6.1200J/18.062J *Mathematics for Computer Science* Tuesday 13th February, 2024
Massachusetts Institute of Technology, Spring 2024
Z. Abel, B. Chapman, E. Demaine revised Tuesday 13th February, 2024

Problem Set 2

- **Due Date:** 11:59pm on **Tuesday 20th February, 2024**
- **Days Covered**: 03 and 04 (including Lecture, Warm-Up, and Recitation)

Problem 1. Outlining Proofs [10 points]

See lecture 02 (or the corresponding lecture notes) for a discussion of outlining proofs, even with only partial information. Practice this skill by outline proofs for each of the "theorems" below as much as you can, using the techniques indicated. Pretend that the underlined words are meaningful but that their precise meanings are not available here. This means your "proofs" will have missing steps that are impossible to complete without definitions for these words, but that's fine — we're interested in the parts of the proof that can be completed *even without knowing or considering* the underlined terms' meanings. You should break down the proof as granularly as you can using just the given information, and at any step that needs additional information, identify the remaining task or tasks using square brackets. The example seen is lecture looks like this:

Theorem: "For every integer n, the number n is fooish precisely when $n+1$ is barsome."

Proof Outline. Suppose n is any integer; we must show $F(n)$ and $B(n+1)$ both imply each other.

To prove $F(n)$ IMPLIES $B(n+1)$, first assume $F(n)$ is true. [TODO: prove $B(n+1)$.]

To prove $B(n+1)$ IMPLIES $F(n)$, instead assume $B(n+1)$ is true. [TODO: prove $F(n)$.] □

(a) [3 pts] Theorem: "Every natural number is tall or wide, but not both." (Proof method: proof by cases.)

(b) [3 pts] Theorem: "There exists a happy natural number between 10 and 1000 that has no happy proper divisors." (Proof method to use: choose 25 as the example.)

(c) [4 pts] Theorem: "There are no devious natural numbers." (Proof method to use: regular induction, with base cases 0 and 1.)

Hint: Be sure to clearly identify your predicate $P(n)$, and to precisely specify any assumptions and/or goals in your base cases and inductive step.

Problem 2. Spotting Errors [15 points]

Define a sequence of integers $(x_1, x_2, x_3, \ldots)$ as follows: $x_1 = 4$, $x_2 = 13$, and for all $i \geq 3$, $x_i = 6x_{i-1} - 8x_{i-2}$. So the sequence begins with $(x_1, x_2, x_3, x_4, \ldots) = (4, 13, 46, 172, \ldots,)$. Our goal is to prove that for all $i \geq 1$, $x_i > 0$.

Addled Abra tries to prove the claim directly by strong induction:

> *Proof.* We'll use strong induction with inductive hypothesis $P(i) :=$ "$x_i > 0$" to prove that $P(i)$ holds for every $i \geq 1$.
>
> Base Cases, $P(1)$ and $P(2)$: $x_1 = 4 > 0$ and $x_2 = 13 > 0$.
>
> Inductive Step: Let's use strong induction, so suppose $i \geq 2$, and we can assume $P(1), P(2), \ldots, P(i)$, i.e., we can assume that $x_1 > 0$, $x_2 > 0$, $\ldots$, $x_i > 0$. We must show $P(i+1)$, i.e., that x_{i+1} is also > 0. Well, $x_{i+1} = 6x_i - 8x_{i-1} > 0 - 8x_{i-1}$, but, uh, ... Huh, I don't think this is working. □

Abra gets points for honesty, and goes to the instructors for help.

(a) [3 pts] Befuddled Brynmor tries to help by proving the claim as follows. What is his mistake?

> *Proof.* We'll use the stronger induction hypothesis $Q(i) :=$ "$x_i \geq 2^i$", using strong induction to show that $Q(i)$ holds for every $i \geq 1$.
>
> Base Cases, $Q(1)$ and $Q(2)$: $x_1 = 4 \geq 2^1$ and $x_2 = 13 \geq 2^2$.
>
> Inductive Step: Suppose $i \geq 2$. Assume $x_k \geq 2^k$ for $1 \leq k \leq i$, and let's prove that $x_{i+1} \geq 2^{i+1}$. Consider $x_{i+1} = 6x_i - 8x_{i-1}$. By the inductive hypothesis know that $x_i \geq 2^i$ and $x_{i-1} \geq 2^{i-1}$. Plug those two inequalities into $x_{i+1} = 6x_i - 8x_{i-1}$ and you get $x_{i+1} \geq 6 \cdot 2^i - 8 \cdot 2^{i-1} = 6 \cdot 2 \cdot 2^{i-1} - 8 \cdot 2^{i-1} = 4 \cdot 2^{i-1} = 2^{i+1}$. That completes the inductive step, so $x_i \geq 2^i$ for all i.
>
> Since $2^i \geq 1$, we have that $x_i \geq 1$, as desired. □

(b) [3 pts] Erroneous Erik tries to help by proving the claim as follows. What is his mistake?

> *Proof.* We'll use (regular) induction on the stronger hypothesis $R(i) :=$ "$x_i \geq 3x_{i-1}$", proving that $R(i)$ holds for every $i \geq 2$.
>
> Base case, $R(2)$: $x_2 = 13 \geq 12 = 3x_1$.
>
> Inductive Step: Suppose $i \geq 2$. Assuming that $x_i \geq 3x_{i-1}$ (i.e., $R(i)$) is true, let's show that $x_{i+1} \geq 3x_i$ (i.e., $R(i+1)$) is also true. Consider $x_{i+1} = 6x_i - 8x_{i-1}$. By the inductive hypothesis we know that $x_i \geq 3x_{i-1}$, so $\frac{8}{3}x_i \geq 8x_{i-1}$. Plug that into $x_{i+1} = 6x_i - 8x_{i-1} = \frac{10}{3}x_i + \frac{8}{3}x_i - 8x_{i-1}$ and you get $x_{i+1} \geq \frac{10}{3}x_i$. Since $x_i > 0$, $\frac{10}{3}x_i > 3x_i$, so $x_{i+1} \geq 3x_i$. That completes the inductive step, so $x_i \geq 3x_{i-1}$ for all $i \geq 2$.
>
> We know that $x_1 > 0$, and for all $i \geq 2$, $x_i \geq 3x_{i-1}$. Also, $x_{i-1} > 0$, so $x_i > 0$ for all i. □

(c) [3 pts] Overzealous Zach tries to help by proving the claim as follows. What is his mistake?

> *Proof.* We'll use strong induction on the stronger induction hypothesis $S(i) :=$ "$x_i = 4^i$ ", proving that $S(i)$ holds for every $i \geq 1$.
>
> Base case, $S(1)$: $x_1 = 4 = 4^1$.
>
> Inductive Step: Suppose $i \geq 1$. If $S(1), \ldots, S(i)$ are all true, let's show that $S(i+1)$ is true, i.e., $x_{i+1} = 4^{i+1}$. We know $x_{i+1} = 6x_i - 8x_{i-1}$. By the inductive hypothesis (specifically $S(i-1)$ and $S(i)$) we know that $x_{i-1} = 4^{i-1}$ and $x_i = 4^i$. Plug those into $x_{i+1} = 6x_i - 8x_{i-1}$ and you get $x_{i+1} = 6 \cdot 4^i - 8 \cdot 4^{i-1} = 6 \cdot 4 \cdot 4^{i-1} - 8 \cdot 4^{i-1} = 16 \cdot 4^{i-1} = 4^2 4^{i-1} = 4^{i+1}$. That completes the inductive step, so $x_i = 4x_{i-1}$ for all $i \geq 1$.
>
> Since $4^i \geq 1$, we have that $x_i \geq 1$, as desired. □

Hint: Zach's claim is false if $i = 2$. If you know the base case $i = 1$, what part of the inductive step when $i = 1$ fails?

(d) [6 pts] Prove the original claim that for all $i \geq 1$, $x_i > 0$.

Hint: See if you can fix Erroneous Erik's argument. What stronger inductive hypothesis will you use?

Problem 3. Integer Multiplication from Bit Shifts [17 points]

Multiplying and dividing an integer n by 2 requires only a one-bit left or right shift of the binary representation of n, which is a fast, hardware-supported operations on most computers. For example, the number 6 can be represented in binary as (0110); multiplying 6 by 2 yields 12, which is represented as (1100). The number 18 can be represented in binary as (10010); dividing 18 by 2 yields 9, which is represented as (01001).

In this problem, we will show that the following simple algorithm (state machine) computes the product of two nonnegative integers x and y using just these shift operations, along with integer addition:

The set of **states** is $\mathbb{N}^3 = \{(r, s, a) \mid r, s, a \in \mathbb{N}\}$, i.e., the set of triples of nonnegative integers. The **start state** is $(x, y, 0)$. The **transitions** are as follows:

$$(r, s, a) \mapsto \begin{cases} (2r, s/2, a) & \text{for even } s > 0, \\ (2r, (s-1)/2, a + r) & \text{for odd } s > 0. \end{cases}$$

No transitions are defined starting from triples in which $s = 0$.

We will show that this state machine eventually reaches a *final* state with no transitions remaining (the algorithm doesn't run forever), and that this final state (r_f, s_f, a_f) has $a_f = x \cdot y$. Thus, the algorithm computes the desired answer.

(a) [2 pts] Compute the full sequence of transitions from starting state $(5, 22, 0)$. Does it correctly compute $5 \cdot 22 = 110$?

(b) [4 pts] *Invariant:* Define $P(r, s, a) :=$ "$rs + a = xy$". Prove that P is an invariant of the state machine.

(c) [1 pts] *Final states:* A *final* state is one from which no transitions are possible. Which states are final in this state machine?

(d) [3 pts] *Partial correctness:* Use Parts (b) and (c) to conclude that, in any reachable final state (r_f, s_f, a_f), a_f must be equal to the product xy.

Now we consider termination. For a natural number n, let bitcount(n) denote the number of bits used when n is written in binary. For example, bitcount(5) = bitcount$(101_2) = 3$, bitcount$(1) = 1$, and we'll say that bitcount$(0) = 0$. (Note: This can be written explicitly as bitcount$(n) = \lceil \log_2(n + 1) \rceil$.)

(e) [5 pts] *Termination:* Prove that bitcount(s) is a strictly decreasing derived variable. Explain why this implies that the algorithm always terminates, that is, it has no infinite executions.

(f) [2 pts] *Time bound:* Explain why Part (e) implies that, from ay starting state $(x, y, 0)$, the algorithm terminates after at most bitcount$(y) = \lceil \log_2(y + 1) \rceil$ steps.

Problem 4. Invariant Enlightenment [8 points]

The ideal 6.1200 classroom has assigned desks (each student sits at the same position every day) arranged in a square grid. Students are working together to reach Invariant Enlightenment: a profound understanding of invariants so thorough that the knowledge radiates around them in a glowing aura. Invariant Enlightenment never goes away (it's an invariant, after all!) and can sometimes be taught to other students.

Here is an illustration of a 6×6-seat classroom with seats represented by squares. The locations of students who have initially been enlightened are marked with an asterisk.

*				*	
	*				
		*	*		
		*			
			*		*

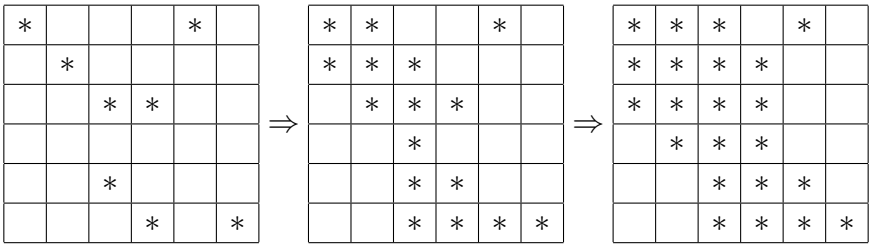
Every day, students talk to their neighbors about invariants in an attempt to reach enlightenment. On each day, a student is enlightened if either

- the student was already enlightened on a previous day, or

- the student was adjacent to *at least two* students who were enlightened on an earlier day (these neighbors worked together to teach the student all about invariants).

Here *adjacent* means the students' individual squares share an edge (front, back, left or right); they are not adjacent if they only share a corner point. So each student is adjacent to 2, 3 or 4 others.

In the example, Invariant Enlightenment is taught to more students as shown below:



In this example, over the next few days, all students reach enlightenment.

Theorem. *If fewer than n students among those in an $n \times n$ arrangment are initially enlightened, and additional students reach enlightenment only by being taught by two or more neighbors, then there will be at least one student who never reaches enlightenment.*

Prove this theorem.

Hint: You'll want to find an applicable preserved state predicate or monotonic derived variable that can help you argue about the set of enlightened students as time proceeds. Make sure to prove your claims.

In this problem and many others, finding the right property can be challenging! If you are stuck, ask at Office Hours or on Piazza for an extremely powerful one-word clue (and even more hints as necessary)!

6.1200J Mathematics for Computer Science

Spring 2024