Cardinality

Problem Set Three checkpoint due in the box up front.

You can also turn in Problem Set Two using a late period.

Recap from Last Time

Functions

- A **function** f is a mapping such that every element of A is associated with a single element of B.
- If f is a function from A to B, then
  - we call A the **domain** of f.
  - we call B the **codomain** of f.
- We denote that f is a function from A to B by writing

$$\boldsymbol{f : A \to B}$$

Injections and Surjections

- A function $f : A \to B$ is an **injection** iff

for any $a_0, a_1 \in A$:
if $f(a_0) = f(a_1)$, then $a_0 = a_1$.

- *At most* one element of the domain maps to each element of the codomain.
- A function $f : A \to B$ is a **surjection** iff

for any $b \in B$, there exists an $a \in A$ where $f(a) = b$.

- *At least* one element of the domain maps to each element of the codomain.

Bijections

- A function that is injective and surjective is called **bijective**.
- *Exactly one* element of the domain maps to any particular element of the codomain.

Cardinality Revisited

Cardinality

- Recall (from *lecture one!*) that the **cardinality** of a set is the number of elements it contains.
- If S is a set, we denote its cardinality by $|S|$.
- For finite sets, cardinalities are natural numbers:
  - $|\{1, 2, 3\}| = 3$
  - $|\{100, 200, 300\}| = 3$
- For infinite sets, we introduced **infinite cardinals** to denote the size of sets:

$$|\mathbb{N}| = \aleph_0$$

Defining Cardinality

- It is difficult to give a rigorous definition of what cardinalities actually are.
  - What is 4? What is $\aleph_0$?
- **Idea:** Define cardinality as a *relation* between two sets rather than as an absolute quantity.
- We'll define what these relations between sets mean without actually defining what "a cardinality" actually is:

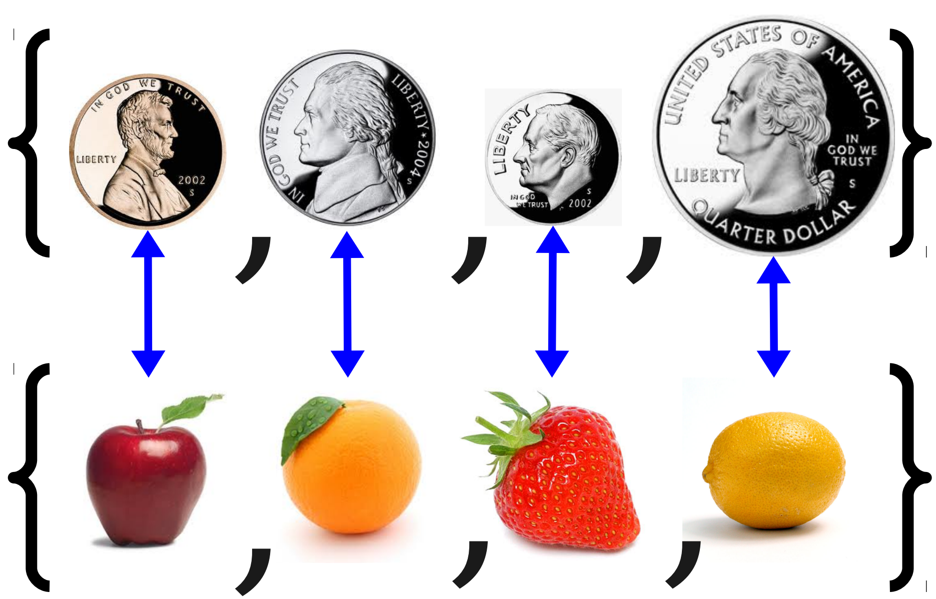
$$|S| = |T| \quad |S| \neq |T| \quad |S| \leq |T| \quad |S| < |T|$$

- Cardinality exists *between* sets!

Comparing Cardinalities

- The relationships between set cardinalities are defined in terms of functions between those sets.
- $|S| = |T|$ is defined using bijections.

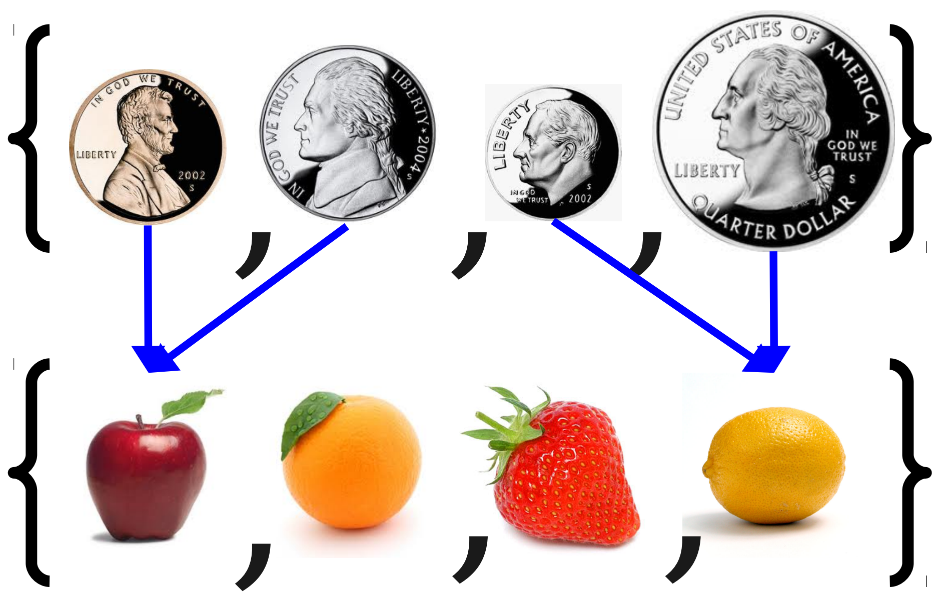
$|S| = |T|$ iff there exists a bijection $f : S \to T$



Comparing Cardinalities

- The relationships between set cardinalities are defined in terms of functions between those sets.
- $|S| = |T|$ is defined using bijections.

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

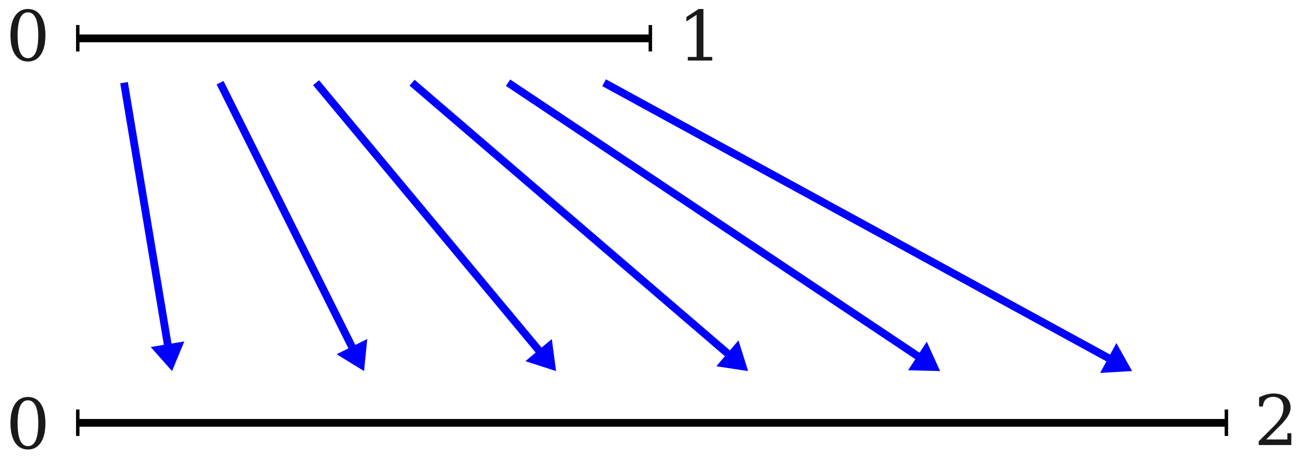


Properties of Cardinality

- Equality of cardinality is an equivalence relation.
- For any sets R, S, and T:
  - $|S| = |S|$. ***(reflexivity)***
  - If $|S| = |T|$, then $|T| = |S|$. ***(symmetry)***
  - If $|R| = |S|$ and $|S| = |T|$, then $|R| = |T|$. ***(transitivity)***
- ***Read the course notes for proofs of these results!***

Infinity is Weird…

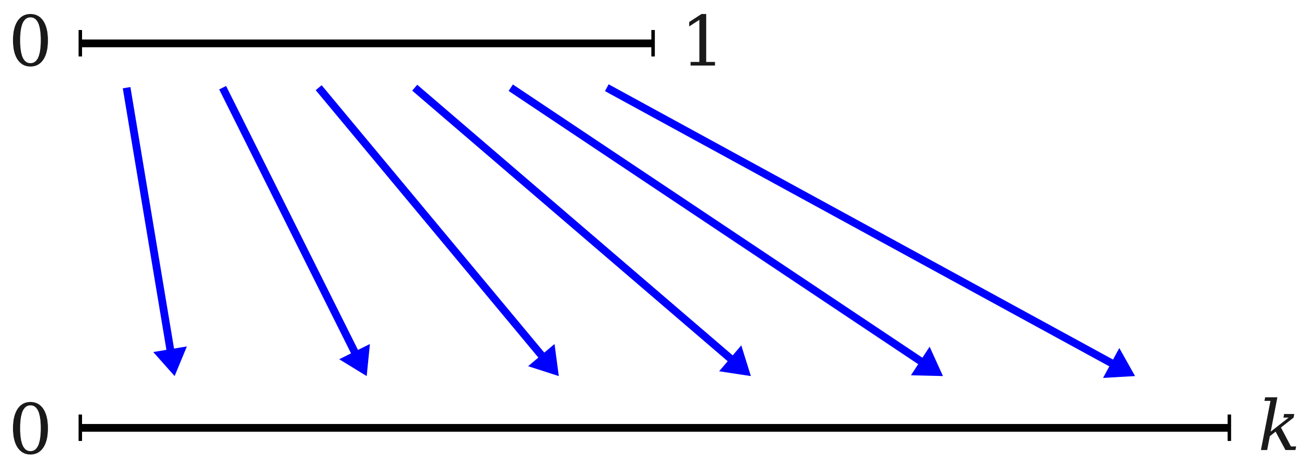
Home on the Range



$$f : [0, 1] \to [0, 2]$$
$$f(x) = 2x$$

$$|[0, 1]| = |[0, 2]|$$

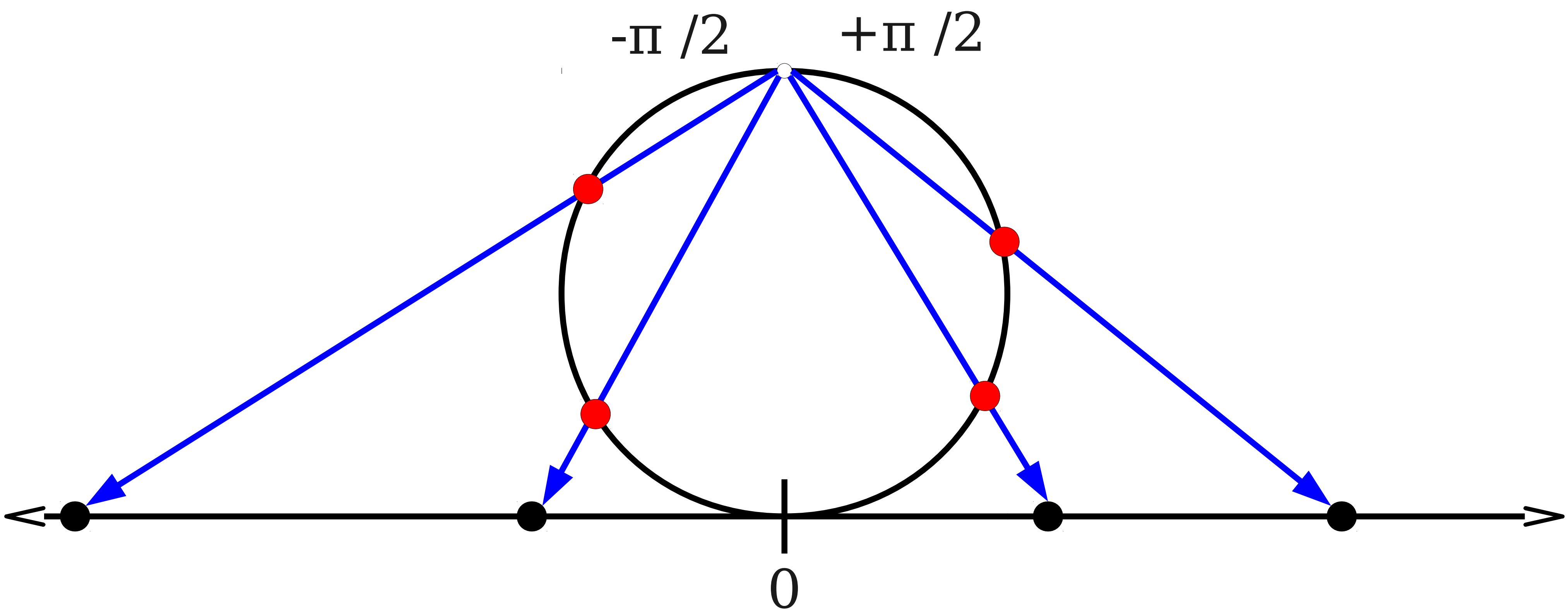
Home on the Range



$$f : [0, 1] \to [0, k]$$
$$f(x) = kx$$

$$|[0, 1]| = |[0, k]|$$

Put a Ring On It

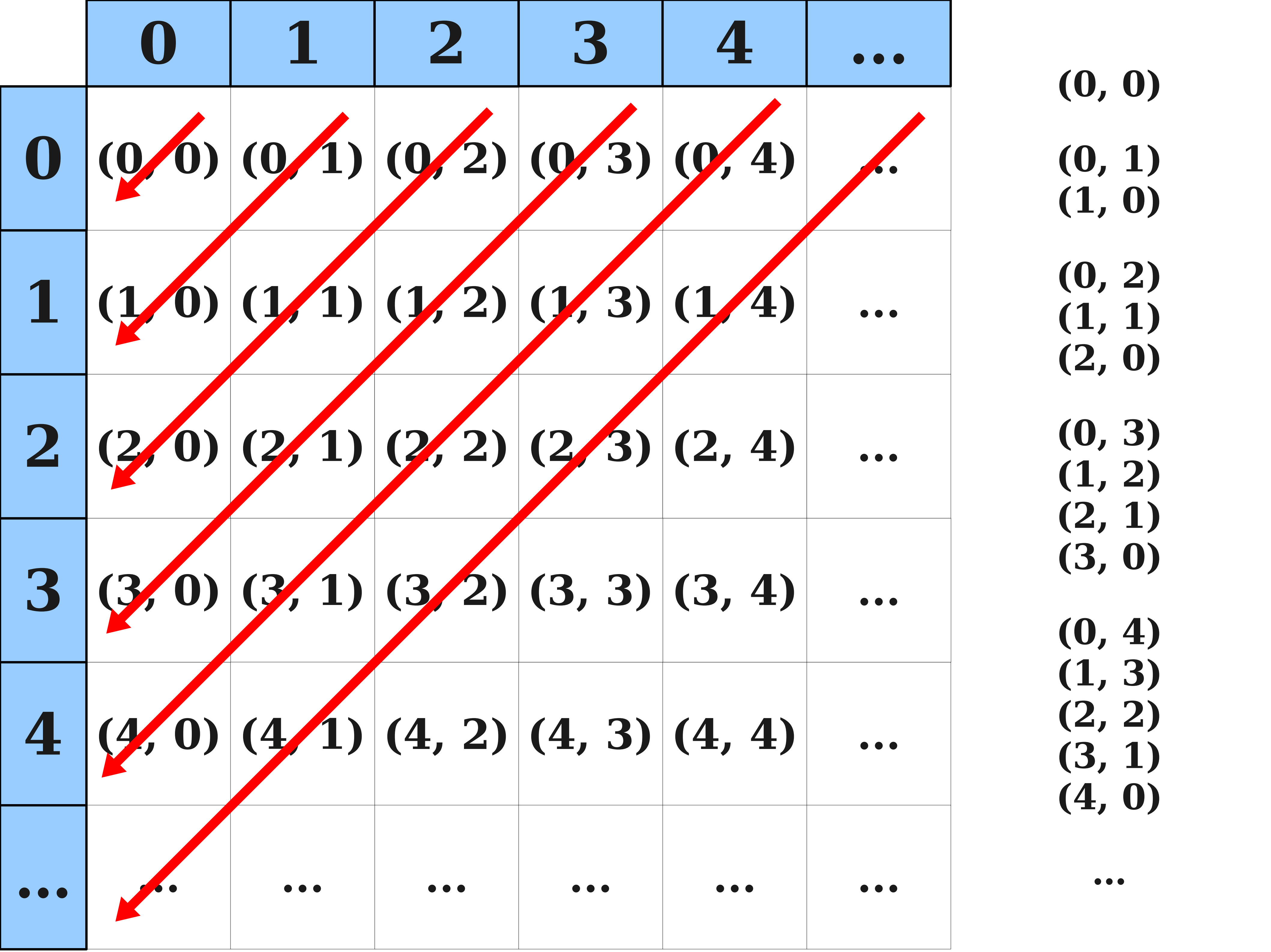


$$f : (-\pi/2, \pi/2) \to \mathbb{R}$$

$$f(x) = \tan x$$

$$|(-\pi/2, \pi/2)| = |\mathbb{R}|$$

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


0
1
2
3
4
...
0
(0, 0)
(0, 1)
(0, 2)
(0, 3)
(0, 4)
...
1
(1, 0)
(1, 1)
(1, 2)
(1, 3)
(1, 4)
...
2
(2, 0)
(2, 1)
(2, 2)
(2, 3)
(2, 4)
...
3
(3, 0)
(3, 1)
(3, 2)
(3, 3)
(3, 4)
...
4
(4, 0)
(4, 1)
(4, 2)
(4, 3)
(4, 4)
...
...
...
...
...
...
...
...
(0, 0)
(0, 1)
(1, 0)
(0, 2)
(1, 1)
(2, 0)
(0, 3)
(1, 2)
(2, 1)
(3, 0)
(0, 4)
(1, 3)
(2, 2)
(3, 1)
(4, 0)
...

Diagonal 0

$f(0, 0) = 0$

Diagonal 1

$f(0, 1) = 1$
$f(1, 0) = 2$

Diagonal 2

$f(0, 2) = 3$
$f(1, 1) = 4$
$f(2, 0) = 5$

Diagonal 3

$f(0, 3) = 6$
$f(1, 2) = 7$
$f(2, 1) = 8$
$f(3, 0) = 9$

Diagonal 4

$f(0, 4) = 10$
$f(1, 3) = 11$
$f(2, 2) = 12$
$f(3, 1) = 13$
$f(4, 0) = 14$

$$f(a, b) = \begin{array}{c}\text{The number of elements on}\\ \text{all previous diagonals}\\ + \\ \text{The index of the current}\\ \text{pair on its diagonal}\end{array}$$

Diagonal 0

$f(0, 0) = 0$

Diagonal 1

$f(0, 1) = 1$
$f(1, 0) = 2$

Diagonal 2

$f(0, 2) = 3$
$f(1, 1) = 4$
$f(2, 0) = 5$

Diagonal 3

$f(0, 3) = 6$
$f(1, 2) = 7$
$f(2, 1) = 8$
$f(3, 0) = 9$

Diagonal 4

$f(0, 4) = 10$
$f(1, 3) = 11$
$f(2, 2) = 12$
$f(3, 1) = 13$
$f(4, 0) = 14$

$$f(a, b) = (a + b)(a + b + 1) / 2 \; + \; \text{The index of the current pair on its diagonal}$$

Diagonal 0

$f(0, 0) = 0$

Diagonal 1

$f(0, 1) = 1$
$f(1, 0) = 2$

Diagonal 2

$f(0, 2) = 3$
$f(1, 1) = 4$
$f(2, 0) = 5$

Diagonal 3

$f(0, 3) = 6$
$f(1, 2) = 7$
$f(2, 1) = 8$
$f(3, 0) = 9$

Diagonal 4

$f(0, 4) = 10$
$f(1, 3) = 11$
$f(2, 2) = 12$
$f(3, 1) = 13$
$f(4, 0) = 14$

$$f(a, b) = \begin{array}{c} (a + b)(a + b + 1) / 2 \\ + \\ a \end{array}$$

Diagonal 0

$f(0, 0) = 0$

Diagonal 1

$f(0, 1) = 1$
$f(1, 0) = 2$

Diagonal 2

$f(0, 2) = 3$
$f(1, 1) = 4$
$f(2, 0) = 5$

Diagonal 3

$f(0, 3) = 6$
$f(1, 2) = 7$
$f(2, 1) = 8$
$f(3, 0) = 9$

Diagonal 4

$f(0, 4) = 10$
$f(1, 3) = 11$
$f(2, 2) = 12$
$f(3, 1) = 13$
$f(4, 0) = 14$

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

This function is called **Cantor's Pairing Function.**

$\mathbb{N}$ and $\mathbb{N}^2$

- ***Theorem:*** $|\mathbb{N}| = |\mathbb{N}^2|$.
- To formalize, can show the Cantor pairing function is injective and surjective.
- Lots of icky tricky math; see appendix at the end of the slides for details.

Announcements

Midterm Rescheduling

- Need to take the midterm at an alternate time? We'll send out an email about that later today.
- Tentative alternate times: night before the exam and morning of the exam.
- Let us know if neither of these work for you.

Recitation Sessions

- We've added a few new recitation sections to our offerings.
- Check the “Office Hours” link for more details!

Your Questions

How would we check our own proofs for “correctness” when syntax is an important part of the proof?

Could you explain how to use the phrase
“without loss of generality?”

Back to CS103...

Differing Infinities

Unequal Cardinalities

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

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

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

There are no bijections $f : A \to B$

- Need to show that *no possible function* from A to B is a bijection.

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

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

Our Goal

- We need to show the following:

There is no bijection $f : \mathbb{N} \to \mathbb{R}$

- This is a different style of proof from what we have seen before.
- To prove it, we will do the following:
  - Assume for the sake of contradiction that there is a bijection $f : \mathbb{N} \to \mathbb{R}$.
  - Derive a contradiction by showing that f cannot be surjective.
  - Conclude our assumption was wrong and that no bijection can possibly exist from $\mathbb{N}$ to $\mathbb{R}$.

The Intuition

- Suppose we have a function $f : \mathbb{N} \to \mathbb{R}$.
- We can then list off an infinite sequence of real numbers

$$r_0, r_1, r_2, r_3, r_4, \ldots$$

by setting $r_n = f(n)$.

- We will show that we can always find a real number d such that

For any $n \in \mathbb{N}$: $r_n \neq d$.

Rewriting Our Constraints

- Our goal is to find some $d \in \mathbb{R}$ such that

For any $n \in \mathbb{N}$: $r_n \neq d$.

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

$$r_0 \neq d$$

$$r_1 \neq d$$

$$r_2 \neq d$$

$$r_3 \neq d$$

$$\dots$$

The Critical Insight

- **Key Proof Idea:** Build the real number d out of infinitely many "pieces," with one piece for each number r_n.
  - Choose the 0th piece such that $r_0 \neq d$.
  - Choose the 1st piece such that $r_1 \neq d$.
  - Choose the 2nd piece such that $r_2 \neq d$.
  - Choose the 3rd piece such that $r_3 \neq d$.
  - …
- Building a "frankenreal" out of infinitely many pieces of other real numbers.

Building our “Frankenreal”

- Goal: build “frankenreal” d out of infinitely many pieces, one for each r_k.
- One idea: Define d via its decimal representation.
- Choose the digits of d as follows:
  - The 0^{th} digit of d is not the same as the 0^{th} digit of r_0.
  - The 1^{st} digit of d is not the same as the 1^{st} digit of r_1.
  - The 2^{nd} digit of d is not the same as the 2^{nd} digit of r_2.
  - …
- So $d \neq r_n$ for any $n \in \mathbb{N}$.

Building our "Frankenreal"

- If r is a real number, define $r[n]$ as follows:
  - $r[0]$ is the integer part of r.
  - $r[n]$ is the nth decimal digit of r, if $n > 0$.
- Examples:
  - $\pi[0] = 3$ $(-e)[0] = -2$ $5[0] = 5$
  - $\pi[1] = 1$ $(-e)[1] = 7$ $5[1] = 0$
  - $\pi[2] = 4$ $(-e)[2] = 1$ $5[2] = 0$
  - $\pi[3] = 1$ $(-e)[3] = 8$ $5[3] = 0$

Building our "Frankenreal"

- We can now build our frankenreal d.
- Define $d[n]$ as follows:

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

- Now, $d \neq r_n$ for any $n \in \mathbb{N}$:
  - If $r_n[n] = 0$, then $d[n] = 1$, so $r_n \neq d$.
  - If $r_n[n] \neq 0$, then $d[n] = 0$, so $r_n \neq d$.

0	$\longleftrightarrow$	8.	6	7	5	3	0	...
1	$\longleftrightarrow$	3.	1	4	1	5	9	...
2	$\longleftrightarrow$	0.	1	2	3	5	8	...
3	$\longleftrightarrow$	-1.	0	0	0	0	0	...
4	$\longleftrightarrow$	2.	7	1	8	2	8	...
5	$\longleftrightarrow$	1.	6	1	8	0	3	...
...	$\longleftrightarrow$	...	...	...	...	...	...	...

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

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

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

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

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

8.	1	2	0	2	3	...

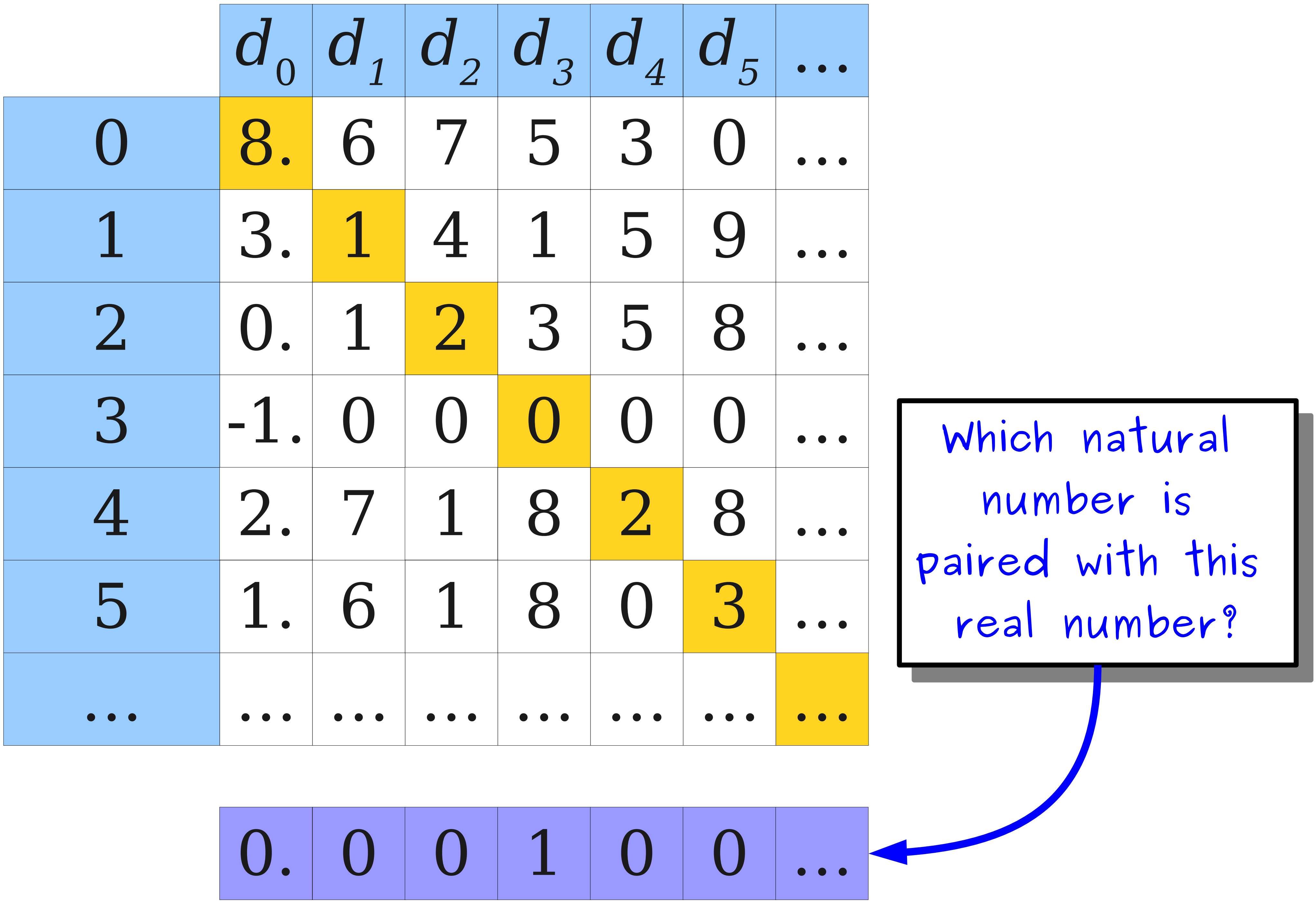
	d_0	d_1	d_2	d_3	d_4	d_5	...
0	8.	6	7	5	3	0	...
1	3.	1	4	1	5	9	...
2	0.	1	2	3	5	8	...
3	-1.	0	0	0	0	0	...
4	2.	7	1	8	2	8	...
5	1.	6	1	8	0	3	...
...	...	...	...	...	...	...	...

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

0.	0	0	1	0	0	...

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

0.	0	0	1	0	0	...



d_0 d_1 d_2 d_3 d_4 d_5 ...
0 8. 6 7 5 3 0 ...
1 3. 1 4 1 5 9 ...
2 0. 1 2 3 5 8 ...
3 -1. 0 0 0 0 0 ...
4 2. 7 1 8 2 8 ...
5 1. 6 1 8 0 3 ...
... ...
Which natural number is paired with this real number?
0. 0 0 1 0 0 ...

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

0.	0	0	1	0	0	...

Which natural number is paired with this real number?

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

0.	0	0	1	0	0	...

Which natural number is paired with this real number?

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

0.	0	0	1	0	0	…

Which natural number is paired with this real number?

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

0.	0	0	1	0	0	...

Which natural number is paired with this real number?

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

Which natural number is paired with this real number?

0.	0	0	1	0	0	...

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

0.	0	0	1	0	0	...

Which natural number is paired with this real number?

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

0.	0	0	1	0	0	...

Which natural number is paired with this real number?

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

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

Case 1: $f(n)[n] = 0$.

Case 2: $f(n)[n] \neq 0$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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

Case 2: $f(n)[n] \neq 0$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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 $f(n) \neq d$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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 $f(n) \neq d$.

In either case, we see $f(n) \neq d$. This contradicts the fact that $f(n) = d$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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 $f(n) \neq d$.

In either case, we see $f(n) \neq d$. This contradicts the fact that $f(n) = d$. We have reached a contradiction, so our assumption must have been wrong.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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 $f(n) \neq d$.

In either case, we see $f(n) \neq d$. This contradicts the fact that $f(n) = d$. We have reached a contradiction, so our assumption must have been wrong. Thus $|\mathbb{N}| \neq |\mathbb{R}|$.

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

Proof: By contradiction; suppose that $|\mathbb{N}| = |\mathbb{R}|$. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$.

Let's introduce some new notation. For any real number r, let $r[0]$ be the integer part of r, and for $n > 0$ let $r[n]$ be the nth digit in the decimal representation of r.

Now, consider the real number d defined by the following decimal representation:

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

Since $d \in \mathbb{R}$ and f is a bijection, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. Consider these two cases concerning the nth digit of $f(n)$:

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 $f(n) \neq d$.

In either case, we see $f(n) \neq d$. This contradicts the fact that $f(n) = d$. We have reached a contradiction, so our assumption must have been wrong. Thus $|\mathbb{N}| \neq |\mathbb{R}|$. ■

Diagonalization

- The proof we just worked through is called a **proof by diagonalization** and is a powerful proof technique.
- Suppose you want to show $|A| \neq |B|$:
  - Assume for contradiction that $f : A \to B$ is surjective. We'll find $d \in B$ such that $f(a) \neq d$ for any $a \in A$.
  - To do this, construct d out of "pieces," one piece taken from each $a \in A$.
  - Construct d such that the ath "piece" of d disagrees with the ath "piece" of $f(a)$.
  - Conclude that $f(a) \neq d$ for any $a \in A$.
  - Reach a contradiction, so no surjection exists from A to B.

A Silly Observation…

Ranking Cardinalities

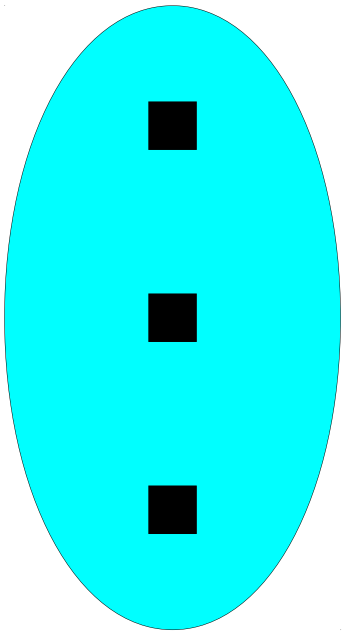
- We define $|S| \leq |T|$ as follows:

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

Ranking Cardinalities

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

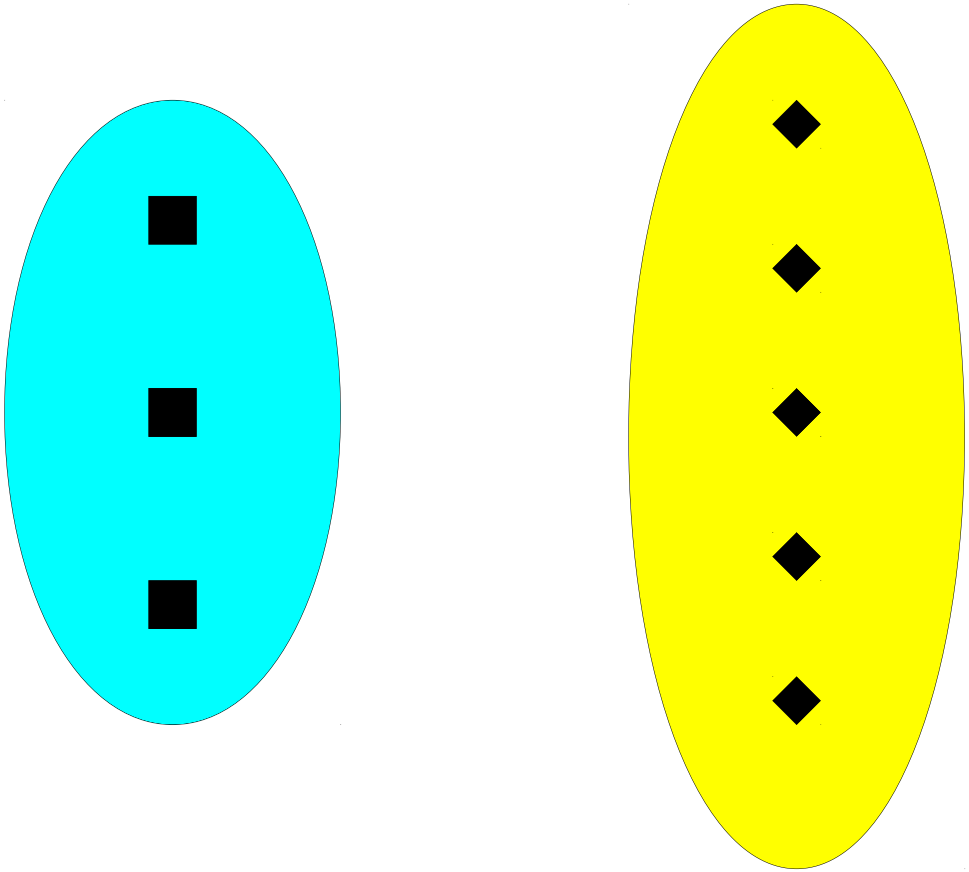
  $|S| \leq |T|$ iff there is an injection $f : S \to T$



Ranking Cardinalities

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

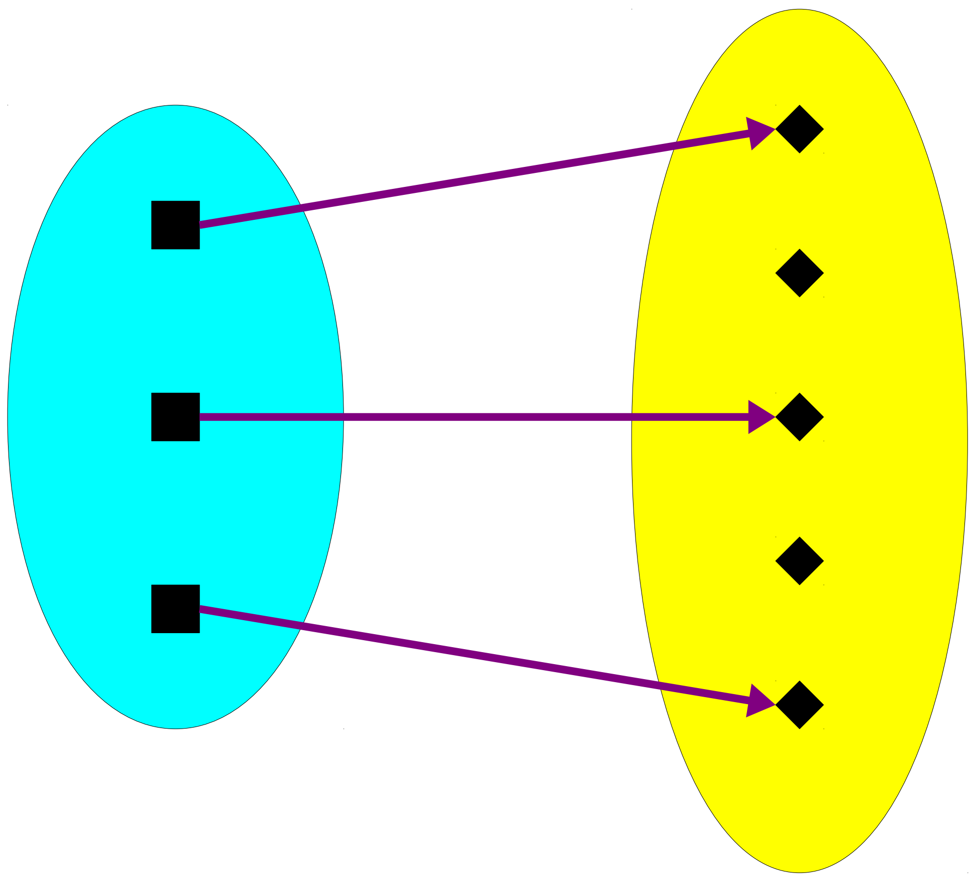
  $|S| \leq |T|$ iff there is an injection $f : S \to T$



Ranking Cardinalities

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

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



Ranking Cardinalities

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

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

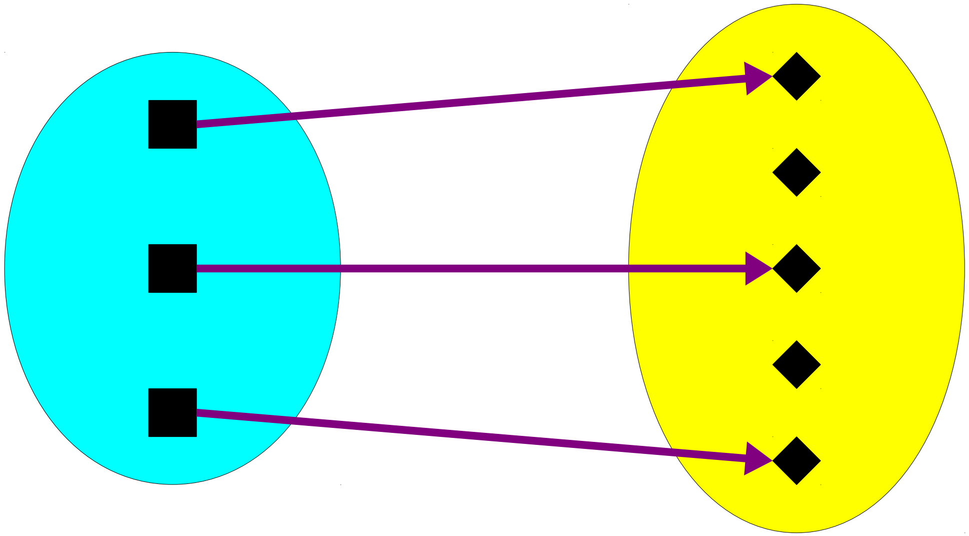
- For any sets R, S, and T:
  - $|S| \leq |S|$.
  - If $|R| \leq |S|$ and $|S| \leq |T|$, then $|R| \leq |T|$.
  - If $|S| \leq |T|$ and $|T| \leq |S|$, then $|S| = |T|$. (This is called the **Cantor-Bernstein-Schroeder theorem**, though it was originally proven by Richard Dedekind.)
  - Either $|S| \leq |T|$ or $|T| \leq |S|$.

Comparing Cardinalities

- Formally, we define < on cardinalities as

$$\mathbf{|}\boldsymbol{S}\mathbf{| < |}\boldsymbol{T}\mathbf{| \text{ iff } |}\boldsymbol{S}\mathbf{| \leq |}\boldsymbol{T}\mathbf{| \text{ and } |}\boldsymbol{S}\mathbf{| \neq |}\boldsymbol{T}\mathbf{|}$$

- 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

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

- 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:

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

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

Proof: We exhibit an injection from $\mathbb{N}$ to $\mathbb{R}$. Let $f(n) = n$. Then $f : \mathbb{N} \to \mathbb{R}$, since every natural number is also a real number.

We further claim that f is an injection. To see this, suppose that for some $n_0, n_1 \in \mathbb{N}$ that $f(n_0) = f(n_1)$. We will prove that $n_0 = n_1$. To see this, note that

$$n_0 = f(n_0) = f(n_1) = n_1$$

Thus $n_0 = n_1$, as required, so f is an injection from $\mathbb{N}$ to $\mathbb{R}$. Thus $|\mathbb{N}| \leq |\mathbb{R}|$. ■

Cantor's Theorem Revisited

Cantor's Theorem

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

$$\textbf{For every set } S\textbf{: } |S| < |\wp(S)|$$

- 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 that

For any set S: $|S| \neq |\wp(S)|$.

- Prove, for every set S, that

There is no bijection $f : S \to \wp(S)$.

- Prove this by contradiction:
  - Assume that there is a set S where there is a bijection $f : S \to \wp(S)$.
  - Derive a contradiction by showing that f is not a bijection.

The Diagonal Argument

- Suppose that we have a function $f : S \to \wp(S)$.
- We want to find a "frankenset" $D \in \wp(S)$ such that for any $x \in S$, we have $f(x) \neq D$.
- Idea: Use a diagonalization argument.
  - Build D from many "pieces," one "piece" for each $x \in S$.
  - Choose those pieces such that the xth "piece" of $f(x)$ disagrees with the xth "piece" of D.
- Hard part: What will our "pieces" be?

The Key Idea

- Want to construct D such that

The xth “piece” of $f(x)$ is different from the xth “piece” of D

- Idea: Have the xth “piece” of D be whether or not D contains x.
- Define D such that

D contains x iff $f(x)$ does not contain x

- More formally, we want

$$x \in D \quad \text{iff} \quad x \notin f(x)$$

- Most formally:

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

x_0

x_1

x_2

x_3

x_4

x_5

$\ldots$

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

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

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

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

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

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

$$\dots$$

x_0	x_1	x_2	x_3	x_4	x_5	…

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

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

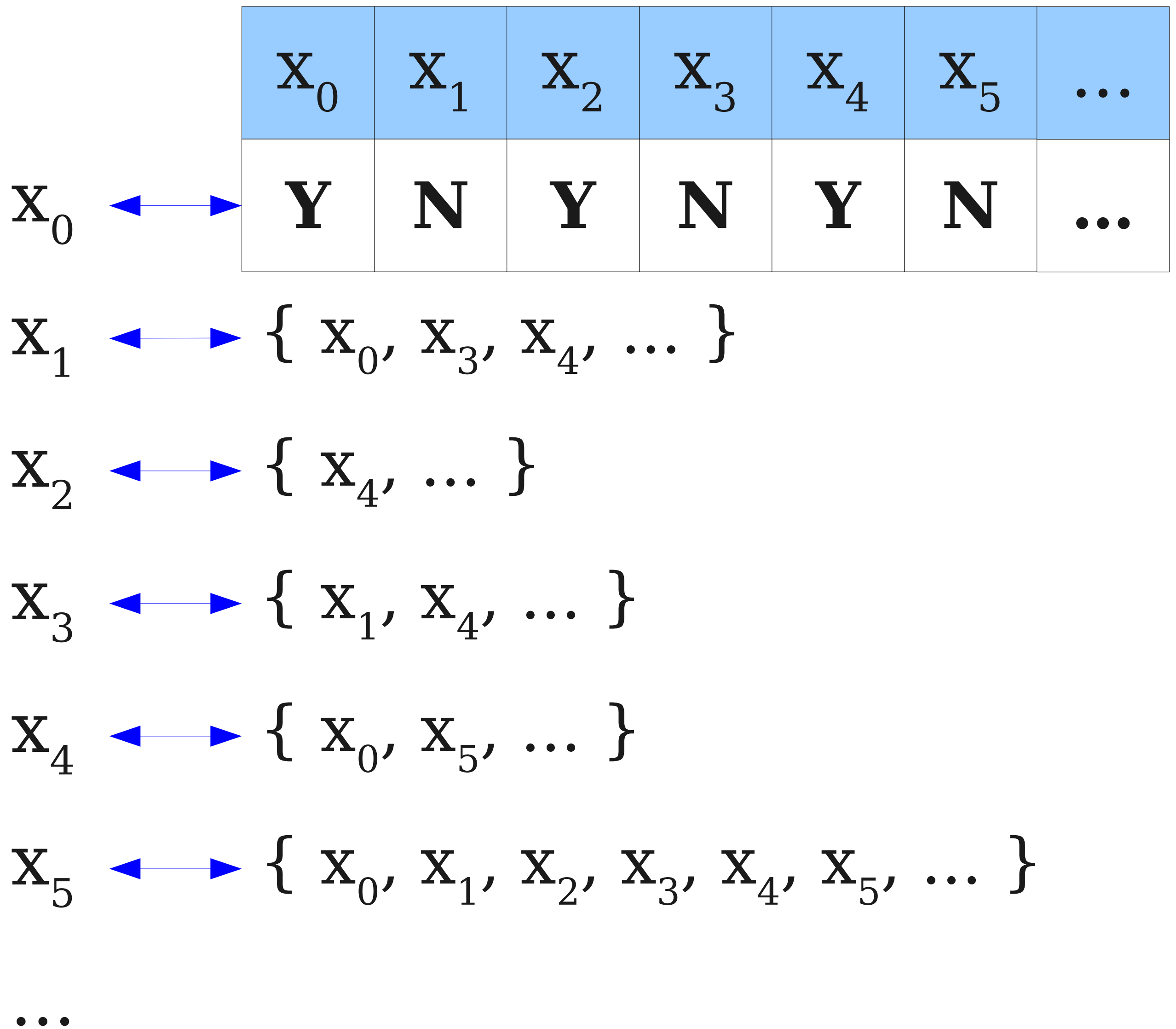
$$x_2 \longleftrightarrow \{ x_4, \dots \}$$

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

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

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

…



x_0 x_1 x_2 x_3 x_4 x_5 ...
x_0 Y N Y N Y N ...
x_1 $\{x_0, x_3, x_4, \ldots\}$
x_2 $\{x_4, \ldots\}$
x_3 $\{x_1, x_4, \ldots\}$
x_4 $\{x_0, x_5, \ldots\}$
x_5 $\{x_0, x_1, x_2, x_3, x_4, x_5, \ldots\}$
...

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \longleftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	**…**
$x_1 \longleftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	**…**

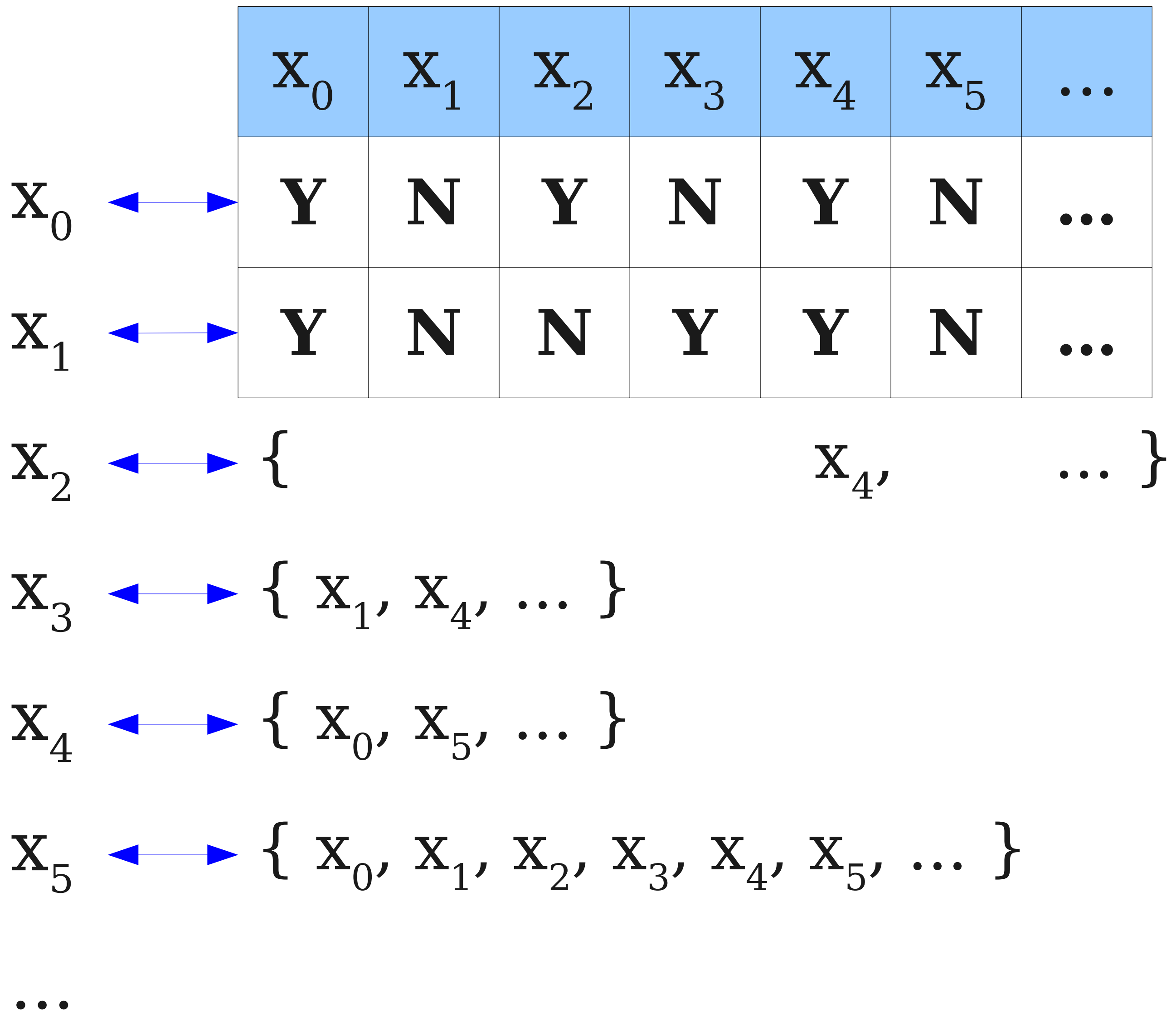
$x_2 \longleftrightarrow \{\ x_4,\ \dots\ \}$

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

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

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

…



x0 x1 x2 x3 x4 x5 …
x0 ↔ Y N Y N Y N …
x1 ↔ Y N N Y Y N …
x2 ↔ { x4, … }
x3 ↔ { x1, x4, … }
x4 ↔ { x0, x5, … }
x5 ↔ { x0, x1, x2, x3, x4, x5, … }
…

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
$x_1 \leftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
$x_2 \leftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	…

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

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

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

…

		x_0	x_1	x_2	x_3	x_4	x_5	…
x_0	$\leftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	…
x_1	$\leftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	…
x_2	$\leftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	…

$$x_3 \leftrightarrow \{ \quad x_1, \quad x_4, \quad \ldots \}$$

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

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

…

		x_0	x_1	x_2	x_3	x_4	x_5	$\ldots$
x_0	$\longleftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	**...**
x_1	$\longleftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	**...**
x_2	$\longleftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	**...**
x_3	$\longleftrightarrow$	**N**	**Y**	**N**	**N**	**Y**	**N**	**...**

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

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

$\ldots$

	x_0	x_1	x_2	x_3	x_4	x_5	…
$x_0 \longleftrightarrow$	**Y**	**N**	**Y**	**N**	**Y**	**N**	**…**
$x_1 \longleftrightarrow$	**Y**	**N**	**N**	**Y**	**Y**	**N**	**…**
$x_2 \longleftrightarrow$	**N**	**N**	**N**	**N**	**Y**	**N**	**…**
$x_3 \longleftrightarrow$	**N**	**Y**	**N**	**N**	**Y**	**N**	**…**
$x_4 \longleftrightarrow$	**Y**	**N**	**N**	**N**	**N**	**Y**	**…**

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

…

	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**	...
...	...	...	...	...	...	...	...

	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**	...
...	...	...	...	...	...	...	...

	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**	...
...	...	...	...	...	...	...	...

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

Flip all Y's to N's and vice-versa to get a new set

N	**Y**	**Y**	**Y**	**Y**	**N**	…

	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**	…
…	…	…	…	…	…	…	…

$\{\ \mathbf{x_1},\ \mathbf{x_2},\ \mathbf{x_3},\ \mathbf{x_4},\ \dots\ \}$

Flip all Y's to N's and vice-versa to get a new 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**	**…**

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**	…

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**	…

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**	…

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**	…

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**	…

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**	…

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**	…

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**	…

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**	…

Which row in the table is paired with this set?

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{\ x \in S \mid x \notin f(x)\ \}$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$.

Case 2: $y \in f(y)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$.

Case 2: $y \in f(y)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$. Since $y \in f(y)$ and $y \notin D$, we see $f(y) \neq D$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$. Since $y \in f(y)$ and $y \notin D$, we see $f(y) \neq D$.

In both cases we find $f(y) \neq D$, contradicting $f(y) = D$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$. Since $y \in f(y)$ and $y \notin D$, we see $f(y) \neq D$.

In both cases we find $f(y) \neq D$, contradicting $f(y) = D$. We have reached a contradiction, so our assumption must have been wrong.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$. Since $y \in f(y)$ and $y \notin D$, we see $f(y) \neq D$.

In both cases we find $f(y) \neq D$, contradicting $f(y) = D$. We have reached a contradiction, so our assumption must have been wrong. Thus for every set S, we have $|S| \neq |\wp(S)|$.

Theorem: For any set S, we have $|S| \neq |\wp(S)|$.

Proof: By contradiction; assume that there is a set S where $|S| = |\wp(S)|$. This means there is a bijection $f : S \to \wp(S)$. Define the set $D = \{ x \in S \mid x \notin f(x) \}$. Since every $x \in D$ also satisfies $x \in S$, we see that $D \subseteq S$. Thus $D \in \wp(S)$.

Since $D \in \wp(S)$ and f is a bijection, there is some $y \in S$ where $f(y) = D$. Now, either $y \in f(y)$ or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \notin f(y)$. By our definition of D, we have $y \in D$. Since $y \notin f(y)$ and $y \in D$, we see $f(y) \neq D$.

Case 2: $y \in f(y)$. By our definition of D, we have $y \notin D$. Since $y \in f(y)$ and $y \notin D$, we see $f(y) \neq D$.

In both cases we find $f(y) \neq D$, contradicting $f(y) = D$. We have reached a contradiction, so our assumption must have been wrong. Thus for every set S, we have $|S| \neq |\wp(S)|$. ■

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.

Next Time

- **Propositional Logic**
  - How do we reason about how different statements entail one another?
- **First-Order Logic**
  - How do we reason about collections of objects?

Appendix: Proof that $|\mathbb{N}^2| = |\mathbb{N}|$

Proving Surjectivity

- Given just the definition of our function:

  $$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

  It is not at all clear that every natural number can be generated.
- However, given our intuition of how the function works (crawling along diagonals), we can start to formulate a proof of surjectivity.

Proving Surjectivity

$$\boldsymbol{f(a, b) = (a + b)(a + b + 1) / 2 + a}$$

- What pair of numbers maps to 137?
- We can figure this out by first trying to figure out what diagonal this would be in.

Proving Surjectivity

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

- What pair of numbers maps to 137?
- We can figure this out by first trying to figure out what diagonal this would be in.

	0	**1**	**2**
0	**(0, 0)**	**(0, 1)**	**(0, 2)**
1	**(1, 0)**	**(1, 1)**	**(1, 2)**
2	**(2, 0)**	**(2, 1)**	**(2, 2)**

Proving Surjectivity

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

- What pair of numbers maps to 137?
- We can figure this out by first trying to figure out what diagonal this would be in.

	0	**1**	**2**
0	**(0, 0)**	**(0, 1)**	**(0, 2)**
1	**(1, 0)**	**(1, 1)**	**(1, 2)**
2	**(2, 0)**	**(2, 1)**	**(2, 2)**

Proving Surjectivity

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

- What pair of numbers maps to 137?
- We can figure this out by first trying to figure out what diagonal this would be in.

	0	**1**	**2**
0	**(0, 0)**	**(0, 1)**	**(0, 2)**
1	**(1, 0)**	**(1, 1)**	**(1, 2)**
2	**(2, 0)**	**(2, 1)**	**(2, 2)**

Total number of elements before

Row 0: 0
Row 1: 1
Row 2: 3
Row 3: 6
Row 4: 10
...
Row m: $m(m + 1) / 2$

Proving Surjectivity

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

- What pair of numbers maps to 137?
- We can figure this out by first trying to figure out what diagonal this would be in.
  - Answer: Diagonal 16, since there are 136 pairs that come before it.
- Now that we know the diagonal, we can figure out the index into that diagonal.
  - 137 – 136 = 1.
- So we'd expect the first entry of diagonal 16 to map to 137.

$$f(1, 15) = 16 \times 17 / 2 + 1 = 136 + 1 = 137$$

Generalizing Into a Proof

- We can generalize this logic as follows.
- To find a pair that maps to n:
  - Find which diagonal the number is in by finding the largest d such that

$$d(d + 1) / 2 \leq n$$

  - Find which index the in that diagonal it is in by subtracting the starting position of that diagonal:

$$k = n - d(d + 1) / 2$$

  - The kth entry of diagonal d is the answer:

$$f(k, d - k) = n$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$.

Intuitively, d is the diagonal containing n.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$.

Intuition: k is the position within this diagonal.

Now, we need to rigorously establish that we came up with a legal pair, and that the pair actually maps to n.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$.

We need to formalize our intuition by showing that d gives an index on this diagonal.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$.

> If m and n are natural numbers or integers, then $m < n$ iff $m + 1 \leq n$. This fact is remarkably useful in proofs on $\mathbb{N}$ or $\mathbb{Z}$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$d + 1 \leq k$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$d + 1 \leq k$$
$$d + 1 \leq n - d(d + 1) / 2$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$d + 1 \leq k$$
$$d + 1 \leq n - d(d + 1) / 2$$
$$d + 1 + d(d + 1) / 2 \leq n$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$d + 1 \leq k$$
$$d + 1 \leq n - d(d + 1) / 2$$
$$d + 1 + d(d + 1) / 2 \leq n$$
$$(2(d + 1) + d(d + 1)) / 2 \leq n$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$d + 1 \leq k$$
$$d + 1 \leq n - d(d + 1) / 2$$
$$d + 1 + d(d + 1) / 2 \leq n$$
$$(2(d + 1) + d(d + 1)) / 2 \leq n$$
$$(d + 1)(d + 2) / 2 \leq n$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k\\
&d + 1 \leq n - d(d + 1) / 2\\
&d + 1 + d(d + 1) / 2 \leq n\\
&(2(d + 1) + d(d + 1)) / 2 \leq n\\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$.

We have a valid pair! All that's left to do now is to show that index k on diagonal d maps to n.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$f(k, d - k) = (k + d - k)(k + d - k + 1) / 2 + k$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k
\end{aligned}$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$
\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k \\
&= d(d + 1) / 2 + n - d(d + 1) / 2
\end{aligned}
$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$
\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k \\
&= d(d + 1) / 2 + n - d(d + 1) / 2 \\
&= n
\end{aligned}
$$

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$
\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k \\
&= d(d + 1) / 2 + n - d(d + 1) / 2 \\
&= n
\end{aligned}
$$

Thus there is a pair $(a, b) \in \mathbb{N}^2$ (namely, $(k, d - k)$) such that $f(a, b) = n$.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$
\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k \\
&= d(d + 1) / 2 + n - d(d + 1) / 2 \\
&= n
\end{aligned}
$$

Thus there is a pair $(a, b) \in \mathbb{N}^2$ (namely, $(k, d - k)$) such that $f(a, b) = n$. Consequently, f is surjective.

Lemma: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$ be a function from $\mathbb{N}^2$ to $\mathbb{N}$. Then f is surjective.

Proof: Consider any $n \in \mathbb{N}$. We will show that there exists a pair $(a, b) \in \mathbb{N}^2$ such that $f(a, b) = n$.

Consider the largest $d \in \mathbb{N}$ such that $d(d + 1) / 2 \leq n$. Then, let $k = n - d(d + 1) / 2$. Since $d(d + 1) / 2 \leq n$, we have that $k \in \mathbb{N}$. We further claim that $k \leq d$. To see this, suppose for the sake of contradiction that $k > d$. Consequently, $k \geq d + 1$. This means that

$$
\begin{aligned}
&d + 1 \leq k \\
&d + 1 \leq n - d(d + 1) / 2 \\
&d + 1 + d(d + 1) / 2 \leq n \\
&(2(d + 1) + d(d + 1)) / 2 \leq n \\
&(d + 1)(d + 2) / 2 \leq n
\end{aligned}
$$

But this means that d is not the largest natural number satisfying the inequality $d(d + 1) / 2 \leq n$, a contradiction. Thus our assumption must have been wrong, so $k \leq d$.

Since $k \leq d$, we have that $0 \leq k - d$, so $k - d \in \mathbb{N}$. Now, consider the value of $f(k, d - k)$. This is

$$
\begin{aligned}
f(k, d - k) &= (k + d - k)(k + d - k + 1) / 2 + k \\
&= d(d + 1) / 2 + k \\
&= d(d + 1) / 2 + n - d(d + 1) / 2 \\
&= n
\end{aligned}
$$

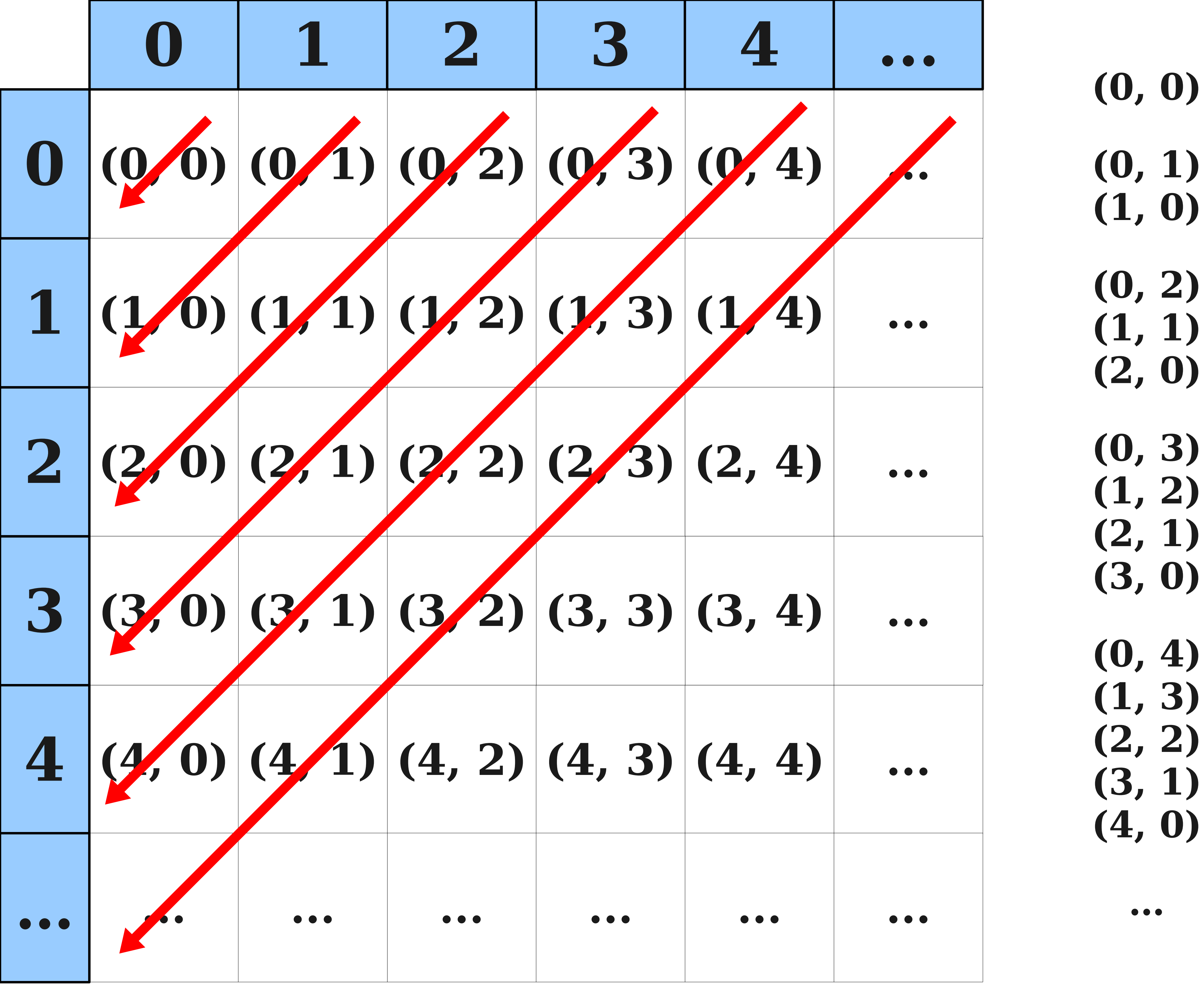
Thus there is a pair $(a, b) \in \mathbb{N}^2$ (namely, $(k, d - k)$) such that $f(a, b) = n$. Consequently, f is surjective. ■

Proving Injectivity

- Given the function

$$\boldsymbol{f(a, b) = (a + b)(a + b + 1) / 2 + a}$$

- It is not at all obvious that f is injective.
- We'll have to use our intuition to figure out why this would be.



0 1 2 3 4 ...
0 (0, 0) (0, 1) (0, 2) (0, 3) (0, 4) ...
1 (1, 0) (1, 1) (1, 2) (1, 3) (1, 4) ...
2 (2, 0) (2, 1) (2, 2) (2, 3) (2, 4) ...
3 (3, 0) (3, 1) (3, 2) (3, 3) (3, 4) ...
4 (4, 0) (4, 1) (4, 2) (4, 3) (4, 4) ...
... ...
(0, 0)
(0, 1)
(1, 0)
(0, 2)
(1, 1)
(2, 0)
(0, 3)
(1, 2)
(2, 1)
(3, 0)
(0, 4)
(1, 3)
(2, 2)
(3, 1)
(4, 0)
...

Proving Injectivity

$$\boldsymbol{f(a, b) = (a + b)(a + b + 1) / 2 + a}$$

- Suppose that $f(a, b) = f(c, d)$. We need to prove $(a, b) = (c, d)$.
- Our proof will proceed in two steps:
  - First, we'll prove that (a, b) and (c, d) have to be in the same diagonal.
  - Next, using the fact that they're in the same diagonal, we'll show that they're at the same position within that diagonal.
  - From this, we can conclude $(a, b) = (c, d)$.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

The point of this lemma is to let us "read off" what diagonal we are in just by looking at **a** and **b**. We will need this in a second.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \end{aligned}$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$m'(m' + 1) / 2 \geq (a + b + 1)(a + b + 2) / 2$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$
\begin{aligned}
f(a, b) &= (a + b)(a + b + 1) / 2 + a \\
&\geq (a + b)(a + b + 1) / 2 \\
&= m(m + 1) / 2
\end{aligned}
$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$
\begin{aligned}
m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\
&= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2
\end{aligned}
$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \end{aligned}$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \\ &> (a + b)(a + b + 1) / 2 + a \end{aligned}$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \\ &> (a + b)(a + b + 1) / 2 + a \\ &= f(a, b) \end{aligned}$$

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \\ &> (a + b)(a + b + 1) / 2 + a \\ &= f(a, b) \end{aligned}$$

Thus m' does not satisfy the inequality.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \\ &> (a + b)(a + b + 1) / 2 + a \\ &= f(a, b) \end{aligned}$$

Thus m' does not satisfy the inequality. Consequently, $m = a + b$ is the largest natural number satisfying the inequality.

Lemma: Suppose $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then the largest $m \in \mathbb{N}$ for which $m(m + 1) / 2 \leq f(a, b)$ is given by $m = a + b$.

Proof: First, we show that $m = a + b$ satisfies the above inequality. Note that if $m = a + b$, we have

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &\geq (a + b)(a + b + 1) / 2 \\ &= m(m + 1) / 2 \end{aligned}$$

So m satisfies the inequality.

Next, we will show that any $m' \in \mathbb{N}$ with $m' > a + b$ will not satisfy the inequality. Take any $m' \in \mathbb{N}$ where $m' > a + b$. This means that $m' \geq a + b + 1$. Consequently, we have

$$\begin{aligned} m'(m' + 1) / 2 &\geq (a + b + 1)(a + b + 2) / 2 \\ &= ((a + b)(a + b + 2) + 2(a + b + 1)) / 2 \\ &= (a + b)(a + b + 1) / 2 + a + b + 1 \\ &> (a + b)(a + b + 1) / 2 + a \\ &= f(a, b) \end{aligned}$$

Thus m' does not satisfy the inequality. Consequently, $m = a + b$ is the largest natural number satisfying the inequality. ■

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$.

Intuitively, this proves that (a, b) and (c, d) belong to the same diagonal.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$f(a, b) = (a + b)(a + b + 1) / 2 + a$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \end{aligned}$$

This step works because we know that any number $\boldsymbol{n}$ bigger than $\boldsymbol{a + b}$ doesn't satisfy

$$\boldsymbol{n(n + 1) / 2 \leq f(a, b)}$$

This means that

$$\boldsymbol{f(a, b) < n(n + 1) / 2.}$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \end{aligned}$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$
\begin{aligned}
f(a, b) &= (a + b)(a + b + 1) / 2 + a \\
&< (c + d)(c + d + 1) / 2 \\
&\leq (c + d)(c + d + 1) / 2 + c \\
&= f(c, d)
\end{aligned}
$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$.

Now that we've got these points in the same diagonal, we just need to show that they have the same index.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$
$$(a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$
$$(a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c$$
$$(a + b)(a + b + 1) / 2 + a = (a + b)(a + b + 1) / 2 + c$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$
$$(a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c$$
$$(a + b)(a + b + 1) / 2 + a = (a + b)(a + b + 1) / 2 + c$$
$$a = c$$

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$
$$(a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c$$
$$(a + b)(a + b + 1) / 2 + a = (a + b)(a + b + 1) / 2 + c$$
$$a = c$$

Since $a = c$ and $a + b = c + d$, we have that $b = d$.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$f(a, b) = f(c, d)$$
$$(a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c$$
$$(a + b)(a + b + 1) / 2 + a = (a + b)(a + b + 1) / 2 + c$$
$$a = c$$

Since $a = c$ and $a + b = c + d$, we have that $b = d$. Thus $(a, b) = (c, d)$, as required.

Theorem: Let $f(a, b) = (a + b)(a + b + 1) / 2 + a$. Then f is injective.

Proof: Consider any $(a, b), (c, d) \in \mathbb{N}^2$ such that $f(a, b) = f(c, d)$. We will show that $(a, b) = (c, d)$.

First, we will show that $a + b = c + d$. To do this, assume for the sake of contradiction that $a + b \neq c + d$. Then either $a + b < c + d$ or $a + b > c + d$. Assume without loss of generality that $a + b < c + d$.

By our lemma, we know that $m = a + b$ is the largest natural number such that $f(a, b) \leq m(m + 1) / 2$. Since $a + b < c + d$, this means that

$$\begin{aligned} f(a, b) &= (a + b)(a + b + 1) / 2 + a \\ &< (c + d)(c + d + 1) / 2 \\ &\leq (c + d)(c + d + 1) / 2 + c \\ &= f(c, d) \end{aligned}$$

But this means that $f(a, b) < f(c, d)$, contradicting that $f(a, b) = f(c, d)$. We have reached a contradiction, so our assumption must have been wrong. Thus $a + b = c + d$. Given this, we have that

$$\begin{gathered} f(a, b) = f(c, d) \\ (a + b)(a + b + 1) / 2 + a = (c + d)(c + d + 1) / 2 + c \\ (a + b)(a + b + 1) / 2 + a = (a + b)(a + b + 1) / 2 + c \\ a = c \end{gathered}$$

Since $a = c$ and $a + b = c + d$, we have that $b = d$. Thus $(a, b) = (c, d)$, as required. ■