## CSE 417 Autumn 2025

# Lecture 3: Proof Techniques

Nathan Brunelle

# Concept check quizzes

Many students haven’t done it yet 🙁

Remember: unlimited submissions, and are marked “incomplete” ***until you get every question right***.

**One-time extension** for everyone until **11:59pm tonight**!

Be sure to get those in on time going forward.

# Homework 1

HW 1 due this Friday at 11:59pm.

- **Problem 1 (Grading ChatGPT):** Read ChatGPT's response to a question about stable matchings, and explain where the LLM made mistakes.

- **Problem 2 (Business profit):** Write a super simple algorithm for a basic task, and prove its correctness (today's lecture!)

# Todo

- **Homework 1 due this Friday at 11:59pm**
- **Reading + Concept checks for each lecture!**

# Proof writing practice

# Proof Techniques

- **Claim:** If property P is true, then property Q is true.
- **Direct proof:** Start with statement “P is true”, then write down a sequence of consequences until reaching “Q is true”.
- **Indirect Proof (by contrapositive):** Start with statement “Q is false”, then write down a sequence of consequences until reaching “P is false”.
- **Contradiction:** Start with the statement “P is true and W is false”, then write a sequence of consequences until reaching a statement that is obvious impossible.
- **Counterexample (for proving false):** Give one thing that has property P but not Q.
- **Cases:** If there are multiple ways for property P to be true, you can consider each different way separately.

# Let’s Practice! (Example 1)

# Example 1

- **Claim:** If $n$ and $m$ are both odd, then $n + m$ is even.

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $n$ and $m$ are both odd<br><br>**End with:** $n + m$ is even | **Start with:** $n + m$ is odd<br><br>**End with:** at least one of $n$ and $m$ is even | **Start with:** $n$, $m$, and $n + m$ are all odd<br><br>**End with:** something that's clearly wrong | Find an example of odd $n$ and $m$ such that $n + m$ is also odd. |

- Do you think the statement is true or false?
- Which strategy seems easiest to you?

# Example 1: Direct proof

**Claim:** If $n$ and $m$ are both odd, then $n + m$ is even.

**Proof:** suppose $n$ and $m$ are both odd

# Example 1: Indirect proof

**Claim:** If $n$ and $m$ are both odd, then $n + m$ is even.

**Proof:** Suppose $n + m$ is odd

# Example 1: Proof by Contradiction

**Claim:** If $n$ and $m$ are both odd, then $n + m$ is even.

**Proof:** suppose, towards reaching a contradiction, that $n$, $m$, and $n + m$ are all odd

# Let’s Practice! (Example 2)

# Example 2

- **Claim:** If $n$ and $m$ are both integers, then $n^2 - 4m \neq 2$

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $n$ and $m$ are both integers<br><br>**End with:** $n^2 - 4m \neq 2$ | **Start with:** $n^2 - 4m \neq 2$<br><br>**End with:** at least one of $n$ and $m$ is not an integer | **Start with:** $n$ and $m$ are integers such that $n^2 - 4m = 2$<br><br>**End with:** something that's clearly wrong | Find an example of integers $n$ and $m$ such that $n^2 - 4m = 2$. |

- Do you think the statement is true or false?

- Which strategy seems easiest to you?

# Example 2: Direct proof

**Claim:** If $n$ and $m$ are both integers, then $n^2 - 4m \neq 2$

**Proof:** suppose $n$ and $m$ are both integers

# Example 2: Indirect proof

**Claim:** If $n$ and $m$ are both integers, then $n^2 - 4m \neq 2$

**Proof:** Suppose $n^2 - 4m = 2$

# Example 2: Proof by Contradiction

**Claim:** If $n$ and $m$ are both integers, then $n^2 - 4m \neq 2$

**Proof:** suppose, towards reaching a contradiction, that we have integers $n$ and $m$ such that $n^2 - 4m = 2$

# Let’s Practice! (Example 3)

# Example 3

- **Claim:** If $4n^3 + 8$ is even then $n$ is even

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $4n^3 + 8$ is even<br><br>**End with:** $n$ is even | **Start with:** $n$ is odd<br><br>**End with:** $4n^3 + 8$ is odd | **Start with:** $n$ is odd and $4n^3 + 8$ is even<br>**End with:** something that's clearly wrong | Find an example of an odd integer $n$ such that $4n^3 + 8$ is even |

- Do you think the statement is true or false?
- Which strategy seems easiest to you?

# Example 3: Indirect proof

**Claim:** If $4n^3 + 8$ is even then $n$ is even

**Proof:** Suppose $n$ is even

# Example 3: Counterexample

**Claim:** If $4n^3 + 8$ is even then $n$ is even

**Proof:** let $n = ???$

# Let’s Practice! (Example 4)

# Example 4

- **Claim:** If $n^3 + 5$ is odd then $n$ is even

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $n^3 + 5$ is odd<br><br>**End with:** $n$ is even | **Start with:** $n$ is odd<br><br>**End with:** $n^3 + 5$ is even | **Start with:** $n$ and $n^3 + 5$ are both odd<br>**End with:** something that's clearly wrong | Find an example of an odd integer $n$ such that $n^3 + 5$ is odd |

- Do you think the statement is true or false?

- Which strategy seems easiest to you?

# Example 4: Direct proof

**Claim:** If $n^3 + 5$ is odd then $n$ is even

**Proof:** suppose $n^3 + 5$ is odd

# Example 4: Indirect proof

**Claim:** If $n^3 + 5$ is odd then $n$ is even

**Proof:** Suppose $n$ is odd

# Example 4: Proof by Contradiction

**Claim:** If $n^3 + 5$ is odd then $n$ is even

**Proof:** suppose, towards reaching a contradiction, that we have an even integer $n$ such that $n^3 + 5$ is even

# Let’s Practice! (Example 5)

# Example 5

- **Claim:** If $nm$ is even then at least one of $n$ and $m$ is even

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $nm$ is even<br><br>**End with:** $n$ is even or $m$ is even (or both) | **Start with:** both $n$ and $m$ are odd<br><br>**End with:** $nm$ is even | **Start with:** $nm$ is even and both of $n$ and $m$ are odd<br>**End with:** something that's clearly wrong | Find an example of an odd integers $n$ and $m$ such that $nm$ is even |

- Do you think the statement is true or false?

- Which strategy seems easiest to you?

# Example 5: Direct proof

**Claim:** If $nm$ is even then at least one of $n$ and $m$ is even

**Proof:** suppose $nm$ is even

# Example 5: Indirect proof

**Claim:** If $nm$ is even then at least one of $n$ and $m$ is even

**Proof:** Suppose $n$ and $m$ are both odd

# Example 5: Proof by Contradiction

**Claim:** If $nm$ is even then at least one of $n$ and $m$ is even

**Proof:** suppose, towards reaching a contradiction, that we have odd integers $n$ and $m$ such that $nm$ is even

# Let’s Practice! (Example 6)

# Example 6

- **Claim:** If $x^2(y^2 - 2y)$ is odd then both $x$ and $y$ are odd

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $x^2(y^2 - 2y)$ is odd<br><br>**End with:** both $x$ and $y$ are odd | **Start with:** at least one of $x$ and $y$ is even<br><br>**End with:** $x^2(y^2 - 2y)$ is even | **Start with:** $x^2(y^2 - 2y)$ is odd and at least one of $x$ or $y$ is even<br>**End with:** something that's clearly wrong | Find pair of integers $x$ and $y$ where at least one is even and $x^2(y^2 - 2y)$ is odd |

- Do you think the statement is true or false?
- Which strategy seems easiest to you?

# Example 6: Direct proof

**Claim:** If $x^2(y^2 - 2y)$ is odd then both $x$ and $y$ are odd

**Proof:** suppose $x^2(y^2 - 2y)$ is odd

# Example 6: Indirect proof

**Claim:** If $x^2(y^2 - 2y)$ is odd then both $x$ and $y$ are odd

**Proof:** Suppose that $x$ is even or $y$ is even

# Example 6: Proof by Contradiction

**Claim:** If $x^2(y^2 - 2y)$ is odd then both $x$ and $y$ are odd

**Proof:** suppose, towards reaching a contradiction, a pair of integers $x$ and $y$ (not both odd) such that $x^2(y^2 - 2y)$ is even

# Let’s Practice! (Example 7)

# Example 7

- **Claim:** If $4n^3 + 8$ is odd then $n$ is even

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| **Start with:** $4n^3 + 8$ is odd<br><br>**End with:** $n$ is even | **Start with:** $n$ is odd<br><br>**End with:** $4n^3 + 8$ is even | **Start with:** $n$ and $4n^3 + 8$ are both odd<br>**End with:** something that's clearly wrong | Find an example of an odd integer $n$ such that $4n^3 + 8$ is odd |

- Do you think the statement is true or false?
- Which strategy seems easiest to you?

# Example 7: Direct Proof

**Claim:** If $4n^3 + 8$ is odd then $n$ is even

**Proof:** Suppose $4n^3 + 8$ is odd

# Example 7: Indirect proof

**Claim:** If $4n^3 + 8$ is odd then $n$ is even

**Proof:** Suppose $n$ is even

# Example 7: Proof by Contradiction

**Claim:** If $4n^3 + 8$ is odd then $n$ is even

**Proof:** suppose, towards reaching a contradiction, that we have an odd integer $n$ such that $4n^3 + 8$ is odd

# Example 7: Counterexample

**Claim:** If $4n^3 + 8$ is even then $n$ is even

**Proof:** let $n = ???$

# Vacuous Truth

- If we have a claim of the form “If property P is true then property Q is true” and it is impossible for property P to be true, the entire statement is actually a true statement!
- We say that statement is “vacuously true”

# Review: What is correctness?

# Review: Correctness

**Algorithm:** A list of unambiguous instructions to solve a class of computational problems

An algorithm is **correct** for a given problem if it has:

1. **Soundness:** Running it never raises exceptions/errors
2. **Termination:** All loops terminate
3. **Validity:** The output meets the problem specification

# Review: Selection sort (1/6)

**Input:** Array $A[1 \dots n]$ of numbers

**Goal:** A permutation of $A$ that is sorted in decreasing order

1. **for** $i = 1, \dots, n$ **do**
2. Let $A[j]$ be the maximum element of $A[i \dots n]$.
3. Swap $A[i]$ and $A[j]$.
4. **return** $A$

# Review: Selection sort (2/6)

**Q:** Explain why “no exceptions” is true for this algorithm.

**A:** Two things:

1. Array access on $\boldsymbol{i}$ is within bounds because $\mathbf{1} \leq \boldsymbol{i} \leq \boldsymbol{n}$ (line 1).
2. Maximum element $\boldsymbol{A}[\boldsymbol{j}]$ exists because $\boldsymbol{i} \geq \mathbf{1}$, so $\boldsymbol{A}[\mathbf{1} \ldots \boldsymbol{i}]$ is nonempty.

**Note:** The concept of “error” in pseudocode is broader than code: whenever you say “let $\boldsymbol{x}$ be the …,” make sure it exists!

**Q:** “loops terminate”?

**A:** For-loops always terminate!

# Selection sort (3/6)

**Q:** What are some loop invariants that will help us show "meets specification"?

**A:** Here are some natural ideas:

1. After every iteration, array $\boldsymbol{A}$ is a permutation of the original.
2. After iteration $\boldsymbol{i}$, subarray $\boldsymbol{A}[\mathbf{1} \ldots \boldsymbol{i}]$ is sorted in decreasing order.

# Selection sort (4/6)

1. After every iteration, array $A$ is a permutation of the original.

*Proof*. **Before the loop starts:** $A$ is unchanged.

**After each iteration:** By the previous iteration, $A$ starts out as a permutation of the original array.

Because we only modify $A$ by swapping elements, it remains a permutation of the original at the end of this iteration.

# Selection sort (5/6)

2. After iteration $\boldsymbol{i}$, subarray $\boldsymbol{A[1 \dots i]}$ is sorted in decreasing order.

*Proof*. **Before the loop starts:** $\boldsymbol{A[1 \dots 0]}$ is empty.

**After each iteration:** By the previous iteration, $\boldsymbol{A[1 \dots i-1]}$ starts out sorted in decreasing order.

To show $\boldsymbol{A[1 \dots i]}$ ends up sorted, we need $\boldsymbol{A[i-1] \geq A[i]}$.

(Then let's look at the code again to see what happens.)

# Selection sort (6/6)

**Input:** Array $A[1 \dots n]$ of numbers

**Goal:** A permutation of $A$ that is sorted in decreasing order

1. **for** $i = 1, \dots, n$ **do**
2. Let $A[j]$ be the maximum element of $A[i \dots n]$.
3. Swap $A[i]$ and $A[j]$.
4. **return** $A$

Stuck because this iteration doesn't give any information about $A[i-1]$!

Instead, *strengthen the loop invariant* to know more about $A[i-1]$.

# Alternative invariant (1/3)

2. After iteration $\boldsymbol{i}$, subarray $\boldsymbol{A}[\mathbf{1} \dots \boldsymbol{i}]$ each index $\boldsymbol{j}$ where $\mathbf{1} \leq \boldsymbol{j} \leq \boldsymbol{i}$ contains the $\boldsymbol{j}$th largest element of $\boldsymbol{A}$.

*Proof*. **Before the loop starts:** $\boldsymbol{A}[\mathbf{1} \dots \mathbf{0}]$ is empty.

**After each iteration:** By the previous iteration, each index of $\boldsymbol{j}$ of $\boldsymbol{A}[\mathbf{1} \dots \boldsymbol{i} - \mathbf{1}]$ contains the $\boldsymbol{j}$th largest element of $\boldsymbol{A}$.

We need to prove that index $\boldsymbol{i}$ contains the $\boldsymbol{i}$th largest element of $\boldsymbol{A}$ after iteration $\boldsymbol{i}$.

# Alternative invariant (2/3)

**After each iteration:** By the previous iteration, each index of $j$ of $A[1 \dots i-1]$ contains the $j$th largest element of $A$.

**To prove that index $i$ also contains the $i$th largest element of $A$ after iteration $i$:**

Lines 2 and 3 of the algorithm guarantee that index $i$ will contain the largest element from $A[i \dots n]$. This means that so long as that value is less than or equal to everything currently in the range $A[1 \dots i-1]$ our invariant holds.

That statement is guaranteed by the previous iteration!

# Alternative Invariant (3/3)

**What we know now**: Every index of $i$ of $A[1 \ldots n]$ contains the $i$th largest element of $A$.

**What we need to show**: At the end of our algorithm, $A$ is in decreasing order.

**Final step**: Show that if every index of $i$ of $A[1 \ldots n]$ contains the $i$th largest element of $A$, then $A$ is in decreasing order.

# Final step

**Claim**: If every index of $i$ of $A[1 \dots n]$ contains the $i$th largest element of $A$, then $A$ is in decreasing order.

**Assumption**: every index of $i$ of $A[1 \dots n]$ contains the $i$th largest element of $A$

**Conclusion**: $A$ is in decreasing order

| Direct Proof | Indirect Proof | Contradiction | Counterexample |
|---|---|---|---|
| Every index $i$ contains he $i$th largest element | $A$ is not in decreasing order | Every index $i$ contains he $i$th largest element and $A$ is not in decreasing order | Find a permutation of $A$ that is not in decreasing order, but every index $i$ contains he $i$th largest element |

# Indirect proof

**Claim**: If $A$ is not in decreasing order then some index of $i$ of $A[1 \dots n]$ does not contain the $i$th largest element of $A$

**Proof**: Suppose that $A$ is not in decreasing order. This means that there is at least one pair of indices $i + 1$ and $i$ such that $\mathrm{A}[i] < A[i + 1]$. Select $i$ so that this is the first such pair.

Since this is the first out-of-order pair, we can conclude that $\mathrm{A}[i]$ is smaller than or equal to all values in the range $\mathbf{A}[1 \dots i - 1]$, and so there are at least $i - 1$ elements greater than or equal to $\mathrm{A}[i]$. Since $\mathrm{A}[i] < A[i + 1]$ as well, there are at least $i$ elements greater than $\mathrm{A}[i]$, so $\mathrm{A}[i]$ is not the $i$th largest element of $A$.

# Contradiction

**Claim**: If every index of $i$ of $A[1 \dots n]$ contains the $i$th largest element of $A$, then $A$ is in decreasing order.

**Proof**: We proceed by contradiction. Suppose we have a permutation of that is not in decreasing order, but every index $i$ contains he $i$th largest element.

Because every index $i$ contains the $i$th largest element, we know that there are not more than $i - 1$ elements that are greater than $\mathrm{A}[i]$.

If $A$ is not in decreasing order. This means that there is at least one pair of indices $i + 1$ and $i$ such that $\mathrm{A}[i] < A[i + 1]$. Select $i$ so that this is the first such pair.

Since this is the first out-of-order pair, we can conclude that $\mathrm{A}[i]$ is smaller than or equal to all values in the range $\mathbf{A}[1 \dots i - 1]$, and so there are at least $i$ elements greater than or equal to $\mathrm{A}[i]$. Since $\mathrm{A}[i] < A[i + 1]$ as well, there are at least $i$ elements greater than $\mathrm{A}[i]$. This contradicts the assumption that index $i$ contains the $i$th largest element.

# Proof writing tips

- Writing proofs often involves failing. If some path seems like a dead end, try at different approach!
- Start by first guessing whether the statement is true or false.
- Next, write out what each proof strategy requires us to demonstrate. Then try to guess at which one seems easiest, start working on that one
- Repeatedly apply definitions of things to re-express statements. Write down all things you can think of that are true and relevant based on those statements
- If you get stuck, transition to another strategy. If you keep getting stuck, return to a previous one
- Proof techniques are not exclusive. You may find that you embed one strategy for one part of a larger proof
- If you’re getting frustrated, come to office hours!

# Final reminders

HW1 released at 11:30am!

I have OH now-12:30pm:

- Meet at front of classroom, we'll walk over together
- CSE (Allen) 214 if you're coming later

Nathan has online OH 12–1pm:

- Link on Canvas/course website
- https://washington.zoom.us/my/nathanbrunelle