i+1$ then σ is called a **simple** or **elementary** transposition.

Question: Can any $\sigma \in S_n$ be written as a product of (simple) transpositions?

That is, can we decompose σ into a product on non-disjoint 2-cycles?

Is this decomposition unique and if so how many are there?

Example:

$(134) = (14)(13)$

$1 \to 3$, $3 \to 1 \to 4$, $4 \to 1$

$(1423) = (13)(12)(14)$

$1 \to 4$, $4 \to 1 \to 2$, $2 \to 1 \to 3$, $3 \to 1$

Writing a Cycle as Product of Transpositions

Theorem 153 (Decomposition of Permutations)**.** *If $(a_1 a_2 \cdots a_k)$ is a k-cycle then*

$$(a_1 a_2 a_3 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_4)(a_1 a_3)(a_1 a_2)$$

or

$$(a_1 a_2 a_3 \cdots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-2} a_{k-1})(a_{k-1} a_k).$$

Proof: Outline of proof for first form.

To see why this is true we read RHS from right to left:

$a_1 \to a_2$. Then we never touch the element in position 2 again (it does not appear in any more cycles) and therefore a_1 is in the correct place.

$a_2 \to a_1 \to a_3$. We never touch a_3 again so a_2 remains in the correct place.

$a_3 \to a_1 \to a_4$. We never touch a_4 again so a_3 remains in the correct place.

Finally, $a_{k-1} \to a_1 \to a_k$, and $a_k \to a_1$.
This shows that all elements end up in their correct places.

Writing a Cycle as Product of Transpositions

Corollary 154 (Permutations as Products of Transpositions)**.** *All permutations can be written as a product of transpositions (and 1-cycles).*

Note:

1. Decomposition of permutations is not unique (two forms given).
2. The transpositions need not be simple.
3. In both of the given forms all transpositions are distinct. If repeats are allowed then there are even more possibilities, e.g.,

$$(25) \;=\; (45)(24)(45)$$

Check: on RHS, $4 \to 5 \to 4, \quad 5 \to 4 \to 2, \quad 2 \to 4 \to 5$. Same as LHS.

59 Parity of Permutations

Parity of Permutations

Definition 155 (Parity of Permutation)**.** The parity of a permutation is even if it can be written as the product of an even number of transpositions, and odd if it can be written as a product of an odd number of transpositions.

Definition 156 (Sign of Permutation)**.** The sign of a permutation, denoted sgn is defined as

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 \text{ if } \sigma \text{ is even} \\ -1 \text{ if } \sigma \text{ is odd} \end{cases}$$

Note: Fixed points (1-cycles) have sgn $= +1$.

Parity of Permutations

Theorem 157 (Parity of Permutations)**.** *The parity of the number of transpositions cannot vary and* $\operatorname{sgn}(\sigma)$ *is constant.*

Proof – Exercise: Given two different expressions for a permutation σ in terms of transpositions, can you prove that the number of transpositions in these two expressions must either both be even, or both be odd?

From $\sigma = (a_1 a_2 a_3 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_4)(a_1 a_3)(a_1 a_2)$

$\Rightarrow \operatorname{sgn}(\sigma) = (-1)^{k-1}$ (for a k-cycle),

and hence in general

$$\operatorname{sgn}(\sigma) = \prod_{\text{cycles}} (-1)^{|\text{cycle}|-1},$$

where |cycle| is the length of the cycle.

Example: $\sigma = 43512768 = (14)(235)(67) \quad \Rightarrow \text{sgn}(\sigma) = (-1)(-1)^2(-1) = +1$

60 Alternating Group

Alternating Group

From the following facts

1. If $\sigma, \tau \in S_n$ and $\text{sgn}(\sigma) = \text{sgn}(\tau) = +1 \quad \Rightarrow \quad \text{sgn}(\sigma \circ \tau) = +1$.
2. $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$, since cycles written backwards have the same length.
3. $\text{sgn}(\sigma_{\text{I}}) = +1$

we get

Theorem 158 (Alternating Group)**.** *The set of even permutations in S_n form a subgroup called the* **alternating group** *which is denoted A_n and we have $|\, A_n \,| = \frac{n!}{2}$.*

Element of S_3 and A_3

Write out all elements of S_3, first in two line notation, then as cycles, and finally in terms transpositions. Read off the elements of A_3.

$$\begin{array}{lr}
\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_{\text{I}} & \text{even} \\
\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23) & \text{odd} \\
\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12) & \text{odd} \\
\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123) = (13)(12) & \text{even} \\
\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) = (12)(13) & \text{even} \\
\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13) & \text{odd}
\end{array}$$

We read off that: $\quad A_3 \;=\; \{\sigma_{\text{I}}, (123), (132)\}$

Exercise

Example: Let σ be a permutation of $\{1, 2, \cdots, n\}$ consisting of l disjoint cycles, including possible fixed points. Show that $\text{sgn}(\sigma) = (-1)^{n-l}$.

Example: Show that (123) *generates* A_3, i.e. all elements of A_3 can be expressed as products of (123).

Notation: $A_3 = \langle(123)\rangle$.

61 Elementary transpositions

Reordering Permutations

The following simple 'bubble sort' algorithm can be used to reorder any permutation back to σ_{I}.

Algorithm 159 (Bubble Sort)**.** Any list of elements from $\{1, 2, \ldots, n\}$ can be sorted (ordered) by repeatedly switching the leftmost 'out-of-order' pair of elements.

Example: Sort the permutation 31542 by bubble sort.

$$31542 \overset{\substack{\text{switch}\\\text{pos }(12)}}{\longmapsto} 13542 \overset{\substack{\text{switch}\\\text{pos }(34)}}{\longmapsto} 13452 \overset{\substack{\text{switch}\\\text{pos }(45)}}{\longmapsto} 13425 \overset{\substack{\text{switch}\\\text{pos }(34)}}{\longmapsto} 13245 \overset{\substack{\text{switch}\\\text{pos }(23)}}{\longmapsto} 12345$$

In terms of neighbour switching we can write

$$\sigma \overset{(12)}{\longmapsto} \sigma^{(1)} \overset{(34)}{\longmapsto} \sigma^{(2)} \overset{(45)}{\longmapsto} \sigma^{(3)} \overset{(34)}{\longmapsto} \sigma^{(4)} \overset{(23)}{\longmapsto} \sigma_{\mathrm{I}}$$

Reordering Permutations

Note:

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 5 & 4 & 2\end{pmatrix} \circ (12) = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 5 & 4 & 2\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 5 & 4 & 2\end{pmatrix} \circ (34) = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 5 & 2\end{pmatrix}$$

We see that switching entries i and $i+1$ is the same as composition on the **right** with the 2-cycle $(i\ i+1)$, i.e., $\sigma \circ (12) = \sigma^{(1)}$, $\sigma^{(1)} \circ (34) = \sigma^{(2)}$, etc., and

$$\sigma \circ (12) \circ (34) \circ (45) \circ (34) \circ (23) = \sigma_{\mathrm{I}}$$

From which is follows that

$$\sigma = (23) \circ (34) \circ (45) \circ (34) \circ (12)$$

Note: We have thus written σ as a composition (product) of **elementary** transpositions and our working suggests this can always be done.

Permutations from Elementary Transpositions

Theorem 160 (Permutations from Elementary Transpositions)**.** *Permutations $\sigma \in S_n$ can be written as products of elementary transpositions.*

The theorem follows from the following procedure

1. Decompose each cycle of $\sigma \in S_n$ into a composition of transpositions using the results from Week 9 Lecture 3.

2. Decompose each transposition into a composition of elementary transpositions using the next theorem.

Definition 161 (Elementary Transpositions of S_n)**.** The **elementary transpositions** for S_n are $s_i = (i\ i+1)$, i.e.,

$$s_1 = (12),\ \ s_2 = (23),\ \ s_3 = (34),\ \ \cdots,\ \ s_{n-1} = (n-1\ n).$$

Transpositions from Elementary Transpositions

Theorem 162 (Transpositions from Elementary Transpositions)**.** *Let s_i be the elementary transpositions for S_n. Then, for $i < j$ the transposition $(i\,j)$ can be written*

$$(i\,j) = s_{j-1}s_{j-2}\cdots s_{i+1}s_i s_{i+1}\cdots s_{j-2}s_{j-1},$$

Proof: "Follow the composition" and check $i \longmapsto j \longmapsto i$.

$s_{j-1}s_{j-2}\cdots s_{i+1}s_i s_{i+1}\cdots s_{j-2}s_{j-1} =$

$(j{-}1\ j)\circ(j{-}2\ j{-}1)\circ\cdots\circ(i{+}1\ i{+}2)\circ(i\ i{+}1)\circ(i{+}1\ i{+}2)\circ\cdots\circ(j{-}2\ j{-}1)\circ(j{-}1\ j)$.

We see $\ j \mapsto j-1 \mapsto j-2 \mapsto \cdots \mapsto i+2 \mapsto i+1 \mapsto i$.

Now i doesn't appear again so all in all $j \mapsto i$.

If we start with i nothing happens until we hit $(i\ i{+}1)$ and then

$$i \mapsto i+1 \mapsto i+2 \mapsto \cdots \mapsto j-2 \mapsto j-1 \mapsto j.$$

Inverses as Elementary Transpositions

Theorem 163 (Inverses as Elementary Transpositions)**.** *If $\sigma \in S_n$ and*

$$\sigma \ = \ s_{i_1}s_{i_2}\cdots s_{i_{k-1}}s_{i_k}$$

then

$$\sigma^{-1} \ = \ s_{i_k}s_{i_{k-1}}\cdots s_{i_2}s_{i_1},$$

i.e., just reverse the order of the elementary transpositions.

Proof: Form $\sigma \circ \sigma^{-1}$ and use $s_i^2 = \sigma_{\mathrm{I}}$.

Transpositions from Elementary Transpositions

Any transposition can be written as a product of elementary transpositions.

Example:

$$(24) = (34)(23)(34) = s_3 s_2 s_3.$$

This can be shown by the shuffling action on (a, b, c, d):

$$\begin{aligned} s_3 s_2 s_3(a, b, c, d) &= s_3 s_2(a, b, d, c) = s_3(a, d, b, c) \\ &= (a, d, c, b) = (24)(a, b, c, d). \end{aligned}$$

$$(25) = (45)(34)(23)(34)(45) = s_4 s_3 s_2 s_3 s_4$$

$$s_4s_3s_2s_3s_4(a,b,c,d,e) = s_4s_3s_2s_3(a,b,c,e,d)$$
$$= s_4s_3s_2(a,b,e,c,d) = s_4s_3(a,e,b,c,d)$$
$$= s_4(a,e,c,b,d) = (a,e,c,d,b) = (25)(a,b,c,d,e).$$

Symmetric Group

We have shown that any cycle can be written as a product of transpositions.

Then we showed that any transposition can be written as a product of elementary transpositions ($s_i = (i\ i+1)$).

Thus *any* permutation $\sigma \in S_n$ can be written as a product of s_i's.

We have therefore shown that

Theorem 164 (S_n is Generated by Elementary Transpositions)**.** *Let s_i be the elementary transpositions for S_n. Every $\sigma \in S_n$ can be written as a product of s_i's and we say that the set of s_i's* **generate** *S_n, and write*

$$S_n = \langle s_i \mid i = 1, 2\cdots, n-1\rangle.$$

Permutations as Words

Previous theorem says a permutation $\sigma \in S_n$ is a **word** in the alphabet

$$S = \{s_1, s_2, \ldots, s_{n-1}\}$$

Question: What is the **shortest** word?

There are many ways to write a given $\sigma \in S_n$ as (shortest length) product of elementary transpositions.

Example: Consider $\sigma = 4213$

$\sigma = 4213 = (143) = (13) \circ (14) = s_2s_1s_2 \circ s_3s_2s_1s_2s_3$ length $= 8$.

However, $\sigma = s_3s_1s_2s_1 = s_1s_3s_2s_1 = s_3s_2s_1s_2$

Check: $s_3s_1s_2s_1 = (34)(12)(23)(12) = (143)(2)$

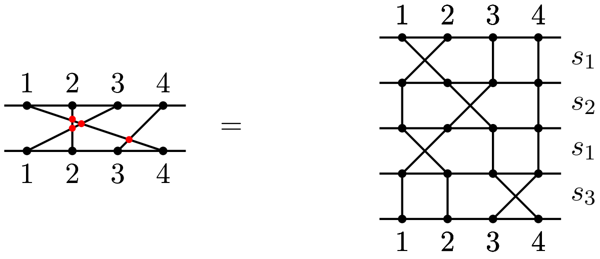
or $s_1s_3s_2s_1 = (12)(34)(23)(12) = (143)(2)$

62 Inversions

Inversions

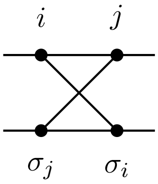
So if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, then the shortest word is $w_\sigma = s_3s_1s_2s_1$.

Looking at the bipartite graph for σ reveals a secret:



Graph has four crossings, and it is no coincidence that the length of w_σ is 4.

Inversions

A cross 

corresponds to two entries out of order: $i < j$, $\sigma_i > \sigma_j$.

Definition 165 (Inversion)**.** An **inversion** of a permutation σ is a pair (i, j) such that $i < j$ and $\sigma_i > \sigma_j$. The set of inversions of σ is denoted

$$I_\sigma = \{(i, j) \mid i < j,\ \sigma_i > \sigma_j\}.$$

Note: The bigger number σ_i appear before σ_j in $(\sigma_1 \sigma_2 \dots \sigma_n)$.

Bonus: Bipartite graph gives decomposition as elementary transpositions.

Read from top to bottom and record crossings in order of appearance.

Inversions

Example: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ then

$$I_\sigma = \{(1,2), (1,3), (1,4), (2,3)\}.$$

All pairs in $\sigma = (4, 2, 1, 3)$ are given by the table

4	2	1	3
4	2		
4		1	
4			3
	2	1	
	2	3	
		1	3
1	2	3	4

Four pairs out of order. **Positions** of the elements give the entries in I_σ.

Reduced Words

Theorem 166 (Length of Shortest Word)**.** *The length $\ell(w_\sigma)$ of a shortest word $w_\sigma \in S_n$ representing σ by elementary transpositions equals the number of inversions of σ, i.e., if $\ell(w_\sigma)$ is minimal then $\ell(w_\sigma) = |I_\sigma|$.*

Definition 167 (Reduced Word)**.** A minimum length word is called a *reduced word.*

63 Algebraic Relations for s_i's

Algebraic Relations for s_i's

Elementary transpositions, s_i, are characterised by three algebraic relations:

1. $s_i^2 = \sigma_{\mathrm{I}}$ (the identity permutation)
2. $s_i s_j = s_j s_i, \quad |i - j| > 1$ (commutation relation)
3. $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ (the braid relation)

Exercise: Check that these relations are true.

Note: The proof that any two expressions for a permutation σ in terms of s_i's, can be converted from one expression to the other via a sequence of operations of the form (1), (2), and (3) is lengthy and not part of the course.

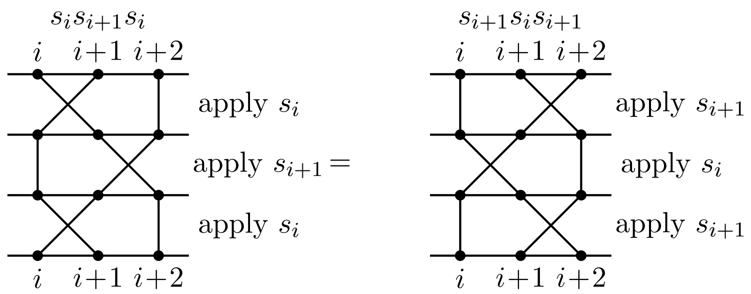
Relation (1) reduces the number of s_i's by two (shortens the word).

Relations (2) and (3) don't change the number s_i's, but re-orders them.

Thus the **parity** of the number of elementary transpositions is conserved by the algebraic relations.

Braid Relation

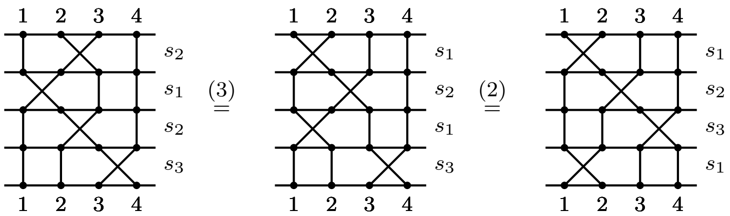
We can represent the braid relation visually as follows:



So pictorially the braid relation is like a reflection in a line through $i+1$.

Algebraic Relations in Action – Graphically

Return to $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, with $w_\sigma = s_3 s_1 s_2 s_1$.



Reduced Word - Example

Example: Find all reduced words for $w_\sigma = s_1 s_3 s_2 s_3 s_1$.

64 Alternating group

The Alternating Group

Recall: If σ and π are even permutations, then by inspection $\sigma\pi$ is also even. We also have that σ^{-1} is even, and the identity permutation I is even, and so even permutations form a *group*, called the alternating group.

We denote the alternating group of n elements as A_n.

We will now specify a generating set for A_n. Elements of A_n can be written as a product of an even number of transpositions. We know that the elementary transpositions generate S_n, and so we have

$$A_n = \langle s_i s_j \mid 1 \le i < j \le n-1 \rangle.$$

How can we be sure $i < j$ is sufficient?

Because we can generate $s_j s_i$ with $i < j$

$$\begin{aligned} s_j s_i &= s_i s_j \qquad \text{when } j > i+1 \text{ from (2)} \\ s_{i+1} s_i &= s_i^2 s_{i+1} s_i = s_i(s_i s_{i+1} s_i) = s_i(s_{i+1} s_i s_{i+1}) = (s_i s_{i+1})^2. \end{aligned}$$

Generating Set for A_n

We can go one step further. Note that for $i < j$ we have

$$s_i s_j = s_i s_{i+1}^2 s_{i+2}^2 \cdots s_{j-1}^2 s_j = (s_i s_{i+1})(s_{i+1} s_{i+2}) \cdots (s_{j-1} s_j).$$

So any $s_i s_j$ with $i < j$ can be generated by $s_i s_{i+1}$! Thus

$$A_n = \langle s_i s_{i+1} \mid 1 \le i \le n-2 \rangle = \langle (i\ i+1\ i+2) \mid 1 \le i \le n-2 \rangle$$

Exercise: Show that $s_i s_{i+1} = (i\ i{+}1\ i{+}2)$

Definition 168 (Elementary 3-cycles)**.** A 3-cycle is **simple** or **elementary** if it is of the form $(i\ i{+}1\ i{+}2)$.

Theorem 169 (A_n Generated by Elementary 3-cycles)**.** *If $\sigma \in A_n$ then σ can be decomposed into a product of elementary 3-cycles and A_n is thus generated by elementary 3-cycles.*

This generating set will form the basis for our understanding of the 15-puzzle.

65 The 15-puzzle

The 15-puzzle

The 15-puzzle was invented towards the end of the 19$^{\text{th}}$ Century, and started a world-wide craze bigger than that of the Rubik's cube in the 1980's. See `http://en.wikipedia.org/wiki/15-puzzle`.

The 15-puzzle consists of a 4×4 grid with tile labelled 1 to 15 and an empty cell. The tiles may be slid into an adjacent empty cell (called a legal move).

Typical challenge: Change configuration A to configuration B?

Change a random (scrambled) configuration into the ordered configuration:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Objectives

We are going to study the 15-puzzle as a mathematical object.

- How to prove or characterise which configurations can be legally obtained?
- Idea: map configurations to permutations and moves to the action of a permutation on the configuration.

We prove a connection to the alternating group A_n by showing two things:

- *Only* even permutations of the numbers $1, \cdots, 15$ can be achieved. (Hence, the tiles labelled 14 and 15 can't be swapped, as this corresponds to a single transposition).
- *All* even permutations of the numbers $1, \cdots, 15$ can be achieved.

Note: The 15-puzzle can be generalised to an $n \times m$ grid with $n \times m - 1$ tiles and a empty cell.

Grid Representation

There are many ways to map configurations to permutations. The obvious one is to label cells 1 to 16 and then $\sigma(i)$ = label of the tile above i.

For example (with clockwise cell numbering)

4	1
3	2

$$\longrightarrow \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (4, 1, 2, 3) = (1432)$$

Move 3 up:

3	1
4	2

$$\longrightarrow \qquad \mu = (3, 1, 2, 4) = (132)(4) = (1432)(14)$$

Moving the tile with 3 resulted in right-composition with the transposition (14).

Right-Composition

Recall: Right composition by two-cycle (ij) swaps values at positions i and j.

$$\begin{aligned} \sigma' &= \sigma(ij), \qquad \sigma = (\sigma_1, \ldots, \sigma_i, \ldots, \sigma_j, \ldots, \sigma_n) \\ &= (\sigma_1, \ldots, \sigma_j, \ldots, \sigma_i, \ldots, \sigma_n) \end{aligned}$$

Exercise: Characterise *left* composition by (ij).

Only Even Permutations are Possible

Theorem 170 (Only Even Permutations are Possible)**.** *On an $m \times n$ board with moves consisting of swapping the "empty" cell with a neighbouring tile only even permutations of the tiles are permitted.*

Proof: Our goal is to characterise possible configurations where the empty tile remains fixed, i.e. in the bottom right corner.

Swapping the empty tile with a neighbour corresponds to a *transposition*.

If we must return the empty tile to its starting position, then we have

$$\begin{aligned} \#\text{ of up slides} &= \#\text{ of down slides} \\ \#\text{ of left slides} &= \#\text{ of right slides} \\ \Rightarrow \text{Total slides} &= (\#\text{ up}) + (\#\text{ down}) + (\#\text{ left}) + (\#\text{ right}) \\ &= 2(\#\text{ up}) + 2(\#\text{ left}) \;=\; \text{even number} \end{aligned}$$

So the final configuration must be reached via an even number of transpositions, and hence corresponds to an even permutation in S_{nm-1}.

Exercise: Why is this true for S_{nm-1}, even though we have $n \times m$ tiles?

Notes on the Grid Representation

1. Grid permutation representation requires us to work with $S_{n\times m}$.
2. Configurations related by sliding the empty cell along cell labels correspond to **different** permutations, e.g.:

4	1
3	2

(4,1,2,3)

1	4
3	2

(1,4,2,3)

1	2
3	4

(1,2,4,3)

1	2
4	3

(1,2,3,4)

3. To get the permutation we must "look under" the tile to see the cell label.

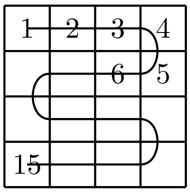
The representation we shall look at next reduces $n \times m$ to $n \times m - 1$ and fixes the problems with (2) and (3) from the grid representations.

All Even Permutations are Possible

Theorem 171 (All Even Permutations are Possible). *On an $m \times n$ board with moves consisting of swapping the "empty" tile with a neighbouring tile all even permutations of the tiles are permitted.*

Proof: This is surprisingly non-trivial. See e.g. `http://www.cs.cmu.edu/afs/cs/academic/class/15859-f01/www/notes/15-puzzle.pdf` for a proof by Archer in the American Mathematical Monthly (1999).

First we need a different representation: "Snake pattern representation"



$\sigma(i)$ is the position of tile i along the snake *ignoring* the blank $\Rightarrow \sigma \in S_{15}$

Snake Pattern Representation

Example: Can target configuration be reached from initial configuration?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Target configuration

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Initial configuration

$$
\begin{aligned}
\sigma_{\mathrm{i}} &= (1,2,3,4,8,7,6,5,9,10,11,12,15,14,13) \\
&= (58)(67)(13\ 15) = \quad \text{odd permutation}
\end{aligned}
$$

$$
\begin{aligned}
\sigma_{\mathrm{t}} &= (1,2,3,4,8,7,6,5,9,10,11,12,14,15,13) \\
&= (58)(67)(13\ 14\ 15) = \quad \text{even permutation}
\end{aligned}
$$

Since moves correspond to even permutations, they cannot produce the target configuration from the initial configuration.

Blank can be moved along the snake without changing the permutation $\Rightarrow$ map from puzzle configurations to permutations is not one-to-one but 16 to 1.

66 7-Puzzles

7-Puzzles

For simplicity we now focus on 2×4 grids.

We prove that each permutation gives rise to a puzzle configuration.

In fact 7 configurations related to each other by blank slides along the snake. Initial configuration:

1	2	3	4
5	6	7	

$\sigma_{\mathrm{i}} = (1,2,3,4,7,6,5) = (57)$

Target configuration:

1	2	3	4
5	7	6	

$\sigma_{\mathrm{t}} = (1,2,3,4,6,7,5) = (567)$

7-Puzzles

Moving a tile into the blank changes the permutation of the configuration

$$p \xrightarrow{\text{move}} q$$

which is represented by **right** composition

$$\sigma_p = \sigma_q \mu,$$

where μ is the permutation corresponding to the slide.

Many slide moves correspond to longer composition sequences:

$$\sigma_r = \sigma_0 \mu_1 \mu_2 \cdots \mu_r.$$

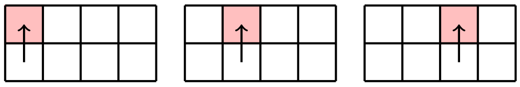
So for 7-puzzles the questions are

- $(567) \stackrel{?}{=} (57)\mu_1 \cdots \mu_r$ with μ_i permutations corresponding to legal moves.

- If not, does every even permutation correspond to a legal configuration?

7-Puzzle: Fundamental Moves

For the 7-puzzle and the snake representation we only need **three** different fundamental permutations.

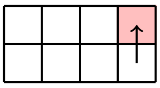
Move: 

Permutation: μ_1 μ_2 μ_3

Thus μ_i corresponds to moving the tile in column i up from bottom to top row (and μ_i^{-1} is the top to bottom move).

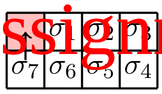
Recall that horizontal slides do not change the permutation.

So we can always make those "for free".

Note:  is not required. Why is that?

7-Puzzle: Fundamental Permutations

As permutations the moves correspond to

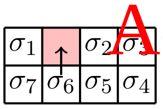


$$(\sigma_7, \sigma_1, \ldots, \sigma_6) = (\sigma_1, \ldots, \sigma_7)\mu_1$$

Hence $\mu_1 = (1765432)$, a 7-cycle. Check this!

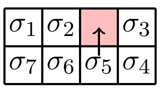
Note that μ_1 is **independent** of the tile permutation σ.

Likewise for μ_2 and μ_3:



$$(\sigma_1, \sigma_6, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_7) = (\sigma_1, \ldots, \sigma_7)\mu_2$$

Hence $\mu_2 = (26543)$, a 5-cycle (check).



$$(\sigma_1, \sigma_2, \sigma_5, \sigma_3, \sigma_4, \sigma_6, \sigma_7) = (\sigma_1, \ldots, \sigma_7)\mu_3$$

Hence $\mu_3 = (354)$, a 3-cycle (check).

7-Puzzle: Even Permutations

Now

$$\begin{aligned} \text{sign}(\mu_1) &= (-1)^6 = +1 \\ \text{sign}(\mu_2) &= (-1)^4 = +1 \\ \text{sign}(\mu_3) &= (-1)^2 = +1 \end{aligned}$$

so these are all even permutations.

$\sigma_{\text{t}} = (567)$ can never equal $\sigma_{\text{i}}\mu_1 \cdots \mu_r = (57)\mu_1 \cdots \mu_r$ as their signs are different.

We now show that μ_1, μ_2, μ_3 and their inverses generate A_7, the alternating group on seven symbols.

Recall that A_n is generated by all 3-cycles $(i\ i+1\ i+2)$, $i = 1, \ldots, n-2$.

A_7 is generated by:

$$h_1 = (123), h_2 = (234), h_3 = (345) = \mu_3^{-1}, h_4 = (456), h_5 = (567).$$

Relation to Alternating Group

We need the following result.

Lemma 172. *If $\alpha = (\alpha_1\alpha_2 \ldots \alpha_k)$ is a k-cycle and $\sigma \in S_n$ then*

$$\sigma(\alpha_1\alpha_2 \ldots \alpha_k)\sigma^{-1} = (\sigma(\alpha_1)\sigma(\alpha_2) \ldots \sigma(\alpha_k)).$$

Proof: Note that α sends $\alpha_i \mapsto \alpha_{i+1}$, and consequently $\sigma\alpha\sigma^{-1}$ sends $\sigma(\alpha_i) \mapsto \alpha_i \mapsto \alpha_{i+1} \mapsto \sigma(\alpha_{i+1})$.

Example:

$$\mu_1\mu_3^{-1}\mu_1^{-1} = \mu_1 h_3 \mu_1^{-1} = (1765432)(345)(1234567) = (234) = h_2.$$

Relation to Alternating Group

Likewise

$$\begin{aligned}
\mu_1^2 h_3 \mu_1^{-2} &= (1642753)(345)(1357246) = (123) = h_1, \\
\mu_2^{-1} h_3 \mu_2 &= (23456)(345)(26543) = (456) = h_4, \\
\mu_1^{-1} h_4 \mu_1 &= (1234567)(456)(1765432) = (567) = h_5.
\end{aligned}$$

So all the elementary 3-cycles in A_7 can be written as compositions of the 7-puzzle permutations μ_1, μ_2 and μ_3 and their inverses!

$$\begin{aligned}
h_1 &= (123) = \mu_1^2\mu_3^{-1}\mu_1^{-2}, \\
h_2 &= (234) = \mu_1\mu_3^{-1}\mu_1^{-1}, \\
h_3 &= (345) = \mu_3^{-1}, \\
h_4 &= (456) = \mu_2^{-1}\mu_3^{-1}\mu_2, \\
h_5 &= (567) = \mu_1^{-1}\mu_2^{-1}\mu_3^{-1}\mu_2\mu_1.
\end{aligned}$$

Note: The inverse of a 3-cycle h_i is h_i^2 (as $h_i^3 = \sigma_{\mathrm{I}}$).

Puzzle Moves Generate $A_{n\times m-1}$

Theorem 173 (Puzzle Moves Generate $A_{n\times m-1}$)**.** *The three moves μ_1, μ_2 and μ_3 and their inverses generate the group A_7. Similarly, the moves of the 15-puzzle generate A_{15}.*

Note: For the 15-puzzle the snake-permutation has 9 moves and inverses.

To prove the result using the "grid permutation" representation requires 48 moves μ_i (and their inverses).

For each of the 48 moves (and inverses) need to

1. Compute the parity.
2. Write the 14 generators h_i of A_{16} as products of the moves permutations.

For the snake-representation we need to write the 13 generators h_i of A_{15} as products of the 9 moves permutations (and their inverses)

7-Puzzle

Example: Are these positions of a 7-puzzle related by legal moves?

4		1	2
7	3	6	5

6	2	1	5
4	3	7	

Answer: The positions are not related by legal moves.

15-Puzzle

Example: Are these positions of a 15-puzzle related by legal moves?

1	3	2	4
5	6	7	15
12	10	11	9
13	14	8	

15	2	3	4
7	5	6	8
9	10	11	12
1	14	13	

Answer: The positions are not related by legal moves.

67 Designs

Designs – Introduction

Suppose we wish to conduct a taste test to compare 9 different varieties of coffee. We have limited resources (and time), and so wish to do this as fairly as possible. What are some considerations?

- Assign varieties of coffee to different households, but can't have a household comparing all 9 varieties. Their opinion of the 9$^{\text{th}}$ variety would be unreliable due to saturation of taste.
- Compare pairs of varieties.

- Want any given variety to be compared with all the others.
- For fairness, all pairs should be compared the same number of times.

How can we do this?

Designs – Introduction

Solution: Let the varieties of coffee be numbered $1, \cdots, 9$:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array}$$

Now there are $\binom{9}{2} = 36$ possible pairs of coffee varieties.

Twelve households are each given 3 varieties to compare.

3 varieties has 3 pairs so each possible pairing amongst the 9 varieties will be rated by exactly one household.

This way every variety is compared against the others by some household.

The varieties of coffee can be distributed as follows.

$$\{1,2,3\},\ \{4,5,6\},\ \{7,8,9\},\ \{1,4,7\},\ \{2,5,8\},\ \{3,6,9\},$$
$$\{1,5,9\},\ \{2,6,7\},\ \{3,4,8\},\ \{1,6,8\},\ \{2,4,9\},\ \{3,5,7\}.$$

Designs – Definition

The previously problem is an example of a **combinatorial design** problem.

The term design comes from the design of statistical experiments, i.e. the field of "experimental design".

Used in biology, social sciences, software testing and other fields.

More formally, a design is a (finite) family of subsets of a set which obeys certain properties.

Definition 174 (Design)**.** A **design** is a pair $(X, \mathcal{A})$ such that

1. X is a set of elements (points, varieties).
2. $\mathcal{A}$ is a collection (multiset) of nonempty subsets of X called **blocks**.

Designs – Definition

Note: The properties or conditions on $\mathcal{A}$ can be very general but typically involve *incidence*: set membership, set intersection and so on. For this reason, a design as defined above is also called an **incidence structure**.

We will see that the study of designs is a "big" field. Block designs are also related to (block) error correcting codes.

The general definition of designs is extremely broad and in particular $\mathcal{A}$ may contain *repeated blocks* (hence multiset in the definition).

In the previous design, each household tests the same number of varieties, and thus the opinion of each household has equal weight.

Designs – More Definitions

Each pair of varieties was in the same number of subsets (blocks).

Definition 175 (Designs).

- A design with no repeated blocks is said to be **simple**.
- A design is **regular** if every variety (element) occurs equally often. A regular design is also called a **1-design**.
- A block is **complete** if it contains every variety (incomplete otherwise).
- A design is **incomplete** if at least one block in incomplete.
- If x and y are any two different varieties in an incomplete design the number of blocks containing both x and y is the **covalency** denoted λ_{xy}.
- A **balanced incomplete block design (BIBD)**, or a **2-design**, is a regular incomplete design in which $\lambda_{xy} = \lambda$ is constant.

Designs – Notation

Notation 176 (Designs).

- # subsets = # blocks = b.
- # elements = # varieties = v.
- # subsets containing any one variety = r.

- # varieties in each subset = k ($< v$).
- # times a pair of varieties are compared = λ.

A BIBD can be specified by these parameters in the order (b, v, r, k, λ).

Note: We will prove in a following theorem that the number of appearances of a given variety, r, is determined by v, k, and λ.

A BIBD with parameters (b, v, r, k, λ) is also called a **2-(v, k, λ) design**.

Example: Our previous example is a $(12, 9, 4, 3, 1)$ design.

$$\{1,2,3\},\ \{4,5,6\},\ \{7,8,9\},\ \{1,4,7\},\ \{2,5,8\},\ \{3,6,9\},$$
$$\{1,5,9\},\ \{2,6,7\},\ \{3,4,8\},\ \{1,6,8\},\ \{2,4,9\},\ \{3,5,7\}.$$

Balanced Incomplete Block Designs

Theorem 177 (BIBD). *In a balanced incomplete block design with* (b, v, r, k, λ),

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

Proof: Count the number of pairs a given variety, x is in, in two ways.

Method 1: The element x is in r_x blocks (note, we don't assume r_x is the same for each x). In each block, it can be paired with $k-1$ other varieties, and hence x is in $r_x(k-1)$ pairs.

Method 2: The element x can be paired with $v-1$ other varieties. Each of these pairs must, by definition, appear λ times in the design, and hence x is in $(v-1)\lambda$ pairs. Thus,

$$r_x(k-1) = \lambda(v-1) \quad \Rightarrow \quad r_x = \lambda\frac{v-1}{k-1}.$$

Note: As a *consequence* of the fairness requirements (each block has the same weight k and each pair is compared exactly λ times) it follows that r_x is independent of x, and given by the equation above.

Regular Designs

Theorem 178 (Regular Designs)**.** *In any regular design,* $bk = vr$.

Proof: Count the number of varieties in all of the blocks in two ways.

Method 1: There are v varieties, which each appear r times, and thus the total number of appearances is vr.

Method 2: There are b blocks, which each contain k varieties, and thus the total number of appearances is bk. Thus

$$rv = bk \quad \Rightarrow \quad r = \frac{bk}{v}.$$

Note: Taken together $rv = bk$ and $r(k-1) = \lambda(v-1)$, gives us two equations between the 5 parameters of a BIBD, thus only 3 parameters can be chosen independently. For this reason BIBD's are often written simply as (v, k, λ).

Importantly, not all choices are possible, as b, v, r, k, λ must be integers.

68 Incidence matrix

Incidence Matrix

Definition 179 (Incidence Matrix)**.** A design can be represented by an **incidence matrix** M where the rows represent blocks S_i and the columns represent varieties v_j and the entries $M_{ij} = 1$ if variety $v_j \in S_i$, 0 otherwise.

Example: The incidence matrix for the $(7, 7, 4, 4, 2)$ design

$\{3,5,6,7\}$, $\{1,4,6,7\}$, $\{1,2,5,7\}$, $\{1,2,3,6\}$, $\{2,3,4,7\}$, $\{1,3,4,5\}$, $\{2,4,5,6\}$ is

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

Incidence Matrix

Key facts about the incidence matrix of any (b, v, r, k, λ) BIBD.

- There are b rows.
- Each row has k 1's (number of varieties in a block).
- There are v columns.
- Each column has r 1's (number of appearances of each variety).
- There are exactly λ 1's in common between any two columns.

  Consider columns i and j: The values of entries are are both 1 on those occasions when varieties i are j are in the same block. This must occur exactly λ times, by definition.

Properties of the Incidence Matrix

Theorem 180 ($M^{\mathrm{T}}M$)**.** *Let J be the $v \times v$ matrix consisting of all 1's, then the incidence matrix M of any BIBD satisfies*

$$M^{\mathrm{T}}M = (r-\lambda)I + \lambda J.$$

Proof: Assume that we have $i, j \in \{1, \cdots, v\}$. Now,

$$\begin{aligned}(M^{\mathrm{T}}M)_{ij} &= (\text{row } i \text{ of } M^{\mathrm{T}}) \cdot (\text{column } j \text{ of } M)\\ &= (\text{column } i \text{ of } M) \cdot (\text{column } j \text{ of } M)\\ &= r\delta_{ij} + \lambda(1-\delta_{ij})\\ &= (r-\lambda)\delta_{ij} + \lambda \cdot 1.\end{aligned}$$

Hence

$$M^{\mathrm{T}}M = (r-\lambda)I + \lambda J.$$

Inequalities for BIBD

Theorem 181 (Inequalities for BIBD)**.** *The parameters of any BIBD satisfies $b \geq v$ and $r \geq k$.*

Proof: We have $r(k-1) = \lambda(v-1) \quad \Rightarrow \quad \lambda = r\dfrac{k-1}{v-1} < r$ since $k < v$, so

$$\det(M^{\mathrm{T}}M) = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & & & & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda - r & r-\lambda & 0 & \cdots & 0 \\ \lambda - r & 0 & r-\lambda & \cdots & 0 \\ \vdots & & & & \vdots \\ \lambda - r & 0 & 0 & \cdots & r-\lambda \end{vmatrix}$$

$$= \begin{vmatrix} r+(v-1)\lambda & \lambda & \lambda & \cdots & \lambda \\ 0 & r-\lambda & 0 & \cdots & 0 \\ 0 & 0 & r-\lambda & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & r-\lambda \end{vmatrix}$$

$$= (r+(v-1)\lambda)(r-\lambda)^{v-1} = rk(r-\lambda)^{v-1}$$

$$\neq 0.$$

Proof – Continued

$\det(M^{\mathrm{T}}M) = rk(r-\lambda)^{v-1} \neq 0$.

Assume $b < v$.

Then we could add $(v-b)$ additional rows of 0s to make a square matrix M_1.

Now,

$$M_1^{\mathrm{T}}M_1 = M^{\mathrm{T}}M \qquad \text{by inspection additional rows just give } 0 \times 0$$

$$\Rightarrow \det(M^{\mathrm{T}}M) = \det(M_1^{\mathrm{T}}M_1) = \det(M_1)^2 = 0$$

But, $\det(M^{\mathrm{T}}M) \neq 0$ so assumption is false. Thus $b \geq v$.

Since $b \geq v$, the relation $bk = vr$ implies $r \geq k$.

69 Kirkman's schoolgirl problem

Kirkman's Schoolgirl Problem and Resolvable Designs

- Designs were a topic of recreational interest for their combinatorial properties in the 19th Century, pioneered by Steiner.
- The most famous design problem was Kirkman's schoolgirl problem, which was posed in 1850:

  Every day of the week a teacher takes 15 schoolgirls on a walk. During the walk the girls are grouped in triplets. Can the teacher construct the triplets so that after the seven walks each pair of girls has walked in the same triplet once and only once?

- A Kirkman triple is a Steiner triple $(v, 3, 1)$, with the additional condition that it must be possible to partition the blocks such that each partition contains each element once (the design is said to be resolvable).

- Question makes sense for number of schoolgirls $v = 3, 9, 15, 21, \cdots$.

70 Steiner triple systems

Steiner Triple Systems

Definition 182 (Steiner Triple System)**.** A **Steiner triple system** or order v is a BIBD with parameters $(v, 3, 1)$.

Note: Since BIBD's with $k = 2$ are trivial Steiner triple system are the simplest "interesting" designs.

Example: The simplest case is $(7, 3, 1)$ so $v = 7$ varieties, $k = 3$ varieties in each sub-set and each pair of varieties are compared $\lambda = 1$ times.

Using our equalities from previous lecture we also have

$$r = \frac{\lambda(v-1)}{k-1} = \frac{6}{2} = 3, \qquad rv = bk \Rightarrow b = v = 7$$

The (unique) solution is

$$\{1,2,3\},\ \{1,4,5\},\ \{1,6,7\},\ \{2,4,6\},\ \{2,5,7\},\ \{3,4,7\},\ \{3,5,6\}$$

Steiner Triple Systems

The incidence matrix of this design

$$\{1,2,3\},\ \{1,4,5\},\ \{1,6,7\},\ \{2,4,6\},\ \{2,5,7\},\ \{3,4,7\},\ \{3,5,6\}$$

is:

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

Example: The first design we looked at is a $(9, 3, 1)$ Steiner triple system.

This again is a unique solution (up to permutations and so on).

Steiner Triples

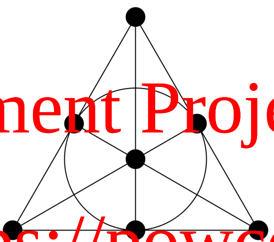
How many Steiner triples are there?

- $(v, 3, 1)$ designs exist if and only if $v = 1$ or $3 \pmod 6$.

- Known up to $v = 19$, but it is a hard problem. No reason to think that there is a simple closed form answer and so one has to count them via computer.
- Online encyclopedia of integer sequences (OEIS) # A030128, number of Steiner triples: 1, 0, 1, 0, 0, 0, 30, 0, 840, 0, 0, 0, 1197504000, 0, 60281712691200, 0, 0, 0, 1348410350618155344199680000, $\cdots$
- # A030129, number of non-isomorphic (distinct) Steiner triples: 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 2, 0, 80, 0, 0, 0, 11084874829, $\cdots$
- Unless someone finds a better algorithm (which avoids generating all distinct triples), then finding out the answer for $n = 21$ will take hundreds of thousands of CPU years.

Steiner Triple-(7,3,1)

(7,3,1) can be represented geometrically such that the elements $1, 2, \cdots, 7$ are points, and the blocks are lines.



This is the simplest example of a finite projective plane.

- Any 2 points lie on exactly 1 line.
- Any 2 lines meet at exactly 1 point.
- There are 4 points such that no line is incident with more than two of them. This condition excludes trivial, non-interesting cases.

Finite projective planes of order n are equivalent to square designs of order $(n^2 + n + 1, n + 1, 1)$.

Square Designs

Definition 183 (Square Designs)**.** A **square design** (or **symmetric design**) is a BIBD with $b = v$ and since $rv = bk$ it follows that $r = k$.

A square design is usually specified by the three parameters (v, k, λ) only.

Square Designs

Theorem 184 (Rows of Square Designs)**.** *For square designs the number of 1's agreeing in any two* rows *equals λ.*

Note: For any design the number of 1's agreeing in any two columns is λ.

Proof: In Practice Class 11 you will prove that $M^{\mathrm{T}}M = M\,M^{\mathrm{T}}$.
Assume that we have $i, j \in \{1, \cdots, v\}$, with $i \neq j$. Now,

$$\begin{aligned}
(M^{\mathrm{T}}\,M)_{ij} &= (\text{row } i \text{ of } M^{\mathrm{T}}) \cdot (\text{column } j \text{ of } M) \\
&= (\text{column } i \text{ of } M) \cdot (\text{column } j \text{ of } M) \\
&= \#\text{ of 1's which match up between colums } i \text{ and } j \; = \; \lambda \\
(M\,M^{\mathrm{T}})_{ij} &= (\text{row } i \text{ of } M) \cdot (\text{column } j \text{ of } M^{\mathrm{T}}) \\
&= (\text{row } i \text{ of } M) \cdot (\text{row } j \text{ of } M) \\
&= \#\text{ of 1's which match up between rows } i \text{ and } j,
\end{aligned}$$

as required.

71 Resolvable designs

Resolvable Designs

Definition 185 (Resolvable Design)**.** A design is said to be **resolvable** if the subsets can be partitioned so that each partition contains each of the elements once.

Note: A necessary condition for this to be possible is that k divide v.

Example: Our previous (12,9,4,3,1) design is resolvable.

$$\{1,2,3\},\ \{4,5,6\},\ \{7,8,9\},\ \{1,4,7\},\ \{2,5,8\},\ \{3,6,9\},$$
$$\{1,5,9\},\ \{2,6,7\},\ \{3,4,8\},\ \{1,6,8\},\ \{2,4,9\},\ \{3,5,7\}.$$

{123}	{456}	{789}
{147}	{258}	{369}
{159}	{267}	{348}
{168}	{249}	{357}

Properties of Kirkman Triples and Resolvable Designs

Definition 186 (Parallel Classes and Resolvable Designs)**.** Let $(X, \mathcal{A})$ be a BIBD with parameters (v, k, λ). A **parallel class** in $(X, \mathcal{A})$ is a subset of disjoint blocks from $\mathcal{A}$ whose union is X. A partition of $\mathcal{A}$ into r parallel classes is called a **resolution**, and $(X, \mathcal{A})$ is said to be a **resolvable** BIBD if $\mathcal{A}$ has at least one resolution.

For Kirkman triples $(v, 3, 1)$ we have

- $r = \dfrac{\lambda(v-1)}{k-1} = \dfrac{1}{2}(v-1), \quad b = \dfrac{vr}{k} = \dfrac{1}{6}v(v-1).$

- $\#$ parallel classes $= r$, $\quad \#$ blocks per class $= v/k$.

Theorem 187 (Inequality for Resolvable Designs)**.** *For resolvable designs, the inequality $b \geq v$ is strengthened to $b \geq v + r - 1$.*

Note: This was proved by Bose in 1942.

Solutions for Kirkman Triples

- $v = 3$: trivial, the 3 schoolgirls take a walk (note this is not an incomplete block as $b = k$).
- $v = 9$: corresponds to our earlier (12,9,4,3,1) design.

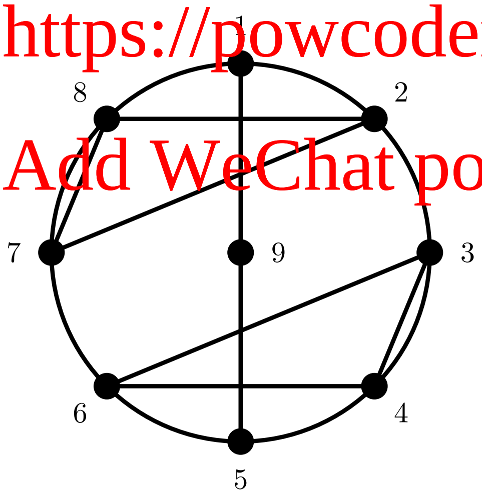
1	2	3	1	4	7	1	5	9	1	6	8
4	5	6	2	5	8	2	6	7	2	4	9
7	8	9	3	6	9	3	4	8	3	5	7

Only 1 solution in this case.

Solution can be obtained from a simple geometric design. Take a circle and place 8 points equidistantly on the perimeter with a 9th point at the centre.

This construction is from the chapter "Dinner Guests, Schoolgirls and Handcuffed Prisoners", in The Last Recreations, by Martin Gardner. Many nice constructions and fun problems - highly recommended reading.

Solution for Kirkman Triple, $v = 9$



Solution for Kirkman Triple, $v = 9$

Now rotate the circle in either direction one step at a time to four different positions. (The fifth step brings the pattern back to what it was originally.)

At each step copy down the triplet indicated by the ends and the centre of the straight line and the two triplets indicated by the corners of the two triangles. The three triplets found at each of the disk's four position give the triplets for each of the four days.

Labels of points on circle change as $a \mapsto (a \bmod 8) + 1$, while 9 stays put. So

1	5	9		1	3	8		1	2	4		1	6	7
2	7	8		2	6	9		3	7	9		2	3	5
3	4	6		4	5	7		5	6	8		4	8	9

This solution seems to be different from the design given above for the schoolgirl problem, but by substituting

$$1 \mapsto 1,\ 2 \mapsto 5,\ 3 \mapsto 7,\ 4 \mapsto 9,\ 5 \mapsto 3,\ 6 \mapsto 8,\ 7 \mapsto 6,\ 8 \mapsto 4,\ 9 \mapsto 2$$

we get the original design.

Solution for Kirkman triple, $v = 15$

Since 1922 the case of $v = 15$ has been known to have seven basic solutions.

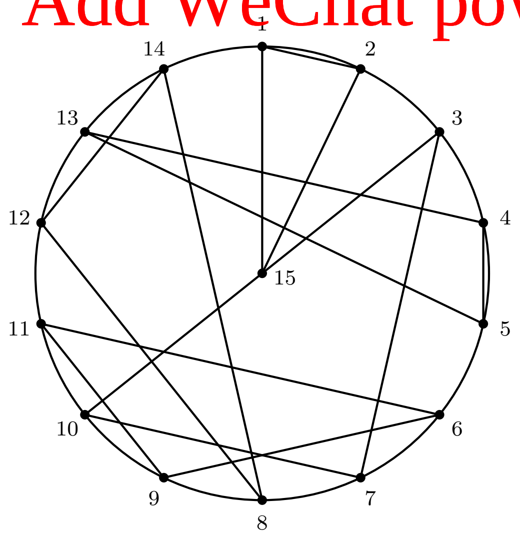
They can be generated by different patterns of triangles, with or without a diameter line.

One pattern of five triangles is shown below. In this case the disk must be rotated two units at a time to seven different positions. At each position the corners of each triangle provide one of the five triplets for that day.

So labels of points: $\quad a \mapsto (a + 1 \bmod 14) + 1,\ a \leq 14,\ \ 15 \mapsto 15.$

1	2	15		1	6	7			1	5	8
3	7	10		2	10	14			2	3	11
4	5	13		3	4	15	$\cdots$	$\cdots$	4	7	9
6	9	11		5	9	12			6	10	12
8	12	14		8	11	13			13	14	15

Geometric Solution for Kirkman Triple, $v = 15$



72 Hadamard matrices

Hadamard Matrices

Definition 188 (Hadamard Matrix)**.** A **Hadamard matrix** is a $n \times n$ matrix with ± 1 entries which satisfies

$$HH^{\mathrm{T}} = nI.$$

Note: By the definition the *rows* of a Hadamard matrix are orthogonal.

$\det(HH^{\mathrm{T}}) = \det(H)^2 = n^n$, so $|\det(H)| = n^{n/2}$.

This is the maximum possible value for ± 1 matrices.

$HH^{\mathrm{T}} = nI$ implies $H^{-1} = \frac{1}{n}H^{\mathrm{T}}$ and since $H^{-1}H = I$ we also have

$$H^{\mathrm{T}}H = nI.$$

So H^{T} is also a Hadamard matrix.

It also shows that the *columns* of a Hadamard matrix are orthogonal.

Hadamard Matrices

Example: For $n = 1$ and 2 we have

$$H_1 = \begin{pmatrix} +1 \end{pmatrix} \qquad H_2 = \begin{pmatrix} +1 & +1 \\ -1 & +1 \end{pmatrix}$$

It is possible to construct larger Hadamard matrices from smaller ones via matrix tensor product, e.g.,

$$H_4 = H_2 \otimes H_2 = \begin{pmatrix} +H_2 & +H_2 \\ -H_2 & +H_2 \end{pmatrix} = \begin{pmatrix} +1 & +1 & +1 & +1 \\ -1 & +1 & -1 & +1 \\ -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 \end{pmatrix}$$

Note: This construction can be repeated so

$$H_8 = H_2 \otimes H_4 = \begin{pmatrix} +H_4 & +H_4 \\ -H_4 & +H_4 \end{pmatrix}$$

This shows that there are Hadamard matrices of every size $n = 2^k, k \in \mathbb{N}$.

Size of Hadamard Matrices

Theorem 189 (Size of Hadamard Matrices)**.** *Hadamard matrices must have size $n = 1, 2,$ or $4k$.*

Proof: Assume that $n \geq 3$. Choose the Hadamard matrix to have its first row is all 1's (just multiply columns by ± 1 as required).

All other rows are orthogonal to the first, and so have $n/2$ $+1$'s and $n/2$ -1's.

Permute columns so that all 1's on the second row are to the left.

Finally, permute the columns within the left half so that the $+1$'s on the third row appear before the -1's, and likewise for the right half. Then

$$H = \begin{pmatrix} +1\cdots+1 & +1\cdots+1 & +1\cdots+1 & +1\cdots+1 \\ +1\cdots+1 & +1\cdots+1 & -1\cdots-1 & -1\cdots-1 \\ +1\cdots+1 & -1\cdots-1 & +1\cdots+1 & -1\cdots-1 \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Let the number of columns that start $+\,+\,+$ equal a, that start $+\,+\,-$ equal b, that start $+\,-\,+$ equal c, that start $+\,-\,-$ equal d.

Size of Hadamard Matrices

Let the number of columns that start $+\,+\,+$ equal a, that start $+\,+\,-$ equal b, that start $+\,-\,+$ equal c, and that start $+\,-\,-$ equal d.

Clearly,

$$a+b+c+d = n. \tag{3}$$

The rows are orthogonal so we get by taking dot-products of rows 1 and 2:

$$a+b-c-d = 0. \tag{4}$$

And similarly from rows 1 and 3 and rows 2 and 3 we get

$$a-b+c-d = 0, \tag{5}$$

$$a-b-c+d = 0. \tag{6}$$

Now $(2)+(3) \Rightarrow a=d,\;\; (2)+(4) \Rightarrow a=c,\;\; (3)+(4) \Rightarrow a=b,$ so

$$4a = n.$$

Since a is an integer, the result follows.

Hadamard Matrices and Square Designs

Theorem 190 (Hadamard Matrices and Square Designs)**.** *Hadamard matrices of size $n = 4k$ are in bijection to incidence matrices of square designs with parameters $(4k-1, 2k-1, k-1)$.*

Proof: Let $n = 4k$. Set first row and first column to all $+1$'s.

All other rows and columns must have $n/2$ $+1$'s and $n/2$ -1's.

Delete the first row and column.

Convert the -1's to 0's, and call the matrix $\overline{M}$.

Consider $\overline{M}$ as an incidence matrix: it has $b = 4k-1$, $v = 4k-1$, there are $2k-1$ 1's in each row and column, and the number of 1's which align in any two rows (or columns) is $k-1$.

This last fact is equivalent to our derivation that $a = n/4$ above. Since rows 2 and 3 are not special, *any* 2 rows must have exactly $n/4$ pairs of 1's in common columns, $n/4$ pairs of 0's.

Thus $\overline{M}$ is the incidence matrix of a $(4k-1, 2k-1, k-1)$ square design.

Hadamard Conjecture

The key open question in this topic is whether or not this statement is true:

Conjecture 191 (Hadamard)**.** *Hadamard matrices of size* $4k \times 4k$ *exists for all* $k \in \mathbb{N}$*.*

Note: Size $n = 668 = 4 \times 167$ smallest unresolved case, i.e., it is known that Hadamard matrices exists for $k \le 166$.

- Topic of much interest.
- Deep connections to other topics including error-correcting codes.
- Some asymptotic results exist, based on constructions and recursions, but they are not sufficiently strong.
- Major advance will be needed to find a Hadamard matrix of size $n = 668$, let alone answer the general question.

73 Error correcting codes

Error Correcting Codes

Context: We are attempting to transmit a message in binary code, and wish to avoid loss or corruption of data in case of noise, which may "flip" some of the binary digits.

Definition 192 (Codewords and Hamming Distance)**.** A **codeword** is a binary word, i.e., a word consisting of 0's and 1's. The **Hamming distance** p between codewords is defined as the number of digits which are different, e.g. for

$$p = 4: \qquad \begin{array}{ccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \uparrow & & \uparrow & \uparrow & \uparrow & & \end{array}$$

Note: If $\left\lfloor \frac{p-1}{2} \right\rfloor$ digits are reversed then the altered codeword is closest to a unique codeword in the set, and can be corrected.

Error Correcting Codes

Example: Suppose we have just two codewords

$$\begin{array}{ccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ \uparrow & & \uparrow & \uparrow & \uparrow & & \end{array}$$

Here $p = 4 \Rightarrow$ then $\left\lfloor \frac{4-1}{2} \right\rfloor = 1$ bit can be corrected.

If the message received was 0 1 0 1 0 0 0. This has distance 1 from the first code word, and distance 3 from the second codeword, and so could be corrected.

If the message received was 0 1 0 0 0 0 0. This has distance 2 from the first code word, and distance 2 from the second codeword, and so the message cannot be corrected.

Error Correcting Codes and Designs

The topics of block codes and block designs are intimately connected.

The first error correcting code, invented by Hamming in 1950, is related to the (7,4,1) square design and projective plane.

To convert a square design to a code:

- Take each row as a codeword.
- Each codeword has k 1s and $v - k$ 0s.
- Each pair of codewords have λ 1s in common.
- The remaining $(k - \lambda)$ 1s in each codeword must be aligned with zeroes.
- Thus there are $2(k - \lambda)$ different bits, which can correct $k - \lambda - 1$ errors.

Error Correcting Codes from Hadamard Matrices

- From the square design corresponding to a Hadamard matrix one obtains a code that can correct $n/4 - 1$ errors.
- Some of these codes are linear, which makes them easily computable.
- In 1961, using the computational resources of JPL, Golomb and Baumert found the first examples of Hadamard matrices of size 92×92 and 184×184.
- In 1971 Mariner 9 used the code derived from the Hadamard matrix $n = 32$.

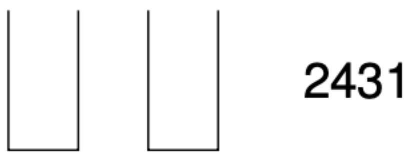
Pattern Avoiding Permutations

- In the 1st edition of Vol. 1 of "The Art of Computer Programming", Knuth asked which permutations various data structures can generate or sort.
- One question was "which permutations could be generated by a single stack?" Knuth solved this problem completely.
- Answer: σ is a stack sortable permutation if and only if it does not involve the permutation 231.
- Trying to sort 231 with a single stack:

Two Stacks in Parallel or Series

- In the problem section Knuth asked the same question of several other structures, such as two stacks in parallel. This can sort 231.

- Two stacks in series can sort 2431, which a single stack can't.



Patterns and Pattern Avoidance

Definition 1 (Pattern)**.** Let $\sigma \in S_n$ be a permutation of length n and $\tau \in S_k$ a permutation of length k, with $k \leq n$. τ occurs as a **pattern** in σ if for a subsequence of σ of length k the elements of the subsequence occur in the same relative order as the elements of τ.

Example: 1324 occurs twice as a pattern in 153264: 153264 and 153264

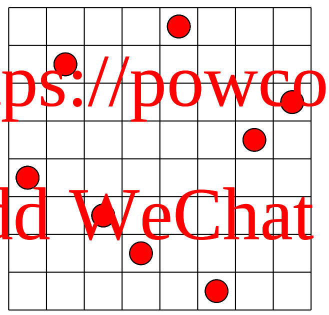
Definition 2 (Pattern Avoiding Permutations)**.** If a permutation τ does not occur in σ, σ is said to be a **pattern avoiding permutation** (PAP) with respect to τ.

Notation 3 (Number of Pattern Avoiding Permutations)**.** The number of permutations $\sigma \in S_n$ avoiding τ will be denoted as $S_n(\tau)$.

Grid Representation of Permutations

One can represent $\sigma \in S_n$ on a $n \times n$ square grid by filling in the cells (i, σ_i).

Example: The grid representation of $47328156 \in S_8$.



The pattern 231 The pattern 132 The pattern 1423

Pattern Avoiding Permutations

Theorem 4 (Number of 132 Avoiding Permutations)**.** *The number of permutations, $S_n(132)$, of length n avoiding the pattern 132 is C_n, the n'th Catalan number.*

Proof: Consider any permutation $\sigma \in S_n$ avoiding 132.

Assume that $\sigma_i = n$, that is, n appears in position i.

Any entry to the left of n must be larger than any entry to the right of n. If not we could find $\sigma_l < \sigma_r$ such that $\sigma_l \cdots n \cdots \sigma_r$ forms a 132 pattern.

This now means that the entries to the left of n and those to the right of n must both avoid 132 *independently* of each other.

Now, n can appear anywhere, so

$$S_n(132) = \sum_{i=1}^{n} S_{i-1}(132)S_{n-i}(132), \;\; S_0(132) = 1.$$

Beyond Knuth

- Knuth's work inspired responses by Tarjan (1972) and Pratt (1973).
- Pratt noted that the questions about permutations were more general, and of more interest, than the restricted questions on data structures.
- Since then, the study of PAPs has become an active field in its own right.
- Stanley and Wilf conjectured (late 1980s) that for every permutation τ, the number $S_n(\tau)$ of length n PAPs is at most κ^n.

  Note: There are $n!$ permutations so non-trivial conjecture.
- Arratia (1999) observed that this is equivalent to the convergence of

$$\kappa \;=\; \lim_{n\to\infty} S_n(\tau)^{1/n}.$$

- This was proved by Marcus and Tardos in 2004.
- Key question. Classify PAPs by the possible values of κ. PAPs with the same κ form a so-called Wilf class.

Wilf Classes for Patterns with $n < 4$.

- For $n = 2$, $\tau = 12$ or $\tau = 21$ and only the strictly decreasing/increasing permutations avoid these patterns, respectively.
- For $n = 3$, there are six permutations, forming 3 classes as the problem is symmetrical.

  For a given pattern τ look at the reverse pattern τ' (for $\tau = 132$ we have $\tau' = 231$). If σ avoids τ then the reverse of σ avoids τ'. This sets up an easy bijection to show $S_n(\tau) \;=\; S_n(\tau')$.
- For all 3 classes, $S_n(\tau) = C_n$, the n'th Catalan number.
- **Proof** that $S_n(132) = S_n(312)$.

  Consider the complement $\overline{\sigma}$ of $\sigma \in S_n$ defined by $\overline{\sigma}_i = n + 1 - \sigma_i$.

  Now 312 is the complement of 132 and if σ avoids 132 then $\overline{\sigma}$ avoids 312 and vice versa again setting up a simple bijection.

Left-Right Minima

Definition 5 (Left-Right Minimum)**.** A left-right minimum of a permutation σ is an index σ_j such that $\sigma_j < \sigma_i$, $i < j$.

σ_j is a left-right minimum if all entries appearing before σ_j and larger than σ_j.

Note: The left-right minima of σ form a *decreasing* subsequence.

Example:

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

has three left-right minima, 4, 3 and 1.

Note: σ_1 (leftmost entry) and the entry 1 are always left-right minima.

Wilf Class for 123

Theorem 6 (Wilf Class for 123)**.** *For all $n > 0$, $S_n(123) = S_n(132)$.*

Proof: We define a bijection from 132– to 123–avoiding permutations.

Take a 132-avoiding permutation and fix the left-right minima in place.

Remove all the elements that are not left-right minima.

Put the removed elements back into the empty slots in decreasing order. Note that this will not change the set of left-right minima. Why is this?

The resulting permutation in a union of two decreasing sequences and it is therefore 123-avoiding.

Wilf Classes for Patterns with $n = 4$.

- For $n = 4$, it turns out that the 24 possible permutations give rise to 3 distinct Wilf classes.
- For 1234, Gessel (1990) proved that

$$S_n(1234) = \frac{1}{(n+1)^2(n+2)} \sum_{k=0}^{n} \binom{2k}{k} \binom{n+1}{k+1} \binom{n+2}{k+1},$$

$$S_n(1234) \sim \frac{81\sqrt{3}}{16\pi} \cdot 9^n \cdot n^{-4}.$$

- The associated generating function is a 3rd order linear, homogeneous ODE whose solution is known in terms of hypergeometric functions.

$$\begin{aligned} &(x^2 - 11x^3 + 19x^4 - 9x^5)\frac{d^3G_{1234}(x)}{dx^3} \;+\; (9x - 90x^2 + 153x^3 - 72x^4)\frac{d^2G_{1234}(x)}{dx^2} \\ &\quad + (16 - 154x + 264x^2 - 126x^3)\frac{dG_{1234}(x)}{dx} \;-\; (32 - 72x + 36x^2)G_{1234}(x) \\ &\quad = 0 \end{aligned}$$

The second class, 1342.

- For 1342, Bóna (1997) showed that

$$S_n(1342) = (-1)^n \frac{(2+3n-7n^2)}{2} + 6\sum_{i=2}^{n} (-1)^{n-i}\, 2^i\, \frac{(2i-4)!}{i!(i-2)!} \binom{n-i+2}{2}.$$

- The generating function satisfies the linear ODE

$$(1-7x-8x^2)\frac{d^2 G_{1342}(x)}{dx^2} + (8-28x)\frac{dG_{1342}(x)}{dx} - 12G_{1342}(x) = 0.$$

- It can be exactly solved

$$G_{1342}(x) = \frac{32x}{1+20x-8x^2-(1-8x)^{3/2}},$$

  giving

$$S_n(1342) \sim \frac{64}{243\sqrt{\pi}} 8^n n^{-5/2}.$$

The third class, 1324.

- This class remains unsolved. Can prove

$$S_n(1342) < S_n(1234) < S_n(1324) \text{ for } n > 6.$$

- κ is not known. Rigorous bounds are $9.81 < \kappa < 13.002$.
- Johansson and Nakamura (2014) calculated $S_n(1324)$ for $n \le 30$.

- Conway, Guttmann and Zinn-Justin (2017) improved this to $n \le 50$.
- They conjectured

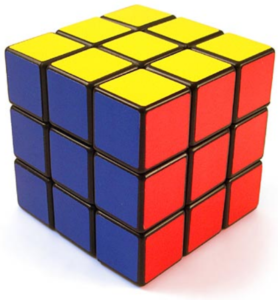
$$S_n(1324) \sim B \cdot \kappa^n \cdot \mu_1^{\sqrt{n}} \cdot n^g,$$

  where $\kappa = 11.600 \pm 0.003$, $\mu_1 = 0.0400 \pm 0.0005$ and $g = -1.1 \pm 0.1$.

- The stretched exponential term $\mu_1^{\sqrt{n}}$ is a new feature that had not previously been reported and it is not proved.

75 Rubik's cube

Rubik's cube objectives

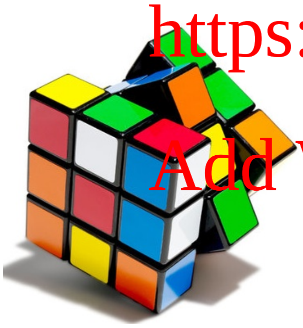
 

- Prove or characterise which configurations can be legally obtained.
- **Idea:** Map configurations to permutations and moves to the action of a permutation on the configuration.
- Calculate the number of different colour patterns possible by rotating the six outer faces of the cube.

Moves

There are two types of move:

- Middle moves and Face move

Middle moves: only middle layer moves (picture)

- Middle right, down or back

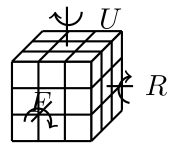
All can be achieved by face moves so won't be considered any further.

Face moves

The outer face moves are called

front (F)	right (R)	up (U)
back (B)	left (L)	down (D)

and refer to the position of the faces relative to the person holding the cube.



Rotations are words in $\{F, L, B, U, R, D\}$ (clockwise rotations by $90°$ and their inverses $F^{-1}, L^{-1}, B^{-1}, U^{-1}, R^{-1}, D^{-1}$ (anti-clockwise rotations).

Example: The set of face moves: $U^{-1}RU$,

(reading right to left) denotes rotating the up face $90°$ clockwise, then rotating the right face $90°$ clockwise and finally rotating the up face $90°$ anti-clockwise.

75.1 Configurations

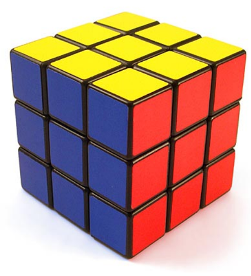
Configurations

How do we characterise all possible configurations?

We can treat the following as (almost) independent pieces of information

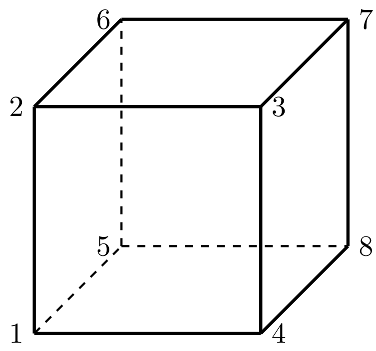
- position of corner cubes (with 3 visible faces)
- position of edge cubes (with 2 visible faces)

- orientation of corner cubes
- orientation of edge cubes



Corners

Label corners:



The elementary rotations can be expressed as permutations of the corner labels: $F = (1234)$, i.e. 1 goes to 2, 2 goes to 3, 3 goes to 4 and 4 goes to 1.

Corners

Notation 7 (Elementary Moves)**.** Each elementary move corresponds to a permutation $\rho \in S_8$

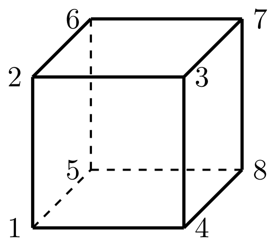
$$
\begin{aligned}
F &= (1234) & F^{-1} &= (1432)\\
B &= (5876) & B^{-1} &= (5678)\\
L &= (1562) & L^{-1} &= (1265)\\
R &= (3784) & R^{-1} &= (3487)\\
U &= (2673) & U^{-1} &= (2376)\\
D &= (1485) & D^{-1} &= (1584)
\end{aligned}
$$

Example: What is the effect of $U^{-1}R^{-1}UR$?

$$(2376)(3487)(2673)(3784) = (34)(67)$$

i.e. corners 3 and 4 are swapped, as well as corners 6 and 7.

Corners



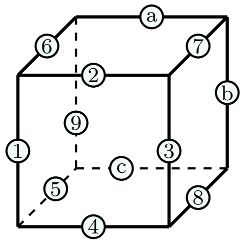
Example: Without computing, show that $\tau = F^{-1}UF^{-1}URU^{-1}$ cannot interchange two corners leaving others fixed.

- A single pair swap is odd: $\rho = (ij)$.
- All elementary moves are 4-cycles, and hence odd.

- τ consists of six elementary moves, and hence is even, and therefore cannot swap a single pair.

Edges

Label the edges:



Each elementary move corresponds to a permutation $\sigma \in S_{12}$.

$$\begin{aligned}
F &= (1234) & F^{-1} &= (1432)\\
B &= (9cba) & B^{-1} &= (9abc)\\
L &= (1596) & L^{-1} &= (1695)\\
R &= (37b8) & R^{-1} &= (38b7)\\
U &= (26a7) & U^{-1} &= (27a6)\\
D &= (48c5) & D^{-1} &= (45c8)
\end{aligned}$$

Note: Same elementary moves but different permutations.

Positions

Thus the **positions** of all cubes represented by a **pair** of permutations (ρ, σ) with $\rho \in S_8$ and $\sigma \in S_{12}$ with composition rule

$$(\rho', \sigma') \circ (\rho, \sigma) = (\rho' \circ \rho, \sigma' \circ \sigma).$$

Example: Compute the effect on the cube positions of the moves $B^{-1}RB$.

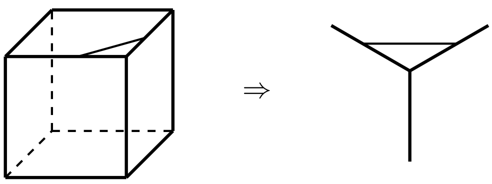
$$\begin{aligned}
B^{-1}RB &= \Big((5678), (9abc)\Big)\Big((3784), (37b8)\Big)\Big((5876), (9cba)\Big)\\
&= \Big((3854), (37c8)\Big)
\end{aligned}$$

$B^{-1}RB$ cyclically permutes the corner cubes 3, 8, 5 and 4 as well as cyclially permutes the edge cubes 3, 7, c and 8.

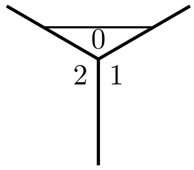
Orientations

What about orientations?

Define a rotation with respect to a mark or standard configuration:

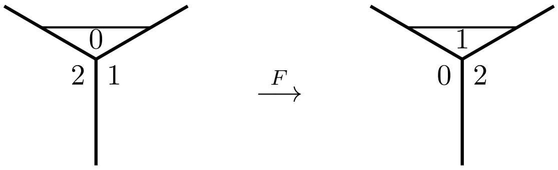


With respect to the standard (= solve) configuration, label each corner cube $0, 1, 2$ clockwise with the 0 inside the mark:



Orientations

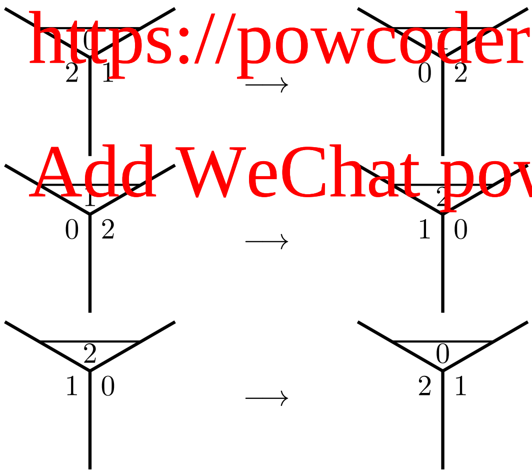
Under F, corner 3 goes to corner 4, and the orientation of corner 4 becomes that of corner 3 rotated **anti-clockwise** over $2\pi/3$. In mod 3 arithmetic:



corner at 3 corner at 4

mod 3 arithmetic

Let x_i be the value of the orientation variable in mark of corner i (i.e. in the solved configuration $x_i = 0$ for all i).



Are all of the form $x_i \mapsto x_i + 1 \pmod 3$.

Orientations

Example:

$$F(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_4 + 2, x_1 + 1, x_2 + 2, x_3 + 1, x_5, x_6, x_7, x_8)$$

or

$$R(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_1, x_2, x_4 + 1, x_8 + 2, x_5, x_6, x_3 + 2, x_7 + 1)$$

or

$$U(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_1, x_3, x_7, x_4, x_5, x_2, x_6, x_8)$$

All calculations are $\pmod 3$.

So corner configurations are labeled by 8-tuples $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$, and a key observation is that for cube moves

$$x_1 + x_2 + \ldots + x_8 = 0 \pmod 3.$$

Configurations

How do we characterise all possible configurations?

We can treat the following as (almost) independent pieces of information

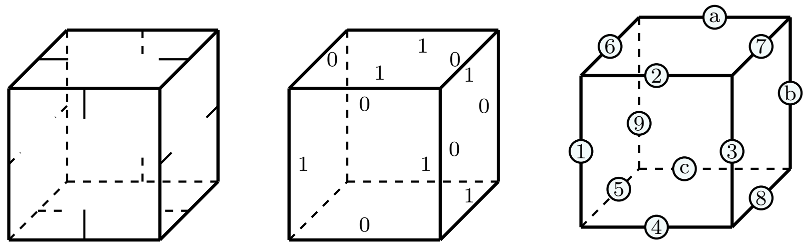
- position of corner cubes (with 3 visible faces)
- position of edge cubes (with 2 visible faces)
- orientation of corner cubes
- orientation of edge cubes

We have almost characterised cube configurations using triples (ρ, σ, x):

- $\rho \in S_8$ labels corner **positions**
- $\sigma \in S_{12}$ labels edge **positions**
- $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ with $x_1 + x_2 + \ldots + x_8 = 0 \pmod 3$ labels corner **orientations**

Edge Orientations

Edges come in two orientations, so we put marks and associate a variable y_i with each edge cube with $y_i = 0$ if the mark is present, and $y_i = 1$ if not.



Example: So mod 2 we get

$$R(y_1, \ldots, y_c) = (\ldots, y_8 \overset{3}{+} 1, \ldots, y_3 \overset{7}{+} 1, y_b \overset{8}{+} 1, \ldots, y_7 \overset{b}{+} 1, y_c).$$

Configurations

So a configuration of the cube is represented by (ρ, σ, x, y) where

- $\rho \in S_8$ are corner **positions**
- $\sigma \in S_{12}$ are edge **positions**
- $x = (x_1, \ldots, x_8)$ with $x_1 + x_2 + \ldots + x_8 = 0 \pmod 3$ are corner **orientations**
- $y = (y_1, \ldots, y_c)$ with $y_1 + y_2 + \ldots + y_c = 0 \pmod 2$ are edge **orientations**

As a group this is

$$S_8 \times S_{12} \times \mathbb{Z}_3^7 \times \mathbb{Z}_2^{11} / \mathbb{Z}_2$$

- not $\mathbb{Z}_3^8$ because one corner is fixed as a reference
- not $\mathbb{Z}_2^{12}$ because one edge is fixed as a reference
- quotient of $\mathbb{Z}_2$ because mixed parities of ρ and σ are not allowed.

The group structure implies that there exist moves that, say, change position of corners without changing edge cubes or orientations.

Cubology

Theorem 8 (First Law of Cubology)**.** *For any sequence of elementary moves:*

1. $\mathrm{sgn}(\rho) = \mathrm{sgn}(\sigma)$
2. $x_1 + x_2 + \ldots + x_8 = 0 \pmod 3$
3. $y_1 + y_2 + \ldots + y_{12} = 0 \pmod 2$

Proof: First, this holds for the standard configuration.

1. Elementary moves on corners and edges are 4-cycles $\Rightarrow$ all odd parity. Corners and edges change simultaneously so parities are "in sync".
2. Check that this holds for all elementary moves:
   - x_i's in U or D do not change
   - x_i's in R, L, F or B: two x_i's increase by $1 \pmod 3$ and two decrease by $1 \pmod 2$, so no change in $x_1 + x_2 + \ldots + x_8 = 0 \pmod 3$
3. Check explicitly that for all moves U, D, R, L, F and B the sum $y_1 + y_2 + \ldots + y_{12} = 0 \pmod 2$ does not change.

Cubology

Theorem 9 (Existence of Move Sequence)**.** *Every configuration satisfying the First Law can be attained by a sequence of elementary moves.*

Sketch of proof: The six-step strategy in the printed notes shows that any configuration can be obtained from the standard configuration (by "reverse solving").

Cubology

Theorem 10 (Number of Configurations)**.** *The number of possible configurations of Rubik's cube is (consistent with First Law)*

$$\frac{1}{12} \cdot 8! \cdot 12! \cdot 3^8 \cdot 2^{12} \approx 4.3 \times 10^9.$$

Proof: First we count the sizes of the 4 contributions to the configurations

- $8! = |S_8|$.
- $12! = |S_{12}|$.
- $3^8 \Rightarrow$ each $x_i \in \{0, 1, 2\}$.
- $2^{12} \Rightarrow$ each $y_i \in \{0, 1\}$.

But there are some constraints which reduce the count:

- $\frac{1}{2}$ as $\mathrm{sgn}(\rho) = \mathrm{sgn}(\sigma)$.
- $\frac{1}{3}$ as last corner cannot be chosen arbitrarily.
- $\frac{1}{2}$ as last edge cannot be chosen arbitrarily.