CSCA67 Tutorial, Week 5[1]

1 Review of last week's lecture

Direct and indirect proof techniques

So far, we have seen 2 proof techniques for proving an implication $p \to q$ such as "If $n \in \mathbb{Z}$, then $4 \nmid (n^2 - 3)$":

- direct proof
- (indirect) proof by contradiction

We have also seen **proof by contraposition**. We know what the *contrapositive* of an implication $p \to q$ is...$\neg q \to \neg p$ and that they are equivalent. Recall that each proof takes a different form:

	Direct Proof	Contraposition	Contradiction
Assumption(s)	p eg., $n \in \mathbb{Z}$	$\neg q$ eg., $4 \mid (n^2 - 3)$	$p \wedge \neg q$ eg., $n \in \mathbb{Z} \wedge 4 \mid (n^2 - 3)$
What to prove	q eg., $4 \nmid (n^2 - 3)$	$\neg p$ eg., $n \notin \mathbb{Z}$	some contradiction exists

Many statements are much easier to prove using one proof technique than another. In fact, some statements *cannot* be proven using every technique. Thus, we have to carefully choose the technique we will use.

One approach we can take to choosing our proof technique is to identify, for each possible technique, what our proof would assume and what its conclusion would be (as above). We may find that the assumptions for one technique offer much more information than the assumptions for another.

For example, if we would like to prove "If $n \in \mathbb{Z}$, then $4 \nmid (n^2 - 3)$", and we attempt a direct proof, we start with the assumption that $n \in \mathbb{Z}$. This offers us very little information about n, which we need in order to start building a logical chain towards our conclusion $4 \nmid (n^2 - 3)$.
However, if we attempt a contrapositive proof of this statement, we start with the assumption $4 \mid (n^2 - 3)$. This offers us much more initial information: for instance, we can then write $n^2 - 3 = 4k$, $k \in \mathbb{Z}$.

Don't forget that most of the statements we are asked to prove can be restated using the universal quantifier: for example, "If $n \in \mathbb{Z}$, then $4 \nmid (n^2 - 3)$" can be restated as "$\forall n \in \mathbb{Z}$, $4 \nmid (n^2 - 3)$".
We can demonstrate for some value of n, eg. $n = 2$, that $4 \nmid (n^2 - 3)$. But we cannot show that $4 \nmid (n^2 - 3)$ is true for every $n \in \mathbb{Z}$, since $\mathbb{Z}$ is countably infinite. To prove that this statement is true, we need a full proof.

However, to prove that this type of statement is false, we can simply find a counterexample - in this case, a value of n such that $4 \nmid (n^2 - 3)$, since this means that $4 \nmid (n^2 - 3)$ is not true *for all* n.

2 Direct and contrapositive proofs

Q: *Let* $a, b, c \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *If* $a \equiv_n b$, *then* $ca \equiv_n cb$.

Recall that $x \equiv_n y$ means that $x \bmod n = y \bmod n$, and also that $n \mid (x - y)$ where $x > y$.

Direct proof 1:

Suppose $a \equiv_n b$.
This means $n \mid (a - b)$, so there is an integer d for which $a - b = nd$. We multiply both sides of this by c to

[1] Compiled by G. Singh Cadieux

get $ac - bc = ndc$.
Consequently, there is an integer $e = dc$ for which $ac - bc = ne$, so $n|(ac - bc)$ and consequently $ac \equiv_n bc$.

Direct proof 2:

Suppose $a \equiv_n b$.
This means $a \bmod n = b \bmod n = r$ for some remainder $r \in \mathbb{Z}$.
Then by the divison theorem, we can write $a = k_1 n + r$ and $b = k_2 n + r$, where $k_1, k_2 \in \mathbb{Z}$.

$$\begin{aligned} c(b-a) &= c((k_2 n + r) - (k_1 n + r)) \\ bc - ac &= c((k_2 n + r) - (k_1 n + r)) \\ &= c(k_2 n - k_1 n) \\ &= n(c(k_2 - k_1)) \end{aligned}$$

Consequently, $n|(bc - ac)$ and so $ca \equiv_n cb$.

Q: *Let $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.*

Proof by contrapositive:

Suppose x is not odd.
WTP: $x^3 - 1$ is not even.

Thus x is even, so $x = 2a$ for some $a \in \mathbb{Z}$. Then

$$\begin{aligned} x^3 - 1 &= (2a)^3 - 1 \\ &= 8a^3 - 1 \\ &= 8a^3 - 2 + 1 \\ &= 2(4a^3 - 1) + 1 \\ &= 2b + 1, \text{ where } b = 4a^3 - 1 \in \mathbb{Z} \end{aligned}$$

Therefore $x^3 - 1$ is odd if x is even, and by contraposition, x is odd if $x^3 - 1$ is even.

Q: *If $a \equiv_4 0$ or $a \equiv_4 1$, then $\binom{a}{2}$ is even.*

We prove this directly.

Case 1: Assume $a \equiv_4 0$.
Then $a \bmod 4 = 0 \bmod 4 = 0$. So a is a multiple of 4.
Since $a = 4k_1$ for some $k_1 \in \mathbb{N}$, we have

$$\begin{aligned} \binom{a}{2} &= \frac{a!}{(a-2)!2!} \\ &= \frac{a(a-1)}{2} \\ &= \frac{4k_1(4k_1 - 1)}{2} \\ &= 2k_1(4k_1 - 1) \\ &= 2m, \text{ where } m = k_1(4k_1 - 1) \in \mathbb{Z} \end{aligned}$$

Hence $\binom{a}{2}$ is even if $a \equiv_4 0$.

Case 2: Assume $a \equiv_4 1$.

Then $a \bmod 4 = 1 \bmod 4 = 1$.

Since $a = 4k_2 + 1$ for some $k_2 \in \mathbb{N}$, we have

$$\begin{aligned}\binom{a}{2} &= \frac{a!}{(a-2)!2!} \\ &= \frac{a(a-1)}{2} \\ &= \frac{(4k_2+1)((4k_2+1)-1)}{2} \\ &= 2k_2(4k_2+1) \\ &= 2\ell, \text{ where } \ell = k_2(4k_2+1) \in \mathbb{Z}\end{aligned}$$

Hence $\binom{a}{2}$ is even if $a \equiv_4 1$.

□

3 Additional practice problems

Q: Prove the following statements using contrapositive proof:

Suppose $a, b \in \mathbb{Z}$. If $a^2(b^2 - 2b)$ is odd, then a and b are odd.

Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.

Suppose $x \in \mathbb{R}$. If $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$, then $x \geq 0$.

Q: Prove the following statements using either direct or contrapositive proof:

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.

If $a, b \in \mathbb{Z}$ and a and b have the same parity (that is, a and b are both odd or both even), then $3a + 7$ and $7b - 4$ do not.