INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAIʻI at MĀNOA

Ch 1.8: Proof Methods and Strategy

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Proof by Cases

- A proof by cases shows that a proposition is true by considering different cases separately.
- Let n be an non-negative integer.
- Aims to prove conditional statement to of the form:

$$(P_1 \vee P_2 \vee \cdots \vee P_n) \Rightarrow Q$$

- By proving each of the cases n cases:

$$(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q) \wedge \cdots \wedge (P_n \Rightarrow Q)$$

Proof by Cases

- Proposition: If n is an integer such that $n \neq 0$, then $n^2 - n$ is even.

Proof by Cases

- Proposition: If n is an integer such that $n \neq 0$, then $n^2 - n$ is even.
- Proof:

Proof by Cases

- Proposition: If n is an integer such that $n \neq 0$, then $n^2 - n$ is even.
- Proof: Let n be an arbitrary integer such that $n \neq 0$.

Proof by Cases

- Proposition: If n is an integer such that $n \neq 0$, then $n^2 - n$ is even.
- Proof: Let n be an arbitrary integer such that $n \neq 0$.

  Case 1: Assume n is even so that for some integer k, $n = 2k$.

$$
\begin{aligned}
n^2 - n &= (2k)^2 - 2k \\
&= 4k^2 - 2k \\
&= 2(2k^2 - k) \\
&= 2k', \text{ for some integer } k' = 2k^2 - k\ .
\end{aligned}
$$

  By definition of an even integer, $n^2 - n$ is even.

Proof by Cases

- Proposition: If n is an integer such that $n \neq 0$, then $n^2 - n$ is even.
- Proof: Let n be an arbitrary integer such that $n \neq 0$.

  Case 2: Assume n is odd so that for some integer k, $n = 2k + 1$.

$$\begin{aligned}
n^2 - n &= (2k+1)^2 - (2k+1) \\
&= 4k^2 + 4k + 1 - 2k - 1 \\
&= 4k^2 + 2k \\
&= 2(2k^2 + k) \\
&= 2k', \text{ for some integer } k' = 2k^2 + k\ .
\end{aligned}$$

  By definition of an even integer, $n^2 - n$ is even. ■

Exhaustive Proof

- An exhaustive proofs are used to prove propositions with a relatively small number of cases.
- Individually prove each case with specific values.

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.

- Proof:

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.
- Proof: Let n be an arbitrary positive integer such that $n \leq 4$.

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.
- Proof: Let n be an arbitrary positive integer such that $n \leq 4$.

  Case 1: Let $n = 1$.

$$(n+1)^3 \geq 3^n$$
$$\Rightarrow 2^3 \geq 3^1$$
$$\Rightarrow 8 \geq 3 .$$

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.

- Proof: Let n be an arbitrary positive integer such that $n \leq 4$.

  Case 2: Let $n = 2$.

$$(2+1)^3 \geq 3^n$$

$$\Rightarrow 3^3 \geq 3^2$$

$$\Rightarrow 27 \geq 9 .$$

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.

- Proof: Let n be an arbitrary positive integer such that $n \leq 4$.

  Case 3: Let $n = 3$.

$$(3+1)^3 \geq 3^n$$
$$\Rightarrow 4^3 \geq 3^3$$
$$\Rightarrow 64 \geq 27\ .$$

Exhaustive Proofs

- Proposition: If n is a positive integer such that $n \leq 4$ then $(n+1)^3 \geq 3^n$.

- Proof: Let n be an arbitrary positive integer such that $n \leq 4$.

  Case 4: Let $n = 4$.

$$(4+1)^3 \geq 4^n$$

$$\Rightarrow 5^3 \geq 3^4$$

$$\Rightarrow 125 \geq 81 . \blacksquare$$

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

Proof by Cases

- Proposition: Show that for all real numbers x and y,

$$|xy| = |x||y|$$

- Proof:

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$
- Proof: Let x and y be arbitrary real numbers.

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$
- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$.

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

  Case 1: Assume $x \geq 0$ and $y \geq 0$.
  Case 2: Assume $x \geq 0$ and $y < 0$.
  Case 3: Assume $x < 0$ and $y \geq 0$.
  Case 4: Assume $x < 0$ and $y < 0$.

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

  Case 1: Assume $x \geq 0$ and $y \geq 0$. Since xy is non-negative,
$$|xy| = xy = |x||y| \; .$$

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

  Case 2: Assume $x \geq 0$ and $y < 0$. Since xy is negative,
$$|xy| = -xy = x(-y) = |x||y| \ .$$

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

  Case 3: Assume $x < 0$ and $y \geq 0$. Since xy is negative,
$$|xy| = -xy = (-x)y = |x||y| \ .$$

Proof by Cases

- Proposition: Show that for all real numbers x and y,
$$|xy| = |x||y|$$

- Proof: Let x and y be arbitrary real numbers. Note that for any real number a, if $a \geq 0$ then $|a| = a$. Similarly, if $a < 0$ then $|a| = -a$. We consider 4 cases.

  Case 4: Assume $x < 0$ and $y < 0$. Since xy is non-negative,
$$|xy| = xy = (-x)(-y) = |x||y| . \blacksquare$$

Without Loss of Generality

- In the previous proposition (Slide 6), Case 2 and Case 3 are almost identical
  - Roles of x and y are switched based on which variable is negative.

Case 2: Assume $x \geq 0$ and $y < 0$. Since xy is negative,

$$|xy| = -xy = x(-y) = |x||y| .$$

Case 3: Assume $x < 0$ and $y \geq 0$. Since xy is negative,

$$|xy| = -xy = (-x)y = |x||y| .$$

Without Loss of Generality

- The phrase "*without loss of generality*" is used in proofs to simplify arguments by focusing on one specific case, with the understanding that the remaining case(s) follow the same reasoning
- Used frequently for:
  - Symmetric cases
  - Redundant cases

Without Loss of Generality

- We can combine Case 2 and Case 3

  Case 2: Without loss of generality, assume $x \geq 0$ and $y < 0$. Since xy is negative,

$$|xy| = -xy = x(-y) = |x||y| .$$

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.
- Proof:

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof:

  Hint #1: Use a proof by contraposition. Recall that

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$$

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof:

Hint #1: Use a proof by contraposition. Recall that

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$$

Hint #2: Use proof by cases and “without loss of generality”

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof: Let x and y be arbitrary integers. We proceed with proof by contraposition. Assume x and y are not both even. That is, either x or y is odd or both are (but not both even). Without loss of generality, assume x is odd such that $x = 2a + 1$ for some integer a.

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof: Let x and y be arbitrary integers. We proceed with proof by contraposition. Assume x and y are not both even. That is, either x or y is odd or both are (but not both even). Without loss of generality, assume x is odd such that $x = 2a + 1$ for some integer a.
  Case 1: Assume y is even so that there exists an integer b such $y = 2b$.

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof: Let x and y be arbitrary integers. We proceed with proof by contraposition. Assume x and y are not both even. That is, either x or y is odd or both are (but not both even). Without loss of generality, assume x is odd such that $x = 2a + 1$ for some integer a.
  Case 1: Assume y is even so that there exists an integer b such $y = 2b$.
  $$\begin{aligned} x + y &= (2a + 1) + (2b) \\ &= 2a + 2b + 1 \\ &= 2(a + b) + 1 \ . \end{aligned}$$
  By definition, $x + y$ is odd.

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof: Let x and y be arbitrary integers. We proceed with proof by contraposition. Assume x and y are not both even. That is, either x or y is odd or both are (but not both even). Without loss of generality, assume x is odd such that $x = 2a + 1$ for some integer a.
  Case 2: Assume y is odd so that there exists an integer b such $y = 2b + 1$.

Exercise

- Proposition: Let x and y be integers. If xy and $x + y$ are both even, then x and y are also both even.

- Proof: Let x and y be arbitrary integers. We proceed with proof by contraposition. Assume x and y are not both even. That is, either x or y is odd or both are (but not both even). Without loss of generality, assume x is odd such that $x = 2a + 1$ for some integer a.
  Case 2: Assume y is odd so that there exists an integer b such $y = 2b + 1$.
  $$\begin{aligned} xy &= (2a + 1)(2b + 1) \\ &= 2ab + 2a + 2b + 1 \\ &= 2(ab + a + b) + 1 \ . \end{aligned}$$
  By definition, xy is odd. ■

Existence Proofs

- An existance proof is used to prove propositions of the form

$$\exists x(P(x))$$

- A constructive existance proof aims to find an element a such that $P(a)$ is true
- A nonconstructive existance proof uses indirect proof methods such as proof by contradiction

Existence Proofs

- Proposition: There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Existence Proofs

- Proposition: There exists a positive integer that can be written as the sum of cubes of positive integers in two different ways.

- Proof:

$$1729 = 1000 + 729 = 10^3 + 9^3$$
$$= 1728 + 1 = 12^3 + 1^3 .$$

  We showed that 1729 can be written as the sum of cubes of positive integers in two different ways. ■

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.
- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

  Case 1: Assume $\sqrt{2}^{\sqrt{2}}$ is rational.

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

  Case 1: Assume $\sqrt{2}^{\sqrt{2}}$ is rational. Then we have shown that for $x = \sqrt{2}$ and $y = \sqrt{2}$, $x^y = \sqrt{2}^{\sqrt{2}}$ is rational.

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

  Case 2: Assume $\sqrt{2}^{\sqrt{2}}$ is irrational.

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

  Case 2: Assume $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$,

Existence Proofs

- Proposition: There exists irrational number x and y such that x^y is rational.

- Proof: Recall that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

  Case 2: Assume $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$,

$$
\begin{aligned}
x^y &= \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} \\
&= \left(\sqrt{2}^{\sqrt{2}\cdot\sqrt{2}}\right) \\
&= \sqrt{2}^{2} \\
&= 2\ , \text{ which is rational. } \blacksquare
\end{aligned}
$$

Uniqueness Proofs

- A uniqueness proof is used to prove propositions of the form

$$\exists! x(P(x))$$

- Need to show
  - *Existence:* an element x with $P(x)$ exists.
  - *Uniqueness:* If element x and y with $P(x)$ and $P(y)$ exists, then x and y are the same element, i.e.,

$$x = y$$

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.
- Proof: Assume a and b are arbitrary real numbers such that $a \neq 0$.

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.
- Proof: Assume a and b are arbitrary real numbers such that $a \neq 0$. Let r be a real number such that $r = -b/a$.

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Assume a and b are arbitrary real numbers such that $a \neq 0$. Let r be a real number such that $r = -b/a$. Notice that,

$$\begin{aligned} ar + b &= a(-b/a) + b \\ &= -b + b \\ &= 0\ . \end{aligned}$$

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Assume a and b are arbitrary real numbers such that $a \neq 0$. Let r be a real number such that $r = -b/a$. Notice that,

$$\begin{aligned} ar + b &= a(-b/a) + b \\ &= -b + b \\ &= 0\ . \end{aligned}$$

Therefore, an element r that satisfies the proposition exists.

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Let s be an arbitrary real number such that $as + b = 0$.

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Let s be an arbitrary real number such that $as + b = 0$.

$$ar + b = as + b$$
$$\Rightarrow ar = as$$
$$\Rightarrow r = s . \blacksquare$$

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Let s be an arbitrary real number such that $as + b = 0$.

$$ar + b = as + b$$
$$\Rightarrow ar = as$$
$$\Rightarrow r = s . \blacksquare$$

Question: Is there another way to show that $r = s$?

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Let s be an arbitrary real number such that $as + b = 0$.

$$ar + b = as + b$$
$$\Rightarrow ar = as$$
$$\Rightarrow r = s . \blacksquare$$

- *Question:* Is there another way to show that $r = s$?
  - *Yes!* Using systems of linear equations

Uniqueness Proofs

- Proposition: If a and b are real numbers such that $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- Proof: Let s be an arbitrary real number such that $as + b = 0$.

$$\begin{array}{r} (ar + b = 0) \\ -\,(as + b = 0) \\ \hline a(r - s) = 0 \\ r - s = 0 \\ r = s\,. \blacksquare \end{array}$$

Exercise

- Proposition: Let x and y be real numbers.

$$\mathtt{max}(x, y) + \mathtt{min}(x, y) = x + y$$

Exercise

- Proposition: Let x and y be real numbers.

$$\texttt{min}(x, y) = \frac{x + y - |x - y|}{2}$$

and

$$\texttt{max}(x, y) = \frac{x + y + |x - y|}{2}$$

Exercise

- Proposition: Let x and y be real numbers. Prove the triangle inequality

$$|x| + |y| \geq |x + y|$$