Theory of Computation

Unit 1: Logic and Models of Proof

Syedur Rahman
Lecturer, CSE Department
North South University
syedur.rahman@wolfson.oxon.org

Theory of Computation Lecture Notes

Acknowledgements

- These lecture notes contain some material from the following sources:

  [ICM] C. Runciman: *Introduction to Computer Mathematics,* University of York, 2003

  [Rosen] K. Rosen: *Discrete Mathematics and Its Applications,*, 5th Edition, Tata McGraw-Hill, 2002

Some Basic Connectives

A **statement** is a collection of symbols that has a truth value – either false (F) or true (T).

E.g. London is in UK, 1+1=5

Connectives are symbols that are used to form larger statements out of smaller ones.

Some Basic Connectives

A **disjunction** is a compound statement in which two substatements are connected by $\vee$ ('or').

A **conjunction** is a compound statement in which two substatements are connected by $\wedge$ ('and').

The **negation** of statement p is $\neg p$, meaning 'p is not the case'.

The '**implies**' connective $p \Rightarrow q$ can be read as 'if p then q' or 'p guarantees q' or 'p is sufficient for q'.

The '**if and only if**' connective $p \Leftrightarrow q$ reads 'p is both necessary and sufficient for q'.

Propositions

A **proposition** is a statement in which basic substatements are variables each with *F* and *T* as possible values.

Example: p, $\neg p$, $p \wedge q$, $p \vee \neg q$, etc.

Two propositions *x* and *y* are **logically equivalent** ($x \equiv y$) if the final columns of their truth tables are identical, i.e. *x* and *y* have the sae truth value regardless of the values of their variables.

Example: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Connectives and Rules in Propositional Logic

high priority

$\neg$	not
$\wedge$	and
$\vee$	or
$\Rightarrow$	implies
$\Leftrightarrow$	if and only if

low priority

xor	**exclusive or**	$p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$
$\downarrow$	**negated or**	$p \downarrow q \equiv \neg(p \vee q)$
$\uparrow$	**negated and**	$p \uparrow q \equiv \neg(p \wedge q)$
$\Rightarrow$	**implication**	$p \Rightarrow q \equiv \neg p \vee q$
$\Leftrightarrow$	if and only if	$p \Leftrightarrow q \equiv (q \Rightarrow p) \wedge (p \Rightarrow q)$

$$\left.\begin{array}{l} p \vee p \equiv p \\ p \wedge p \equiv p \end{array}\right\} \textit{idempotence}$$

$$\left.\begin{array}{l} (p \vee q) \vee r \equiv p \vee (q \vee r) \\ (p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \end{array}\right\} \textit{associativity}$$

$$\left.\begin{array}{l} p \vee \neg p \equiv T \\ p \wedge \neg p \equiv F \end{array}\right\} \textit{excluded middle}$$

$$\left.\begin{array}{l} p \vee q \equiv q \vee p \\ p \wedge q \equiv q \wedge p \end{array}\right\} \textit{commutativity}$$

$$\left.\begin{array}{l} p \vee F \equiv p \\ p \wedge T \equiv p \end{array}\right\} \textit{identity}$$

$$\left.\begin{array}{l} p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \\ p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \end{array}\right\} \textit{distributivity}$$

$$\left.\begin{array}{l} p \vee T \equiv T \\ p \wedge F \equiv F \end{array}\right\} \textit{strictness}$$

$$\left.\begin{array}{l} \neg(p \vee q) \equiv (\neg p) \wedge (\neg q) \\ \neg(p \wedge q) \equiv (\neg p) \vee (\neg q) \end{array}\right\} \textit{de Morgan}$$

$$\neg\neg p \equiv p \quad \textit{double negation}$$

$$\left.\begin{array}{l} p \vee (p \wedge q) \equiv p \\ p \wedge (p \vee q) \equiv p \end{array}\right\} \textit{absorption}$$

From [ICM]

Arguments

An **argument** is an assertion of the form $P_1, P_2 \ldots P_n \vdash Q$, where propositions $P_1, P_2 \ldots P_n$ are its premises and proposition Q is its conclusion.

An argument is **valid** if whenever its premises are true, its conclusion is alse; otherwise the argument is **fallacious**.

Modus ponens *is the argument* $p, p \Rightarrow q \vdash q$.
Modus tollens *is the argument* $p \Rightarrow q, \neg q \vdash \neg p$.
reductio ad absurdum *is the argument* $p \Rightarrow q, p \Rightarrow \neg q \vdash \neg p$

From [ICM]

Predicate Logic

A **predicate** is a proposition $p(v_1, v_2, \ldots v_n)$ depending on variables $v_1, v_2, \ldots v_n$. Given a value for each v_i, p defines a statement that is true or false.

Examples:

- *even*(*x*) ≡ '*x* is an even number'
- *divides*(*x*,*y*) or its short form *x*|*y* ≡ '*x* divides *y*'
- *age(s,x)* ≡ '*s* is *x* years old'
- *adult*(*s*) ≡ '*s* is at least 18 years old'

Quantifiers

∃ **Existential quantifier**: A formula $\exists x,p(x)$ reads 'there exists a value of x such that $p(x)$ is true'. Examples:

$\exists$x, *horse*(x) reads 'there is a horse'

$\exists$x,(*horse*(x) $\wedge$ *colour*(x)=*black*) reads 'there is a horse which is black'

∀ **Universal quantifier**: A formula $\forall x,p(x)$ reads 'for all values of x, $p(x)$ is true'. Example:

$\forall x,$(*horse*(x) $\Rightarrow$ *quadruped*(x)) reads 'if x is a horse then it is a quadruped' or in other words 'all horses are quadrupeds'

Another Example

Remember the example:

age(s,x) ≡ *'s* is *x* years old'

adult(*s*) ≡ *'s* is at least 18 years old'

How do we define *adult*(*s*) using logic?

adult(*s*) ≡ *s* has an age $x \wedge x \geq 18$

adult(*s*) ≡ $\exists x,(age(s,x) \wedge x \geq 18)$

Quantifiers and De Morgan

De Morgan's law extends over quantifiers:

$$\exists x, \neg p(x) \equiv \neg(\forall x, p(x))$$
$$\forall x, \neg p(x) \equiv \neg(\exists x, p(x))$$

Example:

$\neg(\exists x, unicorn(x)) \equiv \forall x, \neg unicorn(x)$ ≡ there is no unicorn

Restricting Predicates

Often the range of values for a predicate are restricted:

$\forall x,(p(x) \Rightarrow q(x))$ reads 'for all x of type p, $q(x)$ is true'.
$\exists x,(p(x) \wedge q(x))$ reads 'for some x of type p, $q(x)$ is true'.

Extended De Morgan works for restricted predicates too:

$$\neg(\forall x,(p(x) \Rightarrow q(x))) \equiv \exists x, \neg(p(x) \wedge q(x))$$
$$\neg(\exists x,(p(x) \wedge q(x))) \equiv \forall x, \neg(p(x) \Rightarrow q(x))$$

Commutability

Quantifiers may commutate only in case of similar ones.

Therefore the following are true:

$$\exists x, \exists y, p(x,y) \equiv \exists y, \exists x, p(x,y)$$

$$\forall x, \forall y, p(x,y) \equiv \forall y, \forall x, p(x,y)$$

And the following is NOT true:

$$\forall x, \exists y, p(x,y) \equiv \exists y, \forall x, p(x,y)$$

Witness and Counterexamples

For an existential formula $\exists x,p(x)$ a witness is a value of x for which $p(x)$ is true, thereby proving $\exists x,p(x)$.

For an universal formula $\forall x,p(x)$ a counterexample is a value of x for which $p(x)$ is false, thereby exposing the falsehood of $\forall x,p(x)$.

Methods of Proof

- Direct Proofs
- Indirect Proofs
- Vacuous Proofs
- Proof by Contradiction
- Proof by Cases
- Existence Proofs
- Counterexamples
- Uniqueness Proofs
- Proof by Induction

Theorems and Proofs

- A **theorem** is a statement that can be shown to be true
- One can demonstrate that a theorem is true with a sequence of statements that for an argument called a **proof**.
- The statements used in a proof include **axioms** or **postulates** (underlying assumptions about mathematical structures), while **rules of inference** tie together the steps of a proof.
- A **fallacy** is argument that is not valid because of incorrect reasoning.
- A **lemma** is a simple theorem used in proving other theorems.
- A **corollary** is a proposition that can be established directly from a theorem that has been proved.
- A **conjecture** is a statement whose truth value is unknown. Once a conjecture is shown to be true via a proof it becomes a theorem
- For an implication $p \Rightarrow q$, p is called the **hypothesis** and q is its **conclusion**.

Direct Proofs

An implication $p \Rightarrow q$, can be proved by showing whenever p is true then q must be true.

For example, consider the following definitions:

A integer n is even if there exists another integer k such that $n=2k$ and it is odd if there exists another integer k such that $n=2k+1$. A number can be either even or odd and not both.

Now we are told to attempt a direct proof of the theorem "If n is an odd integer then n^2 is an odd integer."

Indirect Proofs

Since $p \Rightarrow q$ is equivalent to its contrapositive $\neg q \Rightarrow \neg p$, one can prove it is true by proving that contrapositive is true.

Prove that "If $3n+2$ is odd, then n is odd" via indirect proof

Vacuous and Trivial Proofs

If for an implication $p \Rightarrow q$, its hypothesis p is always false then the statement $p \Rightarrow q$ is always true.

E.g. $P(x) \equiv x^2 > x$ where x is a natural number.

Prove that "$P(0) \Rightarrow \forall n\ P(n)$"

Prove by Contradiction

While proving p is true, suppose that a contradiction q can be found so that $\neg p \Rightarrow q$ is true, that is $\neg p \Rightarrow F$ is true. Then the proposition $\neg p$ must be true. Consequently p is true. One can find a contradiction such that $\neg p \Rightarrow r \wedge \neg r$, therefore p is true.

Show that at least four of any 22 days must fall on the same day of the week.

Proof: Let p be the proposition "at least four of any 22 days must fall on the same day of the week". Suppose $\neg p$ is true. i.e. at most three of any 22 days must fall on the same day of the week. Since a week has 7 days, this implies at most 21 days are picked. Therefore, we have a contradiction, making $\neg p \Rightarrow r \wedge \neg r$ true, where r is the statement "22 days were chosen". Therefore p is true.

From [Rosen]

Proof by Cases

To prove an implication of the form:

$(p_1 \vee p_2 \vee \ldots p_n \Rightarrow q)$

Since we know

$[(p_1 \vee p_2 \vee \ldots p_n \Rightarrow q)] \Leftrightarrow [(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots (p_n \Rightarrow q)]$

All we have to do is prove all $p_i \Rightarrow q$ are true where $i = 1, 2, \ldots, n$

For example: Use a proof by cases to show that $|xy| = |x||y|$ where x and y are real numbers. Remember that $|x|=x$, if $x \geq 0$ and $|x|=-x$ if $x<0$

Prove of Equivalence

In order to prove that $p \Leftrightarrow q$, one can use the tautology:

$$p \Leftrightarrow q \equiv p \Rightarrow q \wedge q \Rightarrow p$$

So by individually proving $p \Rightarrow q$ is true and $q \Rightarrow p$ is true, one can prove $p \Leftrightarrow q$ is true as a whole.

Witnesses and Counter-examples

Existential Proof

For an existential formula, $\exists x,p(x)$ a **witness** is a value of x making $p(x)$ true, thereby proving $\exists x,p(x)$ true as a whole.

Proof by Counter-example

For a universal formula, $\forall x,p(x)$ a **counter-example** is a value of x making $p(x)$ false, thereby proving $\forall x,p(x)$ false as a whole.

Uniqueness Proof

Existence: We show that an element x with the desired property exists, i.e. $\exists x\, p(x)$

Uniqueness: We show that if $y \neq x$, then y can not have the desired property, i.e. $\exists x\, p(x) \wedge \forall y\, (x \neq y) \Rightarrow \neg p(x)$
or $\exists x\, p(x) \wedge \forall y\, p(y) \Rightarrow y = x$

Example: Show that every integer has an additive inverse, i.e. show that for every integer p there is a unique integer q such that $p+q=0$

Uniqueness Proof

Existence: We show that an element x with the desired property exists, i.e. $\exists x\, p(x)$

Uniqueness: We show that if $y \neq x$, then y can not have the desired property, i.e. $\exists x\, p(x) \wedge \forall y\, (x \neq y) \Rightarrow \neg p(x)$
or $\exists x\, p(x) \wedge \forall y\, p(y) \Rightarrow y = x$

Example: Show that every integer has an additive inverse, i.e. show that for every integer p there is a unique integer q such that $p+q=0$

Proof: If p is an integer, we find that p+q=0 when q=-p and q is also an integer. Thus, we have proven the existence part.

To show that q is unique, suppose that r is an integer with $r \neq q$ such that $p+r=0$. Then $p+r=p+q$. By subtracting p from both sides we have $q=r$, which contradicts our assumption $r \neq q$. Consequently, there is a unique integer q such that $p+q=0$

From [Rosen]

Weak Natural Induction

For any predicate p(n) over the natural numbers 0,1,2,3,… **weak natural induction** is the argument:

$$p(0), (\forall k,\, p(k) \Rightarrow p(k+1)) \vdash \forall n,\, p(n)$$

where $p(0)$ is the base case

$\forall k,\, p(k) \Rightarrow p(k+1)$ is the inductive case

For example, prove that:

$0 + 1 + 2 + \ldots + n = n \times (n+1)/2$

An example of natural induction

You are required to prove that $1+2+3+\ldots+n = n(n+1)/2$
We say $P(k)$ is true iff $1+2+3+\ldots+n = k(k+1)/2$

BASIC STEP: $P(1)$ is true since $1 = 1(1+1)/2$
INDUCTIVE STEP: If $P(k)$ is true then
$(1)+(2)+(3)+\ldots+(k)+(k+1) = k(k+1)/2 + (k+1)$
$= (k^2+k)/2 + (k+1)$
$= (k^2 + k + 2k + 2)/2$
$= (k+1)(k+2)/2$
So we have established that if $P(k)$ is true then
$(1)+(2)+(3)+\ldots+(k)+(k+1) = (k+1)(k+2)/2$ i.e. $P(k+1)$ is true.

From the base case $P(1)$ is true. From the inductive step $P(k) \Rightarrow P(k+1)$ i.e. $P(1) \Rightarrow P(2)$ and then $P(2) \Rightarrow P(3)$ and so on. So $P(k)$ is true for all positive integers k. Therefore we have proved the relationship using induction.

From [Rosen]

Strong Natural Induction

For any predicate p(n) over the natural numbers 0,1,2,3,… **strong natural induction** is the argument:

$$\forall k, ((\forall j, j<k \Rightarrow p(j)) \Rightarrow p(k) \vdash \forall n, p(n)$$