COT3100
Module 1

Ian Zou

September 23, 2025

1.4 - Predicates and Quantifiers

Definition 1.4.1. *(Predicate Logic)*

The statement $x > 3$ (or "x is greater than 3") has two parts:

1. *Subject*: the variable x

2. *Predicate*: "is greater than 3"

The **predicate** refers to a property that the *subject* can have.

Definition 1.4.2. *(Propositional Function)*

A **propositional function** is a statement containing variables that become a proposition when each of the variables are assigned a value or bound by a quantifier.

Example.

$P(x)$ can be denoted as " x is greater than 3."

$P(x)$ is a *propositional function*. We can evaluate P at a given x (for example $P(2)$) by plugging in the value for x. Since the proposition $2 > 3$ is false, $P(2)$ is false.

Definition 1.4.3. *(Preconditions)*

A **precondition** is a statement that is used to describe valid input.

Definition 1.4.4. *(Postconditions)*

A **postcondition** is a statement that used to describe the output that should satisfy when the program has run.

Definition 1.4.5. *(Quantifiers)*

Quantifiers		
Statement	**True**	**False**
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

The **universal quantifier** ($\forall$) and **existential quantifier** ($\exists$) have *higher precedence* than all other logical operators in propositional calculus.

Definition 1.4.6. *(Quantifiers Over Finite Domains)*

When the domain of a quantifier is finite, quantified statements can be expressed using propositional logic.

Example.

What is the truth value of $\forall x P(x)$ where $P(x)$ is the statement "$x^2 < 10$" and the domain consists of the positive integers not exceeding 4?

The statement $\forall x P(x)$ is equivalent to $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$. Because $P(4)$, which is the statement "$4^2 < 10$" is false, it follows that $\forall x P(x)$ is false.

Definition 1.4.7. *(Binding Variables)*

When a quantifier is used on the variable x, it is **bound**. Otherwise, it is said to be **free**. All variables that occur in a propositional function must be *bound* to turn it into a proposition.

Definition 1.4.8. *(Scope)*

The **scope** of a quantifier is the part of a logical expression to which it applies. A variable is only *bound* when it exists within the *scope* of a quantifier; it is *free* outside of the *scope*.

Definition 1.4.9. *(Logical Equivalences Involving Quantifiers)*

Statements involving predicates and quantifiers are **logically equivalent** if and only if they have the same truth value no matter which predicates are substitutes and which domain is used for the variables.

Definition 1.4.10. *(De Morgan's Laws)*

De Morgan's Laws for Quantifiers			
Negation	**Equivalent**	**True**	**False**
$\neg\exists x P(x)$	$\forall x\neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x\neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

3

1   1.5 - Nested Quantifiers

Definition 1.5.1. *(Nested Quantifiers)*

A **nested quantifier** is where a quantifier exists within the scope of another quantifier.

Quantifications of Two Variables		
Statement	**True**	**False**
$\forall x \forall y P(x,y)$ $\forall y \forall x P(x,y)$	$P(x,y)$ is true for every pair x, y.	There exists a pair x, y for which $P(x,y)$ is false.
$\forall x \exists y P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is false for every y.
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y.	For every x, there is a y for which $P(x,y)$ is false.
$\exists x \exists y P(x,y)$ $\exists y \exists x P(x,y)$	There exists a pair x, y such that $P(x,y)$ is true.	For every pair x, y, $P(x,y)$ is false.

Corollary.

$$\exists y \forall x P(x,y) \not\equiv \forall x \exists y P(x,y)$$

$\exists y \forall x P(x,y)$: There is a y that makes $P(x,y)$ true for every x.

y is independent of x. If we pick a value of y, but there is an x for which $P(x,y)$ is false, then the statement is false.

$\forall x \exists y P(x,y)$: For every x, there exists a y such that $P(x,y)$ is true.

y is dependent on x. We iterate through x, then see if we can pick a value for y for which $P(x,y)$ is true.

Example. Translate $\forall x(C(x) \lor \exists y(C(y) \land F(x,y)))$ into English.

$C(x)$: x has a computer.
$F(x,y)$: x and y are friends.
The domain of x and y consists of all students in the school.

Translation: "For every student x in the school, they either have a computer, or there exists a student y that has a computer and is friends with student x."

Definition 1.5.2. *(Negation of Nested Quantifiers)*

Statements involving nested quantifiers can be negated by successively applying the rules for negating statements involving a single quantifier.

1.6 - Rules of Inference

Definition 1.6.1. *(Valid Arguments in Propositional Logic)*

An **argument** in propositional logic is a sequence of propositions. All but the final propositions in the argument are called **premises**, and the final proposition is called the **conclusion**.

Let p be "You have a current password", and q be "You can log onto the network." Consider the proposition: "If you have a current password, then you can log onto the network." Then, the **valid argument** has the **argument form**:

$$p$$
$$\underline{p \to q}$$
$$\therefore \quad q$$

This form of argument is **valid** because whenever all premises are true, the conclusion must also be true.

Definition 1.6.2. *(Rules of Inference)*

Rules of inference are valid argument forms that can be used in a *proof* that arguments are valid.

Truth tables can always show an argument is valid, but some propositions are too complicated to use truth tables. That's where *rules of inference* come in handy.

Rules of Inference		
Rule of Inference	**Tautology**	**Name**

p $\underline{p \rightarrow q}$ $\therefore \quad q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	**Modus Ponens**
$\neg q$ $\underline{p \rightarrow q}$ $\therefore \quad \neg p$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	**Modus Tollens**
$p \rightarrow q$ $\underline{q \rightarrow r}$ $\therefore \quad p \rightarrow r$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	**Hypothetical Syllogism**
$p \vee q$ $\underline{\neg p}$ $\therefore \quad q$	$((p \vee q) \wedge \neg p) \rightarrow q$	**Disjunctive Syllogism**

p $\therefore \quad p \vee q$	$p \to (p \vee q)$	**Addition**
$p \wedge q$ $\therefore \quad p$	$(p \wedge q) \to p$	**Simplification**
p q $\therefore \quad p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	**Conjunction**
$p \vee q$ $\neg p \vee r$ $\therefore \quad q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	**Resolution**

Definition 1.6.3. *(Rules of Inference for Quantified Statements)*

Rules of Inference for Quantified Statements	
Rule of Inference	**Name**
$$\frac{\forall x P(x)}{\therefore \ \ q \vee r}$$	**Universal Instantiation**
$$\frac{P(c)}{\therefore \ \ \forall x P(x)}$$	**Universal Generalization**
$$\frac{\exists x P(x)}{\therefore \ \ P(c)}$$	**Existential Instantiation**
$$\frac{P(c)}{\therefore \ \ \exists x P(x)}$$	**Existential Generalization**

1.7 - Proofs

Formal proofs are usually harder to follow and generally not meant for human consumption.

Definition 1.7.1. *(Informal Proofs)*

Informal proofs are designed for human consumption, where more than one rule of inference is used in each step, some steps may be skipped, and axioms being assumed.

Definition 1.7.2. *(Theorem)*

A **theorem** (also referred to as a **fact** or **result**) is a statement that can be shown to be true. It may be the universal quantification of a conditional statement with one or more premises and a conclusion, but it may also be some other type of logical statement.

In mathematical writing, the term *theorem* is usually reserved for a statement that is **considered somewhat important**.

Example.

Many thoerems assert that a property holds for all elements in a domain, which requires a universal quantifier. The standard convention is to omit it. Thus:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$"

is equal to

"For all positive real numbers x and y, then $x^2 > y^2$"

Definition 1.7.3. *(Proposition)*

A **proposition** is a statement that could be true or false. Less important theorems are sometimes called **propositions**.

Definition 1.7.4. *(Proof)*

A **proof** is a valid demonstration that a *theorem* is true.

Definition 1.7.5. *(Axiom)*

A **axiom** (also referred to as **postulates**) are statements we assume to be true. Axioms may be used within proofs.

Definition 1.7.6. *(Lemma)*

A **lemma** is a less important theorem used to prove other theorems.

If an underlying proof is complicated to understand, it may help to demonstrate it by using and proving a series of lemmas.

Definition 1.7.7. *(Corollary)*

A **corollary** is a theorem that can be established directly from a proved theorem.

Definition 1.7.8. *(Conjecture)*

A **conjecture** is a statement that is proposed to be a true statement, usually on the basis of some partial evidence.

When a definitive proof has been found for a conjecture, it becomes a theorem.

Definition 1.7.9. *(Odd/Even)*

The integer n is **even** if there exists an integer k such that $n = 2k$.

The integer n is **odd** if there exists an integer k such that $n = 2k + 1$.

Definition 1.7.10. *(Direct Proof)*

A **direct proof** of $p \rightarrow q$ is constructed by assuming p is true, constructing subsequent steps using rules of inference, and finally showing that q must also be true.

Example.

Give a direct proof of the theorem: "If n is an odd integer, then n^2 is odd."

Note that this theorem states $\forall x P(n) \rightarrow Q(n)$.

The first step is to assume n is odd, and by the definition of an odd integer, $n = 2k + 1$ where k is some integer.

We want to show that n^2 is odd. If we square both sides, we get $n^2 = (2k+1)^2$, which expands to $n^2 = 4k^2 + 4k + 1$.

We can then factor out the 2 in order to get $n^2 = 2(k^2 + 2k) + 1$, which puts the equation into the form of the definition of an odd integer. Thus, n^2 is odd if n is odd.

Definition 1.7.11. *(Proof by Contraposition)*

A **proof by contraposition** of $p \rightarrow q$ is constructed by making use of $p \rightarrow q \equiv -q \rightarrow -p$. We assume $-q$ and use axioms, definitions, previously proven theorems, and rules of inference to show that $-p$.

A good way to tell when a *proof by contraposition* is useful is by analyzing whether the contrapositive is able to be proved easily by a direct proof. In other words, if q is simpler to prove, **use a *proof by contraposition***.

Example.

Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

There is no direct proof to show that $3n + 2 = 2k + 1$, and thus we need to use a *proof by contraposition.*

We start by assuming $-q$, so we assume n is even. By the definition of an even integer, $n = 2k$ for some integer k.

Now, we may substitute n for $2k$, and thus we have $3(2k) + 2$. We can factor out the 2, and get $3n + 2 = 2(3k + 1)$. This is in the form of the definition of an even integer, and thus proves that $3n + 2$ is even.

Because the negation of the conclusion implies that the hypothesis is false, the original conditional statement is true. In order words, by proving the contrapositive, we proved the original statement.

Definition 1.7.12. *(Vacuous Proof)*

A **vacuous proof** proves $p \rightarrow q$ is true based on the fact that p is false, since a conditional statement with a false hypothesis is guaranteed to be true.

Example.

Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$.

$P(0)$ is "If $0 > 1$, then $0^2 > 0$. $0 > 1$ is false. Thus, $P(0)$ is true. The fact that $0^2 > 0$ is false is irrelevant. We are proving $P(0)$ (the if-then claim), not whether the result is true or false.

Definition 1.7.13. *(Trivial Proof)*

A **trivial proof** proves $p \to q$ is true based on the fact that q is true, since a conditional statement with a true conclusion is, well, true.

Example.

Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$. The domain is all nonnegative integers. Show that $P(0)$ is true.

$P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." This is true, since $a^0 = 1$ and $b^0 = 1$, which satisfies $a^0 \geq b^0$. Since the conclusion is true, $P(0)$ is true. It is irrelevant whether the hypothesis is satisfied.

Definition 1.7.14. *(Proof by Contradiction)*

A **proof by contradiction** proves p if we can show that $-p \to (r \wedge -r)$, where r is some proposition. Since $r \wedge -r$ is a contradiction, p must be true if $-p$ implies a contradiction.

Example.

Prove that $\sqrt{2}$ is irrational by giving a proof of contradiction.

Let p be " $\sqrt{2}$ is irrational." We start by stating that $-p$ is true, or $\sqrt{2}$ is rational.

If $\sqrt{2}$ is rational, then there exist integers a and b such that $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and both a and b have no common factors. Here, we are using the fact that every rational number can be written in lowest terms.

We can square both sides and get $2 = \frac{a^2}{b^2}$, and thus $a^2 = 2b^2$.

By the definition of even integers, a^2 is even. Because multiplication is a closed operation, then a must also be even. By the definition of even integers, $a = 2c$ where c is an arbitrary integer.

Thus, we can say that $(2c)^2 = 2b^2$, which expands to $4c^2 = 2b^2$.

If we rearrange the terms, we can get $b^2 = 2c^2$. By the definition of even integers, b^2 is even, which we know means that b is also even. However, because we have shown that both a and b is even, it cannot be that a and b have no common factors, as the common factor between two even integers is 2. Thus, we have a contradiction.

Since if $\sqrt{2}$ is rational, then there is a contradiction, $\sqrt{2}$ must be irrational. Thus, p is true.

Definition 1.7.15. *(Proof of Equivalence)*

A **proof of equivalence** proves $p \leftrightarrow q$ by proving that $p \rightarrow q$ and $q \rightarrow p$ are true.

We can establish any chain of conditional statements as long as it is possible to reach any other conditional statement by working through the chain. We can show that $p1$, $p2$, and $p3$ are equivalent if $p1 \rightarrow p2$, $p2 \rightarrow p3$, and $p3 \rightarrow p1$. This is also equivalent to $p1 \leftrightarrow p2 \leftrightarrow p3$.

1.8 - Proofs

Definition 1.8.1. *(Proof by Cases)*

A **proof by cases** is used when a single argument cannot be used to prove all cases. A hypothesis made of a disjunction of propositions can be proved by proving each of the n conditional statements individually, and it must cover all possible cases that arise in a theorem.

Definition 1.8.2. *(Exhaustive Proof)*

An **exhaustive proof** is a proof that establishes a result by checking all possible cases.

Example.

Prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Since the domain is limited, we can use a *proof of exhaustion* for when $n = 1$, $n = 2$, $n = 3$, and $n = 4$.

Definition 1.8.3. *(Uniqueness Proof)*

Some theorems assert that there is exactly one element with a property exists. We can prove this with an **uniqueness proof**.

Existence: We show that an element x with the desired property exists.
Uniqueness: We show that if x and y both had a desired property, than $x = y$.

Example. Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Note that if $r = -\frac{b}{a}$ is a solution of $ar + b = 0$ because $a(\frac{-b}{a}) + b = 0$ and $-b + b = 0$. Therefore, a solution exists and proves existence.

Then, we suppose that s is a real number such that $as + b = 0$. We can then say that $ar + b = as + b$. If we subtract b on both sides, we get $ar = as$, and if we divide a, we get $r = s$. s matches the desired property of r, and we have proved that $r = s$. Thus, we have proved uniqueness.