# Problem Set 1

*Due*: February 11

**Reading:** Part I.*Proofs*, Chapters 1.*What is a Proof?*, 2.*The Well Ordering Principle*, 3.*Propositional Formulas*. These assigned readings **do not include the Problem sections**. (Many of the problems in the text will appear as class or homework problems.)

*Reminder*: Email comments on the reading are due at times indicated in the online tutor problem set TP.2. Reading Comments count for 3% of the final grade.

## Problem 1.

The fact that that there are irrational numbers $a, b$ such that $a^b$ is rational was proved in Problem 1.2 of the course text. Unfortunately, that proof was *nonconstructive*: it didn't reveal a specific pair, $a, b$, with this property. But in fact, it's easy to do this: let $a ::= \sqrt{2}$ and $b ::= 2\log_2 3$.

We know $\sqrt{2}$ is irrational, and obviously $a^b = 3$. Finish the proof that this $a, b$ pair works, by showing that $2\log_2 3$ is irrational.

## Problem 2.

Use the Well Ordering Principle to prove that

$$n \leq 3^{n/3} \tag{1}$$

for every nonnegative integer, $n$.

*Hint:* Verify (1) for $n \leq 4$ by explicit calculation.

## Problem 3.

Describe a simple recursive procedure which, given a positive integer argument, $n$, produces a truth table whose rows are all the assignments of truth values to $n$ propositional variables. For example, for $n = 2$, the table might look like:

| | |
|---|---|
| T | T |
| T | F |
| F | T |
| F | F |

Your description can be in English, or a simple program in some familiar language (say Scheme or Java), but if you do write a program, be sure to include some sample output.

## Problem 4.

Prove that the propositional formulas

$$P \text{ OR } Q \text{ OR } R$$

and

$$(P \text{ AND NOT}(Q)) \text{ OR } (Q \text{ AND NOT}(R)) \text{ OR } (R \text{ AND NOT}(P)) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

are equivalent.

**Problem 5.**
For $n = 40$, the value of polynomial $p(n) ::= n^2 + n + 41$ is not prime, as noted in Section 1.1 of the course text. But we could have predicted based on general principles that no nonconstant polynomial can generate only prime numbers.

In particular, let $q(n)$ be a polynomial with integer coefficients, and let $c ::= q(0)$ be the constant term of $q$.

**(a)** Verify that $q(cm)$ is a multiple of $c$ for all $m \in \mathbb{Z}$.

**(b)** Show that if $q$ is nonconstant and $c > 1$, then there are infinitely many $n \in \mathbb{N}$ such that $q(n)$ is not prime.

*Hint:* You may assume the familiar fact that the magnitude of any nonconstant polynomial, $q(n)$, grows unboundedly as $n$ grows.

**(c)** Conclude immediately that for every nonconstant polynomial, $q$, there must be an $n \in \mathbb{N}$ such that $q(n)$ is not prime.

## Optional:

**Problem 6.**
There are adder circuits that are much faster than the ripple-carry circuits of Problem 3.5 of the course text. They work by computing the values in later columns for both a carry of 0 and a carry of 1, *in parallel*. Then, when the carry from the earlier columns finally arrives, the pre-computed answer can be quickly selected. We'll illustrate this idea by working out the equations for an $n + 1$-bit parallel half-adder.

Parallel half-adders are built out of parallel "add1" modules. An $n + 1$-bit add1 module takes as input the $n+1$-bit binary representation, $a_n \ldots a_1 a_0$, of an integer, $s$, and produces as output the binary representation, $c\, p_n \ldots p_1\, p_0$, of $s + 1$.

**(a)** A 1-bit add1 module just has input $a_0$. Write propositional formulas for its outputs $c$ and $p_0$.

**(b)** Explain how to build an $n + 1$-bit parallel half-adder from an $n + 1$-bit add1 module by writing a propositional formula for the half-adder output, $o_i$, using only the variables $a_i$, $p_i$, and $b$.

We can build a double-size add1 module with $2(n + 1)$ inputs using two single-size add1 modules with $n + 1$ inputs. Suppose the inputs of the double-size module are $a_{2n+1}, \ldots, a_1, a_0$ and the outputs are $c, p_{2n+1}, \ldots, p_1, p_0$. The setup is illustrated in Figure 1.

Namely, the first single size add1 module handles the first $n + 1$ inputs. The inputs to this module are the low-order $n + 1$ input bits $a_n, \ldots, a_1, a_0$, and its outputs will serve as the first $n + 1$ outputs $p_n, \ldots, p_1, p_0$ of the double-size module. Let $c_{(1)}$ be the remaining carry output from this module.

The inputs to the second single-size module are the higher-order $n + 1$ input bits $a_{2n+1}, \ldots, a_{n+2}, a_{n+1}$. Call its first $n + 1$ outputs $r_n, \ldots, r_1, r_0$ and let $c_{(2)}$ be its carry.

**(c)** Write a formula for the carry, $c$, in terms of $c_{(1)}$ and $c_{(2)}$.

**(d)** Complete the specification of the double-size module by writing propositional formulas for the remaining outputs, $p_i$, for $n + 1 \leq i \leq 2n + 1$. The formula for $p_i$ should only involve the variables $a_i$, $r_{i-(n+1)}$, and $c_{(1)}$.

**(e)** Parallel half-adders are exponentially faster than ripple-carry half-adders. Confirm this by determining the largest number of propositional operations required to compute any one output bit of an $n$-bit add module. (You may assume $n$ is a power of 2.)

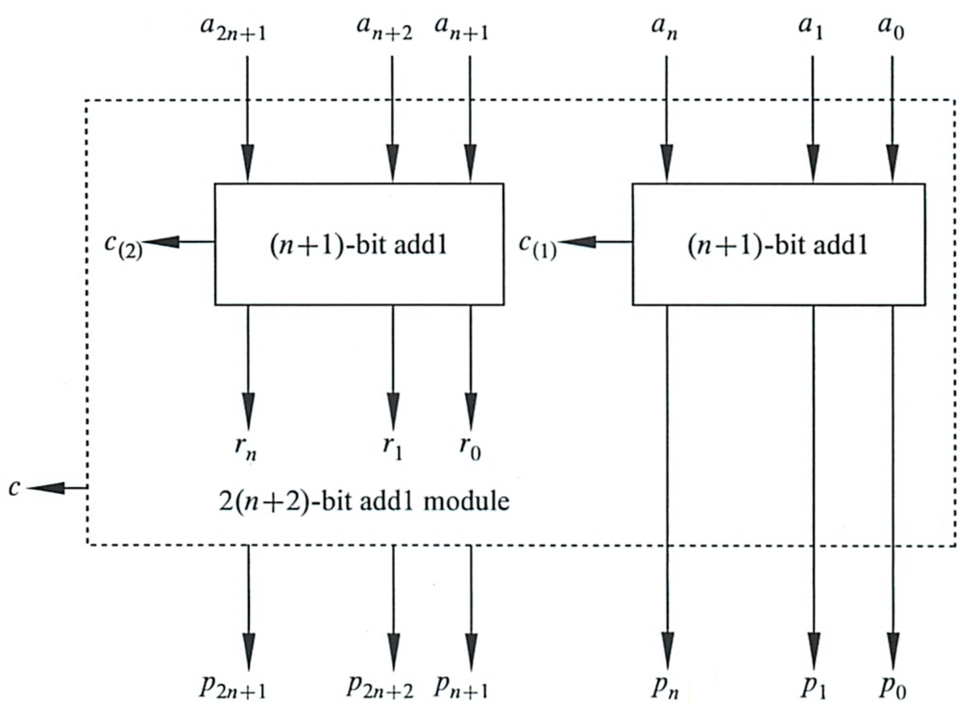



**Figure 1** Structure of a Double-size Add1 Module.

# 6.042 P-Set 1 Doing

2/4

1. No solutions in text

$a = \sqrt{2}$

$b = 2\log_2 3$

$\sqrt{2}^{2\log_2 3}$

$= 3$

$y = \log_b x \Leftrightarrow x = b^y$

Show $2\log_2 3$ is irrational

- that is non divisable by integers

1.8 does this for $\sqrt{2}$

? Just calculate and see ??

I seem to be mostly copying boiler plate

I don't think copying 2 pages of the book is right!

---

Not same way

$2\log_2 n$

Don't have WOP

No integers exist - write $\log_2 n$ as $\frac{m}{n}$

disregard 2

$\log_2 3 \in$ irrational

$= \frac{m}{n}$

What do to $\log_2$

$$\log_2 3 = \frac{m}{n}$$

$$n \log_2 3 = m$$

$$\frac{n \log 3}{\log 2} = m$$

$$n \log 3 = m \log 2$$

$$2^{n \log_2 3} = 2^m$$

$$\cancel{2\ 2 = 2^m}$$

$$2^n \cdot 3 = 2^m$$

has a factor 3 - contridiction

$$2^{2 \cdot 3} = 2^6$$

$$2^2 \cdot 2^3 =$$

2. Grrr

Think I got it

By copying examples

Seems like stupid proof

But its not by other methods

↳ comparing #s

- saying always non neg, etc

Why do I need to test them

Still don't get why add +1

Is proof like cases - like stamp

Find n that is least

m must be > 5

~~[illegible]~~ Find something less than m

Just -1 would fit

Plug in + simplify

3. Recursive

Assign to n variables

So n=3 has $2^3$ rows

So write a program

Should actually do it

---

I did this in class

- need to start w/ all true
- then swap
- or tree logic


Some table - like from 6.01

- reusing that code - big mistake
- need general tree walking algorithm

Look at last char

Actually tree might be better

- never really learned

Or something clever where first row
half T, half F
then ~~next~~ alternate
last

Let me do 3

$i \rightarrow$ / $\downarrow i$

| | | |
|---|---|---|
| T | T | T |
| T | T | F |
| T | F | T |
| T | F | F |
| F | T | T |
| F | T | F |
| F | F | T |
| F | F | F |
| 4 | 2 | 1 |
| $\frac{8}{2}$ | $\frac{8}{4}$ | $\frac{8}{8}$ |

$\uparrow$
$2^i$

half of ther remaining space
might be caiser in matlab

Getting closish

MatLab

Nice works! → ugly code
240 min

May not be very elegant - but works well!

2

4. Prove equivilant

large truth table

Truth table is only way

5. For $n = 40$ $p(n) = n^2 + n + 41$

- not prime

(seems familiar)

└ Tutor problem

And section 1.1

No non constant polynomial can generate only primes

↳ is this because otherwise it won't be prime

$q(n)$ = polynomial w/ integer coefficients

$c := q(0)$ = constant term

a) $q(cm)$ is multiple of $c$ for all $m \in \mathbb{Z}$

? some polynomial

fill in $n$ as variable

$n^2 + n + c$

$(cm)^2 + cm + c$

How is that showing anything? what principle is that?

- multiple of $c$

- $c$ in every term

1

b If $q$ is non constant and $c > 1$

? I don't get

What principles

b) Do hint

Try to see $q(n)$ as $n \uparrow$

Follows from that

did they just give us the answer?

Oh well go with it

# Student's Solutions to Problem Set 1

**Your name:** Michael Plasmeier

**Due date:** February 11

**Submission date:** 2/11

Table 12

**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]

3. I worked only with course staff

Met w/ Oshani for 15 min

**DO NOT WRITE BELOW THIS LINE**

| Problem | Score |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| Total | |



[1] People other than course staff.

[2] Give citations to texts and material other than the Spring '11 course materials.

1. Theorm: $2\log_2 3$ is irrational

We use proof by WOP.

3 For any positive integers $m$ and $n$ the fraction $\frac{m}{n}$ can be written in lowest terms, that is in the form $m'/n'$ where $m'$ and $n'$ are positive integers with no comon factors.

Suppose to the contrary that there were $m, n \in \mathbb{Z}^+$ such that the fraction $\frac{m}{n}$ cannot be written in lowest terms. Now let $C$ be the set of positive integers that are numerators of such fractions. Then $m \in C$ so $C$ is non-empty. Therefore by WOP there must be a smallest integer $m_0 \in C$. So by definition of $C$ there is an integer $n_0 > 0$ such that,

the fraction $\frac{m_0}{n_0}$ cannot be written in lowest terms

This means that $m_0, n_0$ must have a common factor $p > 1$

(2)

But $\frac{m_0/p}{n_0/p} = \frac{m_0}{n_0}$

So any ways of expressing the left hand fraction in lowest terms would also work for $\frac{m_0}{n_0}$

which implies that $\frac{m_0/p}{n_0/p}$ can not be written in lowest terms either.

So by definition of C, the numerator $m_0/p$ is in C

But $m_0/p < m_0$ which contridicts the fact that $m_0$ is the smallest element of C.

Since the assumption that C is non empty leads to a contridiction, it follows that C must be empty.

That is there are no numerators of fractions that can't be written in lowest terms and hence there are no such fractions, so $2\log_2 3$ must be irrational.

How do these relate?

1. Alternate way.

Proof by contidiction. If $2\log_2 3$ was rational then there would be a way to write it as $\frac{m}{n}$

First if $2\log_2 3$ is rational than $\log_2 3$ would be

Start with

$$\log_2 3 = \frac{m}{n}$$

$$n\log_2 3 = m$$

$$\frac{n\log 3}{\log 2} = m$$

$$n\log 3 = m\log 2$$

$$2^{n\log_2 3} = 2^m$$

$$2^n \cdot 3 = 2^m$$

Contidiction there is a factor of 3, so $2\log_2 3$ can not be rational, and thus must be irrational

$P(n) = n \leq 3^{n/3}$

2. Proof by WOP

Assume there is a set C of counter examples

$$C ::= \{m \in \mathbb{N} \mid P(n) \text{ is false}\}$$ ✓

Assume by proof of contridiction that C is non empty

By WOP there will be a smallest element m

But it clearly holds for $m=0$ 4

$0 \leq 3^{0/3}$

$0 \leq 3^0$ ✓

$0 \leq 1$

So $m \geq 1$. So $m-1$ is non-negitive, and since it is smaller than m, $P(n)$ must hold. That is

$m-1 \leq 3^{(m-1)/3}$

It also holds for $m = 1, 2, 3, 4$ (see next page) by your logic

Contradicting the fact that $P(n)$ does hold for m, m can be $\geq 5$ prove why it can't be $\geq 5$

It follows that there is no nonnegitive integer for which $P(n)$ fails so $P(n)$ must hold for all non negitive integers.

Test at $n=1$

$1 \overset{?}{\leq} 3^{1/3}$

$1 \leq 1.44$

Test at $n=2$

$2 \overset{?}{\leq} 3^{2/3}$

$2 \leq 2.08$

Test at $n=3$

$3 \leq 3^{3/3}$

$3 \leq 3$

Test at $n=4$

$4 \leq 4.32$

Michael Plasmeier
Oshani
Table 12
#3



10/10

Note: not recursiv.

```
    %length of each section before it alternates; gets sucessivly smaller
    %for each column
    len = numrows/2^j;
    i = 1; %rows are i
    current = 0; %to start
    while i <= numrows
        ct = 1; %reset section
        if current == 1 %flip bit
            current = 0;
        else
            current = 1;
        end
        while ct <= len %output number in that section
            table(i, j) = current;
            ct = ct + 1;
            i = i+1;
        end
    end
    j = j + 1;
end

table
```

```
>> truthtable(2)

table =

     1     1
     1     0
     0     1
     0     0

>> truthtable(3)

table =

     1     1     1
     1     1     0
     1     0     1
     1     0     0
     0     1     1
     0     1     0
     0     0     1
     0     0     0

>> truthtable(4)

table =

     1     1     1     1
     1     1     1     0
     1     1     0     1
     1     1     0     0
     1     0     1     1
     1     0     1     0
     1     0     0     1
     1     0     0     0
     0     1     1     1
     0     1     1     0
     0     1     0     1
     0     1     0     0
     0     0     1     1
     0     0     1     0
     0     0     0     1
     0     0     0     0

>> truthtable(5)

table =

     1     1     1     1     1
     1     1     1     1     0
     1     1     1     0     1
     1     1     1     0     0
```

```
     1     1     0     1     1
     1     1     0     1     0
     1     1     0     0     1
     1     1     0     0     0
     1     0     1     1     1
     1     0     1     1     0
     1     0     1     0     1
     1     0     1     0     0
     1     0     0     1     1
     1     0     0     1     0
     1     0     0     0     1
     1     0     0     0     0
     0     1     1     1     1
     0     1     1     1     0
     0     1     1     0     1
     0     1     1     0     0
     0     1     0     1     1
     0     1     0     1     0
     0     1     0     0     1
     0     1     0     0     0
     0     0     1     1     1
     0     0     1     1     0
     0     0     1     0     1
     0     0     1     0     0
     0     0     0     1     1
     0     0     0     1     0
     0     0     0     0     1
     0     0     0     0     0

>> truthtable(6)

table =

     1     1     1     1     1     1
     1     1     1     1     1     0
     1     1     1     1     0     1
     1     1     1     1     0     0
     1     1     1     0     1     1
     1     1     1     0     1     0
     1     1     1     0     0     1
     1     1     1     0     0     0
     1     1     0     1     1     1
     1     1     0     1     1     0
     1     1     0     1     0     1
     1     1     0     1     0     0
     1     1     0     0     1     1
     1     1     0     0     1     0
     1     1     0     0     0     1
     1     1     0     0     0     0
     1     0     1     1     1     1
     1     0     1     1     1     0
```

```
     1     0     1     1     0     1
     1     0     1     1     0     0
     1     0     1     0     1     1
     1     0     1     0     1     0
     1     0     1     0     0     1
     1     0     1     0     0     0
     1     0     0     1     1     1
     1     0     0     1     1     0
     1     0     0     1     0     1
     1     0     0     1     0     0
     1     0     0     0     1     1
     1     0     0     0     1     0
     1     0     0     0     0     1
     1     0     0     0     0     0
     0     1     1     1     1     1
     0     1     1     1     1     0
     0     1     1     1     0     1
     0     1     1     1     0     0
     0     1     1     0     1     1
     0     1     1     0     1     0
     0     1     1     0     0     1
     0     1     1     0     0     0
     0     1     0     1     1     1
     0     1     0     1     1     0
     0     1     0     1     0     1
     0     1     0     1     0     0
     0     1     0     0     1     1
     0     1     0     0     1     0
     0     1     0     0     0     1
     0     1     0     0     0     0
     0     0     1     1     1     1
     0     0     1     1     1     0
     0     0     1     1     0     1
     0     0     1     1     0     0
     0     0     1     0     1     1
     0     0     1     0     1     0
     0     0     1     0     0     1
     0     0     1     0     0     0
     0     0     0     1     1     1
     0     0     0     1     1     0
     0     0     0     1     0     1
     0     0     0     1     0     0
     0     0     0     0     1     1
     0     0     0     0     1     0
     0     0     0     0     0     1
     0     0     0     0     0     0

>>
```

4.

| P | Q | R | P OR Q OR R | P AND NOT (Q) | Q AND NOT (R) | R AND NOT (P) | P AND Q AND R | (Long Statement) |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

7

Explanation?

5. $p(n) = n^2 + n + 41$

$q(n)$ = polynomial w/ integer coefficents

$c = q(0)$, the constant term

4/10

a) $q(cm)$ is a multiple of $c$ for all $m \in \mathbb{Z}$

$$\underbrace{a}_{\text{integers}}(cm)^2 + \underbrace{b}_{\text{integers}}(cm) + c$$

$c$ is in every term, so all items are a multiple of $c$

b) $q$ is non constant and $c > 1$, then there are $\infty$ many $n \in \mathbb{N}$ such that $q(n)$ is not prime

As $n$ grows, $q(n)$ will grow along with it because "$q(n)$ grows unboundedly as $n$ grows"

And because there are $\infty$ly many composite numbers, there are infinitely many $n \in \mathbb{N}$ such that $q(n)$ is not prime.

C. Thus for every non constant polynomial $q$, there must be an $n \in \mathbb{N}$ such that $q(n)$ is not prime.

# Solutions to Problem Set 1

**Reading:** Part I. *Proofs: Introduction*, Chapter **??**, *What is a Proof?*; Chapter **??**, *The Well Ordering Principle*; and Chapter **??** through 3.5, covering *Propositional Logic*. These assigned readings **do not include the Problem sections.** (Many of the problems in the text will appear as class or homework problems.)

*Reminder*: Email comments on the reading are due at times indicated in the online tutor problem set TP.2. Reading Comments count for 3% of the final grade.

**Problem 1.**
The fact that that there are irrational numbers $a, b$ such that $a^b$ is rational was proved in Problem **??** of the course text. Unfortunately, that proof was *nonconstructive*: it didn't reveal a specific pair, $a, b$, with this property. But in fact, it's easy to do this: let $a ::= \sqrt{2}$ and $b ::= 2\log_2 3$.

We know $\sqrt{2}$ is irrational, and obviously $a^b = 3$. Finish the proof that this $a, b$ pair works, by showing that $2\log_2 3$ is irrational.

**Solution.** *Proof.* Suppose to the contrary that $2\log_2 3$ was rational. Then $\log_2 3$ must also be rational, say $\log_2 3 = m/n$ for some positive integers $m$ and $n$. So $m = n\log_2 3$. Now raising 2 to each side of this equation gives

$$2^m = 2^{n\log_2 3} = (2^{\log_2 3})^n = 3^n. \tag{1}$$

But this is impossible, since right hand side of (1) is divisible by 3 and the left hand side is not.

So $2\log_2 3$ must be irrational. ■

not a nice fraction

**Problem 2.**
Use the Well Ordering Principle to prove that

$$n \leq 3^{n/3} \tag{2}$$

for every nonnegative integer, $n$.

*Hint:* Verify (2) for $n \leq 4$ by explicit calculation.

**Solution.** Suppose to the contrary that (2) failed for some nonnegative integer. Then by the WOP, there is a least such nonnegative integer, $m$.

But $0 \leq 3^{0/3}$, so $m \neq 0$. Also, $1^3 \leq 3^1$, so taking cube roots, $1 \leq 3^{1/3}$, which implies $m \neq 1$. Likewise, $2^3 \leq 3^2$, so taking cube roots, $2 \leq 3^{2/3}$, which implies $m \neq 2$. Similar simple calculations show that $m \neq 3, 4$, so we know that $m \geq 5$.

Now since $m > m - 3 \geq 0$ and $m$ is the least nonnegative integer for which the inequality (2) fails, the inequality must hold when $n = m - 3$. So

$$\begin{aligned} 3^{m/3} &= 3 \cdot 3^{(m-3)/3} \\ &\geq 3 \cdot (m-3) && \text{(by (2) for } n = m-3) \end{aligned} \tag{3}$$

Also,

$$\begin{aligned} 3 \cdot (m-3) &= 3m - 9 \\ &> 3m - 2m && \text{since } m > 9/2 \\ &= m. \end{aligned} \tag{4}$$

Combining (3) and (4), we get

$$m \le 3^{m/3},$$ should reduce to same thing

contradicting the assumption that (2) fails for $n = m$.

This contradiction implies that there cannot be a nonnegative integer for which (2) fails. By the WOP, this means that (2) must hold for all nonnegative integers. ■

**Problem 3.**
Describe a simple recursive procedure which, given a positive integer argument, $n$, produces a truth table whose rows are all the assignments of truth values to $n$ propositional variables. For example, for $n = 2$, the table might look like:

| | |
|---|---|
| **T** | **T** |
| **T** | **F** |
| **F** | **T** |
| **F** | **F** |

Your description can be in English, or a simple program in some familiar language (say Scheme or Java), but if you do write a program, be sure to include some sample output.

**Solution.** Start with an $n = 1$ table, namely a one-column table whose first row consists of a **T** entry and second row an **F** entry. Build the $n + 1$ table recursively by taking an $n$ table and attaching a **T** at the beginning of every row, then taking another $n$ table and attaching a **F** at the beginning of every row, and finally placing the first table above the second table.

Here's a Scheme program that carries out this procedure:

```
(define (truth-values n)
   (if (= n 1) '((T) (F))
       (let ((table (truth-values (- n 1))))
            (append
               (map (lambda (row) (cons 'T row)) table)
               (map (lambda (row) (cons 'F row)) table)))))
(truth-values 3)
;Value 17: ((t t t) (t t f) (t f t) (t f f)
            (f t t) (f t f) (f f t) (f f f))
```

■

**Problem 4.**
Prove that the propositional formulas

$$P \text{ OR } Q \text{ OR } R$$

and

$$(P \text{ AND NOT}(Q)) \text{ OR } (Q \text{ AND NOT}(R)) \text{ OR } (R \text{ AND NOT}(P)) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

are equivalent.

**Solution.** We compare $(P \text{ OR } Q \text{ OR } R)$ and $K ::= (P \text{ AND NOT}(Q)) \text{ OR } (Q \text{ AND NOT}(R)) \text{ OR } (R \text{ AND NOT}(P)) \text{ OR } (P \text{ AND } Q \text{ AND } R)$ using a truth table:

| $P$ | $Q$ | $R$ | $P \vee Q \vee R$ | $P \wedge \overline{Q}$ | $Q \wedge \overline{R}$ | $R \wedge \overline{P}$ | $P \wedge Q \wedge R$ | $K$ |
|---|---|---|---|---|---|---|---|---|
| T | T | T | **T** | F | F | F | T | **T** |
| T | T | F | **T** | F | T | F | F | **T** |
| T | F | T | **T** | T | F | F | F | **T** |
| T | F | F | **T** | T | F | F | F | **T** |
| F | T | T | **T** | F | F | T | F | **T** |
| F | T | F | **T** | F | T | F | F | **T** |
| F | F | T | **T** | F | F | T | F | **T** |
| F | F | F | **F** | F | F | F | F | **F** |

Both ($P$ OR $Q$ OR $R$) and $K$ have identical truth tables, thus the two statements are equivalent. ■

**Problem 5.**
For $n = 40$, the value of polynomial $p(n) ::= n^2 + n + 41$ is not prime, as noted in Section **??** of the course text. But we could have predicted based on general principles that no nonconstant polynomial can generate only prime numbers.

In particular, let $q(n)$ be a polynomial with integer coefficients, and let $c ::= q(0)$ be the constant term of $q$.

**(a)** Verify that $q(cm)$ is a multiple of $c$ for all $m \in \mathbb{Z}$.

**Solution.** Say $q(n) = c + \sum_{i=1}^{k} a_i n^i$ where $a_i \in \mathbb{Z}$. Then

what?

$$q(cm) = c + \sum_{i=1}^{k} a_i \left(c^i m^i\right) = c\left(1 + \sum_{i=1}^{k} a_i m^i c^{i-1}\right).$$

■

**(b)** Show that if $q$ is nonconstant and $c > 1$, then there are infinitely many $q(n) \in \mathbb{N}$ that are not primes.

*Hint:* You may assume the familiar fact that the magnitude of any nonconstant polynomial, $q(n)$, grows unboundedly as $n$ grows.

**Solution.** If $|q(cm)| > c > 1$, then $q(cm)$ won't be prime because by part (a), it has $c$ as a factor. Since $|q(n)|$ grows unboundedly with $n$, there will be infinitely many different such values of $q(cm)$ as $m$ grows. ■

think got this

**(c)** Conclude immediately that for every nonconstant polynomial, $q$, there must be an $n \in \mathbb{N}$ such that $q(n)$ is not prime.

**Solution.** By part (b), the only remaining case is when $c \leq 1$. But in that case $q(n)$ is not prime for $n = 0$. ■

## Optional:

**Problem 6.**
There are adder circuits that are much faster than the ripple-carry circuits of Problem 3.4 of the course text. They work by computing the values in later columns for both a carry of 0 and a carry of 1, *in parallel*. Then,

when the carry from the earlier columns finally arrives, the pre-computed answer can be quickly selected. We'll illustrate this idea by working out the equations for an $n+1$-bit parallel half-adder.

Parallel half-adders are built out of parallel "add1" modules. An $n+1$-bit add1 module takes as input the $n+1$-bit binary representation, $a_n \ldots a_1 a_0$, of an integer, $s$, and produces as output the binary representation, $c\ p_n \ldots p_1\ p_0$, of $s+1$.

**(a)** A 1-bit add1 module just has input $a_0$. Write propositional formulas for its outputs $c$ and $p_0$.

**Solution.**

$$p_0 = a_0 \text{ XOR } 1 = \text{NOT}(a_0) \tag{5}$$

$$c = a_0. \tag{6}$$

■

**(b)** Explain how to build an $n+1$-bit parallel half-adder from an $n+1$-bit add1 module by writing a propositional formula for the half-adder output, $o_i$, using only the variables $a_i$, $p_i$, and $b$.

**Solution.**

$$o_i = (b \text{ AND } p_i) \text{ OR } (\text{NOT}(b) \text{ AND } a_i)$$

■

We can build a double-size add1 module with $2(n+1)$ inputs using two single-size add1 modules with $n+1$ inputs. Suppose the inputs of the double-size module are $a_{2n+1}, \ldots, a_1, a_0$ and the outputs are $c, p_{2n+1}, \ldots, p_1, p_0$. The setup is illustrated in Figure 1.

Namely, the first single size add1 module handles the first $n+1$ inputs. The inputs to this module are the low-order $n+1$ input bits $a_n, \ldots, a_1, a_0$, and its outputs will serve as the first $n+1$ outputs $p_n, \ldots, p_1, p_0$ of the double-size module. Let $c_{(1)}$ be the remaining carry output from this module.

The inputs to the second single-size module are the higher-order $n+1$ input bits $a_{2n+1}, \ldots, a_{n+2}, a_{n+1}$. Call its first $n+1$ outputs $r_n, \ldots, r_1, r_0$ and let $c_{(2)}$ be its carry.

**(c)** Write a formula for the carry, $c$, in terms of $c_{(1)}$ and $c_{(2)}$.

**Solution.**

$$c = c_{(1)} \text{ AND } c_{(2)}.$$

■

**(d)** Complete the specification of the double-size module by writing propositional formulas for the remaining outputs, $p_i$, for $n+1 \le i \le 2n+1$. The formula for $p_i$ should only involve the variables $a_i$, $r_{i-(n+1)}$, and $c_{(1)}$.

**Solution.** The $n+1$ high-order outputs of the double-size module are the same as the inputs if there is no carry from the low-order $n+1$ outputs, and otherwise is the same as the outputs of the second single-size add1 module. So

$$p_i = (\text{NOT}(c_{(1)}) \text{ AND } a_i) \text{ OR } (c_{(1)} \text{ AND } r_{i-(n+1)}). \tag{7}$$

for $n+1 \le i \le 2n+1$. ■

**(e)** Parallel half-adders are exponentially faster than ripple-carry half-adders. Confirm this by determining the largest number of propositional operations required to compute any one output bit of an $n$-bit add module. (You may assume $n$ is a power of 2.)

**Solution.** The most operations for an output are those specified in formula (7). So it takes at most 4 additional operations to get any one double-size output bit from the single-size output bits that it depends on. It takes $\log_2 n$ doublings to get to from 1-bit to $n$-bit modules, so the largest number of operations needed for any one output bit is $4\log_2 n$.

This observation also shows that the *total* number of operations used in the parallel adder to calculate *all* the output digits is propositional to $n \log_2 n$. This is larger than the total for a ripple-carry adder by a factor proportional to $\log_2 n$. ■

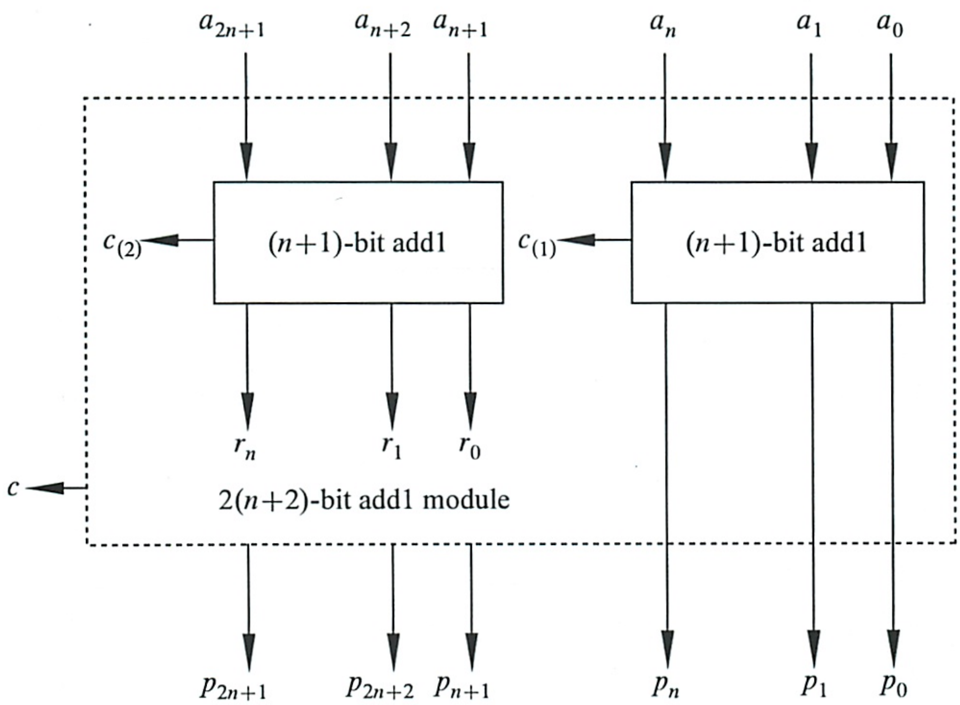



**Figure 1** Structure of a Double-size Add1 Module.

6.042 Tutor

2/19

TP4

$Q(x, y)$ statement

x has been contestant on TV show y

X set of students

Y set of TV shows

No student has ever been contestant

1. $\forall x \forall y$ Not $(Q(x,y))$

3 Not $(\forall x \forall y \; Q(x,y))$

1,3 $\otimes$

4 Not $(\exists x \exists y \; Q(x,y))$

1, 4 ✓ I see now

~~#2~~

TP5

Determine which are true over given range

$\forall x \; E y \quad 2x - y = 0$

②

So for all x, can be 1 y to fix
Both variables over certain range

non neg int ✓
int ✓
real 1

2. $\forall x \; \exists y \;\; x - 2y = 0$

non neg int

$5 - 2y = 0$

$y = 2.5$ X

int X

real ✓

3. $\forall x \;\; x < 10$ implies $(\forall y \;\; y <$ x implies $y < 9)$

implies again
- true if if-part false or then part true

non neg int ✓
int ✓
real ✓

(3)

(really know the reading!)

4. $\forall x \exists y [y > x$ and $\exists z \; y + z = 100]$

z can always fix - but not if must be (F)

Can $y > x$ always

non neg int ×

int ✓

real ✓

So non neg int 1, 3 ✓

int 1, 3, 4 ✓

real 1, 2, 3, 4 ✗

- guessing its 2 from pattern

1, 3, 4 ✗

- guessing 3

1 2 4 ✓

Counter example for 3

$x = 9.5$

oh duh

(4)

TPC Which are valid

1. $\exists x \exists y\ P(x,y)$ implies $\exists y \exists x\ P(x,y)$

normally flipping does not work
but here maybe

2. $\forall x \exists y\ Q(x,y) \rightarrow \exists y \forall x\ Q(x,y)$

say no

3. $\exists x \forall y\ R(x,y) \rightarrow \forall y \exists x\ R(x,y)$

no

4. $\text{Not}(\exists x\ S(x)) \rightarrow \forall x\ \text{Not}(S(x))$

in the book - equivilant

So 1,4 valid ⊗

(I wish it would tell you)

1,~~2~~3,4 ⊗

4 ⊗

1,3,4 ✓

(5)

1. Quantifyers of the <u>same type</u> can be reordered

2. example $Q(x,y)$ be ~~All~~ $y > x$ and suppse non neg int

left side asserts for every natural #
there is a larger natural # - true
right asorts that there exists a
natural # greater than <u>every other</u> natural #
which ~~is~~ false, so statement is false
(this class is all about special cases)

3. Suppose left is true
Then there exists an $x_0$ such that for all
$y$ ~~and~~ $R(x_0, y)$ is true
Thus for all $y$ there exists <u>an</u> $x$ (ie $x_0$)
such that $R(x,y)$ is true

4. If Its not true that there is an ele w/ property S
then every element in domain must not have
property S. Conversly if every element in domain
does not have S, it can't be true that some el has property S

⑥

TP 2.3 makeup

P = get a A on final

Q = do every exercise in book

R = A in final

a. get an A in class, but do not do every exercise
(this was previous class)

~~A~~P AND NOT Q ✗

Or something implies

└ if if-false or then → true

Not Q → ~~A~~ P ✗

That just seems wrong

P → Not Q

Oh A in the class

R and not Q ✓

b) ~~[illegible]~~

$P \wedge Q \wedge R$ ✓

1

c) To get A in class, you must get A on final

here is implies

$R \to P$ ✓

If Q is not true statement is still true → <u>valid</u>

d)

You get A ~~class~~ final, but don't do every exercise

P ⊗

R and not Q ⊗

P and not Q ⊗

$P \to$ not Q ⊗

$\bar{Q} \to P$ ⊗

or iff ?

$P \leftrightarrow \bar{Q}$ ⊗

what is it, give up

$P \wedge \bar{Q} \wedge R$

Oh I did not read the whole thing!

darn – read better!

6.042 2/11

*Mathematics for Computer Science*
MIT 6.042J/18.062J

# Predicate Logic
# Quantifiers $\forall, \exists$



Logic of quantifiers

## Predicates

**Propositions with variables**

**Example:**

$$P(x,y) ::= [x + 2 = y]$$



Can't tell till know x, y

## Predicates

$$P(x,y) ::= [x + 2 = y]$$

now a proposition

x = 1 and y = 3: P(1,3) is true

x = 1 and y = 4: P(1,4) is false

NOT(P(1,4)) is true



## Quantifiers

$\forall x$ For ALL x

$\exists y$ There EXISTS some y



## $\forall$ is like AND

Let s range over 6.042 staff = domain

P(s) ::= [s is Pumped about 6.042]

$$\forall s.\ P(s)$$

same as

P(Stav) AND P(Rich) AND P(Megumi) AND...AND P(Oscar)

holds for all elements



can cover # of things

## $\exists$ is like OR

Let t range over 6.042 staff

B(t) ::= [t took 6.042 Before]

$$\exists t.\ B(t)$$

same as

B(Stav) OR B(Rich) OR B(Megumi) OR...OR B(Oscar)





Need to specify what values x, y - what is the set? the domain (domain of discourse)

Y has the property that something smaller than it

## Existential Quantifier

Let x, y range over $\mathbb{N}$ ∈ nonneg int

$Q(y) ::= \exists x.\ x < y$

Q(3) is T ([x<3] is T for x=1)

Q(1) is T ([x<1] is T for x=0)

Q(0) is F ([x<0] is not T for any x in $\mathbb{N}$)



## Universal Quantifier

x, y range over $\mathbb{N}$

$R(y) ::= \forall x.\ x < y$ Says y is the biggest thing there is

R(1) is F ([x<1] is F for x=5)

R(8) is F ([x<8] is F for x=12)

$R(10^{100})$ is F ($[x<10^{100}]$ is F for $x=10^{100}$)



always false

Say ∀x - makes it an assertion abt all y

∈ is a member of

## virus attack, I: ∀∃

$\forall v \in$ virus . $\exists d \in$ defense. d protects against v

For every virus, I have a defense:

every virus has a defense

against MYDOOM, use Defender

against ILOVEYOU, use Norton

against BABLAS, use Zonealarm...

∀∃ is expensive!



have to buy too much software!

Much better

## virus attack, II: ∃∀

$\exists d \in$ defense . $\forall v \in$ virus. d protects against v

That's what we want!

Example: d is MITviruscan, protects against *all* viruses



(much clearer)

## Alternating Quantifiers

$G ::= \forall x \exists y.\ x < y$

x, y range over Domain of Discourse ∈ need to tell

| *Domain* | *G is:* |
|---|---|
| $\mathbb{N}$ | T |
| ints < 0 | F |
| reals < 0 | T |

can't have anything bigger than −1

for every x, let y be $\frac{x}{2}$



~~There is a biggest y that is bi~~

for every x, there is something bigger

there is no largest x

## Reverse the Quantifiers

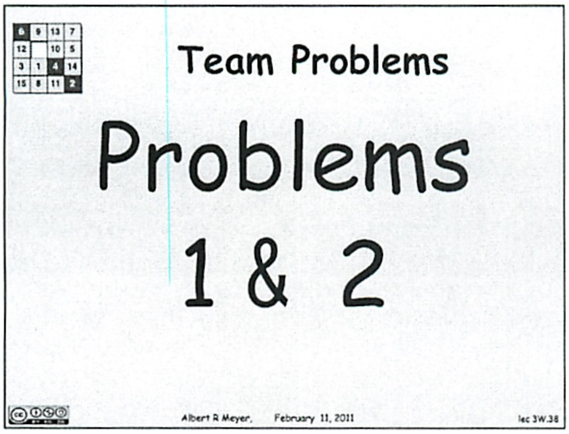
$H ::= \exists y \forall x.\ x \leq y$

| *Domain* | *H is:* |
|---|---|
| $\mathbb{N}$ | F |
| $\mathbb{Z}^-$ | T can't be itself |
| $\mathbb{R}^-$ | F |



Y is bigger than everything

(2)




New slides

All that $\underbrace{\text{glitters}}_{G}$ is not $\underbrace{\text{gold}}_{Au}$

literal $\forall x.[G(x) \to \text{Not}(Au(x))]$

— not what he meant

But gold glitters.

He means Not everything that glitters is gold

$\text{Not}(\forall x.[G(x) \to Au(x)])$

You must figure out what is actually meant.

---

Validity more complicated

$\forall z.[P(z) \text{ and } Q(z)] \to [\forall x.P(x) \land \forall y.Q(y)]$

First need domain of discourse

③ Assumes its for both
What propertiy is P, Q

But this is valid for everything
How can you prove this?
- This is often an axom
- what is more basic than this
How to think intuitivly about this?

Proof strategy

Assume left is T, then prove right side T
↳ that is $Q(z)$ and $P(z)$ holds for when $val(z)$ may get in the domain

C is some domain element

So $Q(c)$ and $P(c)$ holds, so $Q(c)$ ~~holds~~ by itself holds.

universal generalization
But c can be any element of domain
So $\forall x\, Q(x)$

Validity argument →
Similary conclude $\forall y.\, P(y)$ Therefore $\forall x\, Q(x)$ and $\forall y\, P(y)$ $\square$

he swapped b/w x, y variables

(4)

## Universal Generalization (UG)

$$\frac{P(c)}{\forall x.\ P(x)}$$

proiding c does not occur in P

~~More Validities~~

## Similar Example is Not Valid

$$\forall z.\ P(z) \text{ or } Q(z)] \to [\forall x.\ P(x) \text{ or } \forall y\ Q(y)]$$

Marble colors example

Proof: by counter model:

Assume left is true, show right is F

domain ::= $\{1, 2\}$

$Q(z) ::= [z = 1]$

$P(z) ::= [z = 2]$

## De Morgan's Law

$$\text{Not}(\forall x.\ P(x)) \leftrightarrow \exists y.\ \text{Not}(P(y))$$

# In-Class Problems Week 2, Fri.

**Problem 1.**
For each of the logical formulas, indicate whether or not it is true when the domain of discourse is $\mathbb{N}$, (the nonnegative integers 0, 1, 2, ...), $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rationals), $\mathbb{R}$ (the real numbers), and $\mathbb{C}$ (the complex numbers). Add a brief explanation to the few cases that merit one.

$$\exists x. x^2 = 2$$
$$\forall x.\exists y. x^2 = y$$
$$\forall y.\exists x. x^2 = y$$
$$\forall x \neq 0.\exists y. xy = 1$$
$$\exists x.\exists y. x + 2y = 2 \text{ AND } 2x + 4y = 5$$

**Problem 2.**
The goal of this problem is to translate some assertions about binary strings into logic notation. The domain of discourse is the set of all finite-length binary strings: $\lambda$, 0, 1, 00, 01, 10, 11, 000, 001, .... (Here $\lambda$ denotes the empty string.) In your translations, you may use all the ordinary logic symbols (including =), variables, and the binary symbols `0`, `1` denoting 0, 1.

A string like $\texttt{01}x\texttt{0}y$ of binary symbols and variables denotes the *concatenation* of the symbols and the binary strings represented by the variables. For example, if the value of $x$ is `011` and the value of $y$ is `1111`, then the value of $\texttt{01}x\texttt{0}y$ is the binary string `0101101111`.

Here are some examples of formulas and their English translations. Names for these predicates are listed in the third column so that you can reuse them in your solutions (as we do in the definition of the predicate NO-1S below).

| Meaning | Formula | Name |
|---|---|---|
| $x$ is a prefix of $y$ | $\exists z\ (xz = y)$ | PREFIX$(x, y)$ |
| $x$ is a substring of $y$ | $\exists u \exists v\ (uxv = y)$ | SUBSTRING$(x, y)$ |
| $x$ is empty or a string of 0's | NOT(SUBSTRING$(\texttt{1}, x)$) | NO-1S$(x)$ |

**(a)** $x$ consists of three copies of some string.

**(b)** $x$ is an even-length string of 0's.

**(c)** $x$ does not contain both a 0 and a 1.

**(d)** $x$ is the binary representation of $2^k + 1$ for some integer $k \geq 0$.

**(e)** An elegant, slightly trickier way to define NO-1S$(x)$ is:

$$\text{PREFIX}(x, \texttt{0}x). \tag{*}$$

Explain why (*) is true only when $x$ is a string of 0's.

**Problem 3.**
Provide a counter model for the invalid implication. Informally explain why the other one is valid.

1. $\forall x. \exists y. P(x, y)$ IMPLIES $\exists y. \forall x. P(x, y)$

2. $\exists y. \forall x. P(x, y)$ IMPLIES $\forall x. \exists y. P(x, y)$

**Problem 4.**
When the Poet says "There is a season for every purpose under heaven." Which of the following does he mean:

$$\exists s \in \text{Season}. \forall p \in \text{Purpose}. s \text{ is for } p \tag{1}$$

or

$$\forall p \in \text{Purpose}. \exists s \in \text{Season}. s \text{ is for } p \tag{2}$$

Briefly explain.

# W2 Fri

2/11

1a. $\sqrt{2}$ is true

$-\sqrt{2}$

$\mathbb{N}$ F ← missed

$\mathbb{Z}$ × ✓

$\mathbb{Q}$ × ✓

$\mathbb{R}$ ✓ ✓

$\mathbb{C}$ ✓ ✓

b true in all cases ✓

c Can take $\sqrt{\ }$ of any value

Only true in $\mathbb{C}$ ✓

d ~~$\mathbb{Q}$~~ ~~$\mathbb{R}$~~ $\mathbb{Q}$ work since just flip $\frac{a}{b}$ to $\frac{b}{a}$

~~$\mathbb{R}$ ✓~~ $x<0$

$\mathbb{C}$ ✓

e) There is no way to do this

~~$\mathbb{Q}$~~ $2x+4y=4$

$\neq 5$ ✓

did not write down reasons

(2)

2. Try to translate to logic
x, y = variables

a) $\exists z . x = zzz$ ✓

~~???~~ z = is string

Consists of and only of

b) len(x) ~~and~~ mod(2)

? can we do?

No-1s(x) $\cap$

See later

c) No-0s XOR No-1s

? not defined, write out

Not (substring (1, x) AND substring (0, x)) ✓

d) 10

11

101

1001

10001

③

$X = 10 \cup X = 11 \cup$ Prefix$(1, x)$ ~~and~~ $\cap$ Postfix$(1, x)$

$(\exists z \quad zx = y)$

$\|$ $\|$

$\exists z.$ No-1s$(z)$ AND $x = 1z1$

~~(a)~~ b) No-1s$(x)$ AND $\exists z,$ $X = zz$

clever

e) $\exists z \,(xz = 0x)$

X is what goes in the middle here

Some 0 to make this fit must be

a string of 0s

repeated right shifts

(induction-y

(? Better way to explain)

(Alan is being very nice + helping me)

Prof: Prove lenght by ~~taki~~ taking 1 char off string.

~~each~~ repeat till run out of char at same time

(4)

3. Provide a counter model
One is valid, one is invalid

$\forall x. \exists y. P(x,y) \to \exists y. \forall x. P(x,y)$

$\exists y. \forall x. P(x,y) \to \forall x. \exists y. P(x,y)$

This is what the book/class explained, right?

1. is no minimum real #

Our board

Counter example to #1

$x, y \in \mathbb{R}$

let $p(x,y) ::= x = y$

---

Assume $Y$ satisfies $\forall x. P(x,y)$

then for $\forall x$, $Y$ satisfies $P(x,y)$

(5)

4. There is a season for every purpose under heaven.

~~What~~ which is it

$$\exists s \in \text{Season}\ \forall p \in \text{purpose}.\ s \text{ is for } p$$

$$\forall p \in \text{Purpose}.\ \exists s \in \text{Season}.\ s \text{ is for } p$$

2nd one. The means that for all purposes a season exists. Each purpose may have a different season.
(I actually got this myself + put on board)

No explination - how to know

~~On~~ #1 means there is 1 season that fits all purposes.

Would imply that planting + harvesting are appropiate in same season as making snowmen which is nonsenical

# Solutions to In-Class Problems Week 2, Fri.

**Problem 1.**
For each of the logical formulas, indicate whether or not it is true when the domain of discourse is $\mathbb{N}$, (the nonnegative integers 0, 1, 2, ...), $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rationals), $\mathbb{R}$ (the real numbers), and $\mathbb{C}$ (the complex numbers). Add a brief explanation to the few cases that merit one.

$$\exists x.\, x^2 = 2$$
$$\forall x.\exists y.\, x^2 = y$$
$$\forall y.\exists x.\, x^2 = y$$
$$\forall x \neq 0.\exists y.\, xy = 1$$
$$\exists x.\exists y.\, x + 2y = 2 \text{ AND } 2x + 4y = 5$$

**Solution.**

| *Statement* | $\mathbb{N}$ | $\mathbb{Z}$ | $\mathbb{Q}$ | $\mathbb{R}$ | $\mathbb{C}$ |
|---|---|---|---|---|---|
| $\exists x.\, x^2 = 2$ | **F** | **F** | **F** | **T** $(x = \sqrt{2})$ | **T** |
| $\forall x.\exists y.\, x^2 = y$ | **T** | **T** | **T** | **T** $(y = x^2)$ | **T** |
| $\forall y.\exists x.\, x^2 = y$ | **F** | **F** | **F** | **F** (take $y < 0$) | **T** |
| $\forall x \neq 0.\exists y.\, xy = 1$ | **F** | **F** | **T** | **T** $(y = 1/x)$ | **T** |
| $\exists x.\exists y.\, x + 2y = 2 \text{ AND } 2x + 4y = 5$ | **F** | **F** | **F** | **F** | **F** |

■

**Problem 2.**
The goal of this problem is to translate some assertions about binary strings into logic notation. The domain of discourse is the set of all finite-length binary strings: $\lambda$, 0, 1, 00, 01, 10, 11, 000, 001, .... (Here $\lambda$ denotes the empty string.) In your translations, you may use all the ordinary logic symbols (including =), variables, and the binary symbols 0, 1 denoting 0, 1.

A string like $01x0y$ of binary symbols and variables denotes the *concatenation* of the symbols and the binary strings represented by the variables. For example, if the value of $x$ is 011 and the value of $y$ is 1111, then the value of $01x0y$ is the binary string 0101101111.

Here are some examples of formulas and their English translations. Names for these predicates are listed in the third column so that you can reuse them in your solutions (as we do in the definition of the predicate NO-1S below).

| Meaning | Formula | Name |
|---|---|---|
| $x$ is a prefix of $y$ | $\exists z\ (xz = y)$ | PREFIX$(x, y)$ |
| $x$ is a substring of $y$ | $\exists u \exists v\ (uxv = y)$ | SUBSTRING$(x, y)$ |
| $x$ is empty or a string of 0's | NOT(SUBSTRING$(1, x)$) | NO-1S$(x)$ |

**(a)** $x$ consists of three copies of some string.

**Solution.** $\exists y\ (x = yyy)$

■

**(b)** $x$ is an even-length string of 0's.

**Solution.** $\text{NO-1S}(x)$ AND $\exists y\ (x = yy)$

Some students mentioned $\lambda$ in their formulas. Technically, this is not allowed, so they need to justify it by giving a formula that means "$x = \lambda$." This is easy, for example: $x = xx$.

A serious mistake was to try writing a recursive definition of a predicate calculus formula, as in

$$P(x) ::= x = \lambda \text{ OR } \exists y. x = 00y \text{ AND } P(y). \tag{1}$$

Such recursive formulas are, by definition, *not* part of predicate calculus—with good reason. Definition 1 resembles a simple recursive definition of a *procedure* to test if $x$ is an even length string of 0's, and its meaning might be explained in procedural terms. But it's hard to figure out in general what recursively defined formulas mean. For example, let $n$ be an integer-valued variable, and suppose we tried to define a formula, $Q(n)$, that means $n$ is positive:

$$Q(n) ::= (n = 0 \text{ OR NOT}(Q(n+1))) \text{ AND } (n = 1 \text{ OR } Q(n-1)).$$

might succeed in giving a procedural explanation for this example,

■

**(c)** $x$ does not contain both a 0 and a 1.

**Solution.**

$$\text{NOT}[\text{SUBSTRING}(0, x) \text{ AND SUBSTRING}(1, x)]$$

■

**(d)** $x$ is the binary representation of $2^k + 1$ for some integer $k \geq 0$.

**Solution.** $(x = 10)$ OR $(\exists y\ (x = 1y1$ AND $\text{NO-1S}(y)))$ ■

**(e)** An elegant, slightly trickier way to define $\text{NO-1S}(x)$ is:

$$\text{PREFIX}(x, 0x). \tag{*}$$

Explain why (*) is true only when $x$ is a string of 0's.

**Solution.** Prefixing $x$ with 0 rightshifts all the bits. So the $n$th symbol of $x$ shifts into the $(n+1)$st symbol of $0x$. Now for $x$ to be a prefix of $0x$, the $n + 1$st symbol of $0x$ must match the $(n+1)$st symbol of $x$. So if $x$ satisfies (*), the $n$th and $(n+1)$st symbols of $x$ must match. This holds for all $n > 0$ up to the length of $x$, that is, *all* the symbols of $x$ must be the same. In addition, if $x \neq \lambda$, it must start with 0. Therefore, if $x$ satisfies (*), all its symbols must be 0's.

Note that it's easy to see, conversely, that if $x = \lambda$ or $x$ is all 0's, then of course it satisfies (*). ■

**Problem 3.**
Provide a counter model for the invalid implication. Informally explain why the other one is valid.

1. $\forall x. \exists y. P(x, y)$ IMPLIES $\exists y. \forall x. P(x, y)$

2. $\exists y. \forall x. P(x, y)$ IMPLIES $\forall x. \exists y. P(x, y)$

**Solution.** The first implication, $\forall x. \exists y. P(x, y) \longrightarrow \exists y. \forall x. P(x, y)$, is invalid.

One counter model is the predicate $P(x, y) ::= y < x$ where the domain of discourse is the real numbers, $\mathbb{R}$. For every real number $x$, there exists a real number $y$ which is strictly less than $x$, so the antecedent of the implication is true. But there is no minimum real number, so the consequent is false.

The second implication is valid. Let's say that "$x$ is good for $y$" when $P(x.y)$ is true. The hypothesis says that there is some element, call it $g$, that is good for everything. The conclusion is that every element has something that is good for it, which of course is true since $g$ will be good for it.

■

**Problem 4.**
When the Poet says "There is a season for every purpose under heaven." Which of the following does he mean:

$$\exists s \in \text{Season}. \forall p \in \text{Purpose}. s \text{ is for } p \tag{2}$$

or

$$\forall p \in \text{Purpose}. \exists s \in \text{Season}. s \text{ is for } p \tag{3}$$

Briefly explain.

**Solution.** This poetic statement is meant to offer solace: this may be a bad season for you now, but be hopeful, a season that suits your purpose will come. So the appropriate translation would be formula (3), namely that given your Purpose, you can find a season that's good for it. For example, if your purpose is planting, take heart: even though it's Winter now, Spring is coming.

Formula (2) says you can find a single season, say Spring, that's good for every possible Purpose like skiiing, leaf watching, .... This is false, so it's clearly not what the Poet meant. But even though he really meant (3), he used his poetic license to express (3) in a way that mechanically would translate into (2).

Note that a similar statement, "There is a man for all seasons," is famously used to describe one extraordinarily versatile man, Sir Thomas More. So this statement would actually best be translated as

$$\exists x \in \text{men}. \forall s \in \text{seasons}. x \text{ is (good) for } s$$

■

*Mathematics for Computer Science*
MIT 6.042J/18.062J

# Sets & Functions



## 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*?)



## Some sets

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



## Some sets

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

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

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

-- order doesn't matter



## Membership

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

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

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

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



## Synonyms for Membership

$x \in A$
x is an element of A
x is in A

*Examples:*

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

### 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)



### 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:

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



### Subset

examples:

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

$A \subseteq A$, $\varnothing \subseteq$ every set



### $\varnothing \subseteq$ everything

def: $\varnothing \subseteq B$

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



### Defining Sets

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

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

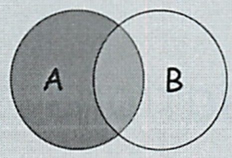


### Defining Sets

The set of even integers:

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

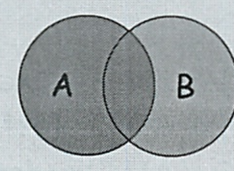
## New sets from old




Venn Diagram for 2 Sets



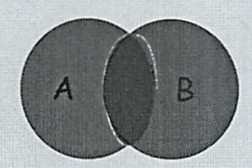
## union




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



## intersection




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



## A set-theoretic equality

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

*proof:* Show these have the same elements, namely,

$x \in$ Left Hand Set iff $x \in$ RHS

for all x.



## A set-theoretic equality

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

proof uses fact from last time:

P OR (Q AND R) equiv

(P OR Q) AND (P OR R)



## 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

$x \in A$ OR $x \in (B \cap C)$ (def of $\cup$) iff

$x \in A$ OR ($x \in B$ AND $x \in C$) (def $\cap$) iff

($x \in A$ OR $x \in B$) AND ($x \in A$ OR $x \in C$)

(by the equivalence)

## 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 $\cap$).

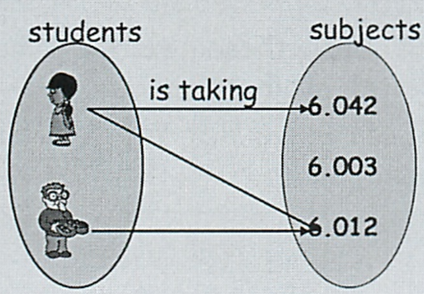
QED



# Relations & Functions

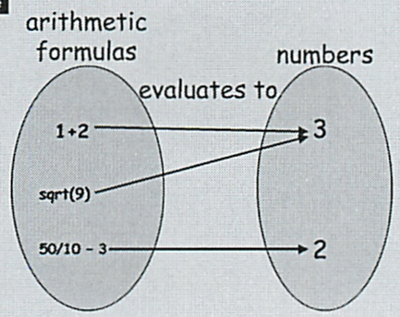


## "is taking subject" relation



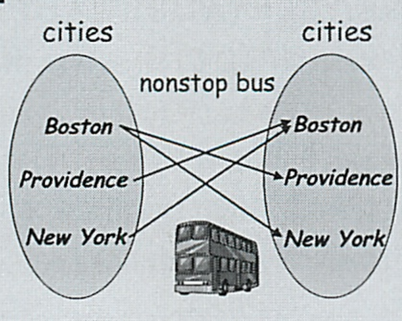



## formula "evaluation" relation





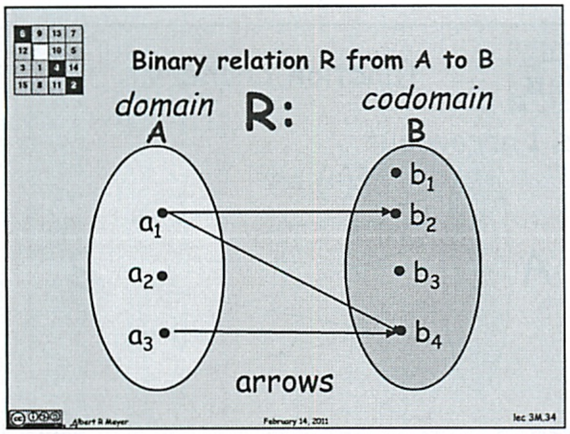

## "nonstop bus trip" relation

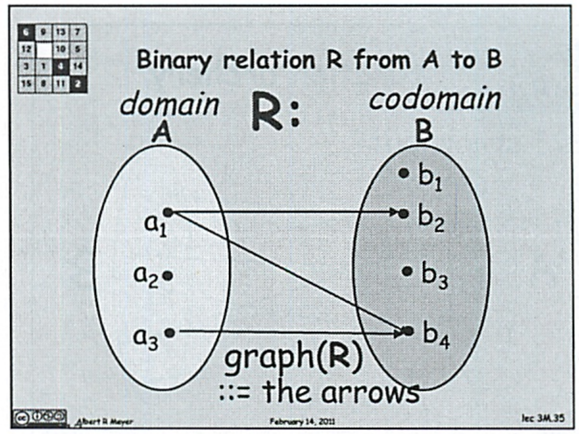


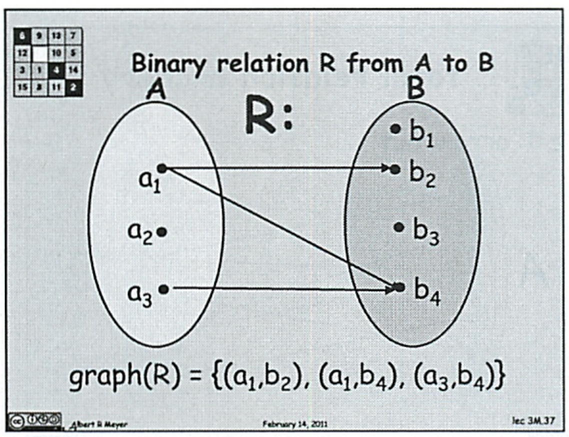


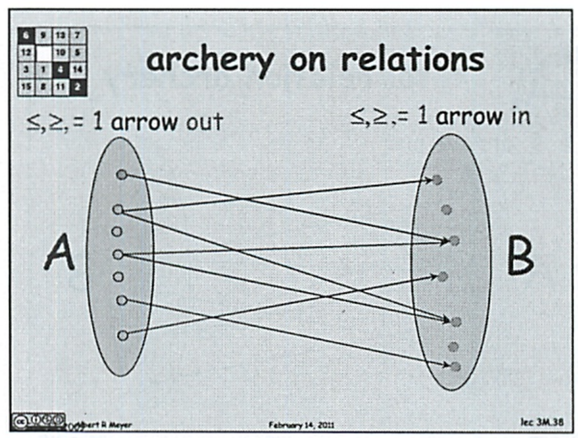

## Binary relations

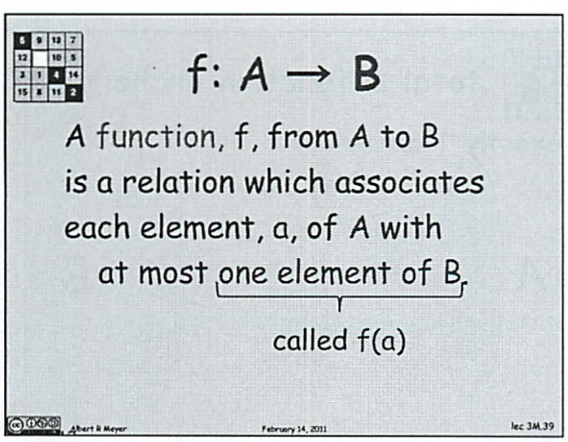
A binary relation, R, from a set A to a set B associates of elements of A with elements of B.

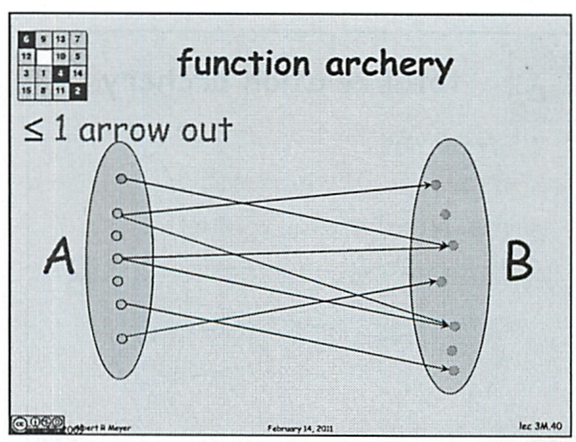

Binary relation R from A to B
domain
A
R:
codomain
B
$b_1$
$a_1$
$b_2$
$a_2$
$b_3$
$a_3$
$b_4$
arrows
Albert R Meyer
February 14, 2011
lec 3M.34

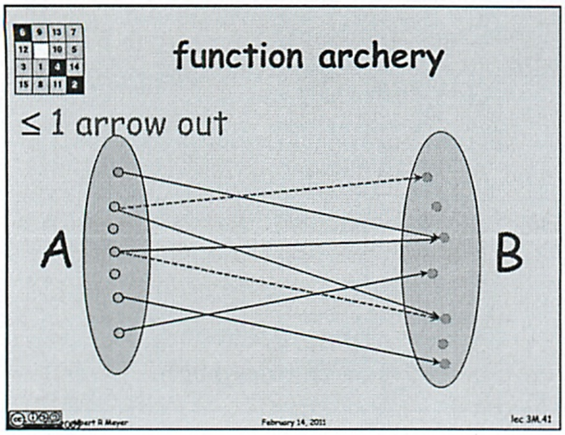

Binary relation R from A to B
domain
A
R:
codomain
B
$b_1$
$a_1$
$b_2$
$a_2$
$b_3$
$a_3$
$b_4$
graph(R)
::= the arrows
Albert R Meyer
February 14, 2011
lec 3M.35

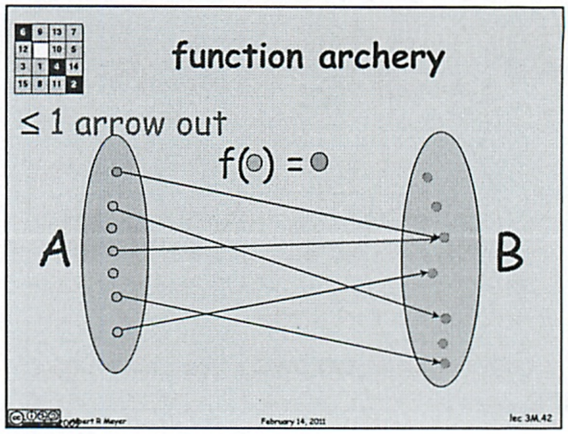

Binary relation R from A to B
A
R:
B
$b_1$
$a_1$
$b_2$
$a_2$
$b_3$
$a_3$
$b_4$
graph(R) = $\{(a_1,b_2), (a_1,b_4), (a_3,b_4)\}$
Albert R Meyer
February 14, 2011
lec 3M.37

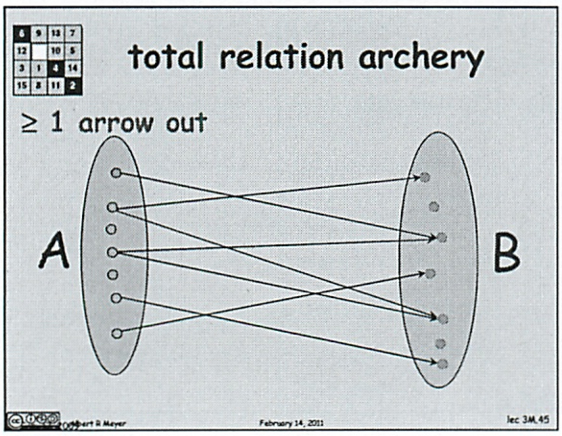

archery on relations
$\le, \ge, =$ 1 arrow out
$\le, \ge, =$ 1 arrow in
A
B
Albert R Meyer
February 14, 2011
lec 3M.38

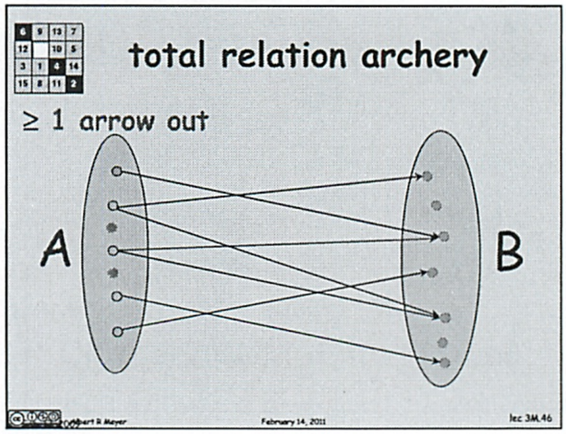

f: A → B
A function, f, from A to B
is a relation which associates
each element, a, of A with
at most one element of B,
called f(a)
Albert R Meyer
February 14, 2011
lec 3M.39

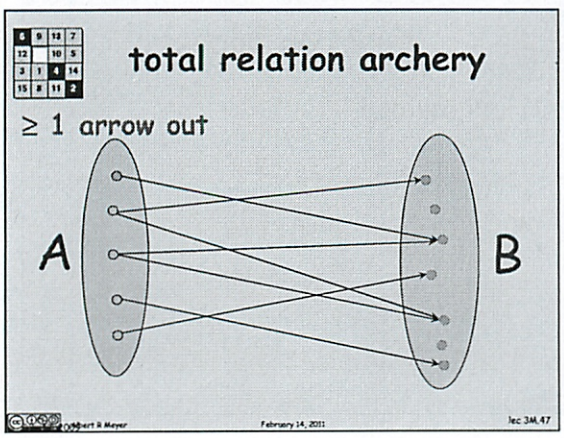

function archery
≤ 1 arrow out
A
B
Albert R Meyer
February 14, 2011
lec 3M.40

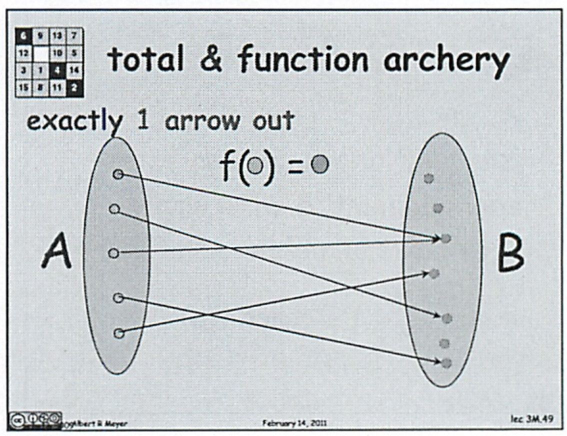

function archery
≤ 1 arrow out
A
B
February 14, 2011
lec 3M.41


function archery
≤ 1 arrow out
f(○) = ●
A
B
February 14, 2011
lec 3M.42

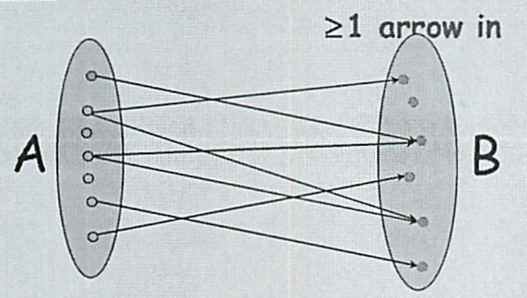

total relation archery
≥ 1 arrow out
A
B
February 14, 2011
lec 3M.45


total relation archery
≥ 1 arrow out
A
B
February 14, 2011
lec 3M.46


total relation archery
≥ 1 arrow out
A
B
February 14, 2011
lec 3M.47

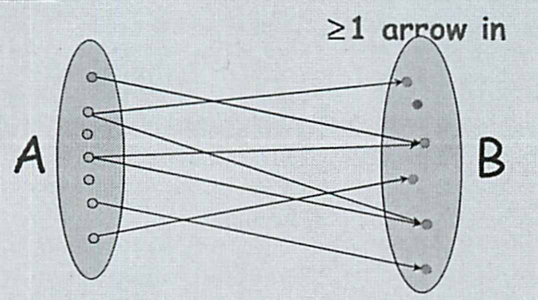

total & function archery
exactly 1 arrow out
f(○) = ●
A
B
February 14, 2011
lec 3M.49

## surjection archery



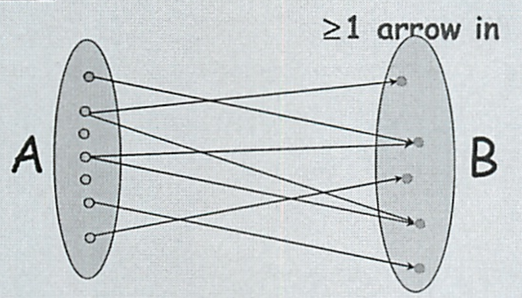



## surjection archery





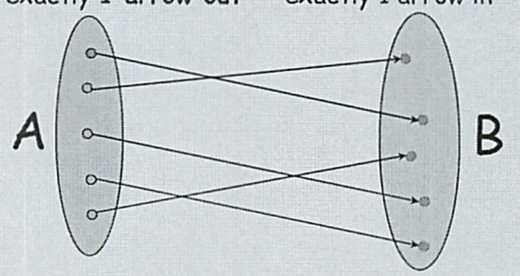

## surjection archery






## bijection archery

exactly 1 arrow out exactly 1 arrow in







## Mapping Rule (bij)

A bijection from
A to B implies

$$|A| = |B|$$

A is *same size as* B



## Team Problems

# Problems 1—4

# 6.042 Sets

2/14

(~~a~~ 5 min late)

~~Sets~~ $\mathbb{N}$

$\mathbb{R}$ etc

$\{$ ele1, ele2, ... $\}$

often sets of mixed type

no notion of order

~~Li~~ Lists are more fundamental in computers

But non-order is important in sets

$x \in A$

↳ 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 ~~[illegible]~~ containment

in or not in ↳ single elements ↳ subsets

2 $\{2\}$

- ~~a~~ a multiset does care

~~AA~~ $\subseteq$ = subset

$A \subseteq B$ ~~[illegible]~~ → 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

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

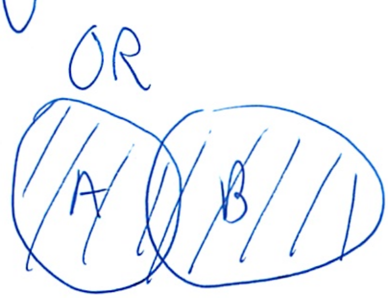
such that

nonneg even

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

---

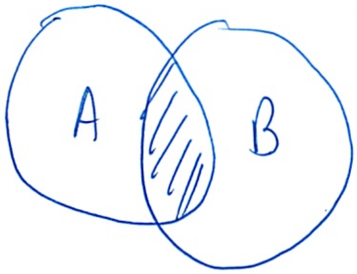
Union $\cup$



③

## ~~A~~ 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 asertion till proposonitul combo of other assertion

Positional combonations

identies - truth table reasons

---

## Relations + functions

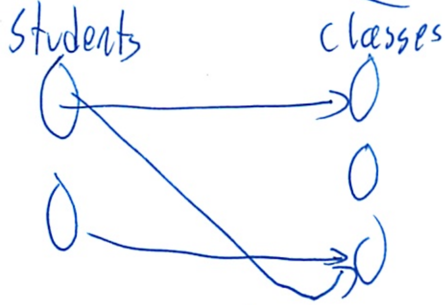
Can build everything out of ~~a~~ sets

- start w/ empty set $\emptyset$
- pedantic

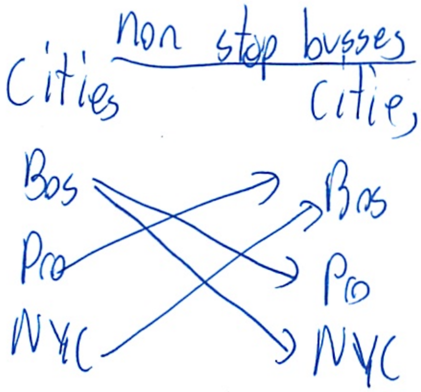
(4)

binary relation
- relation b/w 2 things

relation is taking




3 components of a relation




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

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

<u>archery</u>

Classifying relations w/ # of arrows out or in

is it $\leq, \geq, =$

<u>function</u>

relation between domain + codomain

each element A maps to at ~~one~~ most one element of B

— called $f(a)$

Can just use arrows

— don't need to worry about vocab

(now makes a lot more sense, from 115)

<u>total relation</u> = $\geq 1$ arrow out

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

<u>total and function</u> = exactly 1 arrow out

<u>surjection</u> = at least one arrow in

<u>bijection</u> = perfect correspondance = exactly 1 arrow in and out

perfect line up

$|A| = |B|$ ← same size

6

Miniquiz Wed

- 1 sided notes written or typed

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

February 14
revised Monday 14th February, 2011, 09:53

# 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 that[1]

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

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-away[2] 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 original 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]



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

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

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

[3] David 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:

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

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 is 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.** $A$ surj $B$ iff there is a surjective **function** from $A$ to $B$.

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

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

**(a)** Prove that if $A$ surj $B$ and $B$ surj $C$, then $A$ surj $C$.

**(b)** Explain why $A$ surj $B$ iff $B$ inj $A$.

**(c)** Conclude from (a) and (b) that if $A$ inj $B$ and $B$ inj $C$, then $A$ inj $C$.

## Arrow Properties

**Definition.** A binary relation, $R$ is

- is a *function* when it has the [$\leq 1$ arrow **out**] property.
- is *surjective* when it has the [$\geq 1$ 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 [$\geq 1$ arrows **out**] property.
- is *injective* when it has the [$\leq 1$ arrow **in**] property.
- is *bijective* when it has both the [$= 1$ arrow **out**] and the [$= 1$ 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

2 items {1, 2}

1st player {1}

2nd player {2} wins

3 items {1, 2, 3}

1st player {1, 2} ← but would never do

2nd player {3} wins

3 items alt

1st player {1}

2nd player {2,3} wins

~~1st 3rd 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 alt

1st player n-1 items

2nd player nth item wins

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

Can use trees of cases

---

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

$P \text{ AND } (\overline{Q} \text{ or } Q) = P$ By distributive law of AND

always true

$P \text{ AND True} = P$

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 $(x \in A) \cap \underbrace{(x \notin B \cup x \in B)}_{\text{always true}}$ By distributive law of AND

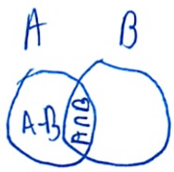
$x \in A$ iff $(x \in A) \cap \text{True}$

x is an ele of A if this is true

$x \in A$ iff $x \in A$ ∎

(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/ in

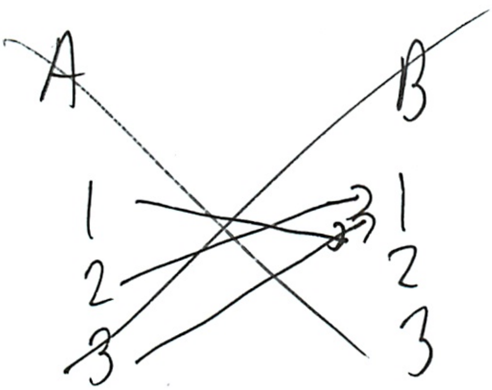
9

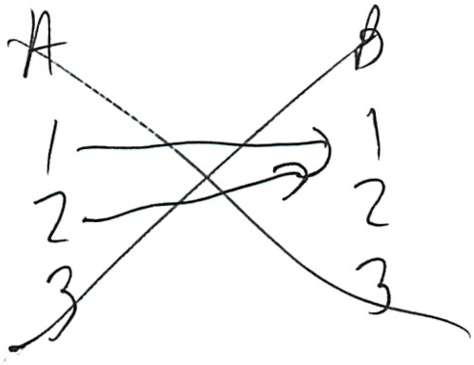
4. No more than 1 arrow at

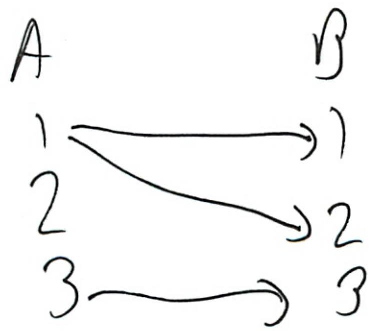
$$A \xrightarrow[\text{maps}]{\text{all of}} B \xrightarrow[\text{maps}]{\text{all of}} C$$

Could draw diagrams

b




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 that[1]

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

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

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

■



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

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

**Problem 2.**
Subset take-away[2] 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 $n = 4$. ■

---

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

[3] David 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:

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

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 is 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.** $A$ surj $B$ iff there is a surjective **function** from $A$ to $B$.

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

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

**(a)** Prove that if $A$ surj $B$ and $B$ surj $C$, then $A$ surj $C$.

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

Like how is that a proof

**(b)** Explain why $A$ surj $B$ iff $B$ inj $A$.

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

**(c)** Conclude from (a) and (b) that if $A$ inj $B$ and $B$ inj $C$, then $A$ inj $C$.

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

# 6.042 Tutor 3

2/15

## 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

$A$ = set

$P(A)$ = power set ~ set of all subsets

6

②

in book

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

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

$\{0,\{0\}\}, \{0\}, \{\{0\}\}, 0$ ✓

weird

How many elements

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

(~~this~~ these are the problems I like)

~~8 +~~

- Think for less elements

2 | ~~B~~ 4 = 2+1+1

3 | ~~B~~ $\{1\}\{2\}\{3\}$

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

$\{1,2,3\}$

$\emptyset$

3+3+1+1 = 8

Order does not matter

(3)

4 {1} . . . 4 n

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

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | { \ | {1, 2} | {1, 3} | {1, 4} |
| 2 | ~~{1, 2}~~ | \ | {2, 3} | {2, 4} |
| 3 | ~~{1, 3}~~ | ~~{2, 3}~~ | \ | {3, 4} |
| 4 | ~~{1, 4}~~ | ~~{2, 4}~~ | ~~{3, 4}~~ | \ |

6

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

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

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

{1, 2, 3, 4} 1

∅ 1

1

1

how would you do a table here

# of elements expand

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

(I like these type of problems)

(4) TP.3.3

## Part 1 Divisability Images

V = relation integers 7 → 15

codomain $\mathbb{Z}$ 2 → 30

mVn → 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 just the results :

| m | n |
|---|---|
| 7 | 2 |
| 8 | 3 |
| 9 | 4 |
| ⋮ | 5 |
| | ⋮ |
| 15 | 30 |

$15 \xrightarrow[\text{of}]{\text{is a divisor}} 30$

10

14

So all the divisors of these values from 2 → 30

(5)

And "$\underline{or}$" so if one is a divisor of one or the other
— or must be both?

~~2 5 10~~
~~2 14~~ ⊗

Z ⊗

10, 20, 30, 14, 28
: So I did divisable in ~~w~~rong way

2. Inverse — so set of m that are in above image
So all the numbers which are divisable by the above #
— so all the ~~ev~~ evens essentially

~~8 10 12 14~~ ⊗

7 10 14 : Items that are divisable above

## Part 2 Total Relations

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

$R(A) = B$ ✓ ✗ : So notes wrong?

$R^{-1}(B) = A$ ✗✓ ✓

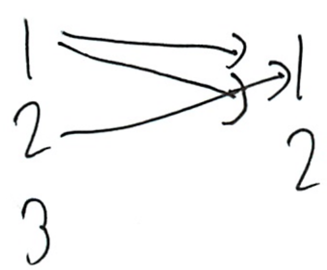
every el of A goes to B

6

# Part 3 Surjective Relation

Relation is surjective iff

- every el of B is mapped to at least once



$R^{-1}(A) = B$ ✓ ✗

↑ how do inverse of reverse

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

So change part 2

$R(B) = A$ ✓ ✗ goes back

$R^{-1}(B) = A$ ×

$R(A) = B$ × ✓ only true

still don't get

↑ not a function

but what does it mean to be valid?

Reverse the direction of arrows

But what is $R(B)$

7

## TP. 3.4 ~~Inverse~~ Relations

Inverse of $R^{-1}$ of $R: A \to B$ is $B \to A$

as defined by $b R^{-1} a \Leftrightarrow a R b$

Like reversing arrow

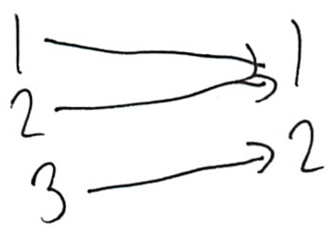
$R$ is total iff $R^{-1}$ is a surjection

↑ exactly 1 arrow out of each

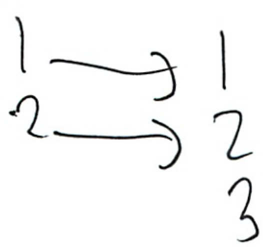
↑ every $\geq 1$ arrow in

¿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 ✗

✗ - never true?

(8)

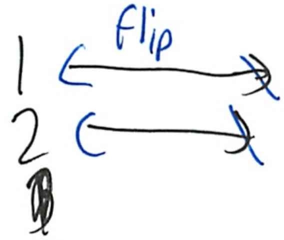
injection ✓

↳ ever arror mapped at least once

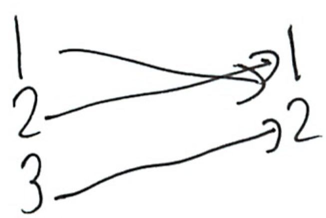
again size!

Or does image mean a certain something

Or are we looking at A?

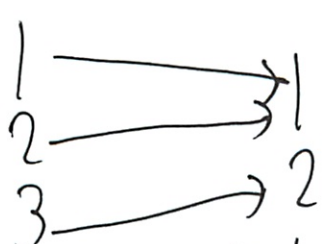



? look here injection



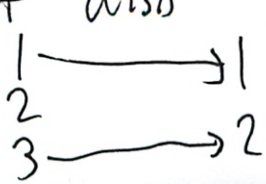
but then this wald be injection as well??

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



>1 arrow in

but also



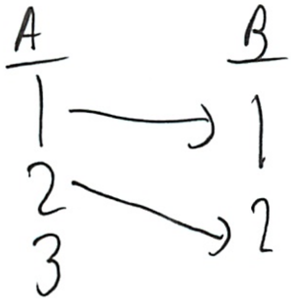
So none? ✗

~~total~~ total ✓ I don't get it!

⑨

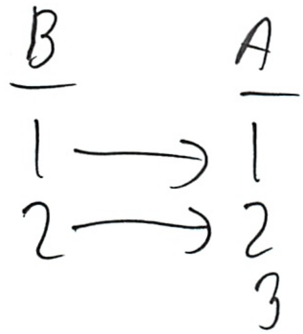
c) $R$ is an injection iff $R^{-1}$ is

↳ at most one in




but none again?

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




total

function

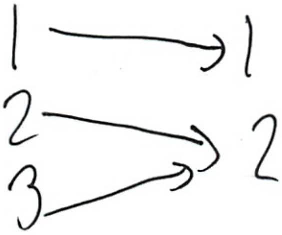
but why is it not total?

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

(10)

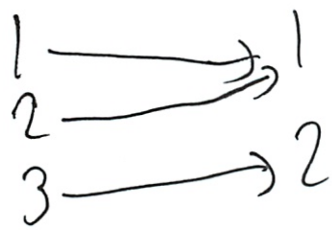
Let me think more about this

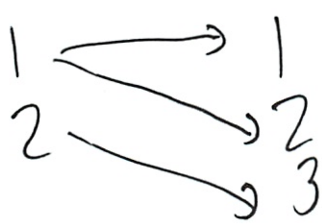
a) function



injection makes sense now

b) surjection





So not total ← is total

but function

but how since at least one

Oh total can be $\geq 1$ arrow out

↳ not nessarly a function!

c makes sense now

(11)

# TP 3.5 In-, Sur-, Bijections

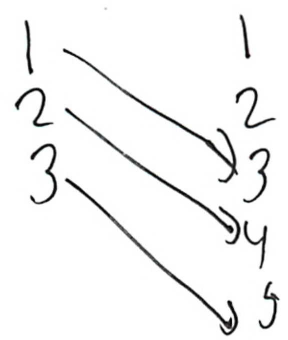
B = Bijection

S = sur, but not bi

I = in but not bi

N = neither inj + sur

a) $x+2$




I since at most 1 ✗

N ✗

S ✗

B ✓ Last try

Oh can be # < 1

Its $\mathbb{R}$

So $0 \to 2$

$-1 \to 1$

(12)

$2x$

| | |
|---|---|
| $-2$ | $-4$ |
| $-1$ | $-2$ |
| $0$ | $0$ |
| $1$ | $2$ |
| $2$ | $4$ |

~~B~~ ~~4~~ ~~3.5~~ 1.5

.75 $\longrightarrow$

so works

but only for rationals ? $\mathbb{Q}$

~~R~~ I (X) ~~xxxx~~

R (✓)

C So you can always /2 to get back

B. $x^2$

Well here neg don't count

| | |
|---|---|
| $-1$ | $-1$ |
| $0$ | $0$ |
| $1$ | $1$ |
| $2$ | $2$ |
| | $4$ |
| $.5 \longrightarrow$ | $.25$ |

but no — Do not S

Can you get 3

$2\sqrt{3} \to$ yeah

(13)

And stuff can be mapped to multiple times

not S

not I    since $(-1)^2 = 1^2$

So not B

N

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) $x \sin x$

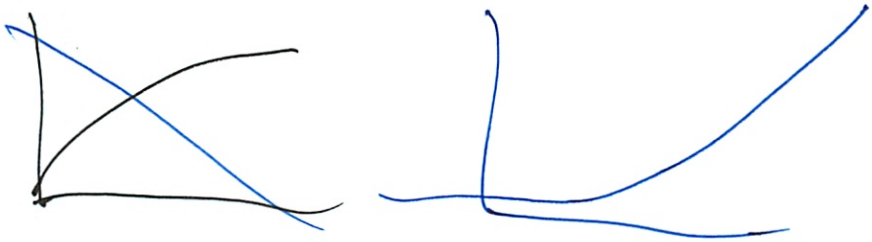
Now can scale this to whatever

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 → I

That was kinda fun

TP 3.6

# 6.042 Cheat Sheet 1

2/16

$::=$ defined to be
$\wedge$ = AND
$\vee$ = OR
$\rightarrow$ = implies
$\neg$ = not
$\leftrightarrow$ = iff, equivilant
$\oplus$ - XOR
$\exists$ = Exists
$\forall$ = for all
$\in$ is a member of
$\subseteq$ subset
$\subset$ subset proper
$P(A)$ power set $2^n$ items
$\mathbb{N}$ = non neg
$\mathbb{Z}$ = int
$\mathbb{Z}^+$ = pos int
$\mathbb{Z}^-$ = neg int
$\mathbb{Q}$ = rational $\mathbb{R}$ = Real
$\mathbb{C}$ = complex
$\lambda$ = empty string

A AND B $\leftrightarrow$ B AND A commutativity
(A AND B) AND C $\leftrightarrow$ A AND (B AND C) assocativity
T AND A $\leftrightarrow$ A identity
F AND A $\leftrightarrow$ F zero
A AND A $\leftrightarrow$ A idempotence
A AND $\bar{A}$ $\leftrightarrow$ F contridictions
Not $(\bar{A})$ $\leftrightarrow$ A double negation
A or $\bar{A}$ $\leftrightarrow$ T validity
A AND (B OR C) $\leftrightarrow$ (A AND B) or (A AND C) distributive
NOT (A AND B) $\leftrightarrow$ $\bar{A}$ or $\bar{B}$ Demorgan AND
NOT (A or B) $\leftrightarrow$ $\bar{A}$ AND $\bar{B}$ Demorgan or

<u>function</u> A $\geq 1$ arrow out
<u>total</u> A $\leq 1$ arrow out
<u>function + total</u> A = 1 out
<u>surjective</u> B $\leq 1$ in
<u>injective</u> B $\geq 1$ in
<u>bijective</u> A = 1 and B = 1 in/out

(12)

Massachusetts Institute of Technology
6.042J/18.062J, Spring '11: Mathematics for Computer Science
Prof. Albert R Meyer revised Tuesday 15th February, 2011, 16:11

# Mini-Quiz Feb. 16 #1

**Your name:** Michael Plasmeier

**Circle the name of your TA:**

Ali Nick Oscar Oshani

- This quiz is **closed book**. Total time is 25 minutes.
- Write your solutions in the space provided. If you need more space, write on the back of the sheet containing the problem. Please keep your entire answer to a problem on that problem's page.
- GOOD LUCK!

20 min - 1st

**DO NOT WRITE BELOW THIS LINE**

| Problem | Points | Grade | Grader |
|---|---|---|---|
| 1 | 5 | 2 | OS |
| 2 | 5 | 5 | OM |
| 3 | 5 | 2 | OM |
| 4 | 5 | 4 | OS |
| Total | 20 | 13 | OS |

**Problem 1 (5 points).**
Prove that $\log_9 12$ is irrational. *Hint:* Proof by contradiction.

Seems like you have not proved this by WOP!

Proof by WOP. Assume that you can write $\log_9 12$ as the quotent of two integers $\left(\frac{m}{n}\right)$ This quotient shold be reduced to its lowest form so it can not be redcued again.

However

$$\log_9 12 = \frac{m}{n}$$ 9 to the power of x

$$9^{\log_9 12} = 9^{m/n}$$

$$12 = 9^{m/n}$$

$\sqrt[\frac{n}{m}]{\phantom{x}}$ $\sqrt[\frac{n}{m}]{\phantom{x}}$

$$9 = \sqrt[n/m]{12}$$

$$9n = 12m$$ – ? really ? is this possible ?

$$n = 4m$$

$12^n = 9^m$

LHS is even, but $9^m$ is odd. This is a contradiction, ∴ it proves that $\log_9 12$ is irrational.

There can never be $\frac{m}{n}$ written in lowest form because m is a factor of n. Thus $\log_9 12$ is irrational

should received P-Set 1

**Problem 2 (5 points).**
Show that there are exactly two truth assignments for the variables P,Q,R,S that satisfy the following formula:

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

*Hint:* A truth table will do the job, but it will have a bunch of rows. A proof by cases can be quicker; if you do use cases, be sure each one is clearly specified.

| P | Q | R | S | $\overline{P}$ or Q | $\overline{Q}$ or R | $\overline{R}$ or S | $\overline{S}$ or P | |
|---|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | T | T | T |
| T | T | T | F | T | T | F | T | F |
| T | T | F | T | T | F | T | T | F |
| T | T | F | F | T | F | T | T | F |
| T | F | T | T | F | T | T | T | F |
| T | F | T | F | F | T | F | T | F |
| T | F | F | T | F | T | T | T | F |
| T | F | F | F | F | T | T | T | F |
| F | T | T | T | T | T | T | F | F |
| F | T | T | F | T | T | F | T | F |
| F | T | F | T | T | F | T | F | F |
| F | T | F | F | T | F | T | T | F |
| F | F | T | T | T | T | T | F | F |
| F | F | T | F | T | T | F | T | F |
| F | F | F | T | T | T | T | F | F |
| F | F | F | F | T | T | T | T | T |

Only 2 rows are true

**Problem 3 (5 points).**
The (flawed) proof below uses the Well Ordering Principle to prove that every amount of postage that can be paid exactly, using only 10 cent and 15 cent stamps, is divisible by 5. Let $S(n)$ mean that exactly $n$ cents postage can be paid using only 10 and 15 cent stamps. Then the proof shows that

other way around

$$S(n) \text{ IMPLIES } 5 \mid n, \quad \text{for all nonnegative integers } n. \qquad (*)$$

Fill in the missing portions (indicated by "...") of the following proof of (*), and at the final line point out where the error in the proof is.

Let $C$ be the set of *counterexamples* to (*), namely

$$C ::= \{n \mid S(n) \text{ and } \text{NOT}(5 \mid n)\}$$

Assume for the purpose of obtaining a contradiction that $C$ is nonempty. Then by the WOP, there is a smallest number, $m \in C$. Then $S(m-10)$ or $S(m-15)$ must hold, because the $m$ cents postage is made from 10 and 15 cent stamps, so we remove one.

So suppose $S(m-10)$ holds. Then $5 \mid (m-10)$, because...

X You can remove 10 cents and it would not change if it's divisable by 5 - even when removing 10 cents since $\frac{10}{5}$ is T

But if $5 \mid (m-10)$, then $5 \mid m$, because...

Again, you can always divide by 5 - never having a smallest counterexample since 10/5 is T

contradicting the fact that $m$ is a counterexample.

Next suppose $S(m-15)$ holds. Then the proof for $m-10$ carries over directly for $m-15$ to yield a contradiction in this case as well. Since we get a contradiction in both cases, we conclude that $C$ must be empty. That is, there are no counterexamples to (*), which proves that (*) holds.

What was wrong/missing in the argument? Your answer should fit in the line below.

−1 m must be larger than a certain value (10)

larger than 0.

Never really got mechanics of this

**Problem 4 (5 points).**

The following predicate logic formula is invalid:

$$\forall x, \exists y. P(x, y) \longrightarrow \exists y, \forall x. P(x, y)$$

Which of the following are counter models for the implication above?

✗ 1. X The predicate $P(x, y) =$ '$yx = 1$' where the domain of discourse is $\mathbb{Q}$.

not always an X

✓ 2. X The predicate $P(x, y) =$ '$y < x$' where the domain of discourse is $\mathbb{R}$.

not all x for that y

✓ 3. X The predicate $P(x, y) =$ '$yx = 2$' where the domain of discourse is $\mathbb{R}$ without 0.

✓ 4. ______ The predicate $P(x, y) =$ '$yxy = x$' where the domain of discourse is the set of all binary strings, including the empty string.

Works y is empty

Fair quiz

# Solutions to Mini-Quiz Feb. 16

**Problem 1 (5 points).**
Prove that $\log_9 12$ is irrational. *Hint:* Proof by contradiction.

**Solution.** *Proof.* Suppose to the contrary that $\log_9 12 = m/n$ for some integers $m$ and $n$. Since $\log_9 12$ is positive, we may assume that $m$ and $n$ are also positive. So we have

$$\begin{aligned} \log_9 12 &= m/n \\ 9^{\log_9 12} &= 9^{m/n} \\ 12 &= \left(9^m\right)^{1/n} \\ 12^n &= 9^m \qquad (1) \end{aligned}$$

But this is impossible, since left hand side of (1) is even, but, because $m$ is positive, the right hand side is odd.

This contradiction implies that $\log_9 12$ must be irrational. ■

**Problem 2 (5 points).**
Show that there are exactly two truth assignments for the variables P,Q,R,S that satisfy the following formula:

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

*Hint:* A truth table will do the job, but it will have a bunch of rows. A proof by cases can be quicker; if you do use cases, be sure each one is clearly specified.

**Solution.** You can deduce the only two possibilities by cases:

If $P$ is false, then in order to have any chance of satisfying clause 4, $S$ must be false. Similarly, if $S$ is false, then in order to satisfy clause 3, $R$ must be false. And similarly, $Q$ must be false. On the other hand, if $P$ is true, then $Q$ must be true to make clause 1 true and have any chances of making the overall expression true. Similarly, If $Q$ is true, then $R$ must be true and if $R$ is true then $S$ is true.

Those arguments prove there are at most 2 cases, but you need to show the assignments we are left with actually satisfy the formula. This can be easily done, by plugging the values into the formula:

If all variables are set to true, then since clause 1 has $Q$ clause 2 has $R$, clause 3 has $S$, and clause 4 has $P$, then every clause is satisfied, and the full AND is satisfied. If all are false, then since clause 1 has $\overline{P}$, clause 2 has $\overline{Q}$ , clause 3 has $\overline{R}$ and clause 4 has $\overline{S}$, then again every clause is satisfied and the overall proposition is satisfied. So both of those satisfy the proposition.

■

**Problem 3 (5 points).**
The (flawed) proof below uses the Well Ordering Principle to prove that every amount of postage that can be paid exactly, using only 10 cent and 15 cent stamps, is divisible by 5. Let $S(n)$ mean that exactly $n$ cents postage can be paid using only 10 and 15 cent stamps. Then the proof shows that

$$S(n) \text{ IMPLIES } 5 \mid n, \quad \text{for all nonnegative integers } n. \tag{*}$$

Fill in the missing portions (indicated by "...") of the following proof of (*), and at the final line point out where the error in the proof is.

Let $C$ be the set of *counterexamples* to (*), namely

$$C ::= \{n \mid S(n) \text{ and NOT}(5 \mid n)\}$$

Assume for the purpose of obtaining a contradiction that $C$ is nonempty. Then by the WOP, there is a smallest number, $m \in C$. Then $S(m-10)$ or $S(m-15)$ must hold, because the $m$ cents postage is made from 10 and 15 cent stamps, so we remove one.

So suppose $S(m-10)$ holds. Then $5 \mid (m-10)$, because...

**Solution.** ...if $\text{NOT}(5 \mid (m-10))$, then $m-10$ would be a counterexample smaller than $m$, contradicting the minimality of $m$. ■

But if $5 \mid (m-10)$, then $5 \mid m$, because...

**Solution.** ...$5 \mid (m-10)$ and $5 \mid 10$, so $5 \mid (m-10+10)$. ■

contradicting the fact that $m$ is a counterexample.

Next suppose $S(m-15)$ holds. Then the proof for $m-10$ carries over directly for $m-15$ to yield a contradiction in this case as well. Since we get a contradiction in both cases, we conclude that $C$ must be empty. That is, there are no counterexamples to (*), which proves that (*) holds.

What was wrong/missing in the argument? Your answer should fit in the line below.

**Solution.** We didn't check $m > 0$, if $m = 0$ neither $S(m-10)$ nor $S(m-15)$ hold. ■

**Problem 4 (5 points).**

The following predicate logic formula is invalid:

$$\forall x, \exists y. P(x,y) \longrightarrow \exists y, \forall x. P(x,y)$$

Which of the following are counter models for the implication above?

1. The predicate $P(x,y) =$ '$yx = 1$' where the domain of discourse is $\mathbb{Q}$.

2. The predicate $P(x,y) =$ '$y < x$' where the domain of discourse is $\mathbb{R}$.

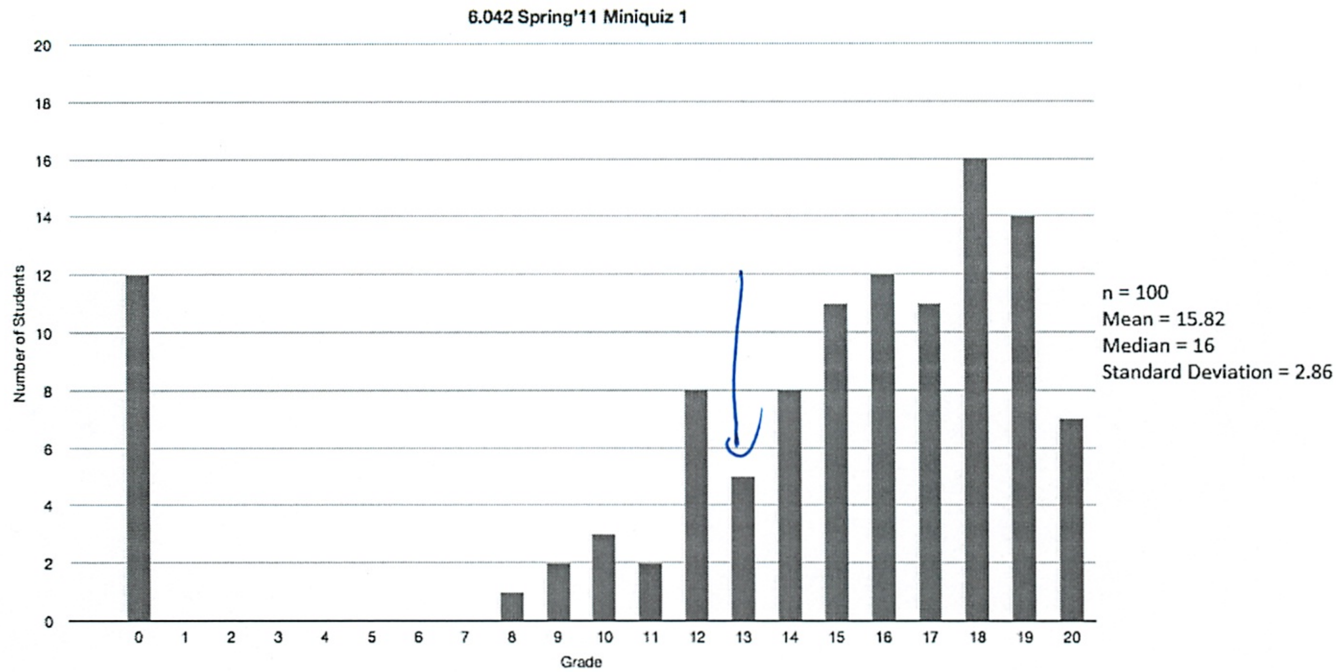
3. The predicate $P(x,y) =$ '$yx = 2$' where the domain of discourse is $\mathbb{R}$ without 0.

4. The predicate $P(x,y) =$ '$yxy = x$' where the domain of discourse is the set of all binary strings, including the empty string.

**Solution.**

1. In the rationals, 0 has no inverse. Hence the hypothesis is false, since not all rationals have inverses. An implication with a false hypothesis is automatically true, so this is not a countermodel.
2. COUNTERMODEL. For every real number $x$, there exists a real number $y$ which is strictly less than $x$. So while the antecedent of the implication is true, the consequence is not since there is no minimum element for the partial order, the strictly less than relation, $<$, on $\mathbb{R}$.
3. COUNTERMODEL. in this case the hypothesis is true, but the conclusion is not: its not possible to find a single number that will do this.
4. In the set of binary strings, both sides of the implication are true if we let $y = \lambda$, the empty string.

■




Bit lower than my usual position