No. 12

Date

from MIT OCW 6.042J Week 2, date: August 16, 2025

1. More Proof Techniques

1.1 Proof by Contradiction

A proof by contradiction / indirect proof:
you show that if a proposition were false, then some logical contradiction or absurdity would follow.
⇒ the proposition must be true

$$\frac{\neg P \longrightarrow F}{P}$$

※ direct proof are generally preferable as a matter of clarity.

1.2 Method

in order to prove a proposition P by contradiction:
1. Write, "We use proof by contradiction."
2. Write, "Suppose P is false."
3. Deduce a logical contradiction.
4. Write, "This is a contradiction. Therefore, P must be true."

Example

Theorem 1.1 $\sqrt{2}$ is irrational.

Proof. We use proof by contradiction.
Suppose the claim is false; that is, $\sqrt{2}$ is rational. Then we can write $\sqrt{2}$ as a fraction a/b in lowest terms.
Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that a is even; that is, a is a multiple of $\sqrt{2}$. Therefore, a^2 must be a multiple of 4.!
Because of the equality $2b^2 = a^2$, we know $2b^2$ must also be a multiple of 4. This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms.
This is a contradiction. Therefore, $\sqrt{2}$ must be irrational. □

1.3 Potential Pitfall

using indirect proof when a direct proof would be simpler:
not wrong, just aren't excellent.

Theorem 1.2

If f and g are strictly increasing functions, then $f+g$ is a strictly increasing function.

- Proof. (direct)

  Let x and y be arbitrary real numbers such that $x>y$. Then:

  $f(x)>f(y)$ (since f is strictly increasing)

  $g(x)>g(y)$ (since g is strictly increasing)

  Adding these inequalities gives:

  $f(x)+g(x)>f(y)+g(y)$

  Thus, $f+g$ is strictly increasing as well.

- Proof. (indirect) ← makes the argument needlessly convoluted

  We use proof by contradiction.

  Suppose that $f+g$ is not strictly increasing. Then there must exist real numbers x and y such that $x>y$, but

  $f(x)+g(x) \leq f(y)+g(y)$

  This inequality can only hold if either $f(x) \leq f(y)$ or $g(x) \leq g(y)$. Either way, we have a contradiction because both f and g were defined to be strictly increasing.

  Therefore, $f+g$ must actually be strictly increasing.

1.4 Proof by Cases

$A \vee (\bar{A} \wedge B)$ and $A \vee B$ were equivalent.

⇒ Another way to prove this would be to reason by cases:

- A is T (True)

  A V anything will have truth value T.

  both expressions are of this form → both have the same truth value, namely T.

- A is F (false)

  A V P will have the same truth as P for any proposition, P.

  → the second expression has the same truth value as B

  the first expression has the same truth value as $\bar{F} \wedge B = B$

  → both expressions will have the same truth value, namely, the value of B

Example

Theorem. Every collection of 6 people includes a club of 3 people or a group of 3 strangers.

Proof. The proof is by case analysis.

Let x denote one of the six people. There are two cases:

1. Among the remaining 5 people, at least 3 have met x.
2. Among the remaining 5 people, at least 3 have not met x.

We first argue that at least one of these cases must hold.

We'll prove this by contradiction. Namely, suppose neither case holds. This means that at most 2 people in the group met x and at most 2 did not meet x. This leaves at least 1 of the remaining 5 people unaccounted for. That is, at least 1 of the people neither met x nor did not meet x, which contradicts our agreement that every pair has met or has not met. So at least one of these two cases must hold.

Case 1: Suppose that at least 3 people that did meet x.

This case splits into two subcases:

Case 1.1: no pair among these people met each other. Then these are a group of at least 3 strangers. So the Theorem holds the subcase.

Case 1.2: some pair among these people have met each other. Then that pair, together with x, form a club of 3 people. So the Theorem holds in this subcase.

This implies that the Theorem holds Case 1.

Case 2: Suppose that there exist at least 3 people that did not meet x.

This case also splits into two subcases:

Case 2.1: every pairs among these people met each other. Then these people are a club of at least 3 people. So the Theorem holds in this subcase.

Case 2.2: some pair among these people have not met each other. Then that pair, together with x, from a group of at least 3 strangers. So the Theorem holds in this subcase.

This implies that the Theorem also holds in Case 2, and therefore holds in all cases.

2 Predicates

A predicate is...
a proposition whose truth depends on the value of one or more variables.

Example
"n is a perfect square."
↳ True for n=4, but false for 5

predicates are often named with a letter
Furthermore a function-like notation is used to denote a predicate supplied with specific variable values.

↳ Example
$P(n)$ = "n is a perfect square."
↳ $P(4)$ is true, $P(5)$ is false

2.1 Quantifying a Predicate

There are a couple of assertion one commonly makes about a predicate:
- it is sometimes true
- it is always true

Example
$x^2 \geq 0$ → always true when x is a real number
$5x^2 - 7 = 0$ → only sometimes true; specifically, when $x = \pm\sqrt{\frac{7}{5}}$

Always True
⇒ ∘ For all n, P(n) is true.
∘ P(n) is true for every n.
Sometimes True
⇒ ∘ There exists an n such that P(n) is true.
∘ P(n) is true for some n.
∘ P(n) is true for at least one n.

2.2 More Cryptic Notation

To say that a predicate $P(n)$ is true for all values of x in some set D:

$\forall x \in D, P(n)$

↳ is read "for all"

To say that a predicate $P(x)$ is true for at least one value of x in D:

$\exists x \in D, P(x)$

↳ is read "there exists"

2.3 Mixing Quantifiers

Example

Goldbach's Conjecture states:

"Every even integer greater than 2 is the sum of two primes."

write this more verbosely ⇓ to make use of quantification clearer

For every even integer n greater than 2, there exist prims p and q such that $n = p+q$.

Let Ev be the set of even integers, let Primes be the set of primes ⇓

$\forall n \in Ev \ \exists p \in Primes \ \exists q \in Primes . \ n = p+q$

2.4 Order of Quantifiers

Swapping the order of different kinds of quantifiers (existential or universal) changes the meaning of a proposition.

Example

Let A be the set of Americans
Let D be the set of dreams
define the predicate $H(a,d)$ to be "American a has dream d."

$\exists d \in D \ \forall a \in A . \ H(a,d)$ ⇒ there is a single dream that every American shares.

$\forall a \in A \ \exists d \in D . \ H(a,d)$ ⇒ every American has their personal dream

2.4. | Variables over Domain

When all the variables in a formula are understood to take values from the same nonempty set, D, it's conventional to omit mention of D.

Example

$\forall x \in D\ \exists y \in D.\ Q(x,y) = \forall x\, \exists y.\ Q(x,y)$

→ D : unnamed nonempty set that x and y range over.

⇒ is called domain of the formula

2.5 Negating Quantifiers

$\neg \forall x, P(x)$ is equivalent to $\exists x, \neg P(x)$

$(\neg \exists x, Q(x)) \longleftrightarrow \forall x, \neg Q(x)$

2.6 Validity

When a propositional formula evaluates to T no matter what truth values are assigned to the individual propositional variables:

it is called valid

Example

- $[P \wedge (Q \vee R)] \longleftrightarrow [(P \wedge Q) \vee (P \wedge R)]$ ⇒ valid
- $\exists x\, \forall y.\ P(x,y) \longrightarrow \forall y\, \exists x.\ P(x,y)$ ⇒ valid

  Proof. Let D be the domain for the variables and P_0 be some binary predicate on D. We need to show that if $\exists x\, \forall y.\ P(x,y)$ holds under this interpretation, then so does $\forall y\, \exists x.\ P(x,y)$.

  So suppose $\exists x\, \forall y.\ P(x,y)$. So some element $x_0 \in D$ has the property that $P_0(x_0, y)$ is true for all $y \in D$. So for every $y \in D$, there is some $x \in D$, namely x_0, such that $P_0(x,y)$ is true.

  That is, $\forall y\, \exists x.\ P(x,y)$ holds under this interpretation, as required.
- $\forall y\, \exists x,\ P(x,y) \longrightarrow \exists x\, \forall y.\ P(x,y)$ ⇒ not valid

  ↑ under this interpetation the conclusion asserts is certainly false

  ⇒ such interpetation is called a counter model to the assertion

3 Mathematical Data Types

a set is ...

a bunch of objects, which are called the "elements"

↳ elements : can be just about anything
(numbers, points in space, or even other sets etc.)

The conventional way to write down a set :
to list the elements inside curly-braces

- the order of elements is not significant
  ex $\{x, y\} = \{y, x\}$
- it doesn't make sense to think of an element appering more than once in a set
  ex $\{x, x\} = \{x\}$

$e \in S$: e is an element of set S
$e \notin S$: e is not an element of set S

3.1 Some Popular Sets

symbol	set	elements
$\emptyset$	the empty set	none
$\mathbb{N}$	natural numbers	$\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	integers	$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
$\mathbb{Q}$	rational numbers	$\frac{1}{2}, -\frac{5}{3}, 16$, etc.
$\mathbb{R}$	real numbers	π, e, -9, etc.
$\mathbb{C}$	complex numbers	i, $\frac{19}{2}$, $\sqrt{2} - ei$, etc.

3.2 Comparing and Combining Sets

$S \subseteq T$: set S is a subset of set T
↳ every elements of S is also an element of T
ex $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{C} \not\subseteq \mathbb{Z}$

$S \subset T$: S is a subset of T, but the two are not equal

$X \cup Y$: the union of sets X and Y
↳ contains all elements appering in X or Y or both

$X \cap Y$: the intersection of X and Y
↳ consists of all elements that appear in both X and Y

$X - Y$: the difference of X and Y
↳ consists of all elements that are in X, but not in Y.

3.2.1 Complement of A Set

D: a particular domain
A: any subset of D
$\Rightarrow \overline{A} := D - A$
↳ the complement of A
= the set of all elements of D not in A

ex $\overline{\mathbb{R}^+} = \mathbb{R}^- \cup \{0\}$

3.2.2 Power Set

$\mathcal{P}(A)$: the powerset of A
↳ the collection of all the elements of a set A
$\Rightarrow B \in \mathcal{P}(A)$ iff $B \subseteq A$

* if A has n elements, then there are 2^n sets in $\mathcal{P}(A)$

3.3 Sequences

sequence : a list of objects called terms or components

- short sequences: described by listing the elements between parentheses
  ex (a, b, c)

the differences between sets and sequences

	sets	sequences
①	the elements are required to be distinct	the terms can be the same
②	the elements don't have specified order	the terms have specified order
③	the empty one : ϕ	the empty one : Λ

↳ ex ② (a, e, c) and (a, c, e) : different sequences / $\{a, e, c\}$ and $\{a, c, e\}$: the same set

$S_1 \times S_2 \times \cdots \times S_n$: a product of sets
↳ new set consisting of all sequences where the first component is drawn from S_1, the second from S_2, and so forth.

ex $\mathbb{N} \times \{a, e\} = \{(0,a), (0,e), (1,a), (1,e), \cdots\}$

S^n : a product of n copies of a set S
ex $\{0,1\}^3 = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$

3.4 Set Builder Notation

Set builder notation: to define a set using a predicate

ex
- $A = \{n \in \mathbb{N} \mid n \text{ is a prime and } n = 4k+1 \text{ for some integer } k\}$
- $B = \{x \in \mathbb{R} \mid x^3 - 3x + 1 > 0\}$
- $C = \{a + bi \in \mathbb{C} \mid a^2 + 2b^2 \leq 1\}$

3.5 Functions

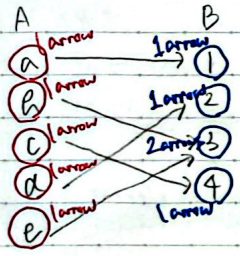
A function assigns the domain (= an element of one set) to the codomain (= elements of another set)

$f : A \to B$ ··· f is a function with domain, A, and codomain, B
$f(a) = b$ ··· f assigns the element $b \in B$ to a

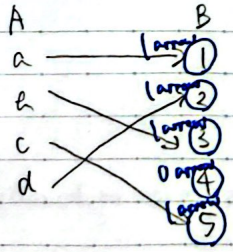
☆ finite functions
can be specified by a table
- $f(P,Q) = [P \to Q]$

P	Q	$f_8(P,Q)$
T	T	T
T	F	F
F	T	T
F	F	T

we say a function $f: A \to B$ is:
- total: if every element of A is assigned to some element of B.
  - ∴ not total ⇒ a partial function
- surjective: if every element of B is mapped to at least once.
- injective: if every element of B is mapped to at most once
- bijective: if f is total, surjective, and injective
  - ↳ each element of B is mapped to exactly once.

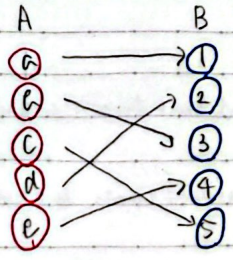


- "f is a function":
  - every point in the domain column, A, has at most one arrow out of it.
- "f is surjective":
  - every point in the codomain column, B, has at least one arrow into it.
- "f is total":
  - every point in the domain column, A, has at least one arrow out of it = it has exactly one arrow (since f is a function)



- "f is injective":
  - every point in the codomain column, B, has at most one arrow into it.

∴ If more than one arrow came out of any point in the first column:
f would be a relation (not function)



- "f is bijective":
  - every point in the A column has exactly one arrow out of it, and every point in the B column has exactly one arrow into it.

everything about a function is captured by three sets:
- domain
- codomain
- the graph of f: $\{(a, b) \mid f(a) = b\}$

the domain: to determine if f is total
the codomain: to tell if it's surjective

Lemma (Mapping Rule)
- If $f: A \to B$ is surjective, then $|A| \geq |B|$.
- If $f: A \to B$ is total and injective, then $|A| \leq |B|$.
- If $f: A \to B$ is bijective, then $|A| = |B|$.
- ※ If A is a finite set, let $|A|$ be its size, that is, the number of element in A.

- if $f: A \to B$, and $A' \subseteq A$,
  $f(A') ::= \{b \in B \mid f(a') = b \text{ for some } a' \in A'\}$.
- the set of values that arise from applying f to all possible arguments: range of f
  $\text{range}(f) ::= f(\text{domain}(f))$

4 Does All This Really Work?

"there is a handful of axioms from which everything else in mathematics can be logically derived."
↳ mainstream mathematics stands today
(but) the essence of truth in mathematics is not completely resolved

- The ZFC axioms weren't etched by God.
- No one knows whether the ZFC axioms are logically consistent.
  ⇒ Math would be broken!
  ↳ such a situation has happened before
  (several mathematicians including Russell discovered that Frege's axioms actually were self-contradictory)
- While the ZFC axioms largely generate the mathematics everyone wants, but they also imply some disturbing conclusions
  (ex) the Banach-Tarski Theorem

- In the 1930's, Gödel proved that exist propositions in ZFC are true, but do not logically follow from the axioms.

Russell's Paradox.

Let S be a variable ranging over all sets, and define
$$W ::= \{S \mid S \notin S\}$$
So by definition,
$$S \in W \text{ iff } S \notin S,$$
for every set S. In particular, we can let S be W, and obtain the contradictory result that
$$W \in W \text{ iff } W \notin W.$$