CSC165H1S Jan. 20th

| Employee | Gender | ~~Salar~~ Salary |
| --- | --- | --- |
| ~~Al~~ | ~~M~~ F | 60,000 |
| ~~B~~ | | 500 |
| C | ~~M~~ | 40,000 |
| ~~D~~ | M | 30,000 |
| E | F | 50,000 |
| F | F | 20,000 |

$P(x) \Rightarrow Q(x)$

considered true except if there is $x$ for which $P(x)$ is true and $Q(x)$ false $P \subseteq Q$ $x \in P$ but $x \notin Q$ means $P \not\subseteq Q$.

$\forall x \in \mathbb{R},\ P(x)$

$$x^2 - 2x + 2 = 0 \Rightarrow x > x + 5$$

$Q(x)$

There is no $x \in \mathbb{R}$, s.t. $x^2 - 2x + 2 = 0$
so there is no $x$ to contradict the claim that $P(x) \Rightarrow Q(x)$ is true.

IF Al Quits,

Consider: Every male employee earns between 25,000 and 45,000
True? Yes. $\forall x \in E, B(x) \Rightarrow M(x)$

The converse is Employees making between 25,000 and 45,000 are male.
True? Yes. double implication $\forall x \in E, M(x) \Rightarrow B(x)$
$\forall x \in E, B \Rightarrow M(x)$

The claims are equivalent
$\forall x \in E, M(x) \Leftrightarrow B(x)$

~~An employee~~ employee is male if only if the employee makes between 25,000 & 40,000.

Consider : $\forall x \in \mathbb{R}, x^2 - 2x + 2 = 0 \iff x > x+5$ $\boxed{\text{True}}$

Consider : $\forall x \in \mathbb{R}, x^2 - 2x + 5 = 0 \Rightarrow x > x+5$ $\boxed{\text{True}}$

$\forall x \in \mathbb{R}, x > x+5 \Rightarrow x^2 - 2x + 2 = 0$ $\boxed{\text{True}}$

no ~~contorexamp~~ countor example so it is true

$\forall x \in \mathbb{R}, \neg P(x)$ $P(x): x^2 - 2x + 2 = 0$

English $\forall x \in \mathbb{R}, \neg Q(x)$ $Q(x): x > x+5$

P is necessary and sufficient for Q

P is true exacthy when Q is true

P ~~is~~implies Q and ~~conves~~ conversely all express equivalant.

How to express that 2 properties are true?

Use And

Claim: The employee makes less than 70,000 and more than 25,000.

$x \in E$, salary $(x) < 75{,}000$ and salary $(x)$

$x = Al$. Claim true

$x = Fb$, Claim ~~Edu~~ false

Salary (Fb) < 70,000 true

Salary (Fb) > 25,000 false

$A(x)$ & $B(x)$

$x \in A \cap B$

$A(x) \wedge B(x)$

~~sets~~ ... this is intersection

logic this combination of ~~cal~~ claims called conjunction.

in English, "and" both groups & joins

~~ex~~ except, There is a pen and a telephone.

Symbols : Let D = set of objects
Let $P(x)$ x is a pen
$T(x)$ x is a telephone

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

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

The sentence

(If) could mean there is an object that is both a pen and a telephone.

$\exists x \in D.\ P(x) \wedge T(x)$

Consider: The solutions are $x<10$ and $x>20$

The solutions are ($x<20$ and $x>10$.) we join / intersect $x>10, x<20$

The Solutions are both $x<10$ and $x$ that is $>20$

graph together $x<10$, $x>20$

Can also combine claims to express that at least one is true

The employee is female or earns more than 35,000.

True for ~~Elo~~ Flo.

True for Carlos

True for Ellen

a union of the two properties

$A(x)$ or $B(x)$

$x \in A \cup B$

$A(x) \vee B(x)$

Jan 23rd CSC165H1S

Tutorial tomorrow only

M–Shw BA2175 → BA1220

① Conjunction / and

All employees make between 25,000 and 75,000.

$\forall x \in E,\ (salary(x) > 25{,}000) \wedge (salary(x) < 75{,}000)$

② disjunction / or

The employee is female or earns more than 35,000.

sentence: $F(x) \vee salary(x) > 35{,}000$

statement: $x = Flo$ Flo female, $salary(Flo) \leq 35{,}000$ True

$x = Carlos$ Carlos male $salary(Carlos) > 35{,}000$ True

$x = Ellen$ $F(Ellen)$ true $salary(Ellen) > 35{,}000$ True

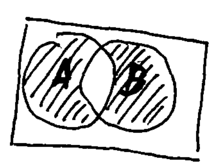
$x = Doug$ $F(Doug)$ False $salary(Doug) < 35{,}000$ False

$A \vee B$ true when A, B or A and B are true.
(inclusive or)


English sometimes means ~~exact~~ exclusive or.
e.g. You may take CSC148 or CSC150 for credit.

"either"

intepretation: can't take both




A xor B true
$(A \wedge \neg B) \vee (B \wedge \neg A)$

[redacted]

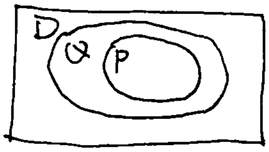
## Restricting Domains

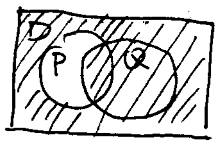
- can use quantification
- implication
- conjunction and disjunction to restrict set of objections

Every D that is a P is also a Q. (Every object in D that has property P also has property Q)

$\boxed{\forall x \in D,\ P(x) \Rightarrow Q(x)}$

$\forall x \in P,\ Q(x)$ when this is true




all object in D lie in shaded area.

negation

$\forall x \in D, \neg P(x) \vee Q(x)$

$A \Rightarrow B$

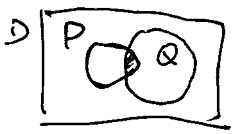
$\Leftrightarrow$

$\neg A \vee B$

---

Every D is a P and a Q (Every object in D has property P and property Q)

$\forall x \in D, P(x) \wedge Q(x)$ when this is a true statement.

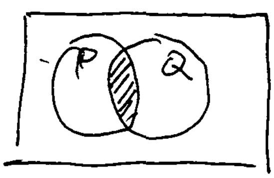



all objects lie in $P \cap Q$ (the shaded area)

---

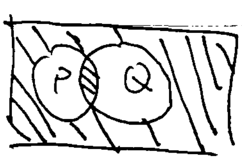
Some D that is a P is also a Q.

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




If this true. the shaded area is not empty.

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




statement is true when shaded area is not empty.

Negation:

symbol $\neg$

Q: when is this statement?

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

A: when $P(x)$ is false for ~~a~~ every $x$ in the domain

i.e. $P(x)$ is true for every $x$ in domain.

so $\neg \exists x \in D\, P(x) \underset{\text{is equal to}}{\Longleftrightarrow} \forall x \in D, \neg P(x)$

words: There is no $x$ such that $P(x)$ is true, equal to, for all $x$, $P(x)$ is false

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

Q:* When is $\forall x \in D, P(x)$ false?

[redacted]

CSC165H1S Jan 25th Rui Qiu

retain: $P(x) \Rightarrow Q(x)$
equivalent to
~~$\neg P(x)$~~ $\neg P(x) \vee Q(x)$

$\neg(\exists x \in D, P(x)) \Leftrightarrow \forall x \in D, \neg P(x)$

words: There is no $x$ for which $P(x)$ is true.
equal to
For all $x$, $P(x)$ is false ($\neg P(x)$ is true)

when is $\forall x \in D, P(x)$ false?
There must be a ~~certain~~ ~~ex~~ counter-example $P(x)$ (being false) $\exists x \in D, \neg P(x)$ $\Leftrightarrow$ $\neg(\forall x \in D, P(x))$

$\exists x \in D$, $P(x)$ is false.

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

[The missing sentences here are word version of the following statements]

define $O(x)$: $x$ earns over 110,000

$\forall x \in O, F(x)$

$\boxed{\forall x \in E, O(x) \Rightarrow F(x)}$

$\neg(\forall x \in E, O(x) \Rightarrow F(x))$

equal to
$\exists x \in E, \neg(O(x) \Rightarrow F(x))$
when false?
$O(x) \wedge \neg F(x)$

$\boxed{\exists x \in E, O(x) \wedge \neg F(x)}$

This is not true, since there is some employee making over 110,000.

Thus its negation must be true.

Consider, Every P is a Q.

$\forall x \in X, P(x) \Rightarrow Q(x)$.

negation:

Not every P is a Q. $\Leftrightarrow$ There is a P which is not a Q.

$\neg(\forall x \in X, P(x) \Rightarrow Q(x))$

$\Leftrightarrow \exists x \in X, P(x) \wedge \neg Q(x)$

There is a P that is a Q.

$\exists x \in X, P(x) \wedge Q(x)$

Negation:

No P is a Q.

$\neg(\exists x \in X, P(x) \wedge Q(x))$.

$\Leftrightarrow \forall x \in X, \neg(P(x) \wedge Q(x))$

$\Leftrightarrow \forall x \in X\ \neg P(x) \vee \neg Q(x)$ ①

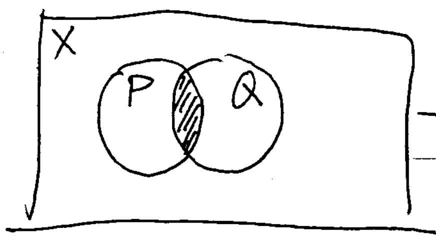
$\Leftrightarrow \forall x \in X\ P(x) \Rightarrow \neg Q(x)$ ②

$\Leftrightarrow \forall x \in X, Q(x) \Rightarrow \neg P(x)$ ③

No P is a Q is equivalent to

Every P is a non-Q.

Every Q is a non-P.




→ negate


rules:

$\neg(\forall x \in X, \cdots) \Leftrightarrow \exists x \in X, \neg(\cdots)$

$\neg(\exists x \in X, \cdots) \Leftrightarrow \forall x \in X, \neg(\cdots)$

$\neg(P(x) \Rightarrow Q(x)) \Leftrightarrow P(x) \wedge \neg Q(x)$

$\neg(P(x) \wedge Q(x)) \Leftrightarrow P(x) \Rightarrow \neg Q(x)$

$\Leftrightarrow Q(x) \Rightarrow \neg P(x)$

$\Leftrightarrow \neg P(x) \vee \neg Q(x)$

Negate the statement:

$\forall x \in X, \exists y \in Y, P(x,y) \Rightarrow Q(x,y)$

$\neg(\forall x \in X, \exists y \in Y, P(x,y) \Rightarrow Q(x,y))$

$\Leftrightarrow \cancel{\exists x \in X, \exists y \in Y}$

$\exists x \in X, \neg(\exists y \in Y, P(x,y) \Rightarrow Q(x,y))$

$\Leftrightarrow \exists x \in X, \forall y \in Y, \neg(P(x,y) \Rightarrow Q(x,y))$

$\Leftrightarrow \exists x \in X, \forall y \in Y, P(x,y) \wedge \neg Q(x,y)$

$P(x) \vee Q(x) \Rightarrow R(x)$

could mean

$(P(x) \vee Q(x)) \Rightarrow R(x)$

or

$P(x) \vee (Q(x) \Rightarrow R(x))$

**Procedure rules**

highest ( )

then $\neg$

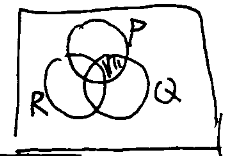
then $\wedge, \vee$

then $\Rightarrow, \Leftrightarrow$

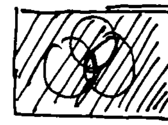
lowest $\exists, \forall$

CSC165H1S Lecture 9 Jan. 27th Rui Qiu

Venn Diagram of $[P(x) \Rightarrow (Q(x) \Rightarrow R(x))]$ is false




8 regions $[P(x) \Rightarrow (Q(x) \Rightarrow R(x))]$ is true



Alternatively use a $\boxed{\text{truth table}}$

| $P(x)$ | $Q(x)$ | $R(x)$ | $Q(x) \Rightarrow R(x)$ | $P(x) \Rightarrow (Q(x) \Rightarrow R(x))$ | $P(x) \wedge Q(x)$ | $P(x) \wedge Q(x) \Rightarrow R(x)$ |
|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T |
| T | T | F | F | F | T | F |
| T | F | T | T | T | F | T |
| T | F | F | T | T | F | T |
| F | T | T | T | T | F | T |
| F | T | F | F | T | F | T |
| F | F | T | T | T | F | T |
| F | F | F | T | T | F | T |

$\therefore \quad P(x) \Rightarrow (Q(x) \Rightarrow R(x)) \Leftrightarrow P(x) \wedge Q(x) \Rightarrow R(x)$

since # of entries is $2^k$ ($k$ = # of predicates),

we use logical arithmetic rules to simplify:

commutativity: $a+b=b+a$ $\quad P \wedge Q \Leftrightarrow Q \wedge P$

associativity: $(a+b)+c=a+(b+c)$ $\quad \overset{\text{logic}}{\Longrightarrow}$ $\begin{cases}(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R) \\ (P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)\end{cases}$

distributivity: $a * (b+c) = a*b + a*c$ $\quad \begin{cases}P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)\end{cases}$

Additive identity : $x + \underline{0} = x$

multiplicative identity : $x \cdot 1 = x$

$\boxed{\text{idempotancy: } 0 * c = 0 \quad 1 * 1 = 1}$ ?

conjunction identity : $P \wedge \underline{(Q \vee \neg Q)} \Leftrightarrow P$, $P \wedge P \Leftrightarrow P$

disjunction identity: $P \vee (Q \wedge \neg Q) \Leftrightarrow P$, $P \vee P \Leftrightarrow P$

Statement "Variable X is not equal to 2 or 3."

Equiv. Expression: not((x==2) or (x==3))

$\Updownarrow$

not (x==2) and not (x==3)

Inequiv. Expression: "not (x==2) or not (x==3)"

$\longrightarrow$ always true ! (X不可能同时取2个values)

Demorgan's Laws

$\neg(P \wedge Q) = \neg P \vee \neg Q$

$\neg(P \vee Q) = \neg P \wedge \neg Q$

Statement "$P \Rightarrow Q \Leftrightarrow \neg P \vee Q$" is true

$\therefore\ \neg(P \Rightarrow Q) \Leftrightarrow \neg(\neg P \vee Q)$

$\Downarrow$

$\neg\neg P \wedge \neg Q$

$P \wedge \neg Q$

$\therefore\ \neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$

Equivalent (Biconditional)

$P \Leftrightarrow Q$

$\Leftrightarrow\ (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

$\Leftrightarrow\ (\neg P \vee Q) \wedge (\neg Q \vee P)$ Demorgan

$\Leftrightarrow\ ((\neg P \vee Q) \wedge \neg Q) \vee ((\neg P \vee Q) \wedge P)$ distributting of "$\vee$"

$\Leftrightarrow\ ((\neg P \wedge \neg Q) \vee \underbrace{(Q \wedge \neg Q)}_{\phi}) \vee (\underbrace{(\neg P \wedge P)}_{\phi} \vee (Q \wedge P))$ of "$\wedge$"

$\Leftrightarrow\ (\neg P \wedge \neg Q) \vee (Q \wedge P)$

CSC165H1 S Jan 30th Rui Qiu

## Multiple Quantifiers

Some Male employee makes less than 55,000.

$\exists x \in E, \neg F(x) \wedge L(x)$

define

$T(x,s)$: "employee x makes salary s"

$\exists x \in E, \exists s \in \mathbb{N}, \neg F(x) \wedge T(x,s) \wedge s \leq 55000$

for salary bound $w$

$\exists x \in E, \exists s \in \mathbb{N}, \neg F(x) \wedge T(x,s) \wedge s \leq w$

For salary bound $w$.

$\exists s \in \mathbb{N}, \exists x \in E, \neg F(x) \wedge T(x,s) \wedge s \leq w$

is equivalent as is

$\exists x \in E, \neg F(x) \wedge (\exists \in \mathbb{N}, T(x,s) \wedge s \leq w)$

$\boxed{\text{The two } \exists \text{ commute}}$

## Mixed qualifiers

Consider: ① $\forall x \in A, \exists y \in B, x+y=5$ (for all, one)

② $\exists y \in B, \forall x \in A, x+y=5$ (for one, all)

Are these statements equivalent?

Consider $A=\{1,2,3,4\}$ $B=\{1,2,3,4\}$

① True ② False

$\therefore \neg(\forall x \in A, \exists y \in B, x+y=5 \iff \exists y \in B, \forall x \in A, x+y=5)$

$\therefore$ cannot commute quantifiers of different type.

Another example:

- $P(m,n)$: "n is the square of m"

$n=m^2$

$\exists m \in \mathbb{N}, P(m,n)$ There is an integer that is the square of another int.

$\exists y \in \mathbb{N}, \exists x \in \mathbb{N}, P(m,n)$

$\exists (m,n) \in X^2, P(m,n)$ same

[redacted]

• every element of $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$

$P(m,n)$ "the product of $m, n$ is an integer"

$m * n \in \mathbb{N}$

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N}, P(m,n)$

$\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, P(m,n)$

$\forall (m,n) \in \mathbb{N}^2, P(m,n)$

domain $P$ people

Likes$(x,y)$: " person $x$ likes person $y$"

• $\boxed{\text{Everyone likes Everyone}}$.

$$\forall x \in P, \forall y \in P, \text{Likes}(x,y)$$
$$\Updownarrow$$
$$\forall y \in P, \forall x \in P, \text{Likes}(x,y)$$

• someone likes someone

$\exists x \in P, \exists y \in P, \text{Likes}(x,y)$

$\exists y \in P, \exists x \in P, \text{Likes}(x,y)$

• Everyone likes someone

$\forall x \in P, \exists y \in P, \text{Likes}(x,y)$ is ~~true~~ this equivalent to:

$\Updownarrow$

$\exists y \in P, \forall x \in P, \text{Likes}(x,y)$

There is someone liked by everyone.

~~$[\neg(\forall x \in P, \exists y \in P, \text{Likes}(x,y)) \Leftrightarrow \exists y \in P, \forall x \in P, \text{Likes}(x,y)]$~~

note: $\exists y \in P, \forall x \in P, \text{Likes}(x,y)$

$\Rightarrow \forall x \in P, \exists y \in P, \text{Likes}(x,y)$

~~Translitute~~ Transitive

have $a, b, c$

runs $a > b$ and $b > c$

then $a > c$

$>$ is ~~translitute~~ transitive.

CSC165H1S 五 Feb 1st Rui Qiu

Statement $P(x) \Rightarrow Q(x) \Leftrightarrow$ its contrapositive : $\neg Q(x) \Rightarrow \neg P(x)$

domain unspecified $(N, R, E)$

predicate $P, Q$ not specified $(x^2<100, x>0,$ x is male ...$)$

Let $D$ represent set of all possible domains

— $P$ — all possible predications

say $\forall D \in D, \forall P \in P, \forall Q \in P, (P(x) \Rightarrow Q(x)) \Leftrightarrow (\neg Q(x) \Rightarrow \neg P(x))$

Truth Table:

| $P$ | $Q$ | $P \Rightarrow Q$ | $\neg Q$ | $\neg P$ | $\neg Q \Rightarrow \neg P$ | $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ |
|---|---|---|---|---|---|---|
| T | T | T | F | F | T | T |
| T | F | F | T | F | F | T |
| F | T | T | F | T | T | T |
| F | F | T | T | T | T | T |

Converse: consider $(P(x) \Rightarrow Q(x)) \overset{?}{\Leftrightarrow} (Q(x) \Rightarrow P(x))$

consider $D = N^+$, $P(x)$ : x is odd, $Q(x)$: x+1 is even

x is odd $\Rightarrow$ x+1 is even $\quad P(x) \Rightarrow Q(x)$

& x+1 is even $\Rightarrow$ x is odd $\quad Q(x) \Rightarrow P(x)$

Consider $D = R$, $P(x)$: "$x>2$", $Q(x)$ "$x^2>4$"

$P(x) \Rightarrow Q(x)$ : $x>2 \Rightarrow x^2>4$ True

$Q(x) \Rightarrow P(x)$ : $x^2>4 \Rightarrow x>2$ False $\Leftarrow$ Counter ex: $x=-3$, $\underbrace{x^2>4}_{T} \Rightarrow \underbrace{x>2}_{F}$ False

$\therefore$ Can say

$\exists D \in D, \exists P \in P, \exists Q \in P$, (not "for all")

$(P(x) \Rightarrow Q(x)) \Leftrightarrow (Q(x) \Rightarrow P(x))$

this statement is said to be satisfiable

* if no domain & predicates can make a statement true, say the statement "unsatisfiable".

Ex: $\neg(\exists D \in D, \exists P \in P, \exists Q \in P, P(x) \wedge \neg P(x))$

# Chapter 4 Proof

[Def'n] : A proof is an argument that shows that a statement is true.

[Theorem] "Every odd integer has a square that is odd."
or "square of every odd ~~number is~~ integer is odd.

Proof:

Convince yourself it's true:
any number is odd if remainder when divided by 2 is 0.

① $\forall x \in \mathbb{Z},\ x^2 \% 2 = 0$. False ← Counter ex: $x = 2, \in \mathbb{Z}$

② $\forall x \in \mathbb{Z}$, $x$ is odd $\Rightarrow x^2$ is odd ;

$P(y)$ : $y$ is odd.

$\forall x \in \mathbb{Z},\ P(x) \Rightarrow P(x^2)$

$\forall x \in \mathbb{Z},\ \cancel{P(2x)}\ P((2x+1)^2)$

$\forall x \in \mathbb{Z},\ P(x) \wedge P(x^2)$ False ← Counter ex: even ~~#~~ numbers

$\exists x \in \mathbb{Z}\ \ P(x) \wedge P(x^2)$ True

Assume $n \in \mathbb{Z}$ is an arbitrary integer

Further assumption : $n$ is odd.

(If we can prove that $n^2$ is odd ~~then~~ then have shown $P(n) \Rightarrow P(n^2)$)

Assume $n \in \mathbb{Z}$

Assume $n$ is odd

$\boxed{\text{show } n^2 \text{ is odd}}$

Then $n^2$ is odd.

Then $n$ is odd $\Rightarrow n^2$ is odd.

Then $\forall n \in \mathbb{Z}$, $n$ is odd $\Rightarrow n^2$ is odd

$n$ is odd

then $n \% 2 == 1$

then $n = 2q + 1$ , $q \in \mathbb{Z}$

$\therefore n^2 = (2q+1)^2$

$n^2 = 4q^2 + 2q + 1$

$= 2(2q^2 + q) + 1$

$\therefore n^2 \% 2 == 1$ ($n^2$ is odd)

CSC165H1S Feb. 3rd Rui Qiu

Theorem:

Every odd int. has a square that is odd.

symbols: $\underbrace{\forall n \in \mathbb{Z}}$, $n$ is odd $\Rightarrow n^2$ is odd.

trying to prove a universal quantification

def$^n$: An integer $n$ is odd if and only if

$\exists q \in \mathbb{Z}$, $n = 2q+1$ ($n \% 2 == 1$)

Assume $n \in \mathbb{Z}$ (arbitrary int.)

(~~domains~~ restriction)

Assume $n$ is odd

(assume antecedent is true)

(need to show consequence must be true)

$\because$ $n$ is odd, ~~then~~ then

$\exists q \in \mathbb{Z}$, $n = 2q+1$

Let $j \in \mathbb{Z}$, be st. $n = 2q+1$

Then $n^2 = (2j+1)^2 = 4j^2 + 4j + 1 = \cancel{2j+1}\ 2(2j^2+2j)+1$

But for integer $j$, $2j^2+2j$ is an integer

So $\exists k \in \mathbb{Z}$, $n^2 = 2k+1$

Then $n^2$ is odd (what we wanted to prove)

Final proof:

domain assumption

Assume $n \in \mathbb{Z}$, # $n$ is an ~~abit~~ arbitrary integer.

Assume $n$ is odd # $n$ is an arb. Int.

$\therefore$ ~~Then~~

Assume ~~anteced~~ antecedent true

Then $\exists q \in \mathbb{Z}$, $n = 2q+1$ # by def'n of odd

Let $j \in \mathbb{Z}$ be s.t. $n = 2j+1$ # label ~~quoul~~ quotient $j$.

# substitution

#algebra

Then $\exists k \in \mathbb{Z}$, $n^2 = 2k+1$ . # $2j^2+2j \in \mathbb{Z}$. when $j \in \mathbb{Z}$.
Then $n^2$ is odd
Then $n$ is odd $\Rightarrow n^2$ is odd.
Thus $\forall n \in \mathbb{Z}$, $n$ is odd $\Rightarrow n^2$ is odd # $n$ is an arbitary int.

pair

Theorem: For every non-negative real number $(x, y)$
if $x$ is greater than $y$,
then their geometric mean, $\sqrt{xy}$
is less than their arithmetic mean $\frac{x+y}{2}$

$$\underbrace{\forall x \in \mathbb{R}^{\geq 0}, \forall y \in \mathbb{R}^{\geq 0}}_{\text{universal quantification}} . \ (x > y) \Rightarrow \frac{x+y}{2} > \sqrt{xy}$$

Proof. Assume $x, y$ are arbitrary ~~numer~~ nonegative real nubers
Assume $x > y$ # assume antecedent.
Then $x - y > 0$
Then $(x-y)^2 > 0$
Then $x^2 - 2xy + y^2 > 0$ ... stucked here
move to the conclusion!

$\frac{x+y}{2} > \sqrt{xy}$

$\Leftrightarrow x+y > 2\sqrt{xy}$
$\Leftrightarrow (x+y)^2 > 4(xy)$ # $x+y > 0$, $2\sqrt{xy} > 0$

$\Leftrightarrow (x+y)^2 - 4xy > 0$
$\Leftrightarrow (x-y)^2 > 0$

$x^2 - 2xy + y^2 + 4xy > 4xy$
$(x+y)^2 > 4xy$

then $x+y > 2\sqrt{xy}$ $(x, y \in \mathbb{R}^{\geq 0})$
$\frac{x+y}{2} > \sqrt{xy}$

Then $\forall x \in \mathbb{R}^{\geq 0}, \forall y \in \mathbb{R}^{\geq 0}$,
$(x > y) \Rightarrow \left(\frac{x+y}{2} > \sqrt{xy}\right)$

This Proof technique is called: Direct Proof of a universally Quantified Implication.

in logic $\Rightarrow$ is transitive

$\forall x \in D, (P(x) \Rightarrow Q(x)) \wedge (Q(x) \Rightarrow R(x))$

Conclude $\forall x \in D, P(x) \Rightarrow R(x)$

Why? $P \subseteq Q \quad Q \subseteq R \quad P \subseteq R$

Logical derivation

Consider $\neg(((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R))$

$\Leftrightarrow \neg(\neg((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \vee (P \Rightarrow R))$ (implication)

$\Leftrightarrow (\neg\neg((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \wedge \neg(P \Rightarrow R))$ (deMorgan)

$\Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \wedge \neg(P \Rightarrow R)$ (double negation)

$\Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee R) \wedge \neg(\neg P \vee R)$ (implication)

$\Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee R) \wedge (P \wedge \neg R)$ (deMorgan)

$\Leftrightarrow ((\neg P \vee Q) \wedge P)) \wedge ((\neg Q \vee R) \wedge \neg R)$ (comm, assoc)

$\Leftrightarrow ((\neg P \wedge P) \vee (P \wedge Q)) \wedge (\neg Q \wedge \neg R) \vee (R \wedge \neg R))$

$\Leftrightarrow P \wedge Q \wedge \neg Q \wedge \neg R$

false

$\therefore ((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$

CSC165H1S Feb 6th Rui Qiu

$P \wedge (P \vee Q) \Leftrightarrow P$
$P \vee (P \wedge Q) \Leftrightarrow P$
Velleman calls these absorption

$P \wedge (Q \wedge \neg Q) \Leftrightarrow Q \wedge \neg Q$

$\Leftrightarrow$

$P \vee (Q \vee \neg Q) \Leftrightarrow Q \vee \neg Q$
absorption law in tut.
(can be used for Q4)

Last week we proved
- $\forall n \in \mathbb{Z}$, $n$ is odd $\Rightarrow n^2$ is odd
- $\forall x \in \mathbb{R}^{\geq 0}, \forall y \in \mathbb{R}^{\geq 0}, x > y \Rightarrow \frac{x+y}{2} > \sqrt{xy}$

- we proceeded directly from assumption about ~~antecedent~~ antecedent ~~and~~ to our consequent.

formal argument: a universally quantified implication

Claim: C1 $\forall x \in D, p(x) \Rightarrow q(x)$
make a change of implications.

$$\left.\begin{array}{ll} C\,2.0 & \forall x \in D,\ p(x) \Rightarrow r_1(x) \\ 2.1 & \forall x \in D,\ r_1(x) \Rightarrow r_2(x) \\ \vdots & \qquad\vdots \\ 2.n & \forall x \in D,\ r_n(x) \Rightarrow q(x) \end{array}\right\} \Rightarrow \forall x \in D,\ p(x) \Rightarrow q(x)$$

(by transitivity of implication)

Proof Structure. DIRECT PROOF OF UNIVERSALLY-QUANTIFIED PREDICATE

Assume $x \in D$
  : # prove $p(x)$
  Then $p(x)$.
Then $\forall x \in D, p(x)$ # $x$ was assumed to be a typical element of D.

- How to figure out a chain of implications?
① make a list of things that $p(x)$ implies.

$p(x) \to r_1(x) \to r_{11}(x), r_{12}(x)$
$p(x) \to r_2(x)$
$p(x) \to r_3(x)$

② make a list of things that imply $q(x)$.

$$\begin{array}{l} S_{11}(x) \\ S_{12}(x) \end{array} \to S(x) \to q(x)$$

$$\begin{array}{l} S_{21}(x) \\ S_{22}(x) \end{array} \to S(x_2) \nearrow$$

THEOREM. $\forall n \in \mathbb{Z}$, n is odd $\Rightarrow n^2$ is odd, is the converse true?

$\hookrightarrow \forall n \in \mathbb{Z}$, $n^2$ is odd $\Rightarrow n$ is odd.

try a direct proof

Assume $n \in \mathbb{Z}$, # n is arbitrary int.

Assume $n^2$ is odd # antecedent

Then $\exists q \in \mathbb{Z}$, $n^2 = 2q+1$ # def$^n$ of odd.

Let $j \in \mathbb{Z}$. be st $n^2 = 2j+1$

Then ... need a sqrt to get to n.

rough work

n is odd

$\exists s \in \mathbb{Z}$, $n = 2s+1$

let $k \in \mathbb{Z}$, be st. $n = 2k+1$

then $n^2 = 4k^2+4k+1$

Consider the contrapositive of stat.

$\forall n \in \mathbb{Z}, \neg(n \text{ is odd}) \Rightarrow \neg(n^2 \text{ is odd})$

or

$\forall n \in \mathbb{Z}$, n is even $\Rightarrow n^2$ is even (similar to odd pbm)

Proof Structure:

Assume $n \in \mathbb{Z}$, # n arbitrary

Assume n is even # antecedent

Then $\exists q \in \mathbb{Z}$, $n = 2q$ # defn of "even"?

Let $j \in \mathbb{Z}$, be st $n = 2j$

Then $n^2 = 4j^2 = 2(2j^2)$

An indirect proof of a universally quantified implication

$\forall x \in D, p(x) \Rightarrow q(x)$

Assume $x \in D$

Assume $\neg q(x)$ # negtion of conclusion

Then

$\vdots$

Then $\neg p(x)$ # negation of assumption

Then $\neg q(x) \Rightarrow \neg p(x)$

Then $p(x) \Rightarrow q(x)$ #contrapositive

Then $\forall x \in D,\ p(x) \Rightarrow q(x)$

1 and itself

Prime numbers $P = \{ p \in \mathbb{N} \mid p$ has exactly 2 unique divisors$\}$

$= \{2, 3, 5, 7, 11, 13, \cdots\}$

How many prime #s ? $\infty$ many.

Theorem: There are an infinite number of prime numbers

$\forall n \in \mathbb{N},\ |P| > n$

?

[redacted]

CSC165H1S Lec 14 Feb 8th Rui Qiu

Test 1 Coverage : to end of Chapter 3 on course notes.

THRM: There are an infinite number of primes.

(Translation) i.e. $P$ = set of prime numbers, $|P|$ cardinality of $P$.

then $\forall n \in N, |P| > n$.

universal quantifier $Q(n)$, a predicate

[Direct Proof] : Assume $n \in \mathbb{N}$

Assume $\neg S$

then $\neg (\forall n \in \mathbb{N}, |P| > n)$

then $\exists n \in \mathbb{N}, |P| \leq n$

let $k \in \mathbb{N}$ ~~best~~ be s.t. $|P| = k$

Then $k \leq n$

then $k > 1$ # since $P_0 = 2$ is prime

$\Leftarrow$

# list all prime numbers $\leftarrow$ then $P = \{P_0, P_1, \cdots, P_{k-1}\}$

let $r = p_0 p_1 \cdots p_{k-1}$

Then $r \in \mathbb{N}$ # since $\mathbb{N}$ closed under multiplication

then $r > 1$

let $t = r + 1$

then $t \in \mathbb{N}$

then $\exists p \in P$, $p$ divides $t$ # $t$ is not prime

let $p_j \in P$ s.t. $p_j$ divides $t$ $\Rightarrow t$ has prime factors

then $\exists m \in \mathbb{N}$ s.t. $t = p_j \cdot m$

Also $p_j$ divides

then $\exists u \in N, r = p_j u$

Consider $t - r = p_j m - p_j u = p_j (m - u)$

then $p_j$ divides $t - r$

then $t - r = 1$

then $p_j$ divides $1$

then $p_j = 1$

then $1 \in P$ (since $p_j \in P$)

but $1 \notin P$ (since 1 has only one divisor)
then $(1 \in P) \wedge (1 \notin P)$
This is a false statement
then $S$ is true.

# (Assume $\neg S$) leads to a statement that is false
# hence $\neg S$ is false
# $S$ is true

$\therefore$ There are an infinite number of primes!

** The proof technique used is called "proof by contradiction"

Q: How to prove an existential claim?
$\exists x \in D, p(x)$
$\rightarrow$ construct an $x \in D$ s.t. $p(x)$ is true.

Prove $\exists x \in \mathbb{R}$ $\underbrace{x^3+3x^2-4x=12}_{p(x)}$.

[Proof]: let $x=2$ # consider a particular value
Then $x \in \mathbb{R}$ # well known
then $x^3+3x^2-4x = 2^3+3\cdot 2^2-4\cdot 2=12$ # Substitution
then $\exists x \in \mathbb{R}$, $x^3+3x^2-4x=12$

CSC165H1S Feb 10th

Rui Qiu

Term Test 1
Tue Feb 14th
$2^{15}-3^{15}$ pm EX 100

Proving a statement about a sequence

sequence: $a_0, a_1, \cdots, a_n \ldots$
Consider the claim:
$\exists i \in \mathbb{N}, a_j \le i \Rightarrow j < i$
T/F depends on sequence

Consider particular sequence
$a_j: 0, 1, 4, 9, \cdots, j^2$
$j \quad 0, 1, 2, 3, \cdots, j$
$a_j = j^2$
Is the claim T/F for this sequence

Claim says $\exists i \in \mathbb{N}, \cdots a_j \le i \Rightarrow j < i$

Since a proof about $\exists$ s
Let $i =$ ____
Then $i \in \mathbb{N}$ # satisfy domain restriction
Assume $j \in \mathbb{N}$ # j is arbitrary
Assume $a_j \le i$
:
Then $j < i$
Then $a_j \le i \Rightarrow j < i$
Then $j \in \mathbb{N}, a_j \le i \Rightarrow j < i$

proving this will depend on value of fact that $j \in \mathbb{N}$ fact that $a_j \le i$

Induction: try $i = 2$

Let $i=2$
Then $i \in \mathbb{N}$
Assume $j \in \mathbb{N}$
Assume $a_j \le i$

Then $a_j \le 2$ # since $i=2$
Then $j^2 \le 2$ # since $a_j = j^2$
Then $j \le \sqrt{2}$ # since $\sqrt{\ }$
Then $j < 2$ # since $\sqrt{2} < 2$
Then $j < i$

~~then $a_j \le i \Rightarrow j < i$~~

~~Then $\forall j \in N, a_j \le i \Rightarrow j < i$~~

Then $\exists i \in N, \forall j \in N, a_j \le i \Rightarrow j < i$

Alternate proof of $a_j \le i \Rightarrow j < i$      true

<u>indirect proof</u> (prove contrapositive)

$\neg(j < i) \Rightarrow \neg(a_j \le i)$

$j \ge i \Rightarrow a_j > i$

Assume $j \ge i$

Then $j \ge 2$

Then $a_j = j^2 \ge 4$

Then $j \ge i \Rightarrow a_j > i$

New problem:

Given 12.345

truncate get 12.

for $x \in \mathbb{R}^+$, use the ~~for~~ floor function to truncate truncate.

\# floor$(x) = \lfloor x \rfloor$ is the largest int. $\le x$

ceil$(x) = \lceil x \rceil$ is the smallest int. $\ge x$

$\lfloor 12.345 \rfloor = 12$

$\lceil 17 \rceil = 17$

$\lfloor -3.14 \rfloor = -4$

floor: $\mathbb{R} \to \mathbb{Z}$

express the definition using ~~loop~~ logic:

$(\lfloor x \rfloor \in \mathbb{Z}) \wedge (\lfloor x \rfloor \le x) \wedge (\forall z \in \mathbb{Z}, z \le x \Rightarrow z \le \lfloor x \rfloor)$

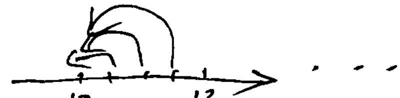
more general

$(\forall x \in \mathbb{R}, y \in \lfloor x \rfloor) \Leftrightarrow (y \in \mathbb{Z}) \wedge (y \le x) \wedge (\forall z \in \mathbb{Z}, z \le x \Rightarrow z \le y)$

A theorem about $\lfloor x \rfloor$

Theorem: $\forall x \in \mathbb{R}$, $\boxed{\lfloor x \rfloor < x + 1}$    goal

- a theorem about $x \in \mathbb{R}$, what about $\lfloor x \rfloor$?

$\lfloor x \rfloor$ is many to one  ...

Proof: Assume $x \in \mathbb{R}$

Let $y = \lfloor x \rfloor$

Then $y \le x$ # def$^n$ of floor

Also $x < x+1$ # $0<1$, add $x$ to both sides

Then $y < x+1$

Then $\lfloor x \rfloor < x+1$

Then $\forall x \in \mathbb{R}, \lfloor x \rfloor < x+1$

## CSC165H1S        Feb 13th        Rui Qiu

### Floor function $\lfloor x \rfloor$:

$x \in \mathbb{R}$, largest integer $\leq x$.

$\forall x \in \mathbb{R}, y = \lfloor x \rfloor \Leftrightarrow y \in \mathbb{Z} \wedge y \leq x \wedge (\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y)$

* Note: we prove that $\forall x \in \mathbb{R} \quad \lfloor x \rfloor < x+1$

[Theorem] : $\forall x \in \mathbb{R}, \lfloor x \rfloor > x-1 \quad (\Leftrightarrow \lfloor x \rfloor + 1 > x)$

[Proof]: <try direct proof>

Assume $x \in \mathbb{R}$   # x is an arbitrary real number

Let $y = \lfloor x \rfloor$  # introduce symbol to stand for $\lfloor x \rfloor$.

Then $y \in \mathbb{Z}$   # from def'n of floor func.

Then $y \leq x$

Then $y+1 > y$   (# since $1>0$)

Then $y+1 \in \mathbb{Z}$   # $\mathbb{Z}$ closed under addition

# Goal: $\lfloor x \rfloor > x-1$ or $y > x-1$ or $y+1 > x$
have not used: $\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y$

$\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y$   # contrapositive: $\forall z \in \mathbb{Z}, \neg(z \leq y) \Rightarrow \neg(z \leq x)$

$\forall z \in \mathbb{Z}, z > y \Rightarrow z > x$

$y+1 \in \mathbb{Z}$

$y+1 > y \Rightarrow y+1 > x$

$\lfloor x \rfloor + 1 > x$

$\lfloor x \rfloor > x-1$

[final proof]:

Assume $x \in \mathbb{R}$

let $y = \lfloor x \rfloor$

Then $y \in \mathbb{Z}$

Then $y \leq x$

then $y+1 > y$

then $y+1 \in \mathbb{Z}$

Then $y+1 > x$   # from def of $\lfloor x \rfloor$, contrapositive of its 3rd term?

then $y > x-1$

then $\lfloor x \rfloor > x-1$

Then $\forall x \in \mathbb{R}, \lfloor x \rfloor > x-1$

Another sequence problem:

sequence $\forall n \in N$, $a_n = \lfloor n/2 \rfloor$

$a_0 = \lfloor 0/2 \rfloor$, $a_1 = \lfloor 1/2 \rfloor$, $\cdots$ $a_2 = a_3 = 1$, $a_4 = a_5 = 2$

Consider the statement (claim):

$\exists i \in N.\ \forall j \in N, j > i \Rightarrow a_j > a_i$

(turn out to be false. * how to prove?)

* Disproving a result $\rightarrow$ show negation!

$\neg(\exists i \in N, \forall j \in N, j > i \Rightarrow a_j = a_i)$

$\Leftrightarrow \forall i \in N, \exists j \in N, \neg(j > i \Rightarrow a_j = a_i)$

$\Leftrightarrow \underline{\forall i \in N}, \exists j \in N, (j > i) \wedge (a_j \neq a_i)$ $\leftarrow$ Prove this

universal quantification

[Proof]: Assume $i \in N$

Let $j = i+2$

Then $j \in N$

Then $j = i+2 > i$

Then $a_j = \lfloor j/2 \rfloor$, $\lfloor (i+2)/2 \rfloor = \lfloor i/2 + 1 \rfloor$

Then $a_j \neq a_i$

Then $(j > i) \wedge (a_j \neq a_i)$

Then $\exists j \in N, (j > i) \wedge (a_j \neq a_i)$

Then $\forall i \in N, \exists j \in N, (j > i) \wedge (a_j \neq a_i)$

Then $\exists i \in N, \forall j \in N, j > i \Rightarrow a_j = a_i$ is false.

CSC 165 H1S Feb 15th Rui Qiu

S: $\forall x \in X, \forall y \in Y, P(x,y) \Rightarrow Q(x,y)$

interpretation:

$x = \mathbb{R}$ $P(x,y)$ "$y \leq x$"

$y = \mathbb{Z}$ $Q(x,y)$ "$y = \lfloor x \rfloor$"

To disprove S

Should you prove

$\forall x \in X, \forall y \in Y, P(x,y) \Rightarrow \neg Q(x,y)$

?

tempting $P \Rightarrow Q$, negate to $P \Rightarrow \neg Q$

$P \Rightarrow Q \Leftrightarrow \neg P \vee Q$

negation $\neg(\neg P \vee Q)$

$P \wedge \neg Q$

How about $\forall x \in X, \forall y \in Y, \neg(P(x,y) \Rightarrow Q(x,y))$ ?

No!

~~Need to be right~~

$\neg S: \neg(\forall x \in X, \forall y \in Y, P(x,y) \Rightarrow Q(x,y))$

$\Leftrightarrow \exists x \in X, \exists y \in Y, \neg(P(x,y) \Rightarrow Q(x,y))$

$\Leftrightarrow \exists x \in X, \exists y \in Y, P(x,y) \wedge \neg Q(x,y)$

Let $x = 2$, Then $x \in \mathbb{R}$

Let $y = 1$ Then $y \in \mathbb{Z}$

Then $P(2,1)$ # since $\leq 2$

Then $\neg Q(2,1)$ # since $1 \neq \lfloor 2 \rfloor$

Consider

$\forall e \in \mathbb{R}, e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R}, 0 < |x-a| < d \Rightarrow |f(x) - l| < e))$

want to prove this for a given func. $f$ and consists $a, d$.

Structure of Proof:

Assume $e \in \mathbb{R}$ # abitrary element of $\mathbb{R}$

Assume $e > 0$ # antecedent

Let $d_e =$ ______

⋮

Then $d_e \in \mathbb{R}$ # verify domain

⋮

Then $d_e > 0$.

Assume $x \in \mathbb{R}$

Assume $0 < |x-a| < d_e$. # antecedent

⋮

Then $|f(x) - l| < e$

Then $0 < |x-a| < d_e \Rightarrow |f(x) - l| < e$

Then $\forall x \in \mathbb{R},\ 0 < |x-a| < d_e \Rightarrow |f(x)-l| < e$

Then $\exists d \in \mathbb{R},\ d > 0 \wedge (\forall x \in \mathbb{R},\ 0 < |x-a| < d_e \Rightarrow |f(x) - l| < e$

Then $e > 0 \Rightarrow (\exists d \in \mathbb{R},\ 0 < |x-a| < d_e \Rightarrow |f(x) - l| < e.))$

Then $\forall e \in \mathbb{R},\ e > 0 \Rightarrow (\exists d \in \mathbb{R},\ d > 0 \wedge (\forall x \in \mathbb{R}.\ 0 < |x-a| < d_e$
$\Rightarrow |f(x) - l| < e))$

to negate this:
start from outside:

recall $\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$

$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q \Leftrightarrow P \Rightarrow \neg Q$

to get

$\exists e \in \mathbb{R}, e > 0 \wedge (\forall d \in \mathbb{R}, d > 0 \Rightarrow (\exists x \in \mathbb{R}.\ 0 < |x-a| < d \wedge |f(x) - l| \geq e))$

Consider

Theorem: If $n$ is natural number, $n^2+n$ is even.

logic: $\forall n \in \mathbb{N},\ n^2+n$ even.

$\forall n \in \mathbb{N},\ \exists z \in \mathbb{N},\ n^2+n = 2i$

approach: show result holds for even $n$.
odd $n$.
Since $n$ is even ~~—~~ or odd, result follows for all.

Assume: $n \in \mathbb{N}$, # $n$ arbitrary
Then $n$ is even or $n$ is odd.
Thus $(\exists i \in \mathbb{N}, n=2i) \vee (\exists i \in \mathbb{N}, n=2i+1)$
Case 1. Assume $\exists i \in \mathbb{N}, n=2i$ # $n$ integer
Let $i_0 \in \mathbb{N}$ best $n=2i_0$
Then $n^2+n = (2i_0)^2 + 2i_0$
$= 2(2i_0^2 + i_0)$
Then $\exists j \in \mathbb{N}, n^2+n=2j$
Then $n^2+n$ is even.
Case 2: Assume $\exists i \in \mathbb{N}, n=2i+1$ # $n$ is odd
Let $i_0 \in \mathbb{N}$. ~~best n~~ $n=2i_0+1$
Then $n^2+n=(2i_0+1)^2+(2i_0+1)$
$= \cancel{2(\ldots)} \; 2(2i_0^2+3i_0+1)$
Then $\exists j \in \mathbb{N}, n^2+n=2j$
Then $n^2+n$ is even
Then $n^2+n$ is even
Then $\forall n \in \mathbb{N}$, $n^2+n$ is ~~even~~ even.

IN GENERAL, WANT TO PROVE $A \Rightarrow B$
~~want to~~ can break $A$ into $A_1, A_2, \ldots A_n$
prove $A_1 \vee A_2 \vee B_3 \vee \cdots \vee A_n \Rightarrow B$
need to prove $A_1 \Rightarrow B$
$A_2 \Rightarrow B$
$\vdots$
$A_n \Rightarrow B$
Then $A \Rightarrow B$
• you need to prove each implication since arbitrary element could be in ~~any~~ any $A$.

Proof by cases.

# CSC165H1S Feb ~~[illegible]~~ 17th Rui Qiu

Theorem: When the square of any integer is divided by 3, the remainder is either 1 or 0.

~~Proof: $\forall n \in \mathbb{Z}$~~

$$\boxed{\begin{array}{l} n \% 3 = 0 \text{ or } 1 \\ \downarrow \\ \exists k \in \mathbb{Z}, \text{ s.t. } n = 3k \\ \exists k \in \mathbb{Z}, \text{ s.t. } n = 3k+1 \end{array}}$$

Proof: $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n^2 = 3k) \vee (\exists k \in \mathbb{Z}, n^2 = 3k+1)$

form universally quantifier disjunction

Is it true?

$n=7$
$n^2=49$
$=3*16+1$

$n=1$
$n^2=1$
$=3*0+1$

$n=10$ $n^2=100$
$=3 \times 33+1$

$n=3$
$n^2=9$
$n^2 = 3 \times 3 + 0$

note: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, (n=3k) \vee (n=3k+1) \vee (n=3k+2)$

$n \% 3 = 0$

$\exists k \in \mathbb{Z}, n = 3k$

Let $j \in \mathbb{Z}, n = 3j$

Then $n^2 = 9j^2$

$= 3(3j^2)$

Then $\exists k \in \mathbb{Z}, n^2 = 3k$

$n \% 3 = 1$

$\exists k \in \mathbb{Z}, n = 3k+1$

Let $j \in \mathbb{Z}, n = 3j+1$

Then $n^2 = (3j+1)^2 = 9j^2 + 6j + 1$

$= 3(3j^2 + 2j) + 1$

Then $\exists k \in \mathbb{Z}, n^2 = 3k+1$

$n \% 3 = 2$

$\exists k \in \mathbb{Z}, n = 3k+2$

Let $j \in \mathbb{Z}, n = 3j+2$

Then $n^2 = (3j+2)^2 = 9j^2 + 12j + 4$

$= 3(3j^2 + 4j + 1) + 1$

Then $\exists k \in \mathbb{Z}, n^2 = 3k+1$

Complete proof:

Assume $n \in \mathbb{Z}$ # n is an arbitrary integer

Then $\exists k \in \mathbb{Z}, (n=3k) \vee (n=3k+1) \vee (n=3k+2)$ # by remainder theorem

Let $k_0 \in \mathbb{Z}, (n=3k_0) \vee (n=3k_0+1) \vee (n=3k_0+2)$

Case 1: Assume $n=3k_0$

Then $n^2=(3k_0)^2$
$=9k_0^2$
$=3(3k_0^2)$

Then $\exists k \in \mathbb{Z}, n^2=3k$

Case 2: Assume $n=3k_0+1$

Then $n^2=(3k_0+1)^2$
$=3(3k_0^2+2k_0)+1$

Then $\exists k \in \mathbb{Z}, n^2=3k+1$

Case 3: Assume $n=3k_0+2$

Then $n^2=9k_0^2+12k_0+4$
$=3(3k_0^2+4k_0+1)+1$

Then $\exists k \in \mathbb{Z}, n^2=3k+1$

Then $\forall n \in \mathbb{Z}, n^2=3k \vee n^2=3k+1$

If ~~must~~ want to prove $Q$, but don't know cases to try

try to ~~p~~ construct some $P$

try to prove $P \vee \neg P \Rightarrow Q$

proof: Case 1: Assume $P$

Then $Q$

Case 2: Assume $\neg P$

Then $Q$

Then $Q$.

Another statement form:

$\boxed{P \Rightarrow Q \vee R}$

note: $Q$ is either true or false

if $Q$ is true, $P \Rightarrow Q \vee R$ is true independent of $P, R$.

if $Q$ is false then $P \Rightarrow Q \vee R$ is true when $P \Rightarrow R$ is true.

Can show
$P \wedge \neg Q \Rightarrow R$
(equivalent
$P \Rightarrow (Q \vee R)$
$\Leftrightarrow \neg P \vee (Q \vee R)$
$\Leftrightarrow (\neg P \vee Q) \vee R$
$\Leftrightarrow$ ~~$\neg P \vee Q$~~ $P \wedge \neg Q \Rightarrow R$)

How to prove $A \Leftrightarrow B$
theorem of statement of the form

$$\left( \begin{array}{l} A \Leftrightarrow C_1 \\ \quad \Leftrightarrow C_2 \\ \quad \dots \\ \quad \Leftrightarrow B \end{array} \right.$$

<u>Alt.</u>
to prove $A \Leftrightarrow B$
prove $A \Rightarrow B$
~~prove~~ and $B \Rightarrow A$

earlier:
proved n is odd then $n^2$ is odd.
$n^2$ is odd then n is odd

So we have proven
n is odd iff $n^2$ is odd.

<u>Theorem</u>
For every int n,
$15 | n$ iff $3 | n$ and $5 | n$.

$a | b$ means
b is divisible by a
$\exists q \in \mathbb{Z}$ s.t. $b = qa$

Proof: ($\Rightarrow$) Prove $\forall n \in \mathbb{Z}$, $15 | n \Rightarrow (3 | n) \wedge (5 | n)$
Assume $n \in \mathbb{Z}$
Assume $15 | n$
Then $\exists k \in \mathbb{Z}$, $n = 15k$
Let $k_0 \in \mathbb{Z}$, $n = 15k_0$
Then $n = 3(5k_0)$
Then $\exists k \in \mathbb{Z}$, $n = 3k$
Then $3 | n$
Then $n = 5(3k_0)$
~~Then $5 | n$~~
Then $\exists k \in \mathbb{Z}$, $n = 5k$
Then $5 | n$
Then $5 | n \wedge 3 | n$
Then $15 | n \Rightarrow (3 | n) \wedge (5 | n)$

($\Leftarrow$) Assume $(3 | n) \wedge (5 | n)$
obvious $15 | n^2$
need to show $\not\forall$ $15 | n^2$

CSC165H1S    Feb 27th    Rui Qiu

Proving an equivalence/bimplication

Theorem

For every integer $n$,

$15|n$ iff $3|n$ and $5|n$

$a|b$ a divides b (b%a == 0)

Proof

Approach

prove ① $\forall n \in \mathbb{Z}$, $3|n \wedge 5|n \Rightarrow 15|n$

② $\forall n \in \mathbb{Z}$, $15|n \Rightarrow 3|n \wedge 5|n$

② ($\Rightarrow$) ~~Assume~~

Assume $n \in \mathbb{Z}$

Assume $15|n$

Then $\exists k \in \mathbb{Z}$, $n = 15k$

Let $k_0 \in \mathbb{Z}$, $n = 15k_0$

Then $n = 3 \cdot 5k_0$

$= 3(5k_0)$

Then $\exists k \in \mathbb{Z}$, $n = 3k$

Then $3|n$

Then $n = 5(3k_0)$

Then $\exists k \in \mathbb{Z}$, $n = 5k$

Then $5|n$

Then $3|n \wedge 5|n$

Then $15|n \Rightarrow 3|n \wedge 5|n$

Then $\forall n \in \mathbb{Z}$, $15|n \Rightarrow 3|n \wedge 5|n$

($\Leftarrow$) ① Prove $\forall n \in \mathbb{Z}$, $3|n \wedge 5|n \Rightarrow 15|n$

Assume $n \in \mathbb{Z}$

Assume $3|n \wedge 5|n$

Then $\exists k \in \mathbb{Z}$, $n = 3k$

Then $\exists m \in \mathbb{Z}$ $n = 5m$

Let $k_0 \in \mathbb{Z}$, $n = 3k_0$

Let $m_0 \in \mathbb{Z}$, $n = 5m_0$

~~sca~~ scratch

$3k_0 = 5m_0$

easy to show

$15|n^2$

want $15|n$

$\exists p_0, p_1, p_2, \cdots p_s \in P, n = p_0, p_1, \cdots p_s$

Let $p_0 = 3, p_1 = 5$

Then $n = (3, 5)(p_2, p_3, \cdots p_s)$

$= 15(p_2 \cdots p_s)$

$= 15 \cdot q$

# $q = p_2 \cdots p_s$

Then $q \in \mathbb{Z}$

# Since $\mathbb{Z}$ closed under $\times$

Then $\exists k \in \mathbb{Z}, n = 15k$

Then $15 | n$

Then ~~3~~ $3|n \wedge 5|n \Rightarrow 15|n$

Then $\forall n \in \mathbb{Z}, 3|n \wedge 5|n \Rightarrow 15|n$

Then $\forall n \in \mathbb{Z}, 3|n \wedge 5|n \Leftrightarrow 15|n$

<u>symbol introduction Rule</u>

Assume $A$

$\vdots$

contradiction

Then $\neg A$ ($\neg$ introduction)

Assume $A$

(direct) $\vdots$

Then $B$

Then $A \Rightarrow B$ ($\Rightarrow$ introduction)

---

Assume $\neg B$

(indirect) $\vdots$

Then $\neg A$

Then $A \Rightarrow B$

Assume $a \in D$

$\vdots$

Then $P(a)$

Then $\forall a \in D, P(a)$ ($\forall$ introduction)

---

$a \in D$

$P(a)$

Then $\exists a \in D, P(a)$ ($\exists$ introduction)

$A$

$B$

Then $A \wedge B$ (introduce $\wedge$)

---

$A$

Then $A \vee B$ (introduce $\vee$)

---

$A \Rightarrow B$

$B \Rightarrow A$

Then $A \Leftrightarrow B$ (introduce $\Leftrightarrow$)

Use known facts eliminate symbols

if u know $A \Rightarrow B$
additional $A$
infor Then $B$

$A \Rightarrow B$
$\neg B$
Then $\neg A$

if u know $A \wedge B$
Then $A$ ~~spe~~ separately
Then $B$

if you know $A \vee B$
additional infor $\neg A$
Then $B$

if you know $\neg A \Rightarrow B$
$\Leftrightarrow \neg(\neg A) \vee B$
$\Leftrightarrow A \vee B$
$\vee$ introduce

if u know $A = B$
Then $A \Rightarrow B$
Then $B \Rightarrow A$

if you know $\forall a \in D, P(a)$
$x \in D$
Then $P(x)$

if u know $\exists x \in D, P(x)$
Let $x_0 \in D$, be such that $P(x_0)$

## Ch5 ~~Algorithm Analysis Analysis and~~ A

~~can you prove~~
~~that the algorithm~~
~~solves g~~

CSC165H1S Feb 29th Rui Qiu

## Ch5 Algorthim Analysis and Asymptotic Analysis

decimal number representation

2031

- 1 → unit position
- 3 → tens
- 0 → hundreds
- 2 → thousands

$1 + 3\times 10 + 0\times 100 + 2\times 1000$

$= 1\times \boxed{10}^0 + 3\times \boxed{10}^1 + 0\times \boxed{10}^2 + 2\times \boxed{10}^3$

base used is $\beta = 10$

"digits" $0, 1, 2, \cdots, 9 = \beta - 1$
integers

other base

$\beta = 16$ ? hexadecimal (old IBM)

$\beta = 8$ octal

$\beta = 3$

$\beta = 2$ binary

come use any base $\beta$ ~~int~~ with $|\beta| > 1$

in general, can represent any integer value as

$$\pm(t_0 \times \beta^0 + t_1 \times \beta^1 + \cdots + t_n \times \beta^n + \cdots)$$

for any base $\beta \in \mathbb{Z}$ has $|\beta| > 1$

$t_i \in \mathbb{Z}$, $0 \le |t_i| < |\beta|$

now mostly

$\beta = 2$

$\beta = 10$

How to convert between bases $\beta=10$ and $\beta=2$?

~~between base~~

$(165)_{10}$ base $\beta=10$

~~This~~ ① Euclideaualgorithim - find the most significant bit first

$2^0=1$

$2^1=2$

$2^2=4$ $\quad 165 = 128 + 32 + 4 + 1$

$2^3=8$ $\quad 165 = 1\times2^7 + 0\times2^6 + 1\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 0\times2^1 + 1\times2^0$

$2^4=16$

$\vdots$ $\quad (165)_{10} = (10100101)_2$

Alternate: find lsb to msb
(% 2, then /2 ~~[illegible]~~
do shift value to right

given $n$, $n \in \mathbb{Z}^+$

```
i=0
do
{ t_i = n % 2

    n = n/2
    i = i+1
} while (n>0)
```

| $n$ | $i$ | $t_i$ |
|---|---|---|
| 165 | 0 | 1 |
| 82 | 1 | 0 |
| 41 | 2 | 1 |
| 20 | 3 | 0 |
| 10 | 4 | 0 |
| 5 | 5 | 1 |
| 2 | 6 | 0 |
| 1 | 7 | 1 |

$\Longrightarrow (165)_{10} = (10100101)_2$

can extend to rational number

$$(\overset{3\,2\,1\,0}{1101}.\overset{-1\,-2\,-3}{101})_2 = (2^3+2^2+2^0+2^{-1}+2^{-3})_{10}$$

$$= (8+4+1+0.5+0.125)_{10}$$

$$= (13.625)_{10}$$

note : $\frac{1}{10} = (0.1)_{10}$
$= (0.00011001100\overline{1100})_2$

- fraction that terminate in decimal isn't guranteed to ~~terminated~~ in binary!

<u>arithmetic</u>

same algorithm as in decimal just remember
$(1)_{10} + (1)_{10} = (10)_2$

$\beta=10$

$$\begin{array}{r} 108 \\ +\,165 \\ \hline 273 \end{array}$$

$\beta=2$

$$\begin{array}{r} 1101100 \\ +\,10100101 \\ \hline 100010001 \end{array}$$

$\rightarrow$ check

$\beta=10$

$$\begin{array}{r} 15 \\ \times\,15 \\ \hline 225 \end{array}$$

$\beta=2$

$$\begin{array}{r} 1111 \\ \times\,1111 \\ \hline 1111 \\ 11110 \\ 111100 \\ +\,1111000 \\ \hline 11100001 \end{array}$$

messy
$\hookrightarrow$ algorithm for binary multiplication
{
proof of correctness

f=0
while (f <= 4))
print ___

CSC165H1 March 2nd Rui Qiu

Base $\beta$ $\beta \in \mathbb{Z}$, $|\beta| > 1$

$x \in \mathbb{R}$ $x = \pm \cdots t_2 \times \beta^2 + t_1 \times \beta^1 + t_0 \cdot \beta^0 + t_{-1} \times \beta^{-1} + t_{-2} \times \beta^{-2} + \cdots$

binary numbers $\beta = 2$

\+ * $(1)_2 + (1)_2 = (10)_2$

A function for multiplying 2 binary numbers.

in binary, $\times 2$ shifts bits to left
$101 \times 10 = 1010$

in binary $/2$ shifts bits to right
$101 / 10 = 10$

"see the sheet and the function"

~~def mu~~

in the end we want ~~z=m×n~~ $z = m \cdot n$
so function returns $m \times n$

If loop ~~varia~~ invariant is valid
then when loop ~~exis~~ exits we have
$z = mn - xy$ and $x = 0$
then $z = mn$

before 1st execution of the loopbody, we have
$x = m, y = n, z = 0$
have
$mn - xy = mn - mn = 0$

so we have
$z = mn - xy$

need to show:
if $z = mn - xy$ at start of loop body
then
$z = mn - xy$ at end of loop body

Let $x_i$ represent the value of variable $x$ before the start of the ith ~~equation~~ iteration of the loop and simarly for $y, z$.

the value of x at end of the $i-1^{st}$ iteration.

Assume $z_i = mn - x_i y_i$ # ~~invariable~~ invariant holds
# at start of loop

~~CASE 1~~ ~~Ass~~ CASE 1: Assume $x_i$ is odd.

$x_i$ $\boxed{\ldots b_2 b_1 1}$

$x_{i+1}$ $\boxed{0 \ldots b_2 b_1}$

Then $z_{i+1} = z_i + y_i$

$x_{i+1} = (x_i - 1)/2$

$y_{i+1} = 2y_i$

so $mn - x_{i+1} y_{i+1}$

$= mn - [(x_i - 1)/2][2y_i]$

$= mn - x_i y_i + y_i$

$= z_i + y_i$

$= z_{i+1}$

Then $z_{i+1} = mn - x_{i+1} y_{i+1}$

CASE 2. Assume $x_i$ is even

Then $z_{i+1} = z_i$

Then $x_{i+1} = x_i/2$

Then $y_{i+1} = y_i * 2$

$x_i$ $\boxed{\ldots b_2 b_1 0}$

$x_{i+1}$ $\boxed{\ldots b_2 b_1}$

Then $mn - x_{i+1} y_{i+1}$

$= mn - (x_i/2)(y_i * 2)$

$= mn - x_i y_i$

$= z_i$

$= z_{i+1}$

Then $z_{i+1} = mn - x_{i+1} y_{i+1}$

Then since $x_i$ is either even or odd, we have

$z_{i+1} = mn - x_{i+1} y_{i+1}$

Then $z_i = mn - x_i y_i \Rightarrow z_{i+1} = mn - x_{i+1} y_{i+1}$

And since $x_{last} = 0$, $z_{last} = mn - x_{last} y_{last} = mn$
and so function returns correct result.

How many iterations of loop body

$m = 10$ ~~#~~ $x = 10 \to x = 1 \to x = 0$ exit loop 2 iterations
$m = 101$ $x = 101 \to x = 10 \to x = 1 \to x = 0$ exit loop 3 iterations
$m = 1101$ $x = 1101 \to x = 110 \to x = 11 \to x = 1 \to x = 0$ exit loop 4 iterations

so, # ~~loop~~ bits is ~~a~~ req'd to represent $m$
is the # of iterations of loop.

CSC 165H1S  March 5th  Rui Qiu

```
def mult (m,n)
    x=m
    y=n
    z=0
    while x!=0:
        if x%2==1:
            z=z+y
        x=x/2      (x=x>>1)
        y=y*2      (y=y<<1)
    return z
```

$m \cdot n = (110111)_2$
$n = 1011$
$m = 101$

$$\begin{array}{r} 1011 \\ \times\ 101 \\ \hline 1011 \\ 0 \\ 1011 \\ \hline 110111 \end{array}$$

A, B, C, A+B+C

| trace | x | y | z |
|---|---|---|---|
| | 101 | $\boxed{1011}$ | 0 |
| | | | 1011 A |
| | 10 | 10110 → C | |
| | 1 | $\boxed{101100}$ | $\boxed{1011}$ → A+B, $z=z+B$ |
| | | | 10111 |
| | 0 | 1011000 | $\boxed{110111}$ A+B+C |

value returned

\# of ---- of loop
= # bits req'd to store m.

$2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$
$b_5\ b_4\ b_3\ b_2\ b_1\ b_0$

if $m \geq 2^{k-1}$
$m < 2^k$  then k bits req'd to store m in binary.

Given m
how to find k ?
use $\log_2 m$

$m=(6)_{10}$  $2^3=8>6$
$2^2=4\leq 6$
need 3 bits
$\log_2 6 = 2.xxx$
$(6)_{10}=(110)_2$

$m=(13)_{10}$
$=(1101)_2$
$2^4=16>13$
$2^3=8\leq 13$
need $k=4$ bits to represent $(13)_{10}$ in binary.
$\log_2 13 = 3.xxx$

$m=8$
$\log_2(8)=3$  $8=2^3$
$(8)_{10}=(1000)_2$
So # bits req'd is not
$\lceil \log_2 m \rceil$

\# bits is
$\lfloor \log_2 m \rfloor + 1$

$\neq \lfloor \log_2 m + 1 \rfloor$

CSC165H1S March 7th Rui Qiu

```
def LS(L,x): search keys
    i=0                    #1
    while i < len(L)       #2
        if L[i]=x:         #3
            return i       #4
        i=i+1              #5
    return -1              #6
```

L=[2,5,3,7]

x=5

# steps req'd 7

in general if $x==L[j]$

# steps executed $1+3(j+1)$

return index i s.t. $\exists L[i]=x$

or $-1$ if $\neg\exists i\in N, L[i]==x$

most # steps when x does not appear in list

#steps is $1+3(\underbrace{len(L)-1}_{j}+1)+2$

$=3\,len(L)+3$

- called worst case runtrace for algorithm
- get a guarantee on max runtime

- How to count # of steps in program?
- might count

function call · 1 step for call
1 step for each param evaluation
to steps to evaluate function.

return statements - 1 step to return
- #steps to evaluate return values

if stat
- 1 step to branch to next stat
- 1 step for each component of condition

assignment
- 1 step for assignment
- # steps required to evaluate RHS

integer arithmetic, float arithmetic, logical arithmetic
, · 1 step for each operation
· using variable
  1 step
· using list element
  1 step
+ # of steps to figure out index.

~~in near~~

in reality -
~~time~~ for each
step varies
(depends on memory use)
for simplicity,
  Count # of steps
later on, we will account for
fact that steps to be different time?

· usually express runtime of an algrithm as a function of ~~size~~ size of the input to algorithm.
for linear search, worst case runtime

$W(n) = 3n + 3$

LS
len(n)

constants
somewhat ~~arbit~~ arbitrary
since come from assuming
all steps take same thing

useful information
runtime grows
~~lin~~ linearly with
list length
e.g. time to search a list of length $10^6$
$\approx 100 \times$ time of search
list length $10^4$

terminology:

$t_P(x)$ — # steps for algorithm P on input X

~~$A_P(x)$~~ $A_P(n)$ — ~~#~~ average # of steps for P on input of ~~size~~ size n.

~~$B_P(x)$~~ $B_P(n)$ — best case # steps for P on input of size n.

$W_P(n)$ — ~~b~~ ~~case~~ worst case # steps for P on input of size n.

$$B_P(n) = \min\{t_P(x) \mid x \in Inputs_P \wedge size(x) = n\}$$

$$W_P(n) = \max\{t_P(x) \mid x \in Inputs_P \wedge size(x) = n\}$$

3 algorithms with worst case runtimes
$3n^2$, $8n^2$ and $\frac{1}{2}n^2$ step.

- only ~~to chu~~ conclusion to make is runtime $\sim n^2$
  double input size, quadruple runtime

$W_{LS}(n) = 3n+3$
$n = len(L)$
$W_{BS}(n) = \cancel{9\lceil \log_2 n \rceil}\ 9\lceil \log_2 n \rceil$

LS, BS are two algorithms that could be used to search a sorted list.

Which algorithm is faster
- depends on size of list

$n=5$, $W_{LS}(5) = 18$ steps
$W_{BS}(5) = 27$ steps
$n=16$, $W_{LS}(16) = 51$ steps
$W_{BS}(16) = 36$ steps
$n=1024$, $W_{LS}(1024) = 3075$
$W_{BS}(1024) = 90$

as n grows, BS becomes much faster than LS.
$n=8$ $W_{LS}(8) = 27$
$W_{BS}(8) = 27$

cutoff / breakpoint in comparison of algorithms.
$\forall n >$ breakpoint, better to use BS.

- insight!
$W_{LS}(n) = 3n+3$
$\Downarrow$
~~W_{LS}~~ $W_{LS}(n) = 2n+3$ steps
improvened only
shifts breakpoint

Important feature is how runtime varies with n.

| $T(n) \backslash n$ | 10 | 100 | 1000 | 10000 | 100,000 |
|---|---|---|---|---|---|
| $\log_2 n$ | 3 | 6 | 9 | 13 | 16 |
| $\sqrt{n}$ | 3 | 10 | 31 | 100 | 316 |
| $n$ | 10 | $10^2$ | $10^3$ | $10^4$ | $10^5$ |
| $n\log_2 n$ | 30 | 600 | 9000 | $13 \times 10^4$ | $16 \times 10^5$ |
| $n^2$ | 100 | 10000 | $10^6$ | $10^8$ | $10^{10}$ |
| $n^3$ | 1000 | $10^6$ | $10^9$ | $10^{12}$ | $10^{15}$ |
| $2^n$ | 1024 | $10^{30}$ | $10^{300}$ | $10^{3000}$ | $10^{30000}$ |

1 billion steps/sec

$10^{16}$ ~~year~~ steps a year

$10^{20}$ steps 10000 years

~~MAT~~ CSC165H1 Mar 9th Rui Qiu

invariant becomes

$\exists k \in N, A[k] = x$

$\wedge \quad \forall j \in N, j < i \Rightarrow A[j] \le x$

algorithm

return $f(n)$ — on input of size $n$

messy → complicated formula.

try to estimate / approximate by $g(n)$

"nice" simple formula

- we want a $g(n)$ to estimate an upperbound of $f(n)$, to within? a ~~consta~~ constant factor for all $n$ after some breakpoint values.
- want a constant $c$, breakpoint $B$, st. $f(n) \le g(n)$ for all $n \ge B$

consider $f, g : N \to R^{\ge 0}$

input runtime

def$^n$: $f(n)$ is $O(g(n))$ if there exists positive constants $C$ and $B$ s.t. $f(n) \le g(n)$ for all $n \ge B$

to within a constant factor, $f(n)$ grows no faster than $g(n)$

Ex:

```
def silly(num)
    num = num · / 561.3
    num = num * 2
    print "num is", num
if __name__ == "__main__"
    n = int (raw_input('Number?'))
    silly (n)
```

no while loop

runtime will be constant independing of input

we say runtime is $O(1)$

constant runtime

$t(n) \le C \cdot 1$ for some constant

Ex:

```
i = 100
while i < n
    sum += 1
    i += 1
```

How does runtime change as $n$ changes

loop body : 2 status → 2 steps

loop condition 1 step

total runtime : $t(n) = 1 + 3(n+100) + 1$

$= 3n + 302 \le 4n$ for $n \ge 500$

There is a $C$ (here $C = 4$) and a breakpoint $B$ ($B = 500$ works), s.t. $t(n) \le cn$ so $t(n)$ is $O(n)$

Ex: $i=1$

```
while i<=n/2
  j=1
  while j<=m*n
    sum += 1
    j += 1
  i += 1
```

How does runtime change

each iterator of inner loop takes constant time $O(i)$

outer loop formula $\lfloor n/2 \rfloor$ times

the # of steps is $C \lfloor n/2 \rfloor n^2$

this is $O(n^3)$ sin $\lfloor \ \rfloor$ only affects constant

CSC165H1S March 12th Rui Qiu

for $f, g\ N \to \mathbb{R}^{\geq 0}$,
$f(n)$ is $O(g(n))$
if $\exists$ positive constants $C$ and $B$ such that
$f(n) \leq C g(n)$
for all $n \geq B$

up to a constant factor, $f(n)$ grows no faster than $g(n)$

last time:
$t(n) = 3n^2 + 3\lfloor n/2 \rfloor + 5$ (run time for given algorithm)
intuition: $\underset{f(n)}{t(n)}$ is $O(\underset{g(n)}{n^2})$
prove it.
by defn of $O$ need to prove
$\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow 3n^2 + 3\lfloor n/2 \rfloor + 5 \leq cn^2$

Structure let $C_0 =$
Let $B_0 =$
Assume $n \in \mathbb{N}$
Assume $n \geq B$
⋮
Then $3n^2 + 3\lfloor n/2 \rfloor + 5 \leq cn^2$

Proof: Let $C_0 = 4$
Then $C_0 \in \mathbb{R}^+$
Let $B_0 = 4$
Then $B_0 \in \mathbb{N}$
Assume $n \in \mathbb{N}$
Assume $n \geq B_0$
Then $n^2 \geq B_0^2$ # since $n^2$ monotone incr
$= 16$
Then $\frac{1}{2}n^2 \geq 5$
Then $n \cdot \frac{n}{2} \geq n \lfloor \frac{n}{2} \rfloor \geq 3 \lfloor \frac{n}{2} \rfloor$ # $n \geq 4$
Then $n^2 \geq 3\lfloor \frac{n}{2} \rfloor + 5$
Then $3n^2 + n^2 \geq 3n^2 + 3\lfloor \frac{n}{2} \rfloor + 5$ # add $3n^2$ to both sides
Then $t(n) \leq 4n^2 = C_0 n^2$

Then $n \geq B_0 \Rightarrow t(n) \leq C_0 n^2$

Then $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow t(n) \leq C_0 n^2$

~~Then~~

Then $\exists C \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B_0 \Rightarrow t(n) \leq C_0 n^2$

Then $t(n)$ is $O(n^2)$

<u>example</u>

```
sum = 0
i = 1
while (i <= n):
    j = 1
    while (j <= i):
        sum = sum + 1
        j = j + 1
    i = i + 1
```

intuitive analysis

- each iteration of innermost loop takes $O(1)$ time
  ↳ constant
- on the ith iteration of the outer loop (know $i \leq n$) $i$ iterations of the inner loop are $\leq n$ performed
- each iteration of outer loop takes $O(n)$ time.
- the outer loop body executed $n$ times
- the overall runtime is $O(n^2)$ time
- looks like an overestimate, since e.g. $i = 4$, inner loop executed 4 x's not $n$ times.

| $i$ | #executions of inner loop | previous argument |
|---|---|---|
| 1 | 1 | $n$ |
| 2 | 2 | $n$ |
| 3 | 3 | $n$ |
| ⋮ | ⋮ | ⋮ |
| $n$ | $n$ | $n$ |
| total: $\frac{1}{2}n^2 + \frac{1}{2}n$ | $\frac{1}{2}n^2 + \frac{n}{2}$ | $n^2$ |

To show $f(n)$ is not $O(g(n))$ — use ~~proof~~ proof by contradiction to disprove.

but $\frac{1}{2}n^2 + \frac{1}{2}n$ is $O(n^2)$

So we end up <u>with</u> same answer in terms of $O$ ~~neither~~ notation (runtime is $O(n^2)$)

- only need the $\frac{1}{2}$ when <u>comparing</u> ~~a~~ runtime with <u>another</u> $O(n^2)$ algorithm.

2 key properties of $O$ notation

- constant factors disappear
  if $d>0$ is a constant
  then $d f(n)$ is $O(f(n))$
  and $f(n)$ is $O(d f(n))$
- low order terms disappear
  e.g. $n^5+n^3+6n^2$ is $O(n^5)$
  $n^2+n\log n$ is $O(n^2)$
  in general, if $n$ goes to $\infty$

$$\lim_{n\to\infty} \frac{h(n)}{f(n)} = 0$$

then $f(n)+h(n)$ is $O(f(n))$

---

following observations

$$\left.\begin{array}{l} 6n \text{ is } O(n) \\ 42n \text{ is } O(n) \\ 165n+2012 \text{ is } O(n) \end{array}\right\} \to O(n) \text{ describes a set of functions}$$

$O(n) = \cancel{g: \mathbb{N} \to \mathbb{R}^{\geq 0}}$
$\{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \leq cn\}$

$6n$ is not $O(\log n)$
$6n$ is not $O(\sqrt{n})$
$6n$ is not $O(165)$

rely on <u>def$^n$</u>

if $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N},$
$\forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \leq cn$
then $\exists \bar{c} \in \mathbb{R}^+, \exists \bar{B} \in \mathbb{N}$
$\forall n \in \mathbb{N}, n \geq \bar{B} \Rightarrow d\,g(n) \leq \bar{c} n$
for $d>0$

CSC165H1S March ~~蕃~~19th Rui Qiu

Suppose $P(n)$ is a predicate for $n \in N$, and also know:

$P(0) \wedge (\forall n \in N, P(n) \Rightarrow P(n+1))$

You know $P(0)$ is true.

$P(1)$ ~~is~~ true # $P(0) \wedge P(0) \Rightarrow P(1)$

$P(2)$ true # $P(1) \wedge P(1) \Rightarrow P(2)$

Then $\forall n \in N, P(n)$ true

Argument called 'Principle of Simple induction'

Prove for $n \in N$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

proved by induction

Let $P(n)$: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Prove $\forall n \in N$, $P(n)$

Prove $\forall n \in N, P(n)$

① prove $P(1)$

Let $n_0 = 0$

Then $\sum_{i=0}^{n_0} i = \sum_{i=0}^{0} i = 0$

Then $\frac{n_0(n_0+1)}{2} = \frac{0 \times 1}{2} = 0$

Then $\sum_{i=0}^{n_0} i = \frac{n_0(n_0+1)}{2}$

Then $P(n_0)$

Then $P(0)$

② prove $\forall n \in N, P(n) \Rightarrow P(n+1)$

proof: Assume $n \in N$.

Assume $P(n)$

Then $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Then $\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$

Then $P(n+1)$

Then $P(n) \Rightarrow P(n+1)$

Then $\forall n \in N, P(n) \Rightarrow P(n+1)$

Then $P(0) \wedge P(n) \Rightarrow P(n+1)$

Then by the principle of simple induction, $\forall n \in N, P(n)$

Consider $P(n)$: $2^n \geq 2n$

① prove $P(0)$:

Let $n_0 = 0$

Then $2^{n_0} = 2^0 = 1$

Then $2n_0 = 0$

Then $2^{n_0} \geq 2n_0$

Then $P(n_0)$

Then $P(0)$

② prove $\forall n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$

Assume $n \in \mathbb{N}$.

Assume $P(n)$

Then $2^n \geq 2n$ # by assumption

Case 1: Assume $n > 0$

Then $2(n+1) = 2n + 2 \leq 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ # $n > 0$

Then $P(n+1)$

Case 2: Assume $n = 0$

Then $2(n+1) = 2(0+1) = 2$

Then $2^{n+1} = 2$

Then $2^{n+1} \geq 2(n+1)$

Then $P(n+1)$

Then in either case, $P(n+1)$

Then $P(n) \Rightarrow P(n+1)$

Then $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

Then $P(0) \wedge P(n) \Rightarrow P(n+1)$

Then by the principle of simple induction, $\forall n \in \mathbb{N}, P(n)$

Consider $P(n)$ $2^n \geq n^3$

| observation: | $2^n$ | $n^3$ |
|---|---|---|
| $n=0$ | $1 \geq 0$ | $P(0)$ ✓ |
| $n=1$ | $2 \geq 1$ | $P(1)$ ✓ |
| $n=2$ | $4 < 8$ | $\neg P(2)$ X |
| $n=3$ | $8 < 27$ | $\neg P(3)$ X |
| ⋮ | | |
| $n=9$ | $512 < 729$ | $\neg P(9)$ X |

$n=10$ $\quad 1024 \geq 1000$ $\quad P(10)$ ✓

$n=11$ $\quad 2048 \geq 1331$ $\quad P(11)$ ✓

What statement $P(n)$ is true

$\forall n \in N, \exists B \in N, n \geq B \Rightarrow 2^n \geq n^3$

$\forall n \in N, n \geq 10 \Rightarrow P(n)$

How to prove? $P(10) \wedge \forall n \in N, n \geq 10 \Rightarrow (P(n) \Rightarrow P(n+1))$

$\forall n \in N \{0,1,2,\cdots,8,9\}, P(n)$

Alt define $Q(n) : 2^{n+10} \geq (n+10)^3$

prove : $\forall n \in N, Q(n)$

prove $Q(0) \wedge (\forall n \in N, Q(n) \Rightarrow Q(n+1))$

CSC165H1S March 21st Rui Qiu

Properties of $O, \Omega, \Theta$

① $O$ is transitive

$a<b \wedge b<c$ then $a<c$

For all functions $f, g, h$ $\mathbb{N} \to \mathbb{R}^{\geq 0}$

$f \in O(g) \wedge g \in O(h) \Rightarrow f \in O(h)$

Proof: Assume $f, g, h$ $\mathbb{N} \to \mathbb{R}^{\geq 0}$

Assume $f \in O(g) \wedge g \in O(h)$

Then $f \in O(g)$

Then $g \in O(h)$

$\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow f(n) \leq c g(n)$

Let $c_0 \in \mathbb{R}^+$, and $B_0 \in \mathbb{N}$, be s.t. $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow f(n) \leq c_0 g(n)$

$\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \leq c h(n)$

Let $c_1 \in \mathbb{R}^+$, and $B_1 \in \mathbb{N}$, be s.t. $\forall n \in \mathbb{N}, n \geq B_1 \Rightarrow g(n) \leq c_1 h(n)$

# need to prove $f \in O(h)$

~~Then $f \in O(h)$~~

~~Then $f \in O(g)$~~

Let $c_2 = \underline{c_0 c_1}$ and $B_2 = \underline{\max(B_0, B_1)}$

Then $c_2 \in \mathbb{R}^+$ and $B_2 \in \mathbb{N}$

Assume $n \in \mathbb{N}$ and $n \geq B_2$

Then $n \geq B_1$

Then $g(n) \leq c_1 h(n)$

Then $n \geq B_0$

Then $f(n) \leq c_0 g(n)$
$\leq c_0 c_1 h(n)$
$= c_2 h(n)$

then $f(n) \leq c_2 h(n)$

Then $\forall n \in \mathbb{N}, n \geq B_2 \Rightarrow f(n) \leq c_2 h(n)$

Then $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow f(n) \leq c h(n)$

Then $f \in O(h)$

Then $f \in O(g) \wedge g \in O(h) \Rightarrow f \in O(h)$

Then $\forall f, g, h: \mathbb{N} \to \mathbb{R}^{\geq 0}$, $f \in O(g) \wedge g \in O(h) \Rightarrow f \in O(h)$

② $f \in O(g) \Leftrightarrow g \in \Omega(f)$

for all $f, g$ $\mathbb{N} \to \mathbb{R}^{\geq 0}$

$f \in O(g) \Leftrightarrow g \in \Omega(f)$

Proof: $(\Rightarrow)$

Prove $f \in O(g) \Rightarrow g \in \Omega(f)$

Assume $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$

Assume $f \in O(g)$

Then $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow f(n) \leq c g(n)$

Let $c_0 \in \mathbb{R}^+, B_0 \in \mathbb{N}$, best $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow f(n) \leq c_0 g(n)$

Let $c_1 = \frac{1}{c_0}, B_1 = B_0$

Then $c_1 \in \mathbb{R}^+, B_1 \in \mathbb{N}$

Assume $n \in \mathbb{N}$ and $n \geq B_1$

Then $f(n) \leq c_0 g(n)$

Then $\frac{1}{c_0} f(n) \leq g(n)$

Then $c_1 f(n) \leq g(n)$

Then $\forall n \in \mathbb{N}, n \geq B_1 \Rightarrow c_1 f(n) \leq g(n)$

Then $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow c f(n) \leq g(n)$

Then $g \in \Omega(f)$

Then $f \in O(g) \Rightarrow g \in \Omega(f)$

Then $\forall f, g, \mathbb{N} \to \mathbb{R}^{\geq 0}, f \in O(g) \Rightarrow g \in \Omega(f)$

$(\Leftarrow)$ Similar to above

③ $\forall f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$

$g \in \Theta(f) \Leftrightarrow g \in O(f).$ ~~$\wedge g \in \Omega$~~ $\wedge\, g \in \Omega(f)$

Proof $(\Rightarrow)$

Assume $f, g : \mathbb{N} \to \mathbb{R}^{\geq 0}$

Assume $g \in \Theta(f)$

$\exists c_1 \in \mathbb{R}^+, \exists c_2 \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B$

$\Rightarrow c_2 f(n) \leq g(n) \leq c_1 f(n)$

Let $c_{10} \in \mathbb{R}^+, c_{20} \in \mathbb{R}^+, B_0 \in \mathbb{N}$. best

$\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow c_{20} f(n) \leq g(n) \leq c_{10} f(n)$

- pull out

  $g(n) \leq c_{10} f(n)$

- pull out

  $g(n) \geq c_{20} f(n)$

$\to g \in O(f)$ and $g \in \Omega(f)$

$\Leftarrow g \in O(f) \wedge g \in \Omega(f)$

⋮ --- choose $B_2 = \max(B_0, B_1)$

⋮

$g \in \Theta(f)$

Q to ponder

① $\exists f, g \in \mathbb{N} \to \mathbb{R}^{\geq 0}, f \in O(g) \wedge g \in O(f)$

② $\exists f, g \in \mathbb{N} \to \mathbb{R}^{\geq 0}, f \notin O(g) \wedge g \notin O(f)$

Apply this to algorithms
- program named $P$
- work for inputs $x$ of input size $size(x)=n$

- $t_P(n)$ - run time of $P$ on input $x$ of size $n$

define $T_P(n)$ = worst case run time for algorithm $P$ on input of size $n$.

$= \max\{t_P(x) \mid x \in I \wedge size(x)=n\}$

set of inputs to $p$

Let $U: \mathbb{N} \to \mathbb{R}^{\geq 0}$
be an upper bound on worst case run time

$T_P(n) \in O(U)$

to prove: $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow T_P(n) \leq cU(n)$

$\Leftrightarrow$ ________ " ________ $\max\{t_P(x) \mid x \in I \wedge size(x) = n\}$

⋮

CSC165H1S March 23rd Rui Qiu

Program P

recursion input $x$, $size(x)=n$

not $t_P(x)$ runtime of a program P on input $x$.

$I$ set of all possible inputs to program

$T_P(n)$ = worst case runtime for $p$ or input ~~of~~ if size $n$

$= \max\{t_P(x) \mid x \in I \wedge size(x)=n\}$

$U: N \to R$ (upper bound in worst condition)

How to show $T_P(n) \in O(U(n))$?

$T_P \in O(U) \iff \exists c \in R^+, \exists B \in N, \forall n \in N, n \geq B \Rightarrow T_P(n) \leq U(n)$

$\iff \cdots \Rightarrow$

$\iff \exists \cdots \exists \cdots \forall x \in I, \cdots \geq B \Rightarrow t_P(x)$

$\therefore$ to show $T_P(n) \in O(U(n))$,

need to find $c, B$ & show for an arbitrary input $x$ of size $n$ the program P takes at least $U(n)$ steps.

Insertion Sort

Intuition - $O(n^2)$

- nested loops

- outer loop dependent on $len A = n$ ← size of inputs

- inner loop too

$\Rightarrow O(n^2)$

To derive $T_{IS}(n) \in O(n^2)$ where $n = len(A)$

To prove: $\exists c \in R^+, \exists B \in N, \forall x \in I, size(x)=n \geq B \Rightarrow t_{IS}(x) \leq cn^2$

(proof): Let $c_0 =$ $B_0$

Then $c_0 \in R^+$ and $B_0 \in N$

Assume input $x$ is an array of length $n \geq B_0$

Then from inner loop we know:

$j > 0$ and $j \leq i < len(A) = n$

(i.e. $i \leq j \leq n$)

~~≤~~ condition

So inner loop executes at most $n-1$ times

inner loop has $\underline{3}$ steps per iteration. and $\underline{1}$ step to exit.

line 5-7 take at most $(3n+1)$ steps

outer loop has $5+(3n+1)$ steps per iteration $= 3n+6$ steps

~~lineats~~ line 2-9 are executed at most $(n-1)<n$ times

so total ~~a~~ runtime is $n(3n+6)+1 + 1$ steps

$\uparrow$ exit $\quad \uparrow$ ~~too~~ line 1

So $t_{IS}(n) < 3n^2+6n+2$

$\leq$ ~~con~~ $c_0 n^2$ for $c_0 = \underline{\underline{11}}$ ~~fo~~ and $B_0 = \underline{\underline{1}}$

Then $\exists\, c \in \mathbb{R}^+, \exists\, B \in \mathbb{N}, \ldots$

Then $T_{IS}(n) \in O(n^2)$

What about lower bounds?

$T_{IS}(n)$ ~~≤Ω~~ $\in \Omega(n^2)$ (will ~~a~~ show time)

Then it follows that $T_{IS}(n) \in \Theta(n^2)$

meaning $T_{IS}(n) \in \Omega(L(n))$ $L: \mathbb{N} \Rightarrow \mathbb{R}$

$\Leftrightarrow \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow c\,L(n) \leq T_P(n)$

$\Leftrightarrow \exists \cdots \exists \cdots \forall\ n \geq B \Rightarrow c\,L(n) \leq \max\{t_P(x) \mid x \in I \wedge \text{size}(x) = n\}$

$\Leftrightarrow \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow \exists x \in I, \text{size}(x) = n \wedge c\,L(n) < t_P(x)$

To prove $T_P(n) \Omega(L(n))$

need to find $c$ & $B$, and

constructed an input $x$ of size $n$ for which two can show the programe $P$

takes at least $c\,L(n)$ steps on input $x$.

The worst case runtime comes when ~~first~~ list is in decreasing order $\big|$ $A[i] > A[i+1]$, $i = 0, \ldots, n$

Insertion sort on ~~initialized~~ iteration $i$

$0\ 1\ 2\ \cdots\ i-1\ \ i\ \ i+1$

$t = F[i]$

in unsorted order

~~insertion~~ insert into $F[0]$ to $F[i-1]$ and maintain sort

CSC165 H1S March 26th Rui Qiu

Last time

$T_{IS}(n) \in O(n^2)$

Now

$\boxed{T_{IS}(n) \in \Omega(n^2)}$

Conclusion

$T_{IS}(n) \in \Theta(n^2)$

$T_p(n) \in \Omega(L(n))$ $\quad L: N \to R^{\geq 0}$

$\Leftrightarrow$

$\exists c \in R^+, \exists B \in N, \forall n \in N, n \geq B$

$\Rightarrow \exists x \in I, size(x) = n \wedge c L(n) \leq t_p(x)$

need to construct an input ~~for~~ which program takes at least $cL(n)$ steps.

IS is slowest when given list in reverse order

(every insertion requires max # of shifts)

Claim: $T_{IS}(n) \in \Omega(n^2)$

Let $C_0 =$ ______, and $B_0 =$ ______.

Then $C_0 \in R^+$ and $B_0 \in N$

Assume $n \in N$ and $n \geq B_0$

Let $A_0 = [n-1, n-2, \ldots, 1, 0]$ # $n \geq 1$ to make nonempty.

Then $A_0 \in I$ and $size(A_0) = n$

in ith iteration of outer loop, and in

inner loop $A_0[j-1] > t = A_0[i]$

for j = 1 to i

inner loop executes i times at cost of 3 steps per iteration

and then 1 for exit.

underestimate in lower bound

So a lower bound on cost of inner loop is $2n+1$ steps

outer loop executes from $i=1$ to $n-1$

And so $T_{IS}(n) \geq \underset{i=1}{3} + \underset{i=2}{5} + \cdots + 2(n-1) + 1$ → out loop exit.

$= 3 + 5 + \cdots + 2n - 1$

~~Both~~ But including step in ~~line~~ line 1

gives $T_{IS}(n) \geq 1 + 3 + 5 + \cdots + 2n - 1$

Sum of first n-1 odds $= n^2$

$$\sum_{i=0}^{n-1} 2i+1$$

$$=\sum_{i=0}^{n-1} 2i + \sum_{i=0}^{n-1} 1$$

$$=2\sum_{i=0}^{n-1} i + \sum_{i=0}^{n-1} 1$$

$$=(n-1)(n-1+1)+n = n^2-n+n = n^2$$

Then $c_0 n^2 \leq T_{IS}(n)$

* Then $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow \exists x \in I,\ size(I)=n \wedge cn^2 \leq T_{IS}(n)$

Then $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow \exists x \in I, size(I)=n \wedge cn^2 \leq T_{IS}(n)$

Then $T_{IS}(n) \in \Omega(n^2)$

(can't construct input for which IS takes $n^3$ steps $\forall n \geq B$.

# Ch6 A TASTE OF Computability Theory

A review of terminology used to describe functions

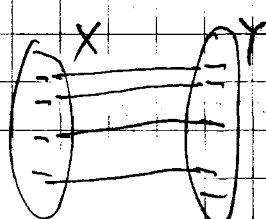
What is a function?

Let $X$ and $Y$ be sets

A function $f$ from $X$ to $Y$

is denoted by $f: X \to Y$

and is a rule that assigns to each element $x \in X$ a unique element $f(x) \in Y$




unique

Symbols: $\forall x \in X, \exists y \in Y$ such that $y=f(x)$

one-to-one

- no 2 x's in X, map to same $y \in Y$

one-to-one

Symbolically: $\forall x \in X, \exists! y \in Y, y=f(x) \wedge \forall x_1 \in X. \forall x_2 \in X, f(x_1)=f(x_2) \Rightarrow x_1=x_2$

(func)

CSC165H1S March 28th Rui Qiu

function $f: X \to Y$

$\forall x \in X, \exists ! y \in Y, y = f(x)$

↳ a unique $y$.

$\forall x \in X, \exists ! y \in Y, y = f(x)$

$\wedge$

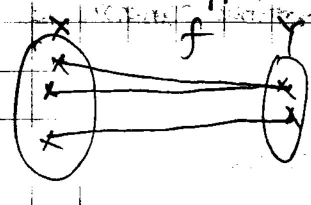
one-to-one

1-1

$\forall x_1 \in X, \forall x_2 \in X, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

A function $f: X \to Y$ is said to be onto iff

$\forall y \in Y, \exists x \in X, f(x) = y$




function

$\forall x \in X, \exists ! y \in Y, y = f(x)$

$\wedge$

$\forall y \in Y, \exists x \in X, f(x) = y$

onto

$f$ is invertible if you can reverse the mapping

$\exists$ a function $f^{-1}: Y \to X$

s.t. $\forall x \in X, f^{-1}(f(x)) = x \wedge \forall y \in Y, f(f^{-1}(y)) = y$

$f$ is invertible iff it is both 1-1 and onto

example: ① $f: \mathbb{N} \to \mathbb{N}$ ② $f(x) = 2x$ ③ $f(x) = \lfloor x/2 \rfloor$ ④ $f(x) = \begin{cases} 10 - x & x \le 10 \\ x & x > 10 \end{cases}$

defined by $f(x) = \lfloor x/2 \rfloor + 2$

| | ① | ② | ③ | ④ |
|---|---|---|---|---|
| is it a function | yes | yes | yes | yes |
| one to one | no $f(0) = 2$, $f(1) = 2$ | yes | no | no |
| ~~one~~ onto | no | ~~yes~~ no since $\neg \exists x \in \mathbb{N}, f(x) = 1$ any odd. | yes $f(2n) = n$ $\forall n \in \mathbb{N}$ | yes $\forall n \in \mathbb{N}, (n \le 10, f(10-n) = n) \wedge (n > 10, f(n) = n)$ |

Since ④ is one-to-one & onto

it is invertible

can show $f$ is its own inverse

$f^{-1}(f(n)) = n$

<u>defn</u>. If there is an invertible function $f: X \to Y$. then we say that $X$ & $Y$ have the same cardinality, and write $|X| = |Y|$ (alt: $\#X = \#Y$)

Let $\mathbb{Z}_n^+$ denote the ~~subject~~ subset of $\mathbb{Z}^+$ consisting of all positive integers $\leq n$

$\mathbb{Z}_0^+ = \phi$, $\mathbb{Z}_1^+ = \{1\}$, $\mathbb{Z}_2^+ = \{1,2\}$, $\mathbb{Z}_n^+ = \{1,2,3,\dots,n\}$

Clearly $|\mathbb{Z}_n^+| = n$

If there is an ~~inva~~ invertible function between a set $X$ and $\mathbb{Z}_n^+$, then $|X| = n$.

- set $X$ is a finite set
- otherwise set is ~~infi~~ infinite

usually describe the function by listing the map

e.g. $X = \{a, 42, \Diamond, !\}$

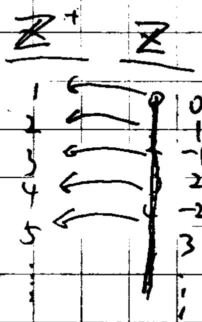
we can list $\mathbb{Z}_4^+$ $X$

and so $|X| = 4$

$1 \longleftrightarrow a$
$2 \longleftrightarrow \Diamond$
$3 \longleftrightarrow 42$
$4 \longleftrightarrow !$

Theorem $|\mathbb{Z}^+| = |\mathbb{Z}|$

~~scr~~ <u>scratch work</u>




What $f: \mathbb{Z}^+ \to \mathbb{Z}$ gives this mapping?

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (1-n)/2 & \text{if } n \text{ is odd} \end{cases}$$

inverse

$$f^{-1}(n) = \begin{cases} 2n & n > 0 \\ 1-2n & n \leq 0 \end{cases}$$

exercise: check

Conclusion:

~~$\#\mathbb{Z}^+$~~

$|\mathbb{Z}^+| = |\mathbb{Z}|$

CSC165H1S March 30th Rui Qiu

Try to find a $g: X \to N$, $f: N \to X$ that is 1-to-1 or onto

elements

| | |
|---|---|
| | 0 |
| $x_0$ | 1 |
| $x_1$ | 2 |
| $x_2$ | 3 |
| $x_3$ | ⋮ |
| ⋮ | |

we can still count the elements in set $X$!

Def'n: A set $X$ is said to be countable iff.
① there is a function $f: \mathbb{N} \to X$ that is onto. or equivalently.
② there is a fun $g: X \to \mathbb{N}$ that is one to one.
Otherwise the set is said to be uncountable.

Claim: $\mathbb{Z}$ is countable.

→ Def'n define $f: \mathbb{N} \to \mathbb{Z}$ by $f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ (1-n)/2 & \text{if } n \text{ odd} \end{cases}$ $* f(n) \geq 0$ $* f(n) < 0$

$m = \frac{1-n}{2} \Rightarrow n = 1-2m$ → onto!

$f(0) = 0$ $f(1) = 0$ → not one-to-one!

Claim: $f: \mathbb{N} \to \mathbb{Z}$ is onto:
$\forall m \in \mathbb{Z}, \exists n \in \mathbb{N}, f(n) = m$

Assume $m \in \mathbb{Z}$
Then $m < 0$ or $m \geq 0$
Case 1 Assume $m < 0$
Let $n_0 = 1 - 2m = 2(m) + 1$
Then $n_0 \in \mathbb{N}$
Then $n_0$ is odd
Then $f(n_0) = \frac{1-n_0}{2} = \frac{1-(1-2m)}{2} = m$
Then $m < 0 \Rightarrow \exists n \in N, f(n) = m$
Case 2 Assume $m \geq 0$
Let $n_0 = 2m$
Then $n_0 \in \mathbb{N}$

Then $n_0$ is even
Then $f(n_0) = \frac{n_0}{2} = \frac{2m}{2} = m$

Then $\exists n \in \mathbb{N}$, $f(n) = m$
Then $m \geq 0 \Rightarrow \exists n \in \mathbb{N}$, $f(n) = m$
Then $\exists n \in \mathbb{N}$, $f(n) = m$.
)

Diagonalization:
The $f$ function is a way to list all the elements in $\mathbb{Z}$.

$f(0), f(1), f(2), f(3). f(4)\ f(5)$ → arguments from $\mathbb{N}$

0 0 1 −1 2 −2 ... → we'll eventually list all elements of

Arguments to show that a set $X$ is countable are often given informally by showing that it is possible to list every element in $X$.
This corresponds to giving $f: \mathbb{N} \to X$ that is onto?

consider the rationals $\mathbb{Q} = \{\frac{n}{d} : n \in \mathbb{Z}, d \in \mathbb{N}^*\}$
consider $\mathbb{Q}^+ = \{\frac{n}{d}, n, d \in \mathbb{N}^+\}$
Claim : $\mathbb{Q}^+$ is countable
Prove by giving informal list argument:
consider sublist 0 : 1/1
sublist 1 : 1/2, 2/1
sublist 2 : 1/3, 2/2, 3/1
3 : 1/4, 2/3, 3/2, 4/1

$\left(\frac{n}{d}\right.$ s.t. $\underline{n+d} = 2$
3
4
$\left.5\right)$

each sublist contains $\frac{n}{d}$ such that $n+d = i$, for $i = 2, 3, 4, \ldots$
The rational $\frac{p}{q}$ appears in position $\underline{\underline{p}}$ in sublist $p+q-2$.
(True for any $p, q \in \mathbb{N}^+$)
Let $f: \mathbb{N} \to \mathbb{Q}^+$ be defined (implicitly) by this listing
Then $f$ is onto because every element of $\mathbb{Q}^+$ will be listed
Then by def'n, $\mathbb{Q}^+$ is countable!

Claim: $\mathbb{Q}$ is countable

Note: $\mathbb{Q} = \mathbb{Q}^+ \cup \{0\} \cup \mathbb{Q}^-$

Let $f: \mathbb{N} \to \mathbb{Q}^+$ be the onto function from previous result

Here is list of all elements in $\mathbb{Q}$: $0, f(0), -f(0), f(1), -f(1), f(2), -f(2)$

$0 \quad 1 \quad -1 \quad \frac{1}{2} \quad -\frac{1}{2} \quad \frac{2}{1} \quad -\frac{2}{1}$

Let $f_1: \mathbb{N} \to \mathbb{Q}$ defined by this listing.

Every elements of $\mathbb{Q}$ will eventually be listed.

Then $f_1$ is onto

Therefore $\mathbb{Q}$ is countable.

CSC165H1 April 2nd Rui Qiu

A set $X$ is countable means

① there is a function $f: \mathbb{N} \to X$ that is <u>onto</u>

or equiv.

② there is a function $g: X \to \mathbb{N}$ that is one-to-one.

- often show set countable by describing a method ~~that~~ is guaranteed to list every element in $X$.
- describe $f(n)$ by saying how to find value in list.

seen for $\mathbb{Q}^+$ — ways to list all elements

- for $\mathbb{Z}$, we ~~does~~ described $f(n)$ and proved onto $\mathbb{Z}$.

- $\mathbb{R}$ — Claim $\mathbb{R}$ is uncountable

countable $\exists f: \mathbb{N} \to X, \forall x \in X, \exists y \in \mathbb{N}, \cancel{f(y) \in}\ f(y) = x$

uncountable $\neg(\qquad) \cancel{\Rightarrow}$

$\forall f: \mathbb{N} \to X, \exists x \in X, \forall y \in \mathbb{N}, f(y) \neq x.$

<u>The real numbers</u>

$r \in \mathbb{R}$

Then $r$ can be expressed as an infinite decimal expansion of form.

$r = m.d_0 d_1 d_2 \ldots$

where $m \in \mathbb{Z}$ and $\forall i \in \mathbb{N}, d_i \in \{0,1,2,3,4,5,6,7,8,9\}$

- for $r$ to have a unique expansion, it cannot end in repeated 9's.

e.g. $1.0\dot{0} = 0.9\dot{9}$

add $\forall i \in \mathbb{N}, d_i = 9 \Rightarrow \exists k \in \mathbb{N}, k > i \wedge d_k \neq 9$

Claim $\mathbb{R}$ is uncountable

~~P~~ Proof technique : proof by contradiction.

Assume $\mathbb{R}$ is countable.

Then $\exists f : \mathbb{N} \to \mathbb{R}$ that is onto.

$\exists f : \mathbb{N} \to \mathbb{R}, \forall x \in \mathbb{R}, \exists y \in \mathbb{N}, f(y) = x$

Let $f_0 : \mathbb{N} \to \mathbb{R}$ be st. $\forall x \in \mathbb{R}, \exists y \in \mathbb{N}, f_0(y) = x$

Then $\forall n \in \mathbb{N}$, $f_0(n)$ is a real number.

Then $f_0(n)$ has an infinite decimal expansion that does not end in repeated 9's.

~~$f_0(k) = i_k . d_0 d_1 d_2$~~

A few function values

$r = f_0(k) = i_k . d_0 d_1 d_2 \cdots d_n$

$\cancel{f_0(0) = i_0 . d_0 d_1 d_2 d_3 \cdots d_n \cdots \in \mathbb{R}}$

$f_0(0) = i_0 . \boxed{d_{00}} d_{01} d_{02} \cdots d_{0n} \cdots \in \mathbb{R}$ $\cancel{f_1(0) = i_1 . d_{11} d_{12} d_{13} \cdots d_{1n} \cdots \in \mathbb{R}}$

$f_0(1) = i_1 . d_{10} \boxed{d_{11}} d_{12} \cdots d_{1n} \cdots \in \mathbb{R}$

$\vdots$

$f_0(2) = i_2 . d_{20} d_{21} \boxed{d_{22}} \cdots d_{2n} \cdots \in \mathbb{R}$ $\cancel{f_2(0) = i_2 . d_{21} d_{22} d_{23} \cdots d_{2n} \cdots \in \mathbb{R}}$

$\vdots$

$f_0(n) = i_n . d_{n0} d_{n1} d_{n2} \cdots \boxed{d_{nn}} \cdots \in \mathbb{R}$ $\cancel{f_n(0) = i_n . d_{n1} d_{n2} d_{n3} \cdots d_{nn} \cdots \in \mathbb{R}}$

(There are an $\infty$ of $f(n)$, $r \neq f(n)$ $\forall n \in \mathbb{N}$, so $f$ not onto)

where $\forall j \in \mathbb{N}$, $i_j \in \mathbb{Z}$ is integer part of $f_0(j)$

and $\forall j \in \mathbb{N}, \forall k \in \mathbb{N}, d_{j,k} \in \{0, 1, \cdots, 9\}$

and no repeating 9's at end.

define $r \in \mathbb{R}$ s.t. $r = 0 . d_0 d_1 d_2 \cdots d_n \cdots$

where $\forall i \in \mathbb{N}, d_i = \begin{cases} 1 & \text{if } d_{i,i} = 0 \\ 0 & \text{if } d_{i,i} \neq 0 \end{cases}$

Since $f_0 : \mathbb{N} \to \mathbb{R}$ is onto, $\exists k \in \mathbb{N}, f_0(k) = r$

$f_0(k) = m_k . d_{k0} . d_{k1} d_{k2} \cdots d_{k0} \cdots$

and $r = 0 . d_0 d_1 d_2 \cdots d_n \cdots$

we have $m_k = 0$ and $\forall i \in \mathbb{N}$,

$d_{k,i} = d_i = \begin{cases} 1 & \text{if } d_{i,i} = 0 \\ 0 & \text{if } d_{i,i} \neq 0 \end{cases}$

in particular, taking $i = k$,

$d_{kk} = d_k = \begin{cases} 1 & \text{if } d_{kk} = 0 \\ 0 & \text{if } d_{kk} \neq 0 \end{cases}$

from which it follows

$d_{k,k} = 0 \Rightarrow d_{k,k} = 1$

$d_{k,k} = 1 \Rightarrow d_{k,k} = 0$

$d_{k,k} = 1 \Leftrightarrow d_{k,k} = 0$

We have a contradiction.

Then our assumption must be false!

Then $\neg$($\mathbb{R}$ is countable)

Then $\mathbb{R}$ is not countable.

Diagonalization Argument

key elements

- construction carried out for arbitrary $f: \mathbb{N} \to \mathbb{R}$
- needed to construct an element $r \in \mathbb{R}$ ← the set under discussion such that $\forall n \in \mathbb{N}$, $f(n) \neq n$.
- then there is no $f: \mathbb{N} \to \mathbb{R}$ that is onto.
- then set is not ~~coo~~ countable.

intuition:

How are $\underbrace{\mathbb{Q}, \cancel{\mathbb{Z}}}$ different from $\mathbb{R}$ ?

I, n, d sign and a number finite # of

Same → all have $\infty$ elements

↑ elements can be described using a finite amount of info.

↑ some elements of $\mathbb{R}$ req an $\infty$ of information

def$^n$ Let $A$ be a set. The power set of $A$, denoted $P(A)$, is the set whose elements are all the subsets of $A$.

$$P(A) = \{X \mid X \subseteq A\}$$

$A = \{5, 12\}$

$P(A) = \{\phi, \{5\}, \{12\}, \{5,12\}\}$

tutorial: $P(\mathbb{N})$

CSC165H1S April 4th Rui Qiu

The Halting Problem

problem write a complete program that assumes the question "will a given program eventually halt or will it go into an infinite loop?"

assume we have written a ~~complete~~ computer function

```
def halt(f, i)          → a valid input to f
    '''Return true iff f(i) will eventually halt.'''
    :  body to be determined.
```

halt must returns True if f(i) will eventually halt. False otherwise.

Assume that a correctly functioning halt function exists.

Prove by contradiction, that this fcn doesn't exist.

Then consider the following:

```
def c(f)
    def halt(f, i):
        :  place statements for halt here

    if halt(f, f):          # line 1
        while True:         # line 2
            pass            # line 3
    else:
        return False        # line 4
```

What is the behaviour of the function call c(c)?

Either c(c) halts or it doesn't halt.

Case 1: Assume c(c) halts.

Then the function call halt(c, c) return True in line 1.

Then c(c) goes into an $\infty$ loop. line 2,3.

Then c(c) halts $\Rightarrow$ c(c) doesn't halt

Case 2: Assume c(c) doesn't halt line 1

Then halt(c, c) returns False

Then c(c) returns false (and $\therefore$ halts) line 4

Then $C(c)$ doesn't halt $\Rightarrow C(c)$ does halt
Then $C(c)$ doesn't halt $\Leftrightarrow C(C)$ does halt
This is a contradiction! (of form $p \Leftrightarrow \neg p$)
Then, by contradiction, halt ~~des~~ does not exist!

The halting problem is an example of a problem that is not computable.

A function ~~$f$~~ $f : A \to B$ is computable
if it can be implemented in a programming language
e.g. $\exists$ a python program, $\forall a \in A \cdot f(a)$ returns the correct value.

Otherwise it is uncomputable.

<u>Exam</u> 3hr
- can bring aid sheet
  - double sided A4
    handwritten
    original — no photocopies.

$\therefore$ exam will <u>not</u> ~~have~~ provide equivalence formula.

Office hours
Starting next week
M–F 2–3pm
(BA 4230)
+ Mon Apr 23 2–4pm.
(avoid ~ Fri Apr 20th / 19th)

<u>Coverage</u>:
Comprehensive
day 1 to today    course notes: to end of section 6.4

$\sim \frac{2}{9}$ Ch1–3

<u>3hr</u>
1hr on material ~~sine~~ since 5.3
$\frac{2hr}{3}$ on Ch1–3, Ch4–5.3, Ch5.4–6.4

$\Rightarrow \sim \frac{2}{9}$ Ch4–5.3
$\sim \frac{5}{9}$ Ch5.4–6.4

1. Find a tight bound on the worst-case running time of the following algorithm.

```
# Precondition: L is a list that contains n > 0 real numbers.
1.  max = 0
2.  for i = 0, 1, ..., n − 1:
3.      for j = i, i + 1, ..., n − 1:
4.          sum = 0
5.          for k = i, i + 1, ..., j:
6.              sum = sum + L[k]
7.          if sum > max:
8.              max = sum
```

$n$ $\leq 2n$ $n$ $\leq 2n^2$ $2n^3$ $\leq 3n^3$ if $n \geq 3$

这三个n都是 worst case 才有的情况.

$2n^3 + 1 \leq 3n^3$

Let $c = 3$ and $B = 3$

Assume $n \in \mathbb{N}$ and $n \geq B = 3$

- The first line takes $1 < n^3$ steps
- The ~~second line~~ loop over $i$ iterates at most $n$ times,
- The loop over $j$ iterates at most $n$ times.
- The loop over $k$ iterates at most $n$ times. for a total of $n$ steps.
- The other statement in the $j$ loop takes 3 steps.

So the loop body for $j$ takes $n+3 \leq 2n$ steps;

so the loop over $j$ takes at most $2n^2$ steps.

So the loop over $i$ takes at most $2n^3$ steps;

The entire algorithm takes at most $2n^3 + n^3 = 3n^3$ steps

$c = 3$

Then $\forall n \in \mathbb{N}, n \geq 3 \Rightarrow T(n) \leq cn^3$.

Then $T(n) \in O(n^3)$.

Assume $n \in \mathbb{N}$ and $n \geq 1$

Then for each value of $i$ in $\{0, \ldots \lfloor n/3 \rfloor\}$

for each value of $j$ in $\{\lfloor 2n/3 \rfloor, \ldots, n-1\}$

$k$ iterates over $\{i, \ldots, j\}$

so the loop for $k$ ~~does~~ has at least $n/3$ steps

$(\lfloor 2n/3 \rfloor - \lfloor n/3 \rfloor \geq n/3)$

...

$T(n) \in \Omega(\frac{n^3}{27})$

$T(n) \in O(n^3) \longrightarrow \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow T(n) \leq cn^3$

$T(n) \in \Omega(n^3) \longrightarrow \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow T(n) \geq cn^3$

$T(n) \in \Theta(n^3)$

Find a tight bound on the worst-case running time

```
# Precondition: L is a list that contains n>0 real numbers.
max = 0
for i = 0, 1, ..., n-1:
    for j = i, i+1, ..., n-1:
        sum = 0
        for k = i, i+1, ..., j:
            sum = sum + L[k]
            if sum > max:
                max = sum
```

Proof Structure:

Let $c' = \cdots$ and $B' = \cdots$

Then $c' \in \mathbb{R}^+$ and $B' \in \mathbb{N}$.

Assume $n \in \mathbb{N}$ and $n \geq B'$ and $L$ is a list of $n$ real numbers.

... show $t(L) \leq c'n^3$ ... ($t(L)$ is the number of steps

2. Prove that $T_{\text{BFT}}(n) \in \Theta(n^2)$, where BFT is the algorithm below.

```
BFT(E, n):
    i = n - 1
    while i > 0:
        P[i] = -1
        Q[i] = -1
        i = i - 1
    P[0] = n
    Q[0] = 0
    t = 0
    h = 0
    while h ≤ t:
        i = 0
        while i < n:
            if E[Q[h]][i] ≠ 0 and P[i] < 0:
                P[i] = Q[h]
                t = t + 1
                Q[t] = i
            i = i + 1
        h = h + 1
```

(Although this is not directly relevant to the question, this algorithm carries out a breadth-first traversal of the graph on $n$ vertices whose adjacency matrix is stored in $E$.)

1. For each equivalence below, either provide a derivation from one side of the equivalence to the other (justify each step of your derivation with a brief explanation — for example, by naming one of the equivalences (see over for a list), or show that the equivalence does not hold (warning: you cannot use a derivation to show non-equivalence — instead, think carefully about what an equivalence means, and how you can disprove it).

(a) $(P \Rightarrow R) \land (Q \Rightarrow R) \iff (P \lor Q) \Rightarrow R$

$(P \Rightarrow R) \land (Q \Rightarrow R)$
$\iff (\neg P \lor R) \land (\neg Q \lor R)$ ~~implication~~
$\iff (R \lor \neg P) \land (R \lor \neg Q)$
$\iff R \lor (\neg P \lor \neg Q)$
$\iff R \lor \neg(P \land Q)$
$\iff \neg(P \land Q) \lor R$
$\iff (P \land Q) \Rightarrow R$

TRUE

P = true
Q = false
R = false

$(P \Rightarrow R) \land (Q \Rightarrow R) \iff (P \lor Q) \Rightarrow R$

$(P \lor Q) \Rightarrow R$
$\iff \neg(P \lor Q) \lor R$ (implication)
$\iff (\neg P \land \neg Q) \lor R$ (Demorgen's)
$\iff (\neg P \lor R) \land (\neg Q \lor R)$ (Distributivity)
$\iff (P \Rightarrow R) \land (Q \Rightarrow R)$ (implication)

(b) $P \Rightarrow (Q \Rightarrow R) \iff (P \Rightarrow Q) \Rightarrow R$

counter-ex:
P: false
Q: false
R: false

FALSE

P: false
Q: true
R: false

TRUE

(c) $P \Rightarrow (Q \Rightarrow R) \iff (P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$

$(P \Rightarrow Q) \Rightarrow (P \Rightarrow R)$
$\iff (\neg P \lor Q) \Rightarrow (\neg P \lor R)$ (implication)
$\iff \neg(\neg P \lor Q) \lor (\neg P \lor R)$ (implication)
$\iff (P \land \neg Q) \lor (\neg P \lor R)$ (DeMorgan's)
$\iff ((P \land \neg Q) \lor \neg P) \lor R$ (associativity)
$\iff ((P \lor \neg P) \land (\neg Q \lor \neg P)) \lor R$ (distributivity)
$\iff (\neg P \lor \neg Q) \lor R$ (Identity)
(commutivity)
$\iff \neg P \lor (\neg Q \lor R)$
$\iff \neg P \lor (Q \Rightarrow R)$
$\iff P \Rightarrow (Q \Rightarrow R)$

**Standard Equivalences** (where $P$, $Q$, $P(x)$, $Q(x)$, *etc.* are arbitrary sentences)

- *Commutativity*
  $P \wedge Q \iff Q \wedge P$
  $P \vee Q \iff Q \vee P$
  $P \Leftrightarrow Q \iff Q \Leftrightarrow P$
- *Associativity*
  $P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$
  $P \vee (Q \vee R) \iff (P \vee Q) \vee R$
- *Identity*
  $P \wedge (Q \vee \neg Q) \iff P$
  $P \vee (Q \wedge \neg Q) \iff P$
- *Absorption*
  $P \wedge (Q \wedge \neg Q) \iff Q \wedge \neg Q$
  $P \vee (Q \vee \neg Q) \iff Q \vee \neg Q$
- *Idempotency*
  $P \wedge P \iff P$
  $P \vee P \iff P$
- *Double Negation*
  $\neg\neg P \iff P$
- *DeMorgan's Laws*
  $\neg(P \wedge Q) \iff \neg P \vee \neg Q$
  $\neg(P \vee Q) \iff \neg P \wedge \neg Q$
- *Distributivity*
  $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$
  $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$
- *Implication*
  $P \Rightarrow Q \iff \neg P \vee Q$
- *Biconditional*
  $P \Leftrightarrow Q \iff (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
- *Renaming* (where $P(x)$ does not contain variable $y$)
  $\forall x, P(x) \iff \forall y, P(y)$
  $\exists x, P(x) \iff \exists y, P(y)$
- *Quantifier Negation*
  $\neg\forall x, P(x) \iff \exists x, \neg P(x)$
  $\neg\exists x, P(x) \iff \forall x, \neg P(x)$
- *Quantifier Commutativity*
  $\forall x, \forall y, S(x,y) \iff \forall y, \forall x, S(x,y)$
  $\exists x, \exists y, S(x,y) \iff \exists y, \exists x, S(x,y)$
- *Quantifier Distributivity* (where $S$ does not contain variable $x$)
  $S \wedge \forall x, Q(x) \iff \forall x, S \wedge Q(x)$
  $S \vee \forall x, Q(x) \iff \forall x, S \vee Q(x)$
  $S \wedge \exists x, Q(x) \iff \exists x, S \wedge Q(x)$
  $S \vee \exists x, Q(x) \iff \exists x, S \vee Q(x)$

2. An "interpretation" for a logical statement consists of a domain $D$ (any non-empty set of elements) and a meaning for each predicate symbol. For example, $D = \{1, 2\}$ and $P(x)$: "$x > 0$" is an interpretation for the statement $\forall x \in D, P(x)$ (in this case, one that happens to make the statement True). For each statement below, provide one interpretation under which the statement is true and another interpretation under which the statement is false—if either case is not possible, explain why clearly and concisely.

   (a) $\forall x \in D, P(x) \iff \exists y \in D, P(y)$

   $D = \{1,2\}$ and $P(x)$: $x > 0$ TRUE

   ~~D=R and~~

   (b) $\forall x \in D, \exists y \in D, P(x,y) \wedge \forall z \in D, P(z,y) \Rightarrow z = x$

1. Consider the following statement:

   If $m$ and $n$ are odd integers, then $mn$ is an odd integer.

   (a) Express the statement using logical notation.

   ~~($m=2k+1$, $n=2j+1$)~~

   $\forall m,n \in \mathbb{Z},\ m\%2=1, n\%2=1 \Rightarrow m\cdot n\%2=1$

   $\forall m,n\in\mathbb{Z}, (\exists k\in\mathbb{Z}, m=2k+1)\wedge(\exists k\in\mathbb{Z}, n=2k+1) \Rightarrow (\exists k\in\mathbb{Z}, m\cdot n=2k+1)$

   (b) This statement can be proven using a direct proof. Write a detailed proof *structure* for the statement. **Don't write a complete proof** — for now, focus on the proof structure only and leave out *all* of the actual "content".

   Assume $\forall m,n\in\mathbb{Z}, m\%2=1,\ n\%2=1$

   ~~then~~

   ⋮

   then $m\cdot n\%2=1$.

   Then $\forall m,n\in\mathbb{Z}, m\%2=1, n\%2=1$

   $\boxed{\text{Assume}}$ $m,n\in\mathbb{Z}$

   $\boxed{\text{Assume}}$ ($m$ is odd $\wedge$ $n$ is odd)

   ⋮

   $\boxed{\text{Then}}$ $m\cdot n$ is odd.

   $\boxed{\text{Then}}$ ($m$ is odd) $\wedge$ ($n$ is odd) $\Rightarrow$ ($m\cdot n$ is odd)

   $\boxed{\text{Then}}$ $\forall m,n\in\mathbb{Z}$, ($m$ is odd) $\wedge$ ($n$ is odd) $\Rightarrow$ ($m\cdot n$ is odd)

   (c) Now, complete the proof of the statement.

   Proof: Assume $m\%2=1$, $n\%2=1$

   ~~then~~ $m=2k+1$, $k\in\mathbb{Z}$

   $n=2j+1$, $j\in\mathbb{Z}$

   $m\cdot n=(2k+1)(2j+1)$

   $=4kj+2k+2j+1$

   $=2(2kj+k+j)+1$

   then $m\cdot n\%2=1$

   Then $\forall m,n\in\mathbb{Z}$ $m\%2=1, n\%2=1 \Rightarrow m\cdot n\%2=1$ ■

   Proof Part:

   Then ($\exists k\in\mathbb{Z}, m=2k+1$) and ($\exists k\in\mathbb{Z}, n=2k+1$)

   Let $i\in\mathbb{Z}$ s.t. $m=2i+1$

   Let $j\in\mathbb{Z}$, s.t. $n=2j+1$

   Then $m\cdot n=4ij+2i+2j+1$

   $=2(2ij+i+j)+1$

   Then $\exists k\in\mathbb{Z}$, s.t. $mn=2k+1$

TUTORIAL # 4 [redacted] Winter 2012

2. Consider the following statement:

If $m$ and $n$ are integers with $mn$ odd, then $m$ and $n$ are odd.

(a) Express the statement using logical notation.

~~$\forall m,n \in \mathbb{Z}, mn\%2=1 \Rightarrow m\%2=1, n\%2=1$.~~

$\forall m,n\in\mathbb{Z}, (\exists k\in\mathbb{Z}, mn=2k+1) \Rightarrow (\exists k\in\mathbb{Z}, m=2k+1)\wedge(\exists k\in\mathbb{Z}, n=2k+1)$

$\forall m\in\mathbb{Z}, n\in\mathbb{Z}. (\exists k\in\mathbb{Z}, mn=2k+1) \Rightarrow (\exists k\in\mathbb{Z}, m=2k+1)\wedge(\exists k\in\mathbb{Z}, n=2k+1)$

(b) This statement can be proven using an indirect proof. Write a detailed proof *structure* for the statement. **Don't write a complete proof** — for now, focus on the proof structure only and leave out *all* of the actual "content".

Assume $m,n\in\mathbb{Z}$

contrapositive: $\forall m\in\mathbb{Z}, n\in\mathbb{Z}, (\exists k\in\mathbb{Z}, m=2k)\vee(\exists k\in\mathbb{Z}, n=2k) \Rightarrow (\exists k\in\mathbb{Z}, mn=2k)$

~~Assume $\forall m,n\in\mathbb{Z}, mn\%2=1$~~

Assume m is even or n is even

~~Assume $\neg(m\%2=1, n\%2=1) \Leftrightarrow (m\%2 != 1 \vee n\%2 != 1)$~~

WLOG assume m is even

⋮

Then m.n is even

~~then $\neg(\forall m,n\in\mathbb{Z}, mn\%2=1) \Leftrightarrow (\exists m,n\in\mathbb{Z}, mn\%2 != 1)$~~

Then (m is even) $\Rightarrow$ m.n is even

~~then $\neg(\exists m,n\in, mn\%2=1) \Rightarrow \neg(m\%2 != 1 \vee n\%2 != 1)$~~

Then mn is odd $\Rightarrow$ (m is odd) $\wedge$ (n is odd)

Then ...

Then $\forall m\in\mathbb{Z}, \forall n\in\mathbb{Z}$, mn is odd $\Rightarrow$ (m is odd) $\wedge$ (n is odd)

(c) Now, complete the proof of the statement.

Proof. ~~Assume $\forall m,n\in\mathbb{Z}, mn\%2=1$~~

~~Assume $\neg(m\%2=1, n\%2=1) \Leftrightarrow (m\%2 != 1 \vee n\%2 != 1)$~~

Assume $\forall m,n\in\mathbb{Z}$

Assume $\exists k\in\mathbb{Z}, mn=2k+1$

Assume $\neg((\exists k\in\mathbb{Z}, m=2k+1)\wedge(\exists k\in\mathbb{Z}, n=2k+1))$

Then $\exists k\in\mathbb{Z}, m=2k$

Let $i\in\mathbb{Z}$ be such that $m=2i$

Then $m\cdot n = 2i\cdot n = 2(i\cdot n)$

Then $m\cdot n$ is an even #

As in Tutorial 1, suppose that you are given seven different programs $A, C, E, G, I, K, M$, each meant to carry out the same task, where programs $C, G, K, M$ are written in Python and programs $A, E, I$ are written in Java. Let $P$ represent the set of all programs (our "universe" or "domain"), $J$ represent the set of all Java programs, and $T$ represent the set of all *correct* programs.

Recall that in class, we have seen how set notation like "$x \in T$" can be expressed in predicate notation as "$T(x)$", and how this can be used to write different sentences symbolically. Make sure that you understand this correspondence well before answering the following questions.

1. For each English sentence below, give representation(s) of the sentence that use the language of symbolic logic. In this course, we prefer that you use quantifiers over the whole universe (in this case $P$) and then use predicate notation to restrict the domain.

   (a) Some incorrect program is written in Java.

   $\exists x \in J, \neg T(x).$ / $\exists x \in P, J(x) \wedge \cancel{\neg} T(x)$ / $\exists x \in T, J(x)$

   (b) No Java program is correct.

   $\forall x \in J, \neg T(x).$

   $\neg \exists x \in P, J(x) \wedge T(x)$ /

   $\forall x \in P, \neg(J(x) \wedge T(x))$

   $\forall x \in P, \neg J(x) \vee \neg T(x)$

   $J(x) \Rightarrow \neg T(x)$

   (c) Only programs written in Python are incorrect.

   $\forall x \in P, \neg T(x) \Rightarrow \neg J(x)$

   $\forall x \in J, T(x).$

   $\forall x \in T, J(x).$

   (d) The program is correct and is written in Python.

   $\exists x \in P. T(x) \wedge \neg J(x)$

   (e) If some Java program is correct, then all Java programs are correct.

   $(\exists x \in P, J(x) \wedge T(x)) \Rightarrow (\forall x \in P, J(x) \Rightarrow T(x))$ /

   $(\exists x \in J, T(x)) \Rightarrow (\forall x \in J, T(x))$

2. Give a *natural* English sentence that captures the meaning of each symbolic sentence below.

   (a) $\exists x \in P, \neg J(x) \wedge T(x)$

   Some programs written in Python are correct.

   (b) $\forall x \in P, \neg J(x) \wedge T(x)$

   All programs written in python are correct.

   (c) $\neg \forall x \in P, T(x) \Rightarrow J(x)$

   None of correct programs are written in Java.

   (d) $\forall x \in P, \neg J(x) \Leftrightarrow T(x)$

   Only programs written in Python are correct.

   (e) $(\forall x \in P, J(x) \Rightarrow T(x)) \vee (\forall x \in P, J(x) \Rightarrow \neg T(x))$

   All programs written in Java are correct or incorrect.

1. Prove or disprove that the set $S_1 = \{(a, b) : a \in \mathbb{N}, b \in \mathbb{N}\}$ is countable.

Examples of elements in $\mathcal{P}(\mathbb{N})$

- $\{0\}$
- $\{1, 4, 5\}$
- $\{\ \}$
- $\{p \in \mathbb{N}, p \text{ is prime}\}$
- $\{2, 2^2, 2^3, 2^4, \ldots\}$
- $\mathbb{N}$

To prove $S$ is countable,

show $\exists f: \mathbb{N} \to S$, $f$ is onto.

or show $\exists f: S \to \mathbb{N}$, $f$ is one-to-one

| | $b=0$ | $b=1$ | $b=2$ ... |
|---|---|---|---|
| $a=0$ | $(0,0)$ | $(0,1)$ | $(0,2)$ |
| $a=1$ | $(1,0)$ | $(1,1)$ | $(1,2)$ |
| $a=2$ | $(2,0)$ | $(2,1)$ | $(2,2)$ |
| ⋮ | | | |

$\underbrace{(0,0)}_{\text{sublist 0}}$ $\underbrace{(1,0)\ (0,1)}_{\text{sublist 1}}$ $\underbrace{(2,0)\ (1,1)\ (0,2)}_{\text{sublist 2}}$

$f_0 : \mathbb{N} \to S_1$ where

$f(n)$ = the element of $S_1$ at position $n$ in the list above.

Therefore $S_1$ is countable.

$f(a,b) = 2^a 3^b$

why is this one-to-one?

Fundamental theorem of arithmetic states that every natural number has a unique prime factorization.

$f: A \to B$, $f$ is one-to-one iff $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_2 = x_1$

Assume $a_1, b_1, a_2, b_2 \in \mathbb{N}$

Assume $2^{a_1} 3^{b_1} = 2^{a_2} 3^{b_2}$ or $f(a_1, b_1) = f(a_2, b_2)$

By the fundamental theorem, $a_1 = a_2$, $b_1 = b_2$

$\Leftarrow$ Therefore $f$ is one-to-one and $S_1$ is countable.

2. Prove or disprove that the set $S_2 = \mathcal{P}(\mathbb{N})$ is countable.

   Recall that the power set of a set $A$, denoted $\mathcal{P}(A)$, is the set of all subsets of $A$. That is $\mathcal{P}(A) = \{X : X \subseteq A\}$.

Prove that $S_2$ is uncountable by contradiction.

$\forall$ sets, $S$, $|P(S)| > |S|$

$\neg \exists f . P(S) \to S, f$ is one-to-one

Assume $S_2$ is countable

$\exists f : \mathbb{N} \to S_2$ st. $S_2$ is onto.

Let $f_0 : \mathbb{N} \to S_2$. $f_0$ is onto.

Then $\forall D \in S_2\ \exists n \in \mathbb{N},\ D = f_0(n)$ (*)

Let $D_0 = \{m \in \mathbb{N} ; m \notin f(m)\}$ → like $f(2) = \{1, 3, 5\}$ "2 not in the set" $f(4) = \{2, 4, 6\}$ "4 in the set!" not this

Then $D_0 \in S_2$

~~Assume~~ Assume $n \in \mathbb{N}$

Either $n \in f_0(n)$ or $n \notin f_0(n)$

Case $n \in f_0(n)$

$n \notin D_0$ because $n \in f_0(n)$

$D \neq f_0(n)$ because $n \in f_0(n)$, $n \notin D_0$

Case $n \notin f_0(n)$

$n \in D_0$ because $n \notin f_0(n)$

$\therefore$ we know $D_0 \neq f_0(n)$

$\therefore D_0 \neq f_0(n)$ in either case

$\forall n \in \mathbb{N},\ D_0 \neq f_0(n)$ (*)

$\exists D \in S_2, \forall n \in \mathbb{N},\ D_0 \neq f_0(n)$ (**)

$\neg \forall D \in S_2, \exists n \in \mathbb{N},\ D_0 = f_0(n)$ contradiction (*)

Then $S_2$ is uncountable.

Prove or disprove each of the following statements. Write detailed proof structures and justify your work.

1. For all real numbers $r, s$, if $r$ and $s$ are both positive, then $\sqrt{r} + \sqrt{s} \neq \sqrt{r+s}$.

$\forall r \in \mathbb{R}, \forall s \in \mathbb{R}, r > 0 \wedge s > 0 \Rightarrow \sqrt{r} + \sqrt{s} \neq \sqrt{r+s}$

Assume $r, s \in \mathbb{R}$

Assume $r > 0 \wedge r > 0$

$\sqrt{r} + \sqrt{s} = \ ?$

<u>Indirect Proof</u>

Assume $r, s \in \mathbb{R}$

Assume $\sqrt{r} + \sqrt{s} = \sqrt{r+s}$

$(\sqrt{r} + \sqrt{s})^2 = (\sqrt{r+s})^2$

$r + 2\sqrt{rs} + s = r + s$

$2\sqrt{rs} = 0$

Then $r = 0 \vee s = 0$

2 Cases:

① $r = 0$

Then $\neg(r > 0)$

$\neg(r > 0) \vee \neg(s > 0)$

$\neg(r > 0 \wedge s > 0)$

② $s = 0$

Then $\neg(s > 0)$

$\neg(s > 0) \vee \neg(r > 0)$

$\neg(r > 0 \wedge s > 0)$

In either case, $\neg(r > 0 \wedge s > 0)$

$\sqrt{r} + \sqrt{s} = \sqrt{r+s} \Rightarrow \neg(r > 0 \wedge s > 0)$

$(s > 0 \wedge r > 0) \Rightarrow (\sqrt{r} + \sqrt{s} \neq \sqrt{r+s})$

Then $\forall r, s \in \mathbb{R}$, $s > 0 \wedge r > 0 \Rightarrow \sqrt{r} + \sqrt{s} \neq \sqrt{r+s}$

2. For all real numbers $x$ and $y$, $x^4 + x^3y - xy^3 - y^4 = 0$ exactly when $x = \pm y$.

$\forall x,y \in \mathbb{R}.\ x^4+x^3y-xy^3-y^4=0 \iff (x=y \lor x=-y)$

~~$\iff x=\pm y$~~

Assume $x, y \in \mathbb{R}$

~~Assume~~ $x^4+x^3y-xy^3-y^4=0 \iff x=\pm y$

2 Cases: Prove that

① $x^4+x^3y-xy^3-y^4=0 \Rightarrow x=\pm y$

Assume $x^4+x^3y-xy^3-y^4=0$

$x^4-y^4+xy(x^2-y^2)=0$

$(x^2+y^2)(x+y)(x-y)+(x+y)(x-y)xy=0$

$(x^2+y^2+x+y)(x+y)(x-y)=0$

$(x^3-y^3)(x+y)=0$

2 cases:

Ⓐ $x^3-y^3=0$

$x^3=y^3$

$x=y$

then $x=y \lor x=-y$

Ⓑ $x+y=0$

$x=-y$

~~then~~ then $x=y \lor x=-y$

In either case $x=\pm y$

Therefore $x^4+x^3y-xy^3-y^4=0 \Rightarrow x=\pm y$

② $x=\pm y \Rightarrow x^4+x^3y-xy^3-y^4=0$

Assume $x=\pm y$

2 cases

⊖ $x=y$

then $x^4+x^3y-xy^3-y^4 = y^4+y^4-y^4-y^4=0$

⊜ $x=-y$

then $x^4+x^3y-xy^3-y^4 = y^4-y^4+y^4-y^4=0$

in either case, $x^4+x^3y-xy^3-y^4=0$

Therefore $x=\pm y \Rightarrow x^4+x^3y-xy^3-y^4=0$

~~Then $\forall x,y \in \mathbb{R}$~~

Then $x^4+x^3y-xy^3-y^4 \iff x=\pm y$

Then $\forall x,y \in \mathbb{R}$, $x^4+x^3y-xy^3-y^4 \iff x=\pm y$

~~MAT~~CSC165H1S March 14th Rui Qiu
to end of §5.3

$6n$ is $O(n)$
$42n$ is $O(n)$
$42n$ is $O(6n+165)$
usually use a simply described function

$4n$ is $O(n^2)$
prefer $4n$ is $O(n)$
since n's growth ~~tighter~~ to $4n$'s
than $n^2$s growth.

$165$ is $O(n)$
for $C_0=1$, $B_0=165$
$\forall n \in \mathbb{N}, n \geq B_0, 165 \leq C_0 n$
but $n$ is not $O(165)$
$\neg(n \text{ is } O(165))$
$\neg(\exists C \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow n \leq C_0 165)$
equivalent: $\forall C \in \mathbb{R}^+, \forall B \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq B \wedge n > C165$.
Proof: Assume $c \in \mathbb{R}^+$, $B \in \mathbb{N}$
Let $n_0 = \max(B, \lceil c \cdot 165 + 1 \rceil)$
Then $n_0 \in \mathbb{N}$
Then $n_0 \geq B$
Then $n_0 \geq \lceil c165 + 1 \rceil$
$> c165$
Then $\exists n \in \mathbb{N}, n \geq B \wedge n > c \cdot 165$
Then $\forall c \in \mathbb{R}^+, \forall B \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq B \wedge n > c \cdot 165$
Then $n$ is not $O(165)$

def'n: for any function of $f: \mathbb{N} \to \mathbb{R}^{\geq 0}$
Let $O(f(n)) = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \leq c \cdot f(n)\}$

The set of all fns that grow no faster than f(n)

you can show that:
$O(1) \subset O(\log_2 n) \subset O(n) \subset O(n^2) \subset O(n^3) \subset O(2^n) \subset O(3^n) \ldots$

How to show $P \subset Q$?

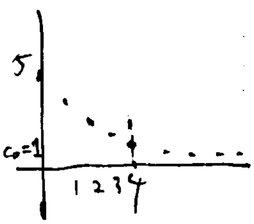
$\forall x \in P, Q(x)$

Ex: $O(5\log n + n^2 + 2n^3/3)$ is $O(n^3)$

$O(12n + n\log n)$ is $O(n \log n)$

$O(12n + n\log n + 2^n + n^2)$ is $O(2^n)$

can apply $O$ to ~~a~~ bound above the growth/decay of any function. $f: \mathbb{N} \to \mathbb{R}^{\geq 0}$




e.g. $f(n) = \frac{5}{n+1}$ $n \in \mathbb{N}$ is $O(1)$

Since $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow \frac{5}{n+1} \leq c \cdot 1$

Proof: Let $C_0 = 1$

Then $C_0 \in \mathbb{R}^+$

Let $B_0 = 4$

Then $B_0 \in \mathbb{N}$

Assume $n \in \mathbb{N}, n \geq B_0$

Then $f(n) = \frac{5}{n+1} \leq \frac{5}{5} = 1 = C_0$

# since $0 < \left|\frac{a}{b}\right| \leq 1$

for $|a| \leq |b|$

and $n+1 \geq 5 \Rightarrow n \geq 4$

Then $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow f(n) \leq C_0 \cdot 1$

Then $\exists C \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow f(n) \leq C_0 \cdot 1$

use $\Omega$ to give lower bounds on the growth of a function

Def'n For any function $f: \mathbb{N} \to \mathbb{R}^{\geq 0}$

Let $\Omega(f(n)) = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \geq c \cdot f(n)\}$

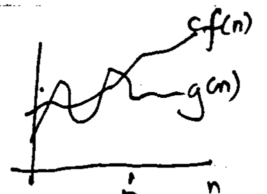
CSC165H1S        Rui Qiu   March 16th

Term test 2   $2^{15}-3^{15}$pm   EX100

up to end of 5.3

the growth of functions

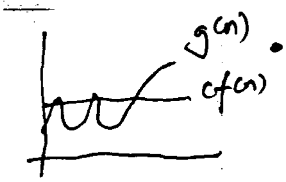
$f: \mathbb{N} \to \mathbb{R}^{\geq 0}$




$O(f) = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \leq cf(n)\}$

Set of fcns that grow no faster than $f$.

think of $O(f)$ as ~~proving~~ providing an upper bound on $g(n)$.




• to get a lower bound on growth of $g(n)$ use $\Omega$

$\Omega(f) = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow g(n) \geq cf(n)\}$

Consider $h: \mathbb{N} \to \mathbb{R}^{\geq 0}$

have proven $h \in O(2^n)$

$h \in \Omega(1)$

$\Theta(f) = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid g \in O(f) \wedge g \in \Omega(f)\} = \{g: \mathbb{N} \to \mathbb{R}^{\geq 0} \mid \exists c_1 \in \mathbb{R}^+, \exists c_2 \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow c_1 f(n) \leq g(n) \leq c_2 f(n)\}$

A more complex example:

Prove that $2n^3 - 5n^4 + 7n^6$ is $O(n^2 - 4n^5 + 6n^8)$

want to prove $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow 2n^3 - 5n^4 + 7n^6 \leq c(n^2 - 4n^5 + 6n^8)$

structure of proof: Let $c_0 = \frac{9}{2}$ Then $c_0 \in \mathbb{R}^+$

Let $B_0 = 0$, Then $B \in \mathbb{N}$

Assume $n \in \mathbb{N}$ and $n \geq B_0$

Then $2n^3 - 5n^4 + 7n^6 \leq \cdots$

$\vdots$

$\leq c_0(n^2 - 4n^5 + 6n^8)$

Then $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow ( \quad ) \leq c( \quad )$
Then $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \ldots$

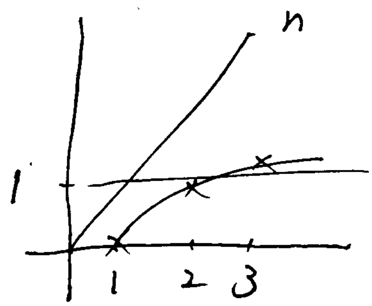
$$2n^3 - 5n^4 + 6n^8 \leq 2n^3 + 7n^6 \quad \text{\# since } -5n^4 \leq 0 \ \forall n \in \mathbb{N}$$
$$\leq 2n^6 + 7n^6 \quad \text{\# since } n^3 \leq n^6, \forall n \in \mathbb{N}$$
$$= 9n^6 \leq 9n^8$$

$$c_0(n^2 - 4n^5 + 6n^8) \geq c_0(-4n^5 + 6n^8) \geq c_0(-4n^8 + 6n^8) \geq c_0 2n^8$$
$$= (\tfrac{9}{2}) 2n^8$$
$$= 9n^8$$

example: consider $f(n) = n$
$h(n) = n \log n$
Claim: $h(n) \in \Omega(f(n))$
$n \log n \in \Omega(n)$

To prove: $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow n \log n \geq cn$

Let $c_0 =$ 1
Then $c_0 \in \mathbb{R}^+$
Let $B_0 =$ 2
Then $B_0 \in \mathbb{N}$
Assume $n \in \mathbb{N}, n \geq B_0$
Then $n \log n \geq \cdot n \cdot$ # for $n \geq 2$
$= 1 \cdot n$
$\geq c_0 n$




Then $\forall n \in \mathbb{N}, n \geq B_0 \Rightarrow n \log n \geq c_0 n$
Then $\exists C \in \mathbb{R}^+ \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow n \log n \geq cn$, then $n \log n \in \Omega(n)$

2012.2.13

1. Write a detailed structured proof that $5n^4 - 3n^2 + 1$ is $\mathcal{O}(6n^5 - 4n^3 + 2n)$.

Def'n of $O(\cdots)$: $\exists c \in \mathbb{R}^+, \exists B \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq B \Rightarrow 5n^4 - 3n^2 + 1 \leq c(6n^5 - 4n^3 + 2n)$

> Scratch work:
>
> $5n^4 - 3n^2 + 1 \leq 5n^4 + 1$
>
> $\leq 5n^4 + n^4$ (if $n \geq 1$)
>
> $\leq 6n^4$
>
> $\leq 6n^5$ (if $n \geq 6$)
>
> $6n^5 - 4n^3 + 2n \geq 6n^5 - 4n^3$
>
> $\geq 6n^5 - 4n^5 = 2n^5$
>
> $\geq n^5$

Proof Structure: Let $c_0 = 1$, then $c_0 \in \mathbb{R}^+$

Let $B_0 = 6$, then $B_0 \in \mathbb{N}$

Assume $n \in \mathbb{N}, n \geq B_0 = 6$

Then $5n^4 - 3n^2 + 1 \leq 5n^4 + 1$

$\leq 5n^4 + n^4$ # since $n \geq 1$

$\leq 6n^4$

$\leq n^5$ # since $n \geq 6$

$\leq 2n^5$

$\leq 6n^5 - 4n^5$

$\leq 6n^5 - 4n^3$

$\leq 6n^5 - 4n^3 + 2n$

Thus $5n^4 - 3n^2 + 1 \leq c_0(6n^5 - 4n^3 + 2n)$ when $n \geq B_0$

Therefore $5n^4 - 3n^2 + 1$ is $O(6n^5 - 4n^3 + 2n)$.

2. Write a detailed structured proof that $6n^5 - 4n^3 + 2n$ is not $\mathcal{O}(5n^4 - 3n^2 + 1)$.

Negation of $\mathcal{O}(\cdots)$: $\forall c \in \mathbb{R}^+, \forall B \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq B \wedge 6n^5 - 4n^3 + 2n > c(5n^4 - 3n^2 + 1)$

Proof Structure: Assume $c \in \mathbb{R}^+, B \in \mathbb{N}$

Let $n_0 = \lceil 3c \rceil + B + 1$ then $n_0 \in \mathbb{N}$

# Then show $n_0 \geq B \wedge (\quad) > c(\quad)$:

---

Then $n_0 = \lceil 3c \rceil + B + 1 \geq B$ # since $c \in \mathbb{R}^+$

Then $n_0 = \lceil 3c \rceil + B + 1 \geq 1$ # since $c \in \mathbb{R}^+$, $B \in \mathbb{N}$

Then $n_0 = \lceil 3c \rceil + 1 + B \geq \lceil 3c \rceil + 1 > 3c$

Then $6n_0^5 - 4n_0^3 + 2n_0 > 6n_0^5 - 4n_0^3$ # since $n_0 \geq 1$

$\geq 6n_0^5 - 4n_0^5$ # since $n_0 \geq 1$

$= 2n_0^5$

$= 2n_0 \cdot n_0^4$

$> 2(3c) \cdot n_0^4$ # since $n_0 > 3c$

$= 6c \cdot n_0^4$

$= c(6n_0^4)$

$= c(5n_0^4 + n_0^4)$

$\geq c(5n_0^4 + 1)$ # since $n_0 \geq 1$

$> c(5n_0^4 - 3n_0^2 + 1)$ # since $n_0 \geq 1$

Thus $n_0 \geq B \wedge 6n_0^5 - 4n_0^3 + 2n_0 > c(5n_0^4 - 3n_0^2 + 1)$

Therefore $\forall c \in \mathbb{R}^+, \forall B \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq B \wedge 6n^5 - 4n^3 + 2n > c(5n^4 - 3n^2 + 1)$

Scratch Work:

$6n^5 - 4n^3 + 2n > 6n^5 - 4n^3$ (if $n \geq 1$)

$\geq 6n^5 - 4n^5$ (if $n \geq 1$)

$= 2n^5$

$5n^4 - 3n^2 + 1 < 5n^4 + 1$ (if $n \geq 1$)

$\leq 5n^4 + n^4$ (if $n \geq 1$)

$= 6n^4$

$6n^5 - 4n^3 + 2n > 2n^5$ if $n \geq 1$

$6n^4 > 5n^4 - 3n^2 + 1$ if $n \geq 1$

$2n^5 > c(6n^4)$

$2n > 6c$

$n > 3c$

$n \geq \lceil 3c \rceil + 1$

$n \geq B$

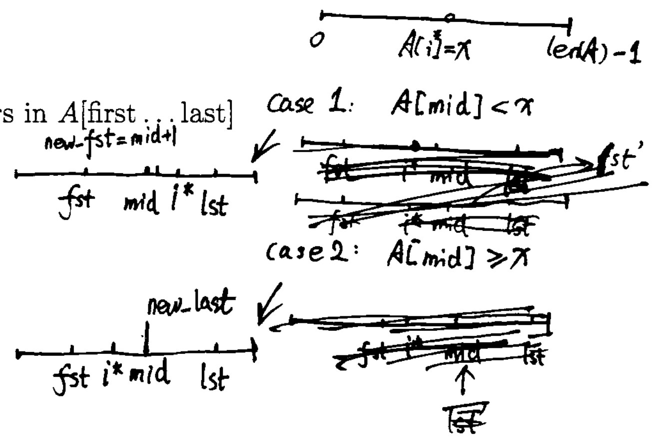
* new condition

$n = \lceil 3c \rceil + 1 + B$

Recall that a **precondition** is a condition that is assumed to be true **before** a set of instructions are executed, a **postcondition** is a condition that is assumed to be true **after** a set of instructions have been executed, and a **loop invariant** is a condition between variables that is always true at the start and at the end of a loop iteration. Another way to say this is that the **loop invariant** is a condition that must be true every time the program evaluates the loop condition.

Now consider the following algorithm (written in pseudo-code, where "=" represents assignment).

```
1 # Precondition: A is a non-empty list of integers (i.e., len(A) > 0) sorted in non-decreasing order
2 #       (i.e., A[0] ⩽ A[1] ⩽ ... ⩽ A[len(A) − 1]) and x is an integer that occurs in A (i.e.,
3 #       ∃i ∈ {0, 1, ..., len(A) − 1}, A[i] = x).
  first = 0
  last = len(A) − 1
1 # Loop Invariant: 0 ⩽ first ⩽ last < len(A) and x occurs in A[first ... last]
2 #       (i.e., ∃i ∈ {first, ..., last}, A[i] = x).
  while first < last:
      midpoint = ⌊(first + last)/2⌋
      if A[midpoint] < x:
          first = midpoint + 1
      else:
          last = midpoint
  index = first
1 # Postcondition: 0 ⩽ index < len(A) and A[index] = x.
```




---

1. Write a detailed argument that shows that the loop invariant holds just before the loop condition is evaluated for the first time, under the assumption that the precondition is true.

1 Assume precondition holds

Then just before the loop condition is evaluated for the first time we know fst = 0, lst = len(A) − 1

lst = len(A) − 1 < len(A)

fst = 0 ≥ 0

Then 0 ≤ fst ≤ lst < len(A)

Then ∃ i ∈ {0, 1, ..., len(A−1)}, A[i] = x

Then ∃ i ∈ {fst, ..., lst}, A[i] = x.

need to show
0 = fst ≤ ... ≤ lst = len(A) − 1
true because len(A) > 0
precondition

2. Assuming that the loop invariant is correct, write a detailed argument that shows that the postcondition will be satisfied once the loop terminates.

2 Assume loop invariant holds

~~Then~~ Assume loop terminates,

Then fst = lst (because fst ≤ last by loop invariant, but fst should not less than last by negation of loop condition)

Then ~~fst~~ idx = fst = lst

Then idx ≥ 0 (fst ≥ 0 by loop invariant)

Then idx < len(A) (lst < len(A) by loop invariant) and fst = lst

Then A[idx] = x (cuz ∃ i ∈ {fst, ~~lst~~ ... lst}, A[i] = x, by loop invariant)

Then 0 ≤ idx < len(A) and A[idx] = x.

3. Write a detailed argument that shows that the loop invariant is correct. That is, show that the loop invariant is true each time the program evaluates the loop condition.

③ Assume precondition holds

Assume loop invariant is true, and the loop carries out at least one more iteration.

Then $fst < lst$

Then $mid = \lfloor (fst + lst)/2 \rfloor > (fst + lst)/2 - 1 > (fst + fst)/2 - 1 = fst - 1$

$mid = \lfloor (fst + lst)/2 \rfloor < \lfloor (lst + lst)/2 \rfloor = lst$

$\Rightarrow fst - 1 < mid < lst$

Case 1: $A[mid] < x$

Then $A[fst] \leq A[fst+1] \leq \cdots \leq A[mid] < x$

$fst' = mid + 1$

$lst' = lst$

Then $0 \leq fst'$ $(0 \leq fst \leq mid < mid+1)$

then $fst' \leq lst$ ( ---) $\Rightarrow fst' \leq lst'$

Then $lst < len(A)$ (by loop invariant) $\Rightarrow$ ~~lst' ≤ len(A)~~ $lst' < len(A)$

Then $\exists i \in \{fst', \ldots, lst'\}, A[i] = x$ (because $\exists i \in \{fst, \ldots, lst\}, A[i] = x$, by loop invariant, $A[fst] \neq x, A[fst+1] \neq x, A[mid] \neq x$)

Then loop invariant is true.

Case 2: $A[mid] \geq x$

4. In order to prove that the algorithm is correct, there is one important property that must be shown (in addition to proving that the loop invariant is correct and that the postcondition holds at the end of the loop). State this property clearly, and then write a detailed argument that it is true.

whether the loop terminates

need to show it can be terminated.

④ check $(lst - fst)$ # it is always decreasing, if it reaches 0, then ~~it~~ the loop terminates.