Recap of last lecture :

- Well ordering principle (WOP) : Every nonempty subset of natural numbers has a smallest element.

- Used WOP to prove :
  - Every natural number > 1 is prime, or can be expressed as product of primes
  - $\nexists\ (a,b,c) \in \mathbb{N}^3$ s.t. $4a^3 + 2b^3 = c^3$.
    - used the following fact : if 2 divides z^3, then 2 divides z. This needs a proof.
  - If a tournament contains a cycle, then it contains a 3 cycle.

- All these proofs had a common template
  - Proof by contradiction
  - Define a non empty subset S of $\mathbb{N}$.
  - By WOP, this set has a minimal element z
  - Show that $\exists$ smaller element $z' \in S$. Hence contradiction.

Recall $\alpha\beta\gamma$ puzzle.

Axiom : $\alpha\beta$

Inference rules : $x\beta \xrightarrow{(1)} x\beta\gamma$ $\qquad$ $x\beta\beta\beta y \xrightarrow{(3)} x\gamma y$

$\alpha x \xrightarrow{(2)} \alpha x x$ $\qquad$ $x\gamma\gamma y \xrightarrow{(4)} xy$

Theorem 4.1 Starting with $\alpha\beta$ and applying inference rules (1) – (4), we cannot derive a string s s.t. (no. of β in s) mod 3 = 0.

Proof: PROOF BY CONTRADICTION.

Suppose, on the contrary, we can derive strings s s.t. (no. of β in s) mod 3 = 0.

Let S be the set of length of such derivations. More formally,

$$S = \left\{ i : \begin{array}{l} \exists \text{ strings } s_1, s_2, \ldots, s_i \\ s_1 = \alpha\beta, \text{ (no. of } \beta \text{ in } s_i) \bmod 3 = 0 \\ \forall j \in \{2, \ldots, i\}, \; s_j \text{ can be derived} \\ \text{from } s_{j-1} \text{ using rules (1) – (4)} \end{array} \right\}$$

By our assumption, S is non-empty, and is subset of $\mathbb{N}$.

By WOP, S has a minimal element, say l.

$l \neq 1$, since all proofs must start with the string $\alpha\beta$, and (no. of β in $\alpha\beta$) mod 3 $\neq$ 0

Claim: If $\ell \in S$ and $\ell > 1$, then $\ell - 1 \in S$.

Proof: Suppose $\ell \in S$, $\ell > 1$. Then $\exists$ sequence $s_1 = \alpha\beta, s_2, \ldots, s_{\ell-1}, s_\ell$ s.t. (no. of β in s_ℓ) mod 3 = 0, and s_j can be derived from s_{j-1} for all $j \in \{2, 3, \ldots, \ell\}$.

s_j is derived from s_{j-1} using one of the four inference rules.

Obs - if rule (1) is used, then (no. of β in $s_{\ell-1}$) mod 3 = 0.

rule (1) only adds γ at the end, therefore no. of β in $s_{\ell-1}$ = no. of β in s_ℓ

Obs - if rule (2) is used, then (no. of β in $s_{\ell-1}$) mod 3 = 0.

using rule (2), if (no. of β in $s_{\ell-1}$) mod 3 = 1, then (no. of β in s_ℓ) mod 3 = 2, and if (no. of β in $s_{\ell-1}$) mod 3 = 2, then (no. of β in s_ℓ) mod 3 = 1. Therefore, if (no. of β in s_ℓ) mod 3 = 0, then (no. of β in $s_{\ell-1}$) mod 3 must be 0.

Obs : if rule (3) is applied, then
(no. of β in $S_{\ell-1}$) mod 3 =
(no. of β in S_ℓ) mod 3 =

Rule (3) removes 3 βs, replaces with γ. Hence no of β mod 3 is preserved.

Obs : if rule (4) is applied, then
(no. of β in $S_{\ell-1}$) mod 3 =
(no. of β in S_ℓ) mod 3 =

Rule (4) removes 2 γs. Hence no of β mod 3 is preserved.

Hence, if $\ell \in S$, then $\ell-1 \in S$.

Using the above claim, we arrive at a contradiction. We assumed that ℓ is the smallest element in S, $\ell > 1$. But we showed that $\ell-1 \in S$.

Questions :

1. If we start with axiom $\alpha\beta\beta$, then Theorem 4.1 does not hold.

You can derive $\alpha\gamma$: $\alpha\beta\beta \xrightarrow{(3)} \alpha\gamma$

Where does the proof break down ?

2. Suppose we start with a stronger version of Thm 4.1 :

Starting with $\alpha\beta$ and applying rules (1) – (4), we cannot derive a string s s.t.

(length of longest consecutive β in s) mod 3 = 0.

Does the above proof still hold ?

3. Suppose we start with axiom $\alpha\beta\beta\gamma\beta$. Can we derive $\alpha\gamma$ using the same set of inference rules ?

LOGIC : Propositional Logic

Def 4.1 Proposition : any stmt that can be assigned T/F.

Examples :

- "5 is a prime number"
- "2 + 2 = 5"

Propositions can be combined using LOGICAL OP. We will use 5 operators : $\neg$ (NOT), $\vee$ (OR), $\wedge$ (AND), $\Rightarrow$ (IMPLIES), $\Leftrightarrow$ (EQUIV)

$\neg P$:

P	$\neg P$
T	F
F	T

$P \vee Q$

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

$P \wedge Q$

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

$P \Rightarrow Q$

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

$P \iff Q$

P	Q	$P \iff Q$
T	T	T
T	F	F
F	T	F
F	F	T

Using these logical operators, we can define Boolean formulae, and we can compute the TRUTH TABLE for any Boolean formula.

Example 1 : $t = \underbrace{(p \Rightarrow q)}_{r} \iff \underbrace{(\neg q \Rightarrow \neg p)}_{s}$

p	q	r	$\neg q$	$\neg p$	s	t
F	F	T	T	T	T	T
F	T	T	F	T	T	T
T	F	F	T	F	F	T
T	T	T	F	F	T	T

t is always true. Therefore, if you have to prove $p \Rightarrow q$, it suffices to prove $(\neg q \Rightarrow \neg p)$. This is a popular proof strategy: PROOF BY CONTRAPOSITION

Example 2: $t = \underbrace{(\neg p \Rightarrow F)}_{r} \Rightarrow p$

p	¬p	r	t
T	F	T	T
F	T	F	T

t is always true, and is also a popular proof strategy:

PROOF BY CONTRADICTION

Example 3: $t = \underbrace{(p \Rightarrow q)}_{r} \Leftrightarrow \underbrace{(\neg p \Rightarrow \neg q)}_{s}$

p	q	r	¬p	¬q	s	t
F	F	T	T	T	T	T
F	T	T	T	F	F	F
T	F	F	F	T	T	F
T	T	T	F	F	T	T

t is not always true. However, this is a common mistake in COL202. If you have to prove $p \Rightarrow q$, it does not suffice to prove $\neg p \Rightarrow \neg q$

Def 4.2 Tautology: a Boolean formula that is always true

Satisfiable: a Boolean formula that is true for some true/false setting of the variables.

Other Tautologies : write truth tables, convince yourself that these are tautologies

- $\Big(p \wedge (p \Rightarrow q)\Big) \Rightarrow q$ ← popular proof strategy. To prove 'q', it suffices to show 'p' and 'p ⇒ q'.
- $\Big(p \wedge (q \vee r)\Big) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
- $(p \vee (q \wedge r)) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
- $\Big((p \Rightarrow q) \wedge (q \Rightarrow r)\Big) \Rightarrow (p \Rightarrow r)$ ← popular proof strategy. To prove 'p ⇒ r', suffices to prove 'p ⇒ q' and 'q ⇒ r'.
- $\neg (p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$
- $\neg (p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$

ALGORITHMS FOR TAUT / SAT :

There exists an algorithm that takes as input a Boolean formula ϕ with n variables, and in $\sim 2^n$ time, can determine if ϕ is tautology or satisfiable.

MILLION DOLLAR QUESTION :

Given a Boolean formula, can we efficiently determine if its a tautology ?
Or determine if its satisfiable ?

PREDICATE LOGIC :

How do we express the following stmt using logic :

" every even number greater than 2 can be expressed as a sum of two primes "

For this, we need predicates like 'Is Prime'.

Def 4.3 : A predicate is a function from a set to $\{T, F\}$.

Examples :

$$Is\,Prime : \mathbb{N} \to \{T, F\}$$

$$Is\,Prime(5) = T, \quad Is\,Prime(4) = F$$

$Is\,Prime(x)$, by itself, is not defined.

$$Is\,Even : \mathbb{N} \to \{T, F\}.$$

New operators : quantifiers

$\forall$: for all

$\exists$: there exists.

Using quantifiers, we can define propositions.

$\forall x : P(x)$

$\exists x : P(x)$

Examples:

$\exists x \in \mathbb{N} : \text{Is Prime}(x)$ T

$\forall x \in \mathbb{N} : \text{Is Prime}(x)$ F

$\forall x \in \mathbb{N} : \text{Is Even}(2 \cdot x + 4)$ T

We can also use the earlier logical operators $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$

LAWS OF PREDICATE LOGIC:

1. $\neg(\forall x \; P(x)) \Leftrightarrow \exists x \; (\neg P(x))$

$\neg(\exists x \; Q(x)) \Leftrightarrow \forall x \; (\neg Q(x))$

2. $\exists x \left(P(x) \vee Q(x)\right) \iff \left(\exists x \; P(x)\right) \vee \left(\exists x \; Q(x)\right)$

$\forall x \left(P(x) \wedge Q(x)\right) \iff \left(\forall x \; P(x)\right) \wedge \left(\forall x \; Q(x)\right)$

NOTE: $\exists x \left(P(x) \wedge Q(x)\right) \not\iff \left(\exists x \; P(x)\right) \wedge \left(\exists x \; Q(x)\right)$

$\forall x \left(P(x) \vee Q(x)\right) \not\iff \left(\forall x \; P(x)\right) \vee \left(\forall x \; Q(x)\right)$

3. $\left(\forall x \; P(x)\right) \vee \left(\forall x \; Q(x)\right) \Rightarrow \forall x \left(P(x) \vee Q(x)\right)$

$\exists x \left(P(x) \wedge Q(x)\right) \Rightarrow \left(\exists x \; P(x)\right) \wedge \left(\exists x \; Q(x)\right)$

The respective converses are not true.

4. $P(a) \Rightarrow \left(\exists x \; P(x)\right)$ PROOF OF EXISTENCE BY EXPLICIT CONST.

'a' is the explicit const.

??

5. $\left(\exists x \; \forall y \; P(x,y)\right) \Rightarrow \left(\forall y \; \exists x \; P(x,y)\right)$

The converse is not true.

$\left(\forall x \; \exists y \; P(x,y)\right)$ does not imply $\left(\exists y \; \forall x \; P(x,y)\right)$

One should be careful when swapping quantifiers.

Summary:

Propositional Logic:

- proposition can be T/F.
- operators $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$. Using these, we can build bigger propositions.
- given a boolean formula, we can write down the truth table to determine if its a tautology, or if its satisfiable.

Using tautologies, we got 'new' proof strategies.

- PROOF BY CONTRAPOSITION
- $(p \wedge (p \Rightarrow q)) \Rightarrow q$
- $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

- Predicate Logic:

Predicate is a fn. from some set S to $\{T, F\}$

Quantifiers: $\forall$ (for all) and $\exists$ (there exists) can be used to define propositions.

Need to be careful when showing / arguing equivalence of propositions involving $\forall$, $\exists$.

- $P(a) \Rightarrow \exists x \; P(x)$
- $\neg(\forall x \; P(x)) \Leftrightarrow \exists x \; \neg P(x)$

  $\neg(\exists x \; P(x)) \Leftrightarrow \forall x \; \neg P(x)$

- $\forall x (P(x) \wedge Q(x)) \Leftrightarrow (\forall x\ P(x)) \wedge (\forall x\ Q(x))$

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

- $(\forall x\ P(x)) \wedge (\forall x\ Q(x)) \Rightarrow \forall x (P(x) \wedge Q(x))$

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

  converses do not hold in general,

- Nested quantifiers

  $(\exists x\ \forall y\ P(x,y)) \Rightarrow (\forall y\ \exists x\ P(x,y))$

  converse does not hold in general.

for example, let $P(x,y) = T$ if $x > y$, where $x, y \in \mathbb{N}$.

$\forall y \in \mathbb{N}$, $\exists x \in \mathbb{N}$ $P(x,y)$: for all y, there exists x s.t. x is greater than y.

However, does there exist an x s.t. for all y, $x > y$?

No, therefore $\exists x \in \mathbb{N}$ $\forall y \in \mathbb{N}$ $P(x,y)$ is not true.

"every even number greater than 2 can be expressed as a sum of two primes"

$$\forall n \in \mathbb{N}: \left[\begin{array}{l} (n > 2 \ \wedge \ \text{Is Even}(n)) \\ \Downarrow \\ (\exists\, p, q \in \mathbb{N} : \text{Is Prime}(p) \wedge \text{Is Prime}(q) \\ \qquad \wedge \ n = p + q \end{array} \right]$$

Is Prime (x) :

$$\forall y \in \{2, 3, \ldots, x-1\}, \ (x \text{ modulo } y \neq 0)$$

remainder when y divides x.