CM1103 PROBLEM SOLVING WITH PYTHON

PROOFS

Dr Jing Wu

School of Computer Science & Informatics

Cardiff University

Direct Proof

A simple example:

Proposition: If $A \subseteq B$ and $B \subseteq C$, then: $A \subseteq C$

Proof:

Let $x \in A$.

Since $A \subseteq B$, we have $x \in B$.

Since $B \subseteq C$, we have $x \in C$.

We showed that for any $x \in A$, we have $x \in C$, so $A \subseteq C$.

Direct Proof

Prove that the sum of any two rational numbers is rational

Proof:

Let r, s be any rational numbers.

By definition: rational numbers are quotient of integers, so,

$r = \frac{a}{b}$ and $s = \frac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$, and $b \neq 0$, $d \neq 0$.

Then

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}.$$

Because products and sums of integers are integers, $ad + bc$ and bd are integers. And because $b \neq 0$ and $d \neq 0$, $bd \neq 0$.

Thus, $r + s$ is rational by definition of rational numbers.

Proof by Cases

Method

1. List all possible cases that will cover every circumstance.
2. For each possible case, prove the conclusion separately.

Proposition: If $\boldsymbol{A \subseteq B}$ or $\boldsymbol{A \subseteq C}$, then: $\boldsymbol{A \subseteq B \cup C}$

Proof:

Case 1: $A \subseteq B$.

Let $x \in A$. Since $A \subseteq B$, it follows that $x \in B$.

Since $B \cup C = \{x : x \in B \text{ or } x \in C\}$,

Therefore, $x \in B \cup C$.

Case 2: $A \subseteq C$.

The proof is analogous to that for *case 1*.

Disproof by Counterexample

Method

To disprove a statement starting with the form “for every $x \in A$,” find an x in A for which the statement is false.

Let A and B be any sets. Does $A \cup B = A \cap B$? Prove your assertion.

$A \cup B \neq A \cap B$

Proof:

For example:

Let $A = \{1\}$ and $B = \{2,3\}$.

Then $A \cup B = \{1,2,3\}$ and $A \cap B = \{\}$.

Therefore, it is not true in general that $A \cup B = A \cap B$.

Proof by Contradiction

Logic:

To prove statement P is *True*, we prove $\neg P$ is *False* instead.

Method:

1. Suppose the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Proof by Contradiction

Proposition: There is no greatest integer.

Proof:

Suppose not. That is, suppose there is a greatest integer N**.**

[We must derive a contradiction.]

Then $N \geq n$ for every integer n. Let $M = N + 1$. Now M is an integer, since it is a sum of integers. Also $M > N$ since $M = N + 1$.
Thus M is an integer that is greater than N. So N is the greatest integer and N is not the greatest integer, which is a **contradiction**.

[This contradiction shows that the supposition is *false*, and hence, that the proposition is *true*.]

Proof by Contradiction

Proposition: The sum of any rational number and any irrational number is irrational.

Proof:

Suppose not.

That is, there is a rational number r and an irrational number s, such that $r + s$ is rational.

[We must derive a contradiction.]

By definition of rational numbers:

$$r = \frac{a}{b} \quad \text{and} \quad \mathrm{r} + s = \frac{c}{d}, \quad \text{for some integers } a, b, c, d, \text{ and } b \neq 0,\ d \neq 0.$$

Then

$$s = \frac{c}{d} - r = \frac{c}{d} - \frac{a}{b} = \frac{bc}{bd} - \frac{ad}{bd} = \frac{bc-ad}{bd}.$$

Since $bc - ad$ and bd are integers, and $bd \neq 0$, s is rational by definition, which contradicts s is an irrational number in the supposition.

[This contradiction shows that the supposition is *false*. Hence, the proposition is true.]

Proof by Contraposition

Logic:

To prove statement “if P then Q”, we prove “if $\neg Q$ then $\neg P$” instead.

Method:

1. Express the statement in the form “if P then Q”.
2. Rewrite this statement in the contrapositive form “if $\neg Q$ then $\neg P$”.
3. Suppose $\neg Q$ is true, and prove $\neg P$ is true.

Proof by Contraposition

Proposition: For all integers n, if n^2 is even then n is even.

Proof:

Suppose n is an odd integer.

[We must show that n^2 is odd.]

By definition of odd, $n = 2k + 1$ for some integer k.
Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
Since $2k^2 + 2k$ is an integer, $n^2 = 2 \times (\text{an integer}) + 1$.
By definition of odd, n^2 is odd [as was to be shown].

Chapter 4: Elementary Number Theory and Methods of Proof. Susanna S. Epp, "Discrete Mathematics with Applications" Fourth Edition.

Proof by Contradiction

Proposition: For all integers n, if n^2 is even then n is even.

Proof (by contradiction):

Suppose not.

That is, there is an integer n such that n^2 is even and n is not even.

[We must derive a contradiction.]

Since n is not even, $n = 2k + 1$ where k is an integer.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Because products and sums of integers are integers, $2k^2 + 2k$ is an integer.

So, $n^2 = 2(an\ integer) + 1$ is an odd number, which contradicts n^2 is even in the supposition.

[This contradiction shows that the supposition is *false*. Hence, the proposition is true.]

Exercise

Prove that for all integers n, (at least) one of n, $n+1$, and $n+2$ is a multiple of 3.

(Hint: either $n = 3q$, or $n = 3q + 1$, or $n = 3q + 2$, where $q \in \mathbb{Z}$)

Proof:

Case 1: If $n = 3q$ where $q \in \mathbb{Z}$, then n itself is a multiple of 3.

Case 2: If $n = 3q + 1$ where $q \in \mathbb{Z}$,
then $n + 2 = 3q + 3 = 3(q + 1)$, so $n + 2$ is a multiple of 3.

Case 3: If $n = 3q + 2$ where $q \in \mathbb{Z}$,
then $n + 1 = 3q + 3 = 3(q + 1)$, so $n + 1$ is a multiple of 3.

Therefore, for all integers $\boldsymbol{n}$, (at least) one of $\boldsymbol{n}$, $\boldsymbol{n+1}$, and $\boldsymbol{n+2}$ is a multiple of $\mathbf{3}$.

Exercise

Prove the following statement:
If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Proof:

Suppose: neither of the numbers is greater than 10.

Let $0 < r \leq 10$ and $0 < s \leq 10$ be the two positive real numbers.

[We must show that their product is **not** greater than 100.]

Since s is positive, multiply both sides of $r \leq 10$ by s, we get

$$r \cdot s \leq 10 \cdot s$$

Multiply both sides of $s \leq 10$ by 10, we get

$$10 \cdot s \leq 10 \cdot 10 = 100$$

Since $\leq$ is transitive, we get $r \cdot s \leq 100$ [as was to be shown].