CMSC 250: Discrete Structures

Summer 2017

Lecture 4 - Outline

June 5, 2017

Introduction to Proofs

More definitions:

A real number is **rational** iff it can be expressed as a ratio of two integers with a non-zero denominator. More formally,

$$r \text{ is rational} \leftrightarrow \exists a, b \in \mathbb{Z}, \text{ s.t. } r = \frac{a}{b} \wedge b \neq 0.$$

The set of rational numbers is denoted $\mathbb{Q}$. Note that we can always demand that we choose an a and b such that they do not share common factors other than 1. If a and b do not have common factors other than 1, they are said to be **relatively prime**.

A real number is **irrational** iff it is not rational. In other words, the set of irrational numbers is $\mathbb{R} \setminus \mathbb{Q}$.

Proofs By Contrapositive

The implication $p \to q$ is logically equivalent to its contrapositive $\neg q \to \neg p$. We can show this:

Prove: Show that $p \to q \equiv \neg q \to \neg p$.

Solution. The truth table below proves the above equivalence.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

This logical equivalence of an implication $p \to q$ and its contrapositive is very useful in proofs. Some proofs may be difficult to tackle directly, but may be made much easier when considering the contrapositive. This is often the case when not enough can be infered from p and q, but more can be infered from their negations $\neg p$ and $\neg q$.

Prove: Prove that for all real numbers a and b, if the product ab is an irrational number, then either a or b, or both must be irrational.

Solution. We will prove the above claim by proving the contrapositive. That is, we will show that if both a and b are rational numbers then their product ab is a rational number. Let $a = \frac{p}{q}$ and $b = \frac{r}{s}$, where p, q, r, and s are integers and $q \neq 0$ and $s \neq 0$. The product ab can be expressed as follows.

$$ab = \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

Let $t = p \times r$ and $u = q \times s$. Note that $t, u \in \mathbb{Z}$. Also, since $q \neq 0$ and $s \neq 0$, $u \neq 0$. Thus, since $ab = \frac{t}{u}$, ab is a rational number by definition.

Example. Prove that for any $x, y, z \in \mathbb{Z}$, if $x = y + z$ is even, then y and z must be either both odd or both even.

Solution. To prove the above claim, we will prove its contrapositive: "If exactly one of y or z is even, then $x = y + z$ is odd".

Without loss of generality, for some integers k and l, let $y = 2k$ be even and $z = 2l + 1$ be odd. Then,

$$\begin{aligned} x =& y + z \\ =& 2k + 2l + 1 \\ =& 2(k + l) + 1 \end{aligned}$$

Let $m = k + l$. Since $x = 2m + 1$, for some $m \in \mathbb{Z}$, $y + z$ is odd by definition.

Proofs By Contradiction

Suppose p is some proposition whose truth we want to deduce. In proof by contradiction, we suppose that p is false and show that this assumption leads logically to a contradiction. By showing this, it also shows that p is true, since the two are logically equivalent, i.e. $p \equiv \neg p \rightarrow C$. We verify this from the truth table given below.

p	$\neg p$	C	$\neg p \to C$
T	F	F	T
F	T	F	F

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

Solution: For the purpose of contradiction, assume that $\sqrt{2}$ is a rational number. Then there are integers a and b ($b \neq 0$) with no common factors such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \qquad (1) \end{aligned}$$

From (1) we conclude that a^2 is even. This implies that a is even. Then, for some integer k, let

$$a = 2k \qquad (2)$$

Combining (1) and (2) we get

$$\begin{aligned} 4k^2 &= 2b^2 \\ 2k^2 &= b^2 \end{aligned}$$

The above equation implies that b^2 is even and hence b is even. Since we know a is even this means that a and b have 2 as a common factor which contradicts the assumption that a and b have no common factors.

We will now give a very elegant proof for the fact that "$\sqrt{2}$ is irrational" using the *unique factorization theorem* which is also called the *fundamental theorem of arithmetic.*

The unique factorization theorem states that every positive number can be uniquely represented as a product of primes. More formally, it can be stated as follows.

> Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that
>
> $$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$
>
> and any other expression of n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.

Prove: Prove that $\sqrt{2}$ is irrational using the unique factorization theorem.

Solution: Assume for the purpose of contradiction that $\sqrt{2}$ is rational. Then there are integers a and b ($b \neq 0$) such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \end{aligned}$$

Let $S(m)$ be the sum of the number of times each prime factor occurs in the unique factorization of m. Note that $S(a^2)$ and $S(b^2)$ is even. Why? Because the number of times that each prime factor appears in the prime factorization of a^2 and b^2 is exactly twice the number of times that it appears in the prime factorization of a and b. Then, $S(2b^2) = 1 + S(b^2)$ must be odd. This is a contradiction as $S(a^2)$ is even and the prime factorization of a positive integer is unique.

We can also use a proof by contradiction to prove logical implications $p \to q$. To do this, we need to figure out how to negate $p \to q$.

Example. Show that $p \to q \equiv \neg p \vee q \equiv (p \wedge \neg q) \to C$.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg p \vee q$	$p \wedge \neg q$	C	$(p \wedge \neg q) \to C$
T	T	F	F	T	T	F	F	T
T	F	F	T	F	F	T	F	F
F	T	T	F	T	T	F	F	T
F	F	T	T	T	T	F	F	T

The above equivalence forms the basis of proofs by contradiction.

Prove. For all integers n, if $3n + 2$ is odd then n is odd. **Solution.** Suppose for the sake of contradiction that $3n + 2$ is odd and n is even. Since n is even, there exists an integer k such that $n = 2k$. Thus $3n + 2$ can be written as

$$\begin{aligned} 3n+2 =& 3(2k)+2 \\ =& 2(3k+1) \end{aligned}$$

Let $\ell = 3k+1$. Since $3n+2 = 2\ell$, for $\ell \in \mathbb{Z}$, it is even by definition. Note that our premise is that $3n+2$ is odd and we have shown that $3n+2$ is even. This is a contradiction. This proves the claim.