GB13624 - Maths for Computer Science

Lecture 2 – Proofs, Part 2

Claus Aranha
caranha@cs.tsukuba.ac.jp

College of Information Science

2022-10-12

Last updated October 9, 2023

Lecture 2 – Outline

In the first lecture, we covered the basic concepts of proofs. This lecture, we we continue this study and introduce a very important proof method: **Induction.**

- **Section 1:** Sets and Relations;
- **Section 2:** Proof by Induction;
- **Section 3:** State Machines;

This lecture covers the textbook's chapters 4, 5 and 6 (and a little of 7).

Part 1: Sets and Relations

Mathematical Set

Mathematical Sets are useful when talking about proofs. Last class we have already used some sets:

- $\mathbb{N}$ – Set of natural (non negative) numbers;
- $\mathbb{Z}$ – Set of integer numbers;
- $\mathbb{R}$ – Set of real numbers;

Characteristics of sets

- Mathematical Sets can mix different "types" of objects:
  - {7, “Aranha”, $\pi/2$, TRUE}
- Mathematical Sets do not have a concept of "order":
  - {7, “Aranha”, $\pi/2$, TRUE} =
  - {TRUE, 7, $\pi/2$, “Aranha”}
- Mathematical Sets do not contain duplicates:
  - {7, π} = {7, π, 7}

Set: Membership

The fundamental property of a set is membership, represented by the symbol $\in$. Note that membership is not recursive!

A = {7,TRUE,π}

- $7 \in A$
- 7 is an element of A,
- $3 \notin A$

B = {7, $\mathbb{Z}$, 3}

- $7 \in B$
- $7 \in \mathbb{Z}$
- $\mathbb{Z} \in B$
- $1 \notin B$

Set: Subsets

Subset

- $A \subset B$ means that every element of A is also an element of B
- $A \subset B$ equiv $\forall x, x \in A \rightarrow x \in B$
- $\mathbb{Z} \subset \mathbb{R}, \mathbb{R} \subset \mathbb{C}, \{3\} \subset \{5, 3, 7\}$

Important!

- $A \subset A$
- $\forall X$ is a set, $\varnothing \subset X$

Difference between Membership and Subset

Membership ($\in, \notin$) indicates if one member is part of a set. Subset ($\subset, \not\subset$) indicates if one set contains the members of other sets.

- $3 \in \{3, 5, 6\}$
- $3 \not\subset \{3, 5, 6\}$

- $\{3\} \subset \{3, 5, 6\}$
- $\{3\} \notin \{3, 5, 6\}$

- $\{3\} \in \{5, 6, \{3\}\}$

Power Set

The Power Set of A is a special set composed of ALL subsets of A.

$$POW(A) = \forall x \subset A, x \in POW(A)$$

For example:

$$POW(\{T, F\}) = \{\{T\}, \{F\}, \{T, F\}, \varnothing\}$$

The definition of power set means that for any set *A* contained in *B*, *A* is an element of POW(B):

$$\mathbb{N} \in POW(\mathbb{R}), \mathbb{N} \subset \mathbb{R}, \mathbb{N} \notin \mathbb{R}$$

Operations on Sets

Finally, You should be familiar with the regular operations on sets:

- Union: $A \cup B \rightarrow x \in A \vee x \in B$
- Intersection: $A \cap B \rightarrow x \in A \wedge x \in B$
- Subtraction: $A - B \rightarrow x \in A \wedge x \notin B$
- Complement: $\overline{A} = D - A$, where D is the domain (the "everything" set or "parent" set of interest).

Sets, Proofs and Predicates

Sets are used often as parts of proofs. We used sets a little bit when we talked about the Well Ordering Principle.

It is common to use predicates to determine what elements are members of a set. For example, $P(X)$ be a predicate that defines A. If $P(X)$ is true for a certain X, then $X \in A$.

Example 1

- $A = x \in \mathbb{N}, \{x < 12 \text{ AND } x \text{ is prime}\} \implies A = \{2, 3, 5, 7, 11\}$

A is the set of "prime numbers smaller than 12"

Example 2

- $B = x \in \mathbb{N}, \{x \text{ is prime AND } x + 2 \text{ is prime}\} \implies$
  $B = \{3(5), 5(7), 11(13), 17(19), 29(31), \ldots\}$

B is the set of "prime numbers x where x+2 is also prime".

Sets and Proofs Example (1)

Prove that the empty set is a subset of every set.

Proof.

Proof by construction:

1. $A \subset B$ means that $\forall x, x \in A \rightarrow x \in B$
2. If $A = \varnothing$ then $x \in A$ is FALSE for $\forall x$, so we can replace "$\forall x \in A$" with FALSE in **(1)**
3. The statement FALSE $\rightarrow x \in B$ is always TRUE.
   (remember that FALSE $\rightarrow X$ is always TRUE)
4. Therefore, $\varnothing \subset B$ is TRUE $\forall B$

$\square$

Sets and Proofs Example (2)

Proof that Union and Intersection are Distributive

$$A \cup (B \cap C) \iff (A \cup B) \cap (A \cup C)$$

Proof.

Proof by sequence of "IFF"s:

1. $x \in A \cup (B \cap C)$ **iff**
2. $x \in A \vee x \in (B \cap C)$ **iff** (definition of union)
3. $x \in A \vee (x \in B \wedge x \in C)$ **iff** (definition of intersection)
4. $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$ **iff** (distributive prop.)
5. $(x \in A \cup B) \wedge (x \in A \cup C)$ **iff** (definition of union)
6. $x \in (A \cup B) \cap (A \cup C)$ (defintion of intersection)

□

Definition of Binary Relations

Binary Relations define an association of elements from one set (the **domain**) to another set (the **co-domain**). We see (binary) relations in many different situations:

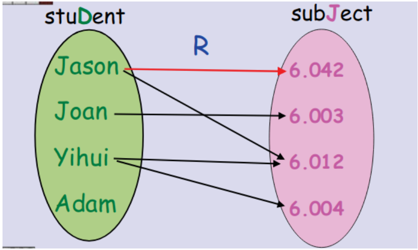
- Functions are a special case of binary relations: f(x) = y.
  - A function associates the set of inputs with the sets of outputs;
- Operations such as set membership can be expressed as binary relations.
  - For example, the predicate $P(x) : xisprime$ defines a binary relation from $\mathbb{N}$ to {TRUE, FALSE}
- "Relational Databases" (for example, SQL) are also based on the idea of binary relations
  - Key of X, member of a table, joint key, etc;

Example of Binary Relation

Let's consider the binary relation from the set of students **(D)** that are registered to the set of subjects **(J).**

Components of a binary relation:

- Domain: Set of Students;
- Co-domain: Set of Classes;
- Relation Graph:
  - Vertices: Union of Domain and Co-domain;
  - Edges: Directed edges from Domain to Co-domain;



Representation of a binary relation:

- $R(\text{Jason}) = \{6.042, 6.012\}$
- Jason R 6.042
- $R(\{\text{Jason, Yihui}\}) = \{6.042, 6.012, 6.004\}$

Relations and Inverse Relations

If we think of a binary relation as a directed graph, the Inverse Relation is the relation defined by the same graph when the edges are reversed:

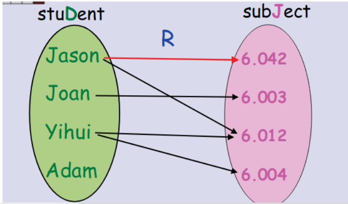
Relation R:

$$R(X) ::= j \in J | \exists d \in X.dRj$$

Reverse Relation R^{-1}:

$$R^{-1}(Y) ::= d \in S | \exists j \in Y.dRj$$

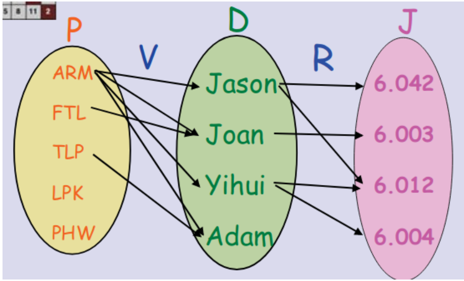
- $R(Jason) = \{6.042, 6.012\}$
- $R^{-1}(6.012) = \{Jason, Yihui\}$



Composite Relations

If we have a relation V from set P to set D, and a relation R from set D to set J, then we can define a composite relation $R \circ V$ from set P to set J (we can also use $R(V)$).

- $R(V(X))$ or $(R \circ V)(X)$
- $R(V(\text{FTL})) = \{6.003\}$
  - professor FTL super**V**ises Joan;
  - Joan is **R**egistered to class 6.003;



Types of Binary Relations

We can classify a binary relation based on the number of degrees (arrows) in the relation graph. Imagine a relation R from X to Y (i.e.: $R(X) = Y$)

Classification of R based on Y:

- **Surjection**: Every element in Y has ≥ 1 in-arrows. (Every Y has **one or more** X)
- **Injection**: Every element in Y has ≤ 1 in-arrows. (Every Y has **one or less** X)

Classification of R based on X:

- **Total**: Every element in X has ≥ 1 out arrows. (Every X has **one or more** Y)
- **Function**: Every element in X has ≤ 1 out arrows. (Every X has **one or less** Y)

An important definition:

- **Bijection**: Every element of X has **exactly one** element of Y, **and vice versa.**

Types of Binary Relations: Examples

Example 1: $g : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, g(x, y) = 1/(x - y)$

- This is a **function**, because each pair (x, y) has at most one output.
- This is not **total**, because not every pair (x, y) has an output: $(x = y)$ has no output.

Example 2: $g_o : \mathbb{R} \times \mathbb{R} - \{x, y | x = y\} \rightarrow \mathbb{R}, g_o(x, y) = 1/(x - y)$

- g and g_o are similar relations, but defined on different domains.
- The domain of g_o removes all (x, y) where $x = y$
- Because of this, g_0 is **function** (every pair has at most one output) and **total** (every pair has at least one output).

Part 2: Induction

An initial induction (1/2)

Imagine that I want to color the natural numbers ($\mathbb{N} \geq 0$), using the following rules:

- Number 0 is red
- Any integer next to a red number is also red

Using these rules, can you imagine how the set $\mathbb{N}$ looks like?

An initial induction (2/2)

Result: 0,1,2,3,4,...

The "rule of reds" gives us a general idea of induction:

- $R(0)$ is True
- $R(0) \to R(1); R(1) \to R(2); R(2) \to R(3); \ldots$
- $R(n) \to R(n+1)$ for every $n \in \mathbb{N}$

Induction can be used to prove a predicate that depends on some $n \in \mathbb{N}$ by modus ponens.

$$\frac{R(0), R(n) \to R(n+1), n \in \mathbb{N}}{\forall n, R(n)}$$

Example of proof by Induction

Let's prove that:

$$P(n) : 1 + r + r^2 + r^3 + \ldots + r^n = \frac{r^{n+1} - 1}{r - 1}, r \neq 1, \forall n \in \mathbb{N}$$

Remember the modus ponens rule for induction:

$$\frac{P(0), P(n) \rightarrow P(n+1), n \in \mathbb{N}}{\forall n, P(n)}$$

To prove the bottom part by induction, we need to prove the top part.

- First Step: Prove $P(0)$
- Second Step: Prove $P(n) \rightarrow P(n+1)$

Example of proof by Induction

Proof.

Proof by induction on n

First Step: Prove $P(0)$

- $P(0)$, left side: $r^0 = 1$
- $P(0)$, right side: $\frac{r^{0+1}-1}{r-1} = \frac{r-1}{r-1} = 1$

Second Step: Prove $P(n) \rightarrow P(n+1)$

- $P(n+1)$, left side: $1 + r + r^2 + \ldots + r^n + r^{n+1}$, which is equal to $P(n) + r^{n+1}$
- Because $P(n)$ is True, $P(n) + r^{n+1} = \frac{r^{n+1}-1}{r-1} + r^{n+1} = \frac{(r^{n+1}-1)}{r-1} + \frac{(r^{n+1}(r-1))}{r-1}$
- Algebra: $\frac{(r^{n+1}-1)+(r^{n+1}(r-1))}{r-1} = \frac{r^{n+1}-1+r^{n+2}-r^{n+1}}{r-1} = \frac{r^{n+2}-1+(r^{n+1}-r^{n+1})}{r-1}$
- $\frac{r^{n+2}-1}{r-1} = \frac{r^{(n+1)+1}-1}{r-1}$, which is the right side of $P(n+1)$

$\square$

Review: Proof Template for Induction

Proof by induction on n
Proof hypothesis: $P(n) = \ldots$ for all $n \in \mathbb{N}.n \geq 0$

First we prove $P(0)$.
$\ldots$ *(calculate that P(0) is True)*
$\ldots$

Second we prove that $\forall n \geq 0, P(n) \rightarrow P(n+1)$
$\ldots$ *(calculate P(n+1) using P(n))*
$\ldots$

This completes the proof that $P(n)$ for all $n \in \mathbb{N}$ $\square$

The Statue Park

A more complex proof by induction

The university is making a new park with the following rules:

- The park is square, with side 2^n;
- In the middle of the park, there is a statue, size 1×1;
- Other than that, the park is made of L-shaped tiles, with size $3m^2$;

How can we prove that it is possible to build this park for any n?

The Statue Park

Drawing Proof

Remember the rule of induction:

- Prove that $P(0)$ is true.
- Assume that $P(n)$ is true, then prove that $P(n) \implies P(n+1)$

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**

BAD Proof by induction: All horses are of the same color

$P(n)$ ::= for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$

BAD Proof by induction: All horses are of the same color

$P(n)$ ::= for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$
  - Subset A $(h_1, h_2, \ldots, h_n)$: has n horses, so all horses have the same color.

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$
  - Subset A ($h_1, h_2, \ldots, h_n$): has n horses, so all horses have the same color.
  - Subset B ($h_2, \ldots, h_n, h_{n+1}$): also has n horses, so all horses have the same color.

BAD Proof by induction: All horses are of the same color

$P(n)$ ::= for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$
  - Subset A ($h_1, h_2, \ldots, h_n$): has n horses, so all horses have the same color.
  - Subset B ($h_2, \ldots, h_n, h_{n+1}$): also has n horses, so all horses have the same color.
  - Horse h_2 is in subset A **and** in subset B, so subset A and B have the same color.

BAD Proof by induction: All horses are of the same color

$P(n) ::=$ for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$
  - Subset A $(h_1, h_2, \ldots, h_n)$: has n horses, so all horses have the same color.
  - Subset B $(h_2, \ldots, h_n, h_{n+1})$: also has n horses, so all horses have the same color.
  - Horse h_2 is in subset A **and** in subset B, so subset A and B have the same color.
- Since we showed that P(n+1) is true if P(n) is true, then all horses for any group size have the same color.

BAD Proof by induction: All horses are of the same color

$P(n)$ ::= for any set with exactly n horses, all horses have the same color.

- **Prove P(1)**: For any set with one horse, all horses have the same (one) color.
- **Assume P(n) is true:** For any set with n horses, all horses have the same color.
- **Show that $P(n) \implies P(n+1)$:**
  - Consider the set of n+1 horses: $H = h_1, h_2, \ldots, h_n, h_{n+1}$
  - Subset A ($h_1, h_2, \ldots, h_n$): has n horses, so all horses have the same color.
  - Subset B ($h_2, \ldots, h_n, h_{n+1}$): also has n horses, so all horses have the same color.
  - Horse h_2 is in subset A **and** in subset B, so subset A and B have the same color.
- Since we showed that P(n+1) is true if P(n) is true, then all horses for any group size have the same color.

QUIZ: What is wrong with this proof?

What is wrong with the horse proof?

The second step, when we show that $P(n) \implies P(n+1)$ is not valid.

- The implication proof depends on "h_i belongs to subsets A and B".
- But is this ALWAYS true?
  - When $n+1=2$, The $n+1$ set is $\{h_1, h_2\}$, set $A = h_1$, set $B = h_2$;
  - But in this case, **there is no h_i that is common to A and B**!
- So the implication proof is not valid when $P(2)$.

Note that this is the only problem with the proof!

Strong Induction

- In regular induction, you assume P(n) to show P(n+1)
- In strong induction, you assume P(0), P(1), P(2) . . . P(n), and use all of them to show P(n+1)

Strong Induction Example: Stacking Game

- Begin with a stack of 10 blocks
- Divide it in two (a,b): for example, 2 and 8 blocks.
- You get $a \times b$ points: 16 points
- Repeat with the new stacks until all stacks have 1 block.

What is the best strategy?

- Simple strategy: $1 \times 9 + 1 \times 8 + 1 \times 7 + 1 \times 6$...
- CS strategy: $5 \times 5 + 2 \times 3 + 2 \times 3$, ...

Strong Induction Example: Stacking Game

- Begin with a stack of 10 blocks
- Divide it in two (a,b): for example, 2 and 8 blocks.
- You get $a \times b$ points: 16 points
- Repeat with the new stacks until all stacks have 1 block.

What is the best strategy?

- Simple strategy: $1 \times 9 + 1 \times 8 + 1 \times 7 + 1 \times 6$... 45 points!
- CS strategy: $5 \times 5 + 2 \times 3 + 2 \times 3$, ...

Strong Induction Example: Stacking Game

- Begin with a stack of 10 blocks
- Divide it in two (a,b): for example, 2 and 8 blocks.
- You get $a \times b$ points: 16 points
- Repeat with the new stacks until all stacks have 1 block.

What is the best strategy?

- Simple strategy: $1 \times 9 + 1 \times 8 + 1 \times 7 + 1 \times 6$... 45 points!
- CS strategy: $5 \times 5 + 2 \times 3 + 2 \times 3$, ... 45 points!

Proof: All strategies have the same score (Part I)

Let us prove by strong inductions that all strategies for the stack game with "n" blocks have the same score:

$$C(n) = \frac{n(n-1)}{2}$$

Base Cases: 0, 1

- When the stack has 0 blocks, I have no moves, so 0 points.
- When the stack has 1 block, I have no moves, so 0 points.

$$C(0) = \frac{0(0-1)}{2}, C(1) = \frac{1(1-1)}{2} = 0$$

Proof: All strategies have the same score (Part II)

Inductive Case $C(n+1)$
By strong induction, we assume that all $C(0) \dots C(n)$ are true.

1. A stack with $n+1$ blocks can be split into two: k and $n+1-k$
2. The score is: $C(n+1) = (k \times (n+1-k)) + C(k) + C(n+1-k)$
3. Using the strong inductive assumption: $\forall m \leq n, C(m) = \frac{m(m-1)}{2}$
4. Transforming (2): $C(n+1) = \frac{2k(n+1-k)}{2} + \frac{k(k-1)}{2} + \frac{(n+1-k)(n-k)}{2}$

... You can finish the calculation from here ;-)

Part 3: State Machines

What are state machines?

State machines are used to represent "step-by-step" processes. They contain:

- A description of each possible state in the machine;
- How the machine transition from one state to another;

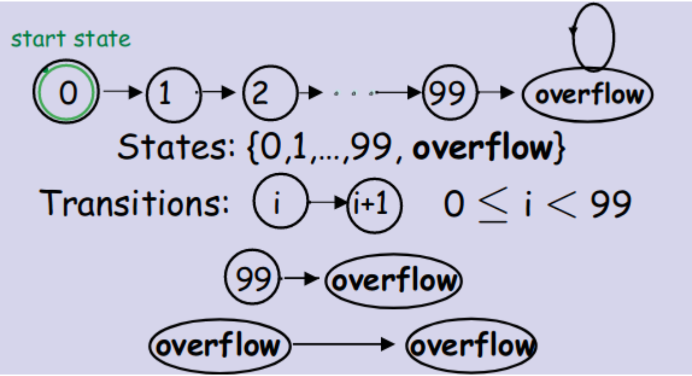
State machines are often used to describe algorithms, programs, logic circuit, decision processes, etc.

State machines are a formal description that can be used to prove the correctness of an algorithm.

Example of a State Machine

State machine for counting from 0 to 99:

- **States:** 0 to 99, overflow.
- **Start State:** 0
- **Transitions:**
  $i \rightarrow i + 1$ if $i < 99$
  $99 \rightarrow$ overflow
  overflow $\rightarrow$ overflow



Note how we can represent the State Machine many different ways.

State Machine for Proofs

Robot 1.0

Imagine a robot moving forwards and backwards on a street. The robot has two speeds:

- The robot can move exactly **five squares** forwards.
- The robot can move exactly **three squares** backwards.

If the robot starts from position 0, is it possible for it to reach position 4?

State Machine for Proofs

Robot 1.1

Imagine a robot moving forwards and backwards on a street. The robot has two speeds:

- The robot can move exactly **nine squares** forwards.
- The robot can move exactly **three squares** backwards.

If the robot starts from position 0, is it possible for it to reach position 4?

State Machine for Proofs

Preserved Invariants

Preserved Invariants are propositions that are always true, after **any** transition of the state machine. We can use preserved invariants to prove which squares the robots can reach.

Robot 1.0

The position of robot 1.0 is always: $s_0 + 5a - 3b$

Robot 1.1

The position of robot 1.1 is always: $s_0 + 9a - 3b$

- $s_0 + 9a - 3b = s_0 + 3(3a - b)$
- The position of robot 1.1 is always s_0 plus a multiple of 3; (Preserved Invariant)
- So it is impossible for robot 1.1 to reach 4 from 0.

Induction with Preserved Invariants

Preserved Invariants can be used together with inductions to prove things about state machines:

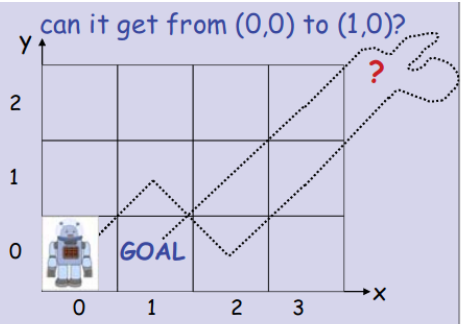
- Prove that $P(s)$ is a preserved invariant. This means that if $P(s)$ is true for some state s, then it will continue to be true after any transition.
- Prove that $P(s)$ is true for the initial state, s_0.
- Conclude that $P(s)$ is always true for the entire state machine.

If $P(s)$ is a "correctness condition" of an algorithm, this method can be used to prove that an algorithm is correct.

State Machine for Proofs

Robot 2.0

Robot 2.0 can move on the diagonals of $\mathbb{Z}^2$: (+1, +1), (-1,-1), (+1,-1), (-1,+1). Starting from (0,0), is it possible for the robot to reach position (1,0)?



QUIZ: Try to prove this by yourself first!

State Machine for Proofs

Robot 2.0 – Solution

We can show that a preserved invariant of robot 2.0 is that the sum of its coordinates is always even (or always odd):

- P(0,0) is true (0+0 is even).
- The steps of the robot are:
  - $+1+1=+2$: even + 2 is still even;
  - $-1-1=-2$: even - 2 is still even;
  - $+1-1=0$: even + 0 is still even;
  - $-1+1=0$: even + 0 is still even;

So we can see that the parity of the position is a preserved invariant. Because the parities of (0,0) and (1,0) are different, it is impossible for robot 2.0 to go from (0,0) to (1,0).

State Machines for Proofs

Fast Exponentiation

This is the end for this lecture. I highly recommend that you watch lecture video 1.9.1 from MIT OCW for a final example with the Fast Exponentiation algorithm.

Summary of the third part: To prove that an algorithm is correct, we need to show that:

- Prove that if the algorihm is in a correct state, it will always stay in the correct state (preserved invariant);
- Prove that the algorithm can reach the correct state from the initial position;
- Prove that the algorithm stops at some point (not an infinite loop).
  - We haven't talked about this part yet, but you can prove this by showing that some variable in the state machine is always decreasing.

Slide Credits

These slides are based on "Mathematics For Computer Science (Spring 2015)", by Albert Meyer and Adam Chlipala, MIT OpenCourseWare. `https://ocw.mit.edu`.

Individual images in some slides might have been made by other authors. Please see the following slides for information about these cases.

Image Credits I

1. Relation Graph Image from MIT OCS