Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Functions
- Function Properties
- Counting Sets
- Morphisms & Isomorphisms
- Fixed Points
- $\mathbb{N}_{def}$

Functions

Definitions

1. *function* (P89)
   - relation
   - uniqueness
2. $f''C = \{y|\exists x(x \in C \wedge (x,y) \in f)\} \subseteq ranf \subseteq B$ (P90)
3. $f \restriction C = \{(x,y)|\exists x(x \in C \wedge (x,y) \in f)\} \subseteq f$ (P90)
4. *injective functions* (P90)
5. *composing functions* (P91)
6. *inverses* (P93)
7. *identity function* (P94)
8. *surjective functions* (P95)
9. *bijection*: both injective and surjective (P95)

Inverse Functions & Identity Functions (P94)

Lemma

Let $f : A \to B$ be a function. The relation f^{-1} is a function with $domf^{-1} = ranf$ and $ranf^{-1} = A$ if and only if f is injective. Moreover, f^{-1} is injective and $f \circ f^{-1} = f^{-1} \circ f = id_A$

Proof.

Suppose $f : A \to B,\ w, x \in A;\ y, z \in B$

1. Given that f^{-1} is a function, then (according to the definition of function) for all $y \in B$ and for all $w, x \in A$ if $(y, x) \in f^{-1}$ and $(y, w) \in f^{-1}$, then $w = x$. This is also the definition of injection for f.
2. Given that f is injective, conversely we can have f^{-1} is a function as well as f^{-1} is injective.
3. For all $a \in A,\ b \in B$, if $(a, b) \in f$, then $(b, a) \in f^{-1}$, $f^{-1}(f(a)) = f^{-1}(b) = a,\ f(f^{-1}(b)) = f^{-1}(a) = b$

Cardinality (P96)

Lemma

If $f : A \to B$ and $g : B \to C$ are bijections, then $g \circ f$ is a bijection.

Proof.

For all $z \in C$, there exists a unique y that $(y, z) \in g$. Similarly, for all $y \in B$, there exists a unique X that $(x, y) \in f$. This means for all $z \in C$, there exists a unique x that $(x, z) \in g \circ f$, thus $g \circ f$ is a bijection. □

Definitions

1. *equal cardinality*: bijection
2. *small or equal cardinality*: injection

If $|A| \leqslant |B|$, then $|A| = |C|$ for some $C \subseteq B$.

Examples for Cardinality (P97-P98)

e.g.

1. $|\mathbb{N}| = |2\mathbb{N}|$ $(f : \mathbb{N} \to \mathbb{N}, f(n) = 2n)$
2. $|\mathbb{N}| = |\mathbb{N} \setminus \{1\}|$ since

$$f : \mathbb{N} \to \mathbb{N}, f(n) = \begin{cases} 0 & n = 0 \\ n+1 & n > 0 \end{cases}$$

3. $|\mathbb{Z}| = |\mathbb{N} \setminus \{1\}|$ since

$$f : \mathbb{N} \to \mathbb{N}, f((-1)^k n) = \begin{cases} 0 & n = 0 \\ 2n+k & n > 0 \end{cases}$$

Theorem

$|\mathbb{Z}| = |\mathbb{N}|$ *(according to e.g.2 and e.g.3)*

Countable Sets & Infinite Sets (P99-P100)

Definitions

For a set A

1. *infinite*: $f : A \to A$ is injective but not surjective.
2. *countable*: $|A| \leqslant |N|$.
3. *countably infinite*: both countable and infinite.

Lemma

If $f : A \to B$ and $g : B \to C$ are injective functions, then $g \circ f$ is an injective function.

Proof.

$f' : A \to ranf, f' = f$ is a bijection. $g' : ranf \to ran(g \circ f), g' = g$ is a bijection. Thus $g' \circ f' : A \to ran(g \circ f)$ is a bijection. Thus $g \circ f : A \to C$ is an injection. $\square$

Countable Sets & Infinite Sets (P101)

Lemma

If B is a countable set and $A \subseteq B$ then A is countable.

Proof.

$|A| \leqslant |B| \leqslant |\mathbb{N}|$ (we can construct an injective function $f : A \to B, f(x) = x$ for $x \in A$) $\square$

Cantor's Pairing Function (P102)

Theorem

$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

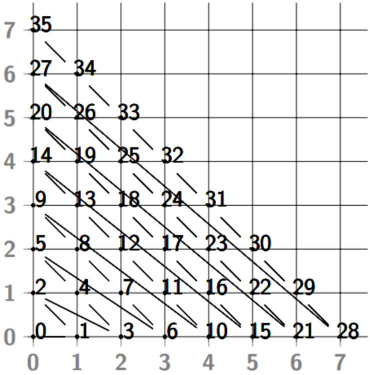
Proof.

Cantor Pairing Function

$\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\pi(x, y) = \frac{1}{2}(x+y)(x+y+1)+y$$

$\square$



Theorem

Cantor's Pairing Function $\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a bijection (according to the figure on the right).

Cantor's Theorem (P104)

Definition

$|A| < |B|$: exists injective functions, exists no bijective functions

Theorem

If A is a set, then there is no injection $f : \mathcal{P}(A) \to A$.

Proof.

This is a proof by contradiction. Let A be a set. Suppose that $f : \mathcal{P}(A) \to A$ is an injection. Since f is injective, $f^{-1} : ranf \to \mathcal{P}(A)$ is a bijection. Let $Z = \{x \in ranf | x \notin f^{-1}(x)\}$. Note that $Z \subseteq A$, and let z=$f(Z)$. Now if $z \in f^{-1}(z) = Z$, then $z \notin f^{-1}(z)$, which is a contradiction. And if $z \notin f^{-1}(z)$, then $z \in Z = f^{-1}(z)$, which is a contradiction (recall Russell's Paradox). $\square$

Cantor's Theorem (P104)

Corollary (Cantor's Theorem)

If A is a set, then $|A| < |\mathcal{P}(A)|$.

Proof.

The function $f = \{(x, \{x\}) \in A \times \mathcal{P}(A) | x \in A\}$ is an injection. □

Uncountable Sets (P105)

Definition
For a set A:
uncountable: not countable ($|A| > |\mathbb{N}|$, recall the definition of countable)

Cantor's Paradox in Naive Set Theory:
If V is the set of all sets, then $\mathcal{P}(V) \subseteq V$, which leads to a contradiction.

Morphisms & Isomorphisms (P106-P107)

- isomorphism: $(x, y) \in R$ iff $(f(x), f(y)) \in S$ (f is a bijection)
- homomorphism: *if* $(x, y) \in R$, then $(f(x), f(y)) \in S$

Isomorphisms are definitely homomorphisms.

Order-Preserving Functions (P108)

Definition

Compare with monotone function in Calculus.

e.g.

- Let $a \in \mathbb{N}$ with $a \neq 0$. The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = ax$ is order-preserving from $(\mathbb{N}, |)$ to $(\mathbb{N}, |)$.
- The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n - 1$ is order-preserving from $(\mathbb{Z}, \leqslant)$ to $(\mathbb{Z}, \leqslant)$, but $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = -n$ is not.

Fixed Points (P109)

Definition

$f(x) = x$

e.g.

The function $f : \mathcal{P}(\mathbb{N} \to \mathcal{P}(\mathbb{N})$ defined by $f(X) = X \setminus \{0\}$ has the property that if $A \subseteq \mathbb{N}$ is such that $0 \notin A$, then A is a fixed point of f.

Tarski-Knaster Theorem (P110-P111)

Theorem

Let $(L, \preceq)$ be a complete lattice. If $f : (L, \preceq) \to (L, \preceq)$ is an order-preserving function, then f has a (least) fixed point.

Proof.

Let $f : (L, \preceq) \to (L, \preceq)$ be order preserving. Consider $X = \{x \in L | f(x) \preceq x\}$ and $a \in \bigwedge X$

Claim I: If $x \in X$, then $f(x) \in X$. To see this, let $x \in X$. Therefore $f(x) \preceq x$. Since f is order preserving, $f(f(x)) \preceq f(x)$. This shows that $f(x) \in X$.

Claim II: $f(a)$ is a lower bound on X. Since f is order preserving. $f(a) \preceq f(x)$. Since $f(x) \preceq x$, it follows that $f(a) \preceq x$.

It follows from Claim II that $f(a) \preceq a$, because a is the g.l.b. of X. Therefore $a \in X$. So, by Claim I, $f(a) \in X$. Therefore $a \preceq f(a)$ and $a = f(a)$. So a is a fixed point of f. □

Schröder-Bernstein Theorem (P112)

Theorem

Let A and B be sets. If there exists $f : A \to B$ that is injective and $g : B \to A$ that is injective, then there exists a bijection $h : A \to B$.

Proof.

Let $f : A \to B$ and $g : B \to A$ be injective functions. We know that $(\mathcal{P}(A), \subseteq)$ is a complete lattice. Define $F : \mathcal{P}(A) \to \mathcal{P}(A)$ by $F(X) = A \setminus g''(B \setminus f''X)$. $F(X)$ is the complement of points in A mapped to be g from the points that are not in the range of f restricted to X.

Claim: F is order-preserving. To see this, let $Y \subseteq Z \subseteq A$. So $f''Y \subseteq f''Z$ and $B \setminus f''Z \subseteq B \setminus f''Y$. Therefore $g''(B \setminus f''Z) \subseteq g''(B \setminus f''Y)$. And so $F(Y) = A \setminus g''(B \setminus f''Y) \subseteq A \setminus g''(B \setminus f''Z)$.

Schröder-Bernstein Theorem (P113)

Proof(continue).

By TK Theorem, F has a fixed point. Let $X \subseteq A$ be such that $F(X) = X$. Let $C = rang$. So $g^{-1} : C \to B$ is an injection and $A \setminus X \subseteq C$. Define

$$h = (f \restriction X) \cup (g^{-1} \restriction (A \setminus X))$$

Now, $domh = A$. We have $ran(g^{-1} \restriction (A \setminus X)) = B \setminus f''X$, so $ranh = B$. Therefore $h : A \to B$ is a bijection. □

Corollary

If $|A| \leqslant |B|$ and $|B| \leqslant |A|$, then $|A| = |B|$.

A Flawed Definition of $\mathbb{N}$ (P114)

Let V be the set of all sets (does such V really exist?) and let L be the set of all sets that have $\emptyset$ as a member:

$$L = \{x \in V | \emptyset \in x\}$$

$(L, \subset)$ is a complete lattice. (why?) Define the **successor operation** $S : V \to V$ by

$$S(x) = x \cup \{x\} \text{ for all } x \in V$$

Define $F : L \to L$ such that for all $A \in L$,

$$F(A) = A \cup S''A$$

A Flawed Definition of $\mathbb{N}$ (P115)

For all $A, B \in L$, if $A \subseteq B$, then $S''A \subseteq S''B$. So F is an order-preserving function on the complete lattice $(L, \subseteq)$.
Therefore, by TK Theorem, F has a least fixed point.
Let $\mathbb{N}_{def}$ be the least fixed point of F. $\mathbb{N}_{def}$ is the $\subset$-least set X such that

$$\emptyset \in X, S(\emptyset) \in X, S(S(\emptyset)) \in X, \cdots$$

By defining

$$\begin{aligned} 0 &:= \emptyset \\ 1 &:= S(\emptyset) = \{\emptyset\} \\ 2 &:= S(S(\emptyset)) = \{\emptyset, \{\emptyset\}\} \\ &\vdots \end{aligned}$$

The set $\mathbb{N}_{def}$ interprets the natural numbers.

A Flawed Definition of $\mathbb{N}$ (P116)

$$\mathbb{N}_{def} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \cdots\}$$

Set n has n elements (cardinality), thus we can define addition($+$) and multiplication($\cdot$) in $\mathbb{N}$:
Let $m = \{0, 1\}, k = \{2, 3\}$

$$\begin{aligned}
\text{Addition}(+) : &|m| = 2, |k| = 2, m \cap k = \emptyset \\
&|m \cup k| = |\{0, 1, 2, 3\}| = |m| + |k| = 4 = |n| \\
&n = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
\text{Multiplication}(\cdot) : &|k \times m| = |\{(0, 2), (2, 3), (1, 2), (1, 3)\}| = 4 = |n|
\end{aligned}$$

$$\forall n \in \mathbb{N}_{def}, S(n) = n + 1$$

Properties of $\mathbb{N}_{def}$ (P118)

- $+$ & $\cdot$: commutativity, associativity, distributivity, identity
- $\leqslant$: a well ordering of $\mathbb{N}_{def}$
- Every $n \in \mathbb{N}_{def}$ except 0 is the successor of some $k \in \mathbb{N}_{def}$, i.e. $n = k + 1$.
- $\mathbb{N}_{def}$ satisfies the principle of induction. If a peoperty $P(x)$ is such that $P(0)$ holds, and $\forall n \in \mathbb{N}_{def}$, if $P(n)$ holds, then $P(n+1)$ holds, then $\forall n \in \mathbb{N}_{def}$, $P(n)$ holds. (proof by contradiction (P119))