Week 6 - Friday

COMP 2230

Last time

- More set theory review
- Russell's Paradox

Questions?

Assignment 3

Logical warmup

- You have 15 bags
- How many marbles do you need so that you can have a different number of marbles in each bag?

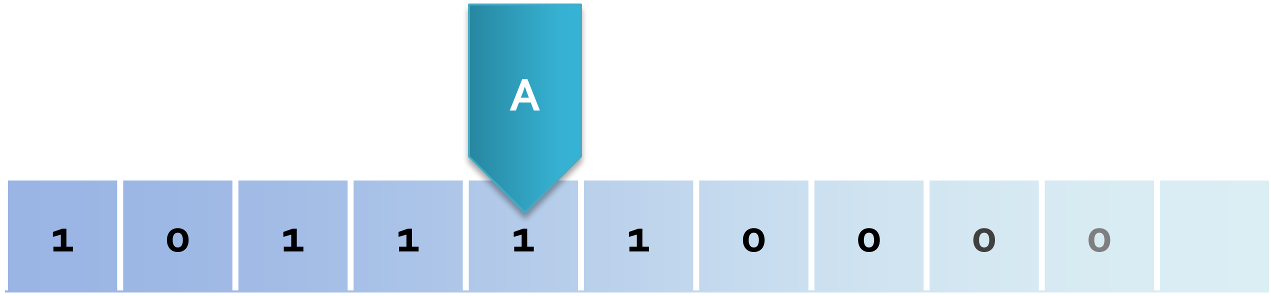
Halting Problem

Applying the idea again

- It turns out that the idea behind Russell's Paradox has practical implications
- It wasn't new, either
- Cantor had previously used a diagonal argument to show that there are more real numbers than rational numbers
- But, unexpectedly, Turing found an application of this idea for computing

Turing machine

- A Turing machine is a mathematical model for computation
- It consists of a head, an infinitely long tape, a set of possible states, and an alphabet of characters that can be written on the tape
- A list of rules saying what it should write and should it move left or right given the current symbol and state



Church-Turing thesis

- If an algorithm exists, a Turing machine can perform that algorithm
- In essence, a Turing machine is the most powerful model we have of computation
- Power, in this sense, means the ***ability*** to compute some function, **not** the ***speed*** associated with its computation

Halting problem

- Given a Turing machine and input x, does it reach the halt state?
- First, recognize that we can encode a Turing machine as input for another Turing machine
  - We just have to design a system to describe the rules, the states, etc.
- We want to design a Turing machine that can read another

Halting problem problems

- Imagine we have a Turing machine $H(m,x)$ that takes the description of another Turing machine m and its input x and returns 1 if m halts on input x and 0 otherwise
- Now, construct a machine $H'(m,x)$ that runs $H(m,x)$, but, if $H(m,x)$ gives 1, then $H'(m,x)$ infinitely loops, and if $H(m,x)$ gives 0, then then $H'(m,x)$ returns 1
- Let's say that d is the description of $H'(m,x)$
- What happens when you run $H'(d,d)$?

Halting problem conclusion

- Clearly, a Turing machine that solves the halting problem **can't** exist
- Essentially, the problem of deciding if a problem is computable is itself uncomputable
- Therefore, there are some problems (called **undecidable)** for which there is no algorithm
- Not an algorithm that will take a long time, but **no algorithm**
- If we find such a problem, we are stuck
- … unless someone can invent a more powerful model of computation

And it gets worse!

- Gödel used diagonalization again to prove that it is impossible to create a consistent set of axioms that can prove everything about the set of natural numbers
- As a consequence, you can create a system that is complete but not consistent
- Or you can create a system that is consistent but not complete
- Either way, there are principles in math in general that are true but impossible to prove, at least with any given system
- You might as well give up on math now

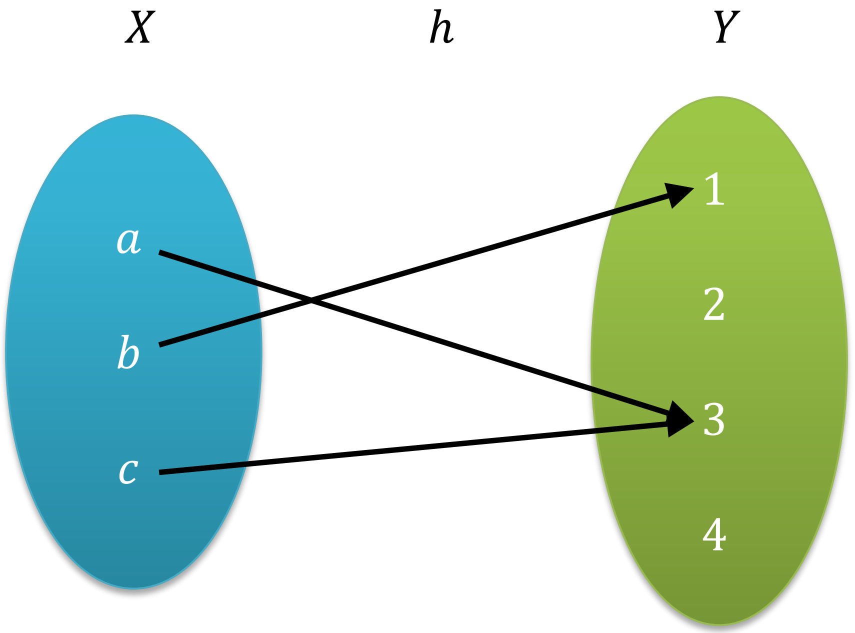
Cardinality

Cardinality

- **Cardinality** gives the number of things in a set
- Cardinality is:
  - **Reflexive:** A has the same cardinality as A
  - **Symmetric:** If A has the same cardinality as B, B has the same cardinality as A
  - **Transitive:** If A has the same cardinality as B, and B has the same cardinality as C, A has the same cardinality as C
- For finite sets, we could just count the things to determine if two sets have the same cardinality

One-to-one functions

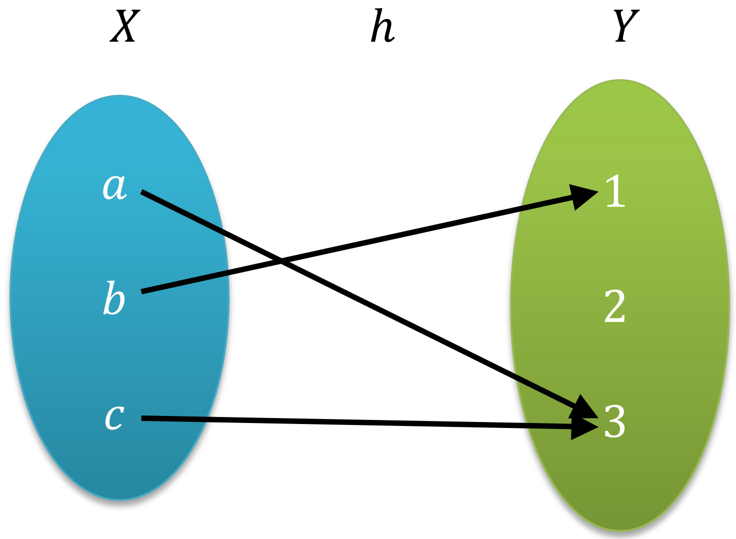
- Let F be a function from X to Y
- F is **one-to-one** (or **injective**) if and only if:
  - If $F(x_1) = F(x_2)$ then $x_1 = x_2$
- Is $f(x) = x^2$ from $\mathbb{Z}$ to $\mathbb{Z}$ one-to-one?
- Is $f(x) = x^2$ from $\mathbb{Z}^+$ to $\mathbb{Z}$ one-to-one?
- Is $h(x)$ one-to-one?



Onto functions

- Let F be a function from X to Y
- F is **onto** (or **surjective**) if and only if:
  - $\forall y \in Y, \exists x \in X$ such that $F(x) = y$

- Is $f(x) = x^2$ from $\mathbb{Z}$ to $\mathbb{Z}$ onto?
- Is $f(x) = x^2$ from $\mathbb{R}^+$ to $\mathbb{R}^+$ onto?
- Is $h(x)$ onto?



Bijective functions

- A **bijective** function $F\colon\ X\ \rightarrow\ Y$ is both:
  - One-to-one (injective)
  - Onto (bijective)

- Every element in X is mapped to exactly one element in Y and vice versa
- Such functions have inverses

Cardinality for infinite sets

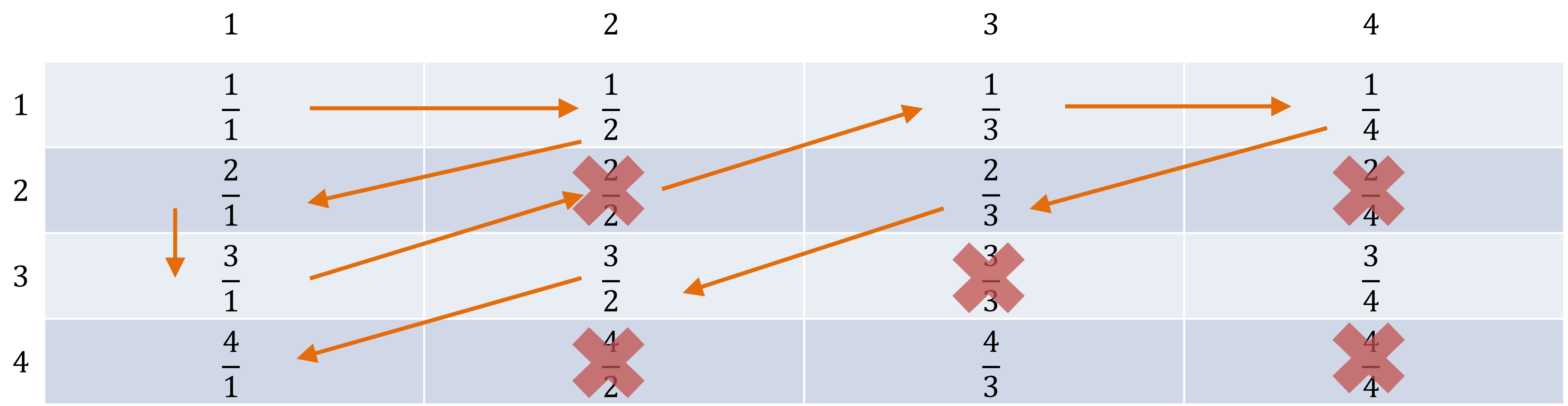
- Because we can't just count the number of things in infinite sets, we need a more general definition
- For any sets A and B, A has the same cardinality as B iff there is a bijective mapping A to B
- Thus, for any element in A, it corresponds to exactly one element in B, and everything in B has exactly one corresponding element in A

Cardinality example

- Show that the set of positive integers has the same cardinality as the set of all integers
- **Hint:** Create a bijective function from all integers to positive integers
- **Hint 2:** Map the positive integers to even integers and the negative integers to odd integers

Countability

- A set is called **countably infinite** if it has the same cardinality as $\mathbb{Z}^+$
- You have just shown that $\mathbb{Z}$ is countable
- It turns out that (positive) rational numbers are countable too, because we can construct a table of their values and move diagonally across it, numbering values, skipping numbers that have been listed already



	1	2	3	4
1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$
2	$\frac{2}{1}$	$\cancel{\frac{2}{2}}$	$\frac{2}{3}$	$\cancel{\frac{2}{4}}$
3	$\frac{3}{1}$	$\frac{3}{2}$	$\cancel{\frac{3}{3}}$	$\frac{3}{4}$
4	$\frac{4}{1}$	$\cancel{\frac{4}{2}}$	$\frac{4}{3}$	$\cancel{\frac{4}{4}}$

Uncountability

- So if the number of integers is the same as the number of rational numbers, that must also be the same as the number of real numbers, right?
- **Wrong.**
- There are **a lot** more real numbers
- The number of real numbers is called uncountable
- It's a larger infinity than the number of integers
- But it's not the largest infinity …
  - There is no largest infinity

Proving that there are more real numbers

- First, let's think about just the real numbers between 0 and 1 (not counting 1)
- Let's just put them in some list, in totally random order
- As long as we can make a numbered list, we can make a bijection with positive integers

Order	Number
1	0.58506706117215100 ...
2	0.30188097640659700 ...
3	0.05925831116503750 ...
4	0.09291012351774230 ...
5	0.79408644654174900 ...
6	0.09792740408760530 ...
7	0.72995316404639900 ...
8	0.26184376611267000 ...
9	0.42370325559805900 ...
...	...

Proof continued

- Let's create a number by going through the list and make a number by taking digit i from column i and adding 1 to it (rolling over to 0 if it's 9)
- For our list: 0.610098276 …
- Now, is our number in the list?
- No! It's impossible, since it's different from every single number in at least one place
- Thus, our assumption that we could make a list of all the real numbers was false (because we couldn't even make a list of the ones from 0 to 1)

Order	Number
1	0.58506706117215100 …
2	0.30188097640659700 …
3	0.05925831116503750 …
4	0.09291012351774230 …
5	0.79408644654174900 …
6	0.09792740408760530 …
7	0.72995316404639900 …
8	0.26184376611267000 …
9	0.42370325559805900 …
…	…

Names

- For future reference, the cardinality of positive integers, countable infinity, is named $\aleph_0$ (pronounced aleph null)
- The cardinality of real numbers, the first uncountable infinity (because there are infinitely many uncountable infinities), is named $\aleph_1$ (pronounced aleph 1)

Relations

Relations

- **Relations** are generalizations of functions
- In a function, an element of the domain must map to exactly one element of the co-domain
- In a relation, an element from one set can be related to any number (from zero up to infinity) of other elements
- Like functions, we're usually going to focus on binary relations
- We can define any binary relation between sets A and B as a subset of $A \times B$

Notation

- For binary relation R,
  - $x\ R\ y \ \leftrightarrow\ (x, y) \in R$
- Let R be a relation from $\mathbb{Z}$ to $\mathbb{Z}$ such that $(x, y) \in R$ iff $x -\ y$ is even
  - Is $1\ R\ 3$?
  - Is $2\ R\ 3$?
  - Is $2\ R\ 2$?
- Let C be a relation from $\mathbb{R}$ to $\mathbb{R}$ such that $(x, y) \in \mathbb{R}$ iff $x^2\ +\ y^2\ =\ 1$
  - Is $(1, 0) \in\ C$?
  - Is $0\ C\ 0$?
  - Is $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$?

Function or not?

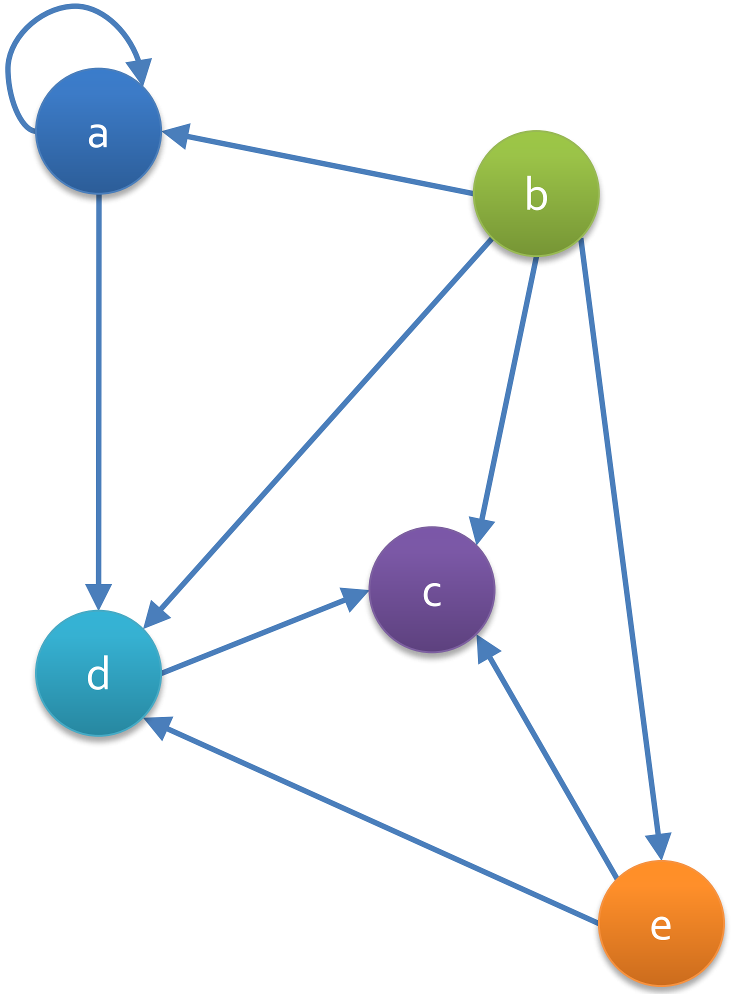
- Consider the sets $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$
- Let R be the relation $\{(2,5), (4,1), (4,3), (6,5)\}$
  - Draw the arrow diagram for R
  - Is R a function?
- Let S be the relation for all $(x, y) \in A \times B$, $(x, y) \in S$ iff $y = x + 1$
  - Draw the arrow diagram for S
  - Is S a function?
- $x^2 + y^2 = 1$ on real numbers is not a function for both reasons

Inverses

- We've relaxed things considerably by moving from functions to relations
- All relations have inverses (just reverse the order of the ordered pairs)
- Example
  - Let $A = \{2,3,4\}$ and $B = \{2,6,8\}$
  - For all $(x, y) \in A \times B$, $x\ R\ y \leftrightarrow x \mid y$
  - List the ordered pairs in R
  - List the ordered pairs in R^{-1}

Directed graphs

- A directed graph describes a relationship between nodes
- One way to record a graph is as a matrix
- We can also think of a directed graph as a relation from a set to itself
- What's the relation for this directed graph?



Upcoming

Next time…

- Reflexivity
- Symmetry
- Transitivity
- Equivalence relations

Reminders

- Work on Assignment 3
  - Due next Friday
- Read 8.2 and 8.3