Great Theoretical Ideas In Computer Science

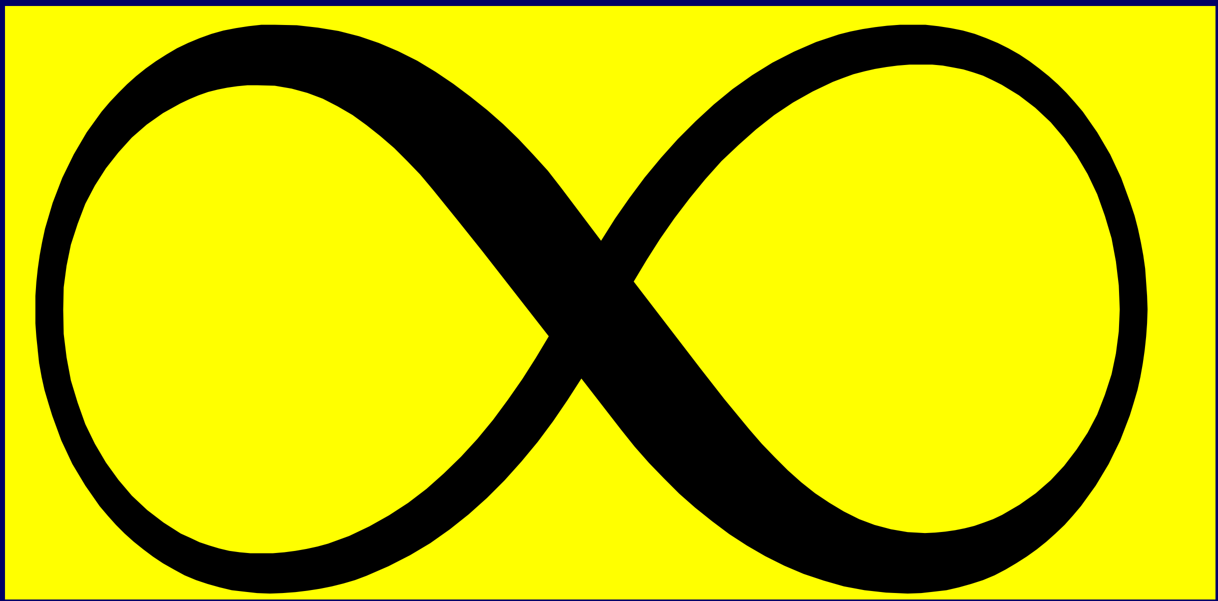
Anupam Gupta

CS 15-251 Fall 2005

Lecture 25 Nov 22, 2005

Carnegie Mellon University

Cantor's Legacy: Infinity And Diagonalization



Ideas from the course

Induction

Numbers

Representation

Finite Counting and Probability

A hint of the infinite

Infinite row of dominoes

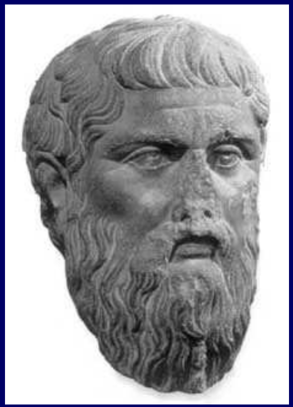
Infinite sums (formal power series)

Infinite choice trees, and infinite probability

Infinite RAM Model

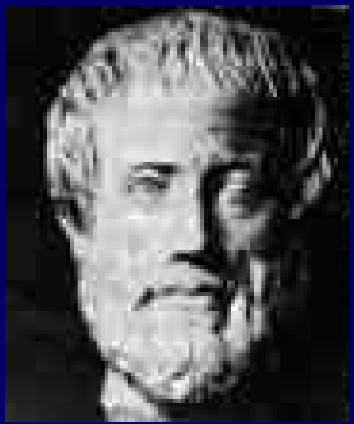
Platonic Version:

One memory location for each natural number 0, 1, 2, …



Aristotelian Version:

Whenever you run out of memory, the computer contacts the factory. A maintenance person is flown by helicopter and attaches 100 Gig of RAM and all programs resume their computations, as if they had never been interrupted.



The Ideal Computer:
no bound on amount of memory
no bound on amount of time

M bits of memory

⇒ 2^M states the machine can have

Ideal Computer is defined as a computer with infinite RAM.

You can run a Java program and never have any overflow, or out of memory errors.

An Ideal Computer

It can be programmed to print out:

π: 3.14159265358979323846264…

2: 2.00000000000000000000000…

e: 2.71828182845904523536…

1/3: 0.33333333333333333333…

ϕ: 1.61803398874989484820045…

Printing Out An Infinite Sequence..

A program P prints out the infinite sequence

$s_0, s_1, s_2, \ldots, s_k, \ldots$

if when P is executed on an ideal computer, it outputs a sequence of symbols such that

-The k^{th} symbol that it outputs is s_k

-For every $k \in \mathbb{N}$, P eventually outputs the k^{th} symbol. I.e., the delay between symbol k and symbol k+1 is not infinite.

Computable Real Numbers

A real number R is computable if there is a program that prints out the decimal representation of R from left to right.

Thus, each digit of R will eventually be output.

Describable Numbers

A real number R is <u>describable</u> if it can be denoted unambiguously by a finite piece of English text.

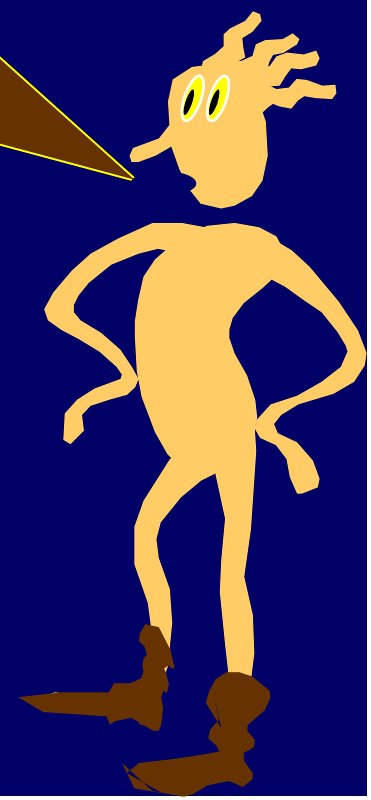
2: "Two."

π: "The area of a circle of radius one."

Are all real numbers describable?

Is every
computable real number, also
a describable real number?

And what about the other
way?



Computable R: some program outputs R
Describable R: some sentence denotes R

Computable $\Rightarrow$ describable

Theorem:

Every computable real is also describable

Computable $\Rightarrow$ describable

Theorem:

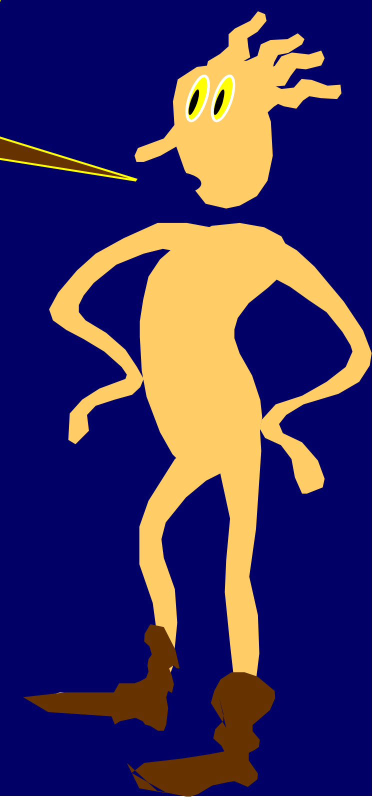
Every computable real is also describable

Proof:

Let R be a computable real that is output by a program P. The following is an unambiguous description of R:

"The real number output by the following program:" P

MORAL: A computer program can be viewed as a description of its output.



Syntax: The text of the program
Semantics: The real number output by P

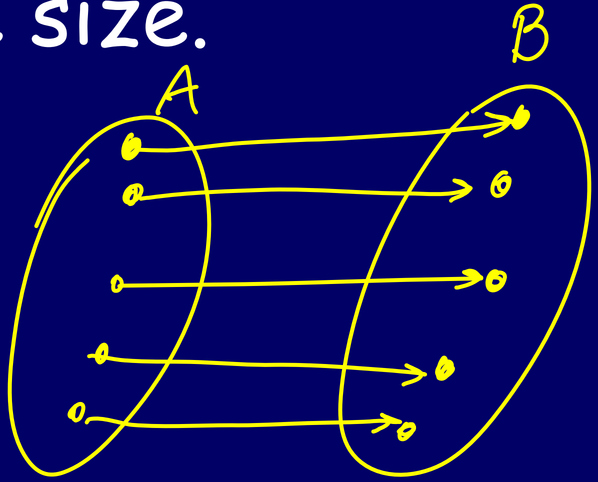
Are all reals describable?
Are all reals computable?

We saw that
computable $\Rightarrow$ describable,
but do we also have
describable $\Rightarrow$ computable?

Questions we will answer in this (and next) lecture…

Correspondence Principle

If two finite sets can be placed into 1-1 onto correspondence, then they have the same size.

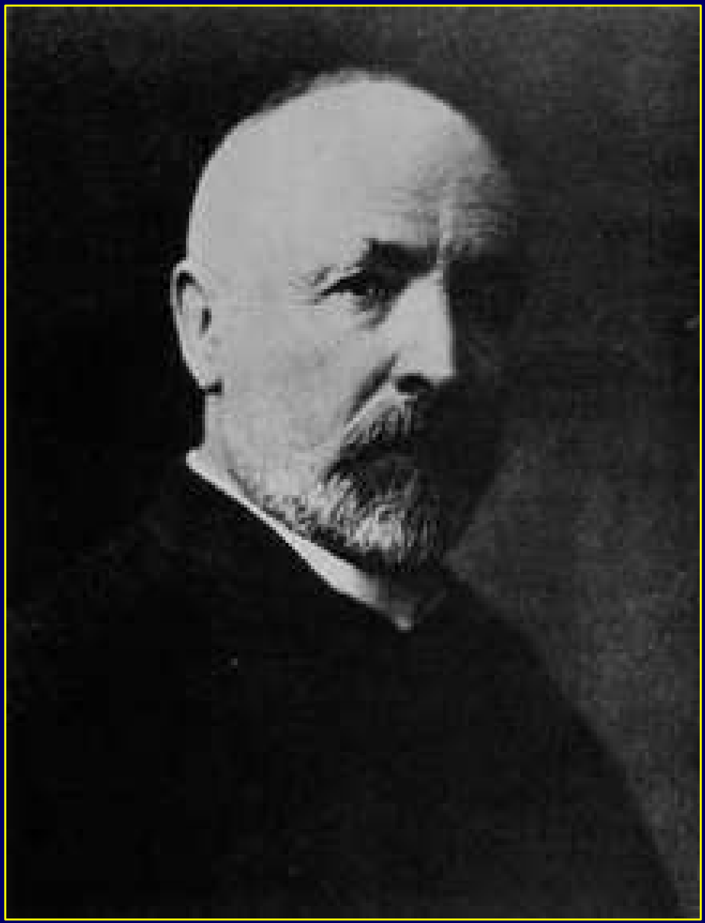


Correspondence Definition

In fact, we can use the correspondence as the definition:

Two finite sets are defined to have the <u>same size</u> if and only if they can be placed into 1-1 onto correspondence.

Georg Cantor (1845-1918)



Cantor's Definition (1874)

Two sets are defined to have the same size if and only if they can be placed into 1-1 onto correspondence.

Cantor's Definition (1874)

Two sets are defined to have the <u>same cardinality</u> if and only if they can be placed into 1-1 onto correspondence.

Do $\mathbb{N}$ and $\mathbb{E}$ have the same cardinality?

$\mathbb{N}$ = { 0, 1, 2, 3, 4, 5, 6, 7, ... }

$\mathbb{E}$ = { 0, 2, 4, 6, 8, 10, 12, ... }

The even, natural numbers.

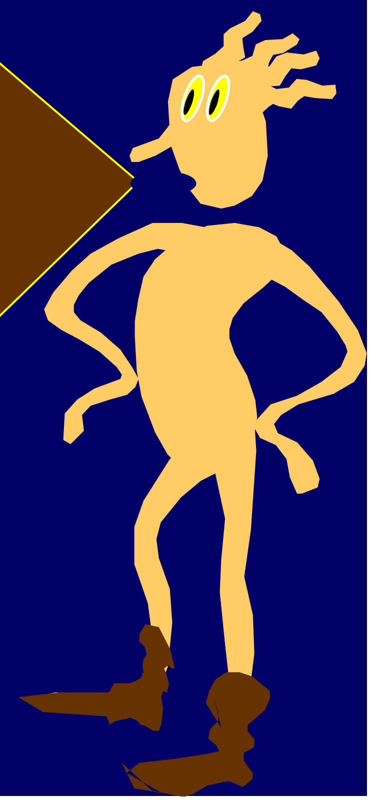
$\mathbb{E}$ and $\mathbb{N}$ do not have the same cardinality! $\mathbb{E}$ is a proper subset of $\mathbb{N}$ with plenty left over.

The attempted correspondence f(x)=x does not take $\mathbb{E}$ *onto* $\mathbb{N}$.

$\mathbb{E}$ and $\mathbb{N}$ do have the same cardinality!

$\mathbb{N}$ = 0, 1, 2, 3, 4, 5, …
$\mathbb{E}$ = 0, 2, 4, 6, 8,10, …

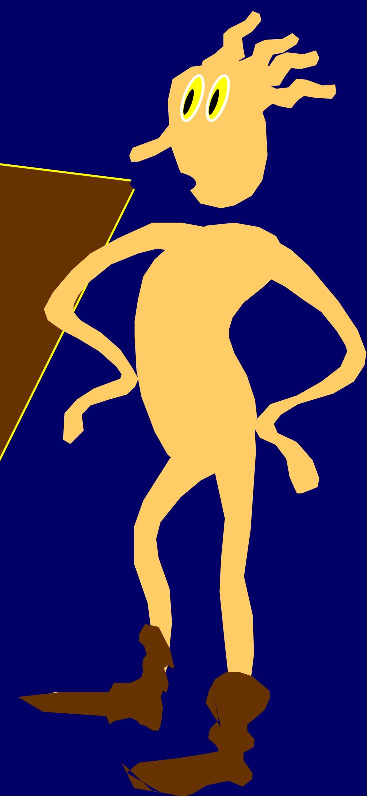
f(x) = 2x is 1-1 onto.



Lesson:

Cantor's definition only requires that *some* 1-1 correspondence between the two sets is onto, not that all 1-1 correspondences are onto.

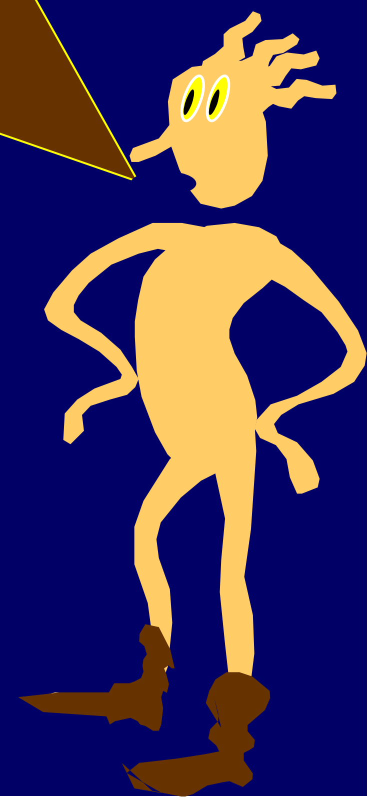
This distinction never arises when the sets are finite.



Cantor's Definition (1874)

Two sets are defined to have the same size if and only if they can be placed into 1-1 onto correspondence.

You just have to get used to this slight subtlety in order to argue about infinite sets!



Do $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality?

$\mathbb{N}$ = { 0, 1, 2, 3, 4, 5, 6, 7, … }

$\mathbb{Z}$ = { …, -2, -1, 0, 1, 2, 3, … }

No way! $\mathbb{Z}$ is infinite in two ways: from 0 to positive infinity and from 0 to negative infinity.

Therefore, there are far more integers than naturals.

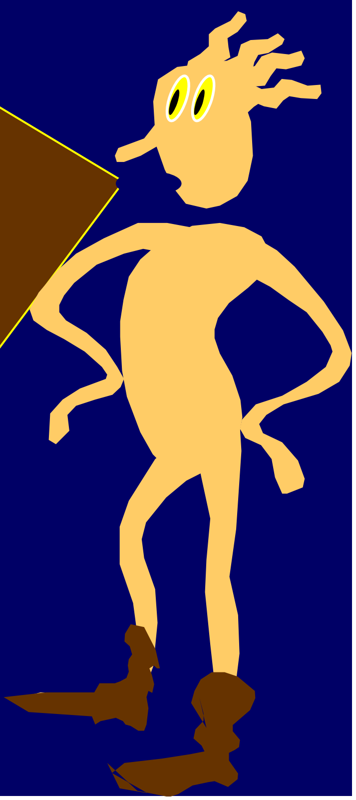
Actually, no!

$\mathbb{N}$ and $\mathbb{Z}$ do have the same cardinality!

$\mathbb{N}$ = 0, 1, 2, 3, 4, 5, 6 …

$\mathbb{Z}$ = 0, 1, -1, 2, -2, 3, -3, ….

$$f(x) = \begin{cases} \lceil x/2 \rceil & \text{if } x \text{ is odd} \\ -x/2 & \text{if } x \text{ is even} \end{cases}$$



Transitivity Lemma

$f : A \to B$ 1-1 onto

$g : B \to C$ 1-1 onto

$h : A \to C \qquad h(x) = g(f(x))$

Claim: h is a 1-1 onto correspondence

$f : \mathbb{E} \to \mathbb{N}$, $g : \mathbb{N} \to \mathbb{Z}$

$\Rightarrow \mathbb{N}, \mathbb{E}, \mathbb{Z}$ have same card.

Transitivity Lemma

Lemma: If

  f: $A \to B$ is 1-1 onto, and

  g: $B \to C$ is 1-1 onto.

Then h(x) = g(f(x)) defines a function

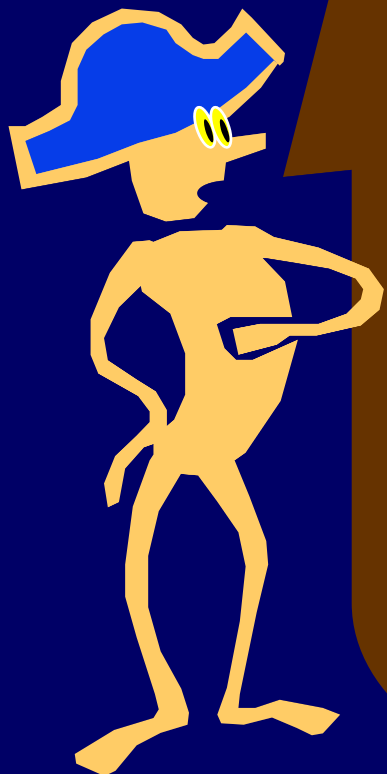
  h: $A \to C$ that is 1-1 onto

Hence, $\mathbb{N}$, $\mathbb{E}$, and $\mathbb{Z}$ all have the same cardinality.

Do $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality?

$\mathbb{N}$= { 0, 1, 2, 3, 4, 5, 6, 7, ... }

$\mathbb{Q}$ = The Rational Numbers

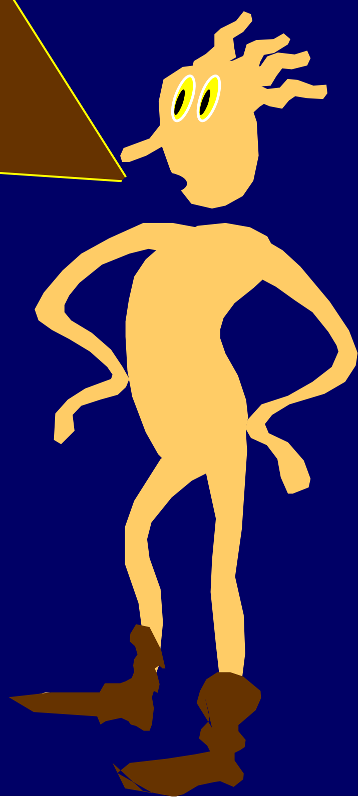


No way!

The rationals are dense: between any two there is a third. You can't list them one by one without leaving out an infinite number of them.

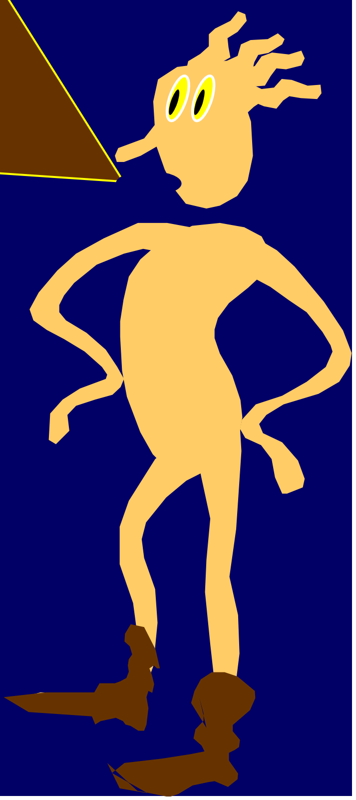
Don't jump to conclusions!

There is a clever way to list the rationals, one at a time, without missing a single one!



First, let's warm up with another interesting example:

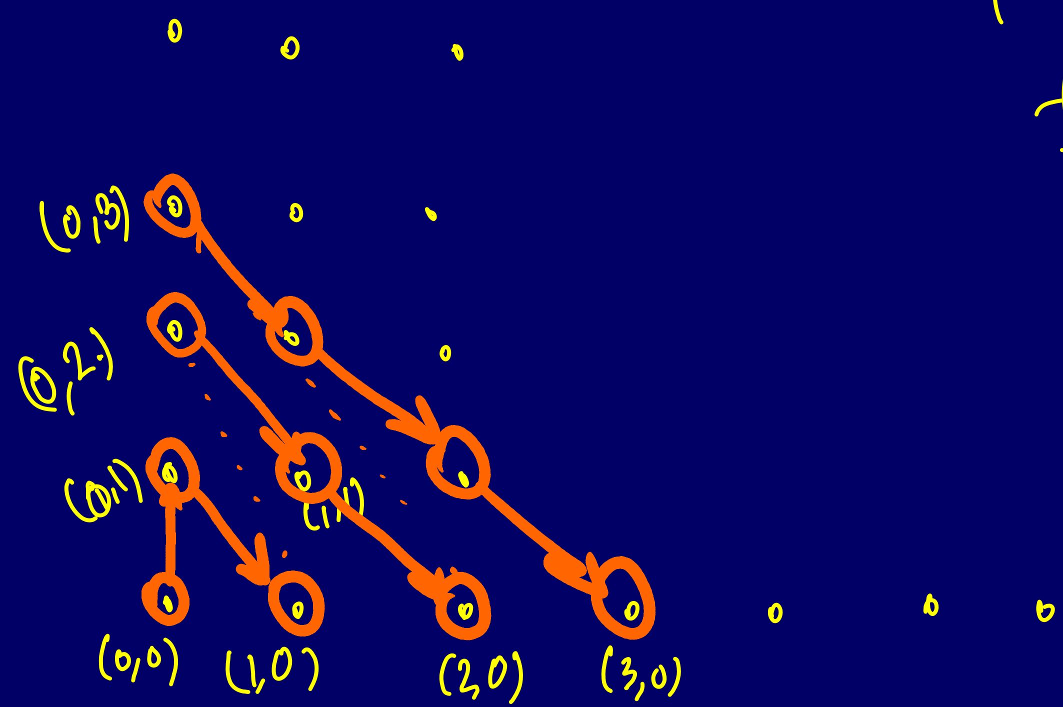
$\mathbb{N}$ can be paired with $\mathbb{N} \times \mathbb{N}$



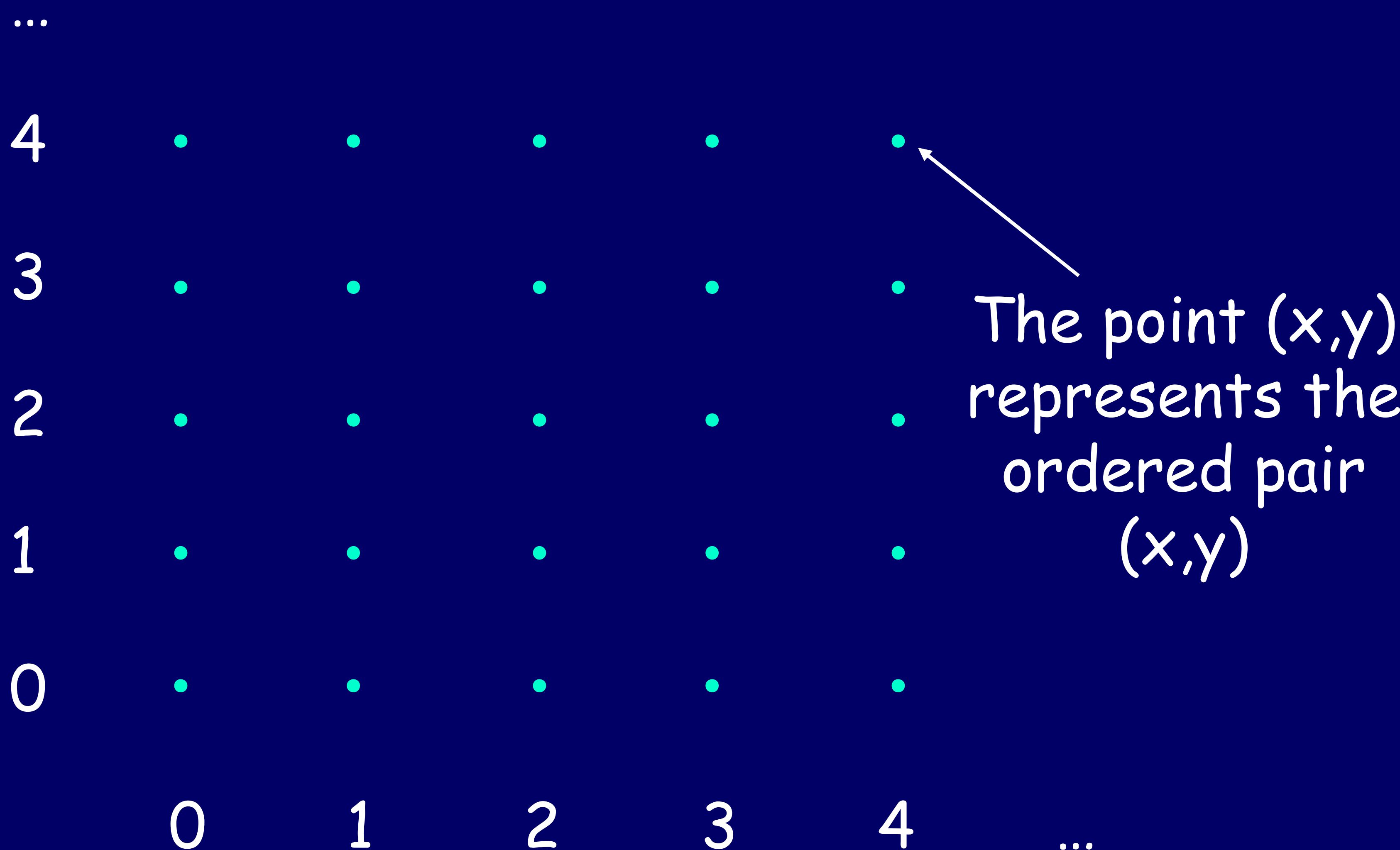
Theorem: $\mathbb{N}$ and $\mathbb{N}\times\mathbb{N}$ have the same cardinality

$\{0, 1, 2, 3 \ldots\ldots\}$

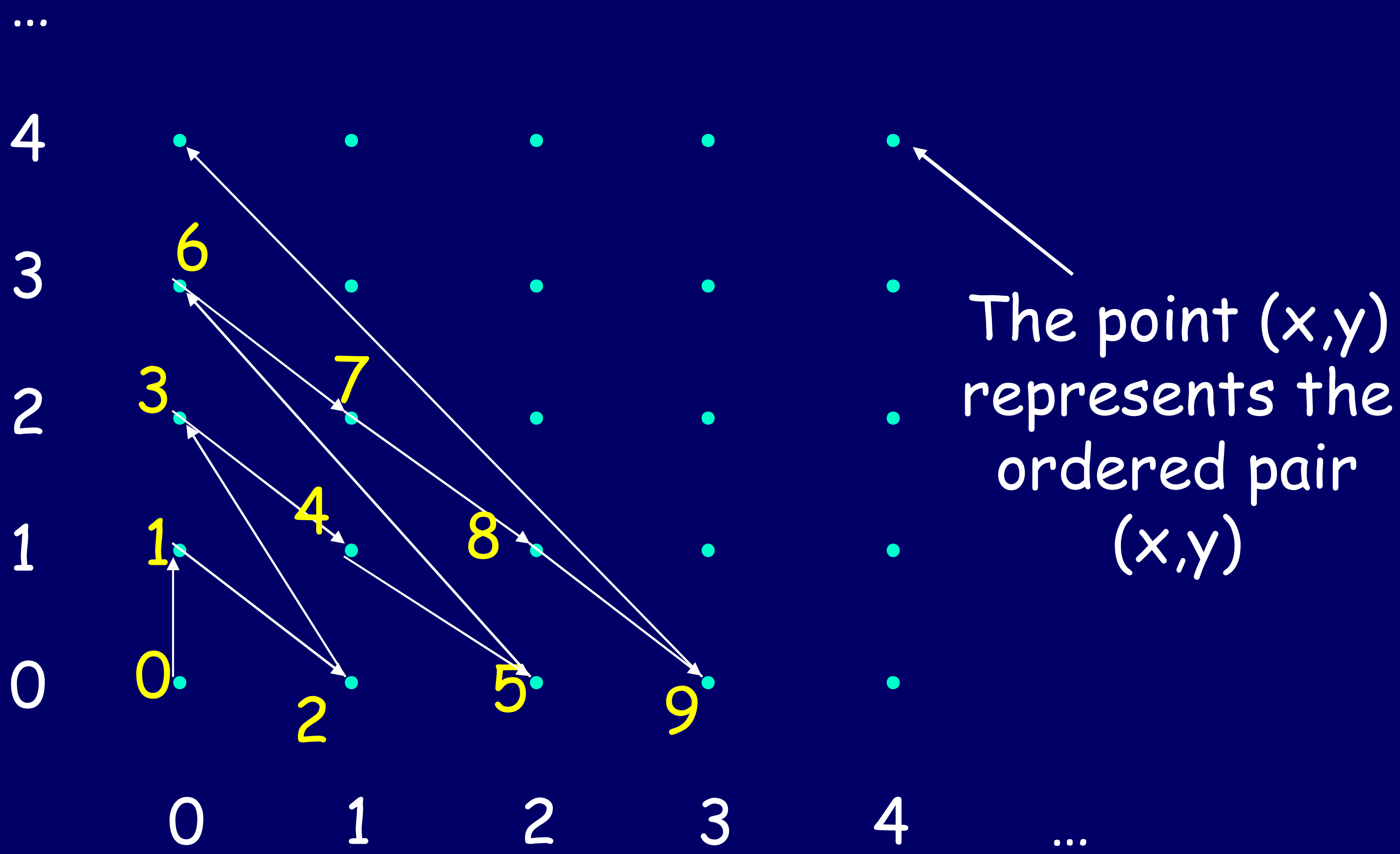
Explicitly state what $f(i)$ is forall $i \in \mathbb{N}$.



Theorem: $\mathbb{N}$ and $\mathbb{N}\times\mathbb{N}$ have the same cardinality



Theorem: $\mathbb{N}$ and $\mathbb{N}\times\mathbb{N}$ have the same cardinality

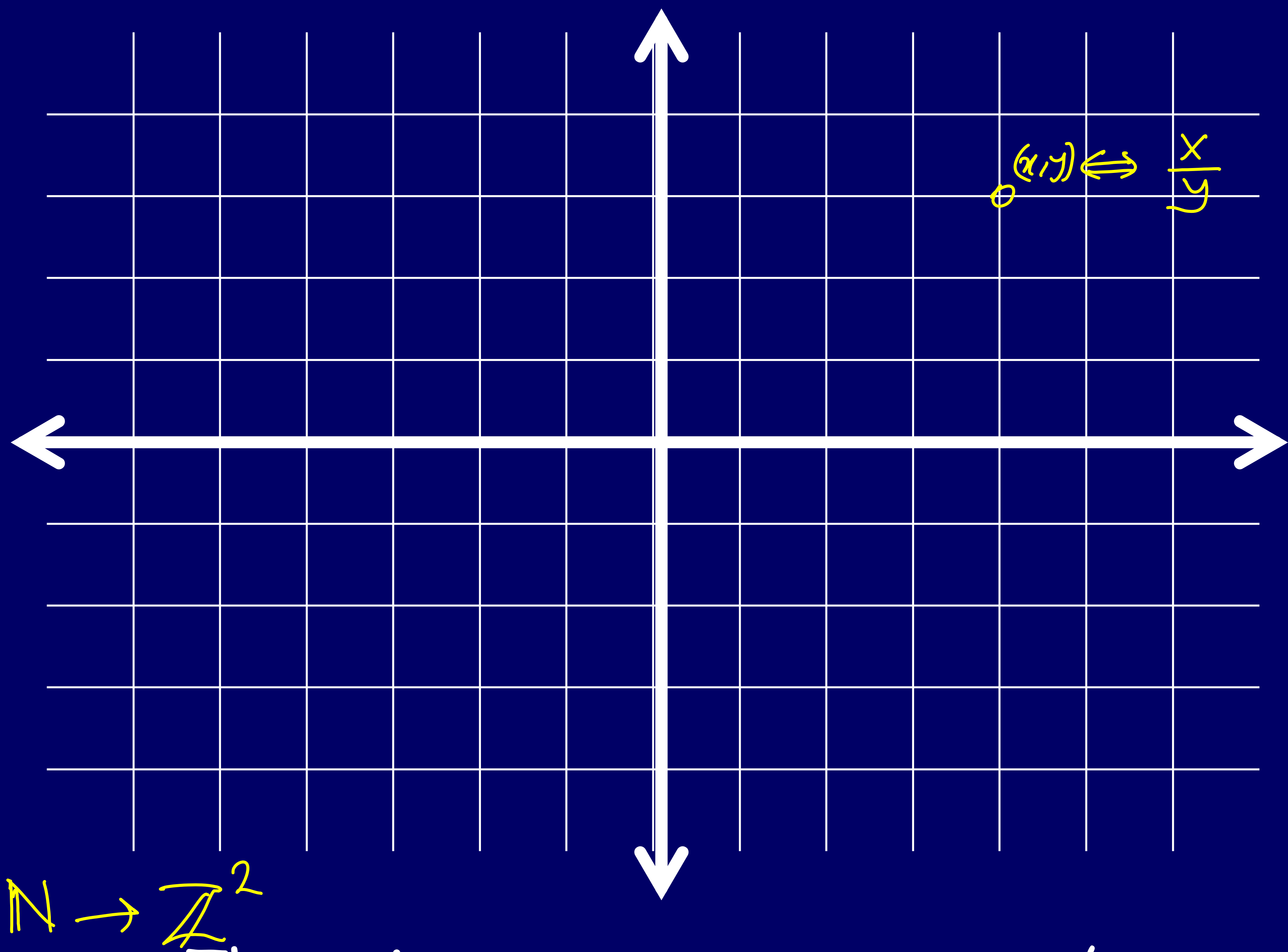


Defining 1-1 onto f: $\mathbb{N} \to \mathbb{N}\times\mathbb{N}$

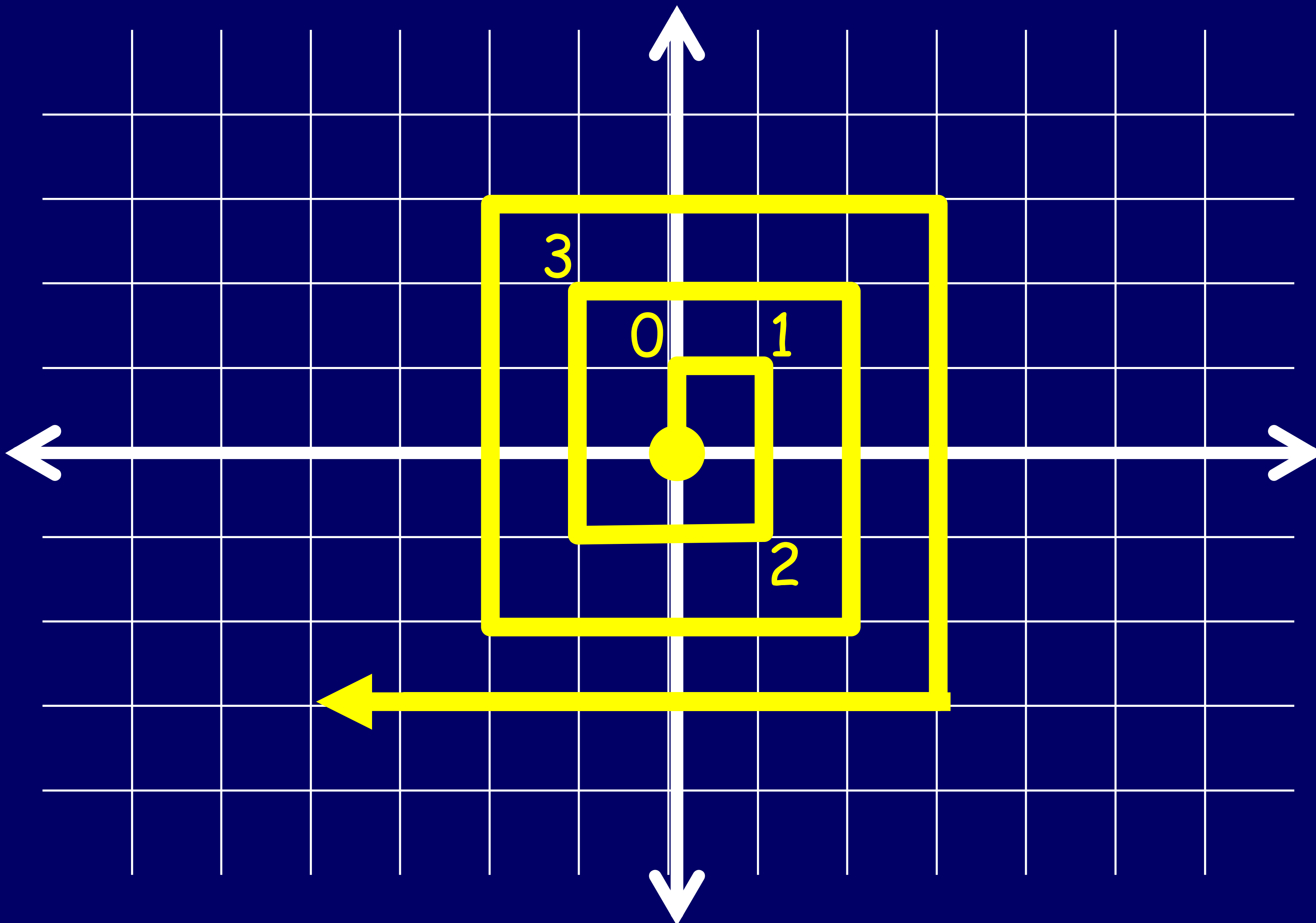
```
let i := 0;        //will range over N

for (sum = 0 to forever) {
  //generate all pairs with this sum
  for (x = 0 to sum) {
    y := sum-x
        define f(i) := the point (x,y)
    i++;
  }
}
```


Onto the Rationals!



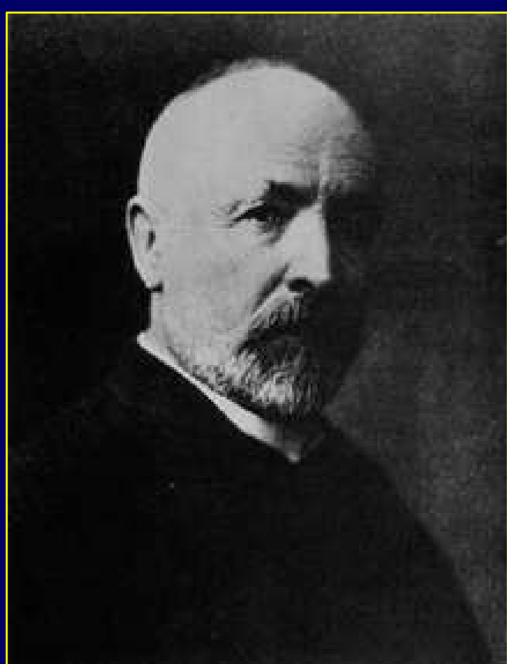
The point at x,y represents x/y

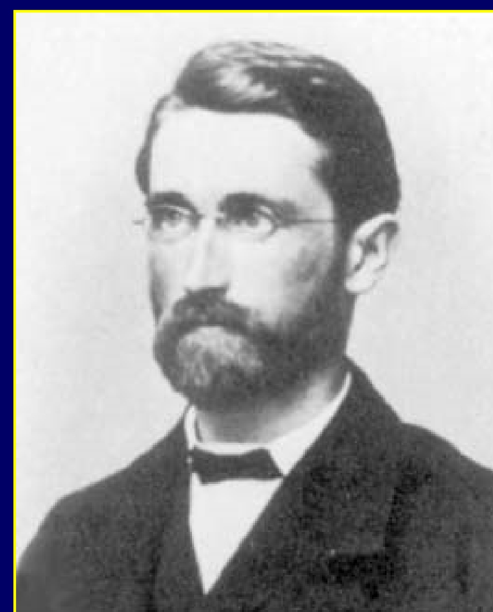


The point at x,y represents x/y

Cantor's 1877 letter to Dedekind:

"I see it, but I don't believe it!"





Countable Sets

We call a set <u>countable</u> if it can be placed into 1-1 onto correspondence with the natural numbers $\mathbb{N}$.

Hence

$\mathbb{N}$, $\mathbb{E}$, $\mathbb{Q}$ and $\mathbb{Z}$ are all countable.

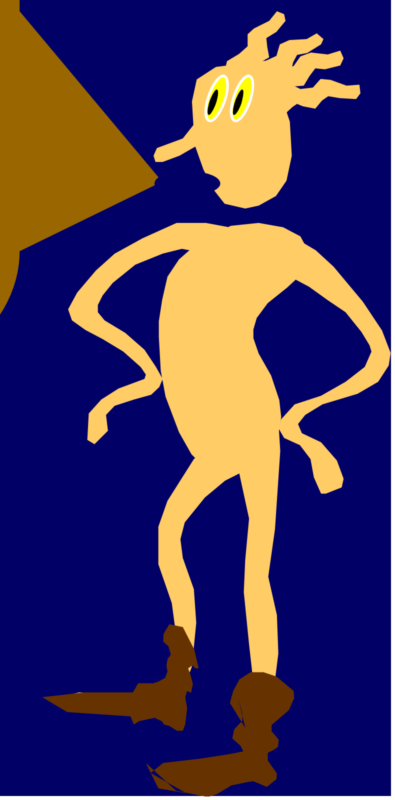
Do $\mathbb{N}$ and $\mathbb{R}$ have the same cardinality?

$\mathbb{N}$ = { 0, 1, 2, 3, 4, 5, 6, 7, … }

$\mathbb{R}$ = The Real Numbers

No way!

You will run out of natural numbers long before you match up every real.

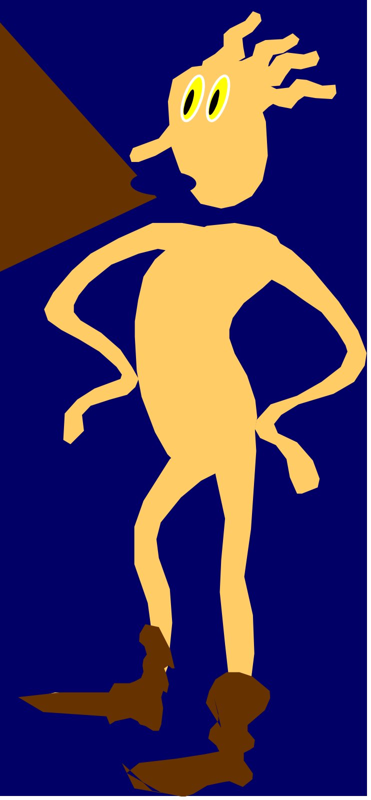


Now hang on a minute!

You can't be sure that there isn't some clever correspondence that you haven't thought of yet.

I am sure!
Cantor proved it.

To do this, he invented a very important technique called "Diagonalization"



Theorem: The set $\mathbb{R}_{[0,1]}$ of reals between 0 and 1 is not countable.

Proof: (by contradiction)

Suppose $\mathbb{R}_{[0,1]}$ is countable.

Let f be a 1-1 onto function from $\mathbb{N}$ to $\mathbb{R}_{[0,1]}$.

Make a list L as follows:

0: decimal expansion of f(0)
1: decimal expansion of f(1)
…
k: decimal expansion of f(k)
…

Theorem: The set $\mathbb{R}_{[0,1]}$ of reals between 0 and 1 is not countable.

Proof: (by contradiction)

Suppose $\mathbb{R}_{[0,1]}$ is countable.

Let f be a 1-1 onto function from $\mathbb{N}$ to $\mathbb{R}_{[0,1]}$.

Make a list L as follows:

0: 0.33333333333333333…
1: 0.314159265657839593…
…
k: 0.235094385543905834…
…

Position after decimal point

Index

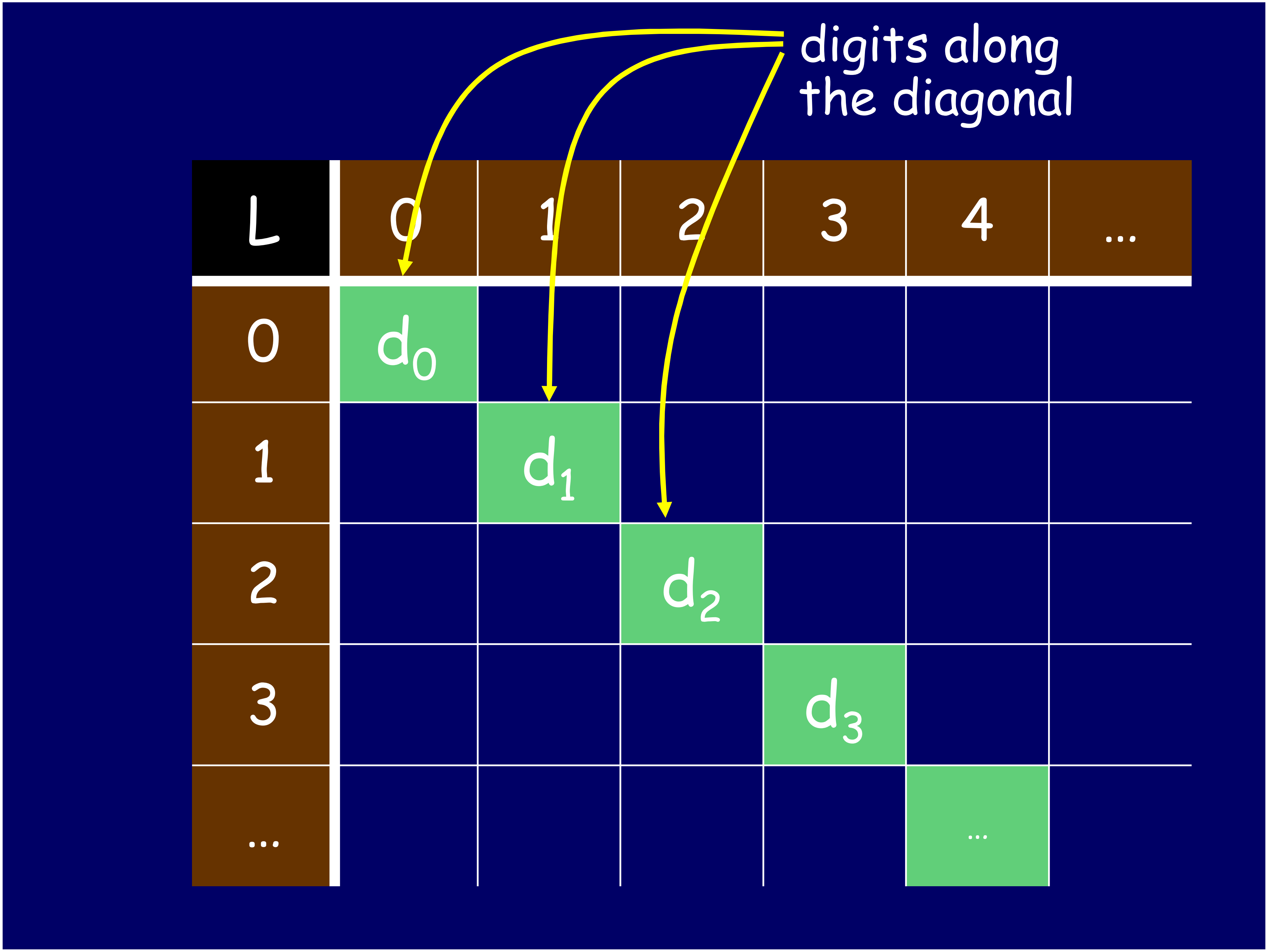
L	0	1	2	3	4	...
0						
1						
2						
3						
...						

Position after decimal point

Index

L	0	1	2	3	4	...
0	3	3	3	3	3	3
1	3	1	4	1	5	9
2	1	2	4	8	1	2
3	4	1	2	2	6	8
...	2	7	3	1	6	4

$Confuse_L$ = 0.66665 .....


digits along the diagonal
L
0
1
2
3
4
...
0
1
2
3
...
d_0
d_1
d_2
d_3
...

L	0	1	2	3	4
0	d_0				
1		d_1			
2			d_2		
3				d_3	
...					...

Define the following real number

$\text{Confuse}_L = .\ C_0 \quad C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \ \ldots$

L	0	1	2	3	4
0	d_0				
1		d_1			
2			d_2		
3				d_3	
…					…

Define the following real number

$$\text{Confuse}_L = .\ C_0 \quad C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \ \ldots$$

$$C_k = \begin{cases} 5, \text{ if } d_k = 6 \\ 6, \text{ otherwise} \end{cases}$$

L	0	1	2	3	4
0	$c_0 \neq d_0$	c_1	c_2	c_3	c_4
1		d_1			
2			d_2		
3				d_3	
...					...

...

$$c_k = \begin{cases} 5, \text{ if } d_k = 6 \\ 6, \text{ otherwise} \end{cases}$$

L	0	1	2	3	4	
0	d_0					
1	C_0	$C_1 \neq d_1$	C_2	C_3	C_4	…
2			d_2			
3				d_3		
…					…	

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

L	0	1	2	3	4
0	d_0				
1		d_1			
2	C_0	C_1	$C_2 \neq d_2$	C_3	C_4
3				d_3	
…					…

…

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

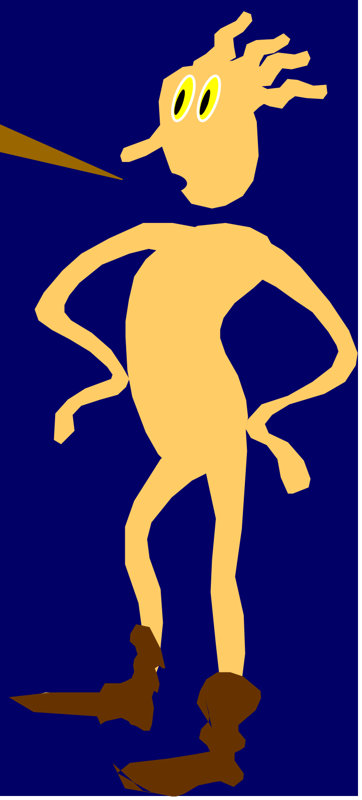
Diagonalized!

By design, $Confuse_L$ can't be on the list L!

$Confuse_L$ differs from the k^{th} element on the list L in the k^{th} position.

This contradicts the assumption that the list L is complete; i.e., that the map f: $\mathbb{N}$ to $\mathbb{R}_{[0,1]}$ is onto.

The set of reals is uncountable!
(Even the reals between 0 and 1.)

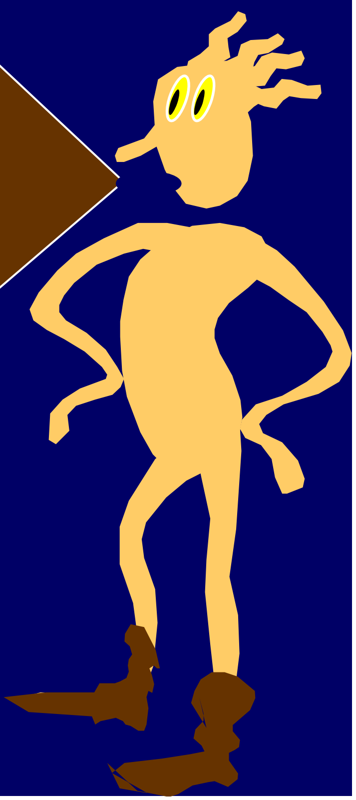


An aside:, you can set up a correspondence between $\mathbb{R}$ and $\mathbb{R}_{[0,1]}$.

Hold it!
Why can't the same argument be used to show that the set of rationals $\mathbb{Q}$ is uncountable?

The argument is the same for $\mathbb{Q}$ until the punchline.

However, since CONFUSE_L is not necessarily rational, so there is no contradiction from the fact that it is missing from the list L.



Another diagonalization proof

Problem from last year's final:

Show that the set of real numbers in [0,1] whose decimal expansion has the property that every digit is a prime number (2,3,5, or 7) is uncountable.

E.g., 0.2375 and 0.55555… are in the set, but
0.145555… and 0.3030303… are not.

Another diagonalization proof

Show that the set of real numbers in [0,1] whose decimal expansion has the property that every digit is a prime number (2,3,5, or 7) is uncountable.

Suppose not. Then there is a 1-1 onto map f from this set to the naturals.
Hence there is a list L of all numbers in this set.

Consider the number $\text{Confuse}_f = 0.\ C_0\ C_1\ C_2\ C_3 \ldots$
defined as follows

C_k	= 3	if the k^{th} bit of the real f(k) = 5
	= 5	otherwise

By construction, Confuse_f differs from f(k) in the k^{th} place.
Hence Confuse_f is not in the list.

But Confuse_f is a number in the set, and hence should have been on the list!
Contradiction!!!

Steps when diagonalizing

Show that the set of real numbers in [0,1] whose decimal expansion has the property that every digit is a prime number (2,3,5, or 7) is uncountable.

A) Assume this set is countable and therefore it can be placed in a list L. Given L, show how to define a number called Confuse.

B) Show that Confuse is not in L.

C) Explain why Confuse not being in L implies the set is not countable.

Back to the questions
we were asking earlier

Are all reals describable?
Are all reals computable?

We saw that
computable ⇒ describable,
but do we also have
describable ⇒ computable?

Questions we will answer in this (and next) lecture…

Standard Notation

Σ = Any finite alphabet

Example: {a,b,c,d,e,…,z}

Σ^* = All finite strings of symbols from Σ including the empty string ε

Theorem: Every infinite subset S of Σ^* is countable

Proof:

Sort S by first by length and then alphabetically.

Map the first word to 0, the second to 1, and so on....

Stringing Symbols Together

Σ = The symbols on a standard keyboard

For example:

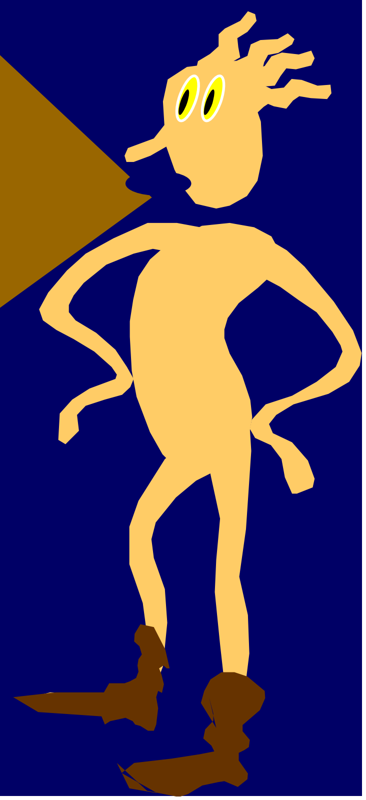
The set of all possible Java programs is a subset of Σ^*

The set of all possible finite pieces of English text is a subset of Σ^*

Thus:

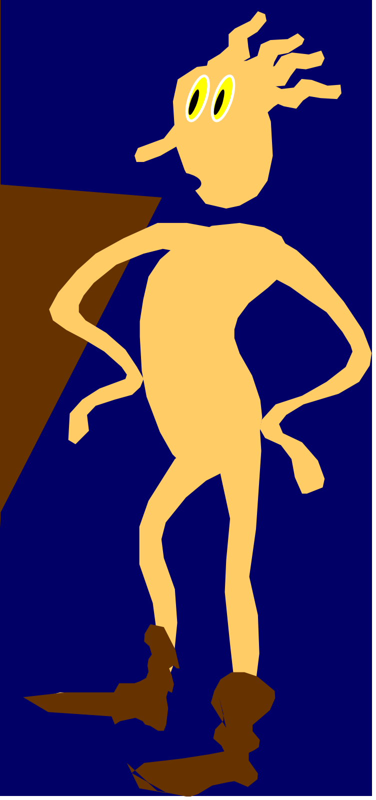
The set of all possible Java programs is countable.

The set of all possible finite length pieces of English text is countable.



There are countably many Java program and uncountably many reals.

Hence,
Most reals are not computable!



I see!
There are countably many descriptions and uncountably many reals.

Hence:
Most real numbers are not describable!

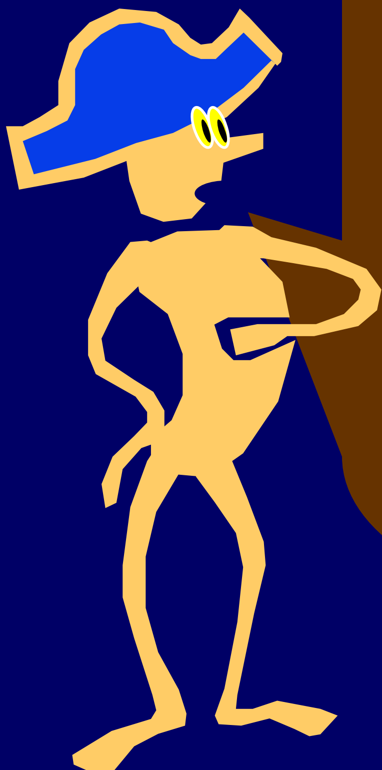
Are all reals describable? **NO**

Are all reals computable? **NO**

We saw that
computable $\Rightarrow$ describable,
but do we also have
describable $\Rightarrow$ computable?

Is there a real number that can be described, but not computed?

Wait till the next lecture!



We know there are at least 2 infinities.
(the number of naturals, the number of reals.)

Are there more?

Definition: Power Set

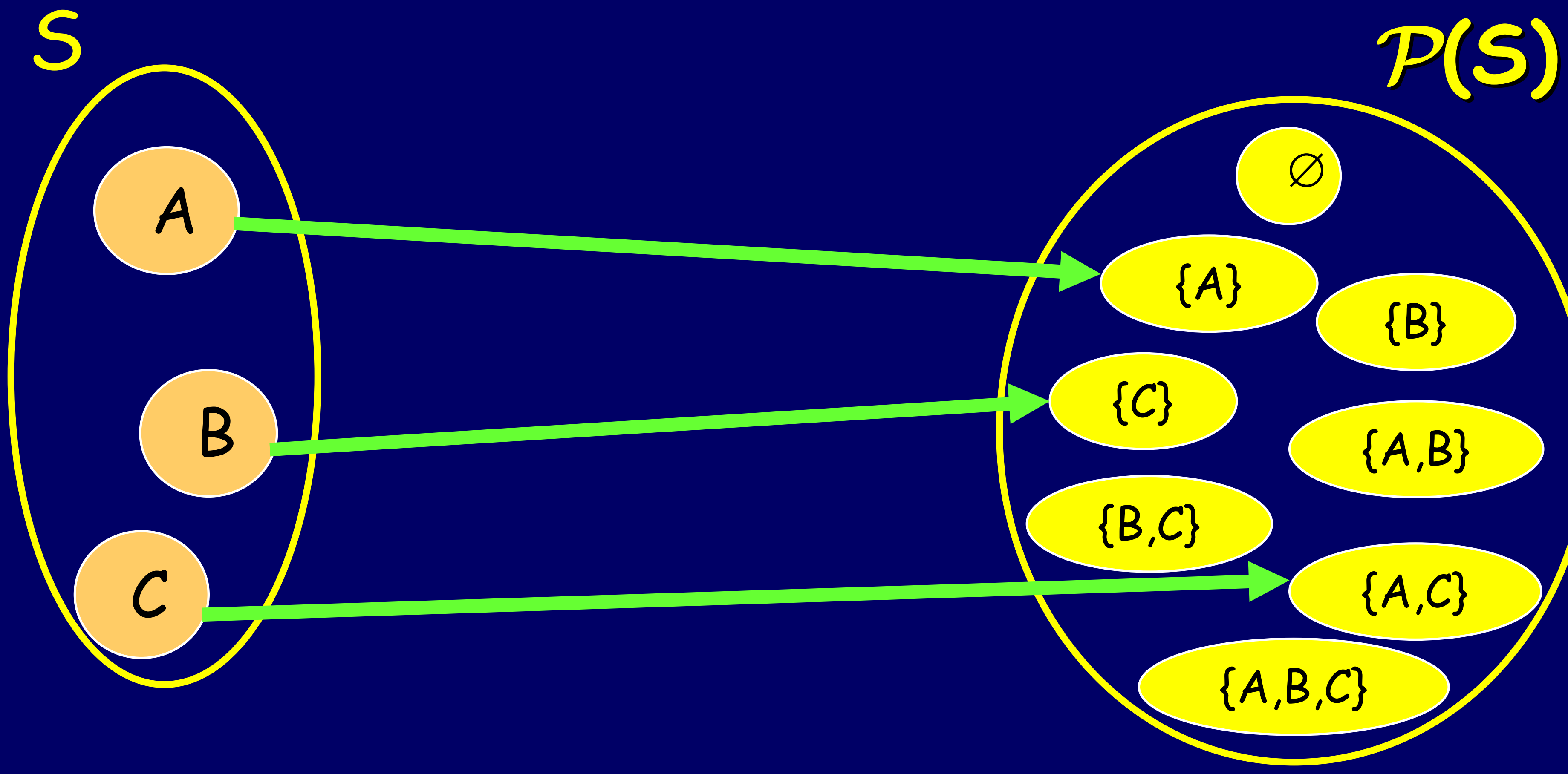
The power set of S is the set of all subsets of S.

The power set is denoted as $\mathcal{P}(S)$.

Proposition:

If S is finite, the power set of S has cardinality $2^{|S|}$

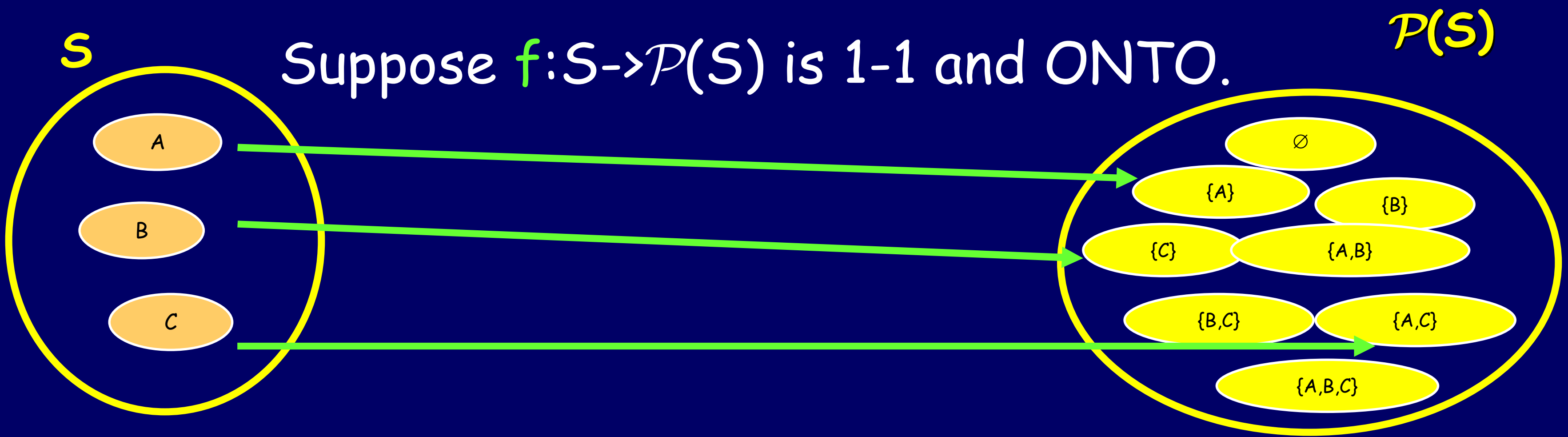
Theorem: S can't be put into 1-1 onto correspondence with $\mathcal{P}(S)$



Suppose f: $S \rightarrow \mathcal{P}(S)$ is 1-1 and ONTO.

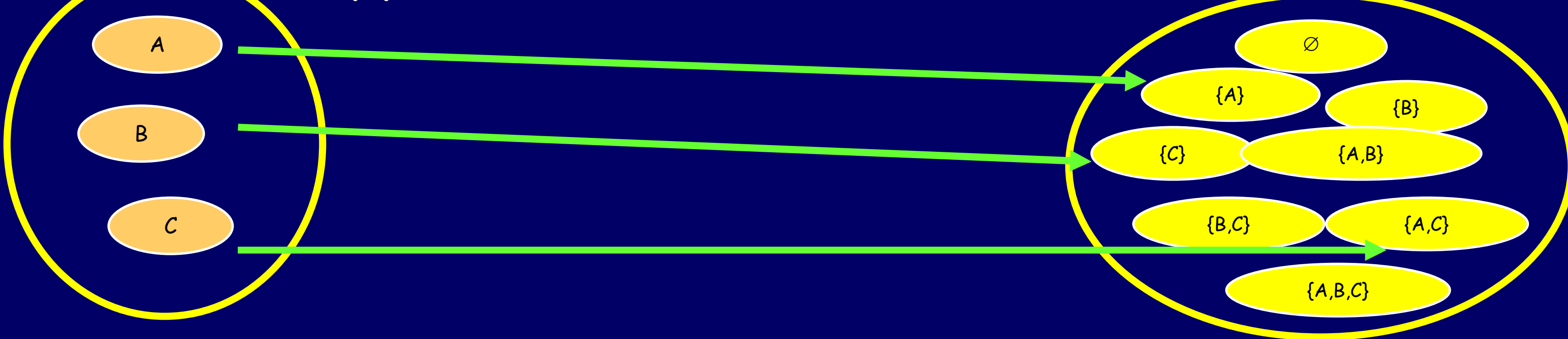
Theorem: S can't be put into 1-1 correspondence with $\mathcal{P}$(S)

Suppose f:S->$\mathcal{P}$(S) is 1-1 and ONTO.



Theorem: S can't be put into 1-1 correspondence with $\mathcal{P}(S)$

Suppose $f: S \to \mathcal{P}(S)$ is 1-1 and ONTO.



E.g. $Confuse_f = \{ B \}$

Let $CONFUSE_f = \{ x \mid x \in S, x \notin f(x) \}$

Since f is onto, exists $y \in S$ such that $f(y) = CONFUSE_f$

Is y in $CONFUSE_f$?

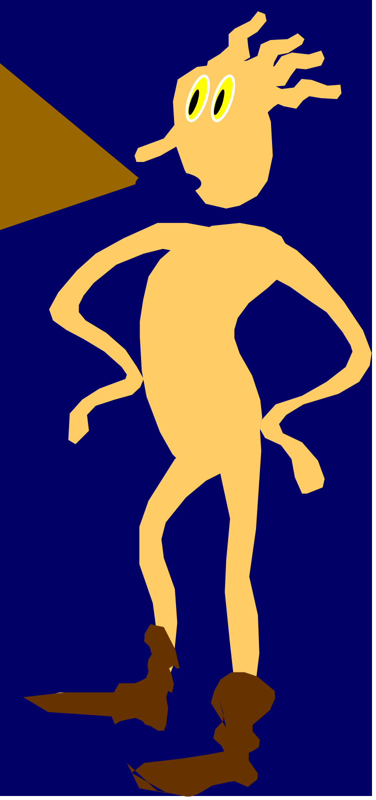
YES: Definition of $CONFUSE_f$ implies no

NO: Definition of $CONFUSE_f$ implies yes $\Rightarrow$ ↯

This proves that there are at least a countable number of infinities.

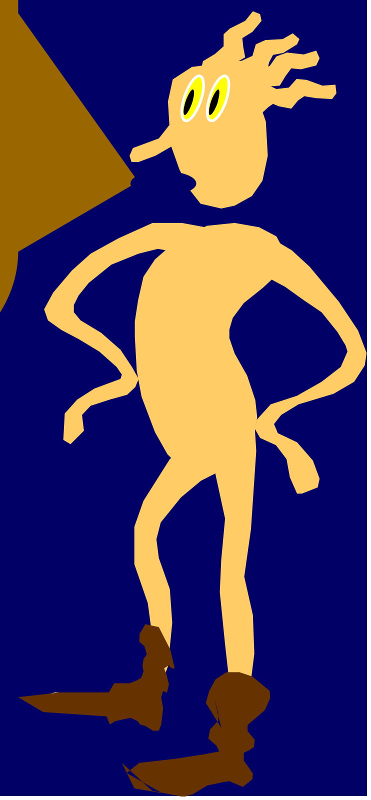
The first infinity is called:

$$\aleph_0$$



$\aleph_0, \aleph_1, \aleph_2, \ldots$

Are there any more infinities?

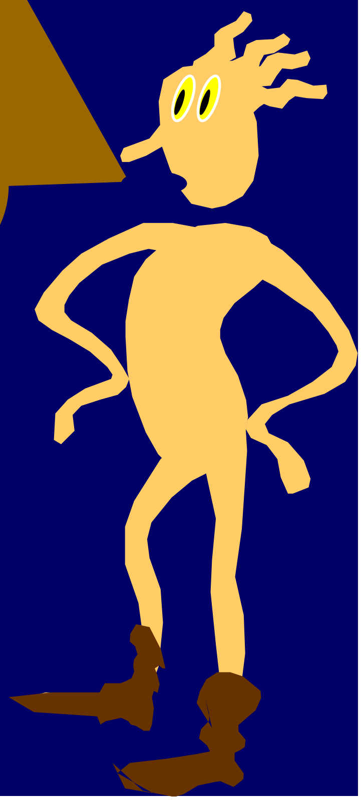


$\aleph_0, \aleph_1, \aleph_2, \ldots$

Let $S = \{\aleph_k \mid k \in \mathbb{N}\}$

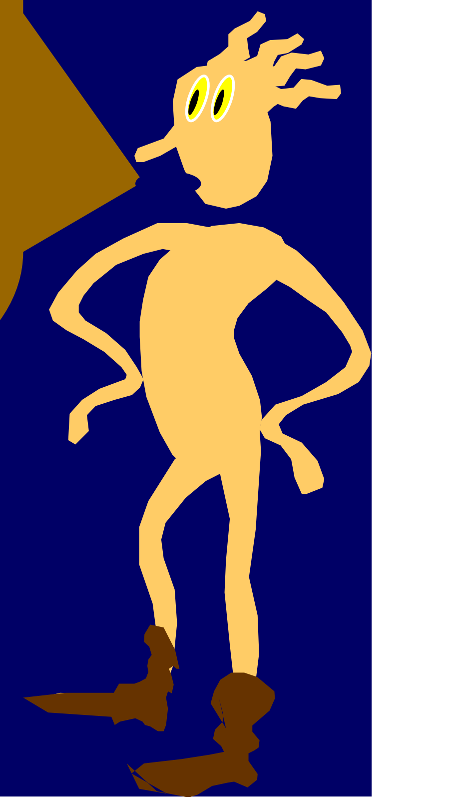
$\mathcal{P}(S)$ is provably larger than any of them.

In fact, the same argument can be used to show that no single infinity is big enough to count the number of infinities!



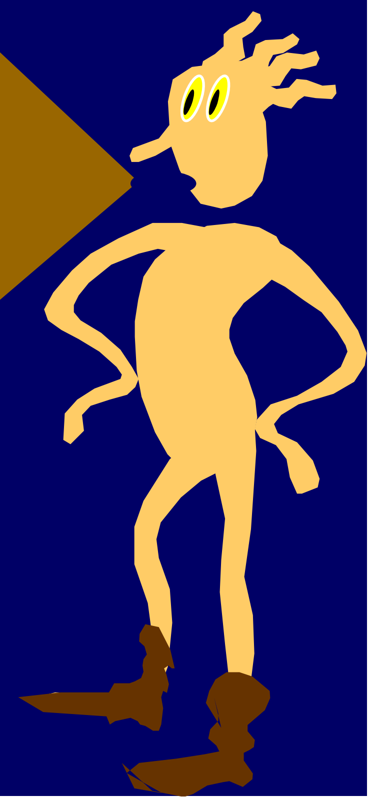
$\aleph_0, \aleph_1, \aleph_2, \ldots$

Cantor wanted to show that the number of reals was $\aleph_1$



Cantor called his conjecture that $\aleph_1$ was the number of reals the "Continuum Hypothesis."

However, he was unable to prove it. This helped fuel his depression.



The Continuum Hypothesis can't be proved or disproved from the standard axioms of set theory!

This has been proved!