Functions

Part Three

Recap from Last Time

Injective Functions

- A function $f : A \to B$ is called ***injective*** (or ***one-to-one***) if each element of the codomain has at most one element of the domain that maps to it.
  - A function with this property is called an ***injection***.
- Formally, $f : A \to B$ is an injection if this statement is true:

$$\forall a_1 \in A. \forall a_2 \in A. (a_1 \neq a_2 \to f(a_1) \neq f(a_2))$$

(*"If the inputs are different, the outputs are different"*)

- Equivalently:

$$\forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \to a_1 = a_2)$$

(*"If the outputs are the same, the inputs are the same"*)

Surjective Functions

- A function $f : A \to B$ is called ***surjective*** (or ***onto***) if each element of the codomain is "covered" by at least one element of the domain.
  - A function with this property is called a ***surjection***.
- Formally, $f : A \to B$ is a surjection if this statement is true:

$$\forall b \in B.\ \exists a \in A.\ f(a) = b$$

(*"For every possible output, there's at least one possible input that produces it"*)

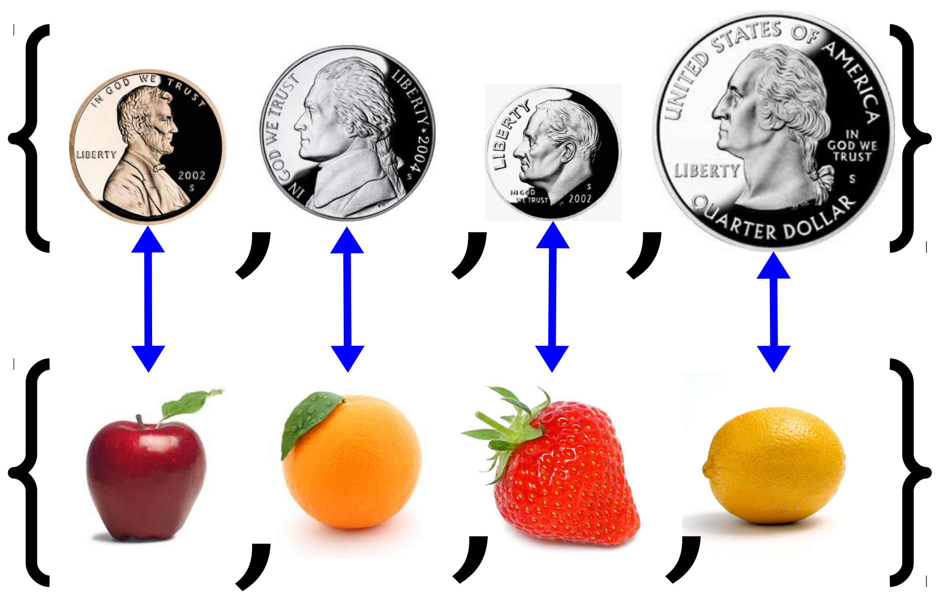
Bijections

- A function that associates each element of the codomain with a unique element of the domain is called ***bijective***.
  - Such a function is a ***bijection***.
- Formally, a bijection is a function that is both ***injective*** and ***surjective***.
- Bijections are sometimes called ***one-to-one correspondences***.
  - Not to be confused with "one-to-one functions."

Comparing Cardinalities

- The relationships between set cardinalities are defined in terms of functions between those sets.
- Here is the formal definition of what it means for two sets to have the same cardinality:

$|S| = |T|$ if there exists a *bijection* $f : S \to T$



Properties of Cardinality

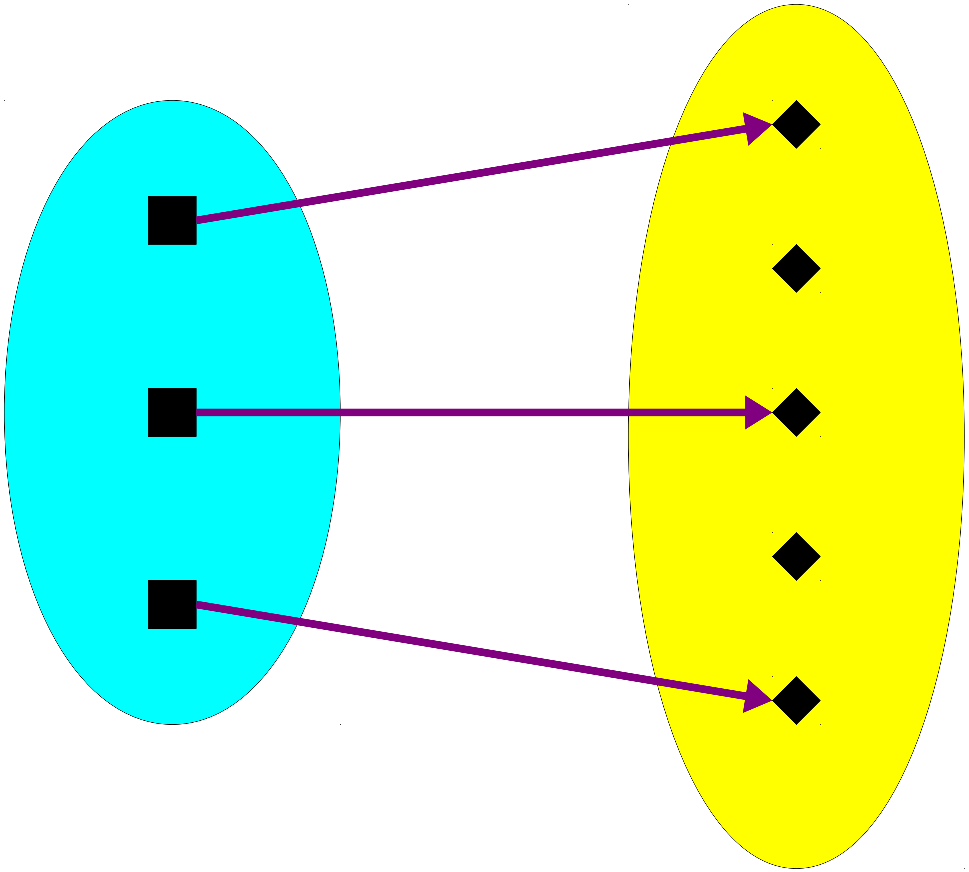
- For any sets R, S, and T, the following are true:
  - $|S| = |S|$.
    - Define $f : S \to S$ as $f(x) = x$.
  - If $|S| = |T|$, then $|T| = |S|$.
    - If $f : S \to T$ is a bijection, then $f^{-1} : T \to S$ is a bijection.
  - If $|R| = |S|$ and $|S| = |T|$, then $|R| = |T|$.
    - If $f : R \to S$ and $g : S \to T$ are bijections, then $g \circ f : R \to T$ is a bijection.

New Stuff!

Ranking Cardinalities

- We define $|S| \leq |T|$ as follows:

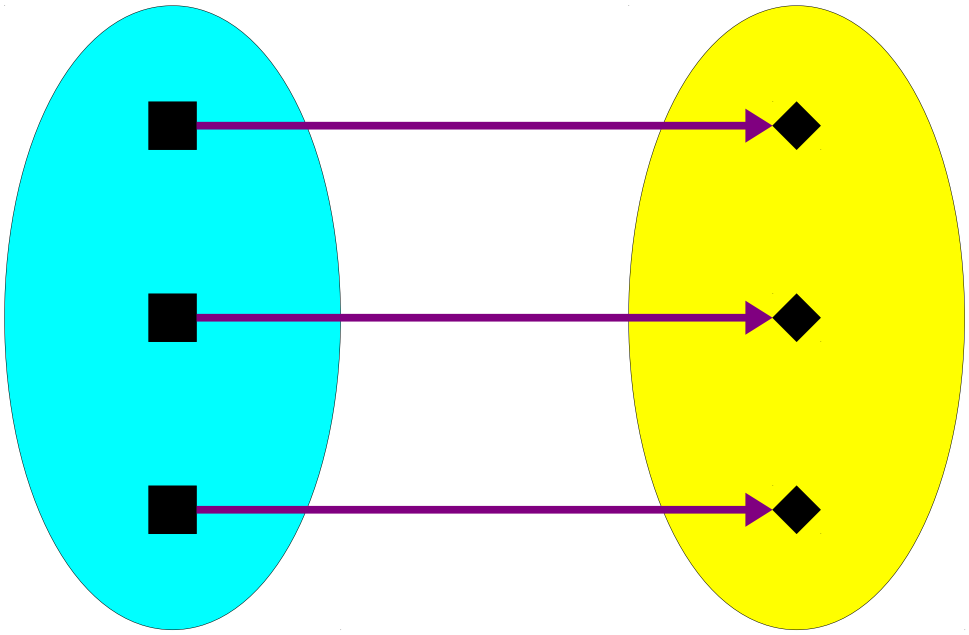
  $|S| \leq |T|$ if there is an injection $f : S \to T$



Ranking Cardinalities

- We define $|S| \leq |T|$ as follows:

  $|S| \leq |T|$ if there is an injection $f : S \to T$



Ranking Cardinalities

- We define $|S| \leq |T|$ as follows:

  $|S| \leq |T|$ if there is an injection $f : S \to T$

- For any sets R, S, and T:
  - $|S| \leq |S|$.
    - Let $f : S \to S$ be $f(x) = x$.
  - If $|R| \leq |S|$ and $|S| \leq |T|$, then $|R| \leq |T|$.
    - The composition of two injections is an injection.
  - Either $|S| \leq |T|$ or $|T| \leq |S|$.
    - This one is harder and requires the ***axiom of choice***. We'll just take it on faith. ☺

Theorem (Cantor-Bernstein-Schroeder): If S and T are sets where $|S| \leq |T|$ and $|T| \leq |S|$, then $|S| = |T|$

(This was first proven by Richard Dedekind.)

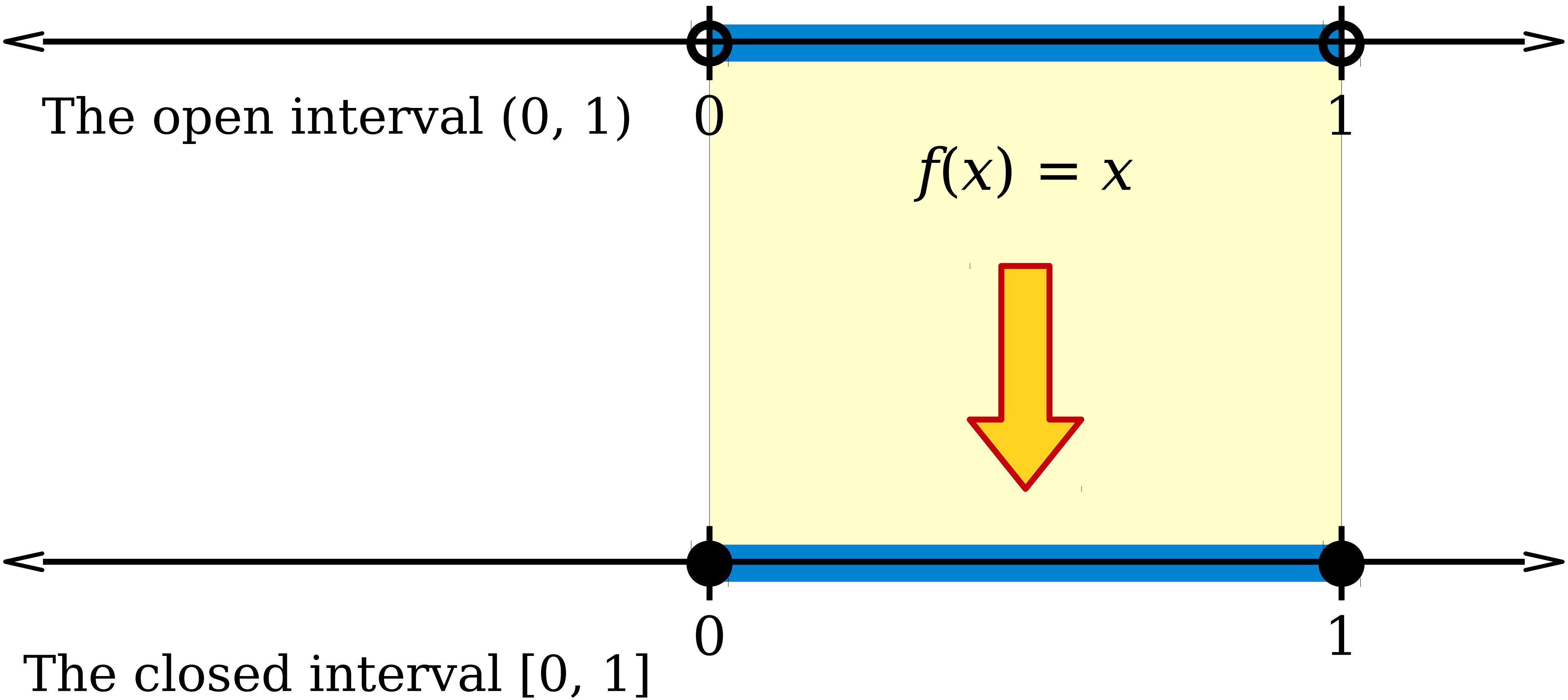
The CBS Theorem

- ***Theorem:*** If $|S| \leq |T|$ and $|T| \leq |S|$, then $|S| = |T|$.
- Isn't this, kinda, you know, obvious?
- Look at the definitions. What does the above theorem actually say?

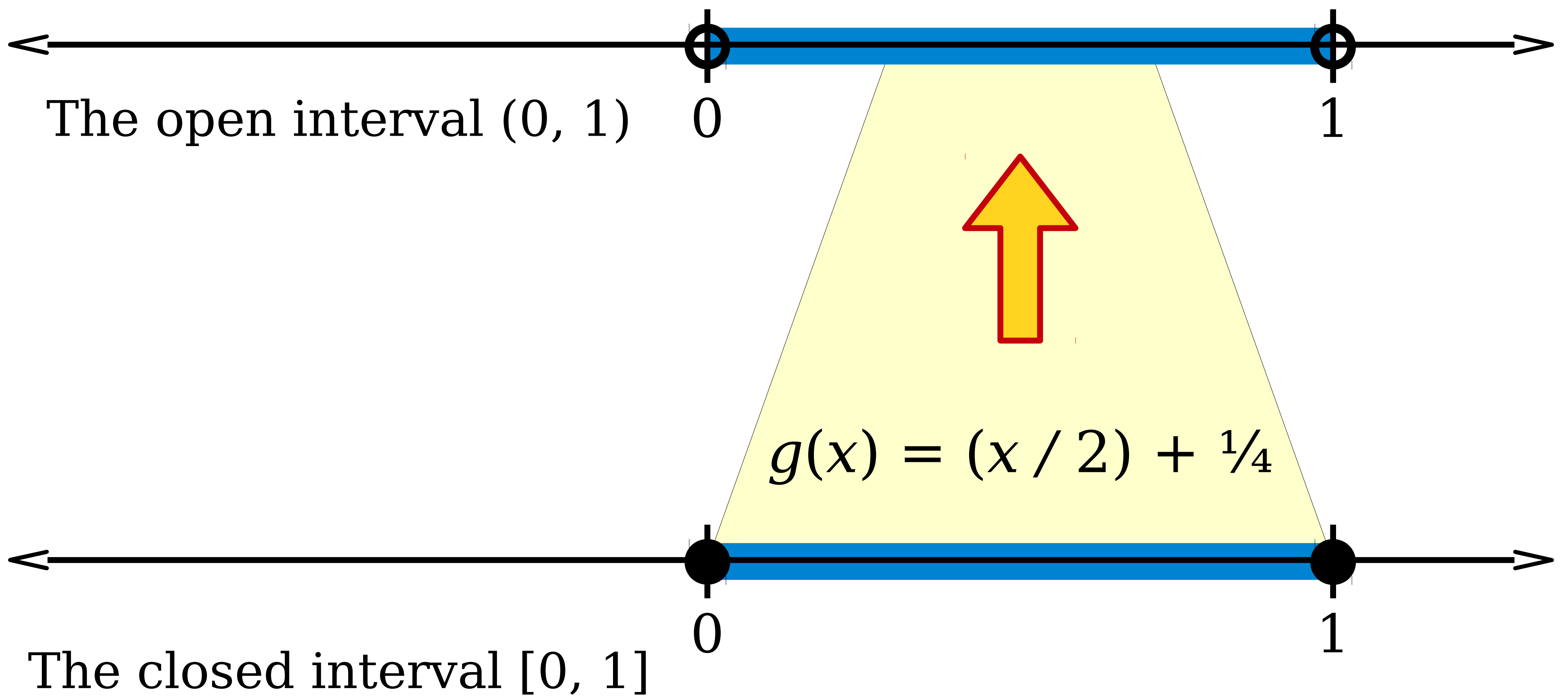
If there is an injection $f : S \to T$ and an injection $g : T \to S$, then there must be some bijection $h : S \to T$.

- This is much less obvious than it looks.

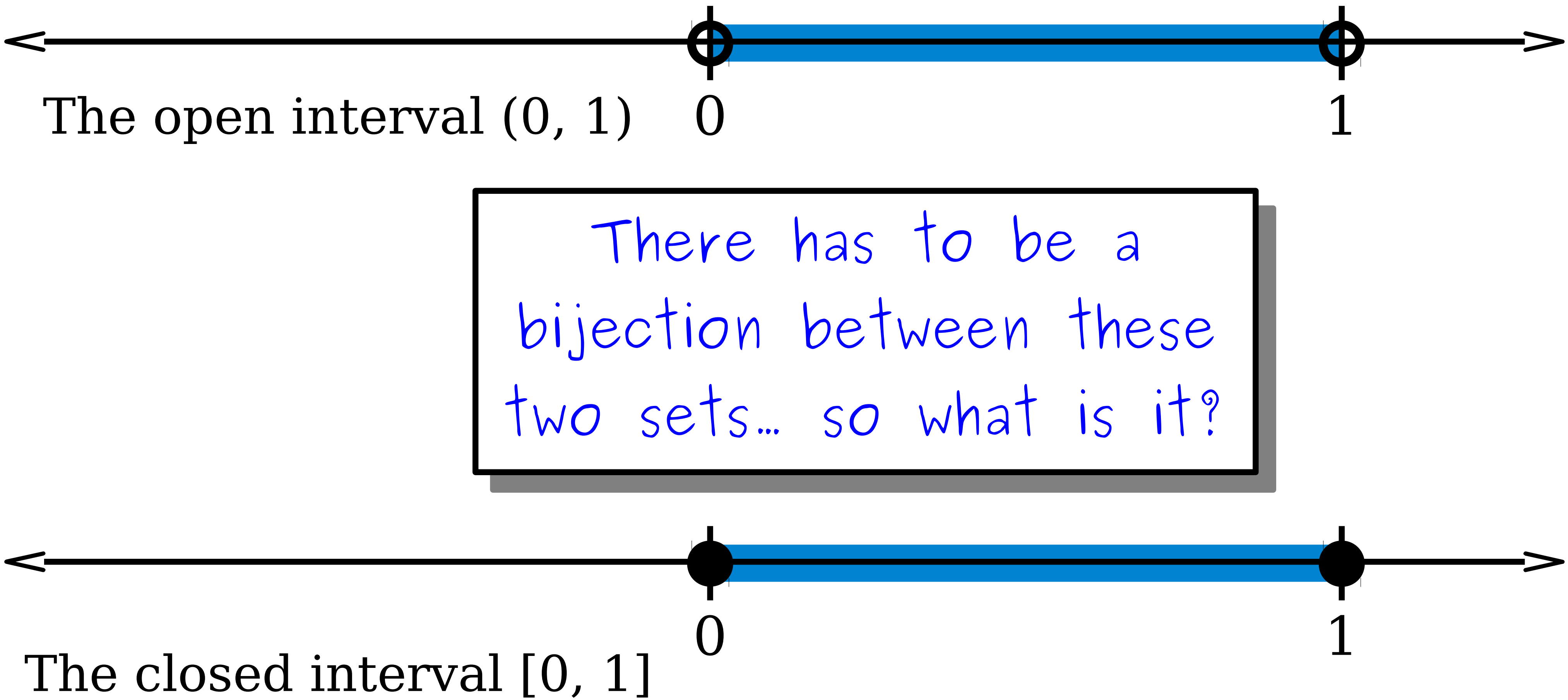
Why CBS is Tricky



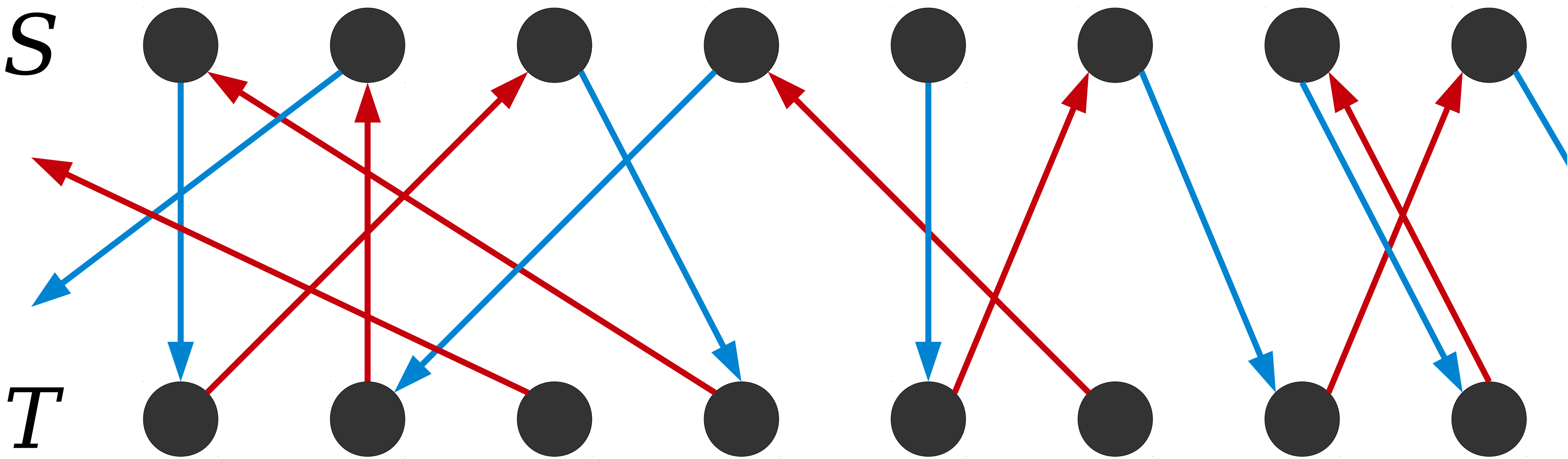
Why CBS is Tricky



Why CBS is Tricky

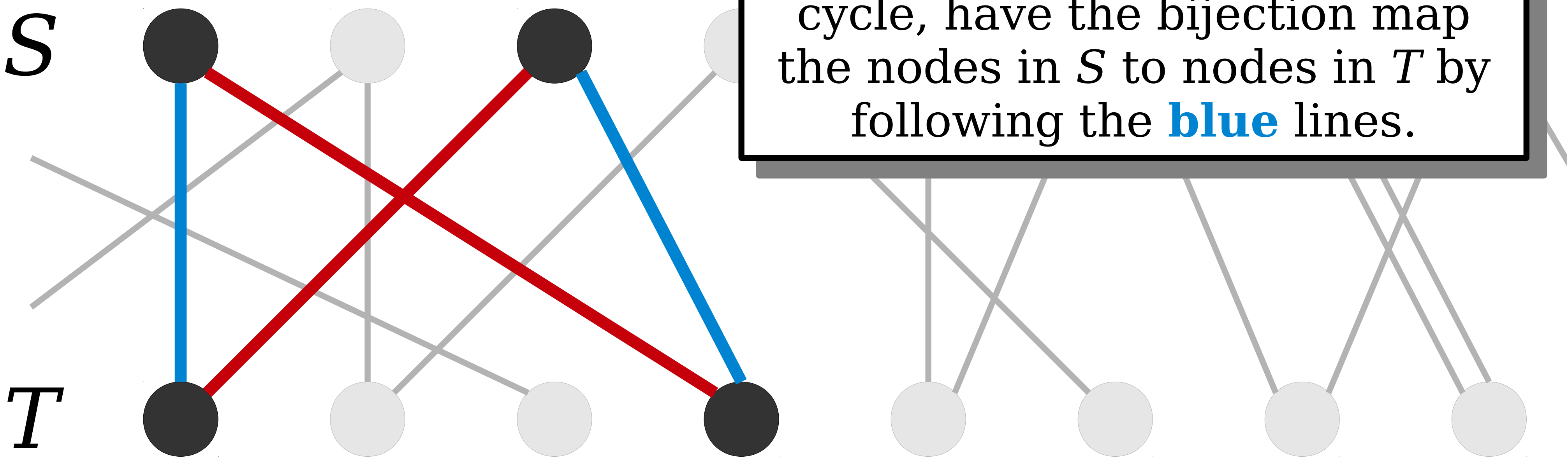


Proving CBS, Intuitively



Blue lines represent the injection $f : S \to T$
Red lines represent the injection $g : T \to S$

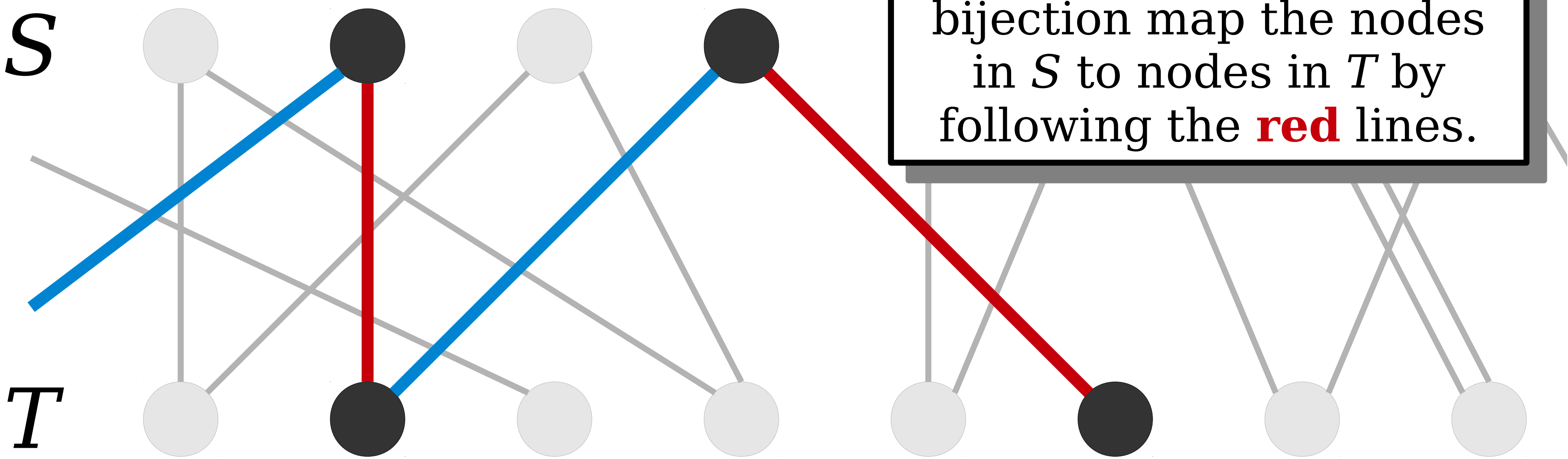
Proving CBS, Intuitively



If the values are linked in a cycle, have the bijection map the nodes in S to nodes in T by following the **blue** lines.

Blue lines represent the injection $f : S \to T$
Red lines represent the injection $g : T \to S$

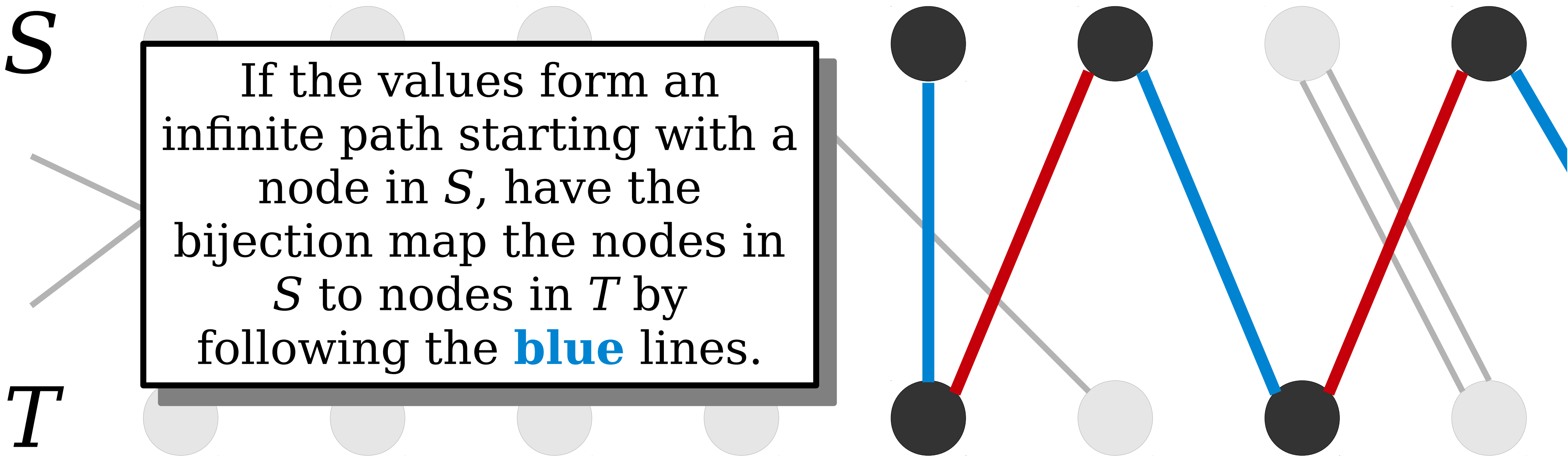
Proving CBS, Intuitively



If the values form an infinite path starting with a node in T, have the bijection map the nodes in S to nodes in T by following the **red** lines.

Blue lines represent the injection $f : S \to T$
Red lines represent the injection $g : T \to S$

Proving CBS, Intuitively



If the values form an infinite path starting with a node in S, have the bijection map the nodes in S to nodes in T by following the **blue** lines.

Blue lines represent the injection $f : S \to T$
Red lines represent the injection $g : T \to S$

Why This Matters

- I chose to sketch out the proof of the CBS theorem because it's a really clever idea.
- Don't worry too much about the specifics of this proof. Think of it as more of a “math symphony.” ☺
- ***Fun Challenge Problem:*** Find an explicit bijection $f : [0, 1] \to (0, 1)$.

An Application

What is $|\mathbb{N}^2|$?

$\mathbb{N}$	0	1	2	3	4	5	6	...

	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 4)	(0, 5)	(0, 6)	(0, ...)
	(1, 0)	(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)	(1, ...)
	(2, 0)	(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	(2, 6)	(2, ...)
$\mathbb{N}^2$	(3, 0)	(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	(3, 6)	(3, ...)
	(4, 0)	(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	(4, 6)	(4, ...)
	(5, 0)	(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	(5, 6)	(5, ...)
	(..., 0)	(..., 1)	(..., 2)	(..., 3)	(..., 4)	(..., 5)	(..., 6)	...

$|\mathbb{N}| \leq |\mathbb{N}^2|$ Find an injection $f : \mathbb{N} \to \mathbb{N}^2$ $\boldsymbol{f(n) = (0, n)}$

$|\mathbb{N}^2| \leq |\mathbb{N}|$ Find an injection $f : \mathbb{N}^2 \to \mathbb{N}$ $\boldsymbol{f(a, b) = 2^a 3^b}$

Counterintuitive result: $|\mathbb{N}| = |\mathbb{N}^2|$

Time-Out for Announcements!

Grace Hopper Conference

- I will be out of town Tuesday through Saturday at the Grace Hopper Conference.
- Class still meets Wednesday / Friday; we'll have someone else cover for me.
- I will probably be very slow to respond over email.
- Our head TA Sal will also be at Grace Hopper; Kevin Gibbons (kgibb@stanford.edu) will be taking over as head TA in the meantime.

Two Google Scholarships

- Google offers $10,000 scholarships that are available if you will be a student next year.
- Two big ones:
  - **Google Anita Borg Scholarship**: Available to women pursuing a CS degree.
  - **Generation Google Scholarship**: Available to students of underrepresented backgrounds pursuing a CS degree.
- Both scholarships have applications due on December 1.
- The bolded terms are links. Click them for details!

A Note on First-Order Logic

- When using quantifiers, you can quantify over everything by saying something like this:

$$\forall x.\ \varphi \qquad \exists x.\ \varphi$$

- You can also quantify over all the elements of a set:

$$\forall x \in S.\ \varphi \qquad \exists x \in S.\ \varphi$$

- However, it's not permitted to write things like:

⚠ $\forall x\ Set(x).\ \varphi \qquad \exists x\ Set(x).\ \varphi$ ⚠

⚠ $\forall\ Set(x).\ \varphi \qquad \exists\ Set(x).\ \varphi$ ⚠

- Even though we know what you mean, it's not syntactically valid to do this. There's no fundamental reason why it *couldn't* be syntactically valid. It just isn't.

Your Questions

"I tend to miss material on slides because your lecture style is pretty fast. Would you be able to post the lecture slides before class so we can cross-reference on our computers?"

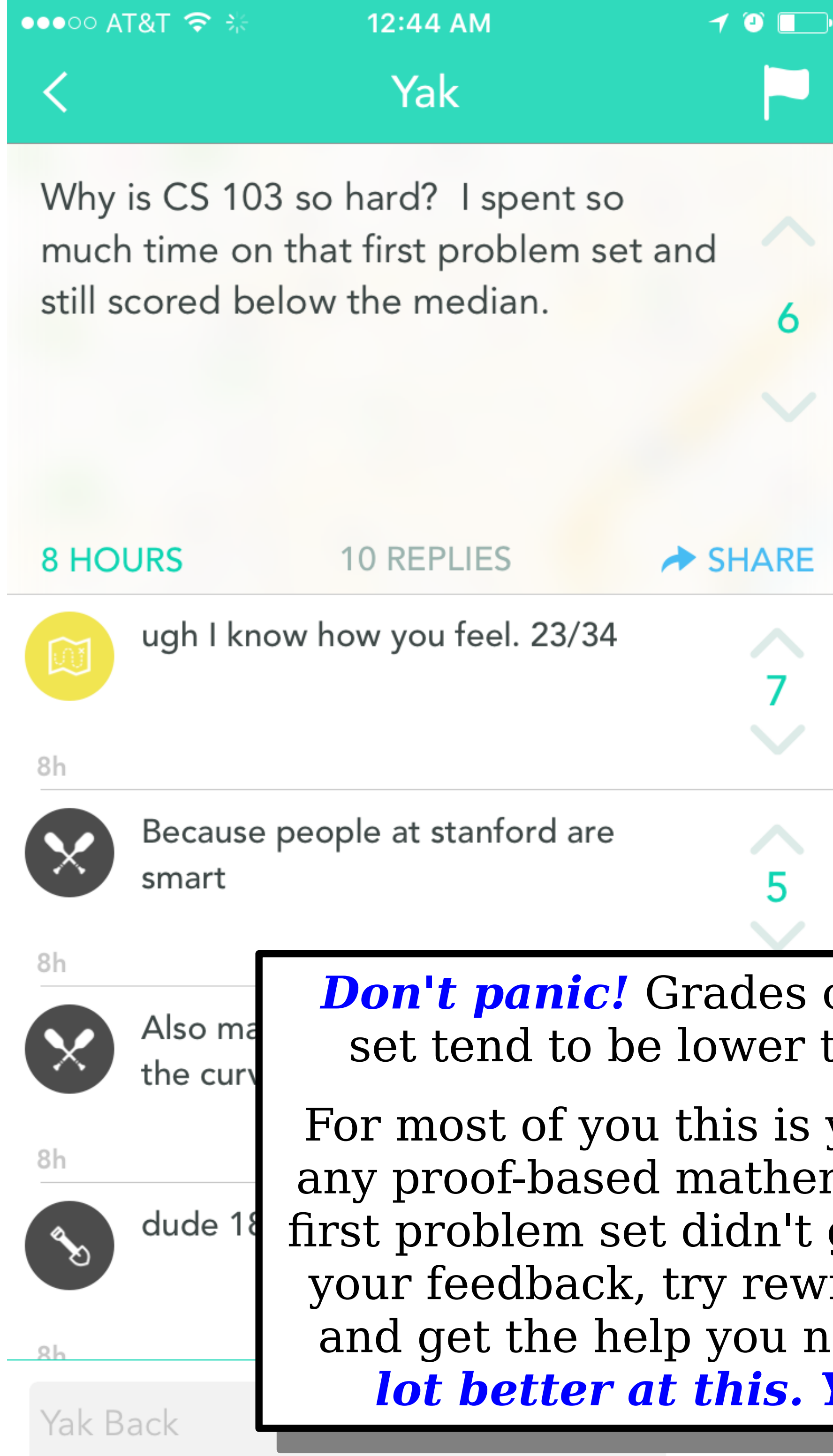
Sorry for going so fast! I typically don't post slides beforehand because (1) I'm a compulsive tinkerer and often make last-minute changes and (2) from experience, when I've done this, people tend to do much worse in the class.

$$
\begin{aligned}
&\forall S.\ (\mathrm{Set}(S)\ \land \\
&\quad \forall p \in S.\ \mathit{Problem}(p)\ \land \\
&\quad \mathit{writtenBy}(\mathit{Keith}, S)\ \land \\
&\quad \mathit{isSecond}(S) \rightarrow \\
&\qquad \forall P.\ (\mathit{People}(P) \rightarrow \mathit{Suffers}(P)) \\
&)
\end{aligned}
$$

First-order logic isn't easy. There are ton of edge cases to consider, and even really simple concepts like the number two are tough to reason about. Plus, quantifiers are super counterintuitive.

Don't panic if you found that problem set challenging. This problem set was designed to make sure that you couldn't coast by with just a cursory understanding of the material. The good news is that once you've worked through these problems once, you'll find that it's significantly easier to solve similar problems in the future.

That said, if you were actually suffering, then you should definitely come talk to us, since it wasn't our intent to make your life miserable.



Don't panic! Grades on the first problem set tend to be lower than on later ones.

For most of you this is your first time doing any proof-based mathematics. It's fine if the first problem set didn't go so well. Look over your feedback, try rewriting your answers, and get the help you need. ***You will get a lot better at this. You can do this!***

“What kind of social responsibility do you think large tech companies have towards the communities they are in (i.e. what do you think of the social problems like gentrification in SF and EPA that have arisen due to Google, FB, etc)?”

A few thoughts:

1. Listen to what the community is saying. Don't presume to know what the community wants or needs. Work with local community leaders to figure out in what ways the company can help.

2. Create good-paying, stable jobs that community members can hold. Offer vocational training to help locals get into those jobs.

3. Look to the past. See what lessons you can learn from other corporations that have largely transformed communities (i.e. Detroit).

Back to CS103!

Unequal Cardinalities

- Recall: $|A| = |B|$ if the following statement is true:

There exists a bijection $f : A \to B$

- What does it mean for $|A| \neq |B|$?

No function $f : A \to B$ is a bijection.

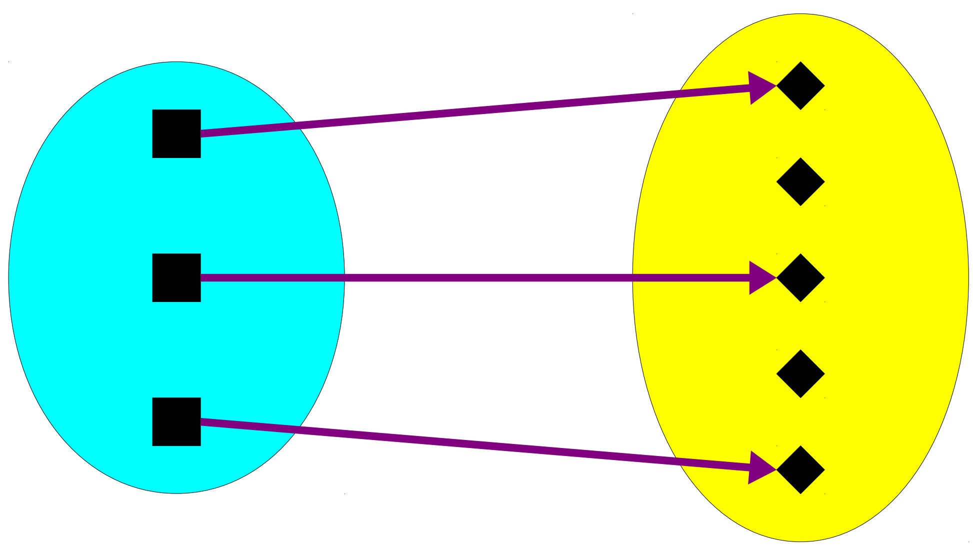
- Need to show that, out of all the (potentially infinitely many) functions from A to B, *not one of them* is a bijection.

Comparing Cardinalities

- Formally, we define < on cardinalities as

$$|S| < |T| \quad \text{if} \quad |S| \leq |T| \text{ and } |S| \neq |T|$$

- In other words:
  - There is an injection from *S* to *T*.
  - There is no bijection between *S* and *T*.



Comparing Cardinalities

- Formally, we define $<$ on cardinalities as

$$|S| < |T| \quad \text{if} \quad |S| \leq |T| \text{ and } |S| \neq |T|$$

- In other words:
  - There is an injection from S to T.
  - There is no bijection between S and T.
- ***Theorem:*** For any sets S and T, exactly one of the following is true:

$$|S| < |T| \qquad |S| = |T| \qquad |S| > |T|$$

What is the relation between $|\mathbb{N}|$ and $|\mathbb{R}|$?

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$

Theorem: $|\mathbb{N}| \neq |[0, 1)|$

Our Goal

- We need to show the following:

No function $f : \mathbb{N} \to [0, 1)$ is bijective

- To prove it, we will do the following:
  - Choose an arbitrary function $f : \mathbb{N} \to [0, 1)$.
  - Show that f cannot be a surjection by finding some $d \in [0, 1)$ that is not mapped to by f.
  - Conclude that this arbitrary function f is not a bijection, so no bijections from $\mathbb{N}$ to $[0, 1)$ exist.

The Intuition

- Suppose $f : \mathbb{N} \to [0, 1)$.
- We can then list off an infinite sequence of real numbers

$$f(0), f(1), f(2), f(3), \ldots .$$

We will show that we can always find a real number $d \in [0, 1)$ such that

If $n \in \mathbb{N}$, then $f(n) \neq d$.

Rewriting Our Constraints

- Our goal is to find some $d \in [0, 1)$ such that

If $n \in \mathbb{N}$, then $f(n) \neq d$.

- In other words, we want to pick d such that

$$f(0) \neq d$$

$$f(1) \neq d$$

$$f(2) \neq d$$

$$f(3) \neq d$$

$$\ldots$$

The Critical Insight

- **Key Idea:** Build the real number d out of infinitely many “pieces,” with one piece for each natural number.
  - Choose the 0^{th} piece such that $f(0) \neq d$.
  - Choose the 1^{st} piece such that $f(1) \neq d$.
  - Choose the 2^{nd} piece such that $f(2) \neq d$.
  - Choose the 3^{rd} piece such that $f(3) \neq d$.
  - …
- This “frankenreal” is specifically constructed so that $f(n) \neq d$ for all $n \in \mathbb{N}$.

		d_0	d_1	d_2	d_3	d_4	d_5	...
0	0.	6	7	5	3	0	9	...
1	0.	1	4	1	5	9	2	...
2	0.	1	2	3	5	8	3	...
3	0.	0	0	0	0	0	0	...
4	0.	7	1	8	2	8	1	...
5	0.	6	1	8	0	3	4	...
...	...	...	...	...	...	...	...	...

0.	6	4	3	0	8	4	...

		d_0	d_1	d_2	d_3	d_4	d_5	...
0	0.	6	7	5	3	0	9	...
1	0.	1	4	1	5	9	2	...
2	0.	1	2	3	5	8	3	...
3	0.	0	0	0	0	0	0	...
4	0.	7	1	8	2	8	1	...
5	0.	6	1	8	0	3	4	...
...	...	...	...	...	...	...	...	...

Set all nonzero values to 0 and all 0s to 1.

0.	0	0	0	1	0	0	...

		d_0	d_1	d_2	d_3	d_4	d_5	...
0	0.	6	7	5	3	0	9	...
1	0.	1	4	1	5	9	2	...
2	0.	1	2	3	5	8	3	...
3	0.	0	0	0	0	0	0	...
4	0.	7	1	8	2	8	1	...
5	0.	6	1	8	0	3	4	...
...	...	...	...	...	...	...	...	...

0.	0	0	0	1	0	0	...

Which natural number is paired with this real number?

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r.

		d_0	d_1	d_2	d_3	d_4	…
0	0.	3	1	4	1	5	…
1	0.	1	0	2	0	3	…
2	0.	8	6	7	5	3	…
3	0.	2	7	1	8	2	…
4	0.	0	0	0	0	0	…
…	0.	…	…	…	…	…	…

***f*(0)**

0.	3	0	7	8	0	…

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r.

		d_0	d_1	d_2	d_3	d_4	…
0	0.	3	1	4	1	5	…
1	0.	1	0	2	0	3	…
2	0.	8	6	7	5	3	…
3	0.	2	7	1	8	2	…
4	0.	0	0	0	0	0	…
…	0.	…	…	…	…	…	…

$f(0)[0]$

0.	3	0	7	8	0	…

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r.

		d_0	d_1	d_2	d_3	d_4	…
0	0.	3	1	4	1	5	…
1	0.	1	0	2	0	3	…
2	0.	8	6	7	5	3	…
3	0.	2	7	1	8	2	…
4	0.	0	0	0	0	0	…
…	0.	…	…	…	…	…	…

0.	3	0	7	8	0	…

***f*(0)[0]**

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r.

		d_0	d_1	d_2	d_3	d_4	…
0	0.	3	1	4	1	5	…
1	0.	1	0	2	0	3	…
2	0.	8	6	7	5	3	…
3	0.	2	7	1	8	2	…
4	0.	0	0	0	0	0	…
…	0.	…	…	…	…	…	…

$f(n)[n]$

0.	3	0	7	8	0	…

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r.

		d_0	d_1	d_2	d_3	d_4	…
0	0.	3	1	4	1	5	…
1	0.	1	0	2	0	3	…
2	0.	8	6	7	5	3	…
3	0.	2	7	1	8	2	…
4	0.	0	0	0	0	0	…
…	0.	…	…	…	…	…	…

0.	0	1	0	0	1	…

0 if $f(n)[n] \neq 0$
1 if $f(n)[n] = 0$

Theorem: $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof: We will prove that $|\mathbb{N}| \neq |[0, 1)|$. Since $|[0, 1)| = |\mathbb{R}|$, this shows that $|\mathbb{N}| \neq |\mathbb{R}|$. To show that $|\mathbb{N}| \neq |[0, 1)|$, we will prove that there is no bijective function $f : \mathbb{N} \to [0, 1)$. To do so, let $f : \mathbb{N} \to [0, 1)$ be an arbitrary function. We will show that it is not surjective.

Let's introduce some new notation. For any $r \in [0, 1)$, let $r[n]$ be the nth decimal digit in the decimal representation of r. Now, let d be the real number whose integer part is zero and whose decimal digits obey the following rules:

$$d[n] = \begin{cases} 1 & \text{if } f(n)[n] = 0 \\ 0 & \text{otherwise} \end{cases}$$

Since d's integer part is zero, we know that $d \in [0, 1)$.

We claim that $f(n) \neq d$ for any $n \in \mathbb{N}$. To see why, consider any $n \in \mathbb{N}$ and look at $f(n)[n]$. There are two possibilities:

Case 1: $f(n)[n] = 0$. By construction $d[n] = 1$, so $f(n) \neq d$.

Case 2: $f(n)[n] \neq 0$. By construction $d[n] = 0$, so $f(n) \neq d$.

Because $f(n) \neq d$ for any $n \in \mathbb{N}$, we see f is not surjective, so f is not a bijection. Since f was chosen arbitrarily, this means that there is no bijection $f : \mathbb{N} \to [0, 1)$, so $|\mathbb{N}| \neq |[0, 1)|$. ■

An Interesting Historical Aside

- The proof we just covered was first discovered by Georg Cantor.
- Interestingly, this was *not* Cantor's first proof that $|\mathbb{N}| \neq |\mathbb{R}|$. He first developed a different proof based on converging sequences of real numbers.
- Curious? Come talk to us after class!

The Grand Finale: **Cantor's Theorem**

Cantor's Theorem

- ***Cantor's Theorem*** is the following:

  If S is a set, then $|S| < |\wp(S)|$

- This is how we concluded that there are more problems to solve than programs to solve them.
- We informally sketched a proof of this in the first lecture.
- Let's now formally prove Cantor's Theorem.

The Key Step

- We need to show the following:

If S is a set, then $|S| \neq |\wp(S)|$.

- To do this, we need to prove this statement:

For any set S, no function
$f : S \to \wp(S)$ is a bijection.

- Our proof of this result has the same basic idea as the proof we just saw: we need to construct a set $D \in \wp(S)$ that is specifically designed so that $f(x) \neq D$ for any $x \in S$.

x_0	x_1	x_2	x_3	x_4	x_5	…

$x_0 \longleftrightarrow \{ x_0, x_2, x_4, \ldots \}$

$x_1 \longleftrightarrow \{ x_0, x_3, x_4, \ldots \}$

$x_2 \longleftrightarrow \{ x_4, \ldots \}$

$x_3 \longleftrightarrow \{ x_1, x_4, \ldots \}$

$x_4 \longleftrightarrow \{ x_0, x_5, \ldots \}$

$x_5 \longleftrightarrow \{ x_0, x_1, x_2, x_3, x_4, x_5, \ldots \}$

…

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	**…**
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	**…**
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	**…**
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	**…**
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	**…**
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**…**
…	**…**	**…**	**…**	**…**	**…**	**…**	**…**

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	…
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**Y**	**Y**	**N**	…

Which row in the table is paired with this set?

	x_0	x_1	x_2	x_3	x_4	x_5	...
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	**...**
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	**...**
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	**...**
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	**...**
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	**...**
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**...**
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**

N	**Y**	**Y**	**Y**	**Y**	**N**	**...**

***f*(x_0)**

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	**…**
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	**…**
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	**…**
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	**…**
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	**…**
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**…**
…	**…**	**…**	**…**	**…**	**…**	**…**	**…**

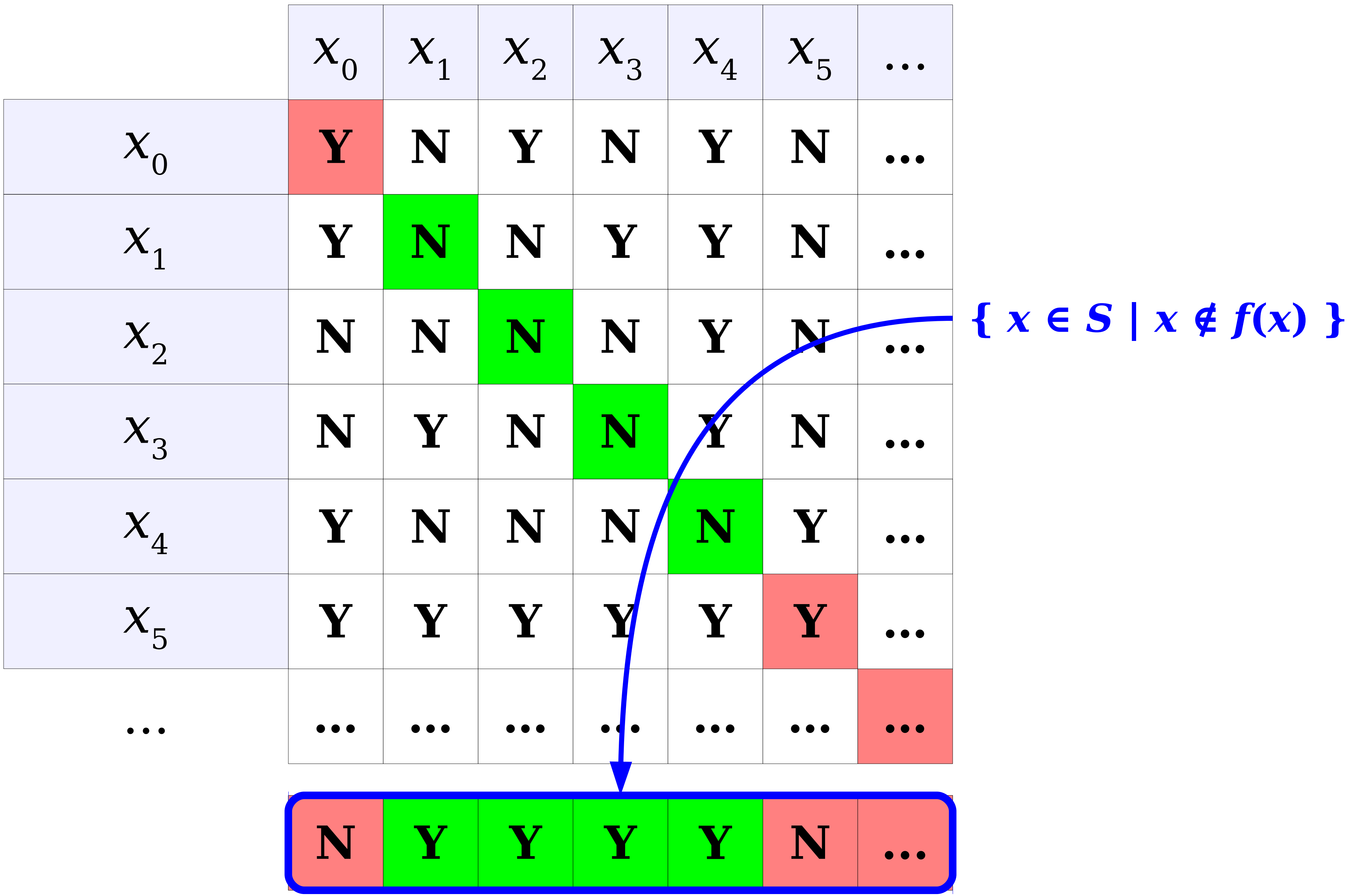
N	**Y**	**Y**	**Y**	**Y**	**N**	**…**

$x_0 \notin f(x_0)$?

	x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	**Y**	**N**	**Y**	**N**	**Y**	**N**	**…**
x_1	**Y**	**N**	**N**	**Y**	**Y**	**N**	**…**
x_2	**N**	**N**	**N**	**N**	**Y**	**N**	**…**
x_3	**N**	**Y**	**N**	**N**	**Y**	**N**	**…**
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	**…**
x_5	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**…**
…	**…**	**…**	**…**	**…**	**…**	**…**	**…**

N	**Y**	**Y**	**Y**	**Y**	**N**	**…**

$x \notin f(x)$?


x0 x1 x2 x3 x4 x5 ...
x0 Y N Y N Y N ...
x1 Y N N Y Y N ...
x2 N N N N Y N ...
x3 N Y N N Y N ...
x4 Y N N N N Y ...
x5 Y Y Y Y Y Y ...
... ...
{ x ∈ S | x ∉ f(x) }
N Y Y Y Y N ...

The Diagonal Set

- Let $f : S \to \wp(S)$ be an arbitrary function from S to $\wp(S)$.
- Define the set D as follows:

$$\boldsymbol{D = \{ x \in S \mid x \notin f(x) \}}$$

("The set of all elements x where x is not an element of the set f(x).")

- This is a formalization of the set we found in the previous picture.
- Using this choice of D, we can formally prove that no function $f : S \to \wp(S)$ is a bijection.

Theorem: If S is a set, then $|S| \neq |\wp(S)|$.

Proof: Let S be an arbitrary set. We will prove that $|S| \neq |\wp(S)|$ by showing that there are no bijections from S to $\wp(S)$.

Suppose for the sake of contradiction that there is a bijective function $f : S \to \wp(S)$. Starting with f, we define the set

$$D = \{ x \in S \mid x \notin f(x) \}. \qquad (1)$$

Since every element of D is also an element of S, we know that $D \subseteq S$, so $D \in \wp(S)$. Therefore, since f is surjective, we know that there is some $y \in S$ such that $f(y) = D$.

We can now ask under what conditions this element y happens to be an element of D. By definition of D, we know that

$$y \in D \text{ iff } y \notin f(y). \qquad (2)$$

By assumption, $f(y) = D$. Combined with (2), this tells us

$$y \in D \text{ iff } y \notin D. \qquad (3)$$

This is impossible. We have reached a contradiction, so our assumption must have been wrong. Therefore, there are no bijections between S and $\wp(S)$, and therefore $|S| \neq |\wp(S)|$, as required. ■

The Diagonal Argument

- ***This proof is tricky.*** It's one of the hardest proofs we're going to encounter over the course of this quarter.
- To help you wrap your head around how it works, we've asked you a few questions about it on Problem Set Three.
- Don't panic if you don't get it immediately; you'll get a really good understanding of how it works if you play around with it.

Concluding the Proof

- We've just shown that $|S| \neq |\wp(S)|$ for any set S.
- To prove $|S| < |\wp(S)|$, we need to show that $|S| \leq |\wp(S)|$ by finding an injection from S to $\wp(S)$.
- Take $f : S \to \wp(S)$ defined as

$$\boldsymbol{f(x) = \{x\}}$$

- Good exercise: prove this function is injective.

Why All This Matters

- Proof by diagonalization is a powerful technique for showing two sets cannot have the same size.
- Can also be adapted for other purposes:
  - Finding specific problems that cannot be solved by computers.
  - Proving Gödel's Incompleteness Theorem.
  - Finding problems requiring some amount of computational resource to solve.
- We will return to this later in the quarter.