6.042 Tutor

2/18

TP.3.6 Mapping Lemma: Size of Domains + Codomains

R = relation

↳ what exactly is a relation again?

the graph between them

(the arrows I guess)

R(S) = image of S under R

↳ a view

$s R t$ iff $t = 2s$

$R(\{0,3,11\}) = \{0,6,22\}$

$R(\mathbb{Z})$ is set of all even intigers

$|S|$ = size

~~R =~~ total

↳ A is finite

$|R(A)|$ ______ $|B|$

- equal to - since one to oe mapping

Finite →

$1 \to 2$
$2 \to 4$
$3 \to 6$
$4 \to 8$
$5 \to 10$

(2)

~~Unless they want 6~~

Can't be that $|B|$ is twice $|R(A)|$

Or is it $|R(A)|$ is the result

So by definition same?

less than or equal to

why?

$R(A) \subseteq B$

b) if R is a surj then $|A|$ ___ $|B|$

every el mapped to at least once

- but what does this have to do with R?

$|A|$ must be $\leq |B|$

$\geq$

I just was not thinking

Mapping Rule

(3) R surj $|R(A)|$ ___ $|B|$

the result

"again same thing"

equals

4. R inj $|R(A)|$ ___ $|A|$

B mapped to at ~~least~~ most once

So $|A| \geq |R(A)|$

$|R(A)| \leq |A|$

equals

5. R bij $|A|$ ___ $|B|$

equals

Mapping Rules

Reread 5.2

9

TP 3.7 Which of the following sets are countable?

What is countable again?

- finite or countably infinite
- ~~ø~~ if elements can be listed in order

1 $\mathbb{N}$

2 $\mathbb{Z}$

3 $\mathbb{Q}$

4 $\mathbb{R}$

5 $\mathbb{C}$

6 $\{0,1\}^{10^{10}}$ - length of 10^{10} bit strings

7 $\{0,1\}^{\omega}$ - ∞ binary seq

8 $\mathbb{Q}^{\omega}$ - ∞ series of rationals

1 2 6 ~~8~~

1 2 3 6

So the rational # as well

I was thinking irrational - grr.

- learn the symbols!

2/18

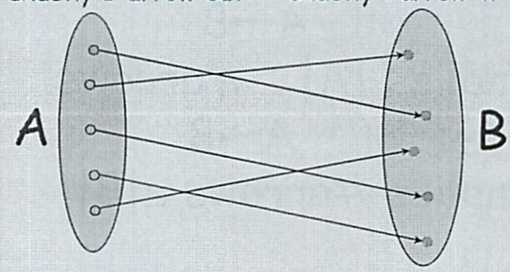
Mathematics for Computer Science
MIT 6.042J/18.062J

Cardinality
(the size of sets)

Albert R Meyer, February 18, 2011 lec 3F.1

bijection archery

exactly 1 arrow out exactly 1 arrow in



 lec 3F.2

Mapping Rule (bij)

A bijection from
A to B implies
$|A| = |B|$
for finite A, B

Albert R Meyer, February 18, 2011 lec 3F.3

pow(A) bijection to bit-strings

A: $\{a_0, a_1, a_2, a_3, a_4, \ldots, a_{n-1}\}$
subset: $\{a_0, \quad a_2, a_3, \quad \ldots, a_{n-1}\}$
string: 1 0 1 1 0 … 1
this defines a bijection, so
n-bit strings = |pow(A)|

Albert R Meyer, February 18, 2011 lec 3F.4

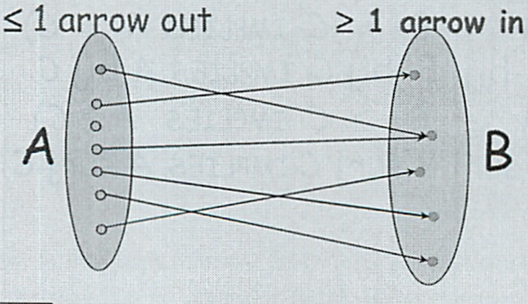
pow(A) bijection to bit-strings

every computer scientist
knows #n-bit strings, so
Corollary:
$|pow(A)| = 2^{|A|}$

Albert R Meyer, February 18, 2011 lec 3F.5

surjective & function

≤ 1 arrow out ≥ 1 arrow in



Albert R Meyer, February 18, 2011 lec 3F.6

Mapping Rule (surj)

[$\leq$1 out] $A \to B$
implies $|A| \geq$ #arrows.
[$\geq$1 in] $A \to B$
implies #arrows $\geq |B|$.

Mapping Rule (surj)

Surjective function from A to B implies

$$|A| \geq |B|$$

for finite A, B

Cantor's Idea

A surj B ::= $\exists$surj func:$A \to B$
think: "A as big as B"
A bij B ::= $\exists$bijection:$A \to B$
think: "A same size as B"

Cantor's Idea

A strict B ::=
B surj A AND NOT(A surj B)
think: "A is smaller than B"
Cantor Thm:
A strict pow(A)

Familiar "size" properties

($A = B = C$ IMPLIES $A = C$)
A bij B bij C IMPLIES A bij C
($A \geq B \geq C$ IMPLIES $A \geq C$)
A surj B surj C IMPLIES A surj C

Familiar "size" properties

($A \geq B \geq A$ IMPLIES $A = B$)
A surj B surj A IMPLIES A bij B
this is NOT obvious:
Schroeder-Bernstein Thm

UNfamiliar "size" property

"size +1 = size"
for ∞-sizes

Same Size Infinite Sets?

{1, 2, 3, 4, ...}
and ↑ ↑ ↑ ↑
{0, 1, 2, 3, ...}
a bijection

Same Size Infinite Sets?

{1, 2, 3, 4, ...}
and ↑ ↑ ↑ ↑
{0, 1, 2, 3, ...}
the "same size"!

pow(N) bij ∞-bit-strings

infinite set N = {0,1,2,...}
subset: {0, , 2, 3, , , 6, ... }
string: 1 0 1 1 0 0 1 ...

a bijection from pow(N) to *infinite* bit-strings, $\{0,1\}^{\omega}$

$\{0,1\}^{\omega}$ is uncountable

A is *countable* iff can be listed $a_0, a_1, a_2, \ldots$

same as surj fcn: $\mathbb{N} \to A$

So $\{0,1\}^{\omega}$ is uncountable, because

$$\underbrace{\mathbb{N} \to \{0,1\}^{\omega}}_{\text{surj}} \underbrace{\to \text{pow}(\mathbb{N})}_{\text{bij}}$$

surj

Team Problems

Problems 1—4

6.042 Cardinality

2/18

"Lecture where we go off the deep end"

math + reasoning
- not intuition

bijection - One arrow out = total, function
One arrow in = injection, surjection

So $|A| = |B|$
but only for finite A, B

Suppose have arbitrary array of N elements
$A: \{a_0, a_1, a_2, \ldots, a_{n-1}\}$
Take a subset
$\{a_0, a_2, a_3, \ldots a_{n-1}\}$
Code
1 0 1 1 ... 1
since a_1 missing

So one uniqully determins the other

\# of n-bit strings $= |pow(A)|$

(2)

Are 2^n of n-bit strings

$$|pow(A)| = 2^{|A|}$$

(we did this before)

bit strings = binary words

Surjective + function

≥ 1 arrow in
↳ implies
arrows $\geq |B|$

≤ 1 arrow out
↳ implies $|A| \geq$ # arrows

So $|A| \geq |B|$

(I should be able to think through this)
for finite A, B

Cantor's Idea

A surj B $::= \exists$ surj func: $A \to B$
"A as big as B"

A bij B $::= \exists$ bijection: $A \to B$
"A same size as B"

(3)

A strict B ::= B surj A AND NOT (A surj B)

~~A~~ is "A is smaller than B"

Cantor Theorm

A strict pow(B)

Familiar size properties

$A = B = C \rightarrow A = C$

A bij B bij C → A bij C

- need to prove lemma - closed under bijection

$A \geq B \geq C \rightarrow A \geq C$

A surj B surj C → A surj C

~~PAK~~ $A \geq B \geq A \rightarrow A = B$

↳ Schroeder - Berntein Theorm

- quite ingenious to prove
- not obvious ; lang ~~A~~ is no $\geq$
- its a highly technical def surj

~~Idea~~ - really try to understand the problem

(4)

Q: Does size mean anything
- very technical definition

Unfamiliar property
- technical definition
- size + 1 = size
for ∞ sizes

Example
$$\{1, 2, 3, \dots\}$$
$$\uparrow\ \uparrow\ \uparrow\ \uparrow$$
$$\{0, 1, 2, 3, \dots\}$$
bijective map n to $n+1$
- by def the same size

- Power ~~size~~ set
- inconsistent?

better way to make sets bigger
add a whole bunch of ele at once
Or exponentiate set
Problem 3 today
- squaring won't get you bigger
- exponentiating

5

pow(N) bij ∞-bit-strings

∞ set $N = \{0, 1, 2, \ldots\}$

Can correspond to an ∞ binary string

Subset $\{0, \ , 2, 3, \ , \ , \ , 6, \ldots\}$

$1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ \ldots$

bij from pow(N) to ∞ bit-strings $\{0,1\}^{\omega}$

So $\{0,1\}^{\omega}$ is uncountable

A is countable if can write down els

$a_0, a_1, a_2, \ldots$

Same as surj fn $N \to A$

~~oth~~ allows you to have repeats

So $\{0,1\}^{\omega}$ is uncountable because no ordaly way to ~~no~~ list them so that you know you have them all

---

Suppose $\underbrace{N \to \underbrace{\{0,1\}^{\omega}}_{} }_{\text{surj}} \underbrace{\to pow(N)}_{\text{bij}}$

$\underbrace{\qquad\qquad}_{\text{surj}}$ — impossible by Cantors' Theorm — contradiction ~~[illegible]~~

Massachusetts Institute of Technology
6.042J/18.062J, Spring '11: Mathematics for Computer Science
Prof. Albert R Meyer

February 18
revised Thursday 17th February, 2011, 00:27

In-Class Problems Week 3, Fri.

in my printout of 2011/2/6 book 5.3.4

Problem 1. **(a)** Several students felt the proof of Lemma 5.2.3 was worrisome, if not circular. What do you think? Hint: Why is third line nessary?

> Lemma 5.2.3. Let A be a set and $b \notin A$. If A is infinite, then there is a bijection from $A \cup \{b\}$ to A.
>
> *Proof.* Here's how to define the bijection: since A is infinite, it certainly has at least one element; call it a_0. But since A is infinite, it has at least two elements, and one of them must not be equal to a_0; call this new element a_1. But since A is infinite, it has at least three elements, one of which must not equal a_0 or a_1; call this new element a_2. Continuing in the way, we conclude that there is an infinite sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ of different elements of A. Now we can define a bijection $f : A \cup \{b\} \to A$:
>
> $$\begin{aligned} f(b) &::= a_0, \\ f(a_n) &::= a_{n+1} && \text{for } n \in \mathbb{N}, \\ f(a) &::= a && \text{for } a \in A - \{b, a_0, a_1, \ldots\}. \end{aligned}$$
>
> ■

(b) Use the proof of Lemma 5.2.3 to show that if A is an infinite set, then A surj $\mathbb{N}$, that is, every infinite set is "as big as" the set of nonnegative integers.

Problem 2.
This problem provides a proof of the [Schröder-Bernstein] Theorem:

$$\text{If } A \text{ surj } B \text{ and } B \text{ surj } A, \text{ then } A \text{ bij } B. \tag{1}$$

(a) It is OK to assume that A and B are disjoint. Why?

(b) Explain why there are total injective functions $f : A \to B$, and $g : B \to A$.

Picturing the diagrams for f and g, there is *exactly one* arrow *out* of each element —a left-to-right f-arrow if the element is in A and a right-to-left g-arrow if the element is in B. This is because f and g are total functions. Also, there is *at most one* arrow *into* any element, because f and g are injections.

So starting at any element, there is a unique, and unending path of arrows going forwards. There is also a unique path of arrows going backwards, which might be unending, or might end at an element that has no arrow into it. These paths are completely separate: if two ran into each other, there would be two arrows into the element where they ran together.

This divides all the elements into separate paths of four kinds:

i. paths that are infinite in both directions,

ii. paths that are infinite going forwards starting from some element of A.

iii. paths that are infinite going forwards starting from some element of B.

iv. paths that are unending but finite.

(c) What do the paths of the last type (iv) look like?

(d) Show that for each type of path, either

- the f-arrows define a bijection between the A and B elements on the path, or
- the g-arrows define a bijection between B and A elements on the path, or
- both sets of arrows define bijections.

For which kinds of paths do both sets of arrows define bijections?

(e) Explain how to piece these bijections together to prove that A and B are the same size.

Problem 3.
The rational numbers fill the space between integers, so a first thought is that there must be more of them than the integers, but it's not true. In this problem you'll show that there are the same number of positive rationals as positive integers. That is, the positive rationals are countable.

(a) Define a bijection between the set, $\mathbb{Z}^+$, of positive integers, and the set, $(\mathbb{Z}^+ \times \mathbb{Z}^+)$, of all pairs of positive integers:

$$\begin{array}{c}
(1,1),(1,2),(1,3),(1,4),(1,5),\ldots \\
(2,1),(2,2),(2,3),(2,4),(2,5),\ldots \\
(3,1),(3,2),(3,3),(3,4),(3,5),\ldots \\
(4,1),(4,2),(4,3),(4,4),(4,5),\ldots \\
(5,1),(5,2),(5,3),(5,4),(5,5),\ldots \\
\vdots
\end{array}$$

(b) Conclude that the set, $\mathbb{Q}^+$, of all positive rational numbers is countable.

Problem 4.
Let $R : A \to B$ be a binary relation. Use an arrow counting argument to prove the following generalization of the Mapping Rule 1.

Lemma. *If R is a function, and $X \subseteq A$, then*

$$|X| \geq |R(X)|.$$

~~Kold~~ ~~IA~~ Problems 3Fri 2/18

1b Def 5.3.5 Set C is ~~countable~~ infinite iff $\mathbb{N} \hookrightarrow C$

— countable if finite or countably infinite

So ~~...~~ $\mathbb{N}$ is countably infinite

A Surj $B \rightarrow |A| \geq |B|$

A surj $N \rightarrow |A| \geq \mathbb{N}$

↑ since is countable infinite

↑ ~~...~~

└ this one may be countable infinite

4. $R: A \rightarrow B$

Use arrow counting to prove Mapping Rule 1

(Lemma 5.2.2 (my book)

A surj $B \rightarrow |A| \geq |B|$)

Lemma If R is a function and $X \subseteq A$ then

$|X| \geq |R(x)|$

↑ is a subset of

So saying

X Surj $R(x)$

↑ every el mapped to at least once

↑ which it must be b/c it is a relation

2) : It would not be in the relation if it was not true

---

3. :: Same # of (+) rationals as (+) integers

: so R(+) rationals are countable

3a (Is that even true)

$\mathbb{Z}^+$ Bij $(\mathbb{Z}^+ \times \mathbb{Z}^+)$

: ~~Know~~

~~what~~ what is the table

- all the pairs of pos integers

Need to define a bijection - not just show that there is one

1a Yes proof seems good

$f(a) := a$ completes the bij for all $x \in A$

Such that $x \notin \{a_0, a_1, a_2, \ldots\}$

✓ TA: handwavy

Use axiom of Choice

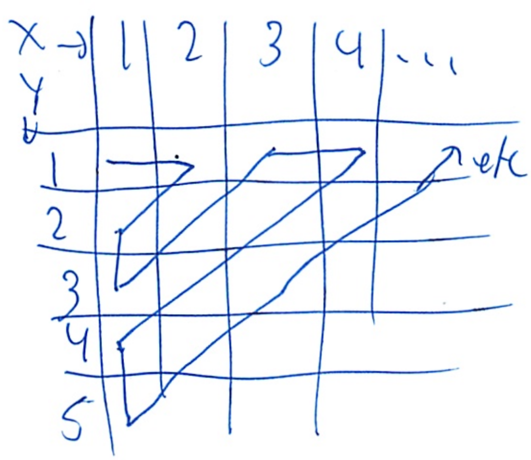
b Repeat the reasoning of the above proof.

A is ∞ implies that there exists an el in A. Call it a_0. Similarly there exists an $a_1, a_2, a_3, a_4 \ldots \in A$

Then our surjective function from $A \to N$ is $f(a_i) = i$

3

3a) (x, y)



~~[illegible]~~ 1 to 1

3b Make first # numerator
Second # denom
Have all of the denom

2a If not disjoint have members in common
There is a 1 to 1 correspondence b/w any shared members of A and B, so that they are an irrelevant in determining if there is a bijection b/w the disjoint subsets of A and B.

↑ bijection ~~[illegible]~~

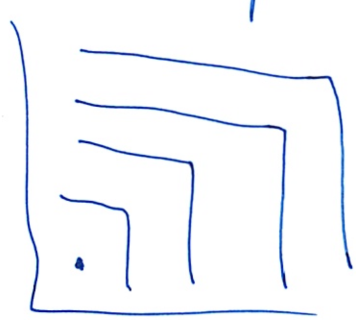
2b ~~[illegible]~~ f ~~that~~ is the ~~[illegible]~~ inverse of the surjective function B→A and g is the inverse of the surj fn A→B

(4)

2c an unending finite path in a loop

2d

3a can do picture proof?



Solutions to In-Class Problems Week 3, Fri.

Problem 1. **(a)** Several students felt the proof of Lemma 5.2.3 was worrisome, if not circular. What do you think?

> Lemma 5.2.3. Let A be a set and $b \notin A$. If A is infinite, then there is a bijection from $A \cup \{b\}$ to A.
>
> *Proof.* Here's how to define the bijection: since A is infinite, it certainly has at least one element; call it a_0. But since A is infinite, it has at least two elements, and one of them must not be equal to a_0; call this new element a_1. But since A is infinite, it has at least three elements, one of which must not equal a_0 or a_1; call this new element a_2. Continuing in the way, we conclude that there is an infinite sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ of different elements of A. Now we can define a bijection $f : A \cup \{b\} \to A$:
>
> $$\begin{aligned} f(b) &::= a_0, \\ f(a_n) &::= a_{n+1} && \text{for } n \in \mathbb{N}, \\ f(a) &::= a && \text{for } a \in A - \{a_0, a_1, \ldots\}. \end{aligned}$$
>
> ■

Solution. There is no "solution" for this discussion problem, since it depends on what seems bothersome.

AN issue that puzzles some students (when they ar challenged about it) is why the third clause in the definition of f is needed since f is already defined on all the a_n's. The answer is that there may be elements left over in A, and to be a bijection, the value of f on each "left-over" element of A has to be defined somehow. In fact, if A is uncountable, there are guaranteed to be such left-over elements.

It may also be bothersome that f is asserted to be a bijection without spelling out a proof. But the bijection property really does follow directly from definition of f, so it shouldn't be much burden for a bothered reader to fill in such a proof.

Another possibly bothersome point is that the proof assumes that if a set is infinite, it must have more than n elements, for every nonnegative integer n. But really that's the definition of infinity: a set is finite iff it has n elements for some nonnegative integer, n, and a set is infinite iff it is *not* finite.

A possibly worrisome point is how you find an element $a_{n+1} \in A$ given $a_0, a_1, \ldots, a_n$. But you don't have to *find* a specific one: there must be an element in $A - \{a_0, a_1, \ldots, a_n\}$—so just pick any one. Actually, the justification for this step is the set-theoretic Axiom of Choice described in the Notes chapter first-order logic, and some logicians do consider it worrisome. ■

(b) Use the proof of Lemma 5.2.3 to show that if A is an infinite set, then A surj $\mathbb{N}$, that is, every infinite set is "as big as" the set of nonnegative integers.

Solution. By the proof of Lemma 5.2.3, there is an infinite sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ of different elements of A. Then we can define a surjective function $f : A \to \mathbb{N}$ by defining

$$f(a) ::= \begin{cases} n, & \text{if } a = a_n, \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

—A total surjective function is not required, but if you want one define $f' : A \to \mathbb{N}$, by

$$f'(a) ::= \begin{cases} n, & \text{if } a = a_n, \\ 0, & \text{otherwise.} \end{cases}$$

■

Problem 2.
This problem provides a proof of the [Schröder-Bernstein] Theorem:

$$\text{If } A \text{ surj } B \text{ and } B \text{ surj } A, \text{ then } A \text{ bij } B. \tag{1}$$

(a) It is OK to assume that A and B are disjoint. Why?

↳ no elements in common $\{1,2,3\}$ $\{4,5,6\}$

Solution. We can always find sets A' bij A and B' bij B such that A' and B' are disjoint. For example, let $A' = A \times \{0\}$ and $B' = B \times \{1\}$. Then if we prove (1) for A' and B', we could conclude it held for A and B because

$$A \text{ bij } A' \text{ bij } B' \text{ bij } B.$$

■

(b) Explain why there are total injective functions $f : A \to B$, and $g : B \to A$.

Solution. B surj A means there is a surjective function $h : B \to A$, so $h^{-1} : A \to B$ will be a total injective relation. Removing all but one h^{-1}-arrow out of each element of A, leaves a total injective *function* $f : A \to B$. Likewise for $g : B \to A$. ■

Picturing the diagrams for f and g, there is *exactly one* arrow *out* of each element —a left-to-right f-arrow if the element is in A and a right-to-left g-arrow if the element is in B. This is because f and g are total functions. Also, there is *at most one* arrow *into* any element, because f and g are injections.

So starting at any element, there is a unique, and unending path of arrows going forwards. There is also a unique path of arrows going backwards, which might be unending, or might end at an element that has no arrow into it. These paths are completely separate: if two ran into each other, there would be two arrows into the element where they ran together.

This divides all the elements into separate paths of four kinds:

i. paths that are infinite in both directions,

ii. paths that are infinite going forwards starting from some element of A.

iii. paths that are infinite going forwards starting from some element of B.

iv. paths that are unending but finite.

(c) What do the paths of the last type (iv) look like?

Solution. An even-length cycle of alternating f- and g-arrows.

■

(d) Show that for each type of path, either

- the f-arrows define a bijection between the A and B elements on the path, or

- the g-arrows define a bijection between B and A elements on the path, or
- both sets of arrows define bijections.

For which kinds of paths do both sets of arrows define bijections?

Solution. For paths that start at a point in A, there will be an f-arrow out of every point on the path, so the f-arrows will define a bijection from the A elements to the B elements on the path. The g-arrows don't define a bijection the other way, because they don't hit the starting point.

For paths that start at a point in B, the g-arrows will define a bijection from the B elements to the A elements, by the same reasoning.

For the other two types of path, every point B element has exactly one f-arrow coming in, so these arrows define a bijection from the A elements to be B elements. Likewise, the g-arrows define a bijectin the other way.

■

(e) Explain how to piece these bijections together to prove that A and B are the same size.

Solution. Define $h : A \to B$ by the rule:

$$h(a) ::= \begin{cases} g^{-1}(a) & \text{if } a\text{'s path starts at a point in } B, \\ f(a) & \text{otherwise.} \end{cases}$$

■

what? thats it?

Problem 3.

The rational numbers fill the space between integers, so a first thought is that there must be more of them than the integers, but it's not true. In this problem you'll show that there are the same number of positive rationals as positive integers. That is, the positive rationals are countable.

(a) Define a bijection between the set, $\mathbb{Z}^+$, of positive integers, and the set, $(\mathbb{Z}^+ \times \mathbb{Z}^+)$, of all pairs of positive integers:

$$\begin{array}{l}
(1,1), (1,2), (1,3), (1,4), (1,5), \ldots \\
(2,1), (2,2), (2,3), (2,4), (2,5), \ldots \\
(3,1), (3,2), (3,3), (3,4), (3,5), \ldots \\
(4,1), (4,2), (4,3), (4,4), (4,5), \ldots \\
(5,1), (5,2), (5,3), (5,4), (5,5), \ldots \\
\vdots
\end{array}$$

Solution. Line up all the pairs by following successive upper-right to lower-left diagonals along the top row. That is, start with (1,1) which is an initial diagonal of length 1. Then follow with the length 2 diagonal (1,2), (2,1), then the length 3 diagonal (1,3), (2,2), (3,1), then the length 4 diagonal (1,4), (2,3), (3,2), (4,1), ... So the line up would be

$$\begin{array}{ccccccccccc}
(1,1) & (1,2) & (2,1) & (1,3) & (2,2) & (3,1) & (1,4) & (2,3) & (3,2) & (4,1) & \ldots \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \ldots
\end{array}$$

It's interesting that this bijection from $(\mathbb{Z}^+ \times \mathbb{Z}^+)$ to $\mathbb{Z}^+$ happens to have a simple formula. The pair (k, m) is the kth element on the diagonal consisting of the $k + m - 1$ pairs whose sum is $k + m$. The total number of elements in all the preceding diagonals is

$$0 + 1 + 2 + \cdots + (k + m - 2) = (k + m - 1)(k + m - 2)/2,$$

so the pair (k, m) is the $(k+m-1)(k+m-2)/2+k$th element in the line-up. ∎

(b) Conclude that the set, $\mathbb{Q}^+$, of all positive rational numbers is countable.

Solution. To show the positive rationals are countable, we want to show how to line them up in a list. To do this, start with a list of all pairs of positive integers such as the one from part (a). Then, going from left to right, replace each pair (m, n) by the positive rational $r ::= m/n$, skipping pairs where r has already appeared:

$$1, 1/2, 2, 1/3, 3, 1/4, 2/3, 3/2, 4, \ldots.$$

This is now the desired list of the positive rationals.

Another, indirect approach is to find surjective functions between $\mathbb{Z}^+$ and $\mathbb{Q}^+$ and back, and than appeal to the Schröder-Bernstein Theorem 5.2.2.

To begin, it's obvious that

$$\mathbb{Q}^+ \text{ surj } \mathbb{Z}^+, \tag{2}$$

since the identity function restricted to the positive integers does the job. Namely, $f : \mathbb{Q}^+ \to \mathbb{Z}^+$ where

$$f(r) ::= \begin{cases} r & \text{if } r \text{ is an integer,} \\ \text{undefined} & \text{otherwise,} \end{cases}$$

is a surjective function.

It's also obvious that

$$(\mathbb{Z}^+ \times \mathbb{Z}^+) \text{ surj } \mathbb{Q}^+$$

since there is a trivial surjective function $g : (\mathbb{Z}^+ \times \mathbb{Z}^+) \to \mathbb{Q}^+$, namely,

$$g(m, n) ::= m/n.$$

It follows from part (a) that

$$\mathbb{Z}^+ \text{ surj } \mathbb{Q}^+. \tag{3}$$

Now (2), (3), and the Schröder-Bernstein Theorem 5.2.2 imply

$$\mathbb{Z}^+ \text{ bij } \mathbb{Q}^+.$$

∎

Problem 4.
Let $R : A \to B$ be a binary relation. Use an arrow counting argument to prove the following generalization of the Mapping Rule 1.

Lemma. *If R is a function, and $X \subseteq A$, then*

$$|X| \geq |R(X)|.$$

Solution. *Proof.* The proof is virtually a repeat of the arrow-counting proof in the text of Mapping Rule 1, namely:

means this, remember

Since R is a function, at most one arrow leaves each element of X, so the number of arrows whose starting point is an element of X is at most the number of elements in X, That is,

$$|X| \geq \#\text{arrows from } X.$$

Also, each element of $R(X)$ is, by definition, the endpoint of at least one arrow starting from X, so there must be at least as many arrows starting from X as the number of elements of $R(X)$. That is,

$$\#\text{arrows from } X \geq |R(X)|.$$

Combining these inequalities immediately implies that $|X| \geq |R(X)|$. ■

An alternative proof appeals to the original Mapping Rule:

Proof. Let R' be the relation R restricted to X. That is, R' has domain X, codomain $R(X)$, and the same arrows as R. Then R' is a function because R is, and R' has the [≥ 1 in] surjective property by definition of its codomain. Hence the surjective function Mapping Rule 1 applied to the surjective function $R' : X \to R(X)$ implies that $|X| \geq |R(X)|$. ■

Tutor

2/4

TP 4.1 Induction

has proven $P(n) \to P(n+3)$

$P(5)$

$n = \mathbb{N}$

1. What can she infer?

   1. $P(n)$ holds for all $n \geq 5$

      - no since not 6

   2. $P(3n)$ holds for all $n \geq 5$

      Yes $n=5$ means 15

      $\frac{15-5}{3}$ no remainder

      actually no!

   3. $P(n)$ for 8, 11, 14

      Yes, by def

   4. $P(n)$ does not hold for $n < 5$

      - does not prove that it does not hold

      No

   5. $\forall n \; P(3n+5)$

      $P(3n+5)$ for all n

(2)

So $n=1$

$3+5=8$

$n=2$

$6+5=11$

$n=3$

14

- which is what we want

- remember $\frac{\_\_ - 5}{3}$

- yes

6. $\forall n \geq 2 \; P(3n-1)$

$n=3$ $\quad 3 \cdot 3 - 1 = 8$

$n=4$ $\quad 12-1=11$

$$\frac{(3n-1)-5}{3}$$

$$\frac{3n-6}{3}$$

$n-3$

and $n \geq 2$

So ~~yes~~ n must be 3 yes

③

7. $P(0) \rightarrow \forall n\, P(3n+2)$

So if if true and prop true

or if false

not $P(0)$ so true

8. $P(0) \rightarrow \forall n\, P(3n)$

same

3 5 6 7 8 ⓧ

3 5 6 ⓧ

(I hate how they won't tell which wrong!)

Look at 7, 8 again

7. If she proves $P(0)$ then $3n+2$

$$\frac{3n+2-\cancel{3}5}{3}$$

$$\frac{3n-3}{3}$$

$$n-1$$

including $P(0)$ so true?

(9)

8. $\frac{3n-5}{3}$

~~3~~ not true

3 5 6 7 (x)

3 5 6 8

So 7 not true, 8 is true

8. If alice knows p is true on 0,
She knows it wil be true on all multiples
of 3 : 3, 6, 9, ...

Oh thats what implies means here!

(5)

2. Which ~~would~~ could Alice prove to conclude $P(n)$ holds for $n \geq 5$

- in addition to what she already proved?

$P(n) \to P(n+3)$

1. $P(0)$
   - would not do anything
   - would prove $0, 3, 6, 9, 12, \ldots$
2. $P(5)$
   again
   $5, 8, 11, 14$ but different!
3. $P(5)$ and $P(6)$
   $5, 8, 11, 14, \ldots$
   $6, 9, 12, 15$ fills in but still gaps
4. $P(0)$ and $P(1)$ and $P(2)$
   Ok here we go
5. $P(5)$, and $P(6)$ and $P(7)$
   Yeah
6. $P(2)$ and $P(4)$ and $P(5)$
   2 5 ← no

6

7. $P(2)$ and $P(4)$ and $P(6)$

2 5 8 11

4 7 10 13

6 9 12 15

Yeah!

8. $P(3)$ and $P(5)$ and $P(7)$

3 6 9 12 15

5 8 11 14

7 10 13

yeah

So this was easy to do

Induction

The Idea of Induction

Color the integers ≥ 0

0, 1, 2, 3, 4, 5, ...

I tell you, 0 is red, & any int next to a red integer is red, then you know that all the ints are red!

The Idea of Induction

Color the integers ≥ 0

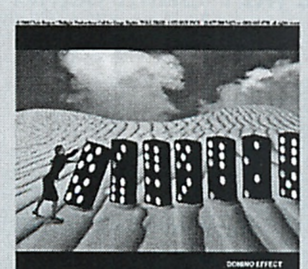
0, 1, 2, 3, 4, 5, ...

I tell you, 0 is red, & any int next to a red integer is red, then you know that all the ints are red!

Induction Rule

$$\frac{R(0),\ \forall n.\, R(n) \text{ IMPLIES } R(n+1)}{\forall m.\, R(m)}$$

Like Dominos...



Example Induction Proof

Let's prove:

$$1+r+r^2+\cdots+r^n = \frac{r^{(n+1)}-1}{r-1}$$

(for $r \neq 1$)

Example Induction Proof

Statements in magenta form a **template for inductive proofs:**

Proof: (by induction on n)

The induction hypothesis, P(n), is:

$$1+r+r^2+\cdots+r^n = \frac{r^{(n+1)}-1}{r-1}$$

(for $r \neq 1$)

Example Induction Proof

Base Case ($n = 0$):

$$\underbrace{1+r+r^2+\cdots+r^0}_{1} \stackrel{?}{=} \frac{r^{0+1}-1}{r-1}$$

$$= \frac{r-1}{r-1} = 1$$

OK!

Example Induction Proof

Inductive Step: Assume P(n) for some $n \geq 0$ and prove P(n+1):

$$1+r+r^2+\cdots+r^{n+1} = \frac{r^{(n+1)+1}-1}{r-1}$$

Example Induction Proof

Now from induction hypothesis P(n) we have

$$1+r+r^2+\cdots+r^n = \frac{r^{n+1}-1}{r-1}$$

so add r^{n+1} to both sides

Example Induction Proof

adding r^{n+1} to both sides,

$$\left(1+r+r^2+\cdots+r^n\right)+r^{n+1} = \left(\frac{r^{n+1}-1}{r-1}\right)+r^{n+1}$$

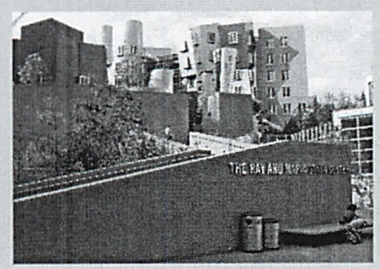
This proves P(n+1)

$$= \frac{r^{n+1}-1+r^{n+1}(r-1)}{r-1}$$

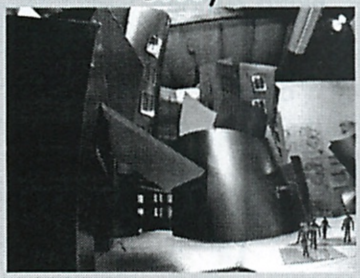
completing the proof by induction.

$$= \frac{r^{(n+1)+1}-1}{r-1}$$

The MIT Stata Center



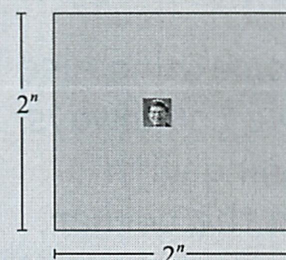
Design Mockup: Stata Lobby



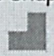
Mockup: Plaza Outside Stata

Goal: Tile the plaza except for 1×1 square in the middle for Bill.

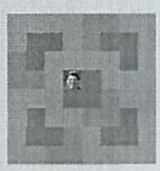
(Picture source: http://www.microsoft.com/presspass/exec/billg/default.asp)



Plaza Outside Stata

Gehry specifies L-shaped tiles covering three squares: 

For example, for 8 x 8 plaza might tile for Bill this way:



Plaza Outside Stata

Theorem: For any $2^n \times 2^n$ plaza, we can make Bill and Frank happy.

Proof: (by induction on n)

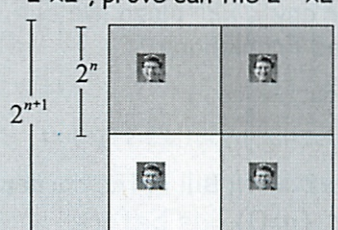
P(n) ::= can tile $2^n \times 2^n$ with Bill in middle.

Base case: (n=0)

 (no tiles needed)

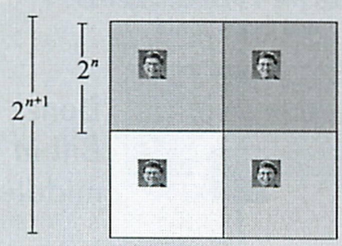
Plaza Outside Stata

Induction step: assume can tile $2^n \times 2^n$, prove can tile $2^{n+1} \times 2^{n+1}$.



Plaza Outside Stata

Now what?...



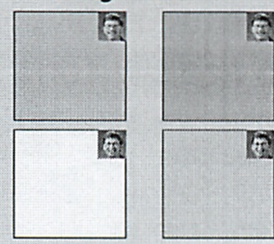
plaza outside Stata

The fix:

prove something else --that we can always find a tiling with Bill in the corner.

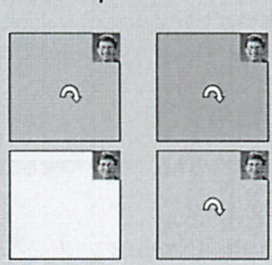
plaza outside Stata

Once have Bill in corner, can get Bill in middle:



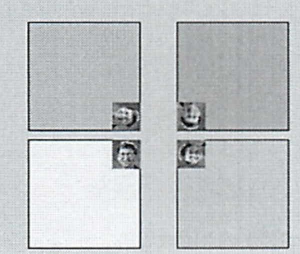
plaza outside Stata

method:
rotate the squares as indicated.



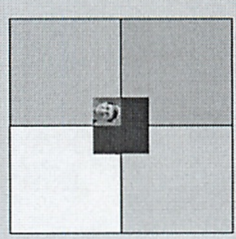
plaza outside Stata

after rotation have:



plaza outside Stata

now group the 4 squares together, and insert a tile.



Done! Bill in middle

plaza theorem

Theorem: For any $2^n \times 2^n$ plaza, we can make Bill and Frank happy.

Proof: (by induction on n)

REVISED induction hypothesis P(n) ::=

can tile $2^n \times 2^n$ with Bill in the corner

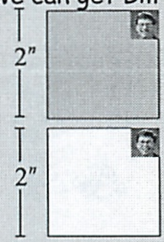
Base case: (n=0) as before

plaza proof

Induction step:

Assume we can get Bill in corner of $2^n \times 2^n$.

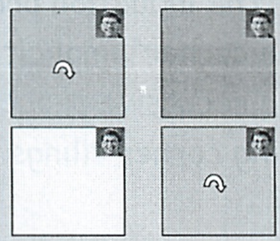
Prove we can get Bill in corner of $2^{n+1} \times 2^{n+1}$.



Albert R Meyer February 22, 2011 lec 4M.33

plaza proof

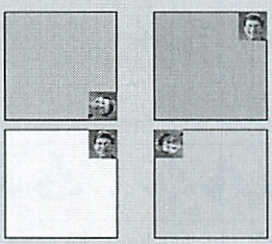
method: rotate the squares as indicated.



Albert R Meyer February 22, 2011 lec 4M.34

plaza proof

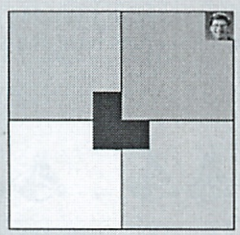
after rotation have:



Albert R Meyer February 22, 2011 lec 4M.35

plaza proof

now group the squares together, and fill the center with a tile.



Done!

Albert R Meyer February 22, 2011 lec 4M.36

ingenious induction hypothesis

Note 1: To prove "Bill in middle," we proved something else: "Bill in corner."

Albert R Meyer February 22, 2011 lec 4M.37

stronger induction hypotheses

Note 2: It may help to choose a stronger hypothesis than the desired result. (example in class problem)

Albert R Meyer February 22, 2011 lec 4M.38

recursive procedure

Note 3: The induction proof of "Bill in corner" implicitly defines a recursive procedure for finding corner tilings.

A False Proof

Theorem: All horses are the same color.

Proof: (by induction on n)

Induction hypothesis:

P(n) ::= any set of n horses have the same color

Base case (n=1):

horse is same color as itself! O.K.

...

A False Proof

(Inductive case)

Assume any n horses have the same color.

Prove that any n+1 horses have the same color.

...

n+1

A False Proof

(Inductive case)

Assume any n horses have the same color.

Prove that any n+1 horses have the same color.

2nd set of n horses have the same color

...

first set of n horses have the same color

A False Proof

(Inductive case)

Assume any n horses have the same color.

Prove that any n+1 horses have the same color.

1[st] and last same color as the middle ones

...

therefore the set of n+1 have the same color!

A False Proof

What's wrong?

Proof that $P(n) \rightarrow P(n+1)$ is wrong if $n = 1$, because there are no "middle" horses!

2nd set of n=1 horses

no horses

1st set of n=1 horses

A False Proof

What's wrong?

Proof that $P(n) \to P(n+1)$ is wrong if $n = 1$, because there are no "middle" horses!

(But proof works for all $n \neq 1$)

Strong Induction

Prove P(0). Then prove P(n+1) assuming all of

$P(0), P(1), \ldots, P(n)$

(instead of just P(n)).

Conclude $\forall m.P(m)$

Postage by Strong Induction

available stamps: 

5¢ 3¢

Thm: Get any amount $\geq$ 8¢

By strong induction with hyp:
P(n) ::= can form n + 8¢.

Postage by Strong Induction

available stamps: 

5¢ 3¢

Thm: Get any amount $\geq$ 8¢

base case P(0): make 0 + 8¢

 O.K.

Postage by Strong Induction

available stamps: 

5¢ 3¢

Thm: Get any amount $\geq$ 8¢

inductive step:
Assume m+8¢ for $n \geq m \geq 0$.
Prove can get n+9¢ .

Postage by Strong Induction

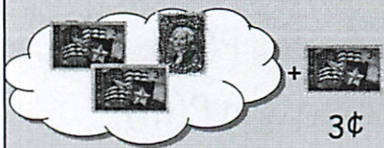
inductive step cases:

n=0, 0+9¢ =

n=1, 1+9¢ = 

Postage by Strong Induction

$n \geq 2$: so by hypothesis can get $(n-2)+8$¢

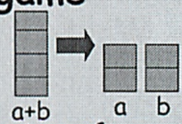


+ 3¢ = n+9¢

⊢(n-2)+8¢⊣

O.K.

Unstacking game



Start: a stack of boxes

Move: split any stack into two of sizes a,b>0

Scoring: $a \cdot b$ points

Keep moving: until stuck

Overall score: sum of move scores

Analyzing the Stacking Game

Claim: Every way of unstacking n blocks gives the same score:

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

Analyzing the Game

Claim: Starting with size n stack, final score will be

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

Proof: by Induction with Claim(n) as hypothesis

Proving the Claim by Induction

Base case n = 0:

$$\text{score} = 0 = \frac{0(0-1)}{2}$$

Claim(0) is O.K.

Proving the Claim by Induction

Inductive step. assume for stacks$\leq$n, and prove $C(n+1)$:

$$(n+1)\text{-stack score} = \frac{(n+1)n}{2}$$

Proving the Claim by Induction

Inductive step.

Case n+1 = 1. verify for 1-stack:

$$\text{score} = 0 = \frac{1(1-1)}{2}$$

C(1) is O.K.

Proving the Claim by Induction

Inductive step.

Case n+1 > 1. Split n+1 into an a-stack and b-stack, where a + b = n +1.

(a + b)-stack score = ab + a-stack score + b-stack score

Proving the Claim by Induction

by strong induction:

$$\text{a-stack score} = \frac{a(a-1)}{2}$$

$$\text{b-stack score} = \frac{b(b-1)}{2}$$

Proving the Claim by Induction

total (a + b)-stack score =

$$ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} =$$

$$\frac{(a+b)((a+b)-1)}{2} = \frac{(n+1)n}{2}$$

so C(n+1) is O.K.

We're done!

Team Problems

Problems

1–4

Induction

2/22

he claims less straightforward than WOP

0 is red
Any int next to a red int is red
some property

$R()$ = red property

$R(0)$, $R(0) \to R(1)$, $R(1) \to R(2)$, $R(2) \to R(3)$, ... $R(n) \to R(n+1)$

So $R(0), R(1), R(2), \ldots, R(n), \ldots$

horizontal line is infrence rule
if top established, bottom is proved

slightly diff from implies $\to$

$$\frac{R(0),\ \forall n.\ R(n) \to R(n+1)}{\forall m.\ R(m)}$$

domain of discourse $\mathbb{N}$

It's like Dominos

$$1 + r + r^2 + \ldots + r^n = \frac{r^{(n+1)} - 1}{r - 1}$$

geometric series

nice closed form formula

(2)

Can check by induction

Proof by induction on n

The induction hypothsis $P(n)$ is

$$1+r+r^2+\dots+r^n = \frac{r^{(n+1)}-1}{r-1}$$

Base case $(n=0)$

$$1+r+r^2+\dots+r^0 = \frac{r^{0+1}-1}{r-1}$$

$$r^0 = \frac{r-1}{r-1}$$

$$1 = 1$$

Induction: Assume $P(n)$ for some $n \geq 0$ and prove $P(n+1)$

(wherever I am I can take another step)

So add to r^{n+1} to both sides

Hope it simplifies

$$1+r+ \dots$$

algebra

$$= \frac{r^{(n+1)+1}-1}{r-1}$$

Proves $(n+1)$ completing ~~proof~~ proof by induction

③

2^n = a power of 2

Statue in the middle

Any one of the 4 middle squares

8x8 tile example in slides

Proof by induction Can tile $2^n \times 2^n$ w/ Bill in middle

Base case $(n=0)$

1×1 tile

Induction $2^{n+1} \times 2^{n+1}$

By thinking of $4 \times 2^n \cdot 2^n$ plazas

But have 4 Bills in the middle

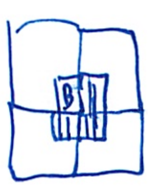
Stuck!

key: Need to find correct hypothesis

— No easy way to find it

corrallory → Prove something else that implies can get Bill in middle

That can always find tiling w/ Bill in corner



fill rest in w/ an L

(4)

Proof by induction on n

Can tile $2^n \times 2^n$ in the corner

Base ($n=0$)

as before

Inductive

Assume can get in corner of $2^n \times 2^n$

Prove we can get Bill in corner of $2^{n+1} \times 2^{n+1}$

(So don't have to show $n=1$, etc)

Implicit in them is some recursive thing

False Theorm: All horses are same color — Theorm not the mistake

Prove by induction on n

Hyp: any set of n horses have same color

Base ($n=1$)

- Only 1 horse, same color as itself

Induction Assume n horses have same color — not the mistake - since assume

Prove that any $n+1$ horses have the same color

$\underbrace{x \overbrace{x \ x \ x \ x}^{\text{2nd set same color}}}_{\text{First set of n are same color}}$

(5)

So ~~Old~~ 1st and last horse are same color as middle

What went wrong?

Proof that $P(n) \to P(n+1)$ is wrong

if $n=1 \to$ there are no middle horses

But works for $n \neq 1$

Strong Induction

Prove ~~All~~ $P(0)$ Then prove $P(n+1)$ assuming all of ~~all~~ the items before $P(0), P(1), \dots P(n)$ instead of just $P(n)$

Example Postage Can get any amt $\geq 8¢$ w/ $\boxed{5¢}$ $\boxed{3¢}$

Proof s.i. Can form $n+8¢$

Base case $(n=8)$

$\boxed{5¢}$ $\boxed{3¢}$

Inductive

Assume $m+8¢$ for $n \geq m \geq 0$

Prove can get to $9¢$

(6)

$n=0 \quad 0+9¢ = \boxed{3}\ \boxed{3}\ \boxed{3}$

$n=1 \quad 1+9¢ = \boxed{5}\ \boxed{5}$

$n \geq 2$ so by hyp

can get $(n-2)+8¢$

$\boxed{5}\ \boxed{5}\ \boxed{3} + \boxed{3} = n+9¢$

$\vdash (n-2)+8 \dashv$

can go from $n-2$ ~~so can do~~

since strong induction

Unstacking game

- skipping now

In-Class Problems Week 4, Tue.

$$\left(2-\frac{1}{n}\right)+\frac{1}{n}-\frac{1}{n+1}$$

$$||$$

$$\boxed{2-\frac{1}{n+1}}$$

Problem 1.
Prove by induction:

$$1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}<2-\frac{1}{n}, \quad (1)$$

for all $n > 1$.

Problem 2. (a) Prove by induction that a $2^n \times 2^n$ courtyard with a 1×1 statue of Bill in *any position* can be covered with L-shaped tiles.

(b) *(Discussion Question)* In part (a) we saw that it can be easier to prove a stronger theorem. Does this surprise you? How would you explain this phenomenon?

Problem 3.
Find all possible amounts of postage that can be paid exactly using 3 and 7 cent stamps. Use induction to prove that your answer is correct.

Problem 4.
The following Lemma is true, but the *proof* given for it below is defective. Pinpoint *exactly* where the proof first makes an unjustified step and explain why it is unjustified.

is an even divisor of

Lemma 4.1. *For any prime p and positive integers $n, x_1, x_2, \ldots, x_n$, if $p \mid x_1x_2\ldots x_n$, then $p \mid x_i$ for some $1 \le i \le n$.*

Bogus proof. Proof by strong induction on n. The induction hypothesis, $P(n)$, is that Lemma holds for n.

Base case $n = 1$: When $n = 1$, we have $p \mid x_1$, therefore we can let $i = 1$ and conclude $p \mid x_i$.

Induction step: Now assuming the claim holds for all $k \le n$, we must prove it for $n + 1$.

So suppose $p \mid x_1x_2\cdots x_{n+1}$. Let $y_n = x_nx_{n+1}$, so $x_1x_2\cdots x_{n+1} = x_1x_2\cdots x_{n-1}y_n$. Since the righthand side of this equality is a product of n terms, we have by induction that p divides one of them. If $p \mid x_i$ for some $i < n$, then we have the desired i. Otherwise $p \mid y_n$. But since y_n is a product of the two terms x_n, x_{n+1}, we have by strong induction that p divides one of them. So in this case $p \mid x_i$ for $i = n$ or $i = n + 1$. ■

$$\frac{1}{(n+1)^2} < \frac{1}{n} - \frac{1}{n+1}$$

$$1 < \frac{(n+1)^2}{n} - \frac{(n+1)^2}{n}$$

In Class Problems

2/22

1. Prove by induction

~~Base case $n=0$~~

$\frac{1}{0^2}$

$n > 1$

$n = 2$

$1 + \frac{1}{4} = 1\frac{1}{4} < 2 - \frac{1}{4}$

n^2 $\quad 1\frac{1}{4} < 1\frac{3}{4}$

2^2

Shown to work

Inductive Case Assume $P(n)$

$n = n+1$ it works for n

add $\frac{1}{(n+1)^2}$

ellipse so keep

$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} < 2 - \frac{1}{n} \cancel{+ \frac{1}{n+1}} \cancel{+ \frac{1}{n}}$

$< 2 - \frac{1}{n+1}$

②

$$1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} + \frac{1}{(n+1)^2} < 2 - \frac{1}{n+1}$$

$$2 - \frac{1}{n} + \frac{1}{n} - \frac{1}{n+1}$$

can show

algebra

can see $P(n)$ case

So drop

$$\frac{1}{(n+1)^2} < \frac{1}{n} - \frac{1}{n+1}$$

Ohhh

Show w/ algebra

$$\frac{1}{n^2+2n+1} < \frac{1}{n} - \frac{1}{n+1}$$

remember fraction algebra rules!

Multiply Through

$$1 < \frac{(n+1)^2}{n} - \frac{(n+1)^{\cancel{2}}}{\cancel{n+1}}$$

$$1 < \frac{n^2+2n+1}{n} - (n+1)$$

$$1 < \frac{\cancel{n^2}}{n} + \frac{2n}{n} + \frac{1}{n} - (n+1)$$

$$1 < \cancel{n} + \cancel{2} + \frac{1}{n} - \cancel{n} - \cancel{1} + 1$$

$$1 < 1 + \frac{1}{n}$$

Inductive case holds

③

2. $2^n \times 2^n$ cortyard

- in notes I believe

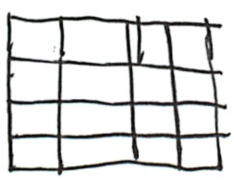
$n=0$ 

$n=1$ 

~~$n=2$~~ 

← This is the same formula, so don't have to include as a special case

2^n so 4



just put 4 of the above together

$n=3$ 2^3 so 8

put 4 of above together

But this is not induction!

Assume works for $2^n \times 2^n$

Show works for $2^{n+1} \times 2^{n+1}$

Just put 4 $2^n \times 2^n$ together which by strong induction we can show that we can orient the tiles in any way so that Bill fits.

(Not very well explained)

Forgot

Pick one

Can put anywhere

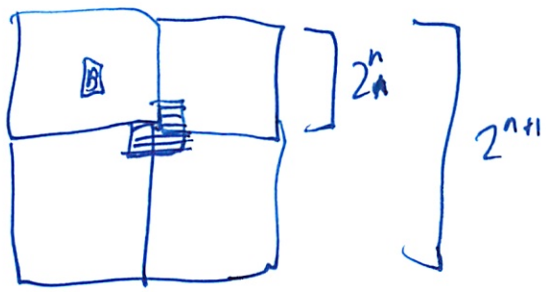
But on other 3

put Bill on corners

And then when put together, replace w L

④

Don't need strong i/ multiple cases



? Is that all you have to say?
I think I am getting the hang of this!

3. Find all amts of postage that can be paid w/ 3,7 cent stamps?

0 works ✓
1 x
2 x
3 $\boxed{3}$ ✓
4 x
5 x
6 $\boxed{3}$ $\boxed{3}$ ✓
7 $\boxed{7}$
8 x
9 $\boxed{3}$ $\boxed{3}$ $\boxed{3}$ ✓
10 $\boxed{7}$ $\boxed{3}$ ✓
11 x
12 $\boxed{3}$ $\boxed{3}$ $\boxed{3}$ $\boxed{3}$

5

13 $\boxed{7}\ \boxed{3}\ \boxed{3}$

14 $\boxed{7}\ \boxed{7}$

15 $\boxed{3}\ \boxed{3}\ \boxed{3}\ \boxed{3}\ \boxed{3}$

16 $\boxed{7}\ \boxed{3}\ \boxed{3}\ \boxed{3}$

12 13 14 actually better

ok this is ~~an~~ our base

Can add 3

Proof by strong induction

Hyp: Can make n postage w/ ~~1~~, 3, 7 ~~¢~~ stamps for $n \geq$ ~~11~~ 12

Base cases

12, 13, 14 above

Induction

Assume P(12)

Can do n+3 by adding a $\boxed{3}$

Should be good

Assume P(13)

Can do n+3 by adding a $\boxed{3}$

Assume P(14)

Can do n+3 by adding a $\boxed{3}$

Solutions to In-Class Problems Week 4, Tue.

Problem 1.
Prove by induction:

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}, \tag{1}$$

for all $n > 1$.

Solution. *Proof.* (By Induction). The induction hypothesis, $P(n)$, is the inequality (1).

Base Case ($n = 2$): The LHS of (1) in this case is $1 + 1/4$ and the RHS is $2 - 1/2$, and

$$\text{LHS } = 5/4 < 6/4 = 3/2 = \text{ RHS},$$

so inequality (1) holds, and $P(2)$ is proved.

Inductive Step: Let $n \geq 2$ be a nonnegative integer, and assume $P(n)$ in order to prove $P(n+1)$. That is, we assume (1). Adding $1/(n+1)^2$ to both sides of this inequality yields

$$\begin{aligned}
&1 + \frac{1}{4} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} \\
&< 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\
&= 2 - \left(\frac{1}{n} - \frac{1}{(n+1)^2}\right) \\
&= 2 - \left(\frac{n^2 + 2n + 1 - n}{n(n+1)^2}\right) \\
&= 2 - \frac{n^2 + n}{n(n+1)^2} - \frac{1}{n(n+1)^2} \\
&= 2 - \frac{1}{n+1} - \frac{1}{n(n+1)^2} \\
&< 2 - \frac{1}{n+1} && \text{(since } n > 0\text{).}
\end{aligned}$$

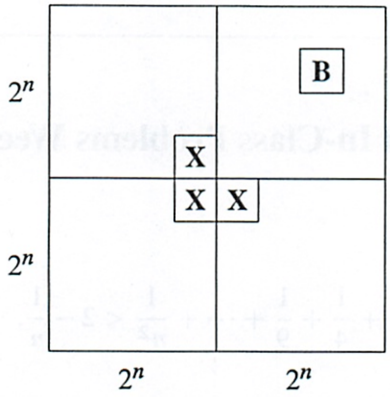
So we have proved $P(n+1)$. ■

Problem 2. (a) Prove by induction that a $2^n \times 2^n$ courtyard with a 1×1 statue of Bill in *any position* can be covered with L-shaped tiles.

Solution. Let $P(n)$ be the proposition that for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that $P(n)$ is true for some $n \geq 0$; that is, for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant contains Bill (**B** in the diagram below). Place a temporary Bill (**X** in the diagram) in each of the three central squares lying outside this quadrant:



Now we can tile each of the four quadrants by the induction assumption. Replacing the three temporary Bills with a single L-shaped tile completes the job. This proves that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. The theorem follows as a special case.

This proof has two nice properties. First, not only does the argument guarantee that a tiling exists, but also it gives a recursive procedure for finding such a tiling. Second, we have a stronger result: if Bill wanted a statue on the edge of the courtyard, away from the pigeons, we could accommodate him! ■

(b) *(Discussion Question)* In part (a) we saw that it can be easier to prove a stronger theorem. Does this surprise you? How would you explain this phenomenon?

Solution. It might seem that it ought to be harder to prove a more general theorem than a less general one, but sometimes not. For example, the more general result might actually be easier because it involves fewer assumptions, and this can help in avoiding the complications of unnecessary hypotheses.

But for an induction proof in particular, using a more general induction hypothesis means we can make a stronger *assumption* in the induction step —namely, we can assume a stronger $P(n)$ —which can make it easier to prove the conclusion of the induction step, namely, $P(n+1)$. ■

Problem 3.
Find all possible amounts of postage that can be paid exactly using 3 and 7 cent stamps. Use induction to prove that your answer is correct.

Solution. *Proof.* We can begin by observing that the following postage amounts can be made by 3 and 7 cent stamps:

$$\begin{aligned}
&0 \text{no stamps}\\
&3 = 3\\
&6 = 3 + 3\\
&7 = 7\\
&9 = 3 + 3 + 3\\
&10 = 3 + 7,
\end{aligned}$$

and these are the only amounts < 12 cents that can be paid. Now we prove that every amount ≥ 12 can also be paid. The proof is by strong induction on n with induction hypothesis

$$S(n) ::= \text{exactly } n + 12 \text{ cents postage can be paid with 3 and 7 cent stamps.}$$

Base case: $S(0)$. 12 cents can be paid using four 3 cent stamps.

Inductive step: We assume the strong hypothesis that $S(k)$ for $n \geq k \geq 0$. Now we mmust prove $S(n+1)$. The proof is by cases:

case $n = 0$: $S(0+1)$ holds because 13 cents postage can be paid using two 3 cents and a 7 cents stamps.

case $n = 1$: $S(1+1)$ holds because 14 cents postage can be paid using two 7 cent stamps.

case $n \geq 2$: Since $n \geq n-2 \geq 0$, we know by strong induction that $S(n-2)$ holds. But including an extra 3 cents stamp in the collection of 3 and 7 cent stamps that paid $(n-2)+12$ cents gives a collection that pays $(n-2)+12+3 = (n+1)+12$ cents, which proves $S(n+1)$.

Since $S(n+1)$ holds in any case, the inductive step has been proved.

It follows by strong induction that every amount of cents postage $\geq$ 12 can be mde with 3 and 7 cent stamps.

■

Problem 4.

The following Lemma is true, but the *proof* given for it below is defective. Pinpoint *exactly* where the proof first makes an unjustified step and explain why it is unjustified.

Lemma 4.1. *For any prime p and positive integers $n, x_1, x_2, \ldots, x_n$, if $p \mid x_1 x_2 \ldots x_n$, then $p \mid x_i$ for some $1 \leq i \leq n$.*

Bogus proof. Proof by strong induction on n. The induction hypothesis, $P(n)$, is that Lemma holds for n.

Base case $n = 1$: When $n = 1$, we have $p \mid x_1$, therefore we can let $i = 1$ and conclude $p \mid x_i$.

Induction step: Now assuming the claim holds for all $k \leq n$, we must prove it for $n+1$.

So suppose $p \mid x_1 x_2 \cdots x_{n+1}$. Let $y_n = x_n x_{n+1}$, so $x_1 x_2 \cdots x_{n+1} = x_1 x_2 \cdots x_{n-1} y_n$. Since the righthand side of this equality is a product of n terms, we have by induction that p divides one of them. If $p \mid x_i$ for some $i < n$, then we have the desired i. Otherwise $p \mid y_n$. But since y_n is a product of the two terms x_n, x_{n+1}, we have by strong induction that p divides one of them. So in this case $p \mid x_i$ for $i = n$ or $i = n+1$. ■

Solution. Notice that nowhere in the proof is the fact that p is prime used. So if this proof were correct, the Lemma would hold not just for prime p, but for any positive integer p. But of course, the Lemma is false when p is not prime, for example if $p = 6$, $x_1 = 3$ and $x_2 = 4$, we have $p \mid x_1 x_2$ but $\text{NOT}(p \mid x_1)$ and $\text{NOT}(p \mid x_2)$. So there has to be something wrong somewhere.

The statement "we have by strong induction that p divides one of them" is the place where the proof breaks down: it appeals to strong induction to justify applying the induction hypothesis for $2 = k \leq n$. But the base case was $n = 1$, so we can't assume $2 \leq n$. Note that the reasoning above is fine for every $n \geq 2$, so the whole proof would be fine if we had an argument to prove the claim for $n+1 = 2$.

Now in fact, if a prime, p divides $x_1 x_2$, it must divide x_1 or x_2; this fact is obvious if we assume the uniqueness of prime factorizations of integers, but the proof here never made use of this fact. An elementary proof of this fact appears in the chapter on number theory.

Notice that uniqueness of prime factorization is a much more general result than the simple Lemma here. This Lemma is even needed in the usual proof about prime factorization, so appealing to it to prove this Lemma would be circular. ■

6.042 Tutor

2/22

TP 4.2 Induction Rules

Identify Induction, S. Ind, WOP, None

1. $$\frac{P(0) \quad \forall m\,(\forall k \le m\ P(k) \to P(m+1))}{\forall n\ P(n)}$$

↙ seems like WOP ↙ put induction

Oh S. ind - ✓

nice watching

2. $$\frac{P(b) \quad \forall k \ge b\ P(k) \to P(k+1)}{\forall k \ge b\ P(k)}$$

Ind ✓

3. $$\frac{\exists n\ P(n)}{\exists m\,[P(m) \text{ and } (\forall k\ P(k) \to k \ge m)]}$$

?: all ks will be larger than m ↙ That work

Ind ✗

WOP? ✓ If let S be set $\{k \mid P(k)\}$ then $\exists n.\ P(n)$ says that S is non empty, and $[P(m)$ and $(\forall k.\ P(k) \to k \ge m)$ says that m is least # in S.

4. $$\frac{P(0), \quad \forall k > 0\ P(k) \to P(k+1)}{\forall n\ P(n)}$$

Ind ✗ really?

S Ind ✗

None ✓ what is it then?

→ Over

Looks like simple induction but antecedent k is strictly > 0
This leaves the possibility that P(0) does not imply P(1)
So prop. may not start.

2

5. $$\frac{\forall m\ (\forall k < m.\ P(k)) \rightarrow P(m)}{\forall n\ \ P(n)}$$

WOP X

S.Ind O

Why did I get them all wrong first?

Looks like #1 but w/o base case

But base case is when $m = 0$

Assumption of implications is "vacuously" true

↳ truth devoid of meaning

Conclusion is precisely that $P(0)$ is true

TP3 Postage by Ind

- Yeah ~~one 2 examp'~~ got much clearer in class today!

Choose a comment

12 or more from $\boxed{4}$ $\boxed{5}$

$\boxed{4}\boxed{4}\boxed{4}$

Any above but strong ind or WOP eaisest

(3)

Oh forgot / missed "or more"

because

I don't get since isn't reg ind best here
- if just want to prove 12 ¢, not any value

All 3 work

Simple requires an ~~extra~~ extra quantifier in induction hyp
- So they are counting this as more difficult
(How are you supposed to know this??)

Strong easiest ~~$Q(n) ::= \text{FORALL } k,\ 12 \le k \le n$ ([4] [5] make postage)~~

Base $n = 12, 13, 14, 15$

~~Having proved forall $n \ge 12$ $P(n)$ would be immediate corollary~~

WOP easy
- set of all counterexamples

{$n \ge 12$ | n-cent postage can't be formed w/ [4] [5]}

Assume set not empty
WOP implies min element
Can prove w/ same base cases
So no counterexamples, so claim true

4

TP 4.4 Bogus Induction

Fibonacci #   0 1 1 2 3 5 8 13

$F(0) = 0$
$F(1) = 1$
$F(n) = F(n-1) + F(n-2)$ for $n \geq 2$

False claim: Every Fib # even
False proof:

...

Where error?

5 suppose $n \geq 2$
How get there?
- Oh from above

(I am always bad at this)

Show $F(n)$ is even assuming $F(k)$ even for all $k < n$
- what k?
- all Fib # before that are even

Well 1 is not even

5 8
5 7 8 It's not the concluding line
58

5

Goal up to 8

really?

Or ~~is~~ are they just blaming it on the conclusion line?

Using st. in. we can conclude that $P(n)$ holds for $n \geq 0$ if we show

$P(0)$ ← lines 3,4

$P(0) \rightarrow P(1)$ ← proved nowhere

what I had!

$[P(0) \wedge P(1)] \rightarrow P(2)$ ← lines 5-7

$[P(0) \wedge P(1) \wedge P(2)] \rightarrow P(3)$

⋮

line 5 right track → would be natural place for prop 2

But saying $n \geq 2$ not $n \geq 1$ it skipps

I zeroed in on that!

Technically no logical error on 5 - simply start of $n \geq 2$ case

But it does make strategic error skipping $n = 1$ case

I thought he said its not the into or assumption line

Well this is conclusion

Mailed in

6

TP 4.5 Integer Multiplication

Suppose ~~#~~ following proc to multiply 2 $\mathbb{N}$ a,b

$x ::= a$
$y ::= b$
$p ::= 0$

If $x = 0$ then output p
If x = even set $x ::= \frac{x}{2}$ $y = 2y$
If x = odd set $x = x-1$ $p = p + y$

What are preserved invariants?
What is this again?
↳ if true for start, true for all reachable states

(1) $a = 4$ $b = 2$
(2). $x = 2$ $y = 4$
(3). $x = 1$ $y = 8$
(4) $x = 0$ $p = 8$

1. $xy = p$
 – no (1)
2. $xy = ab$
 no (4)

7

3. $xy + p = ab$

- yeah
- should check od

5 $a = 1$ $b = 1$

6 $x = 0$ $p = 1$

7 $a = 3$ $b = 6$

8 $x = 2$ $p = 6$

think good ✓

4. $xyp = ab$

no 4 ✓

Which get smaller at every transition?

- every one involved with?
- or all?

1. x ✓
2. xy
   does not get smaller on even?
   same

8

3. $p - y$

$(p + y) - y$

Same ?

4. $x + p$

↑ Sometimes bigger

TP 4.6 Chocolate Bars

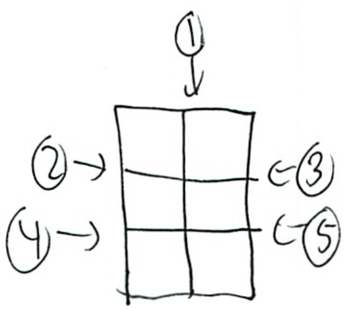
This looks like Stata squares

$m \times n$ sub bars

Want to divide into mn squares

↳ so all parts

Can only make horizontal cuts
vertical



S = # splits obtained

p = # of pieces

↳ individual pieces?

(9)

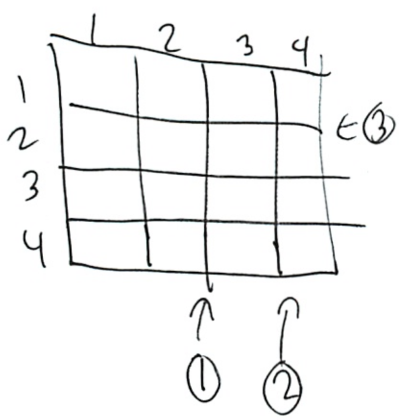
Part 1 Which are preserved invariants?

1. $s = p-1$

So our example

$s=0$ $p=1$
$s=1$ $p=2$
$s=2$ $p=3$
$s=4$ $p=4$
$s=$

So works but more complex



$s=0$ $p=1$
$s=1$ $p=2$
$s=2$ $p=3$
$s=3$ $p=4$

looks true

Is there a better way to prove $n+1$?

2. $s \neq p$
if 1 is true

(10)

3. $s = mn - p$

$s = 0 = 6 - 1$

No

Part 2 Get smaller w/ each transition

1. $mn - p$

↑ gets bigger each time

So yes

2. s

No gets ↑

3. $p - s$

Stays same p ↓ s ↑

Part 3 What # of pieces is at end of process

1. $p = mn - 1$

- no should $p = mn - 1$

(11)

2. $P = S - 1$

No from above $p = s + 1$

3. $p = mn$

Yes

Woot got lot better at that last part

Mathematics for Computer Science
MIT 6.042J/18.062J

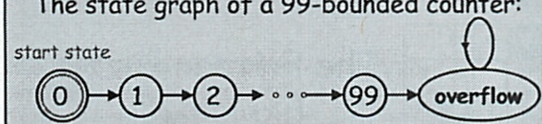
State Machines

State machines

step by step processes (may step in response to input —not today)

State machines

The state graph of a 99-bounded counter:



States: {0,1,...,99, **overflow**}

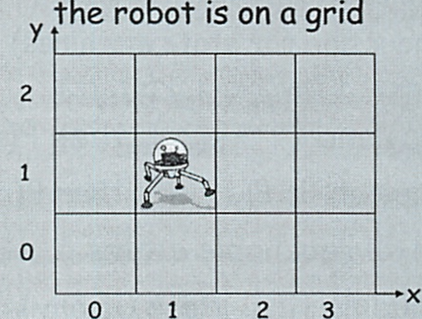
Transitions: $i \rightarrow i+1 \quad 0 \leq i < 99$

$99 \rightarrow$ **overflow**

overflow $\rightarrow$ **overflow**

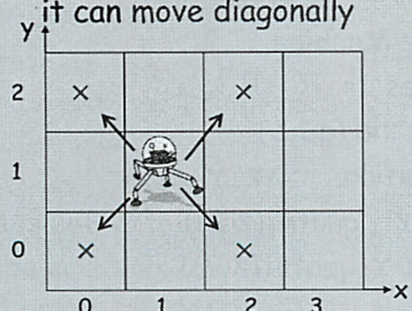
The Diagonal Robot

the robot is on a grid



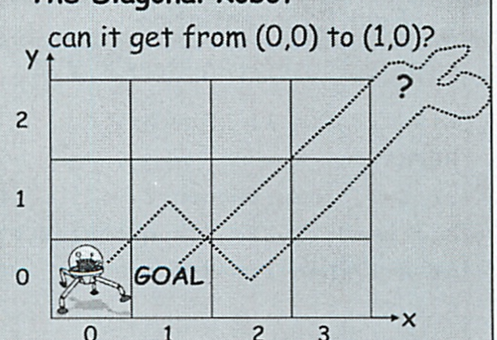
The Diagonal Robot

it can move diagonally



The Diagonal Robot

can it get from (0,0) to (1,0)?



Robot Preserved Invariant

NO! preserved invariant:

$P((x, y))$ ::= $x + y$ is even

move adds ±1 to **both** x & y,
preserving parity of x+y.
Also, $P((0, 0))$ is true.

Robot Preserved Invariant

So in all positions (x,y)
reachable from (0,0),
x + y stays even
But 1 + 0 = 1 is odd, so
(1,0) is not reachable

Floyd's Invariant Principle

(induction for state machines)

Preserved Invariant, P(state):

if P(q) and $q \to r$, then P(r)

Conclusion: if P(start), then P(r)
for all reachable states r,
including final state (if any)

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

The Fifteen Puzzle Explained!

--by similar reasoning
details in problem 2

Fast Exponentiation

compute a^b using registers X,Y,Z

```
X:= a;  Y:= 1;  Z:= b;
REPEAT:
if Z=0, then return Y
R:= remdr(Z,2); Z:= quotnt(Z,2)
if R=1,then Y:= X·Y
X:= X²
```


Fast Exponentiation

State Machine:

States ::= $\mathbb{R} \times \mathbb{R} \times \mathbb{N}$

start ::= (a,1,b)

transitions ::= $(X, Y, Z) \to$

$(X^2,\ Y,\ \text{quotnt}(Z,2))$ if $Z>0$ is even

$(X^2,\ X\cdot Y,\ \text{quotnt}(Z,2))$ if $Z>0$ is odd

Fast Exponentiation

Preserved Invariant: $YX^Z = a^b$

$(X, Y, Z) \rightarrow$ [Z>0 is odd]

$(X^2, X \cdot Y, (Z-1)/2)$

$(X \cdot Y)(X^2)^{(Z-1)/2} = (X \cdot Y)X^{Z-1}$

$= YX^Z = a^b$

O.K.

Partial Correctness

preserved invariant: $YX^Z = a^b$

at end Z=0, so return

$Y = YX^0 = a^b$

O.K.

Fast Termination

at each transition

Z:= quotient(Z,2)

Z= b at start, so Z= 0

in $\leq \log_2(b)$ transitions

O.K.

Robert W Floyd (1934–2001)

Eulogy by Knuth: http://www.acm.org/pubs/membernet/stories/floyd.pdf

Picture source: http://www.stanford.edu/dept/news/report/news/november7/floydobit-117.html

Team Problems

Problems

1 - 3

6.042 State Machines

To prove correct → do induction on steps they take

Invarient

Step by step ~~pro~~ processes

- many steps in response to an input
- not today though

State graph

start

0 → 1 → 2 → 3 → … → 99 → overflow

States $\{0, 1, \ldots, 99, \text{overflow}\}$

Transitions $i \to i+1 \quad 0 \le i < 99$

$99 \to \text{overflow}$

$\text{overflow} \to \text{overflow}$

Diagonal Robot

Can only move diagonally ↖ ↗ ↙ ↘

Can move $\{i \pm 1, j \pm 1\}$

Start $(0,0)$

Can it get from $(0,0)$ to $(1,0)$?

②

<u>No</u> ~~pres~~ preserved invariant

$P((x, y)) ::= x + y$ is even

A move adds ± 1 to both x, y ~~so~~ Preserving

Parity of $x+y$

$x+y$ can $+2, -2, 0$

If odd, it would stay odd

But start even, so stay even

So $(1,0)$ is not reachable

Floyd's Invariant Principal

Restatement of induction for SMs

<u>Preserved invariant</u> $P(\text{state})$:

if $P(q)$ and $q \to r$ then $P(r)$

Preserved no matter where you are

<u>Conclusion</u> if $P(\text{start})$ then $P(r)$ for all reachable r

Prove w/ induction on # of transitions

③

The 15 puzzle

the 6.042 logo

#2 today

Fast Expotientation

Compute a^b using registers X, Y, Z

Typical expoteniitation slow

$X = a \quad Y = 1 \quad Z = b$

Repeat:

if $Z = 0$ then return Y

$R :=$ remainder remdr $(Z, 2)$ $Z =$ quotient quotent $(Z, 2)$

if $R = 1$ then $Y := X \cdot Y$

$X := X^2$

He also wanted to do formal veification of program

State Machine

State $::= \mathbb{Q} \times \mathbb{Q} \times \mathbb{N}$ triples of # -set notation

Start $::= (a, 1, b)$

(9)

transitions ::= $(x, y, z) \rightarrow$

$(x^2, y, \text{quotnt}(z, 2))$ if $z > 0$ and even

$(x^2, x \cdot y, \text{quotnt}(z, 2))$ if $z > 0$ and odd

Preserved Invarient $y x^z = a^b$

Lets verify by checking transition

$(x, y, z) \rightarrow (x^2, x \cdot y), \frac{(z-1)}{2})$ $z > 0$ is odd

$(x \cdot y)(x^2)^{(z-1)/2} = (x \cdot y) x^{z-1}$

simplify

$x \cdot y x^{z-1}$ = so ✓ algebraically

$= y x^z = a^b$

This proves partical correctness

- proves that when there is an answer it is correct
  - a program may run forever
  - might not get an ans everytime
    - Usually prove it will terminate w/ WOP

5

If it stopes when $z=0$

It will return

$$Y = YX^0 = a^b$$

If it stops

But will $z=0$?

- yes b/c ~~zt~~ z always gets smaller
- each step gets halved or 0

$z=b$ at start so $z=0$ in $\leq \log_2(b)$ transitions

basically lenght of b in binary

In-Class Problems Week 4, Wed.

Problem 1.
Multiplying and dividing an integer n by 2 only requires a one digit left or right shift of the binary representation of n, which are hardware-supported fast operations on most computers. Here is a state machine, R, that computes the product of two nonnegative integers x and y using just these shift operations, along with integer addition:

$$\text{states} ::= \mathbb{N}^3 \qquad \text{(triples of nonnegative integers)}$$

$$\text{start state} ::= (x, y, 0)$$

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

(a) Verify that

$$P((r, s, a)) ::= \quad [rs + a = xy] \tag{1}$$

is an invariant of R. How about $Q((r, s, a)) ::= \quad [r = r + 1]$? :-)

(b) Prove that R is partially correct: if R reaches a final state, —a state from which no transition is possible —then $a = xy$.

(c) Briefly explain why this state machine will terminate after a number of transitions bouned by a small constant time the *length* of the binary representation of y.

(bounded.

Problem 2.
In this problem you will establish a basic property of a puzzle toy called the *Fifteen Puzzle* using the method of invariants. The Fifteen Puzzle consists of sliding square tiles numbered $1, \ldots, 15$ held in a 4×4 frame with one empty square. Any tile adjacent to the empty square can slide into it.

The standard initial position is

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

We would like to reach the target position (known in the oldest author's youth as "the impossible"):

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

A state machine model of the puzzle has states consisting of a 4×4 matrix with 16 entries consisting of the integers $1, \ldots, 15$ as well as one "empty" entry—like each of the two arrays above.

The state transitions correspond to exchanging the empty square and an adjacent numbered tile. For example, an empty at position $(2, 2)$ can exchange position with tile above it, namely, at position $(1, 2)$:

n_1	n_2	n_3	n_4
n_5		n_6	n_7
n_8	n_9	n_{10}	n_{11}
n_{12}	n_{13}	n_{14}	n_{15}

$\longrightarrow$

n_1		n_3	n_4
n_5	n_2	n_6	n_7
n_8	n_9	n_{10}	n_{11}
n_{12}	n_{13}	n_{14}	n_{15}

We will use the invariant method to prove that there is no way to reach the target state starting from the initial state.

We begin by noting that a state can also be represented as a pair consisting of two things:

1. a list of the numbers $1, \ldots, 15$ in the order in which they appear—reading rows left-to-right from the top row down, ignoring the empty square, and

2. the coordinates of the empty square—where the upper left square has coordinates $(1, 1)$, the lower right $(4, 4)$.

(a) Write out the "list" representation of the start state and the "impossible" state.

Let L be a list of the numbers $1, \ldots, 15$ in some order. A pair of integers is an *out-of-order pair* in L when the first element of the pair both comes *earlier* in the list and *is larger*, than the second element of the pair. For example, the list $1, 2, 4, 5, 3$ has two out-of-order pairs: (4,3) and (5,3). The increasing list $1, 2 \ldots n$ has no out-of-order pairs.

Let a state, S, be a pair $(L, (i, j))$ described above. We define the *parity* of S to be the mod 2 sum of the number, $p(L)$, of out-of-order pairs in L and the row-number of the empty square, that is the parity of S is $p(L) + i \pmod 2$.

(b) Verify that the parity of the start state and the target state are different.

(c) Show that the parity of a state is preserved under transitions. Conclude that "the impossible" is impossible to reach.

By the way, if two states have the same parity, then in fact there *is* a way to get from one to the other. If you like puzzles, you'll enjoy working this out on your own.

Problem 3.

A classroom is designed so students sit in a square arrangement. An outbreak of beaver flu sometimes infects students in the class; beaver flu is a rare variant of bird flu that lasts forever, with symptoms including a yearning for more quizzes and the thrill of late night problem set sessions.

Here is an illustration of a 6×6-seat classroom with seats represented by squares. The locations of infected students are marked with an asterisk.

*				*	
	*				
		*	*		
		*			
			*		*

Outbreaks of infection spread rapidly step by step. A student is infected after a step if either

- the student was infected at the previous step (since beaver flu lasts forever), or
- the student was adjacent to *at least two* already-infected students at the previous step.

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, the infection spreads as shown below.

*				*	
	*				
		*	*		
		*			
			*		*

$\Rightarrow$

*	*			*	
*	*	*			
	*	*	*		
		*			
		*	*		
		*	*	*	*

$\Rightarrow$

*	*	*		*	
*	*	*	*		
*	*	*	*		
	*	*	*		
		*	*	*	
		*	*	*	*

In this example, over the next few time-steps, all the students in class become infected.

Theorem. *If fewer than n students among those in an $n \times n$ arrangment are initially infected in a flu outbreak, then there will be at least one student who never gets infected in this outbreak, even if students attend all the lectures.*

Prove this theorem.

Hint: Think of the state of an outbreak as an $n \times n$ square above, with asterisks indicating infection. The rules for the spread of infection then define the transitions of a state machine. Show that

$$\begin{aligned} R(q) ::= &\text{The ``perimeter'' of the ``infected region''} \\ &\text{of state } q \text{ is at most } k, \end{aligned}$$

is a preserved invariant.

In Class 4 Wed

2/23

1. $\mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$
   - i like a definition?

$r = X, \mathbb{N}$ values
$s = Y, \mathbb{N}$ "
$a = 0, \mathbb{N}$ "

If ~~is even~~ $s = 0$ stop

If s is even
$r = 2r$
$s = \frac{s}{2}$
~~a~~

If s is odd
$r = 2r$
$s = \frac{s-1}{2}$
$a = a + r$

$P((r, s, a)) = [rs + a = xy]$

a) Is this invarient

(3)

b) R is machine

Partially correct = if you get an ans is correct

$a = xy$

At final $s = 0$

$x\ y$ don't change

a adds r

Just look at the invarient

$rs + a = xy$

$s=0$
at final

so $a = xy$

(why don't I see that?)

c) s gets smaller each transition

y is the start of s

(2)

On tutor tried things at
But ~~dater~~ should look at each option

If #1 $s=0$ no transition ✓ true

If #2 s even ✓

If #3 s odd s minus $\frac{1}{2} \cdot 2r$ } look $-r$ $+r$) 0
a adds r
~~⊗ Not~~ true

$$(2r)\left(\frac{s-1}{2}\right) + (a+r) = xy$$

$$rs - r + a + r$$

$$rs + a = xy$$

Perhaps is true

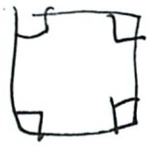
---

a2) $Q((r,s,a)) ::= [r = r+1]$
No - not true by def

(4)

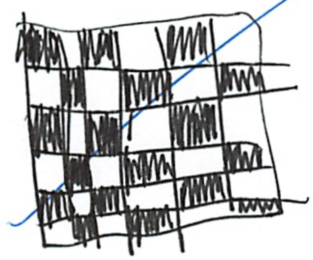
2. 15 Puzzle

3. Whats k?

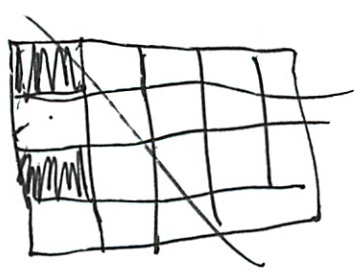


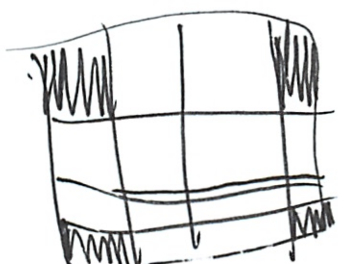
no one would get sick

Or at most checkerboard



No everyone first step





---

3 our board

For all infected cells i, let x_i be border w/ infected cell

If $x_i < 2$ infection will not spread, perim doesn't change

If $x_i = 2$ infection spreads, asorbs 2 borders + gains 2 new

- no net perim change

If $x_i = 3$ infection spreads. Asorbs 3 borders, gains 1

- Net perim -2

(5)

If $x_i = 4$ infection will spread
absorbs 4 borders
Perim ↓ 4

No possible transition that increases perim of infected region

If y students are initally infected, max perim of infected region is 4y if none of the y share a border

The perim of the entire region is 4n, so if $y < n$ the infected region can not have as great a perim as the entire region, so not all of $n \times n$ will be infected

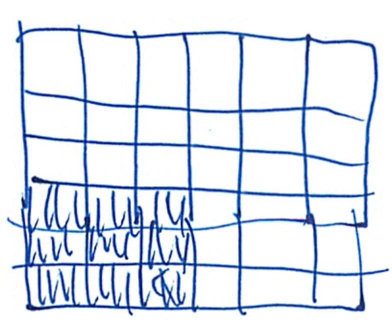
? Does it ans the qu they are asking

Arbitrary N

Just show for one

Just prove if $y < n$

Could do



Won't infect anyone more

The exact opposet we had

6

2.c. Horiz transition does not change row order
No parity change

Vertical - changes row by 1
changes relative order

Pickup 3 or drop 1 or 3 out of order pairs
- depends on initial order

Possible out of order pairs

n_2, n_3

n_2, n_4

n_2, n_5

If were out of order - will still be
If were not out of order - will still be

+ - + -
+ - - +   gaining or losing ordered pair
+ - - +

No way for it to be even
So parity does not change

Solutions to In-Class Problems Week 4, Wed.

Problem 1.
Multiplying and dividing an integer n by 2 only requires a one digit left or right shift of the binary representation of n, which are hardware-supported fast operations on most computers. Here is a state machine, R, that computes the product of two nonnegative integers x and y using just these shift operations, along with integer addition:

$$\text{states} ::= \mathbb{N}^3 \qquad \text{(triples of nonnegative integers)}$$

$$\text{start state} ::= (x, y, 0)$$

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

(a) Verify that

$$P((r, s, a)) ::= \quad [rs + a = xy] \tag{1}$$

is an invariant of R. How about $Q((r, s, a)) ::= \quad [r = r + 1]$? :-)

Solution. Q is a trivial invariant since it is always false.

To prove that P is invariant, assume that $P((r, s, a))$ and $(r, s, a) \longrightarrow (r', s', a')$. We must prove that $P((r', s', a'))$ holds, that is

$$r's' + a' = xy. \tag{2}$$

There are two cases corresponding to the transition cases:

If $s > 0$ is even, then we have that $r' = 2r, s' = s/2, a' = a$. Therefore,

$$\begin{aligned} r's' + a' &= 2r \cdot \frac{s}{2} + a \\ &= rs + a \\ &= xy \qquad \text{(by (1))}. \end{aligned}$$

If $s > 0$ is odd, we have $r' = 2r, s' = (s-1)/2, a = a + r$. So:

$$\begin{aligned} r's' + a' &= 2r \cdot \frac{s-1}{2} + a + r \\ &= r \cdot (s-1) + a + r \\ &= rs + a \\ &= xy \qquad \text{(by (1))}. \end{aligned}$$

So in both cases, (2) holds, proving that P is indeed an invariant. ■

(b) Prove that R is partially correct: if R reachs a final state, —a state from which no transition is possible —then $a = xy$.

Solution. Clearly, P holds for the start state because

$$P((x, y, 0)) \quad \text{iff} \quad [xy + 0 = xy].$$

The final states are those of the form $(r, 0, a)$. By the Invariant Principle, if $(r, 0, a)$ is reachable, then $P((r, 0, a))$ holds, that is,

$$a = r \cdot 0 + a = xy.$$

■

(c) Briefly explain why this state machine will terminate after a number of transitions bouned by a small constant time the *length* of the binary representation of y.

Solution. We claim that the termination condition, $s = 0$, will occur after at most $1 + \log_2 y$ transitions. But each transition reduces the value of s to $\leq s/2$. Hence, after at most $1 + \log_2 y$ transitions, the final value of s is at most $1/2^{1+\log_2 y} = 1/2y$ times its initial value, y. This means the value of s will be less than 1 and so must be 0 at this point if it wasn't 0 earlier. ■

Problem 2.
In this problem you will establish a basic property of a puzzle toy called the *Fifteen Puzzle* using the method of invariants. The Fifteen Puzzle consists of sliding square tiles numbered $1, \ldots, 15$ held in a 4×4 frame with one empty square. Any tile adjacent to the empty square can slide into it.

The standard initial position is

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

We would like to reach the target position (known in the oldest author's youth as "the impossible"):

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

A state machine model of the puzzle has states consisting of a 4×4 matrix with 16 entries consisting of the integers $1, \ldots, 15$ as well as one "empty" entry—like each of the two arrays above.

The state transitions correspond to exchanging the empty square and an adjacent numbered tile. For example, an empty at position $(2, 2)$ can exchange position with tile above it, namely, at position $(1, 2)$:

$$\begin{array}{|c|c|c|c|} \hline n_1 & n_2 & n_3 & n_4 \\ \hline n_5 & & n_6 & n_7 \\ \hline n_8 & n_9 & n_{10} & n_{11} \\ \hline n_{12} & n_{13} & n_{14} & n_{15} \\ \hline \end{array} \longrightarrow \begin{array}{|c|c|c|c|} \hline n_1 & & n_3 & n_4 \\ \hline n_5 & n_2 & n_6 & n_7 \\ \hline n_8 & n_9 & n_{10} & n_{11} \\ \hline n_{12} & n_{13} & n_{14} & n_{15} \\ \hline \end{array}$$

We will use the invariant method to prove that there is no way to reach the target state starting from the initial state.

We begin by noting that a state can also be represented as a pair consisting of two things:

1. a list of the numbers $1, \ldots, 15$ in the order in which they appear—reading rows left-to-right from the top row down, ignoring the empty square, and

2. the coordinates of the empty square—where the upper left square has coordinates $(1, 1)$, the lower right $(4, 4)$.

(a) Write out the "list" representation of the start state and the "impossible" state.

Solution. start: $((1\ 2\ \ldots\ 15), (4, 4))$,
impossible: $((15\ 14\ \ldots\ 1), (4, 4))$.

■

Let L be a list of the numbers $1, \ldots, 15$ in some order. A pair of integers is an *out-of-order pair* in L when the first element of the pair both comes *earlier* in the list and *is larger*, than the second element of the pair. For example, the list $1, 2, 4, 5, 3$ has two out-of-order pairs: (4,3) and (5,3). The increasing list $1, 2 \ldots n$ has no out-of-order pairs.

Let a state, S, be a pair $(L, (i, j))$ described above. We define the *parity* of S to be the mod 2 sum of the number, $p(L)$, of out-of-order pairs in L and the row-number of the empty square, that is the parity of S is $p(L) + i \pmod 2$.

(b) Verify that the parity of the start state and the target state are different.

Solution. The parity of the start state is

$$(0 + 4) \bmod 2 = 0.$$

The parity of the target is

$$((15 \cdot 14/2) + 4) \bmod 2 = 1.$$

■

(c) Show that the parity of a state is preserved under transitions. Conclude that "the impossible" is impossible to reach.

Solution. To show that the parity is constant, consider how moves may affect the parity. There are only 4 types of moves: a move to the left, a move to the right, a move to the row above, or a move to the row below.

Note that horizontal moves change nothing, and vertical moves both change i by 1, and move a tile three places forward or back in the list, L. To consider how the parity is changed in this case, we need to consider only the 3 pairs in L that are between the tile's old and new position. (The other pairs are not effected by the tile's move). This reverses the order of three pairs in L, changing the number of inversions by 3 or 1, but always by an odd amount.

To confirm this last remark, note that if the 3 pairs were all out of order or all in order before, the amount is changed by 3. If two pairs were out of order and 1 pair was in order or if one pair was out of order and two were in order, this will change the amount by 1. So the sum of i and the number of out-of-order pairs changes by an even amount (either 1+3 or 1+1), which implies that its parity remains the same. Since the initial state has parity 0 (even), all states reachable from the initial state must have parity 0, so the target state with parity 1 can't be reachable. ■

By the way, if two states have the same parity, then in fact there *is* a way to get from one to the other. If you like puzzles, you'll enjoy working this out on your own.

Problem 3.
A classroom is designed so students sit in a square arrangement. An outbreak of beaver flu sometimes infects students in the class; beaver flu is a rare variant of bird flu that lasts forever, with symptoms including a yearning for more quizzes and the thrill of late night problem set sessions.

Here is an illustration of a 6×6-seat classroom with seats represented by squares. The locations of infected students are marked with an asterisk.

*				*	
	*				
		*	*		
		*			
			*		*

Outbreaks of infection spread rapidly step by step. A student is infected after a step if either

- the student was infected at the previous step (since beaver flu lasts forever), or
- the student was adjacent to *at least two* already-infected students at the previous step.

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, the infection spreads as shown below.

*				*	
	*				
		*	*		
		*			
			*		*

$\Rightarrow$

*	*			*	
*	*	*			
	*	*	*		
		*			
		*	*		
		*	*	*	*

$\Rightarrow$

*	*	*		*	
*	*	*	*		
*	*	*	*		
	*	*	*		
		*	*	*	
		*	*	*	*

In this example, over the next few time-steps, all the students in class become infected.

Theorem. *If fewer than n students among those in an $n \times n$ arrangment are initially infected in a flu outbreak, then there will be at least one student who never gets infected in this outbreak, even if students attend all the lectures.*

Prove this theorem.

Hint: Think of the state of an outbreak as an $n \times n$ square above, with asterisks indicating infection. The rules for the spread of infection then define the transitions of a state machine. Show that

$$R(q) ::= \text{The “perimeter”' of the “infected region” of state } q \text{ is at most } k,$$

is a preserved invariant.

Solution. *Proof.* Define the *perimeter* of an infected set of students to be the number of edges with infection on exactly one side. Let ν be size (number of edges) in the perimeter.

We claim that ν is never gets bigger. This follows because the perimeter changes after a transition only because some squares became newly infected. By the rules above, each newly-infected square is adjacent to at least two previously-infected squares. Thus, for each newly-infected square, at least two edges are removed from the perimeter of the infected region, and at most two edges are added to the perimeter. Therefore, the perimeter of the infected region cannot increase, so if it is at lk in some state, it stays that way.

Now if an $n \times n$ grid is completely infected, then the perimeter of the infected region is $4n$. Thus, the whole grid can become infected only if the perimeter is initially at least $4n$. Since each square has perimeter 4, at least n squares must be infected initially for the whole grid to become infected. ■