Discrete Mathematics Review
PART II

Liu Ziwei

Fall Term 2019

refer to Qiu Tianyu

Contents

Functions

Function Properties

Definitions

1.function f: A->B (p89)

·relation

·uniqueness

2. $f''C = \{y | \exists x(x \in C \wedge (x,y) \in f)\} \subseteq ranf \subseteq B$ (P90)

3. $f \upharpoonright C = \{(x,y) | \exists x(x \in C \wedge (x,y) \in f)\} \subseteq f$ (P90)

4.injective functions (p90)

5.composing functions $g \circ f = \{(x,y) \mid \exists z((x,z) \in f \wedge (z,y) \in g)\}$ (P91)

6. inverses $f^{-1} = \{(x,y) \in B \times A \mid (y,x) \in f\}$ (P93)

7. identity function $\mathrm{id}_A = \{(x,y) \in A \times A \mid x = y\}$ (P94)

8. surjective functions (P95)

9. bijection: both injective and surjective (P95)

Function Properties

Inverse Functions & Identity Functions (P94)

Lemma

Let $f : A \to B$ be a function. The relation f^{-1} is a function with $\text{dom}f^{-1} = \text{ran}f$ and $\text{ran}f^{-1} = A$ if and only if f is injective. Moreover, f^{-1} is injective and $f^{-1} \circ f = \mathrm{id}_A \quad f \circ f^{-1} = \mathrm{id}_{\mathrm{ran}\ f}$.

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 $(b, a) \in f^{-1}$, $f^{-1}(f(a)) = f^{-1}(b) = a$, $f(f^{-1}(b)) = f^{-1}(a) = b$

Counting Sets

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. $\square$

Definitions

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

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

Counting Sets

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)*

Counting Sets

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.

Counting Sets

Countable Sets & Infinite Sets (P99-P100)

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. $\square$

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 $x \in A$)

Counting Sets

Cantor's Pairing Function (P102)

Theorem

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

Proof.

Cantor Pairing Function

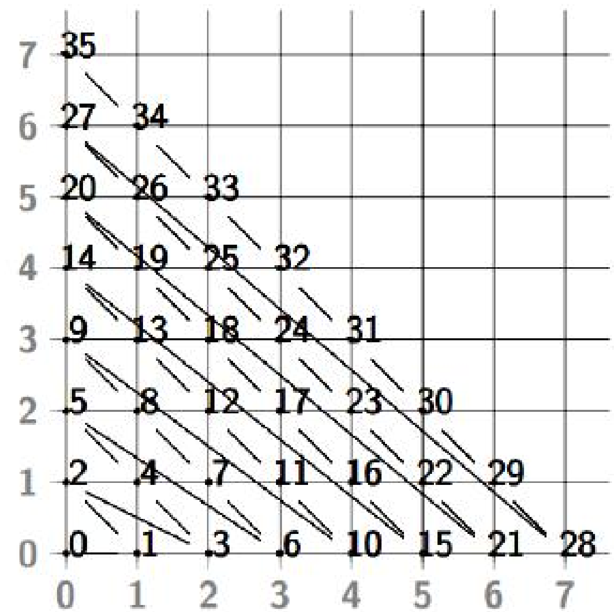
$\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

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

$\square$

Theorem

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



Counting Sets

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). $\square$

Counting Sets

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.

Counting Sets

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

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.

Fixed Points

Order-Preserving Functions (P108)

order-perserving: $f : P_1 \longrightarrow P_2$, *for all* $x, y \in P_1$,

$$\textit{if } x \preceq_1 y, \textit{ then } f(x) \preceq_2 f(y)$$

*Can compare with monotone function in Calculus.

e.g.

(i) *Let* $a \in \mathbb{N}$ *with* $a \neq 0$. *The function* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *defined by* $f(x) = ax$ *is order-preserving from* $(\mathbb{N}, |)$ *to* $(\mathbb{N}, |)$

(ii) *If* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *is an increasing function, then* f *is order-preserving from* $(\mathbb{R}, \leq)$ *to* $(\mathbb{R}, \leq)$

(iii) *The function* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *given by* $f(n) = n - 1$ *is order-preserving from* $(\mathbb{Z}, \leq)$ *to* $(\mathbb{Z}, \leq)$, *but* $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ *defined by* $g(n) = -n$ *is NOT*

Fixed Points

Fixed Points (P109)

Definition: $f(x) = x$

e.g.

(iii) *The function* $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ *defined by* $f(x) = x + 1$ *has no fixed points.*

(iv) *The function* $f : \mathscr{P}(\mathbb{N}) \longrightarrow \mathscr{P}(\mathbb{N})$ *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.

Fixed Points

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. $\square$

Fixed Points

Schroder-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 $f : A \longrightarrow B$ and $g : B \longrightarrow A$ be injective functions. We know that $(\mathscr{P}(A), \subseteq)$ is a complete lattice. Define $F : \mathscr{P}(A) \longrightarrow \mathscr{P}(A)$ by

$$F(X) = A \backslash g``(B \backslash f``X)$$

$F(X)$ is the complement of points in A mapped to by g from the points that are not in the range of f restricted to X. Think about this and convince yourself that a fixed point of this function is what we need!

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

$$F(Y) = A \backslash g``(B \backslash f``Y) \subseteq A \backslash g``(B \backslash f``Z)$$

Fixed Points

Schroder-Bernstein Theorem (P112)

Proof.

(Continued.) By Tarski-Knaster, F has a fixed point. Let $X \subseteq A$ be such that $F(X) = X$.

Let $C = \text{ran } g$. So $g^{-1} : C \longrightarrow B$ is an injection and $A \backslash X \subseteq C$. Define

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

Now, dom $h = A$. We have ran $(g^{-1} \restriction (A \backslash X)) = B \backslash f``X$, so ran $h = B$. Therefore $h : A \longrightarrow B$ is a bijection.

Corollary

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