Nested Quantifiers

- can be thought of as nested loops — for each value of the variable bound by the outside quantifier, step through all values of inner quantifier

- order matters!

e.g. $P(x, y) : x + y = 0$; $x, y$ from $IR$

$\forall x \exists y P(x, y) = T$

$\exists y \forall x P(x, y) = F$
Given: \( L(x, y) : \text{“} x \text{ loves } y \text{”} \)

Express the following using quantifiers:

- "Everybody loves somebody": 
  \[ \forall x \exists y \ L(x, y) \]

- "There is someone whom everybody loves": 
  \[ \exists x \forall y \ L(y, x) \]

- "Nobody loves everybody": 
  \[ \neg \exists x \forall y \ L(x, y) \text{ or } \forall x \exists y \neg L(x, y) \]
Negating nested quantifiers:

- rewrite the following so that negations only appear directly in front of predicates

\[ \neg \forall x \forall y \neg P(x, y) \]
\[ \exists x \exists y \neg P(x, y) \]
\[ \neg (\exists x \exists y \neg P(x, y) \land \forall x \forall y (Q(x, y) \lor \neg R(x, y))) \]
\[ \forall x \forall y P(x, y) \lor \exists x \exists y (\neg Q(x, y) \land R(x, y)) \]
Given: \( T(s, c) \): student \( s \) has taken class \( c \)

- domain of \( s \) = all IIT students
- domain of \( c \) = all CS classes

Translate to English:

\[
\exists x (T(Michael, x) \land T(Shannon, x))
\]

"There is a class that both Michael and Shannon have taken."
Given: $T(s, c)$: student $s$ has taken class $c$

- domain of $s = \text{all IIT students}$
- domain of $c = \text{all CS classes}$

Translate to English:

$$\exists x \forall y \ (x \neq \text{Michael} \land (T(\text{Michael}, y) \rightarrow T(x, y)))$$

"There is a student who has taken all the classes Michael has taken."
Given: \( T(s, c) \): student \( s \) has taken class \( c \)

domain of \( s = \) all IIT students

domain of \( c = \) all CS classes

Translate to English:

\[
\exists x \exists y \forall z \left( (x \neq y) \land \left( T(x, z) \leftrightarrow T(y, z) \right) \right)
\]

"There are two separate students that have taken precisely the same classes."
Proofs
What is a proof?

- mathematical reasoning
- deductive reasoning
- valid argument that establishes the truth of a conjecture
- systematic demonstration that if some set of assumptions (hypotheses) are true, then some conclusion must also be true
- proofs may leverage "known facts"—axioms.
There are many techniques we can use to build proofs, but there is no prescribed recipe for how we go about coming up with a proof!

Good analogy: how to solve a jigsaw puzzle?
Rules of inference describe valid transformations of logical statements based on tautologies.

- **Inference**: (noun) a conclusion reached on the basis of evidence and reasoning

- What logical assertions can we make based on some set of premises?

  e.g., assuming propositions $p, p \rightarrow q$ are true, what can we assert?

  $q$ must be true!
Rule of inference syntax:

premise 1, premise 2, \ldots, premise n

if all are true, conclusion must also be true
Rule: Modus Ponens (Latin: "mode that affirms")

\[ (p \rightarrow q) \land p \rightarrow q \]

\[
\begin{array}{c}
p \rightarrow q \\
p \\
\hline 
q \end{array}
\]

e.g., if the AC is on, I will be cold

the AC is on

therefore, I will be cold
Rule: Modus Tollens (Latin: "mode that denies")

\[(p \rightarrow q) \land \neg q \rightarrow \neg p\]

e.g. if the AC is on, I will be cold

I am not cold

therefore, the AC is not on
Rule: Hypothetical Syllogism

Tautology: \((p \rightarrow q) \land (q \rightarrow r) \rightarrow (p \rightarrow r)\)

\[
\begin{array}{c}
p \rightarrow q \\
q \rightarrow r \\
p \rightarrow r
\end{array}
\]

- if I eat candy, I will be wired
- if I am wired, I can't sleep
- therefore, if I eat candy, I can't sleep
Rule: Disjunctive Syllogism

Tautology: \((\neg p \land (p \lor q)) \rightarrow q\)

\[ \begin{align*}
\neg p & \\
p \lor q & \\
q & \\
\end{align*} \]

e.g., I will not take Econ

I will either take Econ or Soc

Therefore, I will take Soc
Rule: Resolution

tautology: \((p\lor q) \land (\neg p \lor r)) \rightarrow (q \lor r)\)

\[
\begin{array}{c}
p \lor q \\
\neg p \\
\hline
\neg p \lor r \\
q \lor r
\end{array}
\]

\[
\begin{align*}
x &< 10 \text{ or } y > 20 \\
x &\geq 10 \text{ or } z < 0 \\
\therefore \quad y &> 20 \text{ or } z < 0
\end{align*}
\]
Rule: Addition

tautology: \( p \rightarrow (p \lor q) \)

\[
\begin{array}{c}
\frac{p}{p \lor q}
\end{array}
\]

2 + 2 = 4

2 + 2 = 4 or I am a rockstar
Rule: Simplification/Decomposition

tautology: \((p \land q) \rightarrow p\)

\[
\begin{array}{c}
p \land q \\
\hline
p \\
q
\end{array}
\]

- useful for "breaking down" compound hypotheses
Rule: Conjunction/Construction

tautology: \( (p \land q) \rightarrow p \land q \)
Remember that we can also replace any logical expression (or part of a compound expression) with an equivalent one.

E.g. using De Morgan's law

\[
\neg(p \lor q \land r) \\
\neg(p \land q) \land r
\]

\[
\neg(p \land q) \land \neg r
\]
We can also introduce known tautologies based on preceding statements.

E.g., using Disjunctive Syllogism tautology \((\neg p \lor (p \lor q)) \rightarrow q\)

\[\neg(\neg a \land b) \land ((\neg a \land b) \lor c)\]

\[\neg(\neg a \land b) \land ((\neg a \land b) \lor c) \rightarrow c\]

\[c\]
A *valid argument* is a sequence of statements, where each statement either:

- is a *premise* (we can state a premise at any time)
- follows from preceding ones based on rules of inference

The last statement is the conclusion — sometimes (but not always!) what we are trying to prove.
E.g., premises \[ \{ \neg p \rightarrow (q \land r), \quad p \rightarrow s, \quad \neg s \} \]

prove: \( q \)

1. \( p \rightarrow s \) (premise)
2. \( \neg s \) (premise)
3. \( \neg p \) (modus tollens)
4. \( \neg p \rightarrow (q \land r) \) (premise)
5. \( q \land r \) (modus ponens)
6. \( q \) (simplification)
E.g., premises \( \left\{ \begin{array}{l} p \land q \\ p \Rightarrow \neg (q \lor r) \\ s \Rightarrow r \end{array} \right. \)

prove: \( \neg s \)

1. \( p \land q \) (premise)
2. \( p \) \( \Rightarrow \) \( q \) (simplification)
3. \( q \) \( \Rightarrow \) \( 0 \)
4. \( p \Rightarrow \neg (q \lor r) \) (premise)
5. \( \neg (q \lor r) \) (modus ponens)
6. \( \neg q \lor \neg r \) (De Morgan's)
7. \( \neg r \) (D\textprime{}o\'i\textquoteright{} syllogism)
8. \( s \Rightarrow r \) (premise)
9. \( \neg s \) (modus tollens)
Rules of inference for quantified statements:

- Universal instantiation (UI):
  \[ \forall x \, P(x) \quad \Rightarrow \quad P(c) \]

- Universal generalization (UG):
  \[ P(c) \text{ for arbitrary } c \quad \Rightarrow \quad \forall x \, P(x) \]

- Existential instantiation (EI):
  \[ \exists x \, P(x) \quad \Rightarrow \quad P(c) \text{ for some } c \]

- Existential generalization (EG):
  \[ P(c) \text{ for some } c \quad \Rightarrow \quad \exists x \, P(x) \]
E.g. premises \[ \begin{align*}
\forall x \, (P(x) &\rightarrow (Q(x) \land S(x))) \\
\forall x \, (P(x) &\land R(x))
\end{align*} \]
prove: \[ \forall x \, (R(x) \land S(x)) \]

1. \( \forall x \, (P(x) \land R(x)) \) (premise)
2. \( P(c) \land R(c) \) (UI)
3. \( P(c) \) (simplification)
4. \( \forall x \, (P(x) \rightarrow (Q(x) \land S(x))) \) (premise)
5. \( P(c) \rightarrow (Q(c) \land S(c)) \) (UI)
6. \( Q(c) \land S(c) \) (MP)
7. \( S(c) \) (simpl.)
8. \( R(c) \) (simpl.)
9. \( R(c) \land S(c) \) (conj.)
10. \( \forall x \, (R(x) \land S(x)) \) (UG)
Note: mathematical theorems are often stated using free variables in its hypotheses and conclusion, and universal quantification over these free variables is implied.

E.g., conjecture: if $u > 4$ then $2^n > n^2$

\[ P(n) \quad Q(n) \]

i.e., $P(n) \rightarrow Q(n)$ for arbitrary $n$

universal generalization:

we want to prove $\forall n (P(n) \rightarrow Q(n))$

"form" of proof goal: $p \rightarrow q$
Methods of Proof of form $p \rightarrow q$

1. Trivial proof: $q$ known to be true
   
e.g., "if it is raining then $1+2=3"$

2. Vacuous proof: $p$ known to be false
   
e.g., "if $2 > 3$ then Elon Musk is a genius"
Methods of Proof of form $p \rightarrow q$

3. Direct proof: assume $p$; prove $q$
   - use axioms, rules of inference, equivalences

4. Indirect proof
   a) proof of the contrapositive (recall $p \rightarrow q \equiv \neg q \rightarrow \neg p$)
      - assume $\neg q$; prove $\neg p$
   b) proof by contradiction
      - assume $p \land \neg q$; derive a contradiction (e.g., $\bot$)
Methods of Proof of other forms

5. proof of biconditional \( p \iff q \)
   - prove \( p \to q \) and \( q \to p \)

6. proof of conjunction \( p \land q \)
   - prove \( p \) and \( q \) separately

7. if hypothesis is a disjunction, e.g., \( (p \lor p_2 \lor \ldots \lor p_k) \to q \)
   - use equivalence \( (p \lor q) \to r \equiv (p \to r) \land (q \to r) \)
   - \( (p_1 \lor p_2 \lor \ldots \lor p_k) \to q \equiv (p_1 \to q) \land (p_2 \to q) \land \ldots \land (p_k \to q) \)
   - prove each case separately
Methods of Proof involving quantifiers

8. proof of form $\forall x P(x)$
   - show $P(c)$ for arbitrary $c$

9. proof of form $\neg \forall x P(x) \equiv \exists x \neg P(x)$
   - find a counterexample $c$ where $\neg P(c)$

9. proof of form $\exists x P(x)$ — "existence proof"
   - "constructive" proof: find $c$ where $P(c)$
   - "nonconstructive" proof: assume no $c$ exists where $P(c)$; derive a contradiction.
Many others:

- mathematical induction
- structural induction
- cantor diagonalization
- combinatorial proofs
- etc.