Course Notes

# CSCA67 - Discrete Mathematics

UNIVERSITY OF TORONTO SCARBOROUGH


**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 |
|---|---|
| $\wedge$ | "AND" |
| $\vee$ | "OR" |
| $\rightarrow$ | "IF...THEN" |
| $\leftrightarrow$ | "IF AND ONLY IF" |
| $\neg$ | "NOT" |

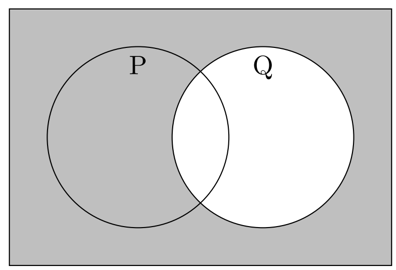
| $P$ | $Q$ | $P \wedge Q$ | $P \vee Q$ | $P \rightarrow Q$ | $P \leftrightarrow Q$ |
|---|---|---|---|---|---|
| T | T | T | T | T | T |
| T | F | F | T | F | F |
| F | T | F | T | T | F |
| F | F | F | F | T | T |

---

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

---

## Order of Operations:

1. NOT($\neg$) 2. AND($\wedge$) 3. OR($\vee$) 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.
$\forall n \in \mathbb{Z}, n \in 2\mathbb{Z} \to n^2 \in 2\mathbb{Z}$
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.

$$10 \equiv_3 7 \Leftrightarrow 10 \text{ mod } 3 = 7 \text{ mod } 3$$

## 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 Basic 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 $\neg(\neg(P \to Q)) \equiv P \land \neg Q$

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**: $X \lor Y \to Q$ Show $X \to Q \land Y \to Q$
**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
$x = 2k + 1$
$(2k + 1)^2 + (2k + 1) + 1$
$= 4k^2 + 6k + 3$
$= 2(2k^2 + 3) + 3$ 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 $\forall x \in \mathbb{Z}, x^2 + x + 1 \in 2\mathbb{Z} + 1$

**Some Definitions:**

**Theorem:** A statement that has already been proved.

**Axiom:** A statement that is self evidently true.

**Identiy:** An equation that is true for all values of an arbitrary variable.

**Proof:** A mathematical argument demonstrating the truth of a proposition.

**Tautology:** A propositional logic formula that always evaluates to True. $(A \lor \neg A)$ - (I'm hungry or I'm not hungry)

**Rational Number:** A number that can be represented as the fraction of two relatively prime integers.

$$A \in \mathbb{Q} \to A = \frac{m}{n}, n \neq 0, m, n \in \mathbb{Z}, gcd(m, n) = 1$$

**Logic in a nutshell**

| Statement | Ways to Prove it | Ways to Use it | How to Negate it |
|---|---|---|---|
| $p$ | • Prove that $p$ is true.<br>• Assume $p$ is false, and derive a contradiction. | • $p$ is true.<br>• If $p$ is false, you have a contradiction. | not $p$ |
| $p$ and $q$ | • Prove $p$, and then prove $q$. | • $p$ is true.<br>• $q$ is true. | (not $p$) or (not $q$) |
| $p$ or $q$ | • Assume $p$ is false, and deduce that $q$ is true.<br>• Assume $q$ is false, and deduce that $p$ is true.<br>• Prove that $p$ is true.<br>• Prove that $q$ is true. | • If $p \Rightarrow r$ and $q \Rightarrow r$ then $r$ is true.<br>• If $p$ is false, then $q$ is true.<br>• If $q$ is false, then $p$ is true. | (not $p$) and (not $q$) |
| $p \Rightarrow q$ | • Assume $p$ is true, and deduce that $q$ is true.<br>• Assume $q$ is false, and deduce that $p$ is false. | • If $p$ is true, then $q$ is true.<br>• If $q$ is false, then $p$ is false. | $p$ and (not $q$) |
| $p \iff q$ | • Prove $p \Rightarrow q$, and then prove $q \Rightarrow p$.<br>• Prove $p$ and $q$.<br>• Prove (not $p$) and (not $q$). | • Statements $p$ and $q$ are interchangeable. | ($p$ and (not $q$)) or ((not $p$) and $q$) |
| $(\exists x \in S)\ P(x)$ | • Find an $x$ in $S$ for which $P(x)$ is true. | • Say "let $x$ be an element of $S$ such that $P(x)$ is true." | $(\forall x \in S)$ not $P(x)$ |
| $(\forall x \in S)\ P(x)$ | • Say "let $x$ be any element of $S$." Prove that $P(x)$ is true. | • If $x \in S$, then $P(x)$ is true.<br>• If $P(x)$ is false, then $x \notin S$. | $(\exists x \in S)$ not $P(x)$ |

Graph from Introduction to mathematical arguments - by Michael Hutchings

# 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, $\sqrt{2} = \frac{m}{n}, \ni: m, n \in \mathbb{Z}, gcd(m,n) = 1, n \neq 0$

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

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.

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

---

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. $QED$

# 5 Induction and the Pigeonhole Principle

**Simple Induction Format:**

Suppose we need to prove $P(n)$ for all natural numbers.

**1. State the Predicates**
$P(n) : \ldots$

**2. Base case**
Prove that $P(n)$ holds when $n$ is the smallest possible natural number.
$P(0) : \ldots$ is True.

**3. Inductive Hypothesis**
Assume that $P(k)$ holds for any arbitrary $k$
$P(k) : \ldots$ is True.

**4. Inductive Step**
Prove that $P(k) \to P(k+1)$
Assume $P(k)$ then show $P(k+1)$

**Example:**
Prove

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

**Stating the Predicate:** $P(n) : \sum_{i=0}^{n} i = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$

**Base case:** $n = 0 : \sum_{i=0}^{0} i = 0 \qquad \frac{0(0+1)}{2} = 0$
Base case holds.

**Inductive Hypothesis:** Assume for any arbitrary $k$, $P(k)$ holds.

**Inductive Step:** Prove $P(k) \to P(k+1)$
$P(k+1) = P(k) + (k+1)$
$P(k+1) = \frac{n(n+1)}{2} + (k+1)$
$P(k+1) = \frac{n(n+1)+2(n+1)}{2}$
$P(k+1) = \frac{(n+1)(n+2)}{2}$

**Conclusion:**
$\therefore P(k) \to P(k+1)$
$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$