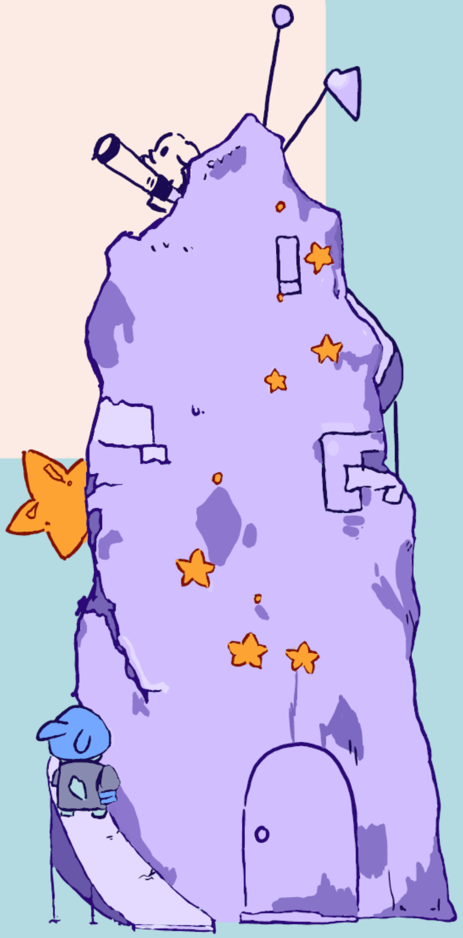
VE203 Midterm Review

Presenter: Yue & Yinchen

2023/6/18



Outline

- Set
- Logic
  - Truth tree
  - Natural induction rule
- Induction
- Function & relation
  - Injective & surjective
  - Properties of relations
- Formal Power Series
  - Application I: Solve linear recurrence
  - Application II: Prove combination identity
  - Application III: Advanced counting technique
- Pigeonhole principle
- Cardinality & Equinumerosity

Set

- Set: an **unordered** collection of **distinct** objects
- $A = B$ if and only if $A \subset B$ and $B \subset A$ / $\forall x \in A, x \in B \; and \; \forall y \in B, y \in A$
- Cardinality
  - ▶ $|A| = n \in \mathbb{N}$ if A is a finite set;
  - ▶ $|A| = \infty$ otherwise. (Question: infinities?)

Set operation:

Subset $A \subseteq B \iff \forall x(x \in A \implies x \in B)$

Union $\cup \mathcal{A} := \{x \mid \exists A \in \mathcal{A}(x \in A)\}$

Intersection $\cap \mathcal{A} := \{x \mid \forall A \in \mathcal{A}(x \in A)\}$

Set difference $A - B = \{x \in A \mid x \notin B\}$

Symmetric difference $A \Delta B = (A - B) \cup (B - A)$

Powerset $P(X) := \{A \mid A \subseteq X\} = \{A \mid \forall x(x \in A \implies x \in X)\}$

Empty set $\emptyset = \{x \mid false\}$

Ordered pair & Cartesian Product

- Kuratowski's definition: $(a,b) := \{\{a\},\{a,b\}\}$
- Property: $(x,y) = (a,b) \iff x = a \;\&\; y = b$
- Valid encode:
  - Ordered pair $(a,b) := \{\{0,a\},\{1,b\}\}$ (the definition of 0 and 1 is not restricted, we only need to know these are two different objects)
  - Ordered triple $(a,b,c) := ((a,b),c)$.
  - n-tuple $(x_0,\ldots,x_{n-1}) := (((x_0,x_1),x_2),\ldots,x_{n-1})$.
- Invalid encode: $(a,b,c) = (d,e,f) \iff a = d \;\&\; b = e \;\&\; c = f$
  - Ordered triple $(a,b,c) := \{\{a\},\{a,b\},\{a,b,c\}\}$ $(a,b,c) := \{\{0,a\},\{1,b\},\{2,c\}\}$
- Cartesian Product

  For two sets X, Y , their Cartesian product is

$$X \times Y := \{(x,y) \mid x \in X \;\&\; y \in Y\} = \{p \mid \exists x \in X \; \exists y \in Y (p = (x,y))\}$$

Some examples:

Logic

Imply: $p \to q \iff \neg p \vee q$

How to prove a statement is true:

- From definition

$$\begin{aligned} x \in (P \cap Q)' \quad & \text{if and only if} \quad x \notin P \cap Q, \\ & \text{if and only if} \quad x \notin P \text{ or } x \notin Q, \\ & \text{if and only if} \quad x \in P' \text{ or } x \in Q', \\ & \text{if and only if} \quad x \in P' \cup Q'. \end{aligned}$$

- Truth table

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

- Truth tree: systematically derive a contradiction from the **assumption** that a certain set of statements is true.
  - Infers which statements are forced to be true under this assumption.
  - When nothing is forced, then the tree branches into the possible options

  All branch lead to contradiction: the original statement is true(as you make the opposite assumption)

  Some branch failed to lead to contradiction: can't derive anything. Giving counter examples can prove the original statement is false / or change the assumption to prove again

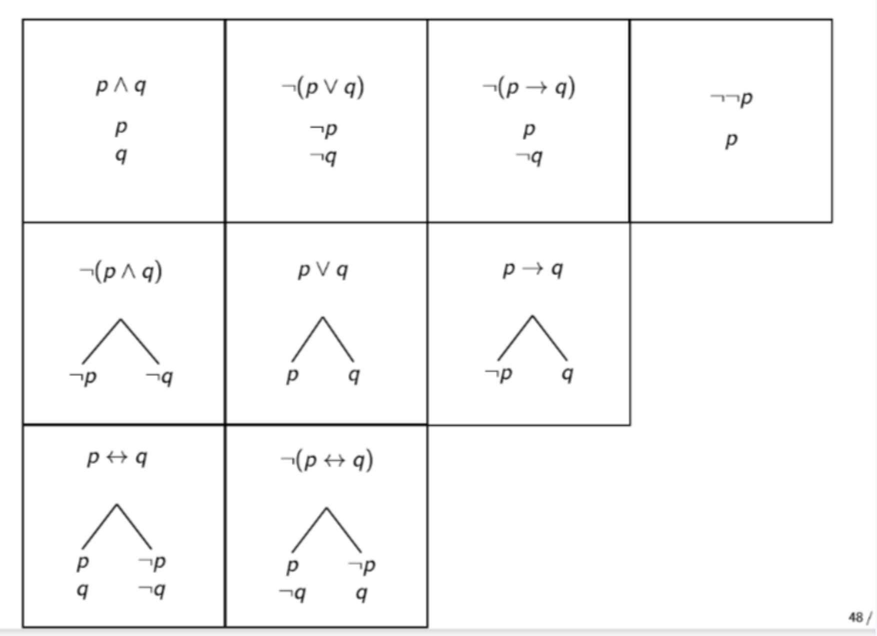
Opposite of the statement you want to prove to be true

- Natural deduction: formally derive the statement from (classical) logical rules

Truth tree

- With logic operator (this table **will not be provided in exam**
- With $\forall$ *and* $\exists$

$$\neg[\exists x \in M : A(x)] \Leftrightarrow \forall x \in M : \neg A(x)$$
$$\neg[\forall x \in M : A(x)] \Leftrightarrow \exists x \in M : \neg A(x)$$



$\exists x,\ P(x)$: exist a that P(a) is true, while a is a new constant symbol here

$P(a)$ should **use a new symbol each time**,
as we don't know what a is, only know a exists

$\forall x,\ \neg P(x)$: can choose arbitrary x. but…how to choose? $\neg P(b)$ is true, but useless

$\neg P(a)$ "**Delay" the choose**! (create contradictory)

Good practice:

Exercise 1.4 (8 pts) Use the truth tree method to justify whether the following entailments are correct, or find a counterexample.

(i) **(2 pts)** $\forall x \exists y (P(x) \vee Q(y)) \vdash \exists y \forall x (P(x) \vee Q(y))$

Natural Deduction Rules

What is the small “a”?
Tags for assumptions!

Assumption

$$\frac{A \in \Gamma}{\Gamma \vdash A}\ \text{(assumption)}$$

Conjunctions

$$\frac{A \quad B}{A \wedge B}\,\wedge\mathrm{I}$$

$$\frac{A \wedge B}{A}\,\wedge\mathrm{E}_1 \qquad \frac{A \wedge B}{B}\,\wedge\mathrm{E}_2$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge\text{-I})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge\text{-E-L}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge\text{-E-R})$$

Absurdities

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ (\bot\text{-E}) \qquad \frac{\bot}{A}\,\bot\mathrm{E}$$

$$\neg A \overset{abbr}{=} A \supset \bot$$

$$\frac{\begin{matrix}[A]^a \\ \vdots \\ \bot\end{matrix}}{\neg A}\,\neg\mathrm{I},a$$

$$\frac{\neg A \quad A}{\bot}\,\neg\mathrm{E}$$

Disjunctions

$$\frac{A}{A \vee B}\,\vee\mathrm{I}_1 \qquad \frac{B}{A \vee B}\,\vee\mathrm{I}_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee\text{-I-L}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee\text{-I-R})$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{A \vee B \quad \begin{matrix}[A]^a \\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]^a \\ \vdots \\ C\end{matrix}}{C}\,\vee\mathrm{E},a$$

Implication

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}\ (\supset\text{-I}) \qquad \frac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B}\ (\supset\text{-E})$$

$$\frac{\begin{matrix}[A]^a \\ \vdots \\ B\end{matrix}}{A \to B}\,\to\mathrm{I},a \qquad \frac{A \to B \quad A}{B}\,\to\mathrm{E}$$

Axiom of the Excluded Middle

$$\frac{}{\Gamma \vdash A \vee \neg A}\ \text{(AEM}$$

only in classical logic,
not in constructive logic

$$\frac{\begin{matrix}[\neg A]^a \\ \vdots \\ \bot\end{matrix}}{A}\,\mathrm{DN},a$$

Interesting fact: these two can not derive each other

- Prove by definition: Prove that for any sets $\mathcal{A}, B$, we have $\bigcup \mathcal{A} \subseteq B \iff \mathcal{A} \subseteq \mathcal{P}(B)$.

(I don't think this would appear in the exam but this can check you understand of definitions)

- Prove by truth tree $((p \to q) \land (\neg r \to \neg q)) \vdash (p \to r)$

- Prove by natural deduction rules $((p \to q) \land (\neg r \to \neg q)) \to (p \to r)$

Induction

Recursive definition

A ***binary tree*** is either:

- the empty tree, denoted by `null`; or
- a root node x, a ***left subtree*** T_ℓ, and a ***right subtree*** T_r, where x is an arbitrary value and T_ℓ and T_r are both binary trees.

Linked Lists

A ***linked list*** is either;

- $\langle\rangle$, known as the ***empty list***; or
- $\langle x, L\rangle$, where x is an arbitrary element and L is a linked list.

Structural proof :

To prove a statement P(t), $\forall\, tree\ t$

1. Prove P(leaf)
2. If P(left), P(right), value x, prove P(node(x, left; right))

To prove a statement P(l), $\forall\, list\ l$

1. Prove P(nil) (empty list)
2. If P(l), and a is an element, prove P(<a, l>)

Induction

Monoid: a set equipped with **an associative binary operation** and **an identity element.**

The order of elements matters(as no commutative rule) but the order of operation(calculate which part first) doesn't matter

```
('a -> 'b -> 'b) -> 'b -> 'a list -> 'b
let rec foldr f a l =
  match l with
  | [] -> a
  | x :: xs -> f x (foldr f a xs)

('a -> 'b -> 'a) -> 'a -> 'b list -> 'a
let rec foldl f a l =
  match l with
  | [] -> a
  | x :: xs -> foldl f (f a x) xs
```

Definition (Monoid)

A ***monoid*** is a triple $(M, e, \star)$, where M is a set, together with an identity element $e \in M$, and a function $M \times M \to M$, such that for all $m, n, p \in M$, the following ***monoid laws*** hold,

- $m \star e = m$ and $e \star m = m$
- $(m \star n) \star p = m \star (n \star p)$

monoid => foldr and foldl have the same effort

Induction

- Weak induction

Natural number

$$\frac{}{zero \ \text{nat}}$$

$$\frac{a \ \text{nat}}{succ(a) \ \text{nat}}$$

Principle of Mathematical Induction

Given a predicate $P : \mathbb{N} \to \mathbb{B}$, then $P(n)$ is true for all $n \in \mathbb{N}$ provided that

(I) **base case**: $P(0)$ is true.

(II) **inductive case**: whenever $P(n)$ is true, $P(n+1)$ is true, i.e.,

$$(\forall n \in \mathbb{N})(P(n) \to P(n+1))$$

In the inductive case, $P(n)$ is called ***inductive hypothesis***, often abbreviated as ***IH***.

As a formula, (I) and (II) can be combined as

$$[P(0) \land (\forall n \in \mathbb{N})(P(n) \to P(n+1))] \vdash (\forall n \in \mathbb{N})P(n)$$

- Strong/complete induction

Supppse over $\mathbb{N}$ we have

(I) $P(0)$.

(II) $(\forall n)[(\forall k < n)P(k) \to P(n)]$.

Then $(\forall n)P(n)$.

Please clearly write the base case, IH and inductive case when you are writing proof

Definition

The set Σ^* of ***strings*** over the alphabet Σ is defined recursively by

- $\varepsilon \in \Sigma^*$, where ε is the empty string containing no symbols.
- If $a \in \Sigma$ and $x \in \Sigma^*$, then $ax \in \Sigma^*$, where $ax := (a, x)$ is an ordered pair.

Note that $\varnothing^* = \{\varepsilon\}$.

Definition

Let Σ be a set of symbols and Σ^* the set of strings over Σ. We can define the ***concatenation*** of two strings, denoted by $\cdot : \Sigma^* \times \Sigma^* \to \Sigma^*$, recursively as follows.

- If $z \in \Sigma^*$, then $\varepsilon \cdot z := z$, where ε is the empty string.
- If $w, z \in \Sigma^*$ and $w = ax$, then $w \cdot z = ax \cdot z := a(x \cdot z)$. $\boldsymbol{a \in \Sigma}$

The concatenation of the strings w_1 and w_2 is often written as the juxtaposition $w_1 w_2$ instead of $w_1 \cdot w_2$.

Exercise 2.2 (2 pts) Show that concatenation of string is associative, i.e., $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in \Sigma^*$.

Given an alphabet $\Sigma = \{a, b, c\}$, a, b, c are distinct. Consider the subset of strings $A \subset \Sigma^*$ recursively defined by

$a \in A$

if x $\in A$, $bx \in A$

if x $\in A$, $xc \in A$

prove that $A = \{b^n a c^m \mid m, n \in \mathbb{N}\}$.

- How to prove two sets are equal
- How to prove the base case
- What is the IH
- How to prove the inductive case

Relation & Function

Relation: subset of a **Cartesian product**

Elements in **relation**: **ordered pairs**

Function: some special **relations**

Ordered pair(Kuratowski): For any x, y, let $(x, y) := \{\{x\}, \{x, y\}\}$.

For two classes X, Y , their **Cartesian product** is $X \times Y := \{(x, y) \mid x \in X \,\&\, y \in Y\}$

A set (or class) R is a binary **relation** if each of its elements is an **ordered pair** (x, y), in which case we write $x\,R\,y :\Longleftrightarrow (x, y) \in R$.

e.g.: $\in = \{(x, y) \mid x \in y\}$.

$domain(R) := \{x \mid \exists y\, ((x, y) \in R)\}$, $range(R) := \{y \mid \exists x\, ((x, y) \in R)\}$.

A **relation** f is a **function** if for each x in domain(f), there exist unique y such that x f y, we denote this y by f(x).

$(\forall x \in A)(\exists! y(xFy))$

If f is a function, domain(f) = X, and range(f) ⊆ Y , then we say that f is a function from X to Y , denoted f : X → Y , and call Y a **codomain** of f.

$$Y^X := \{f \mid f \text{ is a function } X \to Y\}.$$

Operation on Relation/Function

For arbitrary sets/relations/functions A, F, and G,

- The ***inverse*** of F is the set

$$F^{\top} = F^{-1} = \{(y, x) \mid xFy\}$$

- The ***composition*** of F and G is the set (beware of the order)

$$G \mathbin{;} F = F \circ G = \{(x, z) \mid \exists y(xGy \wedge yFz)\}$$

- The ***restriction*** of F to A is the set

$$F|A = \{(x, y) \mid (xFy) \wedge (x \in A)\}$$

- The ***image*** of A ***under*** F is the set

$$F(A) = \mathrm{im}\,(F|A) = \{y \mid (\exists x \in A)(xFy)\}$$

  If F is a function, then $F(A) = \{F(x) \mid x \in A\}$.

Theorem
Given a set A, the triple $(\mathcal{P}(A \times A), \mathbin{;}, \mathrm{id}_A)$ is a monoid.

Injection & Surjection

- For two functions $f, g : X \to Y$, we have $f = g \iff \forall x \in X\ (f(x) = g(x))$
- Partial function: $domain\ f \subseteq A$ Total function: domain $f = A$

Given a function $F: A \to B$, with dom $F = A$ and im$(F) \subset B$,

- Injective/one-to-one: $(\forall x, y \in A)(F(x) = F(y) \to x = y)$.
- Surjective/onto: im(F)=B
- Bijective: injective & surjective

Properties of relations

Partial order:

non-strict: reflexive, antisymmetric, transitive $\leq, \subseteq$

strict: irreflexive, asymmetric,

antisymmetric, transitive $<$

Total order:

partial order + total(any two can be compared)

e.g., divisibility, subset relation are **not** total order

Equivalence relation:

reflexive, symmetric, transitive

e.g.,$=, \equiv, isomorphism$

Definition

A (binary) relation R on A, i.e., $R \subset A \times A$, is

- *reflexive* if $(\forall x \in A)(xRx)$.
- *irreflexive* if $(\forall x \in A)(xRx \to \bot)$.
- *strongly connected* or *total*[3] if $(\forall x, y \in A)(xRy \vee yRx)$.
- *transitive* if $(\forall x, y, z \in A)(xRy \wedge yRz \to xRz)$.
- *symmetric* if $(\forall x, y \in A)(xRy \to yRx)$.
- *anti-symmetric* if $(\forall x, y \in A)(xRy \wedge yRx \to x = y)$.
- *asymmetric* if $(\forall x, y \in A)(xRy \wedge yRx \to \bot)$.

(1) Let X, Y be sets, $R \subseteq X \times Y$ be a binary relation. Let $\mathrm{id}_X, \mathrm{id}_Y$ denote the identity (i.e., equality) relations on X, Y respectively. Consider the following conditions:

(i) $R^{-1} \circ R \subseteq \mathrm{id}_X$	(v) $\mathrm{dom}(R) = X$
(ii) $R^{-1} \circ R \supseteq \mathrm{id}_X$	(vi) $\mathrm{rng}(R) = Y$
(iii) $R \circ R^{-1} \subseteq \mathrm{id}_Y$	(vii) R is a partial function (with $\mathrm{dom}(R) \subseteq X$)
(iv) $R \circ R^{-1} \supseteq \mathrm{id}_Y$	(viii) R^{-1} is a partial function

(a) Prove that each condition on the left is equivalent to one on the right (which?).
(b) Conclude that R is a function $X \to Y$ iff two conditions (which?) on the left hold.
(c) Conclude that R is an injection $X \to Y$ iff some conditions (which?) on the left hold.
(d) Conclude that R is a surjection $X \to Y$ iff some conditions (which?) on the left hold.

Example 2.80. For any set X, there is a bijection between subsets of X and their **indicator** (or **characteristic**) functions:

$$\begin{aligned} \mathcal{P}(X) &\cong 2^X \\ A &\mapsto \begin{pmatrix} \chi_A : X \to 2 = \{0,1\} \\ \qquad x \mapsto \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{else} \end{cases} \end{pmatrix} \\ f^{-1}[\{1\}] &\leftarrow\!\shortmid f. \end{aligned}$$

Example 2.81. For any sets X, Y, Z, we have bijections

$$\begin{aligned} Z^{X\times Y} &\cong (Z^X)^Y \\ f &\mapsto (y \mapsto (x \mapsto f(x,y))) \\ (g(y)(x) \leftarrow\!\shortmid (x,y)) &\leftarrow\!\shortmid g, \end{aligned}$$

and similarly $Z^{X\times Y} \cong (Z^Y)^X$.

Exercise 2.82. Give a bijection $\mathcal{P}(X \times Y) \cong \mathcal{P}(X)^Y$.

Formal Power Series

Definition

A ***formal power series*** is an expression

$$A(x) = \sum_{n \geq 0} a_n x^n$$

which is called the ***generating function*** of the sequence (a_n), where x is usually called the ***variable*** or ***indeterminate***. Specifically, we identify x with the sequence $(0, 1, 0, 0, \dots)$. We also write the scalar coefficients as $[x^n]A(x) = a_n$. In general, the scalar coefficients could be taken as elements of a ring.

Properties of Formal Power Series (Cont.)

- Multiplication: $A(x)B(x) = \sum_{n \geq 0} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n$.
  - commutative: $A(x)B(x) = B(x)A(x)$
  - associative: $(A(x)B(x))C(x) = A(x)(B(x)C(x))$
  - multiplicative identity: $1 \cdot A(x) = A(x)$ for all $A(x)$, where $1 = 1 + 0x + 0x^2 \cdots$
- Distributivity: $A(x)(B(x) + C(x)) = A(x)B(x) + A(x)C(x)$

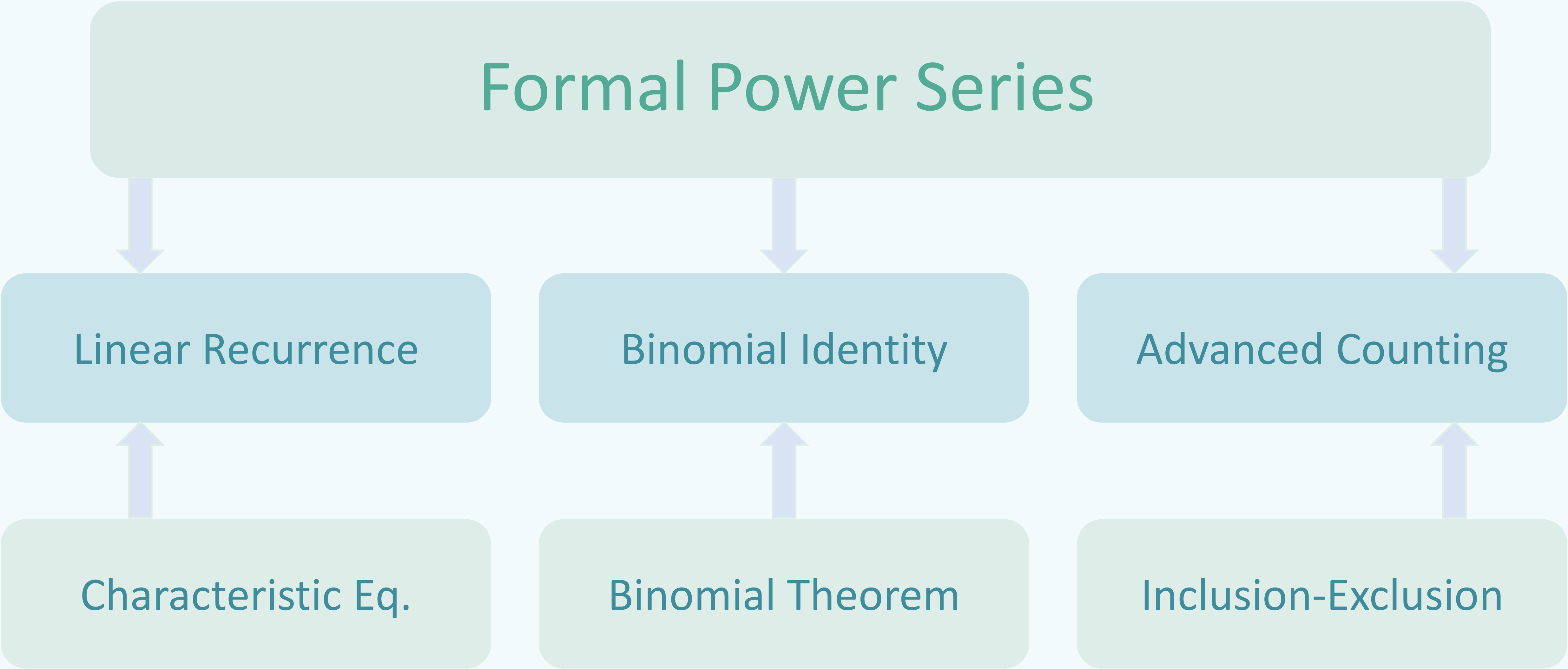
To summarize, formal power series forms a ***commutative ring***.

A generating function is a clothesline on which we hang up a sequence of numbers for display.

一个生成函数就是一根晾衣绳，

我们把一个数列挂在上面供人看。

——H.S.WILF (1989)


Formal Power Series
Linear Recurrence
Binomial Identity
Advanced Counting
Characteristic Eq.
Binomial Theorem
Inclusion-Exclusion

Linear Recurrence Relations

A sequence $(a_n) = (a_0, a_1, a_2, \dots)$ satisfies a (homogeneous) linear recurrence relation of order d if there exists constants $c_1, c_{2,}, \dots, c_d$ with $c_d \neq 0$ such that

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_d a_{n-d}$$

for all $n \geq d$.

Consider the second order case when $d = 2$: $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, $n \geq 2$, $c_2 \neq 0$. We call $\chi(t) = t^2 - c_1 t - c_2$ the ***characteristic polynomial*** of the linear recurrence relation. Let r_1 and r_2 be roots of χ, i.e., $\chi(t) = (t - r_1)(t - r_2)$, or

$$r_{1,2} = \frac{c_1 \pm \sqrt{c_1^2 - 4c_2}}{2}$$

Note that $r_1 \neq 0$ and $r_2 \neq 0$.

Theorem

If $r_1 \neq r_2$, then there exist constants α_1, α_2 such that $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

Theorem

For the second order linear recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, if the characteristic polynomial χ has repeated roots r, i.e., $\chi(t) = (t - r)^2$, then there exist constants α_1 and α_2 such that $a_n = (\alpha_1 + \alpha_2 n) r^n$ for all $n \geq 0$.

General Strategy

Homogeneous solution + (any) particular solution

Example

Find the general solution to

$$(T + 2)(T - 6)a_n = 3^n$$

- Homogeneous solution: $a_n^{(h)} = \alpha_1(-2)^n + \alpha_2 6^n$.
- Particular solution: Try $a_n^{(p)} = d3^n$. ($\Rightarrow d = -1/15$)

General solution

$$a_n = \alpha_1(-2)^n + \alpha_2 6^n - \frac{1}{15}3^n$$

Solving Linear Recurrence

Exercise 2 (10 points)

Find the **general solution** to the following inhomogeneous linear recurrence equation

$$y_{n+2} - 5y_{n+1} + 6y_n = n^2 \cdot 3^n$$

Solution: First note that the homogeneous solution is given by $y_n^{(h)} = c_1 \cdot 2^n + c_2 \cdot 3^n$. Next assume that a particular solution is given by $y_n^{(p)} = (an + bn^2 + cn^3) \cdot 3^n$, then

$$\begin{aligned} y_{n+2} - 5y_{n+1} + 6y_n = {} & [a(n+2) + b(n+2)^2 + c(n+2)^3] \cdot 3^{n+2} \\ & - 5[a(n+1) + b(n+1)^2 + c(n+1)^3] \cdot 3^{n+1} \\ & + 6[an + bn^2 + cn^3] \cdot 3^n && (2) \\ = {} & [a + 7b + 19c + (2b + 21c)n + 3cn^2]3^{n+1} && (3) \\ = {} & [3(a + 7b + 19c) + 3(2b + 21c)n + 9cn^2]3^n && (4) \end{aligned}$$

therefore we have

$$\begin{cases} a + 7b + 19c = 0 \\ 2b + 21c = 0 \\ 9c = 1 \end{cases} \qquad (5)$$

which yields $a = \frac{109}{18}$, $b = -\frac{7}{6}$, $c = \frac{1}{9}$. Therefore we have a particular solution given by

$$y_n^{(p)} = \left(\frac{109}{18}n - \frac{7}{6}n^2 + \frac{1}{8}n^3\right)3^n \qquad (6)$$

hence the general solution is given by

$$y_n = y_n^{(h)} + y_n^{(p)} = c_1 2^n + \left(c_2 + \frac{109}{18}n - \frac{7}{6}n^2 + \frac{1}{8}n^3\right)3^n \qquad (7)$$

where c_1, c_2 are arbitrary constants.

Could you try to solve with generating function?

I tried but 😣 😰 it's too hard....

$$\sum_{n \geq 0} 3^n n^2 x^n = \frac{3x(1+3x)}{(1-3x)^3}$$

Solving Linear Recurrence

To solve $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, let $A(x) = \sum_{n\geq 0} a_n x^n$.

Proof (Formal Power Series, Cont.)

Hence $A(x) = a_0 + a_1 x + c_1 x(A(x) - a_0) + c_2 x^2 A(x)$, hence

$$A(x) = \frac{a_0 + a_1 x - c_1 a_0 x}{1 - c_1 x - c_2 x^2} = \frac{a_0 + a_1 x - c_1 a_0 x}{(1 - r_1 x)(1 - r_2 x)}$$

We can use partial fraction to get (recall that $r_1 \neq r_2$)

$$A(x) = \frac{\alpha_1}{1 - r_1 x} + \frac{\alpha_2}{1 - r_2 x} = \alpha_1 \sum_{n\geq 0} (r_1 x)^n + \alpha_2 \sum_{n\geq 0} (r_2 x)^n$$

that is,

$$\sum_{n\geq 0} a_n x^n = \sum_{n\geq 0} (\alpha_1 r_1^n + \alpha_2 r_2^n) x^n$$

Compare coefficients, we get $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n \geq 0$.

Proof.

Same as before, we get

$$A(x) = \frac{a_0 + (a_1 - c_0 a_1 x)}{(1 - rx)^2}$$

Then by partial fraction, there exist constants β_1, β_2 such that

$$A(x) = \frac{\beta_1}{1 - rx} + \frac{\beta_2}{(1 - rx)^2}$$
$$= \beta_1 \sum_{n\geq 0} (rx)^n + \beta_2 \sum_{n\geq 0} (n+1)(rx)^n$$

Solving Linear Recurrence

Consider the linear recurrence relation given by:

$$a_n = 5a_{n-1} - 6a_{n-2} + 2^n$$

with initial conditions $a_0 = 1, a_1 = 3$.

Find a_n's closed-form expression.

Solving Linear Recurrence

By the recurrence relation,

$$\frac{A(x) - 1 - 3x}{x^2} = 5\frac{A(x) - 1}{x} - 6A(x) + \frac{1}{1 - 2x}$$

Apply partial fraction, we get

$$A(x) = \frac{1 + 5x^2 - 4x}{(1 - 2x)^2(1 - 3x)} = 2\frac{1}{1 - 3x} - \frac{1}{2}\frac{1}{1 - 2x} - \frac{1}{2}\frac{1}{(1 - 2x)^2}$$

Therefore,

$$b_n = [x^n]A(x) = 2 \cdot 3^n - 2^n - \frac{1}{2}n \cdot 2^n$$

Binomial Theorem

Definition

Let $m \in \mathbb{Q}$, define $\binom{m}{0} := 1$, and

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

where $k \in \mathbb{N} \setminus \{0\}$. Note that if $m \in \mathbb{N} \setminus \{0\}$, then $\binom{m}{k} = \frac{m!}{k!(m-k)!}$.

Theorem (Binomial Theorem)

Let $m \in \mathbb{Q}$, then

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

Example

If $m = -1$, then

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

Binomial Coefficient in $\mathbb{N}$

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

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

$$\sum_{k=0}^{n} \binom{k}{m} = \binom{n+1}{m+1}$$

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

Proving Combinational Identities

Exercise 4.6 For integers $n, k \geq 0$, prove Pascal's identity

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

by verifying the following equalities of generating functions.

(i) $\sum_{k \geq 0} \binom{n+1}{k+1} x^k = \sum_{k \geq 0} \left[\binom{n}{k} + \binom{n}{k+1} \right] x^k$

Proving Combinational Identities

$$LHS = \sum_{k\geq 0}\binom{n+1}{k+1}x^k = \frac{1}{x}\cdot\sum_{k\geq 0}\binom{n+1}{k+1}x^{k+1} = \frac{1}{x}\cdot\left(\sum_{k\geq 0}\binom{n+1}{k}x^k - \binom{n+1}{0}x^0\right)$$

$$= \frac{1}{x}\cdot\left(\sum_{k\geq 0}\binom{n+1}{k}x^k - 1\right) = \frac{1}{x}\cdot\left((1+x)^{n+1} - 1\right)$$

$$RHS = \sum_{k\geq 0}\binom{n}{k+1}x^k + \sum_{k\geq 0}\binom{n}{k}x^k = \frac{1}{x}\cdot\left((1+x)^n - 1\right) + (1+x)^n$$

$$= \frac{1}{x}\cdot\left((1+x)^n\cdot(1+x) - 1\right) = LHS$$

Exercise

Prove the **Vandermonde's identity**

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

by evaluate the coefficient of x^r in

$$(1+x)^{m+n} = (1+x)^m \cdot (1+x)^n$$

Advanced Counting Technique

An example from chatGPT

Suppose we have n identical candies and 3 children. How many ways are there to distribute the candies among the children if each child can receive any number of candies (including none)?

Since each child can receive any number of candies, the generating functions for each child can be written as:

$$C_i(x) = 1 + x + x^2 + x^3 + \cdots$$

To find the generating function that represents the distribution of candies among all three children, we multiply the generating functions for each child together:

$$C(x) = C_1(x) \cdot C_2(x) \cdot C_3(x)$$

Advanced Counting Technique

Expanding this product using algebraic multiplication, we get:

$$C(x) = \left(1 + x + x^2 + x^3 + \cdots\right)^3 = (1 - x)^{-3}$$

The coefficient of x^k in the power series expansion represents the number of ways to distribute the k candies among the 3 children.

$$[x^k](1 - x)^{-3} = (-1)^k \cdot \binom{-3}{k} = \binom{k+2}{k} = \binom{k+2}{2}$$

Therefore, the number of ways to distribute the n candies among 3 children is $\binom{n+2}{2}$.

Advanced Counting Technique

Exercise 4.3 Consider $n \in \mathbb{N}$, $n \geq 2000$.

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 \leq n$$

Use generating function to find the number of integer solutions if

(ii) $1 \leq x_i \leq 5$ for $i = 1, \ldots, 6$ and $3 \mid x_7$;

Consider the generating function

$$f(x) = \left(x + x^2 + x^3 + x^4 + x^5\right)^6 \cdot \left(1 + x^3 + x^6 + \cdots\right) \cdot \left(1 + x + x^2 + \cdots\right)$$

Then the number of solutions is the coefficient of x^n.

Inclusion-Exclusion Principle

Notation

Given $I \subset [n]$, we let

$$A_I := \bigcap_{i \in I} A_i,$$

where $A_i \subset X$ for all $i \in I$. For example, $A_{\{1,2,4\}} = A_1 \cap A_2 \cap A_4$. In particular, $A_\varnothing = X$.

Theorem (Inclusion-Exclusion Principle)

Let $A_1, \ldots, A_n$ be subsets of X. Then the number of elements of X which lie in none of the subsets A_i is

$$\sum_{I \subset [n]} (-1)^{|I|} |A_I| = \sum_{r \geq 0} (-1)^r \sum_{|I|=r} |A_I|$$

Inclusion-Exclusion Principle

Corollary

Let $A_1, \cdots, A_n$ be a sequence of (not necessarily distinct) sets, then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\varnothing \neq I \subset \{1,\ldots,n\}} (-1)^{|I|+1} |A_I| .$$

Special Case

When $|I| = |J| \Rightarrow |A_I| = |A_J|$

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{|I|=1} (-1)^{|I|+1} \binom{n}{|I|} |A_I| .$$

Exercise

Exercise

Find the number of non-negative integers solutions of

$$x_1 + x_2 + x_3 + x_4 = 30,$$

such that $3 \leqslant x_i \leqslant 10$ for every $1 \leqslant i \leqslant 4$.

Solution

First, let $y_i = x_i - 3$. We will count integer solutions of the equation

$$y_1 + y_2 + y_3 + y_4 = 18,$$

with $0 \leqslant y_i \leqslant 7$, as there is a straightforward bijection between such solutions and the solutions of the original equation. There are

$$\left(\!\!\binom{4}{18}\!\!\right) = \binom{18+4-1}{18} = 1330$$

non-negative solutions to this equation, when we ignore the upper bounds $y_i \leqslant 7$. Let A_i be the set of solutions with $y_i \geqslant 8$. Then we are interested in $1330 - |A_1 \cap A_2 \cap A_3 \cap A_4|$.

Exercise

To compute $|A_1|$, for example, we used the fact that solutions in A_1 correspond to non-negative integer solutions of $z_1 + y_2 + y_3 + y_4 = 18 - 8$ after substitution $z_1 = y_1 - 8$. Applying inclusion-exclusion, we have

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = \sum_{i=1}^{4} |A_i| - \sum_{1 \leqslant i < j \leqslant 4} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant 4} |A_i \cap A_j \cap A_k|$$

$$= 4 \cdot \binom{(18-8)+4-1}{18-8} - 6 \cdot \binom{(18-2\cdot 8)+4-1}{18-2\cdot 8} + 0 = 1084.$$

The final answer is $1330 - 1084 = 246$.

Pigeonhole Principle

Theorem (Pigeonhole Principle)

No set of the form $[n]$ is equinumerous to a proper subset of itself, where $n \in \mathbb{N}$.

Theorem (Erdős–Szekeres, 1935)

Let $A = (a_1, ..., a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of $s + 1$ terms or a decreasing subsequence of $r + 1$ terms (or both).

Pigeonhole Principle

Homework ex3.6

Given sets A, B s.t. $A \subset B \wedge |A| = |B| < \infty$, use pigeonhole principle to show that $A \supset B$.

Proof by contradiction: Suppose $B \not\subset A$, i.e. $\exists x \in B, x \notin A$. Let

$$C \coloneqq \{x \mid x \in B \wedge x \notin A\} = B - A \neq \emptyset.$$

Now $(\mathrm{B} - C \subset A) \wedge (A \subset B - C)$, because only $x \notin A$ are kicked out. So $A = B - C \Rightarrow |A| = |B| = |B - C|$, but $B - C \subsetneq B$, and both of them are finite sets. By pigeonhole principle, no finite set is equinumerous to its subset, contradiction.

Equinumerosity

Definition

A set A is equinumerous to a set B (written $A \approx B$) if there is a bijection from A to B.

Theorem

For any sets A, B, and C:

- $A \approx A$.
- $A \approx B \Rightarrow B \approx A$.
- $(A \approx B \wedge B \approx C) \Rightarrow A \approx C$.

Warning

NOT an equivalence relation since the it concerns ***all*** sets.

Prove that

1. $\mathbb{Z} \approx \mathbb{N}$
2. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$
3. $(0,1) \approx \mathbb{R}$
4. $[0,1] \approx (0,1)$

Cardinality

Cardinality

For every set A, there is a unique cardinal (or cardinal number) κ with $A \approx \kappa$. We call that κ the ***cardinality*** of A, denoted by $\operatorname{card} A = \kappa$.

Example

- $\operatorname{card}[n] = n$ for all $n \in \mathbb{N}$.
- $\operatorname{card} \mathbb{N} = \aleph_0$ (by Cantor).
- $\operatorname{card} \mathbb{R} = 2^{\aleph_0}$.

Continuum Hypothesis

There is no set S for which $\aleph_0 < |S| < 2^{\aleph_0}$. That is, $2^{\aleph_0} = \aleph_1$.

Caution

$\{X \mid \operatorname{card} X = \kappa\}$ is NOT a set, excpet for $\kappa = 0$.

Cardinality

Definition

A set A is ***dominated*** by a set B (written $A \preceq B$) if there is an injection from A to B.

Definition

We write $\text{card}\, A \leq \text{card}\, B$ if $A \preceq B$.

Definition

A set A is ***countable*** if $A \preceq \mathbb{N}$, i.e., $\text{card}\, A \leq \aleph_0$. Otherwise, it is called ***uncountable***.

Theorem (Cantor-Schröder-Bernstein)

$(\text{card}\, A \leq \text{card}\, B) \wedge (\text{card}\, B \leq \text{card}\, A) \Rightarrow \text{card}\, A = \text{card}\, B$, *i.e.*,
$(A \preceq B) \wedge (B \preceq A) \Rightarrow A \approx B$.

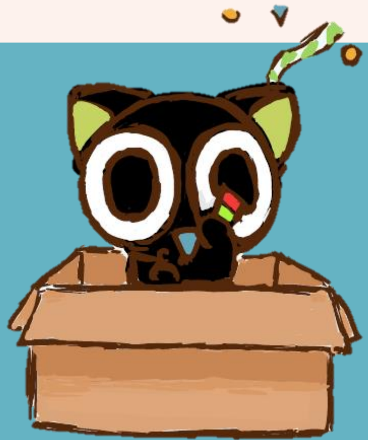
Exercise

Given countably infinite sets A and B, calculate card $A \times B$.

Since both A and B are countably infinite, then $A \approx \mathbb{N}$ and $B \approx \mathbb{N}$. Also note that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$, so $A \times B \approx \mathbb{N}$. Hence $\text{card } A \times B = \text{card } \mathbb{N} = \aleph_0$.

End

~~QAQ~~Q&A



Reference

- Prof. Cai, Runze. MATH2030J SU 2023 Lecture Slides
- E. Knuth, Donald. Translated by Su Daolin. *The art of Computer Programming*, 3rd edition. Beijing: National Defense Industry Press, 2007.6 print.
- Zhao, Jiayuan. VE203 FA 2021 Recitation Class Exercises.
- Umich MATH582 Notes & homework