Proof Methods and Strategy

Section 1.8

Proof by Cases

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

- Use the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow$$
$$[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

- Each of the implications $p_i \rightarrow q$ is a *case*.

Proof by Cases

Example: Let $a \,@\, b = \max\{a, b\} = a$ if $a \geq b$, otherwise $a \,@\, b = \max\{a, b\} = b$.

Show that for all real numbers a, b, c

$$(a \,@ b) \,@\, c = a \,@\, (b \,@\, c)$$

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases

Case 1: $a \geq b \geq c$

$(a \mathbin{@} b) = a$, $a \mathbin{@} c = a$, $b \mathbin{@} c = b$

Hence $(a \mathbin{@} b) \mathbin{@} c = a = a \mathbin{@} (b \mathbin{@} c)$

Therefore the equality holds for the first case.

Similarly for the remaining 5 cases.

(nobody wants to read pages and pages of almost identical arguments, therefore it is often sufficient to prove one case and state that the other cases can be shown to hold similarly…but this must be really true!) ◀

Without Loss of Generality

Example: Show that if x and y are integers and both $x*y$ *and* $x+y$ are even, then both x and y are even. Or symbolically:

$$\forall x \forall y \left[E(x+y) \wedge E(x*y) \rightarrow E(x) \wedge E(y) \right]$$

Proof: Use a proof by contraposition.

$$\forall x \forall y \left[\neg \left(E(x) \wedge E(y) \right) \rightarrow \neg \left(E(x+y) \wedge E(x*y) \right) \right]$$

$$\forall x \forall y \left[\neg E(x) \vee \neg E(y) \rightarrow \neg E(x+y) \vee \neg E(x*y) \right]$$

$$\forall x \forall y \left[O(x) \vee O(y) \rightarrow O(x+y) \vee O(x*y) \right]$$

Suppose x and y are not both even. Then, one or both are odd. *Without loss of generality*, assume that x is odd. Then $x = 2m + 1$ for some integer m.

Case 1: y is even. Then $y = 2n$ for some integer n, we have

$x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

$x * y = (2m + 1) * 2n = 4mn + 2n = 2(2mn+n)$ is even.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so

$x + y = (2m + 1)+(2n + 1) = 2m + 2n + 2 = 2(m + n + 1)$ is even.

$x * y = (2m + 1)\ (2n + 1) = 2(2m * n + m + n) + 1$ is odd.

We only cover the case where x is odd because the case where y is odd is similar (because both * and + are commutative). The use phrase *without loss of generality* (WLOG) indicates this.

Existence Proofs

- Proof of theorems of the form $\exists x P(x)$.
- **Constructive** existence proof:
  - Find an explicit value of *c*, for which *P(c)* is true.
  - Then $\exists x P(x)$ is true by *Existential Generalization* (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3 \quad \blacktriangleleft$$

Counterexamples

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$.
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a *c* such that ¬*P*(*c*) is true or *P*(*c*) is false.
- In this case *c* is called a *counterexample* to the assertion $\forall x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Universally Quantified Assertions

- To prove theorems of the form $\forall x P(x)$,assume *x* is an arbitrary member of the domain (UI) and show that *P*(*x*) must be true. Using UG it follows that $\forall x P(x)$.

  Example: An integer *x* is even if and only if x^2 is even.

  Solution: The quantified assertion is

  $\forall x$ [*x* is even $\leftrightarrow$ x^2 is even]

  We assume *x* is arbitrary.

  Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

  So, we have two cases to consider. These are considered in turn.

Continued on next slide →

Universally Quantified Assertions

Case 1. We show that if x is even then x^2 *is* even using a direct proof (the *only if* part or *necessity*).

If x is even then $x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2 on next slide →

Universally Quantified Assertions

Case 2. We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even.

If x is not even then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

which is odd and hence not even. This completes the proof of case 2.

Since x was arbitrary, the result follows by UG.

Therefore we have shown that x is even if and only if x^2 is even.