101100001000 101100001000 101100001000 101100001000 101100001000

CSCI 2824: Discrete Structures

Lecture 11: Proof Methods and Strategies

Rachel Cox

Department of Computer Science

101100001000 101100001000 101100001000 101100001000 101100001000

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 instead we break this into cases by class

p_1: x is a freshman who studies

$\vdots$

p_4: x is a senior who studies

Want to show $(p_1 \vee p_2 \vee p_3 \vee p_4) \rightarrow q$

Actually showing

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

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.

Scratch work:

$$5\overline{)42}, \quad 42 - 40 = 2, \quad \text{quotient } 8$$

$$\frac{42}{5} = 8 + \frac{2}{5}$$

So a general n:

$$\underbrace{\frac{n}{5} = k + \frac{\text{Remainder}}{5}}$$

The remainder must be 1, 2, 3, or 4

That means $n = 5k + 1$

$n = 5k + 2$

$n = 5k + 3$

or $n = 5k + 4$

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.

Pf: Case 1: let $n = 5k+1$

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

$$n^2 = 5(5k^2+2k)+1$$
$$\frac{n^2}{5} = (5k^2+2k) + \frac{1}{5}$$
Side note

So 1 is the remainder.

Case 2: let $n = 5k+2$

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

So 4 is the remainder.

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 : $n = 5k + 3$

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

4 is the remainder.

Case 4 : $n = 5k + 4$

$$n^2 = 5(5k^2 + 8k + 3) + 1$$

1 is the remainder.

We've exhausted all possible cases, thus the claim holds. ∎

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

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

So let's prove this logical equivalence.

Proof Methods & Strategies– Proof by Cases

There's not necessarily 4 cases.

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

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

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

distrib.

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

This is what we do in a 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.

$\exists !$ means there exists a unique . .

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.

Idea is to show that such a K exists.
Then show that K must be unique.

Proof: Proof of Existence
Suppose n is odd.
Let $n = 2a+1 = K-2 + K+3$

$$2a+1 = 2K+1$$

$$a = K$$

So $n = 2K+1$, thus our $K = \frac{n-1}{2}$.

Proof Methods & Strategies

$0 \cdot x = 0$

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.

Proof of Uniqueness

Suppose there are two such integers.

Assume there is a k such that

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

But also assume there is an m such that

$$n = m-2+m+3$$

Then $k-2+k+3 = m-2+m+3$

$$2k+1 = 2m+1$$

$$2k = 2m \qquad k = m$$

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"

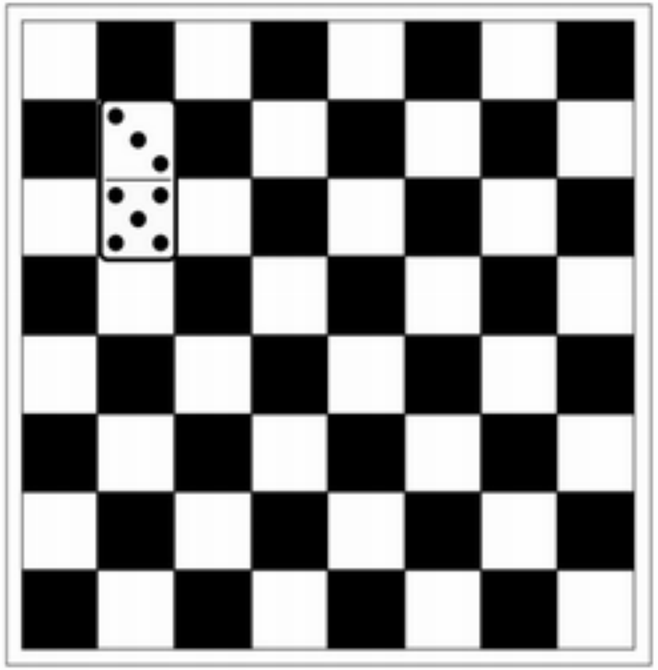
Proof Methods & Strategies – Conditional Proof (specific kind of direct proof)

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.	$\forall x\,(O(x) \to OL(x))$	premise
2.	$O(a) \to OL(a)$	universal instantiation with arbitrary a
3.	$O(a) \land F(a)$	Assumption for conditional proof
4.	$O(a)$	Simplification of (3)
5.	$OL(a)$	modus ponens (2), (4)
6.	$(O(a) \land F(a)) \to OL(a)$	conditional proof (2) – (5)
	$\therefore \forall x\,[(F(x) \land O(x)) \to OL(x)]$	existential generalization of (6)

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

Example: Consider a standard 8x8 chessboard.

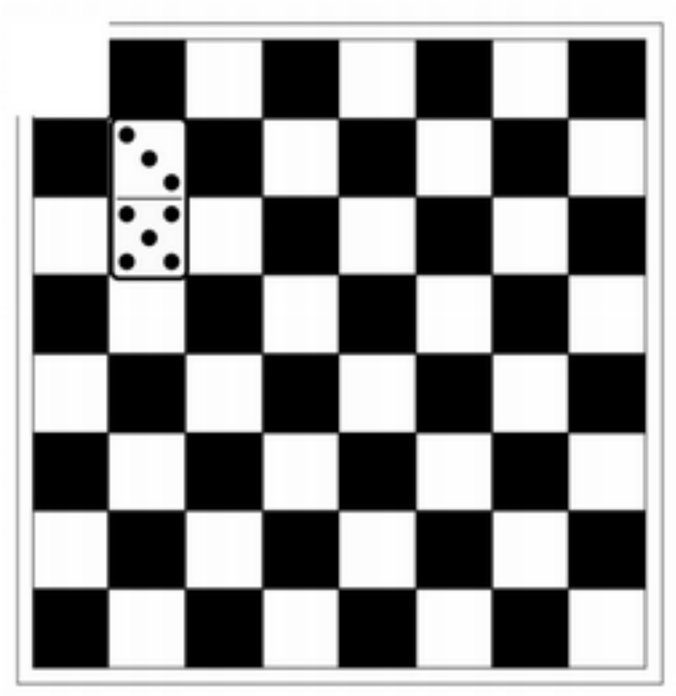


Can you completely cover the board in dominos that are the size of two squares?

yes, this can be done

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

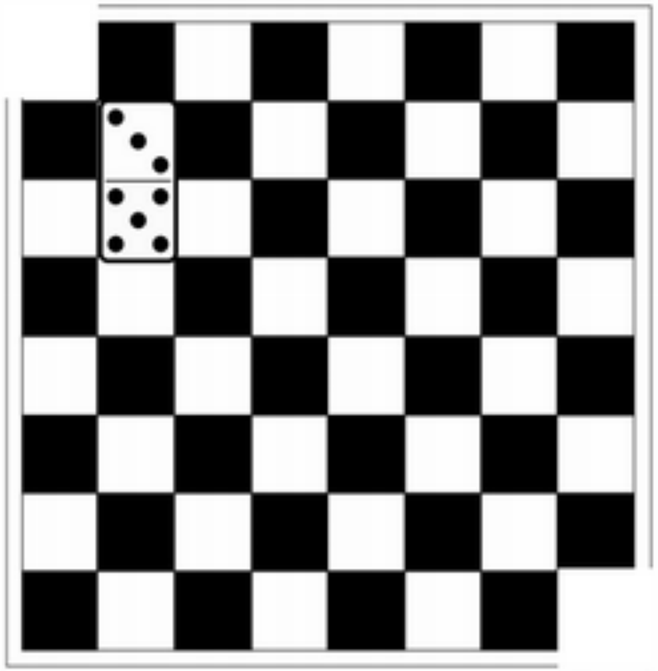
Example: What about if we removed one of the corners?



No! There is an odd number of tiles

Proof Methods & Strategies – Disproving Things / Finding a Counterexample

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



Each domino cover a black and white square, we are short 2 white squares.

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!