Course Notes

CSCA67 - Discrete Mathematics

Instructors:

	Dr. Anna Bretscher	Dr. Richard Pancer
Email:	bretscher@utsc.utoronto.ca	pancer@utsc.utoronto.ca
Office:	IC493	IC490
Office Hours:	Monday 12:10 - 1:30	Monday 11:10 - 12:30
	Wednesday 1:10 - 2:00	Friday 1:30 - 3:00
	Friday 1:10 - 2:00 (will change after week 6)	

1 Propositions, Implications

Definitions:

A **proposition** is a statement that evaluates to True or False. In computer science, its often referred to as a **Boolean expression**.

A **compound roposition** is a proposition statementt that involves multiple propositions joined by connectives. It takes multiple truth values as input and returns a single truth value as output.

A **connective** corresponds to English conjunctions such as ”and”, ”or”, ”not” etc.

Basic connectives and truth tables:

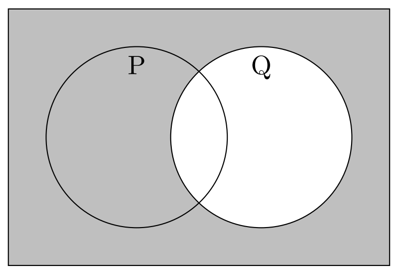
Symbol	Meaning
$\land$	”AND”
$\lor$	”OR”
$\rightarrow$	”IF...THEN”
$\leftrightarrow$	”IF AND ONLY IF”
$\neg$	”NOT”

P	Q	$P \land Q$	$P \lor Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Implication:

Different ways of writing $P \rightarrow Q$:

1. If P then Q
2. If P, Q
3. Q, if P
4. P only if Q
5. P is sufficient for Q
6. Q is neccesary for P
7. If not Q, then not P
8. Not P or Q



Logical Equivalences:

Commutative	$p \land q \iff q \land p$	$p \lor q \iff q \lor p$
Associative	$(p \land q) \land r \iff p \land (q \land r)$	$(p \lor q) \lor r \iff p \lor (q \lor r)$
Distributive	$p \land (q \lor r) \iff (p \land q) \lor (p \land r)$	$p \lor (q \land r) \iff (p \lor q) \land (p \lor r)$
Identity	$p \land T \iff p$	$p \lor F \iff p$
Negation	$p \lor \neg p \iff T$	$p \land \neg p \iff F$
Double Negative	$\neg(\neg p) \iff p$	
Idempotent	$p \land p \iff p$	$p \lor p \iff p$
Universal Bound	$p \lor T \iff T$	$p \land F \iff F$
De Morgan's	$\neg(p \land q) \iff (\neg p) \lor (\neg q)$	$\neg(p \lor q) \iff (\neg p) \land (\neg q)$
Absorption	$p \lor (p \land q) \iff p$	$p \land (p \lor q) \iff p$
Conditional or ($\rightarrow$) Law	$(p \rightarrow q) \iff (\neg p \lor q)$	$\neg(p \rightarrow q) \iff (p \land \neg q)$
Biconditional	$(p \leftrightarrow q) \iff (p \rightarrow q) \land (q \rightarrow p)$	

Order of Operations:

1. NOT($\neg$) 2. AND($\land$) 3. OR($\lor$) 4. Quantifiers($\forall$/$\exists$) 5. ($\rightarrow$ / $\leftrightarrow$)

2 Predicates and Quantifiers

Forall:	$\forall$
There exists:	$\exists$
Negations:	
$\neg\forall = \exists$	$\neg\exists = \forall$

Prove statement in the form of $\exists x \in S, \ni: P(x)$
We simply need to find **one** value of x in the set S, that makes $P(x)$ true.
One value is enough.

Example:
There exists an integer n, such that n^2 is even.
$\exists n \in \mathbb{Z}, \ni: n^2 \in 2\mathbb{Z}$
Let $n = 2$, then $(2)^2 = 4$ which is an even number

Prove statemnet in the form of $\forall x \in S, \ni: P(x)$
This means we must use techniques such as algebraic manipulation to show that:
$P(x)$ holds for every arbitrary $x \in S$

Example:
Forall integers n, if n is odd, then n^2 is odd.
$\forall n \in \mathbb{Z}, n \in 2\mathbb{Z} \rightarrow n^2 \in 2\mathbb{Z}$
Let $n = 2k, k \in \mathbb{Z}$
then $n^2 = (2k)^2 = 4k^2$ which is an even number.
Therefore: Forall integers n, if n is odd, then n^2 is odd. QED

2.1 Modulus

$$10 \textbf{ mod } 3 = 1$$

The modulus or "mod" operator means the remainder when we divide two numbers.
Congruent mod means that two numbers have the same remainder when divided by one number.

$$10 \equiv_3 7 \Leftrightarrow 10 \bmod 3 = 7 \bmod 3$$

2.2 Fundamental Theorem of Arithmetic

The **Fundamental Theorem of Arithmetic** states that any integer greater than 1 is either a **prime** number itself, or can be represented as the unique product of prime numbers.
For example:

$$\begin{aligned} 16 &= 2^4 \\ 18 &= 2^1 \cdot 3^2 \\ 21 &= 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \end{aligned}$$

Numbers that can be written as the unique product of primes are called **Composite Numbers**.
Reminder: a **prime number** is an number that can only be divided evenly by 1 and the number itself.

3 Proofs - Proof Strategies

To prove in the form of $P \to Q$:

Direct Proof: Assume P is true then prove Q

This form works because if we recall the truth table for $P \to Q$,
When P is true, Q must be true for the statement to evaluate to true.

Proof by Contrapositve: Assume $\neg Q$ is true then prove $\neg P$

This form works because the contrapositive is logically equivalent to the original,
$P \to Q \equiv \neg Q \to \neg P$

Proof by Contradiction: Assume $\neg(\neg(P \to Q)) \equiv P \wedge \neg Q$

Then we must derive some sort of contradiction.
Once we arrive at the contradiction, that means one of our assumptions cannot be correct.
for example if $\neg Q$ is false, that means Q is true.

Proof by Cases/Exhaustion: $X \vee Y \to Q$ Show $X \to Q \wedge Y \to Q$
Example:
$x \in \mathbb{Z} \to x^2 + x + 1 \in 2\mathbb{Z} + 1$ ($x^2 + x$ is odd)

Case 1: x is odd
$x = 2k + 1$
$(2k + 1)^2 + (2k + 1) + 1$
$= 4k^2 + 4k + 1 + 2k + 1 + 1$
$= 4k^2 + 6k + 3$
$= 2(2k^2 + 3) + 3$ case holds when x is odd.

Case 2: x is even
$x = 2k$
$(2k^2) + 2k + 1$
$= 4k^2 + 2k + 1$
$= 2(2k^2 + k) + 1$ case holds when x is even.
Since we have proven both case are indepdently even, we can conclude $\forall x \in \mathbb{Z}, x^2 + x + 1 \in 2\mathbb{Z} + 1$

4 Proof of Irrationality

4.1 Approach 1 - Fundamental Theorem of Arithmetic

Prove that $\sqrt{2}$ is irrational.

Assume the contrary that $\sqrt{2}$ is rational.
Then by the definition of rational numbers, $\sqrt{2} = \frac{m}{n}, \ni: m, n \in \mathbb{Z}, gcd(m, n) = 1, n \neq 0$

$$\sqrt{2} = \tfrac{m}{n}$$
$$n\sqrt{2} = m$$
$$2n^2 = m^2$$
$$m = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n} \qquad n = y_1{}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n}$$

Each x, y are primes by the fundamental theorem of arithmetic.

$$m^2 = (x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n})(x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n})$$

This means that m^2 has $2n$ possible factors.

$$2n^2 = 2(y_1{}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n})(y_1{}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n})$$

This means that n^2 has $2n$ possible factors plus one factor 2.

as m^2 has an even number of prime factors, $2n^2$ will have an odd number of prime factors, contradicting the fundamental theorem.

$\therefore \sqrt{2} \in \mathbb{I}$ by contradiction. *QED*

4.2 Approach 2 - Definition of a Rational Number

Prove that $\sqrt{2}$ is irrational.

Assume the contrary that $\sqrt{2}$ is rational.
Then by the definition of rational numbers, $\sqrt{2} = \frac{m}{n}, \ni: m, n \in \mathbb{Z}, gcd(m, n) = 1, n \neq 0$

$gcd(m, n)$ means that m, n MUST be relative prime.

$$\sqrt{2} = \tfrac{m}{n}$$
$$n\sqrt{2} = m$$
$$2n^2 = m^2$$
$$2n^2 = m^2 \Rightarrow m^2 \in 2\mathbb{Z} \Rightarrow m \cdot m \in 2\mathbb{Z}$$

The previousline showed that m is even, so now we can substitute m with any arbitrary even number $2k$.

$$m = (2k), k \in \mathbb{Z}$$
$$2n^2 = (2k^2)$$
$$2n^2 = 4k^2$$
$$n^2 = 2k^2$$
$$n^2 \in 2\mathbb{Z} \Rightarrow n \in 2\mathbb{Z}$$
$$m, n \in 2\mathbb{Z} \Rightarrow gcd(m, n) \neq 1$$

Since m, n are both even, they cannot be relatively prime, $\therefore \sqrt{2} \in \mathbb{I}$ by contradiction. *QED*