CMSC 250: Discrete Structures

Summer 2017

Lecture 3 - Outline

June 2, 2017

Introduction to Proofs

Some Definitions:

- An integer n is **even** iff $n = 2k$ for some $k \in \mathbb{Z}$.

  We can write this using notation as follows:

  $$n \text{ is even } \leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } n = 2k$$

- An integer n is **odd** iff $n = 2k + 1$ for some $k \in \mathbb{Z}$.

  We can write this using notation as follows:

  $$n \text{ is odd } \leftrightarrow \exists k \in \mathbb{Z} \text{ s.t. } n = 2k + 1$$

- An integer n is **prime** iff $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$.
- An integer n is **composite** iff $n > 1$ and n is not a prime.
- An integer b is said to divide a, $a \neq 0$, iff $a = bk$ for some $k \in \mathbb{Z}$. This is normally denoted $b \mid a$.

  We can also say that a is divisible by b in this case.

  We can write this using notation as follows:

  $$b \mid a \leftrightarrow a \neq 0 \wedge \exists k \in \mathbb{Z} \text{ s.t. } a = bk$$

Direct Proofs

Prove: Prove that the sum of two even integers is an even integer.

Solution: Let x and y be arbitrary even integers. We want to show that $x + y$ is also even.

We know that, by the definition of an even integer, $x = 2k$ for some $k \in \mathbb{Z}$ and $y = 2\ell$ for some $\ell \in \mathbb{Z}$. Hence:

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

Let $m = k + \ell$,

$$x + y = 2m$$

Since we have shown that $x + y = 2m$, for some $m \in \mathbb{Z}$, we have, by definition, that $x + y$ is even.

Prove: For all integers x and y, if $6 \mid x$ and $4 \mid y$, then $2 \mid (5x - 7y)$.

Solution: Let x and y be arbitrary integers such that $6 \mid x$ and $4 \mid y$. We want to show that $2 \mid (5x - 7y)$, or equivalently, that $5x - 7y = 2m$, for some $m \in \mathbb{Z}$.

By the definition of divisibility, we have that $x = 6k$, for some $k \in \mathbb{Z}$ and that $y = 4\ell$, for some $\ell \in \mathbb{Z}$. Hence:

$$\begin{aligned} 5x - 7y &= 5(6k) - 7(4\ell) \\ &= 30k - 28\ell \\ &= 2(15k - 14\ell) \end{aligned}$$

Let $m = 15k - 14\ell$,

$$5x - 7y = 2m$$

Since we have shown that $5x - 7y = 2m$, for some $m \in \mathbb{Z}$, we have, by definition, that $2 \mid 5x - 7y$ is even.

Prove: Prove that for any set A and B, $A \setminus (A \setminus B) \subseteq B$.

Solution: Let A and B be arbitrary sets. Let x be an arbitrary element such that $x \in A \setminus (A \setminus B)$. We want to show that $x \in B$.

$$\begin{aligned} x \in A \setminus (A \setminus B) &\implies x \in A \wedge x \notin (A \setminus B) \\ &\implies x \in A \wedge \neg(x \in (A \setminus B)) \\ &\implies x \in A \wedge \neg(x \in A \wedge x \notin B)) \\ &\implies x \in A \wedge (x \notin A \vee x \in B) && \text{(by DeMorgan's Laws)} \\ &\implies (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) && \text{(by Distributive laws)} \\ &\implies F \vee (x \in A \wedge x \in B) && \text{(by Negation laws)} \\ &\implies x \in A \wedge x \in B && \text{(by Identity laws)} \\ &\implies x \in B \end{aligned}$$

Since we have shown that an arbitrary $x \in A \setminus (A \setminus B)$ is also in B, we have proven the claim.

Prove: Prove for any sets A and B, $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$.

Solution: To prove set equality $C = D$, we need to show that $C \subseteq D$ and $D \subseteq C$.

Let A and B be arbitrary sets.

Lemma: Prove that $(A \cup B) \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A)$.

Let x be in arbitrary element such that $x \in (A \cup B) \setminus (A \cap B)$. We want to show that $x \in (A \setminus B) \cup (B \setminus A)$.

$$
\begin{aligned}
x \in (A \cup B) \setminus (A \cap B) &\implies x \in (A \cup B) \wedge x \notin (A \cap B) \\
&\implies (x \in A \vee x \in B) \wedge \neg(x \in (A \cap B)) \\
&\implies (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) \\
&\implies (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) && \text{(by DeMorgan's Laws)} \\
&\implies (x \in A \wedge (x \notin A \vee x \notin B)) \vee (x \in B \wedge (x \notin A \vee x \notin B)) && \text{(by Distributive Laws)} \\
&\implies ((x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B)) \\
&\qquad \vee ((x \in B \wedge x \notin A) \vee (x \in B \wedge x \notin B)) && \text{(by Distributive Laws)} \\
&\implies (F \vee (x \in A \wedge x \notin B)) \vee ((x \in B \wedge x \notin A) \vee F) && \text{(by Negation Laws)} \\
&\implies (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) && \text{(by Identity Laws)} \\
&\implies (x \in A \setminus B) \vee (x \in B \setminus A) \\
&\implies x \in (A \setminus B) \cup (B \setminus A)
\end{aligned}
$$

Since we have shown that an arbitrary $x \in\in (A \cup B) \setminus (A \cap B)$ is also in $(A \setminus B) \cup (B \setminus A)$, we have proven the lemma.

Lemma: Prove that $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$.

Let x be in arbitrary element such that $x \in (A \setminus B) \cup (B \setminus A)$. We want to show that $x \in (A \cup B) \setminus (A \cap B)$.

$$
\begin{aligned}
x \in (A \setminus B) \cup (B \setminus A) &\implies (x \in A \setminus B) \vee (x \in B \setminus A) \\
&\implies (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)
\end{aligned}
$$

Note that we have arrived at two cases here. The first case is $x \in A \wedge x \notin B$. The second case $x \in B \wedge x \notin A$. We can proceed to deal with these separately – as long as we can show $x \in (A \cup B) \setminus (A \cap B)$ in both cases, we are good to go.

Case 1: $x \in A \wedge x \notin B$

$$
\begin{aligned}
x \in A \wedge x \notin B &\implies (x \in A \vee x \in B) \wedge (x \notin B \vee x \notin A) && \text{(think carefully about this step)} \\
&\implies (x \in A \cup B) \wedge \neg(x \in B \wedge x \in A) \\
&\implies x \in A \cup B \wedge \neg(x \in A \cap B) \\
&\implies x \in (A \cup B) \setminus (A \cap B)
\end{aligned}
$$

Case 2: $x \in B \wedge x \notin A$

This case is very similar to Case 1, so we shall omit the details. It simply involves switching the roles of A and B.

Since we have proven both cases, we have proven the lemma. Note how much shorter this proof was using cases – often a good choice of cases helps to make proofs dramatically easier.

Since we have shown that $(A \cup B) \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A)$ and $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$, we have proven the claim.

Cases

We have seen how the use of cases can help to make proofs easier to tackle. Let's explore this a little further with the next proof.

Remember, you are always free to use cases in your proofs. Just remember to make sure that the cases that you choose cover all of the elements that you wish to prove the claim on!

Prove: Prove that, for all integers n, $n^2 + n + 1$ is odd.

Solution: Without splitting into cases, this problem is quite hard to tackle. We know we want to show that $n^2 + n + 1 = 2k + 1$, for some $k \in \mathbb{Z}$, but it is not super clear how we would go about doing this. Let us try to split up the set of all integers into two cases: even and odd.

Case 1: n **is even**

Let n be an arbitrary even integer, such that $n = 2k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n^2 + n + 1 &= (2k)^2 + (2k) + 1 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Let $m = 2k^2 + 2k$,

$$n^2 + n + 1 = 2m + 1$$

Since we have shown that $n^2 + n + 1 = 2m + 1$, for some $m \in \mathbb{Z}$, it is odd by definition.

Case 2: n **is odd**

Let n be an arbitrary even integer, such that $n = 2k + 1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n^2 + n + 1 &= (2k + 1)^2 + 2k + 1 + 1 \\ &= 4k^2 + 4k + 1 + 2k + 2 \\ &= 4k^2 + 6k + 2 + 1 \\ &= 2(2k^2 + 3k + 1) + 1 \end{aligned}$$

Let $m = 2k^2 + 3k + 1$,

$$n^2 + n + 1 = 2m + 1$$

Since we have shown that $n^2 + n + 1 = 2m + 1$, for some $m \in \mathbb{Z}$, it is odd by definition.

Since we have proven the claim in both cases, we have proven the claim.

Catalog of LaTeX Commands

$\implies$ `- \implies` | b | a `- b \mid a`