Cardinality
and
The Nature of Infinity

Recap from Last Time

Functions

- A **function** f is a mapping such that every value in A is associated with a single value in B.
  - For every $a \in A$, there exists some $b \in B$ with $f(a) = b$.
  - If $f(a) = b_0$ and $f(a) = b_1$, then $b_0 = b_1$.
- If f is a function from A to B, we call A the **domain** of f andl B the **codomain** of f.
- We denote that f is a function from A to B by writing

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

Injective Functions

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

$$\textbf{If } f(x_0) = f(x_1)\textbf{, then } x_0 = x_1$$

- An intuition: injective functions label the objects from A using names from B.

Surjective Functions

- A function $f : A \to B$ is called **surjective** (or **onto**) iff each element of the codomain has at least one element of the domain associated with it.
  - A function with this property is called a **surjection**.
- Formally:

For any $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$.

- An intuition: surjective functions cover every element of B with at least one element of A.

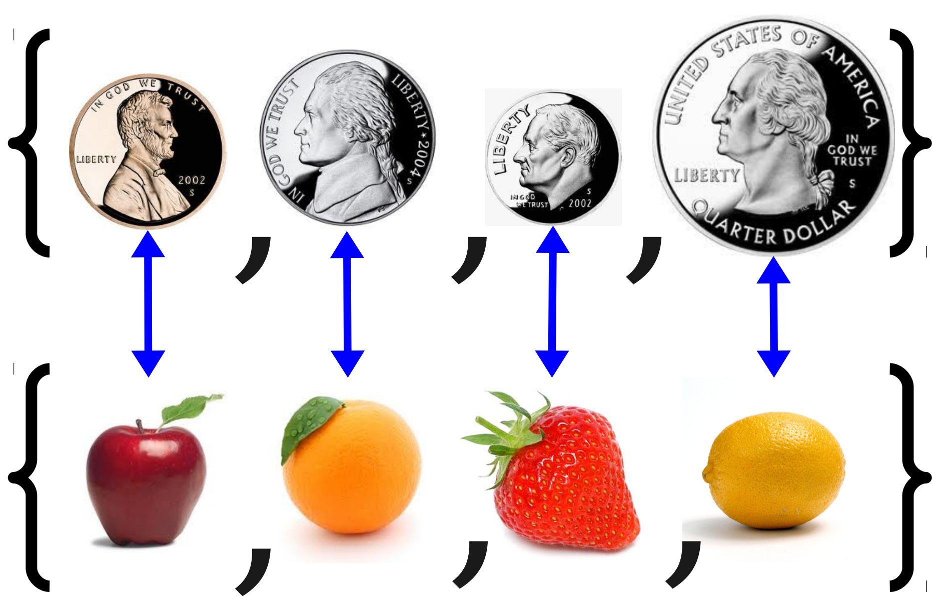
Bijections

- A function that associates each element of the codomain with a unique element of the domain is called **bijective**.
  - Such a function is a **bijection**.
- Formally, a bijection is a function that is both **injective** and **surjective**.
- A bijection is a one-to-one correspondence between two 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 is a bijection $f : S \to T$



The Nature of Infinity

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	...

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	...

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ & \end{cases}$$

Infinite Cardinalities

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	...
$\mathbb{Z}$	0	-1	1	-2	2	-3	3	-4	4	...

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x-1 & \text{otherwise} \end{cases}$$

Theorem: $|\mathbb{Z}| = |\mathbb{N}|$.
Proof: We exhibit a bijection from $\mathbb{Z}$ to $\mathbb{N}$. Let $f : \mathbb{Z} \to \mathbb{N}$ be defined as follows:

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{otherwise} \end{cases}$$

First, we prove this is a legal function from $\mathbb{Z}$ to $\mathbb{N}$. Consider any $x \in \mathbb{Z}$. Note that if $x \geq 0$, then $f(x) = 2x$. Since in this case x is nonnegative, $2x$ is a natural number. Thus $f(x) \in \mathbb{N}$. Otherwise, $x < 0$, so $f(x) = -2x - 1 = 2(-x) - 1$. Since $x < 0$, we have $-x > 0$, so $-x \geq 1$. Then $f(x) = 2(-x) - 1 \geq 2 - 1 = 1$. Thus $f(x)$ is a positive integer, so $f(x) \in \mathbb{N}$. In either case $f(x) \in \mathbb{N}$, so $f : \mathbb{Z} \to \mathbb{N}$.

Next, we prove f is injective. Suppose that $f(x) = f(y)$. We will prove that $x = y$. Note that, by construction, $f(z)$ is even iff z is nonnegative. Since $f(x) = f(y)$, we know x and y must have the same sign. We consider two cases:

Case 1: x and y are nonnegative. Then $f(x) = 2x$ and $f(y) = 2y$. Since $f(x) = f(y)$, we have $2x = 2y$. Thus $x = y$.

Case 2: x and y are negative. Then $f(x) = -2x - 1$ and $f(y) = -2y - 1$. Since $f(x) = f(y)$, we have $-2x - 1 = -2y - 1$, so $x = y$.

Finally, we prove f is surjective. Consider any $n \in \mathbb{N}$. We will prove that there is some $x \in \mathbb{Z}$ such that $f(x) = n$. We consider two cases:

Case 1: n is even. Then $n / 2$ is a nonnegative integer. Moreover, $f(n / 2) = 2(n / 2) = n$.

Case 2: n is odd. Then $-(n + 1) / 2$ is a negative integer. Moreover, $f(-(n + 1) / 2) = -2(-(n + 1) / 2) - 1 = n + 1 - 1 = n$.

Since f is injective and surjective, it is a bijection. Thus $|\mathbb{Z}| = |\mathbb{N}|$. ■

Why This Matters

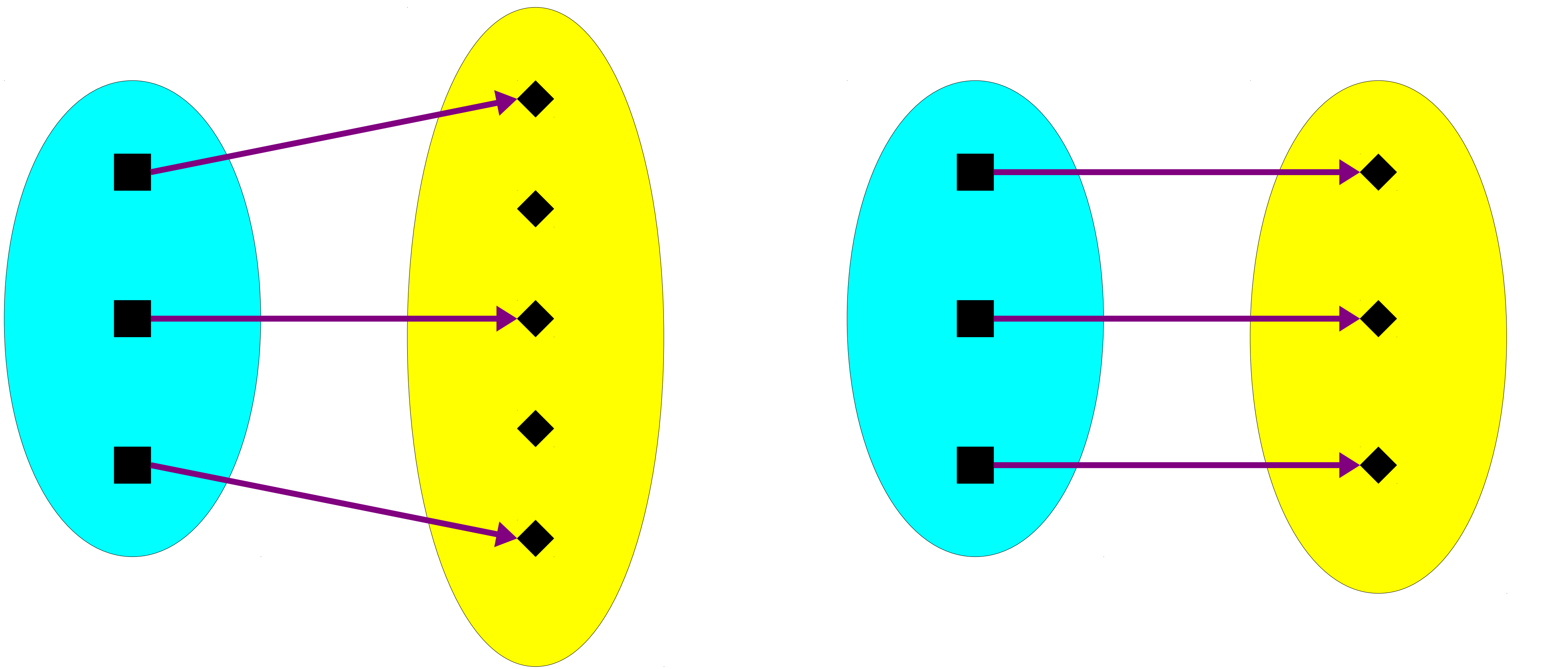
- Note the thought process from this proof:
  - Start by drawing a picture to get an intuition.
  - Convert the picture into a mathematical object (here, a function).
  - Prove the object has the desired properties.
- This technique is at the heart of mathematics.
- We will use it extensively throughout the rest of this lecture.

Cantor's Theorem Revisited

Comparing Cardinalities

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

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

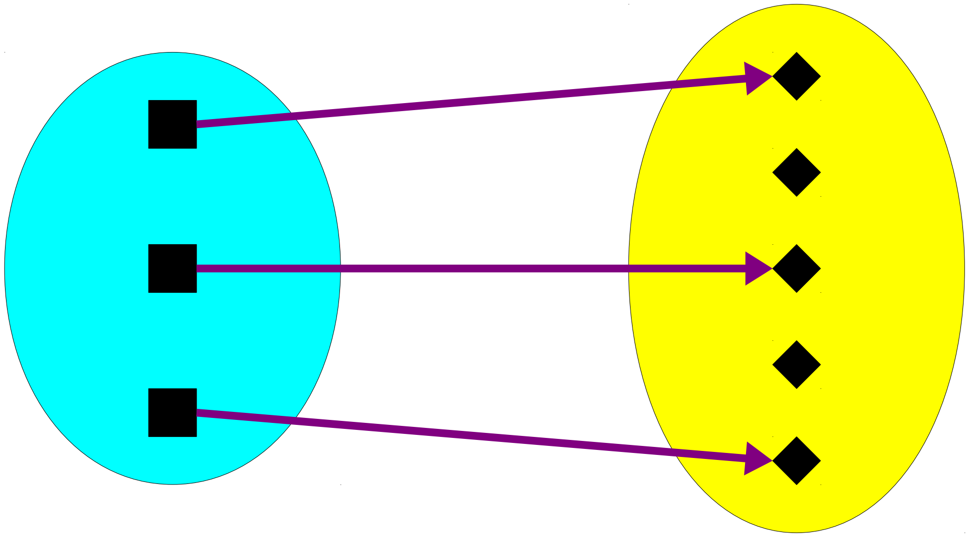


Comparing Cardinalities

- 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*.



Cantor's Theorem

- **Cantor's Theorem** states that

$$\text{For every set } S,\ |S| < |\wp(S)|$$

- 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.

Lemma: For any set S, $|S| \leq |\wp(S)|$.

Proof: Consider any set S. We show that there is an injection $f : S \to \wp(S)$. Define $f(x) = \{x\}$.

To see that $f(x)$ is a legal function from S to $\wp(S)$, consider any $x \in$ S. Then $\{x\} \subseteq S$, so $\{x\} \in \wp(S)$. This means that $f(x) \in \wp(S)$, so f is a valid function from S to $\wp(S)$.

To see that f is injective, consider any x_0 and x_1 such that $f(x_0) = f(x_1)$. We prove that $x_0 = x_1$. To see this, note that if $f(x_0) = f(x_1)$, then $\{x_0\} = \{x_1\}$. Since two sets are equal iff their elements are equal, this means that $x_0 = x_1$ as required. Thus f is an injection from S to $\wp(S)$, so $|S| \leq |\wp(S)|$. ■

The Key Step

- We now need to show that

For any set S, $|S| \neq |\wp(S)|$

- By definition, $|S| = |\wp(S)|$ iff there exists a bijection $f : S \to \wp(S)$.
- This means that

$|S| \neq |\wp(S)|$ iff there is no bijection $f : S \to \wp(S)$

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

	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**	…

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**	…

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?

Formalizing the Diagonal Argument

- Proof by contradiction; assume there is a bijection $f : S \to \wp(S)$.
- The diagonal argument shows that f cannot be a bijection:
  - Construct the table given the bijection f.
  - Construct the complemented diagonal.
  - Show that the complemented diagonal cannot appear anywhere in the table.
  - Conclude, therefore, that f is not a bijection.

	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**	**Y**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**N**	**Y**	**N**	**N**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**N**	**Y**	**N**	…

$f(\mathbf{x_0}) = \{\ \mathbf{x_0}, x_2, x_4, \ldots\ \}$

$f(x_1) = \{\ x_0, x_3, x_4, \ldots\ \}$

$f(x_2) = \{\ x_4, \ldots\ \}$

$f(\mathbf{x_3}) = \{\ x_1, \mathbf{x_3}, x_4, \ldots\ \}$

$f(x_4) = \{\ x_1, x_5, \ldots\ \}$

$f(\mathbf{x_5}) = \{\ x_1, x_4, \mathbf{x_5}, \ldots\ \}$

	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**	**Y**	**Y**	**N**	…
x_4	**Y**	**N**	**N**	**N**	**N**	**Y**	…
x_5	**N**	**Y**	**N**	**N**	**Y**	**Y**	…
…	…	…	…	…	…	…	…

N	**Y**	**Y**	**N**	**Y**	**N**	…

$$f(x_0) = \{\ x_0,\ x_2,\ x_4,\ \dots\ \}$$

$$f(\mathbf{x_1}) = \{\ x_0,\ x_3,\ x_4,\ \dots\ \}$$

$$f(\mathbf{x_2}) = \{\ x_4,\ \dots\ \}$$

$$f(x_3) = \{\ x_1,\ x_3,\ x_4,\ \dots\ \}$$

$$f(\mathbf{x_4}) = \{\ x_1,\ x_5,\ \dots\ \}$$

$$f(x_5) = \{\ x_1,\ x_4,\ x_5,\ \dots\ \}$$

The **diagonal set** D is the set

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

There is no longer a dependence on the existence of the two-dimensional table.

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

Proof: By contradiction; assume that there exists a set S such that $|S| = |\wp(S)|$. This means that there exists a bijection $f : S \to \wp(S)$. Consider the set $D = \{ x \in S \mid x \notin f(x) \}$. Note that $D \subseteq S$, since by construction every $x \in D$ satisfies $x \in S$.

Since f is a bijection, it is surjective, so there must be some $y \in S$ such that $f(y) = D$. Now, either $y \in f(y)$, or $y \notin f(y)$. We consider these cases separately:

Case 1: $y \in f(y)$. By our definition of D, this means that $y \notin D$. However, since $y \in f(y)$ and $f(y) = D$, we have $y \in D$. We have reached a contradiction.

Case 2: $y \notin f(y)$. By our definition of D, this means that $y \in D$. However, since $y \notin f(y)$ and $f(y) = D$, we have $y \notin D$. We have reached a contradiction.

In either case we reach a contradiction, so our assumption must have been wrong. Thus for every set S, we have that $|S| \neq |\wp(S)|$. ■

***Theorem* (Cantor's Theorem)**: For any set S, we have $|S| < |\wp(\mathrm{S})|$.

Proof: Consider any set S. By our first lemma, we have that $|S| \leq |\wp(S)|$. By our second lemma, we have that $|S| \neq |\wp(S)|$. Thus $|S| < |\wp(S)|$. ■

Why All This Matters

- The intuition behind a result is often more important than the result itself.
- Given the intuition, you can usually reconstruct the proof.
- Given just the proof, it is almost impossible to reconstruct the intuition.
- Think about compilation – you can more easily go from a high-level language to machine code than the other way around.

Cantor's *Other* Diagonal Argument

What is $|\mathbb{R}|$?

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

Sketch of the Proof

- To prove that $|\mathbb{N}| < |\mathbb{R}|$, we will use a modification of the proof of Cantor's theorem.
- First, we will directly prove that $|\mathbb{N}| \leq |\mathbb{R}|$.
- Second, we will use a proof by diagonalization to show that $|\mathbb{N}| \neq |\mathbb{R}|$.

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

Proof: We will exhibit an injection $f : \mathbb{N} \to \mathbb{R}$. Thus by definition, $|\mathbb{N}| \leq |\mathbb{R}|$.

Consider the function $f(n) = n$. Since all natural numbers are real numbers, this is a valid function from $\mathbb{N}$ to $\mathbb{R}$. Moreover, it is injective. To see this, consider any $n_0, n_1 \in \mathbb{N}$ such 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 injective. ■

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

- Now, we need to show that $|\mathbb{N}| \neq |\mathbb{R}|$.
- To do this, we will use a proof by diagonalization similar to the one for Cantor's Theorem.
  - Assume there is a bijection $f : \mathbb{N} \to \mathbb{R}$.
  - Construct a two-dimensional table from f.
  - Construct a "diagonal number" from the table.
  - Show the diagonal number is not in the table.
  - Conclude f is not a bijection.

	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.

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	...
...	...	...	...	...	...	...	...

Which natural number is paired with this real number?

0.	0	0	1	0	0	...

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

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

We introduce some new notation. For a real number r, let r_0 be the integer part of r, and let r_n for $n \in \mathbb{N}$, $n > 0$, be the nth digit in the decimal representation of r. Now, define the real number d as follows:

$$d_n = \begin{cases} 1 & \text{if } f(n)_n = 0 \\ 0 & \text{otherwise} \end{cases}$$

Since $d \in \mathbb{R}$, there must be some $n \in \mathbb{N}$ such that $f(n) = d$. So consider $f(n)_n$ and d_n. We consider two cases:

Case 1: $f(n)_n = 0$. Then by construction $d_n = 1$, meaning that $f(n) \neq d$.

Case 2: $f(n)_n \neq 0$. Then by construction $d_n = 0$, meaning that $f(n) \neq d$.

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

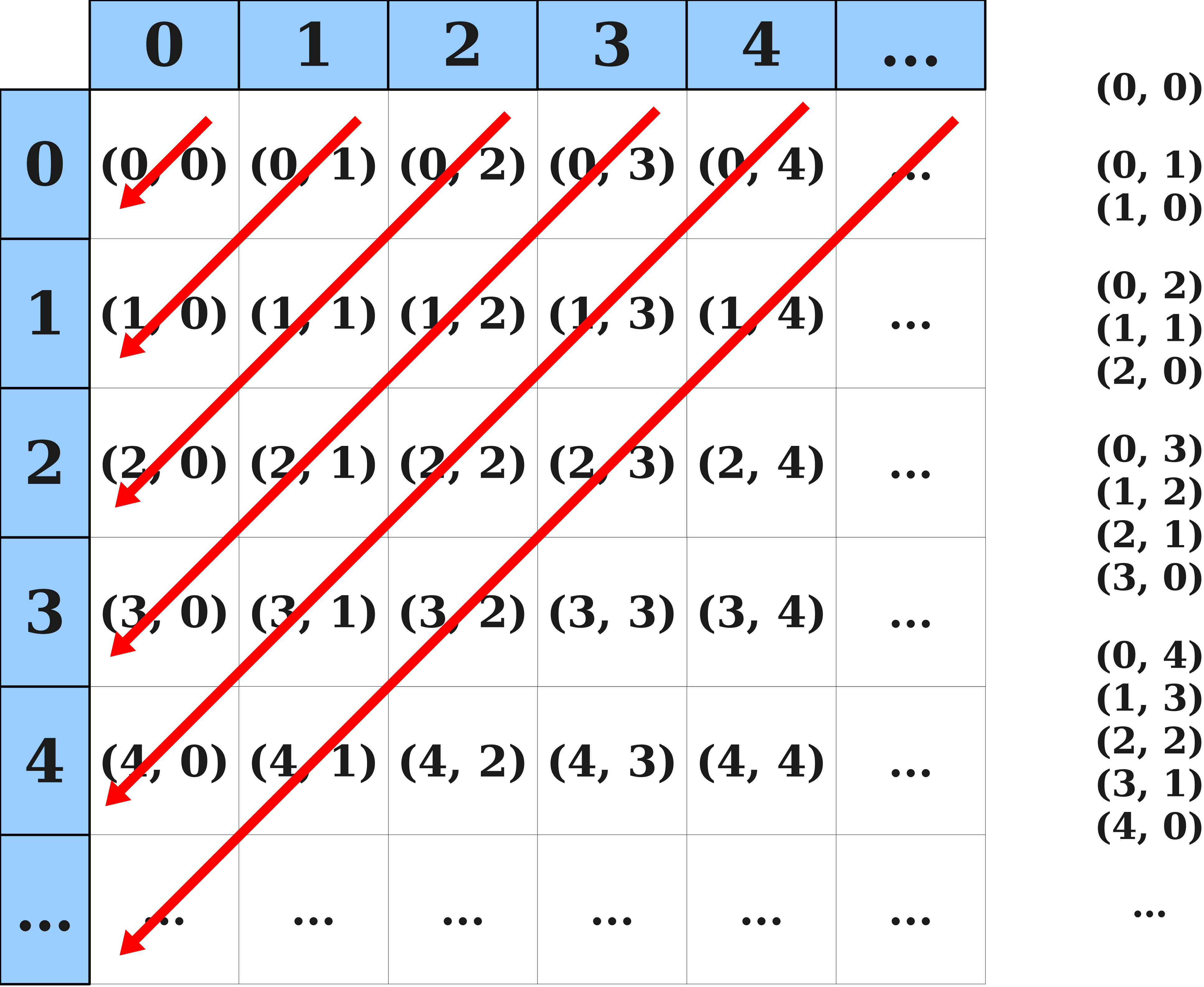
The Power of Diagonalization

- A large number of fundamental results in computability and complexity theory are based on diagonal arguments.
- We will see at least three of them in the remainder of the quarter.

Cantor's *Other Other* Diagonal Argument

(This one is different!)

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

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

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

This function is called
Cantor's Pairing Function.

Theorem: $|\mathbb{N}^2| = |\mathbb{N}|$.

Formalizing the Proof

- We need to show that this function f is injective and surjective.
- These proofs are nontrivial, but have beautiful intuitions.
- I've included the proofs at the end of these slides if you're curious.

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

Proving Surjectivity

- Given just the definition of our function:

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

  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

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

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

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

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.

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

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

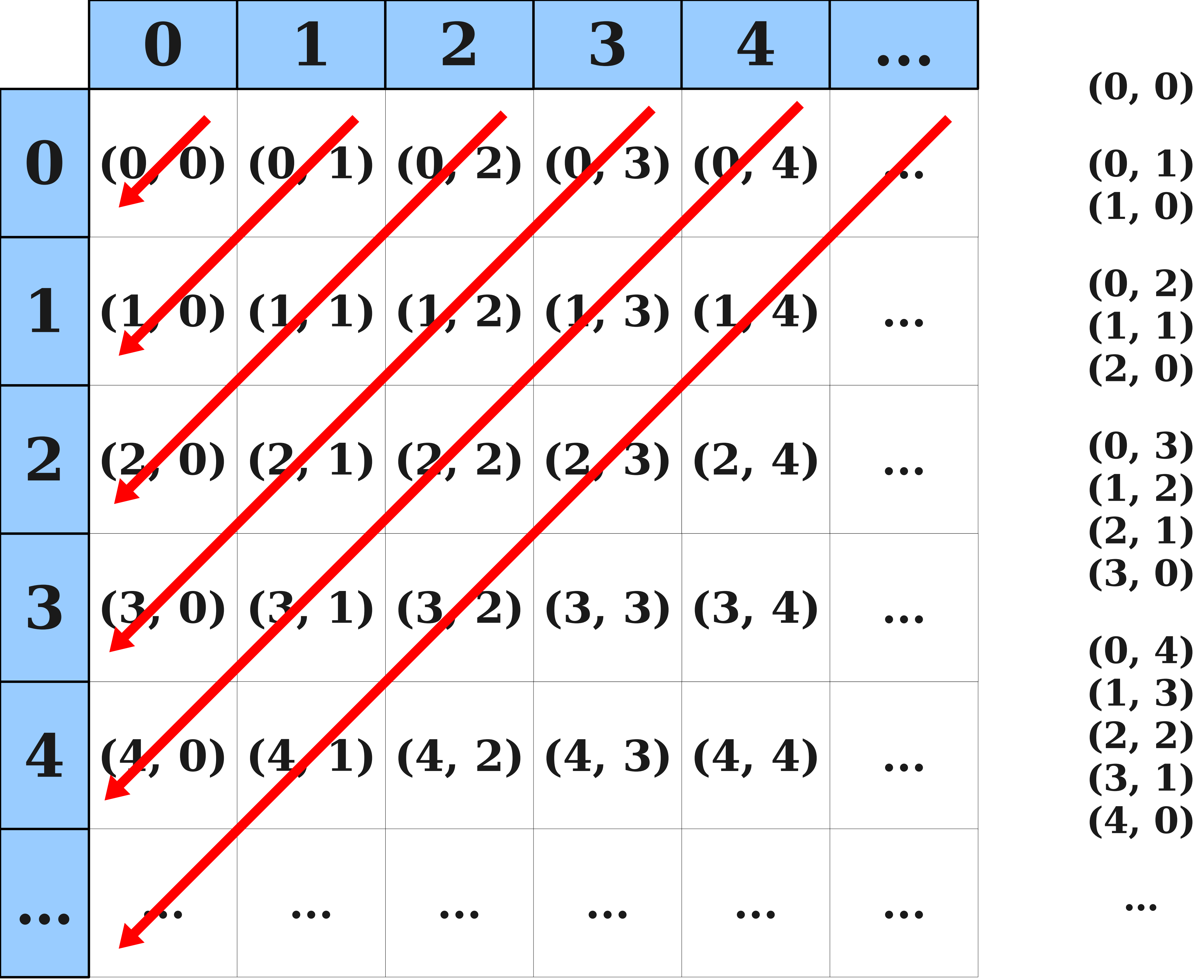
Thus there is a pair $(a, b) \in \mathbb{N}^2$ (namely, $(k, d - k)$) such that $f(a, b) = n$. Consequently, f is surjective. ■

Proving Injectivity

- Given the function

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

- 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, 1) (0, 2) (0, 3) (0, 4) ...
(1, 0) (1, 1) (1, 2) (1, 3) (1, 4) ...
(2, 0) (2, 1) (2, 2) (2, 3) (2, 4) ...
(3, 0) (3, 1) (3, 2) (3, 3) (3, 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 $m = a + b$.

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.

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. ■