Problem 6 [Hard]**: Tarski and First-Order Logic**

In figure 1 we have a Tarski world, the domains for all variables consists of the objects (individual shapes) in the Tarski world. Objects are either circles or triangles. Every object has a shading, either fully shaded or clear (no shading). Finally, an object can be above some other object. We can define these properties as predicates:

- shaded(x) = x is shaded
- triangle(x) = x is a triangle
- circle(x) = x is a circle
- above(x, y) = x is on a row strictly above y

$r_{k+1} = 1 + r_k$ ✗

strict on same colum ✓ ?

strict on row higher ✓ ?

Using these predicates and our logical symbols, we can write statements about this Tarski World into formal logic. For instance, we can translate the statement

"Every shape is a circle or a triangle"

into

$$\forall x,\ \text{circle}(x) \vee \text{triangle}(x)$$

i. (1 point each) State whether the following statements are true or false in this Tarski world.

- Every circle is shaded.
- There is a triangle that is above a circle that is not shaded.

predicates & quantifiers

$\forall x$ predicate$(x) \implies \ldots$

$\forall x$ predicate$(x) \vee$ pred$_2(x)$

$\exists x$ pred$_1(x) \wedge$ pred$_2(x)$

ii. (2 points each) Write the following statements using formal logic

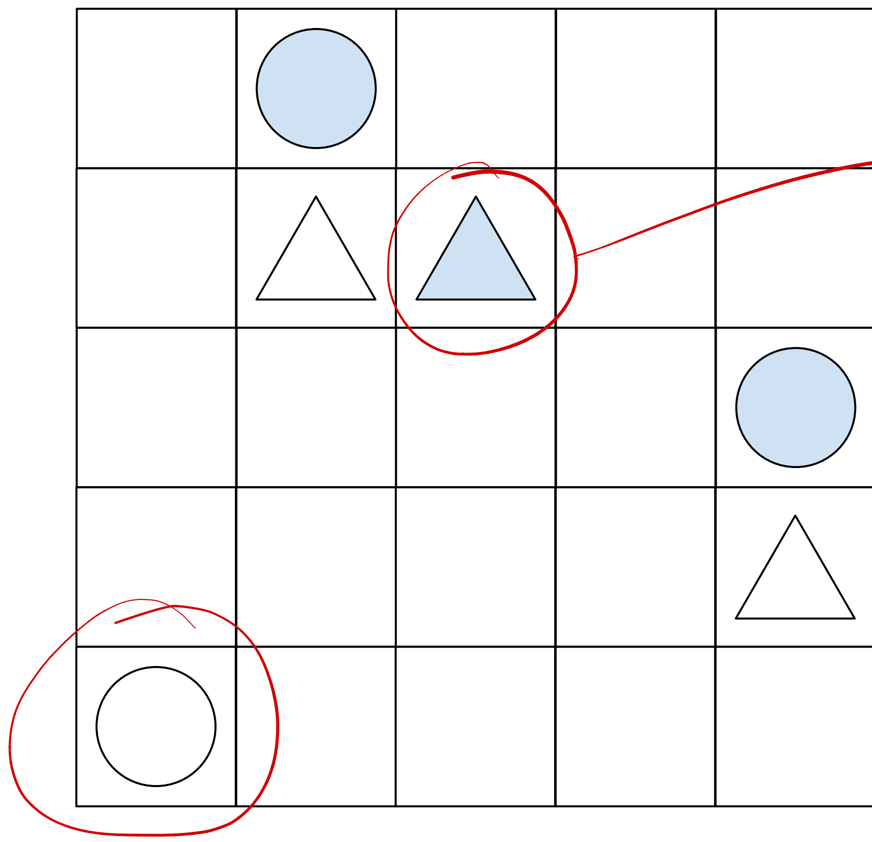
- All triangles are shaded.
- There is a circle that is both shaded and above every triangle.

iii. (2 points each) Negate the following statements in formal logic. Distribute all negations in your solution.

- $\forall x,\ \text{circle}(x) \wedge \neg\, \text{shaded}(x)$
- $\forall x\ \exists y,\ \text{shaded}(x) \implies ((\text{triangle}(y) \wedge \text{shaded}(y)) \wedge \neg\, \text{above}(y, x))$

T if "strict" = any row strict above A

F if "strict" = same column. B



Is this △ above ○ in bottom L corner?

• do they have to be on same column to count as "above" predicate

Figure 1: Figure for problem 4. A Tarski World, a tool for understanding logical statements invented by Jon Barwise and John Etchemendy, named after Alfred Tarski

Common sense
if A then B
if B then C } ⇒ starting at a
$a \to b \Rightarrow c$ (implic. chain)
I get c

analogy
Bos → DEN
DEN → LA } ⇒ Bos → LA

★ problems: no credit, no deadline, no formal grading, and possibly no solutions. If you work on these and need help, let Virgil know by email.

rewrite $a \Rightarrow b$ as $\neg a \lor b$

$[(\neg a \lor b) \land (\neg b \lor c)] \Rightarrow [\neg a \lor c]$

start with this premise

premise $\Rightarrow \dots \Rightarrow \dots \Rightarrow \boxed{a \Rightarrow c}$ conclusion

Problem 7 (no credit) Implication is transitive

If a, b, c are boolean variables, show that $(a \Rightarrow b) \land (b \Rightarrow c) \Rightarrow (a \Rightarrow c)$.
Do this both using a truth table (easy), and by using boolean algebra derivation laws (not so easy)

Problem 8 ★ (no credit) Josephine's Problem

In Josephine's Kingdom every woman has to pass a logic exam before being allowed to marry. Every married woman knows about the fidelity of every man in the Kingdom except for her own husband, and etiquette demands that no woman should be told about the fidelity of her husband. Also, a gunshot fired in any house in the Kingdom will be heard in any other house. Queen Josephine announced that at least one unfaithful man had been discovered in the Kingdom, and that any woman knowing her husband to be unfaithful was required to shoot him at midnight following the day after she discovered his infidelity. How did the wives manage this?

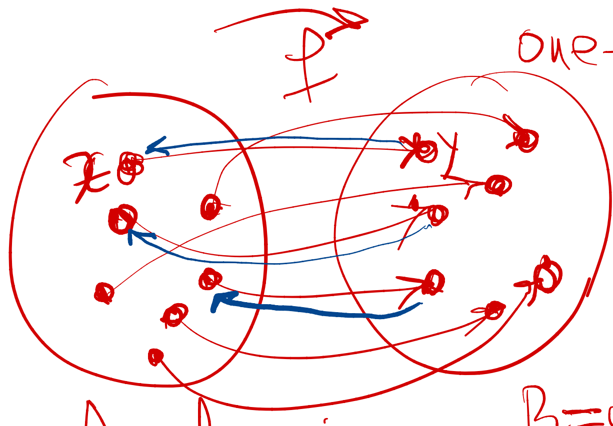
Problem 9 ★★★ (no credit) 4-hemisphere cover

A sphere is covered with some number of "caps" which are hemispheres. Prove that it is possible to choose four hemispheres, and remove all others, while still keeping the sphere covered.

Problem 10 ★★★ (no credit) 4k+1 primes characterization

Fall 2018 2 student solved it in 04/2019

Prove that a prime number p can be written as the sum of two squares $p = a^2 + b^2$ if and only if $p = 1 \pmod 4$.
For example $p = 13 = 4 * 3 + 1$ is such number, therefore is the sum of two squares $13 = 2^2 + 3^2$. But the prime $p = 23 = 4 * 5 + 3 = 3 \bmod 4$ is not, so it cannot be writen as sum of two sqaured integers.



one-to-one map

$f(x)=y$

$x\in A$ $y\in B$

A = domain

B = output/value

f^{-1}

one-to-one

• injectivity: no two x-s give same y

$x_1\neq x_2 \Rightarrow f(x_1)\neq f(x_2)$

• surjectivity: every $\forall y\in B$ is an output

$\exists x \in A, f(x)=y$

EC: Counting with one-to-one functions between sets

very important in math

very simple

A function $f : A \to B$ is "one-to-one" or "bijective" if it has two properties:

•injective: different inputs result in different outputs:
$\forall x \neq y \in A \Rightarrow f(x) \neq f(y)$

•surjective: covers the entire destination set:
$\forall z \in B, \exists x \in A, f(x) = z$

$f(x)=x^2+x+11$

$f(4)=4^2+4+11=31$

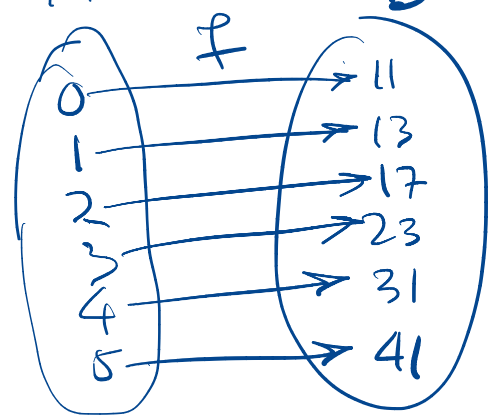
A one-to-one function guarantees that A and B have the same number of elements (sometimes infinite), so if we know the size of A it gives us the size of B or viceversa.

11, 13, 17, 23, 31, 41

EXAMPLE $A = \{0, 1, 2, 3, 4, 5\}$; $B = \{x \text{ prime}; 10 < x < 43; x \notin \{19, 29, 37\}\}$ $f : A \to B$, $f(x) = x^2 + x + 11$ is a bijection (verify that). Then the size of right side set, $|B|$, is the same as $|A| = 6$.

th: if $f: A\to B$ one to one

theory: $f^{-1}: B\to A$ one to one



For the following particular sets A, B show a one-to-one function from A to B, and conclude the size of B. You are asked for a bijective function f written a math expression (like $f(x) = 2x - 1$), not an enumeration of (input,output) pairs.

$B=\{7,14,...70\}$

$|A|=6$ $|B|=6$

Theorem $|A|=|B| \Leftrightarrow \exists$ pairing $\Leftrightarrow$ one-to-one map

$f: A\to B$

$f(x)=7x$

$1\to 7$

$2\to 14$

$\vdots$

$10\to 70$

EC 1 : $A = \{1, 2, 3..., 10\}$; $B = \{x \in N; 2 \le x \le 72; 7 \mid x\}$

multiples of 7 between 2 and 72

EC 2. $A = \mathbb{Z}_{77}$ and $B = \mathbb{Z}_7 \times \mathbb{Z}_{11}$

" if $\exists f: A\to B$ one to one, then $|A|=|B|$ "

• very important as counting technique

$\mathbb{Z}_7=\{$reminders when divide by 7$\}$
$=\{0,1,2,...,6\}$ $|\mathbb{Z}_7|=7$

$\mathbb{Z}_{11}=\{0,1,2,...10\}$ $|\mathbb{Z}_{11}|=11$

$\mathbb{Z}_{77}=\{0,1,2,...76\}$ $|\mathbb{Z}_{77}|=77$

$A=\mathbb{Z}_{77}$

x

$0,1,2...76$

$||=77$

$f(x)=(x \bmod 7, x \bmod 11)$

$f=$ one to one map

pairs $\mathbb{Z}_7$ $\times$ (cartesian) $\mathbb{Z}_{11}=B$

(0,0) (1,0) (6,0)
(0,1) (1,1) (6,1)
(0,2)
...
(0,10) (1,10) (6,10)

$||=77$
$=7\cdot 11$

$x = 39$	$\rightarrow$	4	6
$x = 52$	$\rightarrow$	3	8
$x = 57$	$\leftarrow$	1 ($57 = 7\cdot 8 + 1$)	2 ($57 = 5\cdot 11 + 2$)
49	$\leftarrow$	0 ($49 = 7\cdot 7 + 0$)	5 ($49 = 4\cdot 11 + 5$)

EC5: X a set; $a \in X$

$A = \{S \subset X \mid a \in S\}$ $\quad B = \{S \subset X \mid a \notin S\}$

Example $X = \{0,1,2,3,4\}$ $a = 1$

A: include "1": $\{1\}$; $\{1,0\}$; $\{1,2\}$ $\{1,3\}$ $\{1,4\}$, $\{1,2,3\}$ $\{1,2,4\}$ ... $\{0,1,2,3,4\}$

B: not include "1": $\{0\}$ $\{2\}$ $\{3\}$ $\{4\}$ $\{0,2\}$, $\{0,3\}$ ... $\{2,4\}$ $\{0,2,3,4\}$

$T\cup\{1\} \xleftarrow{f^{-1}} T$

one-to-one map $f(S) = S \setminus \{1\}$

$\Rightarrow |A| = |B|$ equal in size $\quad A \cap B = \emptyset$ disjoint $\quad A \cup B = \mathcal{P}(X)$ union

EC 3. $A = \mathbb{Z}_{240}$ and $B = \mathbb{Z}_{12} \times \mathbb{Z}_{20}$

EC 4. A={reminders coprime with 60}
in other words $A = \{x \in \mathbb{N}; x < 60; gcd(x, 60) = 1\}$.
B={reminders coprime with 12} $\times$ {reminders coprime with 5}, or
$B = \{x \in \mathbb{N}; x < 12; gcd(x, 12) = 1\} \times \{x \in \mathbb{N}; x < 5; gcd(x, 5) = 1\}$.
Conclude that $\phi(60) = \phi(12)\phi(5)$ where ϕ is Euler's totient.

A, B subsets of $\mathcal{P}(X)$ $\Rightarrow |A| = \frac{\mathcal{P}(X)}{2} = |B|$

EC 5. Assume finite set X includes element a. Take A={all subsets of X including a} and B={all subsets of X not including a}

$\Rightarrow |A| = 2^{|X|}/2$

EC 6. Assume finite set X includes elements $a \neq b$. Take A={all subsets of X including a} and B={all subsets of X including b}. Hint: make sure you've got a bijection from A to B, as the most obvious function is not one!

$\mathbb{N} = \{0,1,2,3 \ldots\}$ $\quad \mathbb{Z} = \{0,1,2,\ldots ; -1,-2,\ldots\}$ $\quad \mathbb{Z} = \mathbb{N} \cup \{-1,-2,-3\ldots\}$

EC 7. $A = \mathbb{N}$ (naturals) and $B = \mathbb{Z}$ (integers). For the conclusion we call the size of natural numbers set the "countable infinite cardinal" N_0.

$\mathbb{Z}$ is countable (one-to-one map with $\mathbb{N}$)

"$\mathbb{Z}$ is bigger"? all elem in $\mathbb{N}$ + some extra

$f: \mathbb{N} \to \mathbb{Z}$ one-to-one map

$0 \to 0$
$1 \to -1$
$2 \to +1$
$3 \to -2$
$4 \to +2$
$\vdots$

rewrite:
$\mathbb{N}$: 0 1 2 3 4 5 6 7 8 9 10 ...
$\mathbb{Z}$: 0 -1 +1 -2 +2 -3 +3 -4 +4 -5 +5 ...

(see map) enumerate all $\mathbb{Z}$

EC 8 $A = \mathbb{Z}$ and B = { multiples of 5 } =$\{x \in Z; 5 \mid x\}$.

EC 9 :difficulty ★★. $A = \mathbb{N}$ and $B = \mathbb{Q}_+$ (non-negative rationals/fractions). The conclusion is that the set of positive rational numbers $\mathbb{Q}_+$ has the cardinality of N_0 as $\mathbb{N}$, i.e. $\mathbb{Q}_+$ is "countable". set of rationals is countable.

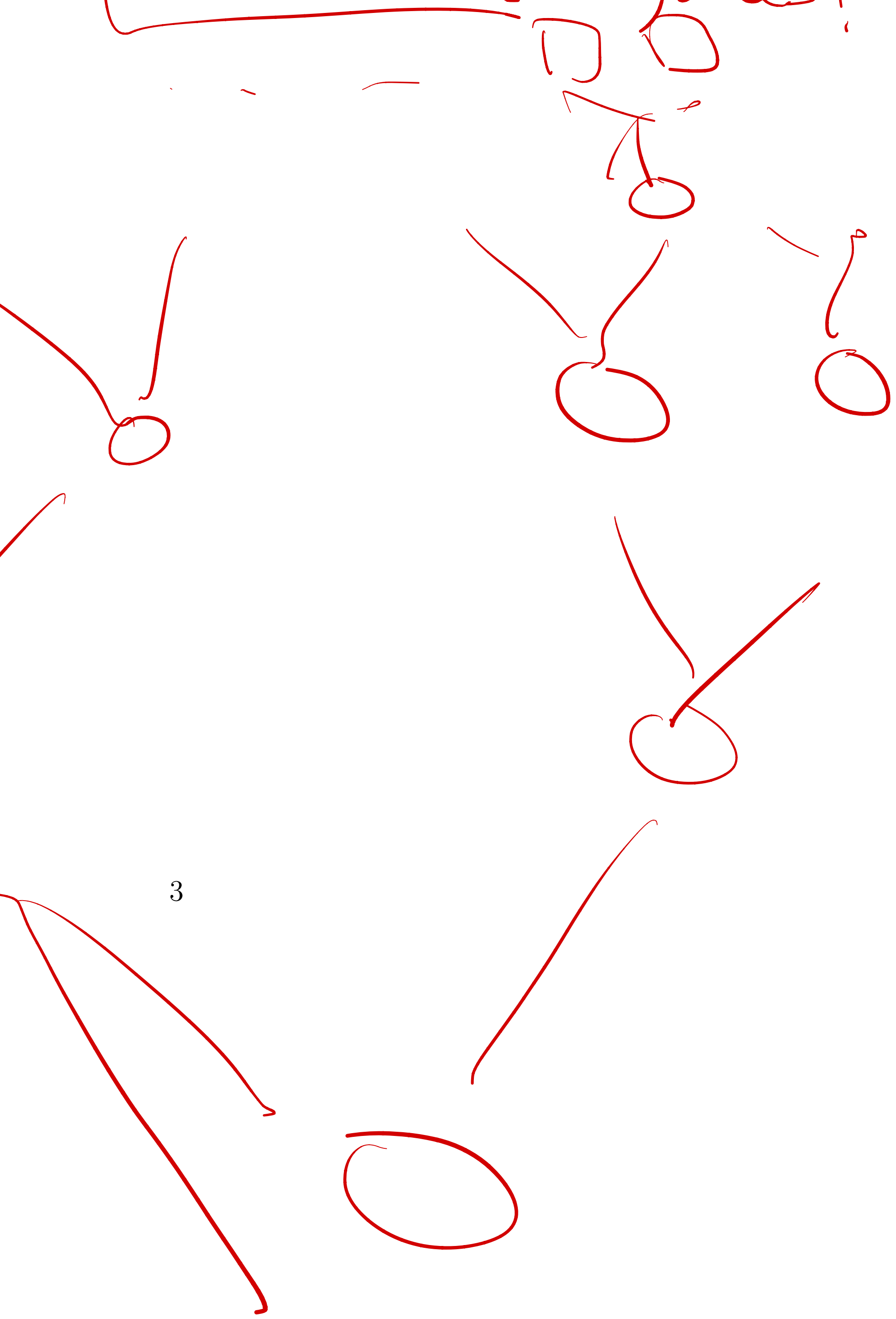
EC 10. EXTRA CREDIT, difficulty ★. $A = \mathbb{Q}^+$(positive rationals) and $B = \mathbb{Q}$ (all rationals/fractions). Using the previous results that $\mathbb{Q}_+$ is countable, and that $\mathbb{Z}$ is countable, show that $\mathbb{Q}$ "countable".

EC 11difficulty ★★. $A = \mathbb{N}$ and $B = \mathbb{R}$ (reals). Show that no bijection is possible, because any function $f : \mathbb{N} \to \mathbb{R}$ cannot cover the entire destination set $\mathbb{R}$, thus $\mathbb{R}$ has "more elements" than $\mathbb{N}$. They are both infinite, but the cardinality of $\mathbb{R}$ is bigger, certainly not "countable"!

EC 12difficulty ★★★. $A = 2^{\mathbb{N}}$ and $B = \mathbb{R}$. Here A is the powerset of $\mathbb{N}$. The function f you are looking for is a one-to-one between subsets of natural numbers (input) and real numbers (output).

loser out immediately

Cute: tournament knockout $\boxed{\text{64 teams}}$ how many games?



$32+16+\dots+1=63$

want to count