Ve203 Discrete math lecture summary

October 15, 2018

Contents

1 Logic

1.1 Notable Preliminaries

1. We say that m divides n, writing $m|n$, if there exists some $k \in \mathbb{N}$ such that $n = m \cdot k$.

2. Whole number: any of the natural numbers (positive or negative) or zero.

3. Least upper bound principle: every nonempty bounded subset of R has a *least upper bound*.

1.2 Propositional Logic

1. letters (A, B, C, p, q ...) are used in propositional logic to denote **propositional variables**.

   Definition 1. A **proposition** is a declarative sentence. I.e. a statement that is *either* true (T) or false (F), but not both.

   > **eg.** Chocolate is very delicious.
   > This statement is not a proposition. You cannot determine whether it is true or false.

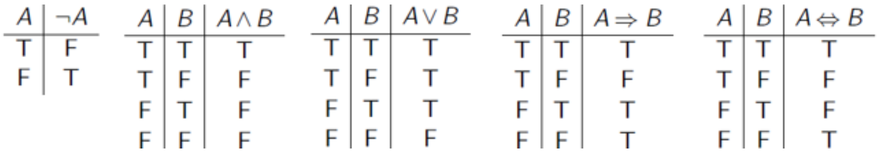
2. Connectives:
   unary $\neg$ not ($\neg A$ is negation of A.)
   binary $\vee$ disjunction
   binary $\wedge$ conjunction
   binary $\Rightarrow$ implication ($A \Rightarrow B$, A: antecedent and B: consequence.)

   > An implication $A \Rightarrow B$ is false only when the antecedent is true and the consequence is false.

   binary $\Leftrightarrow$ biconditional ("A is equivalent to B" or "A if and only if B".)

   Definition 2. Two compound propositions A and B are called **logically equivalent** if $A \Leftrightarrow B$ is a tautology. We then write $A \equiv B$.

   > **de Morgan rules**
   > $\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B), \qquad \neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B)$



A	$\neg A$
T	F
F	T

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	$A \Rightarrow B$
T	T	T
T	F	F
F	T	T
F	F	T

A	B	$A \Leftrightarrow B$
T	T	T
T	F	F
F	T	F
F	F	T

Figure 1: Truth table of the five connectives.

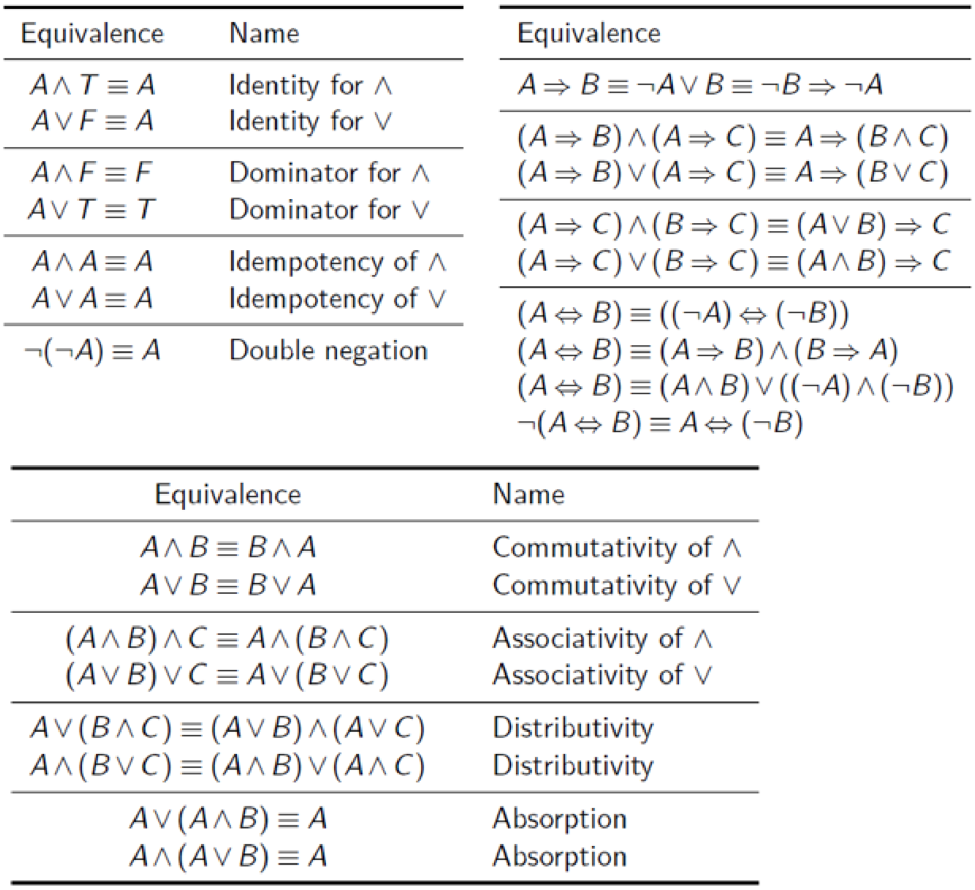
3. **Tautology**: a compound expression that is always true.
   Contradiction: a compound expression that is always false.
   Using truth table to prove an expression is a tautology or contradiction.

4. Contraposition: $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$.

5. A most important equivalence:

$$\neg(A \Rightarrow B) \equiv A \wedge \neg B.$$

6. Argument: a finite sequence of propositions. All propositions except for the final statement are called **premises** (P) while the final statement is called the **conclusion** (C).



Equivalence	Name
$A \wedge T \equiv A$	Identity for $\wedge$
$A \vee F \equiv A$	Identity for $\vee$
$A \wedge F \equiv F$	Dominator for $\wedge$
$A \vee T \equiv T$	Dominator for $\vee$
$A \wedge A \equiv A$	Idempotency of $\wedge$
$A \vee A \equiv A$	Idempotency of $\vee$
$\neg(\neg A) \equiv A$	Double negation

Equivalence
$A \Rightarrow B \equiv \neg A \vee B \equiv \neg B \Rightarrow \neg A$
$(A \Rightarrow B) \wedge (A \Rightarrow C) \equiv A \Rightarrow (B \wedge C)$
$(A \Rightarrow B) \vee (A \Rightarrow C) \equiv A \Rightarrow (B \vee C)$
$(A \Rightarrow C) \wedge (B \Rightarrow C) \equiv (A \vee B) \Rightarrow C$
$(A \Rightarrow C) \vee (B \Rightarrow C) \equiv (A \wedge B) \Rightarrow C$
$(A \Leftrightarrow B) \equiv ((\neg A) \Leftrightarrow (\neg B))$
$(A \Leftrightarrow B) \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$
$(A \Leftrightarrow B) \equiv (A \wedge B) \vee ((\neg A) \wedge (\neg B))$
$\neg(A \Leftrightarrow B) \equiv A \Leftrightarrow (\neg B)$

Equivalence	Name
$A \wedge B \equiv B \wedge A$	Commutativity of $\wedge$
$A \vee B \equiv B \vee A$	Commutativity of $\vee$
$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$	Associativity of $\wedge$
$(A \vee B) \vee C \equiv A \vee (B \vee C)$	Associativity of $\vee$
$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$	Distributivity
$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$	Distributivity
$A \vee (A \wedge B) \equiv A$	Absorption
$A \wedge (A \vee B) \equiv A$	Absorption

Figure 2: Some logical equivalences.

An argument is **valid** if the truth of all premises implies the truth of the conclusion, i.e.

$$(P_1 \wedge P_2 \wedge ... \wedge P_n) \Rightarrow C$$

is a tautology.

Format of writing an argument:

$$\begin{array}{rl} & P_1 \\ & P_2 \\ & \vdots \\ & P_n \\ \hline \therefore & C \end{array}$$

> It is possible for a **valid** argument to lead to a **wrong** conclusion if one or more of its premises are false.
> If, in addition to being valid, an argument has only true premises, we say that the argument is **sound**. In that case, its conclusion is true.

1.3 Predicate Logic

1. Predicate: a declarative sentence involving variables. Substituted variables with appropriate individuals results in a proposition.
   Arity: number of distinct variables appearing in the predicate.

2. **predicate variable** A, B, C...

   variables x, y, z...

   constants a, b, c...

   domain of discourse universe of values that variables take from.

   logic quantifier $\exists$, $\forall$

3. Compound predicate: An Expression involving unspecified variables, also called **formula**, e.g. $A(x, y)$.
   Sentence: all variables in expression have been replaced by constants or bound by quantifiers. These expressions are propositions.

4. Vacuously true: If the domain of the universal quantifier $\forall$ is the empty set $M = \emptyset$, then the statement $(\forall x \in M)A(x)$ is defined to be true regardless of the predicate A(x).

   > A universal statement is true unless there is a counterexample to prove it false.

5. Order of quantifier: different orders of quantifiers can have different meaning if variables bounded by them are different.

6. Tautology in predicate logic: for a predicate logic sentence A, if for every nonempty domain of discourse M equipped with interpretations of the predicate symbols, A is true in M, then A is a tautology.

Application in proof problems: proof by contradiction (Assume a domain where the statement is not valid).

2 Set Theory

Naive Set Theory is defined informally, in natural language. Describable: a well-defined collection of distinct objects.
Axiomatic Set Theory is defined with formal logic.

2.1 Notations

1. For a predicate $P(x)$, the set
$$X = \{x|P(x)\}$$
is the collection of all objects x that satisfies $P(x)$.

2. Equality. Two sets X and Y are equal $(X = Y)$ if for all x, $x \in X$ if and only if $x \in Y$.

3. Empty set.
$$\emptyset \overset{def}{=} \{x|x \neq x\}.$$

4. Premise.
$$\{x \in A|P(x)\} = \{x|x \in A \wedge P(x)\}.$$

2.2 Subset, powerset, cardinality

1. Subset.
$$X \subseteq Y \Leftrightarrow \forall x(x \in X \Rightarrow x \in Y).$$
$X = Y$ iff $X \subseteq Y$ and $Y \subseteq X$.

2. Proper subset. $X \subseteq Y$ but $X \neq Y$. Denote $X \subset Y$.

Either use $\subseteq$, $\subset$ or $\subset$, $\subsetneq$ for subset and proper subset.
To prove a subset is a proper subset, just find at least one element that belongs to the set but not belongs to the subset. Conversely, it can be used with proof by contradiction to prove equivalence of two sets.

Let $A = \{\emptyset, \{\{\emptyset\}\}\}$, $B = \{\emptyset\}$ and $C = \{\{\emptyset\}\}$. $B \subseteq A$ but $B \notin A$, and $C \in A$ but $C \nsubseteq A$.

3. Cardinality. The number of elements in a finite set X. Denote by $\#X$, $|X|$ or $\text{card}(X)$.

4. Powerset. Denoted by$\mathscr{P}(X)$, represents the set of all subsets of X:
$$\mathscr{P}(X) = \{A|A \subseteq X\}.$$
To be noted, $A \in \mathscr{P}(X) \equiv A \subseteq X$.

2.3 Operations on sets

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $(A \cup B) \backslash C = (A \backslash C) \cup (B \backslash C)$
- $(A \cap B) \backslash C = (A \backslash C) \cup (B \backslash C)$
- $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$
- $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$
- $A \backslash B = B^c \cap A$
- $(A \backslash B)^c = A^c \cup B$

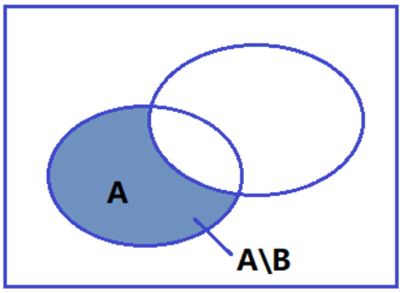


Figure 3: $A \backslash B$

Notation for the union and intersection of $n \in \mathbb{N}$ sets:

$$\bigcup_{k=0}^{n} A_k := A_0 \cup ... \cup A_n,$$

$$\bigcap_{k=0}^{n} A_k := A_0 \cap ... \cap A_n.$$

In particular,

$$\bigcap_{k=0}^{n} A_k \subseteq \bigcup_{k=0}^{n} A_k.$$

Example:

$$X = \{A \in \mathscr{P}(\mathbb{N}) | (\exists k \in \mathbb{N})(\forall n \in \mathbb{N})(n \in A \vee n = k)\}.$$

There are some elements of X that equals $\mathbb{N} \backslash k$ for some $k \in \mathbb{N}$.

X is the collection of subsets of $\mathbb{N}$ but elements in $\bigcup X$ and $\bigcap X$ are numbers.

2.4 Relations

2.4.1 Orderer pair

1. Ordered pair: $(a,b) := \{\{a\},\{a,b\}\}$.

$$(a,b) = (c,d) \Leftrightarrow (a=c) \wedge (b=d).$$

2. Cartesian product of A and B

$$A \times B := \{(a,b) | a \in A \wedge b \in B\}.$$

3. n-fold Cartesian product:

$$A_1 \times ... \times A_n = A_1 \times (A_2 \times ...(A_{n-1} \times A_n)...).$$

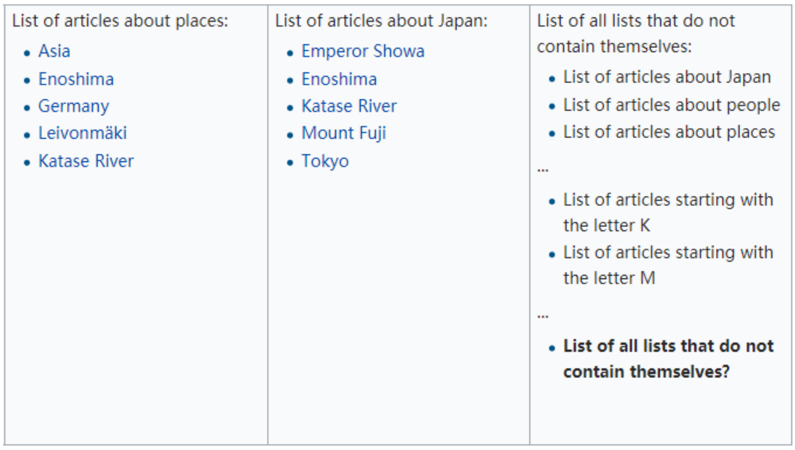
2.4.2 Russell's Paradox

The set of all sets that are not members of themselves is not a set. I.e.

$$R := \{x | x \notin x\} \text{ is not a set.}$$

A concrete example:

eg. Consider lists of encyclopedia entries within the same encyclopedia:



List of articles about places:

- Asia
- Enoshima
- Germany
- Leivonmäki
- Katase River

List of articles about Japan:

- Emperor Showa
- Enoshima
- Katase River
- Mount Fuji
- Tokyo

List of all lists that do not contain themselves:

- List of articles about Japan
- List of articles about people
- List of articles about places

...

- List of articles starting with the letter K
- List of articles starting with the letter M

...

- **List of all lists that do not contain themselves?**

Figure 4: Lists of encyclopedia entries

2.4.3 Notations of Relations

Definition 3. A set R is called a relation if R only contains ordered pairs.

For a relation R, its **domain** and **range** are the sets

$$\text{dom } R = \{x | \exists y((x,y) \in R)\}$$

$$\text{ran } R = \{sy | \exists x((x,y) \in R)\}$$

and the **field** of R is the set Ran $R = \text{ran } R \cup \text{dom } R$.

- For a set M, if $R \subseteq M \times M$, R is a relation on M.
- $(a,b) \in R$: a and b are related by R. Also denoted by aRb.

2.4.4 Properties of Relations

1. Attributes of relations:

   reflexive for all $a \in M$, $(a, a) \in R$.

   symmetric for all $a, b \in M$, if $(a, b) \in R$, then $(b, a) \in R$.

   antisymmetric for all $a, b \in M$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$.

   asymmetric for all $a, b \in M$, if $(a, b) \in R$, then $(b, a) \notin R$.

   transitive for all $a, b, c \in M$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

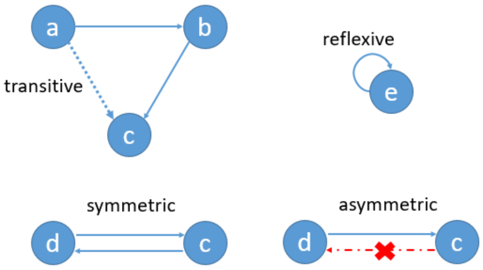


Figure 5: Illustration of relations

2. Equivalence Relations.

   Definition 4. Let R be a relation on a set M. If R is reflexive, symmetric and transitive, then we say that R is an **equivalence relation** on M.

   If R is an equivalence relation on M and $a \in M$, the **equivalence class** of a is

$$[a]_R = \{b \in M | (a, b) \in R\}.$$

   If R is an equivalence relation on a set M, then for all $a, b \in M$, either $[a]_R \cap [b]_R = \emptyset$ or $[a]_R = [b]_R$. In other words, the equivalence classes **partition** the set M.

2.5 Orders

1. Partial order

   Let R be a relation on a set M. If R is reflexive, antisymmetric and transitive, then R is called a partial order. We often write a partial order together with its domain, (M,R), and say that (M,R) is a **partially ordered set** or **poset**.

2. Strict partial order

   Let R be a relation on a set M. If R is asymmetric and transitive, then R is called a strict partial order. We say that (M,R) is a strict partially ordered set or **strict poset**.

3. Linear order

   Let (M,R) be a *partially ordered set.* If for all $x, y \in M$, $(x, y) \in R$ or $(y, x) \in R$, then R is called a linear order or **total order**, and we say that (M,R) is a linearly ordered set or totally ordered set.

   > For a linear ordered set, any two points in set M should be related. However, a linear order R must first be a partial order. Therefore, it must be reflexive, antisymmetric and transitive.

4. Well order

   Let R be a linear order on a set M. We say that R is a well-order if for all $A \subseteq M$, if $A \neq \emptyset$, then there exists $x \in A$, such that for all $y \in A$, if $(y, x) \in R$ then $y = x$. We also say that (M, R) is a **well-ordered set**.

   > This says that every nonempty $A \subseteq M$ has a least element according to R. In an informal but more intuitive way, in every nonempty $A \subseteq M$, there should be an element that can only be the first element in every ordered pairs within the subset.
   > **Question**: can there be two such elements?

   If R is a **linear order** on M and M is **finite** then R is a well-order.

   But M *need not* be finite:

   - The linear order $\leq$ on $\mathbb{N}$ is a well-order.

   It also depends on the relation:

   - The linear order $\geq$ on $\mathbb{N}$ is not a well-order.

   ...and the set itself:

   - The linear order $\leq$ on $\mathbb{R}$ is not a well-order.

2.6 Lattices

1. Upper and lower bound.

   Let $(L, \preceq)$ be a poset and let $S \subseteq L$. We say that $x \in L$ is an upper bound on S if for all $y \in S$, $y \preceq x$. We say that $x \in L$ is a lower bound on S if for all $y \in S$, $x \preceq y$.

2. l.u.b. and g.l.b.

   Let $(L, \preceq)$ be a poset and let $S \subseteq L$. We say that $x \in L$ is a least upper bound (l.u.b.) on S if x is an upper bound on S and for all y, if y is an upper bound on S, then $x \preceq y$. We say that $x \in L$ is a greatest lower bound (g.l.b.) on S if x is a lower bound on S and for all y, if y is a lower bound on S then $y \preceq x$.

3. Lattices.

   Let $(L, \preceq)$ be a **poset**. We say that $(L, \preceq)$ is a lattice if for all $x, y \in L$, the set $\{x, y\}$ has both a l.u.b. and a g.l.b. If $(L, \preceq)$ is a lattice and $x, y \in L$, then we write $x \vee y$ for the l.u.b. of $\{x, y\}$ and $x \wedge y$ for the g.l.b. of $\{x, y\}$.

If $\preceq$ is a linear order on M, then $(M, \preceq)$ is a lattice.
For every two elements $x, y \in M$, since either $(x, y) \in R$ or $(y, x) \in R$, for the pair, one is the l.u.b and the other is the g.l.b.

4. Complete lattices.

   Let $(L, \preceq)$ be a lattice. We say that $(L, \preceq)$ is complete if for every $X \subseteq L$, X has both a least upper bound and a greatest lower bound. If $(L, \preceq)$ is a complete lattice and $X \subseteq L$, then we use $\bigvee X$ to denote the least upper bound of X and $\bigwedge X$ to denote the greatest lower bound of X.

   While for lattice, every set $\{x, y\}$ (a ordered pair) should have g.l.b. and l.u.b., for a complete lattice, every *subset* should have g.l.b. and l.u.b.
   If $(L, \preceq)$ is a nonempty finite lattice then $(L, \preceq)$ is complete.

5. For a complete lattice $(L, \preceq)$,

   there is a maximal element given by $\bigvee L$. Also denoted by $\mathbb{1}$.

   there is a minimal element given by $\bigwedge L$. Also denoted by $\mathbb{0}$.

6. Chain.

   Let $(P, \preceq)$ be a partial order. We say that $X \subseteq P$ is a chain if $(X, \preceq)$ is a **linear** order.

7. Chain complete.

   Let $(P, \preceq)$ be a partial order. We say that $(P, \preceq)$ is chain complete if for all $X \subseteq P$, if X is a chain then X has a least upper bound.

   This definition ensures the existence of a unique least element: the **empty set** is also a subset of P, and according to the definition of chain, $\emptyset \in P$ is a chain. Thus it should have a least upper bound, which is **unique**.
   About greatest elements: no need to be unique.

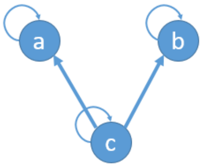


Figure 6: no unique greatest element

Every complete lattice is a chain complete poset: since it is a complete lattice, every subset has a l.u.b., thus so for every chain.

2.7 Functions

1. Definition.

Let $f \subseteq A \times B$ (so f is a relation). We say that f is a function, and write $f : A \to B$, if $dom\ f = A$ and for all $x \in A$ and for all $y, z \in B$, if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

2. Notations.

   For function $f : A \to B$ and $C \subseteq A$,
   $f"C$: $f\{y|\exists x(x \in C \wedge (x, y) \in f)\}$.
   $f \restriction C$: $f\{(x, y)|(x \in C \wedge (x, y) \in f)\}$.
   (This can be remembered as (X, f"X).)

3. Injective.

   Let $f \subseteq A \times B$ be a function. We say that f is injective or one-to-one if for all $x, y \in A$ and for all $z \in B$, if $(x, z) \in f$ and $(y, z) \in f$, then x = y.

4. Composition.

   Let f and g be functions with $ran\ f \subseteq dom\ g$. Then define $g \circ f$ to be the relation
   $$g \circ f = \{(x, y)|\exists z((x, z) \in f \wedge (z, y) \in g)\}.$$
   $g \circ f(a)$ is the same as $g(f(a))$.

5. Inverses and inverse functions.

   Let A be a set. The identity function on A is $id_A = \{(x, y) \in A \times A|x = y\}$.

   Let $f \subseteq A \times B$ be a function. The **inverse** of f , written f^{-1} is the *relation*
   $$f^{-1} = \{(x, y) \in B \times A|(y, x) \in f\}.$$
   The relation f^{-1} is a function iff f is injective. Furthermore, $f^{-1} \circ f = id_A$ and $f \circ f^{-1} = id_{ran\ f}$.

6. Surjective and bijection.

   Let $f \subseteq A \times B$ be a function. We say that f is surjective or onto if for all $x \in B$, there exists $y \in A$ such that $(y, x) \in f$.
   A function is **bijection** if it is both injective and surjective.
   If $f \subseteq A \times B$ and $g \subseteq B \times C$ are bijections, $g \circ f$ is a bijection.

2.8 Cardinality Revisited

1. Definition.
   Sets A, B are said to have the same cardinality and write $|A| = |B|$ if there exists a function $f \subseteq A \times B$ that is a bijection.

   If exists $f \subseteq A \times B$ that is an injection, $|A| \leq |B|$.

   If there exists a function $f \subseteq A \times B$ that is an injection, and there *does not exist a bijection* $g \subseteq A \times B$, then $|A| < |B|$.

2. Infinite sets.

   A set A is infinite if there *exists* $f : A \to A$ that is an injection but not a surjection. This is also called **Dedekind infinite**.

3. Countable sets.

Definition 5. A set A is countable if $|A| \leq |N|$. We say that A is countably infinite if A is 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.

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

4. Cantor's pairing function.
$\pi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, defined by

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

Cantor's pairing function is a bijection. It can be used to prove the theorem $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, which means that $|\mathbb{N} \times \mathbb{N}|$ is countable. It can be further extended to prove that $\mathbb{Q}$ is also countable: each pair (x, y) uniquely determines a rational number.

This definition can be inductively generalized to the Cantor tuple function:

$$\pi^{(n)} : \mathbb{N}^{(n)} \to \mathbb{N}$$

as

$$\pi^{(n)}(k_1, ...k_{n-1}, k_{n-1}) := \pi(\pi^{(n-1)}(k_1, ...k_{n-1}), k_n).$$

5. Cantor's theorem.
If A is a set, then there is no injection $f : \mathscr{P}(A) \to A$.

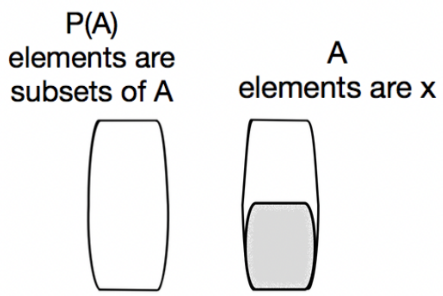


Figure 7: Cantor's theorem

Proof. Let $f : \mathscr{P}(A) \to A$ an injection. f^{-1} : ran $f \to \mathscr{P}(A)$ is a bijection. Let

$$Z = \{x \in \text{ran } f | x \notin f^{-1}(x)\}.$$

$f^{-1}(x)$ is a set!

Since $Z \in \mathscr{P}(A)$, let $f(Z) = z$. Therefore the inverse indicates $Z = f^{-1}(z)$. If $z \in Z$, then $z \notin f^{-1}(z) = Z$. If $z \notin Z$, then $z \in f^{-1}(z) = Z$. Contradict.

□

Corollary: if A is a set, $|A| < |\mathscr{P}(A)|$.

6. Uncountable sets.
A set is uncountable if it's not countable.

   Cantor's paradox: according to Cantor's theorem there is no largest set in terms of cardinality.

   (Inconsistency in Naive Set Theory and Cantor's paradox.)

2.9 Order Preserving Functions

1. Morphisms and Isomorphisms.
Maps that preserve structure between one entity R and another entity S, but are not necessarily bijections, are called morphisms or homomorphisms.

   If (A, R) and (B, S) are structures where A and B are sets (the domains), and S and R are relations, then a homomorphism from (A, R) to (B, S) would be a function $f : A \to B$ such that for all $x, y \in A$,

$$\text{if } (x, y) \in R, \text{ then } (f(x), f(y)) \in S.$$

   If R and S are structures, and f is a bijection between the domains of R and S that preserves all of the structure associated with these domains, then f is called an isomorphism and the structures R and S are said to be isomorphic.

2. Order preserving function.
Let $(P_1, \preceq_1)$ and $(P_2, \preceq_2)$ be partial orders. A function $f : P_1 \to P_2$ is order-preserving if for all $x, y \in P_1$,

$$\text{if } x \preceq_1 y \text{ then } f(x) \preceq_2 f(y).$$

3. Fixed points.
Let A be a set and let $f : A \to A$ be a function. We say that $x \in A$ is a fixed point of f if $f(x) = x$.

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

   Proof. Let $f : (L, \preceq) \to (L, \preceq)$ be order preserving.

   Let
$$X = \{x \in L | f(x) \preceq x\} \text{ and } a = \bigwedge X.$$

   If $x \in X$, then $f(x) \preceq x$. Since f is order preserving, $f(f(x)) \preceq f(x)$. Thus $f(x) \preceq x$. This says if $x \in X, f(x) \in X$.

   Since a is the g.l.b of X, for $x \in X$, $a \preceq x$. Thus $f(a) \preceq f(x) \preceq x$ and thus is also a lower bound on X. Since a is the g.l.b, $f(a) \preceq a$. Thus $a \in X$. This implies $f(a) \in X$. So $a \preceq f(a)$ and $a = f(a)$. So a is a fixed point of f.

   □

Corollary:

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.

5. **Schröder-Bernstein 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. Idea: to construct a bijection.

   - Construct injective functions $f : A \to B$ and $g : B \to A$. Define $F : \mathscr{P}(A) \to \mathscr{P}(A)$ to be

     $$F(X) = A \backslash g\text{''}(B \backslash f\text{''}X).$$

   - Prove that F is order-preserving. Therefore according to Tarski-Knaster, F has a fixed point.

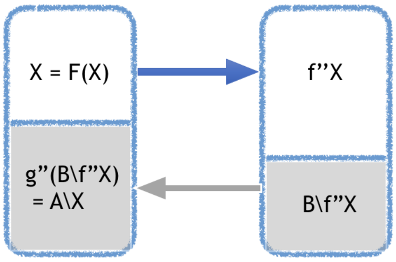
   

   Figure 8: fixed point of F

   - Construct a function $h = (f \restriction X) \cup (g^{-1} \restriction (A \backslash X))$. Prove that it is a bijection.

   □

   Corollary: The $\leq$ relation on cardinalities is antisymmetric. If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

2.10 Induction, Recursion, Counting

2.10.1 A flawed definition of $\mathbb{N}$

1. Pure set theory: the only objects are sets.

2. Preliminaries.

   - Let V be the set of all sets and L the set of all sets with $\emptyset$ as element, $L = \{x \in V | \emptyset \in x\}$. Thus $(L, \subseteq)$ is a complete lattice.
   - Successor operation $S : V \to V$,

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

- $F : L \to L$ for all $A \in L$,

  $$F(A) = A \cup S\text{"}A.$$

  Thus F is an order-preserving function on the complete lattice $(L, \subseteq)$. According to T-K theorem, F has a *least* fixed point.

3. Let $\mathbb{N}_{def}$ be the least fixed point of F. It is the $\subseteq$ −least set X such that

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

4. The natural numbers can be defined by

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

   For all $n \in \mathbb{N}_{def}$, the set n has n elements.

5. Define $+$ and $\cdot$ ($\mathbb{N}_{def} \to \mathbb{N}_{def}$) for all $n, m, k \in \mathbb{N}_{def}$ as
   $n = m \cdot k$ if and only if $|n| = |k \times m|$
   $n = m + k$ iff there exists sets A, B that $A \cup B = \emptyset$, $|A| = m$ and $|B| = k$ and $|A \cup B| = |n|$.

6. The order $\leq$ is a well ordering of $\mathbb{N}_{def}$. This follows from the fact that $\mathbb{N}_{def}$ is the least fixed point in the right lattice.

2.10.2 Induction

1. Principle of Induction.
   If a property $P(x)$ is such that $P(0)$ holds, then for all $n \in \mathbb{N}_{def}$, $P(n)$ holds.

2. Induction arguments. (Two steps)

3. Strong induction.
   To show a property (A) holds for all $n \in \mathbb{N}$ with $n \geq n_0$:
   (1) show that $A(n_0)$ holds.
   (2) show that for all $n \geq n_0$, if for all $n_0 \leq k \leq n$, $A(k)$ holds, then $A(n+1)$ holds.
   (3) conclude that (A) holds for all $n \in \mathbb{N}$ with $n \geq n_0$.

4. Recursive definitions.
   Initial values and a rule.

5. **Principle of structural induction.**
   Let B be a set and let $C_1, ... C_n$ be construction rules. Let A be recursively defined to be the $\subseteq$-least set such that $B \subseteq A$ and A is closed under the rules $C_1, ... C_n$. Let P(x) be a property. If
   (1) for all $b \in B$, $P(b)$ holds
   (2) for all $a_1, ... a_m$ and c and $1 \leq i \leq n$, if $P(a_1), ... P(a_m)$ all hold and c is obtained from $a_1, ... a_m$ by a single application of rule C_i, then P(c) holds.
   Then P(x) holds for every element of A.