

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

Mathematics for Computer Science
MIT 6.042J/18.062J

Sets & Functions

Albert R. Meyer February 14, 2011 lec 3M.1

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

What is a Set?

Informally:

A *set* is a collection of mathematical objects, with the collection treated as a single mathematical object.

(This is circular of course: what's a *collection*?)

Albert R. Meyer February 14, 2011 lec 3M.2

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

Some sets

real numbers, \mathbb{R}
 complex numbers, \mathbb{C}
 integers, \mathbb{Z}
 empty set, \emptyset
 set of all subsets of integers, $\text{pow}(\mathbb{Z})$
 the power set

Albert R. Meyer February 14, 2011 lec 3M.3

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

Some sets

$\{7, \text{"Albert R."}, \pi/2, \top\}$

A set with 4 elements: two numbers, a string, and a Boolean.

Same as

$\{\top, \text{"Albert R."}, 7, \pi/2\}$

-- order doesn't matter

Albert R. Meyer February 14, 2011 lec 3M.4

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

Membership

x is a member of A : $x \in A$

$\pi/2 \in \{7, \text{"Albert R."}, \pi/2, \top\}$

$\pi/3 \notin \{7, \text{"Albert R."}, \pi/2, \top\}$

$14/2 \in \{7, \text{"Albert R."}, \pi/2, \top\}$

Albert R. Meyer February 14, 2011 lec 3M.5

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

Synonyms for Membership

$x \in A$

x is an element of A

x is in A

Examples:

$7 \in \mathbb{Z}$, $2/3 \notin \mathbb{Z}$, $\mathbb{Z} \in \text{pow}(\mathbb{R})$

Albert R. Meyer February 14, 2011 lec 3M.6

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

In or Not In

An element is in or not in a set:
 $\{7, \pi/2, 7\}$ is same as $\{7, \pi/2\}$
 (No notion of being in the set more than once)



Albert R Meyer

February 14, 2011

lec 3M.7

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

Subset (\subseteq)

$A \subseteq B$ A is a subset of B
 A is contained in B

Every element of A is also
 an element of B :

$$\forall x [x \in A \text{ IMPLIES } x \in B]$$



Albert R Meyer

February 14, 2011

lec 3M.8

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

Subset

examples:

$$\mathbb{Z} \subseteq \mathbb{R}, \mathbb{R} \subseteq \mathbb{C}, \{3\} \subseteq \{5, 7, 3\}$$

$$A \subseteq A, \quad \emptyset \subseteq \text{every set}$$



Albert R Meyer

February 14, 2011

lec 3M.9

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

$\emptyset \subseteq \text{everything}$

def: $\emptyset \subseteq B$

$$\forall x \underbrace{[x \in \emptyset \text{ IMPLIES } x \in B]}_{\text{true}}$$



Albert R Meyer

February 14, 2011

lec 3M.10

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

Defining Sets

The set of elements, x , in A
 such that $P(x)$ is true.

$$\{x \in A \mid P(x)\}$$



Albert R Meyer

February 14, 2011

lec 3M.11

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

Defining Sets

The set of even integers:

$$\{n \in \mathbb{N} \mid n \text{ is even}\}$$



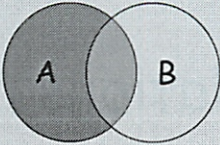
Albert R Meyer

February 14, 2011

lec 3M.12

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

New sets from old



Venn Diagram for 2 Sets

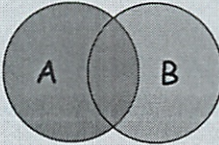
Albert R Meyer

February 14, 2011

lec 3M.14

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

union



$A \cup B ::= \{x \mid x \in A \text{ OR } x \in B\}$

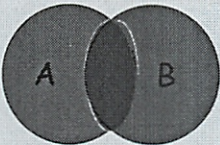
Albert R Meyer

February 14, 2011

lec 3M.15

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

intersection



$A \cap B ::= \{x \mid x \in A \text{ AND } x \in B\}$

Albert R Meyer

February 14, 2011

lec 3M.16

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

A set-theoretic equality

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

proof: Show these have the same elements, namely,

$x \in \text{Left Hand Set}$ iff $x \in \text{RHS}$ for all x .

Albert R Meyer

February 14, 2011

lec 3M.18

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

A set-theoretic equality

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

proof uses fact from last time:

$P \text{ OR } (Q \text{ AND } R) \text{ equiv}$

$(P \text{ OR } Q) \text{ AND } (P \text{ OR } R)$

Albert R Meyer

February 14, 2011

lec 3M.19

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

A set-theoretic equality

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

proof: $x \in A \cup (B \cap C)$ iff
 $x \in A \text{ OR } x \in (B \cap C)$ (def of \cup) iff
 $x \in A \text{ OR } (x \in B \text{ AND } x \in C)$ (def \cap) iff
 $(x \in A \text{ OR } x \in B) \text{ AND } (x \in A \text{ OR } x \in C)$
 (by the equivalence)

Albert R Meyer

February 14, 2011

lec 3M.20

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

A set-theoretic equality

proof:

$(x \in A \text{ OR } x \in B) \text{ AND } (x \in A \text{ OR } x \in C)$ iff
 $(x \in A \cup B) \text{ AND } (x \in A \cup C)$ (def \cup) iff
 $x \in (A \cup B) \cap (A \cup C)$ (def \cap).
 QED



Albert R. Meyer

February 14, 2011

lec 3M.21

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

Relations & Functions



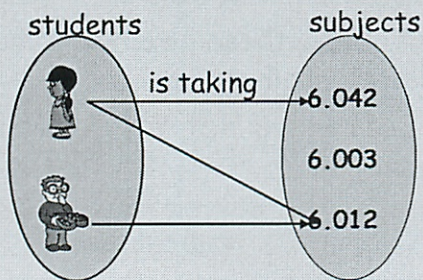
Albert R. Meyer

February 14, 2011

lec 3M.25

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

"is taking subject" relation



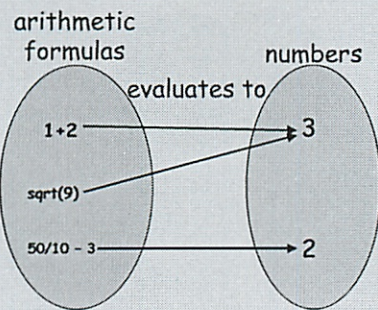
Albert R. Meyer

Copyright © Albert R. Meyer

lec 3M.26

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

formula "evaluation" relation



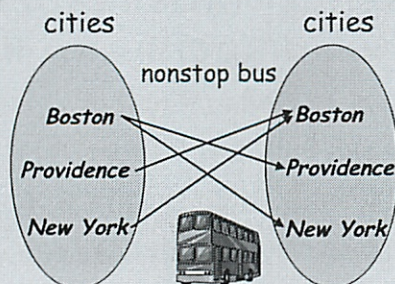
Albert R. Meyer

Copyright © Albert R. Meyer

lec 3M.27

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

"nonstop bus trip" relation



Albert R. Meyer

February 14, 2011

lec 3M.28

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

Binary relations

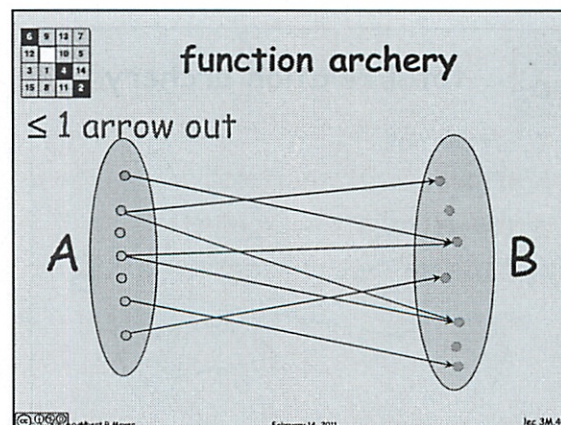
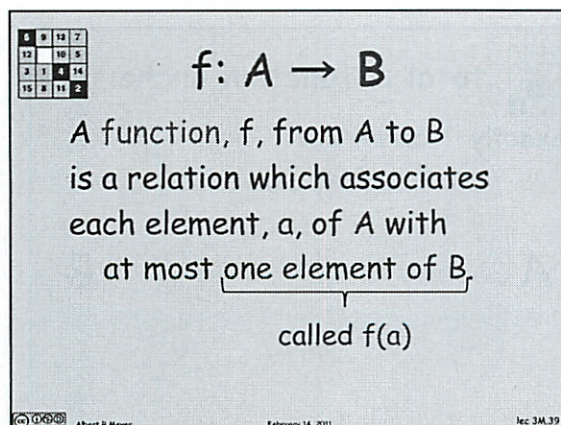
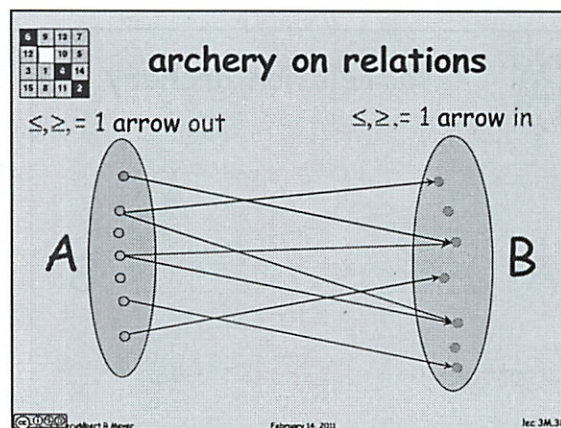
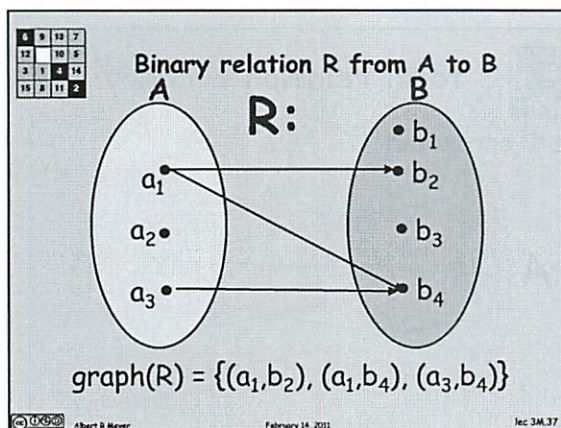
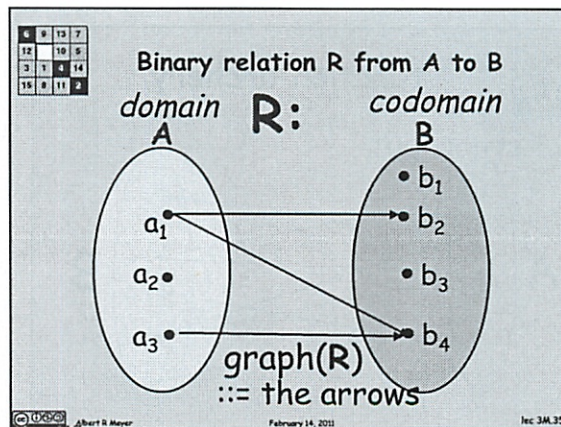
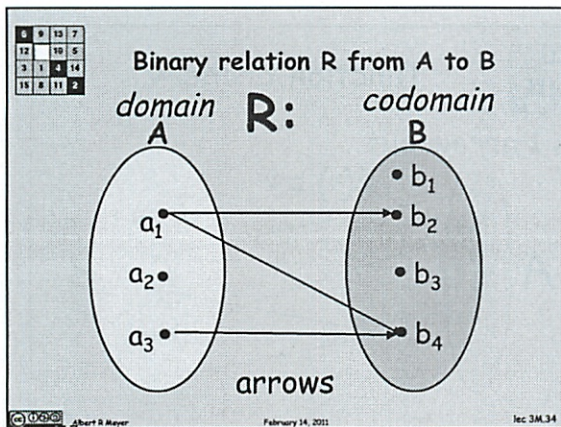
A binary relation, R , from a
 set A to a set B
 associates of elements of
 A with elements of B .

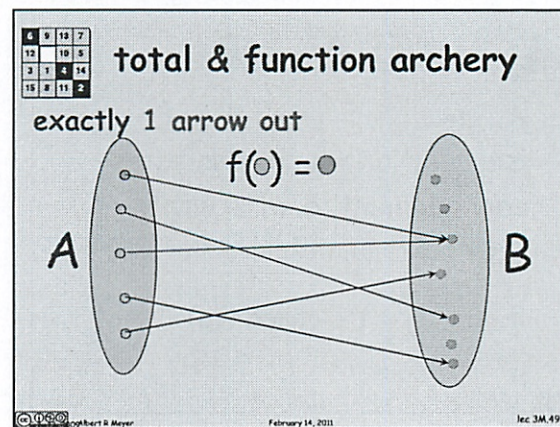
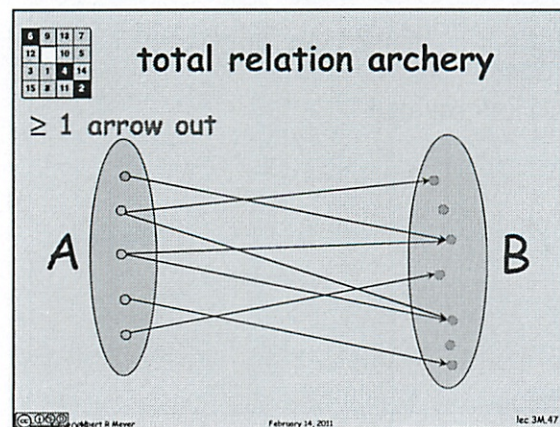
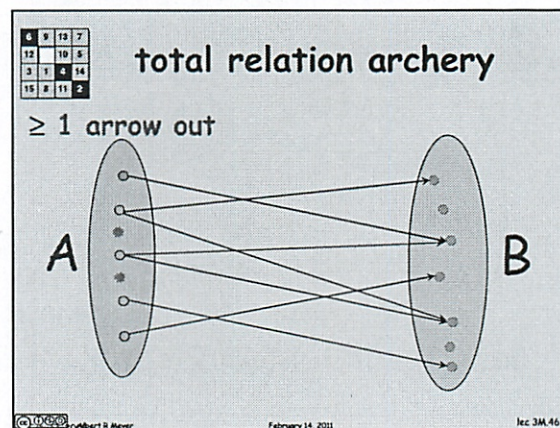
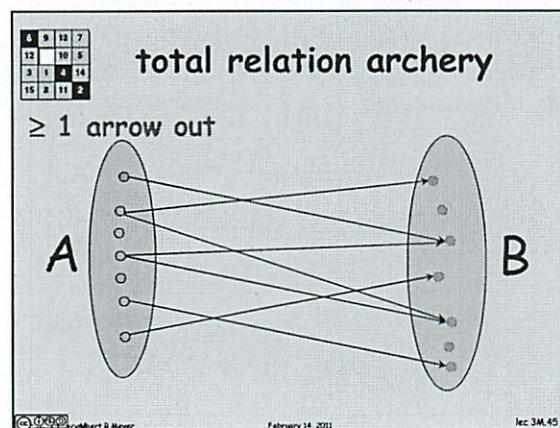
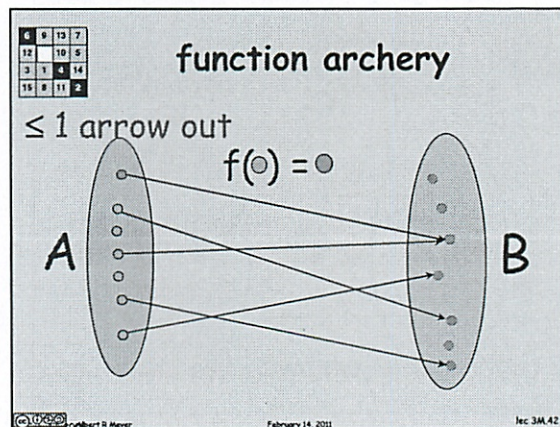
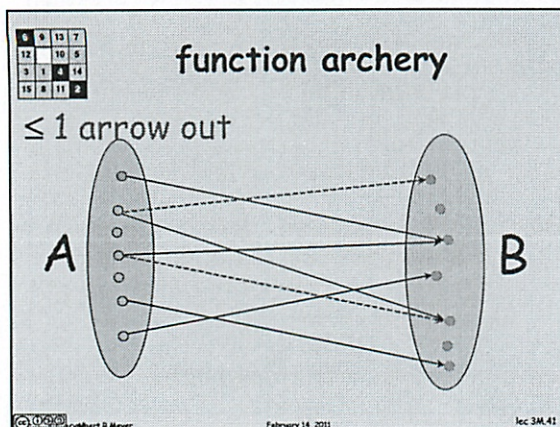


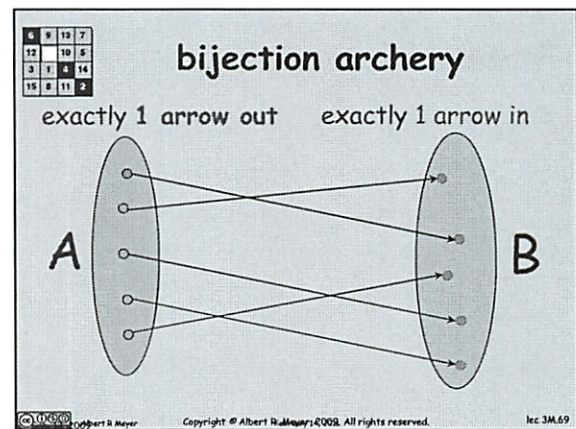
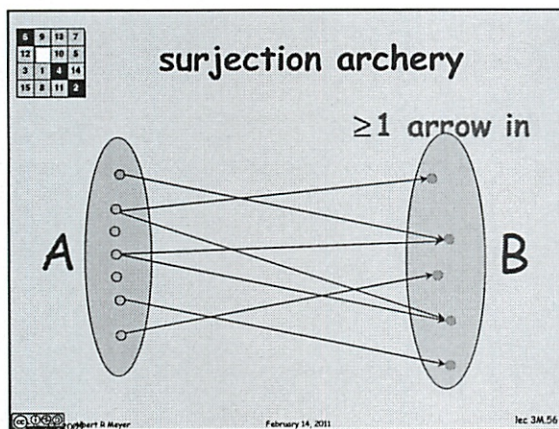
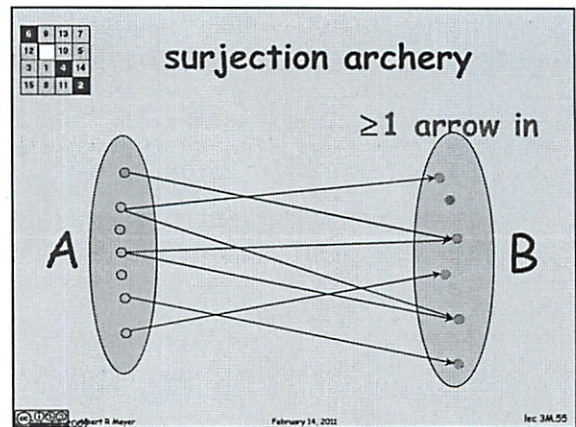
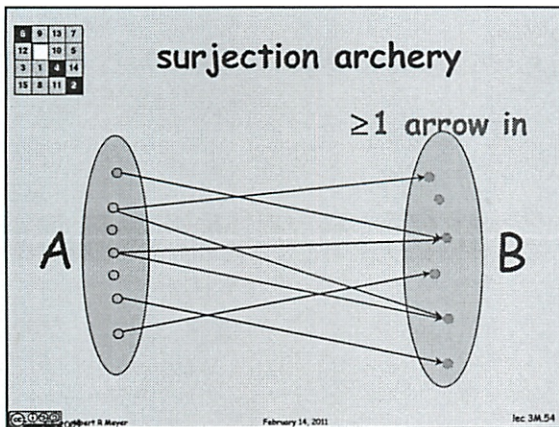
Albert R. Meyer

February 14, 2011

lec 3M.33







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

Mapping Rule (bij)

A bijection from
A to B implies

$$|A| = |B|$$

A is same size as B

lec 3M.70

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

Team Problems

Problems

1—4

lec 3M.71

(5 min late)

~~sets~~ \mathbb{N}
 \mathbb{R} etc

$\{ \text{ele1}, \text{ele2}, \dots \}$

often sets of mixed type

no notion of order

Lists are more fundamental in computers

But non-order is important in sets

$x \in A$

$\hookrightarrow x$ is an element in A

\notin not in set

Can describe any way $7 = \frac{14}{2}$

Power set - set of all subsets

$\mathbb{Z} \in \text{pow}(\mathbb{R})$

Don't confuse membership and
in or not in \hookrightarrow single elements

- a multiset does care

~~membership~~

Containment

\hookrightarrow subsets

$\{2\}$

\subseteq = subset

$A \subseteq B \rightarrow A$ is contained in B

②

Every element of A is also an element of B

$$\mathbb{Z} \subseteq \mathbb{R}$$

$$\mathbb{R} \subseteq \mathbb{C}$$

Don't confuse 3 with $\{3\}$

- type errors in computers

$$\{3\} \subseteq \{5, 7, 3\}$$

↑ everything in here ↑ is in here

$\emptyset \subseteq$ every set

- Since if - part is false in the implication

Defining sets - items that $P(x)$ holds

$$\{x \in A \mid P(x)\}$$

↑
such that

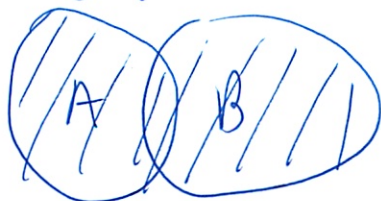
non neg even

$$\{n \in \mathbb{N} \mid n \text{ is even}\}$$

Union \cup

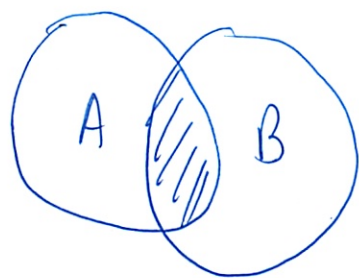
~~A~~

OR



③

Intersection \cap AND



Can use Truth Tables

\times distributes over $+$
 $+$ " " \times

Two sets are equal if they have the same elements

A series of 'iff' proofs

Can verify ~~then~~ with truth table

Keep changing assertion till propositional combo of other assertion

Propositional combinations

identities - truth table reasons

Relations + functions

Can build everything out of ~~a~~ sets

- start w/ empty set \emptyset

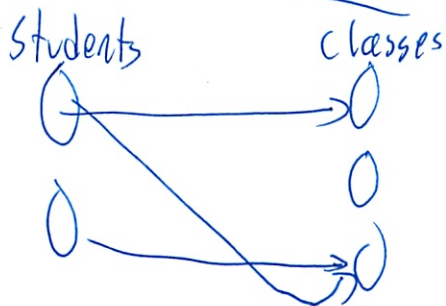
- pedantic

(4)

binary relation

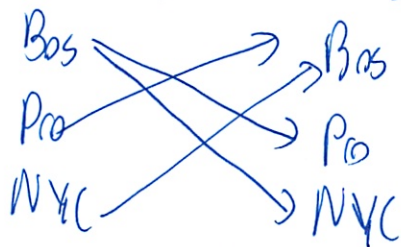
— relation b/w 2 things

relation is taking



3 components
of a relation

non stop busses
Cities cities



2 sets that
happen to be the
same

left set, right set, relation (arrows)

will see a large # of examples

Associates elements of a to b

Domain = left set

Codomain = right set

arrows = graph

$$\text{graph}(R) = \{(a_1, b_2), (a_2, b_2)\}$$

5

May be items w/o arrows or multiple arrows in

range = items in codomain with arrows coming in

Archer

Classifying relations w/ # of arrows out or in

is it $\leq, \geq, =$

function

relation between domain + codomain

Each element A maps to at ~~one~~ most one element of ~~for~~ $A \rightarrow B$
- called $f(a)$

Can just use arrows

- don't need to worry about verbs

(now makes a lot more sense, from H&S)

total relation = ≥ 1 arrow out

- can have more than one, it's not a function

total and function = exactly 1 arrow out

surjection = at least one arrow in

bijection = perfect correspondence = exactly 1 arrow in and out
perfect line up

$|A| = |B|$ same size

⑥

Miniquiz Wed

- 1 sided notes written or typed

In-Class Problems Week 3, Mon.

Problem 1.

Set Formulas and Propositional Formulas.

- (a) Verify that the propositional formula $(P \text{ AND } \overline{Q}) \text{ OR } (P \text{ AND } Q)$ is equivalent to P .
- (b) Prove that¹

$$A = (A - B) \cup (A \cap B)$$

for all sets, A, B , by using a chain of iff's to show that

$$x \in A \text{ IFF } x \in (A - B) \cup (A \cap B)$$

for all elements, x .

Problem 2.

Subset take-away² is a two player game involving a fixed finite set, A . Players alternately choose nonempty subsets of A with the conditions that a player may not choose

- the whole set A , or
- any set containing a set that was named earlier.

The first player who is unable to move loses the game.

For example, if A is $\{1\}$, then there are no legal moves and the second player wins. If A is $\{1, 2\}$, then the only legal moves are $\{1\}$ and $\{2\}$. Each is a good reply to the other, and so once again the second player wins.

The first interesting case is when A has three elements. This time, if the first player picks a subset with one element, the second player picks the subset with the other two elements. If the first player picks a subset with two elements, the second player picks the subset whose sole member is the third element. Both cases produce positions equivalent to the starting position when A has two elements, and thus leads to a win for the second player.

Verify that when A has four elements, the second player still has a winning strategy.³

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer.

¹The set difference, $A - B$, of sets A and B is

$$A - B ::= \{a \in A \mid a \notin B\}.$$

²From Christenson & Tilford, *David Gale's Subset Takeaway Game*, *American Mathematical Monthly*, Oct. 1997

³David Gale worked out some of the properties of this game and conjectured that the second player wins the game for any set A . This remains an open problem.

Problem 3.

The *inverse*, R^{-1} , of a binary relation, R , from A to B , is the relation from B to A defined by:

$$b R^{-1} a \text{ iff } a R b.$$

In other words, you get the diagram for R^{-1} from R by “reversing the arrows” in the diagram describing R . Now many of the relational properties of R correspond to different properties of R^{-1} . For example, R is *total* iff R^{-1} is a *surjection*.

Fill in the remaining entries in this table:

R is	iff	R^{-1} is
total		a surjection
a function		
a surjection		
an injection		
a bijection		

Hint: Explain what’s going on in terms of “arrows” from A to B in the diagram for R .

Problem 4.

Define a *surjection relation*, *surj*, on sets by the rule

Definition. $A \text{ surj } B$ iff there is a surjective **function** from A to B .

Define the *injection relation*, *inj*, on sets by the rule

Definition. $A \text{ inj } B$ iff there is a total injective *relation* from A to B .

- Prove that if $A \text{ surj } B$ and $B \text{ surj } C$, then $A \text{ surj } C$.
- Explain why $A \text{ surj } B$ iff $B \text{ inj } A$.
- Conclude from (a) and (b) that if $A \text{ inj } B$ and $B \text{ inj } C$, then $A \text{ inj } C$.

Arrow Properties

Definition. A binary relation, R is

- is a *function* when it has the $[\leq 1 \text{ arrow out}]$ property.
- is *surjective* when it has the $[\geq 1 \text{ arrows in}]$ property. That is, every point in the righthand, codomain column has at least one arrow pointing to it.
- is *total* when it has the $[\geq 1 \text{ arrows out}]$ property.
- is *injective* when it has the $[\leq 1 \text{ arrow in}]$ property.
- is *bijection* when it has both the $[= 1 \text{ arrow out}]$ and the $[= 1 \text{ arrow in}]$ property.

In Class Problems 3 Mon

2/14

1a Isn't this what we went over in class?

b

2. The 2nd player always wins - means 2nd player always removes last element
1st player can always ~~have~~ let 2nd player win

1 item $\{1\}$

1st player $\{1\}$ - can't move whole set

~~Q~~

2 items $\{1, 2\}$

1st player $\{1\}$

2nd player $\{2\}$ wins

3 items $\{1, 2, 3\}$

1st player $\{1, 2\}$

2nd player $\{3\}$ wins

← but would never do

3 items alt

1st player $\{1\}$

2nd player $\{2, 3\}$ wins

~~1st ~~2nd~~ player $\{3\}$ wins~~

is like starting w/
set of 2

(2)

n items

1st player {1} & he can't take all up front

2nd player rest wins

↳ repeats ~~at a certain pt~~
above case

n items at

1st player {1, 2}

2nd player rest wins

n items at

1st player n-1 items

2nd player nth item wins

But it says
problem is still
open - so no
known solution
Means you're prob
wrong!

Can use trees of cases

$$1a \quad (P \text{ AND } \bar{Q}) \text{ OR } (P \text{ AND } Q) = P$$

$$P \text{ AND } (\bar{Q} \text{ OR } Q) = P$$

↳ always true

By distributive law of AND

$$P \text{ AND True} = P$$

Not close to what we did in class
Other groups did truth table

3

1b. $x \in A$ iff $x \in (A-B) \cup (A \cap B)$ By def. of $A-B$ and AND

$x \in A$ iff $(x \in A \cap x \notin B) \cup (x \in A \cap x \in B)$

$x \in A$ iff $(x \in A) \cap (x \notin B \cup x \in B)$

By distributive law of AND

↑ always true

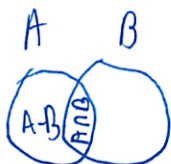
$x \in A$ iff $(x \in A) \cap \text{True}$

↑ x is an ele of A if this is true

$x \in A$ iff $x \in A$ ~~QED~~ ~~■~~

(Study + learn! Be able to do)

TA: Wording + order is not right



3

total	surjection
function	injections
surjection	total
injection	function
bijection	bijection

Replace out w/ is

[Faint handwritten signature]

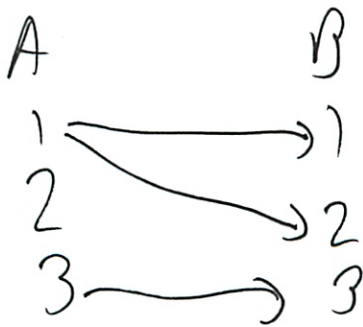
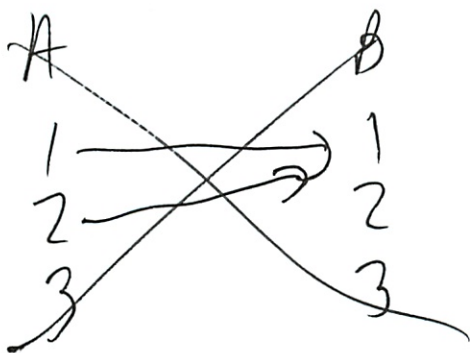
4. No more than 1 arrow at

$A \xrightarrow[\text{maps}]{\text{all of}} B \xrightarrow[\text{maps}]{\text{all of}} C$

Could draw diagrams

The diagram shows two sets of three elements, labeled A and B. Set A contains elements 1, 2, and 3. Set B contains elements 1, 2, and 3. Lines connect elements in A to elements in B: 1 to 1, 1 to 2, 2 to 1, 2 to 2, 3 to 1, and 3 to 2. A diagonal line is drawn across the entire diagram, crossing all connections.

A



Something about arrow counts

Solutions to In-Class Problems Week 3, Mon.

Problem 1.

Set Formulas and Propositional Formulas.

(a) Verify that the propositional formula $(P \text{ AND } \overline{Q}) \text{ OR } (P \text{ AND } Q)$ is equivalent to P .

Solution. There is a simple verification by truth table with 4 rows which we omit.

There is also a simple cases argument: if Q is **T**, then the formula simplifies to $(P \text{ AND } \mathbf{F}) \text{ OR } (P \text{ AND } \mathbf{T})$ which further simplifies to $(\mathbf{F} \text{ OR } P)$ which is equivalent to P .

Otherwise, if Q is **F**, then the formula simplifies to $(P \text{ AND } \mathbf{T}) \text{ OR } (P \text{ AND } \mathbf{F})$ which is likewise equivalent to P .

Finally, there is a proof by propositional algebra:

$$\begin{aligned} (P \text{ AND } \overline{Q}) \text{ OR } (P \text{ AND } Q) &\longleftrightarrow P \text{ AND } (\overline{Q} \text{ OR } Q) && \text{(distributivity)} \\ &\longleftrightarrow P \text{ AND } \mathbf{T} \longleftrightarrow P. \end{aligned}$$

(b) Prove that¹

$$A = (A - B) \cup (A \cap B)$$

for all sets, A, B , by using a chain of iff's to show that

$$x \in A \text{ IFF } x \in (A - B) \cup (A \cap B)$$

for all elements, x .

Solution. Two sets are equal iff they have the same elements, that is, x is in one set iff x is in the other set, for any x . We'll now prove this for A and $(A - B) \cup (A \cap B)$.

$$\begin{aligned} x \in (A - B) \cup (A \cap B) & \\ \text{iff } x \in (A - B) \text{ OR } x \in (A \cap B) & \quad \text{(by def of } \cup) \\ \text{iff } (x \in A \text{ AND } \overline{x \in B}) & \\ \text{OR } (x \in A \text{ AND } x \in B) & \quad \text{(by def of } \cap \text{ and } -) \\ \text{iff } (P \text{ AND } \overline{Q}) \text{ OR } (P \text{ AND } Q) & \quad \text{(where } P ::= [x \in A] \text{ and } Q ::= [x \in B]) \\ \text{iff } P & \quad \text{(by part (a))} \\ \text{iff } x \in A & \quad \text{(by def of } P). \end{aligned}$$

$$A - B ::= \{a \in A \mid a \notin B\}.$$

Problem 2.

Subset take-away² is a two player game involving a fixed finite set, A . Players alternately choose nonempty subsets of A with the conditions that a player may not choose

- the whole set A , or
- any set containing a set that was named earlier.

The first player who is unable to move loses the game.

For example, if A is $\{1\}$, then there are no legal moves and the second player wins. If A is $\{1, 2\}$, then the only legal moves are $\{1\}$ and $\{2\}$. Each is a good reply to the other, and so once again the second player wins.

The first interesting case is when A has three elements. This time, if the first player picks a subset with one element, the second player picks the subset with the other two elements. If the first player picks a subset with two elements, the second player picks the subset whose sole member is the third element. Both cases produce positions equivalent to the starting position when A has two elements, and thus leads to a win for the second player.

Verify that when A has four elements, the second player still has a winning strategy.³

Solution. There are way too many cases to work out by hand if we tried to list all possible games. But the elements of A all behave the same, so we can cut to a small number of cases using the fact that permuting around the elements of A in any game yields another possible game. We can do this by not mentioning specific elements of A , but instead using the *variables* a, b, c, d whose values will be the four elements of A .

We consider two cases for the move of the Player 1 when the game starts:

1. Player 1 chooses a one element or a three element subset. Then Player 2 should choose the complement of Player one's choice. The game then becomes the same as playing the $n = 3$ game on the three element set chosen in this first round, where we know Player 2 has a winning strategy.
2. Player 1 chooses a subset of 2 elements. Let a, b be these elements, that is, the first move is $\{a, b\}$. Player 2 should choose the complement, $\{c, d\}$, of Player 1's choice. We then have the following subcases:
 - (a) Player 1's second move is a one element subset, $\{a\}$. Player 2 should choose $\{b\}$. The game is then reduced to the two element game on $\{c, d\}$ where Player 2 has a winning strategy.
 - (b) Player 1's second move is a two element subset, $\{a, c\}$. Player 2 should choose its complement, $\{b, d\}$. This leads to two subsubcases:
 - i. Player 1's third move is one of the remaining sets of size two, $\{a, d\}$. Player 2 should choose its complement, $\{b, c\}$. The remaining possible moves are the four sets of size 1, where the Player 2 clearly wins after two more rounds.
 - ii. Player 1's third move is a one element set, $\{a\}$. Player 2 should choose $\{b\}$. The game is then reduced to the case two element game on $\{c, d\}$ where Player 2 has a winning strategy.

So in all cases, Player 2 has a winning strategy in the Gale game for $n = 4$. ■

²From Christenson & Tilford, *David Gale's Subset Takeaway Game*, *American Mathematical Monthly*, Oct. 1997

³David Gale worked out some of the properties of this game and conjectured that the second player wins the game for any set A . This remains an open problem.

Problem 3.

The *inverse*, R^{-1} , of a binary relation, R , from A to B , is the relation from B to A defined by:

$$b R^{-1} a \text{ iff } a R b.$$

In other words, you get the diagram for R^{-1} from R by “reversing the arrows” in the diagram describing R . Now many of the relational properties of R correspond to different properties of R^{-1} . For example, R is an *total* iff R^{-1} is a *surjection*.

Fill in the remaining entries in this table:

R is	iff R^{-1} is
total	a surjection
a function	
a surjection	
an injection	
a bijection	

Hint: Explain what’s going on in terms of “arrows” from A to B in the diagram for R .

Solution.

R is	iff R^{-1} is
total	a surjection
a function	an injection
a surjection	total
an injection	a function
a bijection	a bijection

Problem 4.

Define a *surjection relation*, surj , on sets by the rule

Definition. $A \text{ surj } B$ iff there is a surjective **function** from A to B .

Define the *injection relation*, inj , on sets by the rule

Definition. $A \text{ inj } B$ iff there is a total injective *relation* from A to B .

(a) Prove that if $A \text{ surj } B$ and $B \text{ surj } C$, then $A \text{ surj } C$.

Solution. By definition of surj , there are surjective functions, $F : A \rightarrow B$ and $G : B \rightarrow C$.

Let $H ::= G \circ F$ be the function equal to the composition of G and F , that is

$$H(a) ::= G(F(a)).$$

We show that H is surjective, which will complete the proof. So suppose $c \in C$. Then since G is a surjection, $c = G(b)$ for some $b \in B$. Likewise, $b = F(a)$ for some $a \in A$. Hence $c = G(F(a)) = H(a)$, proving that c is in the range of H , as required. ■

(b) Explain why $A \text{ surj } B$ iff $B \text{ inj } A$.

Like how is that a proof

Solution. Proof. (right to left): By definition of inj, there is a total injective relation, $R : B \rightarrow A$. But this implies that R^{-1} is a surjective function from A to B .

(left to right): By definition of surj, there is a surjective function, $F : A \rightarrow B$. But this implies that F^{-1} is a total injective relation from A to B . ■

(c) Conclude from (a) and (b) that if $A \text{ inj } B$ and $B \text{ inj } C$, then $A \text{ inj } C$.

Solution. From (b) and (a) we have that if $C \text{ inj } B$ and $B \text{ inj } A$, then $C \text{ inj } A$, so just switch the names A and C . ■

T.P.3.1 extension granted

$$A = \{a, b, c, d, e\}$$

$$B = \{a, b, c, d, e, f, g, h\}$$

$$A \cup B$$

↑
or

$$\{a, b, c, d, e, f, g, h\}$$



$$A \cap B$$

AND

$$\{a, b, c, d, e\}$$



$$A - B$$

empty set



$$B - A$$

f, g, h

T.P.3.2

$$A = \text{set}$$

$$P(A) = \text{power set} - \text{set of all subsets}$$

↑

②

$$P(\{1, 2\}) = \{1\}, \{2\}, \{1, 2\}, \emptyset \quad \checkmark$$

in both

$$P(\{0, \{0\}\}) = \{ \}$$

$$\{0, \{0\}\}, \{0\}, \{\{0\}\}, 0 \quad \checkmark$$

word

How many elements

$$\{1, 2, \dots, 8\}$$

(these are the problems I like)

~~8~~

Think for less elements

$$2 \mid 4 = 2 + 1 + 1$$

$$3 \mid \{1\} \{2\} \{3\}$$

$$\{1, 2\} \{2, 3\} \{1, 3\}$$

$$\{1, 2, 3\}$$

$$\emptyset$$

$$3 + 3 + 1 + 1 = 8$$

Order does not matter

③

4 {1,3} ... 4
~~{1,2}~~ {2,3} {3,4} {1,3} {1,4}

	1	2	3	4
1	{1}	{1,2}	{1,3}	{1,4}
2	{1,2}	{2}	{2,3}	{2,4}
3	{1,3}	{2,3}	{3}	{3,4}
4	{1,4}	{2,4}	{3,4}	{4}

~~$\frac{1}{2}n^2 - n$~~
 $\frac{1}{2}n^2 - \frac{1}{2}n$

{1,2,3} {1,2,4} {1,3,4} {2,3,4} 4
 {1,2,3,4} 1
 \emptyset 1

how would you do a table here
 # of elements expand

Oh duh - book says 2^n so $2^8 =$ 256

(I like these type of problems)

④ TP.3.3

Part 1 Divisibility Images

$V = \text{relation integers, } 7 \rightarrow 15$

codomain ~~15~~ \mathbb{Z} $2 \rightarrow 30$

$mVn \rightarrow m$ is divisor of n

List the elements of $V(\{10, 14\})$ the image of set

$\{10, 14\}$ under V

(What is image again.)

↳ the arrows / relation?
is it like a view?

So list the results -

$\frac{m}{7}$	$\frac{n}{2}$
7	2
8	3
9	4
\vdots	5
\vdots	\vdots
15	30
10	
14	

So all the divisors of these values
from $2 \rightarrow 30$

5

And "or" so if one is a divisor of one or the other
— or must be both?

~~2 5 10~~
~~2 14~~) (X)
2 (X)

10, 20, 30, 14, 28
? So I did divisible in wrong way

2. Inverse — so set of m that are in above image
So all the numbers which are divisible by the above

— so all the evens essentially

~~8 10 12 14~~ (X)

7 10 14 ? Items that are divisible above

Part 2 Total Relations

~~A~~ set is A relation is total iff

$R(A) = B$ ✓ X ? So notes wrong?

$R^+(B) = A$ X ✓

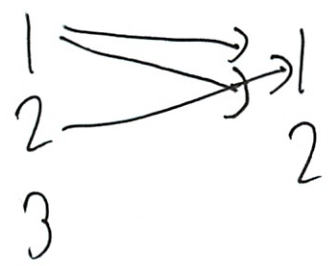
every el of A goes to B

(6)

Part 3 Surjective Relation

~~Defn~~ Relation is surjective iff

- every el of B is mapped to at least once



$R^{-1}(A) = B$ ✓ X

↑ how do inverse of reverse

Book $b R^{-1} a$ iff $a R b$

So change part 2

$R(B) = A$ ✓ X goes back

$R^{-1}(B) = A$ X

$R(A) = B$ X ✓ only true

↑ not a function

but what does it mean to be valid?

Reverse the direction of arrows

But what is $R(B)$

still don't get

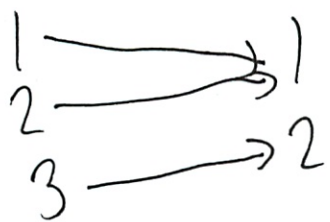
TP. 3.4 Inverse Relations

Inverse of R^{-1} of $R: A \rightarrow B$ is $B \rightarrow A$
as defined by $b R^{-1} a \Leftrightarrow a R b$
Like reversing arrow

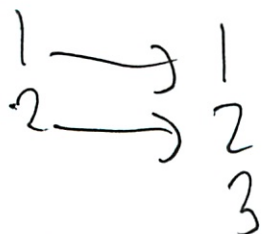
R is total iff R^{-1} is a surjection
 \uparrow exactly 1 arrow out of each
 \uparrow every ≥ 1 arrow in

Does it not depend on size?

a) R is a function iff R^{-1} is a



Again size is important!



would be none
function
total

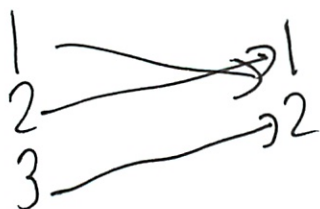
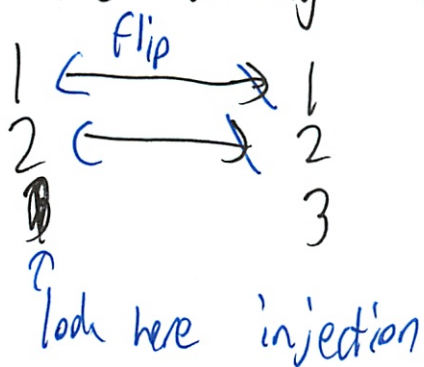
~~(X)~~
~~(X)~~
~~(X)~~ - never true

injection

↳ ever error mapped at least once
again size!

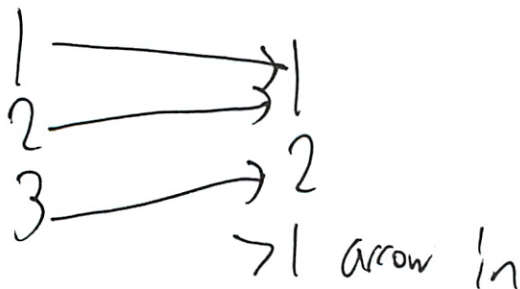
Or does image mean a certain something

Or are we looking at A?

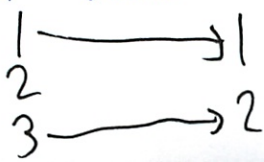


but then this would be injection as well?

b) R is a surjection iff R^{-1} is _____



but also

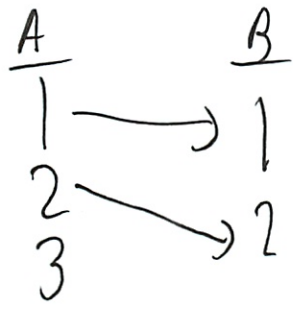


So none? (X)

~~total~~ (✓) I don't get it!

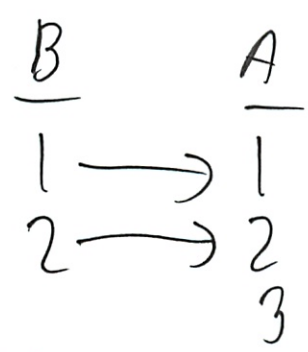
9

c) R is an injection iff R^{-1} is
↳ at most one in



but none again? (X)

Or would you say total since one arrow coming out of B, so



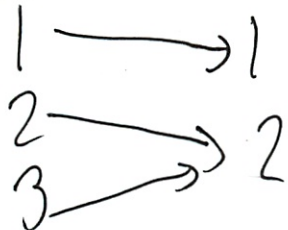
total (X)
function (V)

but why is it not total?

d) R is a bijection iff R^{-1} is
bijection (V)

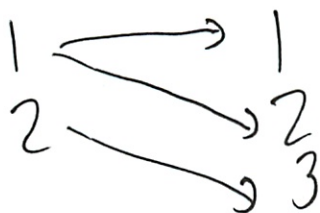
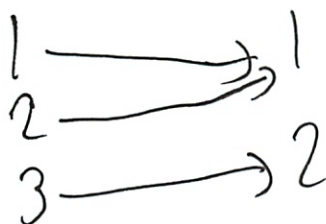
(10) Let me think more about this

a) function



injection makes sense now

b) surjection



So not total \leftarrow is total

but function

but how since at least one

Oh total can be ≥ 1 arrow out

\hookrightarrow not necessarily a function!

c makes sense now

(11)

TP 3.5 In-, Sur-, Bi-jections

$B = \text{Bijection}$

$S = \text{sur, but not bi}$

$I = \text{in but not bi}$

$N = \text{neither inj + sur}$

a) $x + 2$



I since at most 1 \otimes

N \otimes

S \otimes

B \odot Last try

Oh can be $\# < 1$

It's \mathbb{R}

So $0 \rightarrow 2$
 $-1 \rightarrow 1$

(12)

$2x$

-2	-4
-1	-2
0	0
1	2
2	4

~~B~~ ~~BLS~~ 1.5

1.75 \rightarrow
So works

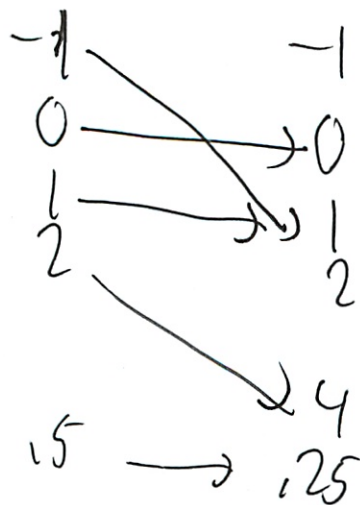
but only for rationals? \mathbb{Q}

~~I~~ ~~X~~ ~~can~~
~~B~~ ~~O~~

C So you can always $\cdot \frac{1}{2}$ to get back

~~B~~ $\times 2$

Well here neg don't count



but no - ~~Do not~~ S

Can you get 3

$2\sqrt{3} \rightarrow$ yeah

13

And stuff can be mapped to multiple times

not S

not I

So not B

N

since $(-1)^2 = 1$



d. x^3

Now $-$ is back

So back to B ?

e) $\sin x$

So any input to between $-1, 1$

So not ~~S~~

not I

So not B

N



f) $x \sin x$

Now can scale this to whatever

S

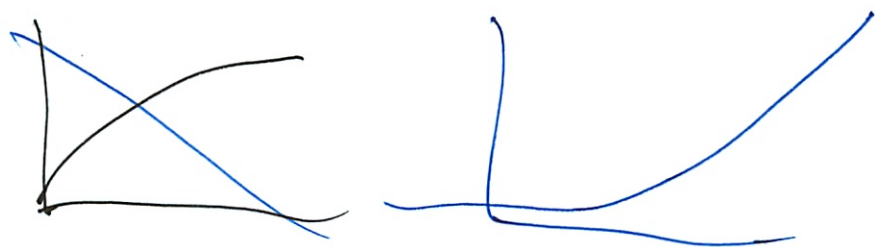


can have everything

not I can be more than 1? guess not if S

14

g) e^x



Can't be < 1 so not S

Can values be more than once? No \rightarrow I (1)


That was kinda fun

TP 3.6

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

Mathematics for Computer Science
MIT 6.042J/18.062J

Set Theory


 Albert R Meyer, February 16, 2011 lec 3W.1

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

Axioms

Equality
 $\forall x [x \in y \leftrightarrow x \in z] \rightarrow y = z$


Power set
 $\forall x \exists p \forall s. s \subseteq x \leftrightarrow s \in p$

 Albert R Meyer, February 16, 2011 lec 3W.2

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

Russell's Paradox


Let $W ::= \{s \in \text{Sets} \mid s \notin s\}$
 so $[s \in W \text{ IFF } s \notin s]$
 Now let s be W , and
 reach a contradiction:
 $[W \in W \text{ IFF } W \notin W]$

 Albert R Meyer, February 16, 2011 lec 3W.5

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

Disaster: Math is broken!


I am the Pope,
 Pigs fly,
 and verified programs
 crash...

 Albert R Meyer, February 16, 2011 lec 3W.6

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

...but paradox is buggy


Assumes that W is a set!
 $[s \in W \text{ IFF } s \notin s]$
 for all sets s
 ...can only substitute
 W for s if W is a set

 Albert R Meyer, February 16, 2011 lec 3W.7

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

...but paradox is buggy

Assumes that W is a set!
 We can avoid the paradox,
 if we deny that W is a set!
 ...which raises the key question:
 just which well-defined
 collections are sets?

 Albert R Meyer, February 16, 2011 lec 3W.8

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

Zermelo-Frankel Set Theory

No simple answer, but the axioms of Zermelo-Frankel along with the Choice axiom (ZFC) do a pretty good job.



Albert R Meyer,

February 16, 2011

lec 3W.10

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

Zermelo-Frankel Set Theory

According to ZF, the elements of a set have to be "simpler" than the set itself. In particular,
no set is a member of itself.



Albert R Meyer,

February 16, 2011

lec 3W.11

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

Zermelo-Frankel Set Theory

This implies that

- (1) the collection of all sets is not a set, and
- (2) W equals the collection of all sets ...which is why it's not a set



Albert R Meyer,

February 16, 2011

lec 3W.12

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

infinite sizes

Are infinite sets the "same size"?
NO, by Russell paradox variant:
Theorem: No $[\geq 1 \text{ in}]$ function from A to $\text{pow}(A)$, even for infinite A



Albert R Meyer,

February 16, 2011

lec 3W.13

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

no surjection from A to $\text{pow}(A)$

Pf by contradiction: suppose surj fcn $f:A \rightarrow \text{pow}(A)$. Let $W := \{a \in A \mid a \notin f(a)\}$, so
 $a \in W$ iff $a \notin f(a)$.
f a surj, so $W = f(a_0)$, some $a_0 \in A$.



Albert R Meyer,

February 16, 2011

lec 3W.14

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

no surjection from A to $\text{pow}(A)$

Pf by contradiction: suppose surj fcn $f:A \rightarrow \text{pow}(A)$. Let $W := \{a \in A \mid a \notin f(a)\}$, so
 $a \in f(a_0)$ iff $a \notin f(a)$.
Now let a be a_0 :
 $a_0 \in f(a_0)$ iff $a_0 \notin f(a_0)$. □



Albert R Meyer,

February 16, 2011

lec 3W.15

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

Team Problems

Problems 1 & 2



Albert R Meyer,

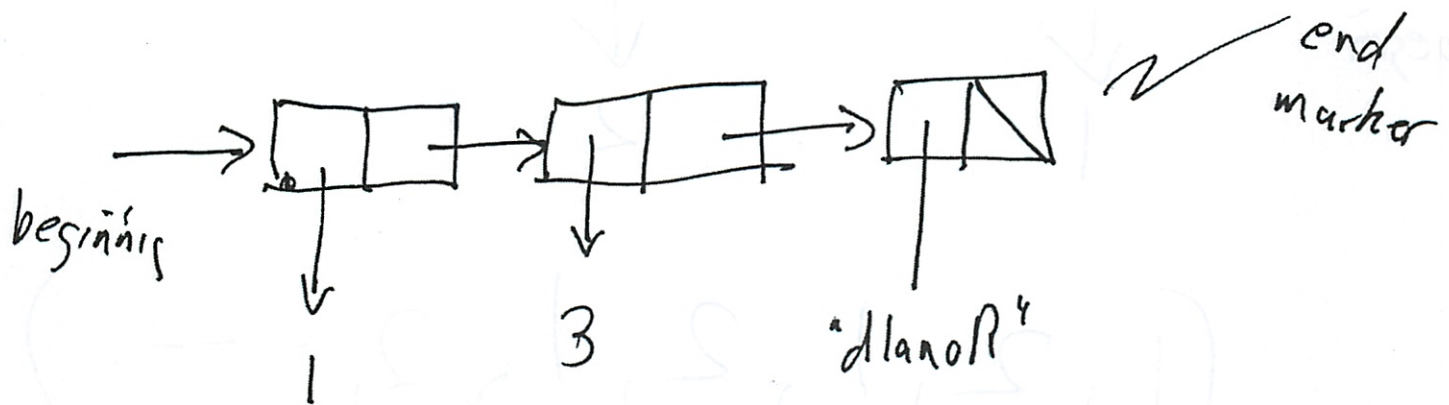
February 16, 2011

lec 3W.17

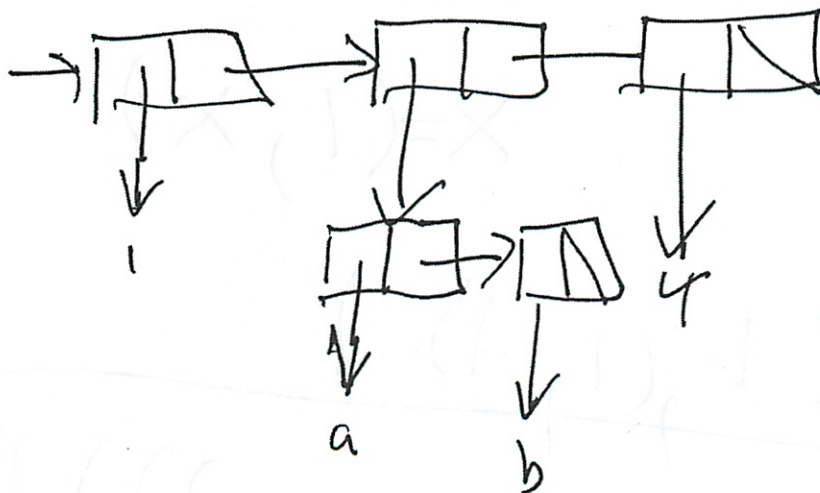
ARM
2/16/11

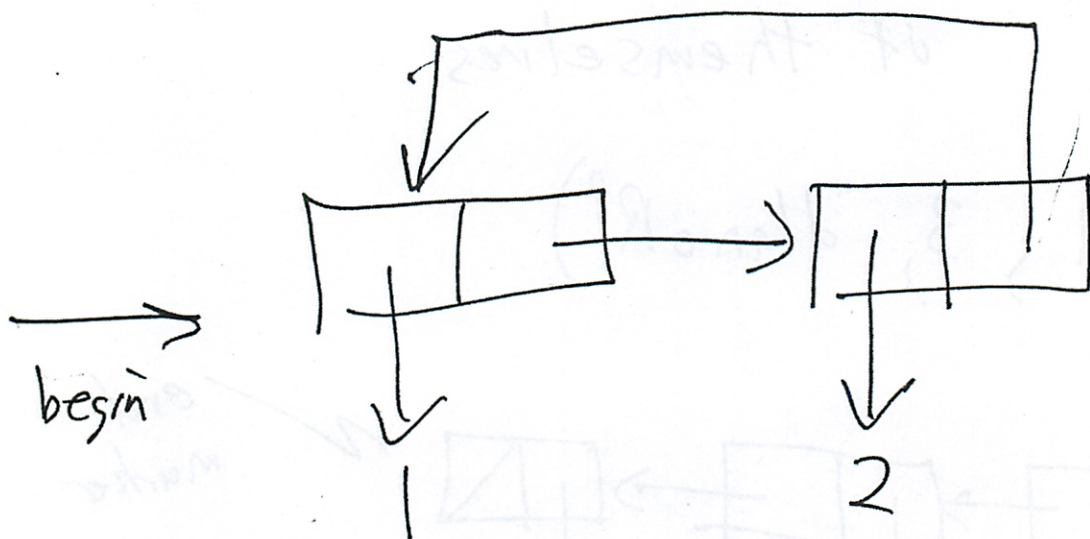
Lists that are members
of themselves

$(1, 3, \text{"dlanoR"})$

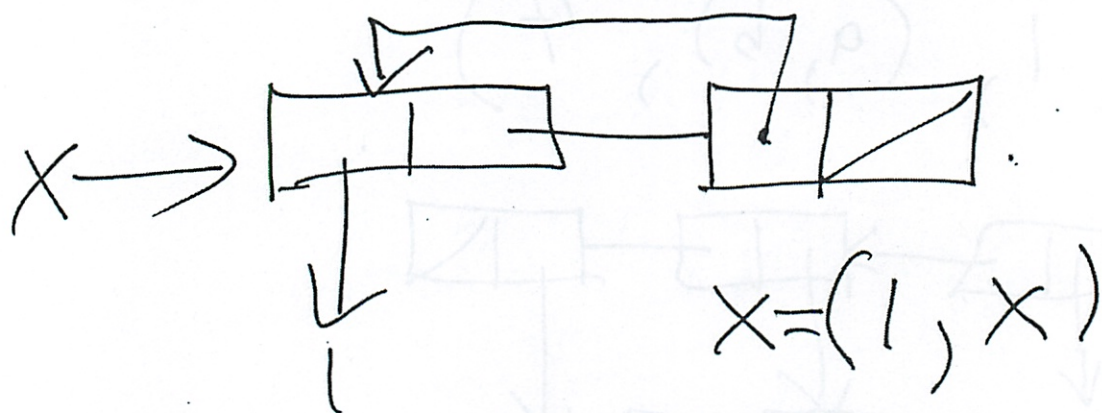


$(1, (a, b), 4)$





$(1, 2, 1, 2, 1, 2, \dots)$



$(1, (1, (1, \dots)))$

Mini Quiz 1

- ~~the~~ (last problem a τ 0 is not counter so not checked)

Can build everything out of sets
- but gets complicated

Russel's Paradox

- Showed much more confusing than they thought

Ideas connected well - Halting problem

Bigger infinities

Basis of complexity theory

Axioms

ZFC enough to build all math

But it can't prove itself

Will not need to know ZFC

Takes too long to build stuff up

Equality

- definition

$$\forall x [x \in y \leftrightarrow x \in z] \rightarrow y = z$$

if they have same elements then it is equal

②

Power Set

$$\forall x \exists p \forall s, s \subseteq x \Leftrightarrow s \in p$$

↑
power set all subsets

\in = member \subset = is a proper subset
 \subseteq = subset of

Only primitive you start w/ is membership

One guy tried to build up all of math from sets

But you could prove $1=0$

So toss 10 years of work out

Russell's Paradox

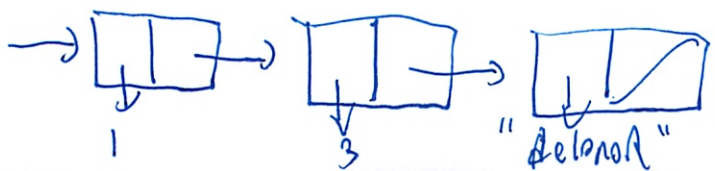
Can a set be a member of itself

Is bread + butter in CS

Python lists

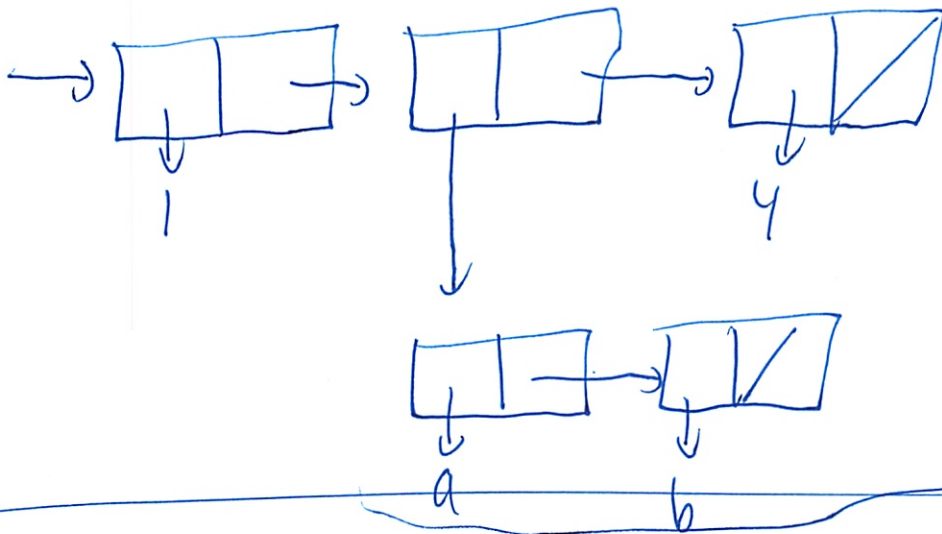
(1, 3, "delanoR")

Objects represented as objects in memory cells

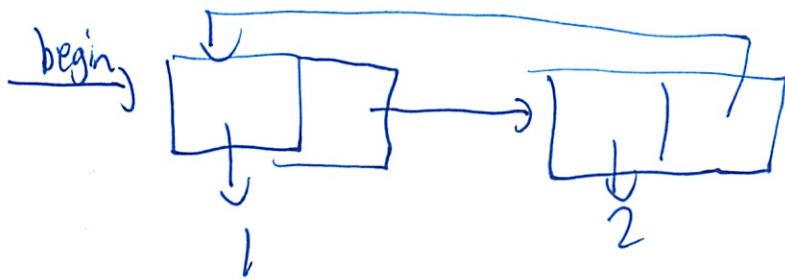


③ Recursive natural 'in C'
List of lists

$(1, (a, b), 4)$

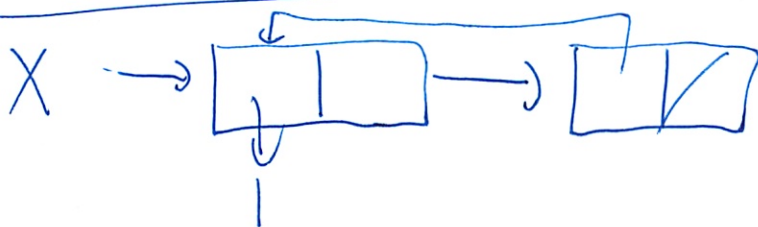


But what if build circular structure



$(1, 2, 1, 2, 1, 2, 1, \dots)$

"perfectly sensible"



infinity deep new

$(1, (1, (1, (1, \dots)))$

④

↑

List that is a member of itself

Not a problem in CS

One of the major problem in CS is that mathematicians disagree

How to reason about these w/o the logical contradictions
- programming logic theory

$$W = \{s \in \text{Sets} \mid s \notin s\}$$

$$\text{So } [s \in W \text{ iff } s \notin s]$$

Now let s be W and reach a conclusion

$$[W \in W \text{ iff } W \notin W]$$

but is the paradox buggy???

That everything is a set?

Is W a set?

- no

- cheat and call it a class

5

Classes

- not a ~~member~~ member of everything

So ~~we~~ what's rule about what is a set or not?

↳ ZFC

Foundation

A set should be built up from other sets

don't want sets members of themselves - so forbid that

So ω equals the collection of all sets - so that's why it is not a set

Infinite Sets

Are all ∞ sets the same size?

- No by Russel Paradox Variation

Theorem No surjective function from A to $P(A)$
 \mathbb{Z} into \mathbb{B}

If you do that must be unnameable elements - not an image - not a surjection

$|A|$ must be $< |P(A)|$
 $n < 2^n$

⑥

When you use definition of surjection
Works for ∞ sets

$$f: A \rightarrow \mathcal{P}(A)$$

$$W := \{a \in A \mid a \notin f(a)\}$$

$$a \in W \text{ iff } a \notin f(a)$$

Suppose

f a surj, so $w = f(a_0)$, some $a_0 \in A$

$$\text{So } a_0 \in f(a_0) \text{ iff } a_0 \notin f(a_0)$$

In-Class Problems Week 3, Wed.

Problem 1.

The method used to prove Cantor's Theorem that the power set is "bigger" than the set, leads to many important results in logic and computer science. In this problem we'll apply that idea to describe a set of binary strings that can't be described by ordinary logical formulas. To be provocative, we could say that we will describe an undecidable set of strings!

The following logical formula illustrates how a formula can describe a set of strings. The formula

$$\text{NOT}[\exists y. \exists z. s = y1z], \quad (\text{no-1s}(s))$$

where the variables range over the set, $\{0, 1\}^*$, of finite binary strings, says that the binary string, s , does not contain a 1.

We'll call such a predicate formula, $G(s)$, about strings a *string formula*, and we'll use the notation $\text{strings}(G)$ for the set of binary strings with the property described by G . That is,

$$\text{strings}(G) ::= \{s \in \{0, 1\}^* \mid G(s)\}.$$

A set of binary strings is *describable* if it equals $\text{strings}(G)$ for some string formula, G . So the set, 0^* , of finite strings of 0's is describable because it equals $\text{strings}(\text{no-1s})$.¹

The idea of representing data in binary is a no-brainer for a computer scientist, so it won't be a stretch to agree that any string formula can be represented by a binary string. We'll use the notation G_x for the string formula with binary representation $x \in \{0, 1\}^*$. The details of the representation don't matter, except that there ought to be a display procedure that can actually display G_x given x .

Standard binary representations of formulas are often based on character-by-character translation into binary, which means that only a sparse set of binary strings actually represent string formulas. It will be technically convenient to have *every* binary string represent some string formula. This is easy to do: tweak the display procedure so it displays some default formula, say *no-1s*, when it gets a binary string that isn't a standard representation of a string formula. With this tweak, *every* binary string, x , will now represent a string formula, G_x .

Now we have just the kind of situation where a Cantor-style diagonal argument can be applied, namely, we'll ask whether a string describes a property of *itself*! That may sound like a mind-bender, but all we're asking is whether $x \in \text{strings}(G_x)$.

For example, using character-by-character translations of formulas into binary, neither the string 0000 nor the string 10 would be the binary representation of a formula, so the display procedure applied to either of them would display *no-1s*. That is, $G_{0000} = G_{10} = \text{no-1s}$ and so $\text{strings}(G_{0000}) = \text{strings}(G_{10}) = 0^*$. This means that

$$0000 \in \text{strings}(G_{0000}) \quad \text{and} \quad 10 \notin \text{strings}(G_{10}).$$

Now we are in a position to give a precise mathematical description of an "undecidable" set of binary strings, namely, let

Theorem. *Define*

$$U ::= \{x \in \{0, 1\}^* \mid x \notin \text{strings}(G_x)\}. \quad (1)$$

The set U is not describable.

Use reasoning similar to Cantor's theorem (repeated below) to prove this Theorem.

Problem 2.

Let $R : A \rightarrow A$ be a binary relation on a set, A . If $a_1 R a_0$, we'll say that a_1 is " R -smaller" than a_0 . R is called *well founded* when there is no infinite " R -decreasing" sequence:

$$\cdots R a_n R \cdots R a_1 R a_0, \quad (2)$$

of elements $a_i \in A$.

For example, if $A = \mathbb{N}$ and R is the $<$ -relation, then R is well founded because if you keep counting down with nonnegative integers, you eventually get stuck at zero:

$$0 < \cdots < n - 1 < n.$$

But you can keep counting up forever, so the $>$ -relation is not well founded:

$$\cdots > n > \cdots > 1 > 0.$$

Also, the \leq -relation on \mathbb{N} is not well founded because a constant sequence of, say, 2's, gets \leq -smaller forever:

$$\cdots \leq 2 \leq \cdots \leq 2 \leq 2.$$

(a) If B is a subset of A , an element $b \in B$ is defined to be *R -minimal in B* iff there is no R -smaller element in B . Prove that $R : A \rightarrow A$ is well founded iff every nonempty subset of A has an R -minimal element.

A logic *formula of set theory* has only predicates of the form " $x \in y$ " for variables x, y ranging over sets, along with quantifiers and propositional operations. For example,

$$\text{isempty}(x) ::= \forall w. \text{NOT}(w \in x)$$

is a formula of set theory that means that " x is empty."

(b) Write a formula, $\text{member-minimal}(u, v)$, of set theory that means that u is \in -minimal in v .

(c) The Foundation axiom of set theory says that \in is a well founded relation on sets. Express the Foundation axiom as a formula of set theory. You may use "member-minimal" and "isempty" in your formula as abbreviations for the formulas defined above.

(d) Explain why the Foundation axiom implies that no set is a member of itself.

Cantor's Theorem

There is no bijection between any set A and its powerset $\mathcal{P}(A)$.

Proof. We show that if g is a total function from A to $\mathcal{P}(A)$, then g does not have the $[\geq 1]$ in, surjection property, and so is certainly not a bijection.

Define

$$A_g ::= \{a \in A \mid a \notin g(a)\}.$$

Since g is total, A_g is a well-defined subset of A , which means it is a member of $\mathcal{P}(A)$. We claim A_g is not in the range of g , and so g is not a surjection.

To prove that $A_g \notin \text{range}(g)$, assume to the contrary that it was in $\text{range}(g)$. That is,

$$A_g = g(a_0)$$

for some $a_0 \in A$. Then by definition of A_g ,

$$a \in g(a_0) \quad \text{iff} \quad a \in A_g \quad \text{iff} \quad a \notin g(a)$$

for all $a \in A$. Now letting $a = a_0$ yields the contradiction

$$a_0 \in g(a_0) \quad \text{iff} \quad a_0 \notin g(a_0).$$



No one really understands problem

5 min left

Solutions to In-Class Problems Week 3, Wed.

Problem 1.

The method used to prove Cantor's Theorem that the power set is "bigger" than the set, leads to many important results in logic and computer science. In this problem we'll apply that idea to describe a set of binary strings that can't be described by ordinary logical formulas. To be provocative, we could say that we will describe an undescribable set of strings!

The following logical formula illustrates how a formula can describe a set of strings. The formula

$$\text{NOT}[\exists y. \exists z. s = y1z], \quad (\text{no-1s}(s))$$

where the variables range over the set, $\{0, 1\}^*$, of finite binary strings, says that the binary string, s , does not contain a 1.

We'll call such a predicate formula, $G(s)$, about strings a *string formula*, and we'll use the notation $\text{strings}(G)$ for the set of binary strings with the property described by G . That is,

$$\text{strings}(G) ::= \{s \in \{0, 1\}^* \mid G(s)\}.$$

A set of binary strings is *describable* if it equals $\text{strings}(G)$ for some string formula, G . So the set, 0^* , of finite strings of 0's is describable because it equals $\text{strings}(\text{no-1s})$.¹

The idea of representing data in binary is a no-brainer for a computer scientist, so it won't be a stretch to agree that any string formula can be represented by a binary string. We'll use the notation G_x for the string formula with binary representation $x \in \{0, 1\}^*$. The details of the representation don't matter, except that there ought to be a display procedure that can actually display G_x given x .

Standard binary representations of formulas are often based on character-by-character translation into binary, which means that only a sparse set of binary strings actually represent string formulas. It will be technically convenient to have *every* binary string represent some string formula. This is easy to do: tweak the display procedure so it displays some default formula, say no-1s, when it gets a binary string that isn't a standard representation of a string formula. With this tweak, *every* binary string, x , will now represent a string formula, G_x .

Now we have just the kind of situation where a Cantor-style diagonal argument can be applied, namely, we'll ask whether a string describes a property of *itself*! That may sound like a mind-bender, but all we're asking is whether $x \in \text{strings}(G_x)$.

For example, using character-by-character translations of formulas into binary, neither the string 0000 nor the string 10 would be the binary representation of a formula, so the display procedure applied to either of them would display no-1s. That is, $G_{0000} = G_{10} = \text{no-1s}$ and so $\text{strings}(G_{0000}) = \text{strings}(G_{10}) = 0^*$. This means that

$$0000 \in \text{strings}(G_{0000}) \quad \text{and} \quad 10 \notin \text{strings}(G_{10}).$$

Now we are in a position to give a precise mathematical description of an "undescribable" set of binary strings, namely, let

Theorem. Define

$$U ::= \{x \in \{0, 1\}^* \mid x \notin \text{strings}(G_x)\}. \quad (1)$$

The set U is not describable.

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer.

¹no-1s and similar formulas were examined in Problem ??, but it is not necessary to have done that problem to do this one.

Use reasoning similar to Cantor's theorem (repeated below) to prove this Theorem.

Solution. By definition (1),

$$x \in U \text{ iff } x \notin \text{strings}(G_x). \quad (2)$$

for $x \in \{0, 1\}^*$.

Also, $U = \text{strings}(G_{x_U})$ by assumption. This means:

$$x \in U \text{ iff } x \in \text{strings}(G_{x_U}). \quad (3)$$

Combining (3) and (2), we have

$$x \notin \text{strings}(G_x) \longleftrightarrow x \in \text{strings}(G_{x_U}), \quad (4)$$

for all $x \in \{0, 1\}^*$. Now plugging in x_U for x in (4) gives an immediate contradiction.

So there cannot be any formula that describes U . ■

Problem 2.

Let $R : A \rightarrow A$ be a binary relation on a set, A . If $a_1 R a_0$, we'll say that a_1 is " R -smaller" than a_0 . R is called *well founded* when there is no infinite " R -decreasing" sequence:

$$\dots R a_n R \dots R a_1 R a_0, \quad (5)$$

of elements $a_i \in A$.

For example, if $A = \mathbb{N}$ and R is the $<$ -relation, then R is well founded because if you keep counting down with nonnegative integers, you eventually get stuck at zero:

$$0 < \dots < n - 1 < n.$$

But you can keep counting up forever, so the $>$ -relation is not well founded:

$$\dots > n > \dots > 1 > 0.$$

Also, the \leq -relation on \mathbb{N} is not well founded because a constant sequence of, say, 2's, gets \leq -smaller forever:

$$\dots \leq 2 \leq \dots \leq 2 \leq 2.$$

(a) If B is a subset of A , an element $b \in B$ is defined to be *R -minimal in B* iff there is no R -smaller element in B . Prove that $R : A \rightarrow A$ is well founded iff every nonempty subset of A has an R -minimal element.

Solution. If there was an infinite R -decreasing sequence (5), then $\{a_0, a_1, \dots\}$ would itself be a nonempty subset of A with no minimal element. This proves the right-to-left direction of the "iff" (by contrapositive).

We'll also prove the left-to-right direction by contrapositive. So suppose B is a nonempty subset of A with no R -minimal element. We will show how to find an infinite R -decreasing sequence of elements of B :

Since B is nonempty, there is an element $b_0 \in B$. Since b_0 cannot be minimal in B , there must be an element $b_1 \in B$ that is R -smaller than b_0 . Again, since b_1 cannot be minimal in B , there must be an R -smaller $b_2 \in B$. Continuing in this way, we obtain an infinite R -decreasing sequence

$$\dots R b_n R \dots R b_1 R b_0.$$

■

A logic *formula of set theory* has only predicates of the form “ $x \in y$ ” for variables x, y ranging over sets, along with quantifiers and propositional operations. For example,

$$\text{isempty}(x) ::= \forall w. \text{NOT}(w \in x)$$

is a formula of set theory that means that “ x is empty.”

(b) Write a formula, $\text{member-minimal}(u, v)$, of set theory that means that u is \in -minimal in v .

Solution.

$$\text{member-minimal}(u, v) ::= u \in v \text{ AND } \forall x \in v. x \notin u.$$

(c) The Foundation axiom of set theory says that \in is a well founded relation on sets. Express the Foundation axiom as a formula of set theory. You may use “member-minimal” and “isempty” in your formula as abbreviations for the formulas defined above.

Solution.

$$\forall x. \text{NOT}(\text{isempty}(x)) \text{ IMPLIES } \exists m. \text{member-minimal}(m, x).$$

(d) Explain why the Foundation axiom implies that no set is a member of itself.

Solution. If $x \in x$, then

$$\dots \in x \in \dots \in x \in x$$

is a \in -decreasing sequence, violating well foundedness of the \in -relation. Alternatively, $\{x\}$ would be a nonempty set with no \in -minimal element.

Cantor's Theorem**There is no bijection between any set A and its powerset $\mathcal{P}(A)$.**

Proof. We show that if g is a total function from A to $\mathcal{P}(A)$, then g does not have the $[\geq 1 \text{ in}]$, surjection property, and so is certainly not a bijection.

Define

$$A_g ::= \{a \in A \mid a \notin g(a)\}.$$

Since g is total, A_g is a well-defined subset of A , which means it is a member of $\mathcal{P}(A)$. We claim A_g is not in the range of g , and so g is not a surjection.

To prove that $A_g \notin \text{range}(g)$, assume to the contrary that it was in $\text{range}(g)$. That is,

$$A_g = g(a_0)$$

for some $a_0 \in A$. Then by definition of A_g ,

$$a \in g(a_0) \quad \text{iff} \quad a \in A_g \quad \text{iff} \quad a \notin g(a)$$

for all $a \in A$. Now letting $a = a_0$ yields the contradiction

$$a_0 \in g(a_0) \quad \text{iff} \quad a_0 \notin g(a_0).$$



Problem Set 2

Due: February 18

Reading: Chapter 1.1, covering *Predicate Formulas*, Chapter 1.2, covering *Sets & Relations*, Chapter 1.3–1.4, covering *Russells' Paradox & The ZFC Story*. Assigned readings **do not include the Problem sections**.

Note Chapter 1.5.2–1.5.3, covering *Cardinality* is due for class on Friday, Feb. 18, but is not covered on the pset.

Reminder: Email comments on the reading are due *before* the class in which the reading is covered. Latest times for comments on different sections are indicated in the online tutor problem set TP.3. Reading Comments count for 3% of the final grade.

Problem 1.

Translate the following sentence into a predicate formula:

There is a student who has emailed exactly two other people in the class, besides possibly herself.

The domain of discourse should be the set of students in the class; in addition, the only predicates that you may use are

- equality, and
- $E(x, y)$, meaning that “ x has sent e-mail to y .”

Problem 2.

Express each of the following predicates and propositions in formal logic notation. The domain of discourse is the nonnegative integers, \mathbb{N} . Moreover, in addition to the propositional operators, variables and quantifiers, you may define predicates using addition, multiplication, and equality symbols, and nonnegative integer constants $0, 1, \dots$, but no *exponentiation* (like x^y). For example, the predicate “ n is an even number” could be defined by either of the following formulas:

$$\exists m. (2m = n), \quad \exists m. (m + m = n).$$

- (a) m is a divisor of n .
- (b) n is a prime number.
- (c) n is a power of a prime.

Problem 3.

Let A , B , and C be sets. Prove that:

$$A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C). \quad (1)$$

Hint: $P \text{ OR } Q \text{ OR } R$ is equivalent to

$$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR } (R \text{ AND } \overline{P}) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

Problem 4.

There is a simple and useful way to extend composition of functions to composition of relations. Namely, let $R : B \rightarrow C$ and $S : A \rightarrow B$ be relations. Then the composition of R with S is the binary relation $(R \circ S) : A \rightarrow C$ defined by the rule

$$a (R \circ S) c ::= \exists b \in B. (b R c) \text{ AND } (a S b).$$

This agrees with the Definition ?? of composition in the special case when R and S are functions.

We can represent a relation, S , between two sets $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ as an $n \times m$ matrix, M_S , of zeroes and ones, with the elements of M_S defined by the rule

$$M_S(i, j) = 1 \quad \text{IFF} \quad a_i S b_j.$$

If we represent relations as matrices in this fashion, then we can compute the composition of two relations R and S by a “boolean” matrix multiplication, \otimes , of their matrices. Boolean matrix multiplication is the same as matrix multiplication except that addition is replaced by OR and multiplication is replaced by AND. Namely, suppose $R : B \rightarrow C$ is a binary relation with $C = \{c_1, \dots, c_p\}$. So M_R is an $m \times p$ matrix. Then $M_S \otimes M_R$ is an $n \times p$ matrix defined by the rule:

$$[M_S \otimes M_R](i, j) ::= \text{OR}_{k=1}^m [M_S(i, k) \text{ AND } M_R(k, j)]. \quad (2)$$

Prove that the matrix representation, $M_{R \circ S}$, of $R \circ S$ equals $M_S \otimes M_R$ (note the reversal of R and S).

Problem 5. To appear.

Problem Set 2

Due: February 18

Reading: Chapter 3.6, covering *Predicate Formulas*, Chapter 4, covering *Sets & Relations*, Chapter 5, covering *Infinite Sets*.

Note: Wednesday lecture will cover Chapter 5.4 & 5.5, on Russell's Paradox & The ZFC Story. This pset does not cover Chapter 5.1–5.3, on Cardinality & the Halting Problem, but these sections are due for Friday lecture, Feb. 18.

Reminder: Email comments on the reading are due *before* the class in which the reading is covered. Latest times for comments on different sections are indicated in the online tutor problem set TP.3. Reading Comments count for 3% of the final grade.

Problem 1.

Translate the following sentence into a predicate formula:

There is a student who has emailed exactly two other people in the class, besides possibly herself.

The domain of discourse should be the set of students in the class; in addition, the only predicates that you may use are

- equality, and
- $E(x, y)$, meaning that “ x has sent e-mail to y .”

Problem 2.

Express each of the following predicates and propositions in formal logic notation. The domain of discourse is the nonnegative integers, \mathbb{N} . Moreover, in addition to the propositional operators, variables and quantifiers, you may define predicates using addition, multiplication, and equality symbols, and nonnegative integer constants $0, 1, \dots$, but no *exponentiation* (like x^y). For example, the predicate “ n is an even number” could be defined by either of the following formulas:

$$\exists m. (2m = n), \quad \exists m. (m + m = n).$$

- (a) m is a divisor of n .
- (b) n is a prime number.
- (c) n is a power of a prime.

Problem 3.

Let A , B , and C be sets. Prove that:

$$A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C). \quad (1)$$

Hint: $P \text{ OR } Q \text{ OR } R$ is equivalent to

$$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR } (R \text{ AND } \overline{P}) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

Problem 4.

There is a simple and useful way to extend composition of functions to composition of relations. Namely, let $R : B \rightarrow C$ and $S : A \rightarrow B$ be relations. Then the composition of R with S is the binary relation $(R \circ S) : A \rightarrow C$ defined by the rule

$$a (R \circ S) c ::= \exists b \in B. (b R c) \text{ AND } (a S b).$$

This agrees with the Definition 4.3.1 of composition in the special case when R and S are functions.

We can represent a relation, S , between two sets $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ as an $n \times m$ matrix, M_S , of zeroes and ones, with the elements of M_S defined by the rule

$$M_S(i, j) = 1 \quad \text{IFF} \quad a_i S b_j.$$

If we represent relations as matrices in this fashion, then we can compute the composition of two relations R and S by a “boolean” matrix multiplication, \otimes , of their matrices. Boolean matrix multiplication is the same as matrix multiplication except that addition is replaced by OR and multiplication is replaced by AND. Namely, suppose $R : B \rightarrow C$ is a binary relation with $C = \{c_1, \dots, c_p\}$. So M_R is an $m \times p$ matrix. Then $M_S \otimes M_R$ is an $n \times p$ matrix defined by the rule:

$$[M_S \otimes M_R](i, j) ::= \text{OR}_{k=1}^m [M_S(i, k) \text{ AND } M_R(k, j)]. \quad (2)$$

Prove that the matrix representation, $M_{R \circ S}$, of $R \circ S$ equals $M_S \otimes M_R$ (note the reversal of R and S).

Problem 5.

The Axiom of Choice says that if s is a set whose members are nonempty sets that are *pairwise disjoint*—that is no two sets in s have an element in common—then there is a set, c , consisting of exactly one element from each set in s .

In formal logic, we could describe s with the formula,

$$\text{pairwise-disjoint}(s) ::= \forall x \in s. x \neq \emptyset \text{ AND } \forall x, y \in s. x \neq y \text{ IMPLIES } x \cap y = \emptyset.$$

Similarly we could describe c with the formula

$$\text{choice-set}(c, s) ::= \forall x \in s. \exists! z. z \in c \cap x.$$

Here “ $\exists! z$.” is fairly standard notation for “there exists a *unique* z .”

Now we can give the formal definition:

Definition (Axiom of Choice).

$$\forall s. \text{pairwise-disjoint}(s) \text{ IMPLIES } \exists c. \text{choice-set}(c, s).$$

The only issue here is that Set Theory is technically supposed to be expressed in terms of *pure* formulas in the language of sets, which means formula that uses only the membership relation, \in , propositional connectives, the two quantifies \forall and \exists , and variables ranging over all sets. Verify that the Axiom of Choice can be expressed as a pure formula, by explaining how to replace all impure subformulas above with equivalent pure formulas.

For example, the formula $x = y$ could be replaced with the pure formula $\forall z. z \in x \text{ IFF } z \in y$.

Doing P-set 2

2/15

- Problem 5 has been added
- now need to re-print

Predicate

watch periods

possibly herself

Seems too simple

Don't need to say domain

Plus not others

Need to include $z \neq s$ otherwise we ban (not allow!)
 $E(s, s)$

2. formal logic notation

\mathbb{N}

$$\exists m. (2m = n) \quad \exists m. (m + m = n)$$

but what is n ?

Oh n is even #

and m must be $\in \mathbb{N}$

a) divisor

WP: also called Factor

divides n w/o remainder

$$m \mid n$$

$$\begin{array}{l} \text{dividend} \rightarrow a \\ \text{divisor} \rightarrow b \end{array} \quad \frac{a}{b} = c$$

$$\text{So } \frac{n}{m} = 0$$
$$\exists 0.$$

b) N is a prime

- there is no divisor

WP: has 2 divisors 1 and itself

③

(WP is helpful w/ these definitions)

So no divisor

$$\forall m \in \mathbb{N} \text{ except } 1, n \quad \frac{n}{m} = p$$

$\exists p \in \mathbb{N}$

W

hope that works

C) n is a power of a prime

WP: Prime Power:

-divisible by just one prime $\#$

(I would have not figured that out)

$\exists m$ such that m is prime and $\frac{n}{m} = p$ and $\frac{n}{p} = q$

And only one of them

p part a

q part b

$$\exists q \in \mathbb{N} \exists p \in \mathbb{N} (\forall m \in \mathbb{N} \text{ And } m \neq 1 \text{ AND } m \neq n \text{ Not } (\frac{n}{m} = p))$$

AND $\frac{n}{p} = q$

(4)

$\exists q \in \mathbb{N} \exists p \in \mathbb{N} (\forall m \in \mathbb{N} \text{ AND } m \neq 1 \text{ AND } m \neq n$
Not $(\frac{n}{m} = p))$ And $\frac{n}{p} = q$ AND $\forall r \in \mathbb{N} r \neq p$

$$\frac{n}{r} \neq q$$

m = possible divisors to prove prime

p there is one that is prime inside

q there is one int (so prime) outside

r things to try not p that no value

mess - but think works

Could have I used iff?

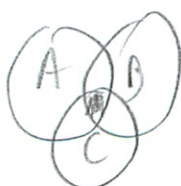
5

3. ? Prove w/ truth table

Or like W3Mon # 1a

Or graphical

(A) (B) (C)



? Power point

- They prob want graphical proofs

How to build ?

- Or forget

6

But ~~an~~ how would you do this otherwise

Hint helps - but how to relate to sets?

Functions?

∩ distributive laws

Or look at ZFC

- in chap 4 so, not so jective

4.1.3 complement of a set

did this in G.041 too

How much is enough to write?

must talk about the items inside

⑦ (lots of topics one after the other, fast paced)

4. extend composite of functions

$$R: B \rightarrow C$$

$$S: A \rightarrow B$$

$$(R \circ S): A \rightarrow B \rightarrow C$$

Oh sub functions 4.3.1

$$i \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & & \end{bmatrix} \quad \text{for arrows}$$

Boolean Matrix Multiplication

- matrix mult

- $+$ \rightarrow OR

\times \rightarrow AND

$$M_S \otimes M_R$$

I don't see what they are doing in notation
but I certainly agree w/ what they are doing
I could do example

⑧

What is $OR_{k=1}^m$

Is it $\sum_{k=1}^m$

I think I can ignore/assume

Don't prove by example

If = to 1 what require

This \rightarrow This not good enough
When it is true

Must apply for n arrows

(I just don't get this class!)

⑨

5. Newly added

Axiom of Choice

Section 6.1.2 ZFC

of my printout of book (older version)

Given a set S whose members are nonempty

Sets no two of which have any element

in common, then there is a set C consisting

of 1 el from each el in S

every thing must be unique

among all sets U

So can pull any random item from each

And have a set

"Pairwise disjoint" $\hat{=}$ $\forall x \in S. x \neq \emptyset$

AND $\forall x, y \in S. x \neq y \rightarrow x \cap y = \emptyset$

Choose set (c_x) $\hat{=}$ $\forall x \in S \exists ! z. z \in C \cap x$
 \uparrow no el in common
 \uparrow cute

Oh cool unique shorthand

\uparrow So c_x is in set

Check

(18)

Def

$\forall s$ pairwise disjoint $\rightarrow \exists c$ choice set (c, s)

= Pure formulas

- write as pure formula

example

$X = Y \rightarrow$ replace $\forall z, z \in X \Leftrightarrow z \in Y$

\uparrow silly

do tomorrow

Who cares if pure?

What is pure

- ~~not~~ membership

- \in

- connectives propositional (And, Or, ...)

- \forall, \exists

- variables over all sets

So what is not pure?

$\neq \emptyset$

\hookrightarrow has at least one element

$\exists x. x \in S$

variables

2/16

Student's Solutions to Problem Set 2

Your name:

Due date: February 18

Submission date:

Circle your TA/LA: Ali Nick Oscar Oshani

Collaboration statement: Circle one of the two choices and provide all pertinent info.

1. I worked alone and only with course materials.
2. I collaborated on this assignment with:

got help from:¹

and referred to:²

DO NOT WRITE BELOW THIS LINE

Problem	Score
1	
2	
3	
4	
5	
Total	

Student's Solutions to Problem Set 2

Your name:	Michael Plasmeier			
Due date:	February 18			
Submission date:	2/18			
Circle your TA/LA:	Ali	Nick	Oscar	<u>Oshani</u>

Table 12

Collaboration statement: Circle one of the two choices and provide all pertinent info.

1. I worked alone and only with course materials.
2. I collaborated on this assignment with:

got help from:¹

Ali's OH

and referred to:²

Wikipedia: divisor

prime

Prime power

Matrix

matrix multiplication

DO NOT WRITE BELOW THIS LINE

Problem	Score
1	
2	
3	
4	
Total	33

~~100~~ 150

: Michael Plasmeier

P-Set 2

2/15

Oshan:

Table 12

#1, S is set of students

$$\exists s \in S, \exists x \in S, \exists y \in S,$$

$$E(s, x) \text{ AND } E(s, y) \text{ (AND } s \neq x \text{ AND } s \neq y \text{ AND } x \neq y)$$

$$\left(\forall z \in S, z \neq s, z \neq x, z \neq y, \text{ NOT } (E(s, z)) \right)$$

↑ no one else

↑
not
the same
person

- O

Oshan

Table 12

$$\#2 a) \exists p \in \mathbb{N}, \frac{n}{m} = p \quad \checkmark$$

$$b) \forall m \in \mathbb{N} \text{ AND } m \neq 1 \text{ AND } m \neq n, \exists p \in \mathbb{N},$$

$$\text{NOT } \left(\frac{n}{m} = p \right) \quad -1$$

 $\exists! m$

c) $\exists m$ (and only 1 m) such that m is prime and a divisor

$$\exists q \in \mathbb{N}, \exists p \in \mathbb{N} \left(\forall m \in \mathbb{N} \text{ AND } m \neq 1 \text{ AND } m \neq n \right.$$

$$\text{NOT } \left(\frac{n}{m} = p \right) \text{ AND } \frac{n}{p} = q \text{ AND } \left(\forall r \in \mathbb{N}, \text{ AND } r \neq p, \right.$$

$$\text{NOT } \left(\frac{n}{r} = q \right)$$

-2

m = possible divisors to prove prime.

p = that there is only one divisor so prime inside

q = that there is only one divisor so prime outside

r = things to try, not p , to show only divisible by 1 prime number

Michael Plasreier

2/15

Oshani

Table 12

#3 Graphical proof

10



$A \cup B \cup C$



$A - B$



$B - C$



$C - A$



$A \cap B \cap C$

#3 alt method.

4.1.3 Complement of a set

$$\bar{A} ::= D - A \text{ for domain } D$$

So $\hat{=}$ all of the elements in D that are not in A
 $(\forall x \in D \text{ AND } x \notin A)$

$$A - B = A \text{ AND } \bar{B} \text{ for domain } A$$

$$B - C = B \text{ AND } \bar{C} \text{ for domain } B$$

$$C - A = C \text{ AND } \bar{A} \text{ for domain } C$$

4.1.2 $\left(\begin{array}{l} \cap = \text{AND} \text{ All elements in both } X \text{ and } Y \\ \cup = \text{Or} \text{ All elements in } X \text{ or } Y \end{array} \right.$

$$(A \cap \bar{B}) \cup (B \cap \bar{C}) \cup (C \cap \bar{A}) \cup (A \cap B \cap C)$$

which matches formula in hint so

$(A \cup B \cup C)$ is equal to

Union $\forall z \exists u \forall x (\exists y, x \in y \text{ AND } y \in z) \text{ iff } x \in u$

Intersection $\exists x. x \in y \text{ or } x \in z$

Michael Plasmeier

Oshani

Table 12

#4

So from 4.3.1

$$f: A \rightarrow B$$

$$g: B \rightarrow C$$

$$g \circ f: A \rightarrow C \quad \text{"composition" } \hat{=} g(f(x))$$

Here

$$R: B \rightarrow C$$

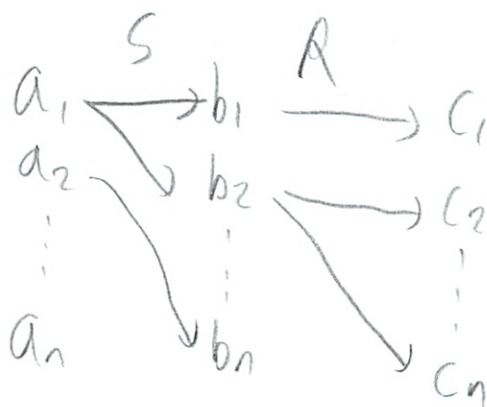
$$S: A \rightarrow B$$

$$R \circ S: A \rightarrow C$$

$$a (R \circ S) c \hat{=} \exists b \in B (b R c) \text{ And } (a S b)$$

Reverse order

$$(a S b) \text{ And } (b R c)$$



①

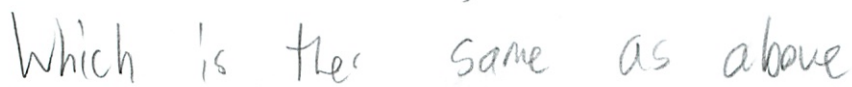
Unclear, ^{to me} see TA for regrade

Say for purpose of argument $n=3$



Now apply operation $M_s \otimes M_r$

Which translates back to



3

Since $a_1 \rightarrow b_2$ does not go anywhere

We can track $a_2 \rightarrow b_3 \rightarrow c_3$

And simplify to $a_2 \rightarrow c_3$

$a_1 \rightarrow b_1$ just forwards and then splits to c_1, c_2

So can go $a_1 \rightarrow c_1$ and $a_1 \rightarrow c_2$

Which the matrix did

How else should I explain it.

see solution

This proof doesn't make much sense to me.
Please read the solution, and see if you understand it. If not come see me. I am happy to help 😊

-Oshani

4

#4 alt method

$M_s(i, k)$ AND $M_R(k, j)$ is true when

An arrow goes from $i \rightarrow k$ and from $k \rightarrow j$. This means there is a connection from $i \rightarrow j$. This connection might not be direct. The and statement collects all of the possible arrows coming in from i to k and going out from $k \rightarrow j$. There must be an arrow from both $i \rightarrow k$ and $k \rightarrow j$ or else there is no connection. The arrow has multiple options of intermediate stops. Only one of them needs to go through, multiple intermediate stops between the same start and end point makes no difference. The matrix is the method that one uses to define the connections.

Michael Plasmeyer

Oshani

Table 12

#5

$\forall s$ pairwise-disjoint(s) $\rightarrow \exists c$ choose-set(c, s)

$\forall s (\forall x \in s, x \neq \emptyset \text{ AND } \forall x, y \in s, x \neq y \rightarrow x \cap y = \emptyset) \rightarrow$

$\exists c (\forall x \in s \exists! z, z \in c \cap x)$

$x = y \quad \forall z \mid z \in x \text{ iff } z \in y$

$x \neq y \quad \forall z \quad z \in x \text{ XOR } z \in y$

$\neq \emptyset \quad \exists x, x \in s$

$= \emptyset \quad \forall x, x \notin s$

Is $\exists! z$ pure? No.

$\exists z, z \in s \text{ AND } \forall y, x \neq z \quad y \notin s$

$\forall s (\forall x \in s, (\exists a, a \in s) \text{ AND } \forall x, y \in s, (\forall b, b \in x \text{ XOR } b \in y$

$\rightarrow \forall x \cap y \neq \emptyset) \rightarrow \forall x \in s (\exists d, d \in s \text{ AND } \forall e,$
 $e \neq d, e \notin s) \text{ ^{impure} } d \in c \cap x$

s is domain of discourse

6

Solutions to Problem Set 2

Reading: Chapter 3.6, covering *Predicate Formulas*, Chapter 4, covering *Sets & Relations*, Chapter 5, covering *Infinite Sets*.

Note: Wednesday lecture will cover Chapter 5.4 & 5.5, on Russell's Paradox & The ZFC Story. This pset does not cover Chapter 5.1–5.3, on Cardinality & the Halting Problem, but these sections are due for Friday lecture, Feb. 18.

Reminder: Email comments on the reading are due *before* the class in which the reading is covered. Latest times for comments on different sections are indicated in the online tutor problem set TP.3. Reading Comments count for 3% of the final grade.

Problem 1.

Translate the following sentence into a predicate formula:

There is a student who has emailed exactly two other people in the class, besides possibly herself.

The domain of discourse should be the set of students in the class; in addition, the only predicates that you may use are

- equality, and
- $E(x, y)$, meaning that “ x has sent e-mail to y .”

Solution. A good way to begin tackling this problem is by working “top-down” to translate the successive parts of the sentence. First of all, our formula must be of the form

$$\exists x.P(x)$$

where $P(x)$ should be a formula that says that “student x has e-mailed exactly two other people in the class, besides possibly herself”.

One way to write $P(x)$ is to give names, say y and z , to the two students whom x has emailed. So we translate $P(x)$ as “besides x , there are two students, y and z , and ...”:

$$\exists y, z. x \neq y \wedge x \neq z \wedge y \neq z \wedge \dots$$

“ x has emailed both y and z , and ...”:

$$E(x, y) \wedge E(x, z) \wedge \dots$$

“if x has emailed somebody, it's either x , y , or z ”:

$$\forall s. E(x, s) \longrightarrow (s = x \vee s = y \vee s = z).$$

Putting these together, we get:

$$\begin{aligned} P(x) ::= & \exists y, z. \quad x \neq y \wedge x \neq z \wedge y \neq z \wedge \\ & E(x, y) \wedge E(x, z) \wedge \\ & [\forall s. E(x, s) \longrightarrow (s = x \vee s = y \vee s = z)] \end{aligned}$$

Problem 2.

Express each of the following predicates and propositions in formal logic notation. The domain of discourse is the nonnegative integers, \mathbb{N} . Moreover, in addition to the propositional operators, variables and quantifiers, you may define predicates using addition, multiplication, and equality symbols, and nonnegative integer constants $0, 1, \dots$, but no *exponentiation* (like x^y). For example, the predicate “ n is an even number” could be defined by either of the following formulas:

$$\exists m. (2m = n), \quad \exists m. (m + m = n).$$

(a) m is a divisor of n .

Solution.

$$m \mid n ::= \exists k. k \cdot m = n$$

■

(b) n is a prime number.

Solution.

$$\text{IS-PRIME}(n) ::= (n \neq 1) \text{ AND } \forall m. (m \mid n) \text{ IMPLIES } (m = 1 \text{ OR } m = n).$$

Note that $n \neq 1$ is an abbreviation of the formula $\text{NOT}(n = 1)$.

■

(c) n is a power of a prime.

Solution. We can say that there is a prime, p , such that every divisor of n not equal 1 to is itself divisible by p :

$$\exists p. [\text{IS-PRIME}(p) \text{ AND } \forall m. (m \mid n \text{ AND } m \neq 1) \text{ IMPLIES } p \mid m].$$

Alternatively, we could say that at most one prime that divides n :

$$\forall p, q. (\text{IS-PRIME}(p) \text{ AND } \text{IS-PRIME}(q) \text{ AND } p \mid n \text{ AND } q \mid n) \text{ IMPLIES } p = q.$$

■

Problem 3.

Let A , B , and C be sets. Prove that:

$$A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C). \quad (1)$$

Hint: $P \text{ OR } Q \text{ OR } R$ is equivalent to

$$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR } (R \text{ AND } \overline{P}) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

Solution. *Proof.* We prove that an element, x , is a member of the left hand side of (1) iff it is a member of the right hand side.

$$x \in A \cup B \cup C$$

$$\text{iff } (x \in A) \text{ OR } (x \in B) \text{ OR } (x \in C) \quad (\text{by def of } \cup)$$

$$\text{iff } ((x \in A) \text{ AND } \overline{(x \in B)}) \text{ OR}$$

$$((x \in B) \text{ AND } \overline{(x \in C)}) \text{ OR}$$

$$((x \in C) \text{ AND } \overline{(x \in A)}) \text{ OR}$$

$$((x \in A) \text{ AND } (x \in B) \text{ AND } (x \in C)) \quad (\text{by the equivalence in the Hint})$$

$$\text{iff } (x \in A - B) \text{ OR } (x \in B - C) \text{ OR } (x \in C - A) \text{ OR}$$

$$(x \in A \cap B \cap C) \quad (\text{by def of } -, \cap)$$

$$\text{iff } x \in (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C) \quad (\text{by def of } \cup)$$

■

Alternative solution by cases:

We prove that the left side is contained in the right side, and that the right side is contained in the left side.

First, we show that the left side is contained in the right side. Let x be any element of $A \cup B \cup C$. Then x belongs to at least one of A , B , and C . We distinguish two cases.

- x belongs to all three sets: Then x belongs to the intersection $A \cap B \cap C$.
- x does *not* belong to all three sets: Then at least one of A , B , C does not contain x . So overall, at least one set contains x and at least one set doesn't. We distinguish cases:
 - If A contains x , then one of B and C must not contain it.
 - * If B does not contain it, then $x \in A - B$.
 - * If B contains it, then C does not, therefore $x \in B - C$.
 - If A does *not* contain x , then one of B and C must contain it.
 - * If C does, then $x \in C - A$.
 - * If C does not contain it, then B does, therefore $x \in B - C$.

In all cases, we end up with x being a member of one of $A - B$, $B - C$, $C - A$, or $A \cap B \cap C$. Therefore, it belongs to the right side. Hence, the set on the left is contained in the set on the right.

Next, we show that the right side is contained in the left. This is easier. Let x belong to the right side. Then it belongs to one of $A - B$, $B - C$, $C - A$, or $A \cap B \cap C$. In the first case, we clearly know $x \in A$. In the second case, $x \in B$. In the third case, $x \in C$. In the last case, $x \in A$ again. So, in all cases, x belongs to one of A , B , or C . So x belongs to the left side. Therefore, the set on the right is contained in the set on the left.

Since each set is contained in the other, they are equal.

■

Problem 4.

There is a simple and useful way to extend composition of functions to composition of relations. Namely, let $R : B \rightarrow C$ and $S : A \rightarrow B$ be relations. Then the composition of R with S is the binary relation $(R \circ S) : A \rightarrow C$ defined by the rule

$$a (R \circ S) c ::= \exists b \in B. (b R c) \text{ AND } (a S b).$$

This agrees with the Definition 4.3.1 of composition in the special case when R and S are functions.

We can represent a relation, S , between two sets $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ as an $n \times m$ matrix, M_S , of zeroes and ones, with the elements of M_S defined by the rule

$$M_S(i, j) = 1 \quad \text{IFF} \quad a_i S b_j.$$

If we represent relations as matrices in this fashion, then we can compute the composition of two relations R and S by a “boolean” matrix multiplication, \otimes , of their matrices. Boolean matrix multiplication is the same as matrix multiplication except that addition is replaced by OR and multiplication is replaced by AND. Namely, suppose $R : B \rightarrow C$ is a binary relation with $C = \{c_1, \dots, c_p\}$. So M_R is an $m \times p$ matrix. Then $M_S \otimes M_R$ is an $n \times p$ matrix defined by the rule:

$$[M_S \otimes M_R](i, j) ::= \text{OR}_{k=1}^m [M_S(i, k) \text{ AND } M_R(k, j)]. \quad (2)$$

Prove that the matrix representation, $M_{R \circ S}$, of $R \circ S$ equals $M_S \otimes M_R$ (note the reversal of R and S).

Solution. Proof. We want to prove that

$$i (R \circ S) j \quad \text{IFF} \quad [M_S \otimes M_R](i, j) = 1. \quad (3)$$

Now

$$\begin{aligned} [M_S \otimes M_R](i, j) &= 1 \\ \text{IFF} \quad &\text{OR}_{k=1}^m [M_S(i, k) \text{ AND } M_R(k, j)] = 1 && \text{(by (2))} \\ \text{IFF} \quad &[M_S(i, k) \text{ AND } M_R(k, j)] = 1 \text{ for some } k, 1 \leq k \leq m && \text{(def. of OR)} \\ \text{IFF} \quad &[M_S(i, k) = 1] \text{ AND } [M_R(k, j) = 1] \text{ for some } k, 1 \leq k \leq m && \text{(def. of AND)} \\ \text{IFF} \quad &i S k \text{ AND } k R j \text{ for some } k, 1 \leq k \leq m && \text{(def. of } M_R, M_S) \\ \text{IFF} \quad &i (R \circ S) j && \text{(def. of } R \circ S). \end{aligned}$$

oh can use ■

Problem 5.

The Axiom of Choice says that if s is a set whose members are nonempty sets that are *pairwise disjoint*—that is no two sets in s have an element in common—then there is a set, c , consisting of exactly one element from each set in s .

In formal logic, we could describe s with the formula,

$$\text{pairwise-disjoint}(s) ::= \forall x \in s. x \neq \emptyset \text{ AND } \forall x, y \in s. x \neq y \text{ IMPLIES } x \cap y = \emptyset.$$

Similarly we could describe c with the formula

$$\text{choice-set}(c, s) ::= \forall x \in s. \exists! z. z \in c \cap x.$$

Here “ $\exists! z$.” is fairly standard notation for “there exists a *unique* z .”

Now we can give the formal definition:

Definition (Axiom of Choice).

$$\forall s. \text{pairwise-disjoint}(s) \text{ IMPLIES } \exists c. \text{choice-set}(c, s).$$

The only issue here is that Set Theory is technically supposed to be expressed in terms of *pure* formulas in the language of sets, which means formula that uses only the membership relation, \in , propositional connectives, the two quantifiers \forall and \exists , and variables ranging over all sets. Verify that the Axiom of Choice can be expressed as a pure formula, by explaining how to replace all impure subformulas above with equivalent pure formulas.

For example, the formula $x = y$ could be replaced with the pure formula $\forall z. z \in x \text{ IFF } z \in y$.

Solution. Here is how the impure subformulas used in the above definition of the Axiom of Choice can be translated into pure formulas:

$x \neq \emptyset$ translates into $\exists y / y \in x$.

$[x \cap y = \emptyset]$ translates into $\text{NOT}(\exists z. z \in x \text{ AND } z \in y)$.

$[z \in x \cap y]$ translates into $z \in x \text{ AND } z \in y$.

$\exists! z. P(z)$ translates into $\exists z. P(z) \text{ AND } \forall w. P(w) \text{ IMPLIES } w = z$.

This last formula is not pure because it uses $=$, but this is ok since we know it can be replaced by a pure formula.

■