CSCI 2824: Discrete Structures

Lecture 11: Proof Methods and Strategies

Rachel Cox

Department of Computer Science

Midterm Exam 1

Tuesday Oct. 1

6:30 - 8:00 pm

Location TBA

Makeup Exam

Wednesday Oct. 2

6:00 - 7:30 pm

Location: ECES 112

Accommodations:

Tuesday Oct. 1

6:30 — depends

Location: ECES 112

Rules of Inference – Fallacies

Fallacy of Denying the Hypothesis

$$\begin{array}{l} p \to q \\ \neg p \\ \hline \therefore \neg q \end{array}$$

Note that if $p = F$ and $q = T$, then both of the premises are true while the conclusion is false.

p	q	$p \to q$	$\neg p$	$(p \to q) \land \neg p$	$\neg q$	$((p \to q) \land \neg p) \to \neg q$
T	T	T	F	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

A valid argument form means that whenever the premises are true, the conclusion must also be true.

Proof Methods & Strategies– Proof by Cases

Example: Suppose you want to prove $p \rightarrow q$ if p is some statement that is true for all CU undergraduates.

"If a *student studies*, then *they are cool*."

Suppose p: If a student studies.

what if we divide p into cases:

p_1: A freshman studies

p_2: A sophomore studies

p_3: A junior studies

p_4: A senior studies

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge (p_4 \rightarrow q) \equiv (p_1 \vee p_2 \vee p_3 \vee p_4) \rightarrow q$$

Proof Methods & Strategies– Proof by Cases

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

$$\begin{array}{r} 8 \\ 5\overline{)40} \\ -40 \\ \hline 0 \end{array} \qquad \begin{array}{r} 8 \\ 5\overline{)41} \\ -40 \\ \hline 1 \end{array} \qquad \begin{array}{r} 8 \\ 5\overline{)42} \\ -40 \\ \hline 2 \end{array} \qquad \begin{array}{r} 8 \\ 5\overline{)43} \\ -40 \\ \hline 3 \end{array} \qquad \begin{array}{r} 8 \\ 5\overline{)44} \\ -40 \\ \hline 4 \end{array}$$

$40 = 5 \cdot 8$ $\quad 41 = 5 \cdot 8 + 1$ $\quad 42 = 5 \cdot 8 + 2$ $\quad 43 = 5 \cdot 8 + 3$ $\quad 44 = 5 \cdot 8 + 4$

Pf: Case 1: Suppose that $n = 5k + 1$ for some integer k.

$$n^2 = (5k+1)^2$$
$$= 25k^2 + 10k + 1$$
$$n^2 = 5(5k^2 + 2k) + 1$$

Since $5k^2 + 2k$ must be an integer → This implies that n^2 leaves a remainder of 1 when divided by 5.

Proof Methods & Strategies– Proof by Cases

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

Case 2: Now suppose when we divide n by 5, it leaves a remainder of 2. let $n = 5k + 2$ for some integer k

$$n^2 = (5k+2)^2$$
$$= 25k^2 + 20k + 4$$
$$= 5(5k^2+4k) + 4$$

Since $5k^2+4k$ is some integer, we've shown that n^2 divided by 5 leaves a remainder of 4.

Proof Methods & Strategies– Proof by Cases

Example: Prove that if n is any integer not divisible by 5, then n^2 leaves a remainder of 1 or 4 when divided by 5.

Case 3:

$$n = 5k + 3$$
$$n^2 = (5k+3)^2$$
$$= 25k^2 + 30k + 9$$
$$= 25k^2 + 30k + 5 + 4$$
$$= 5(5k^2 + 6k + 1) + 4$$

This implies a remainder of 4.

Case 4:

$$n = 5k + 4$$
$$n^2 = (5k + 4)^2$$
$$= 25k^2 + 40k + 16$$
$$= 25k^2 + 40k + 15 + 1$$
$$= 5(5k^2 + 8k + 3) + 1$$

This implies a remainder of 1

Thus n^2 leaves a remainder of 1 or 4. ∎

Proof Methods & Strategies– Proof by Cases

Example: Let's open the hood on the logic here.

Proof by cases logic: We're using the fact (which we still need to show) that

$$\underbrace{(p_1 \vee p_2 \vee p_3 \vee p_4)}_{\text{cover all } p} \rightarrow q \;\equiv\; (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge (p_4 \rightarrow q)$$

Proof By cases

So let's prove this logical equivalence.

$$(p_1 \vee p_2 \vee p_3 \vee p_4) \rightarrow q \equiv \neg(p_1 \vee p_2 \vee p_3 \vee p_4) \vee q \quad \text{RBI}$$

$$\equiv (\neg p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge \neg p_4) \vee q \quad \text{Demorgans}$$

This is what we are trying to prove overall.

$$\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge (\neg p_3 \vee q) \wedge (\neg p_4 \vee q) \quad \text{Distrib.}$$

$$\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q) \wedge (p_4 \rightarrow q) \quad \text{RBI}$$

Proof Methods & Strategies– Proof by Cases

Proof Methods & Strategies– Proof by Construction

Example: Suppose you have two water jugs: one holds 5 gallons and the other holds 3 gallons. Assume you have an endless supply of water. Prove that an algorithm exists that allows you to measure out exactly 4 gallons of water just by transferring water between the two jugs (or pouring it down the drain, if that helps).

Proof Methods & Strategies– Proof by Construction

Example: Suppose you have two water jugs: one holds 5 gallons and the other holds 3 gallons. Assume you have an endless supply of water. Prove that an algorithm exists that allows you to measure out exactly 4 gallons of water just by transferring water between the two jugs (or pouring it down the drain, if that helps).

Proof:

1. Pour 5G into the 5G jug.
2. Pour 3G. from the 5G jug into the 3G jug (leaving 2G in the 5G jug).
3. Pour the 3G in the 3G jug down the drain.
4. Pour the 2G from the 5G jug into the 3G jug.
5. Pour 5G into the 5G jug.
6. Pour 1G from the 5G jug into the 3G jug.

At this point, the 3G jug is full and **5G jug has 4G in it.**□

Proof Methods & Strategies

Proof by Cases (Exhaustive Proof): benefit is that we may have more information about each specific case than we would have about just some general n.

Proof by Construction (Existence Proof): prove the existence of a solution by explicitly constructing it.

Existence and Uniqueness Proofs:

1) Show existence by construction
2) Show uniqueness by supposing there are two such objects that exist but then show they must be equal to each other.

Proof Methods & Strategies

$\exists !$ "there exists a unique"

Example: Show that if n is an odd integer, then there **exists** a **unique** integer k such that n is the sum of k - 2 and k + 3.

1. show existence.
2. show uniqueness.

Pf: First we show existence.
Assume n is an odd integer.
Let $n = 2k+1$ for some integer k.

$$n = k + k + 1$$
$$= k + k + 3 - 2$$
$$= k+3 + k-2$$

We've shown that an integer exists such that $n = (k+3) + (k-2)$.

Proof Methods & Strategies

Example: Show that if *n* is an odd integer, then there **exists** a **unique** integer *k* such that *n* is the sum of *k* - 2 and *k* + 3.

Next we show that k is unique. To demonstrate this, suppose k is not unique.

Let $n = (k_1 - 2) + (k_1 + 3)$ and $n = (k_2 - 2) + (k_2 + 3)$

Since $n = n$

$$(k_1 - 2) + (k_1 + 3) = (k_2 - 2) + (k_2 + 3)$$

$$2k_1 + 1 = 2k_2 + 1$$

$$2k_1 = 2k_2$$

$$k_1 = k_2$$

Thus $\exists!\, k$ such that n is the sum of $k-2$ + $k+3$ $\blacksquare$

Proof Methods & Strategies – Conditional Proof (specific kind of direct proof)

Example: Suppose that anyone who is orange is an oompa-loompa. Let the domain be all people. Prove that all orange factory workers are oompa-loompas.

Let $F(x)$ denote "x is a factory worker"

Let O(x) denote "x is orange"

Let $OL(x)$ denote "x is an oompa-loompa"

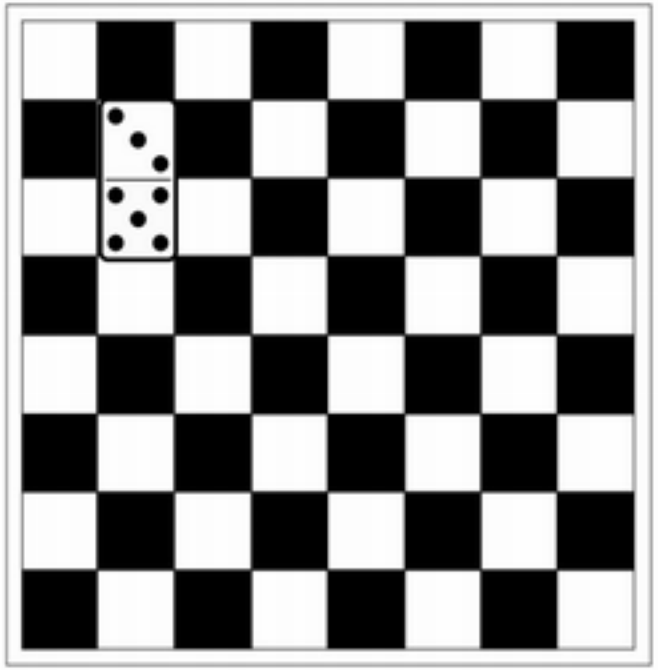
Proof Methods & Strategies – Conditional Proof (specific kind of direct proof)

Example: Suppose that anyone who is orange is an oompa-loompa. Let the domain be all people. Prove that all orange factory workers are oompa-loompas.

	Step	Justification
1.	$\forall x(O(x) \longrightarrow OL(x))$	premise
2.	$O(a) \longrightarrow OL(a)$	Universal instantiation with arbitrary a
3.	$O(a) \wedge F(a)$	Assumption for conditional proof
4.	$O(a)$	Simplification of (3)
5.	$OL(a)$	Modus ponens of (2), (4)
6.	$(O(a) \cancel{\longrightarrow} \wedge F(a)) \longrightarrow OL(a)$	Conditional proof (2)-(5)
	$\therefore \forall x\,[(F(x) \wedge O(x)) \longrightarrow OL(x)]$	

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

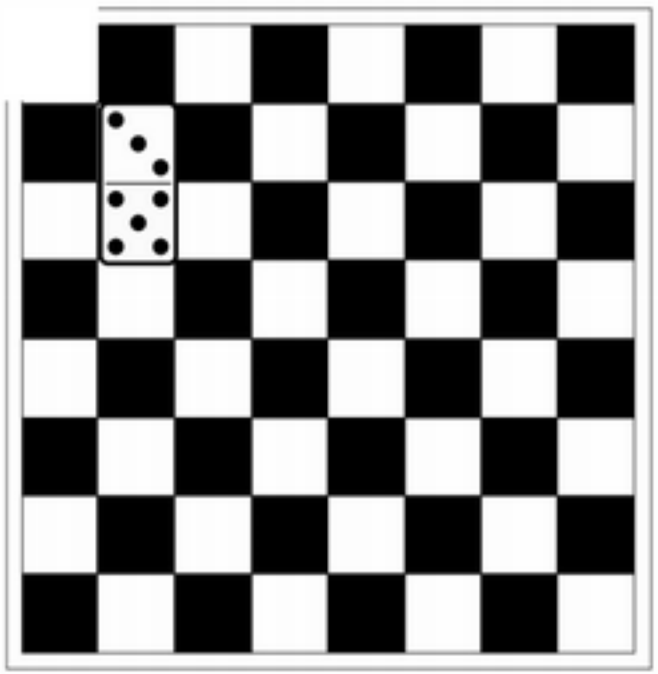
Example: Consider a standard 8x8 chessboard.



Can you completely cover the board in dominos that are the size of two squares?

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

Example: What about if we removed one of the corners?



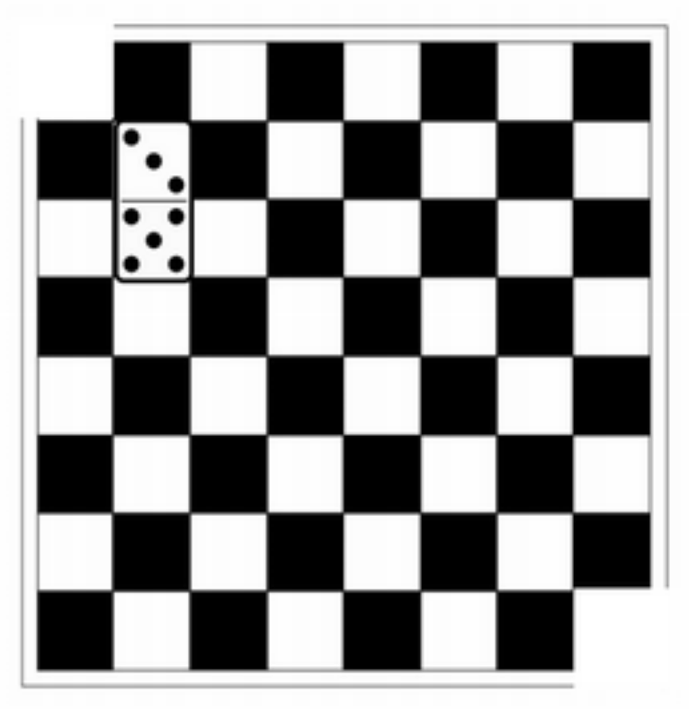
No!

Each domino must cover 1 white square and 1 black square and we now have 1 less white square.

Can't be done.

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

Example: What about if we removed the opposite corner as well?



No!

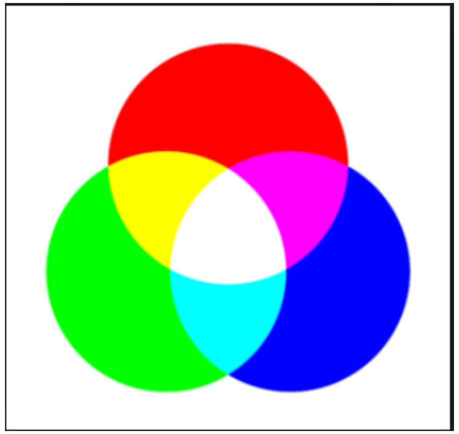
Proof Methods & Strategies

Recap:

- ❖ Proof by cases (exhaustive)
- ❖ Proof by construction (existence) and the typical way for proving uniqueness (suppose two things exist and show they must actually be the same thing.
- ❖ Disproving with a Counterexample

Next time:

- ❖ Sets!



Extra Practice

Example 1: Show that if a, b, and c are real numbers with $a \neq 0$ then there **exists** a **unique** solution x to the equation $ax + b = c$

Example 2: Prove that for real numbers x and y,

$$\max(x, y) + \min(x, y) = x + y$$

Solutions

Example 1: Show that if a, b, and c are real numbers with $a \neq 0$ then there **exists** a **unique** solution x to the equation $ax + b = c$

Existence: Solve for x

$ax + b = c \Rightarrow x = \dfrac{b - c}{a}$ (where here we know that $a \neq 0$)

Uniqueness: Assume x and y are both solutions to the system, then

$$ax + b = c = ay + b \Rightarrow ax + b = ay + b \Rightarrow ax = ay \Rightarrow x = y$$

Since x and y are necessarily the same number, it follows that our solution x is unique

Example 2: Prove that for real numbers x and y,
$\max(x, y) + \min(x, y) = x + y$

Case 1: Assume $x \geq y$. Then $\max(x, y) = x$ and $\min(x, y) = y$
(Here we realize that if $x = y$ then we can decide to choose either)

Thus $\max(x, y) + \min(x, y) = x + y$

Case 2: Assume $x < y$. Then $\max(x, y) = y$ and $\min(x, y) = x$

Thus $\max(x, y) + \min(x, y) = y + x = x + y$

Since the cases cover all possible combinations of x and y and both yield the conclusion, we are done.