Infinity And Diagonalization

$$\infty$$

Attribution

- These slides were prepared for the New Jersey Governor’s School course “The Math Behind the Machine” taught in the summer of 2011 by Grant Schoenebeck
- Large parts of these slides were copied or modified from the previous years’ courses given by Troy Lee in 2010 and Ryan and Virginia Williams in 2009.

Questions?

Questions about infinity

- Is infinity one number?
- If you add one to infinity, you get infinity:
  - What if you square infinity?
  - What if you index infinity by itself?

The Ideal Computer

- An <u>Ideal Computer</u> is defined as a computer with infinite memory.
  - Unlimited memory
  - Unlimited time
  - can run a Java program and never have any overflow or out of memory errors.

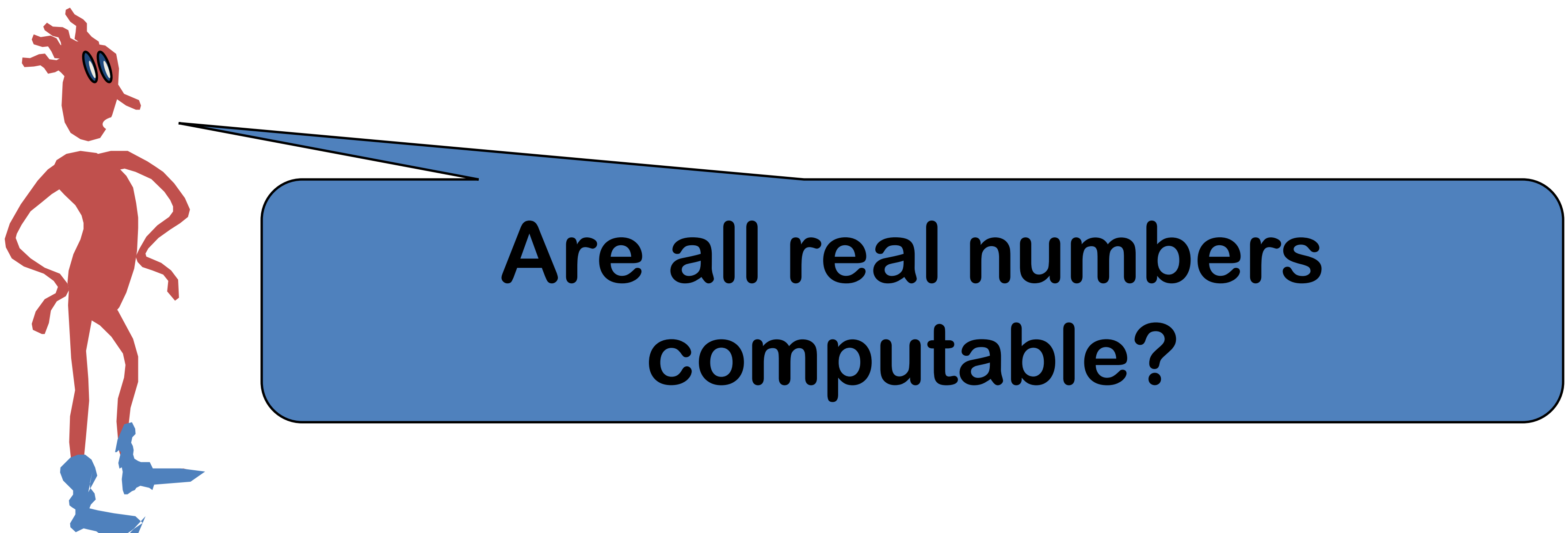
Ideal Computers and Computable Numbers

An Ideal Computer Can Be Programmed To Print Out:

- π: 3.14159265358979323846264…
- 2: 2.00000000000000000000000…
- e: 2.71828182845904523536…
- 1/3: 0.33333333333333333333….

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. Any particular digit of r will eventually be printed as part of the output sequence.

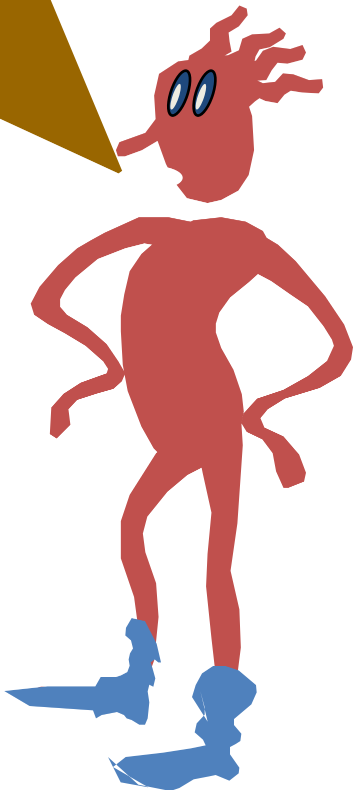


Describable Numbers

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

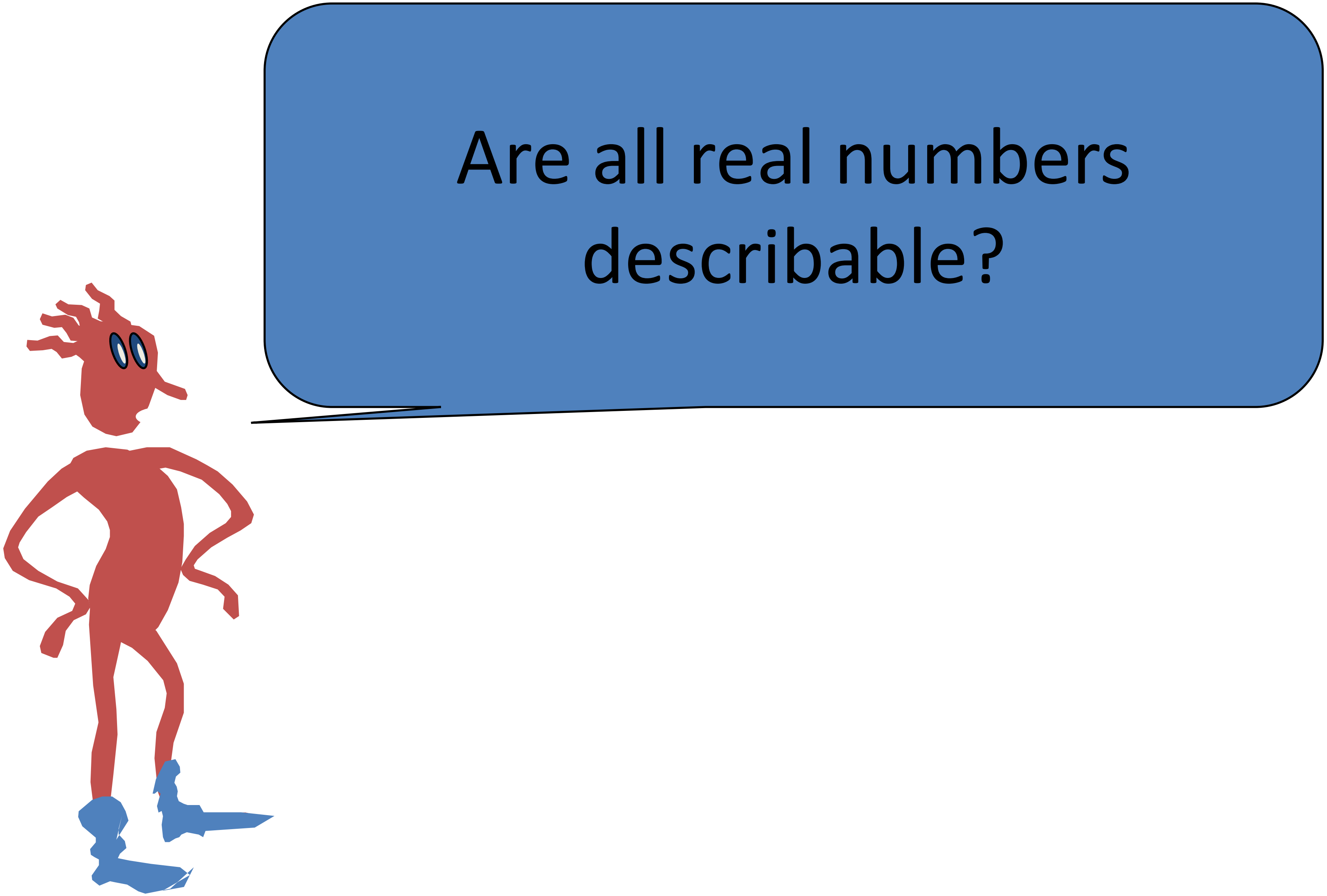
- 2: “Two.”
- π: “The area of a circle of radius one.”

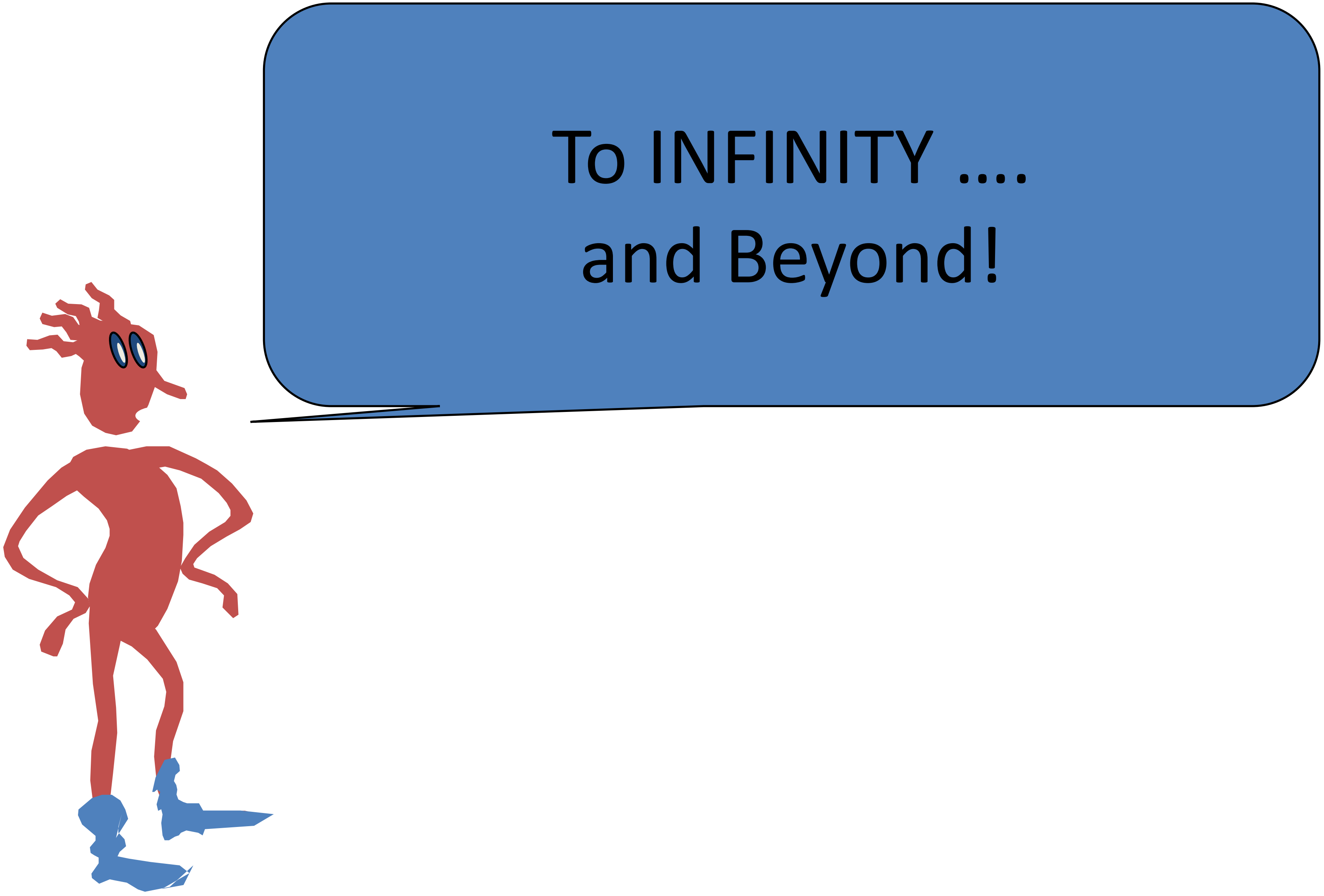
Is every computable real number, also a describable real number?



Computable r: some program outputs r

Describable r: some sentence denotes r


Are all real numbers describable?


To INFINITY ….
and Beyond!

Bijections

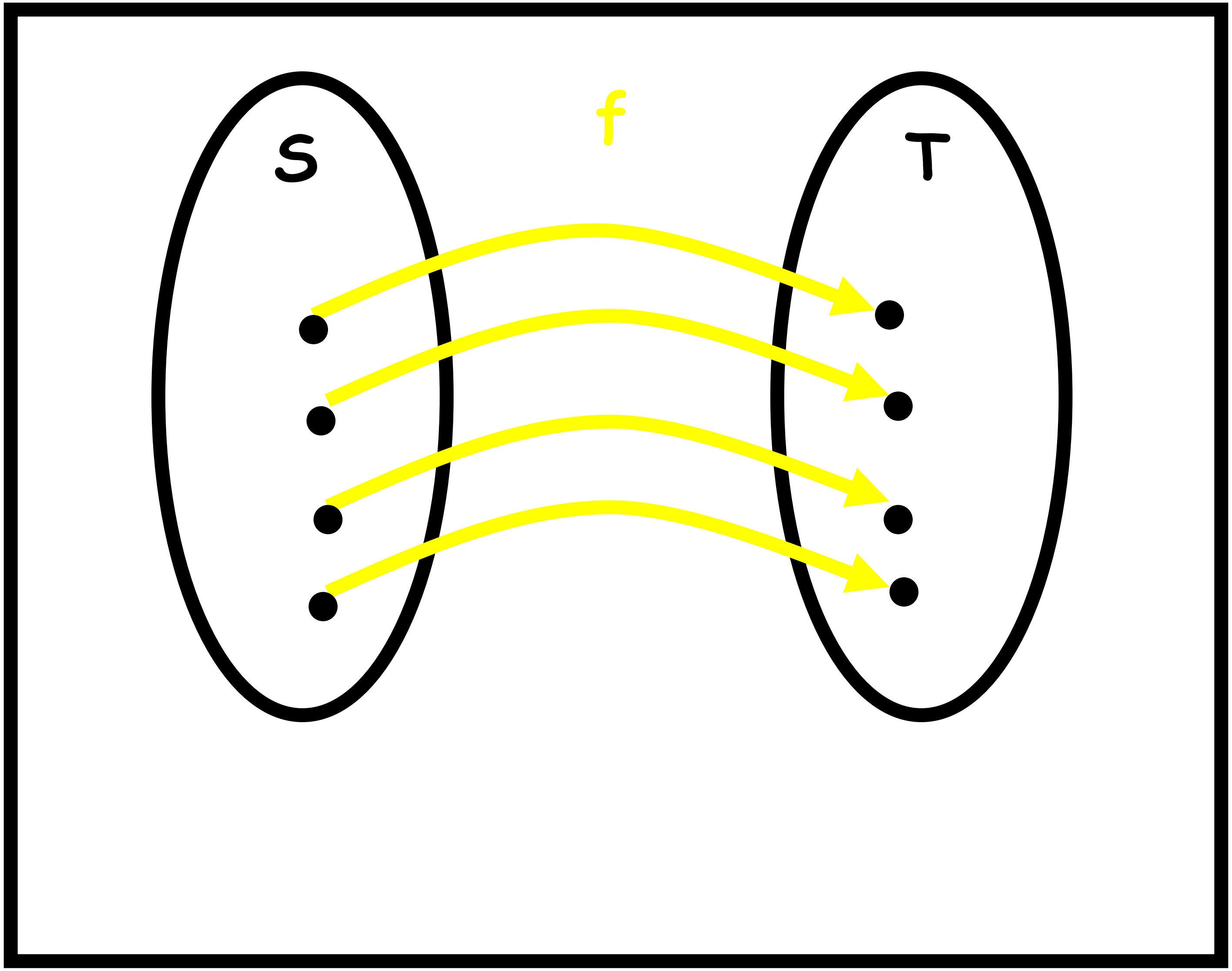
Let S and T be sets.

A function f from S to T is a bijection if:

f is "one to one": $x \neq y$ implies $f(x) \neq f(y)$

f is "onto": for every t in T, there is an s in S such that $f(s) = t$

Intuitively: The elements of S can all be paired up with the elements of T



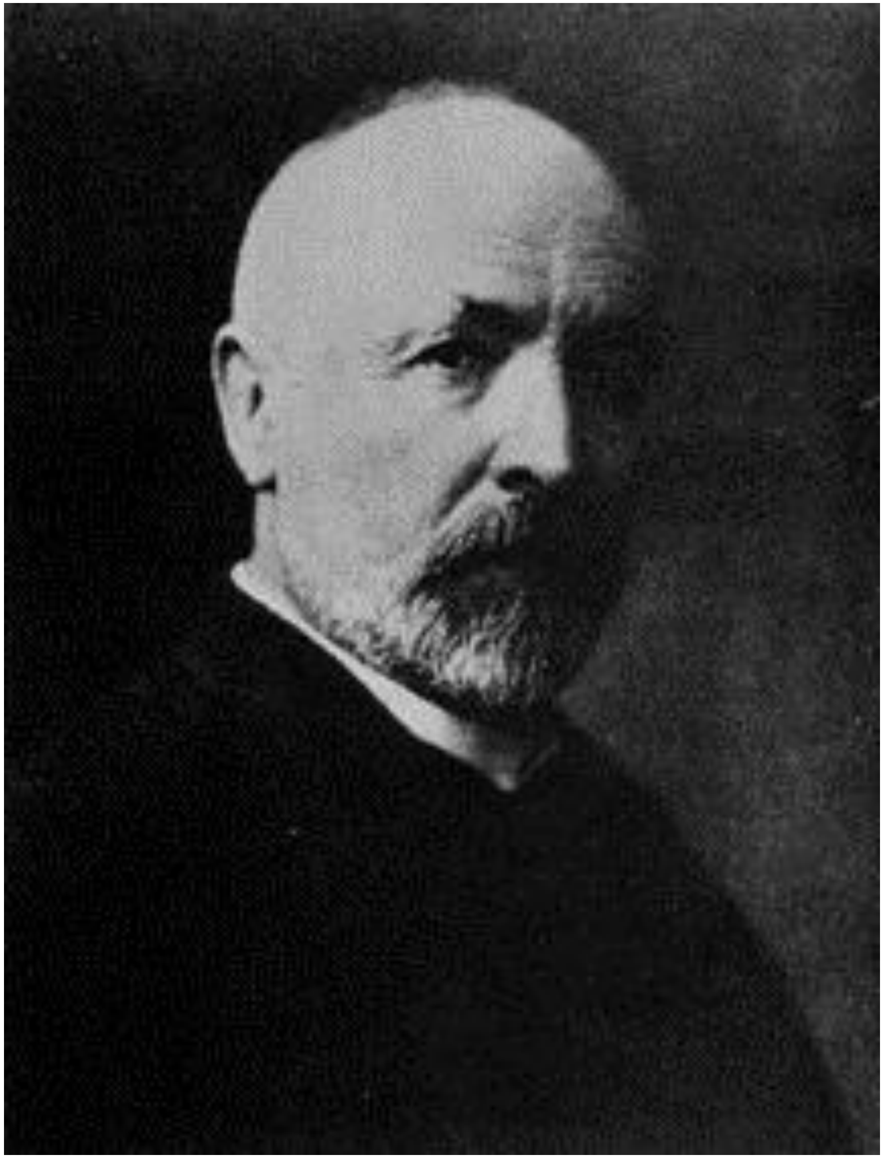
Note: if there is a bijection from S to T then there is a bijection from T to S!

So it makes sense to say “bijection between A and B”

Correspondence Definition

- Two finite sets S and T are defined to have the <u>same size</u> if and only if there is a bijection from S to T.

Georg Cantor (1845-1918)



Cantor's Definition (1874)

- Two **infinite** sets are defined to have the same size
- if and only if there is a bijection between them.

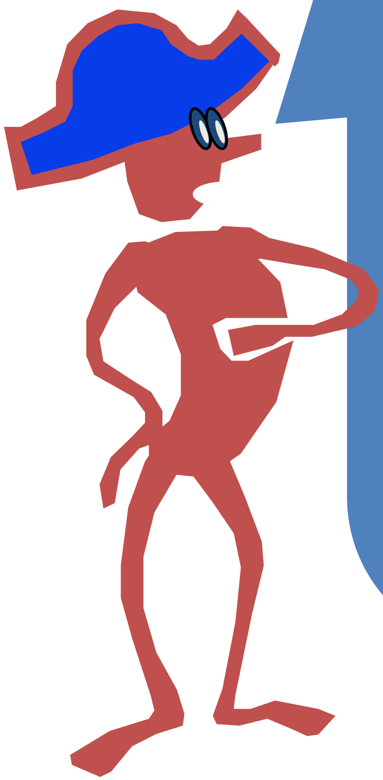
Cantor’s Definition (1874)

- Two **infinite** sets are defined to have the same cardinality
- if and only if there is a bijection between them.

Do **N** and **E** have the same cardinality?

- **N** = { 0, 1, 2, 3, 4, 5, 6, 7, … }

E = { 0, 2, 4, 6, 8, 10, 12, 14, … }



E and **N** do not have the same cardinality!

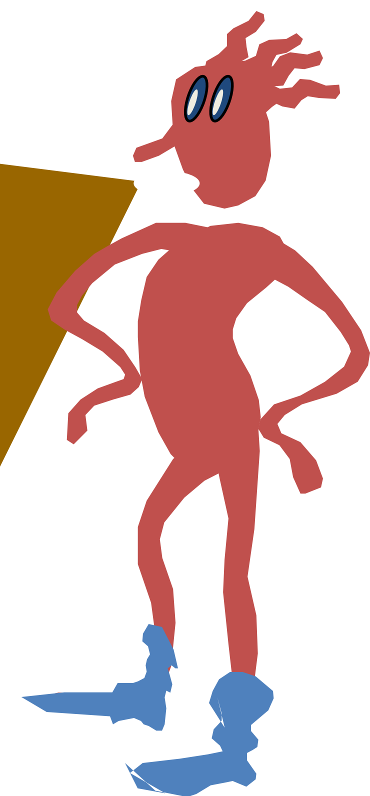
E is a proper subset of **N** with plenty left over.

That is, f(x)=x does not work as a bijection from **N** to **E**

E and **N** do have the same cardinality!

$$\begin{array}{ccccccccc}
 & 0, & 1, & 2, & 3, & 4, & 5, & \ldots & \\
f & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & | \\
 & 0, & 2, & 4, & 6, & 8, & 10, & \ldots &
\end{array}$$

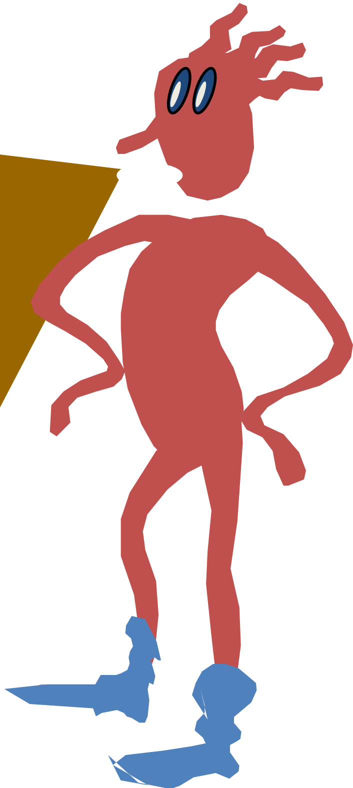
$f(x) = 2x$ is a bijection from **N** to **E**!



Lessons:

Just because some bijection doesn’t work, that doesn’t mean another bijection won’t work!

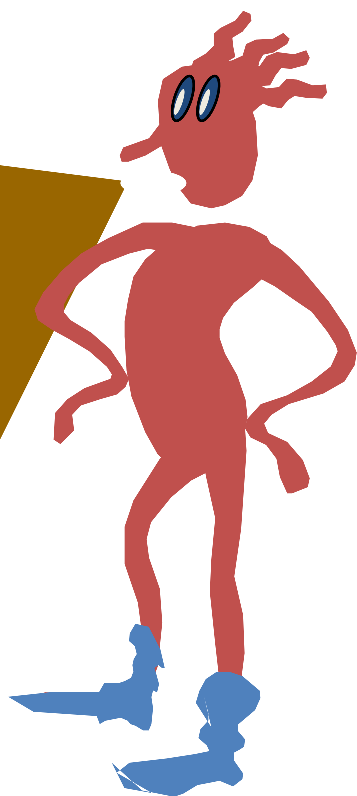
Infinity is a mighty big place.
It allows the even numbers to have room to accommodate all the natural numbers



If this makes you feel uncomfortable…

TOUGH!

It is the price that you must pay to reason about infinity



Do **N** and **Z** have the same cardinality?

N = { 0, 1, 2, 3, 4, 5, 6, 7, …. }

Z = { …, -2, -1, 0, 1, 2, 3, …. }

No way! **Z** is infinite in two ways: from 0 to positive infinity and from 0 to negative infinity.

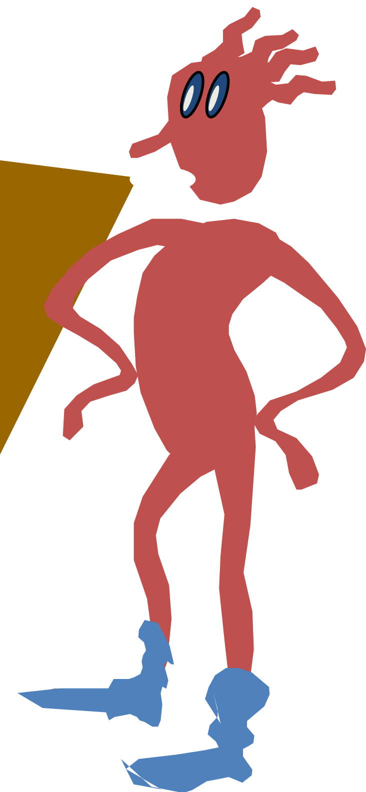
Therefore, there are far more integers than naturals.

Actually, no…

N and **Z** do have the same cardinality!

0, 1, 2, 3, 4, 5, 6 …
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

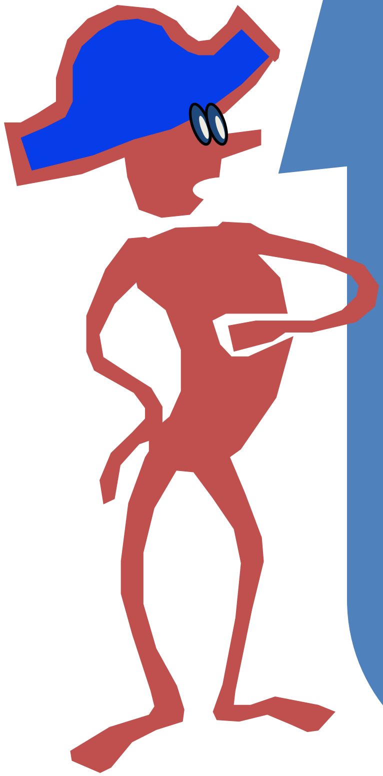
- If $f: A \to B$ and $g: B \to C$ are bijections,
- Then
  $h(x) = g(f(x))$ is a bijection from $A \to C$

- **It follows that $\mathbb{N}$, $\mathbb{E}$, and $\mathbb{Z}$**
- **all have the same cardinality.**

Do **N** and **Q** have the same cardinality?

N = { 0, 1, 2, 3, 4, 5, 6, 7, …. }

Q = The Rational Numbers
(All possible fractions!)



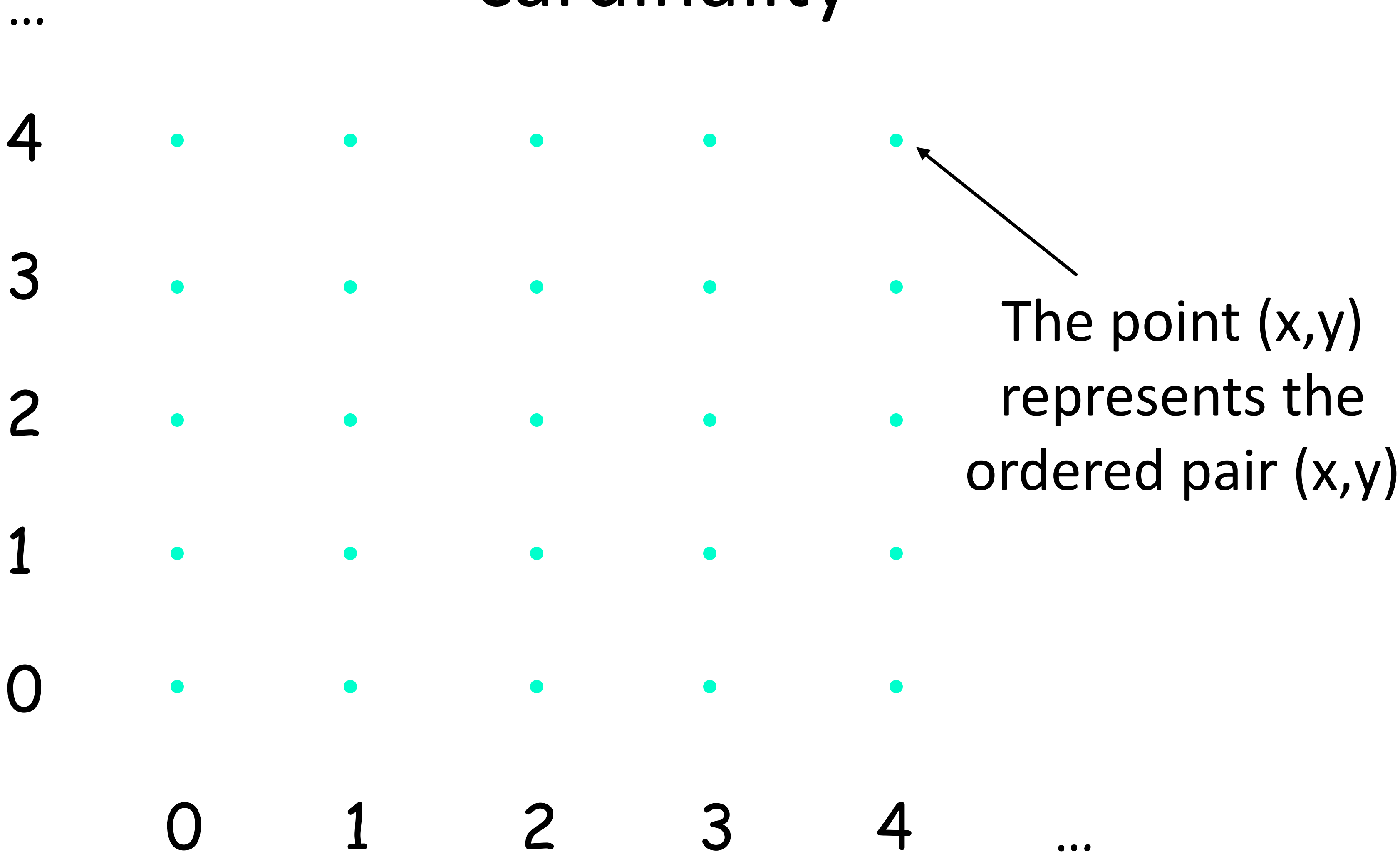
No way!
The rationals are dense: between any two there is a third. You can’t list them one by one without leaving out an infinite number of them.

Don’t jump to conclusions! There is a clever way to list the rationals, one at a time, without missing a single one!

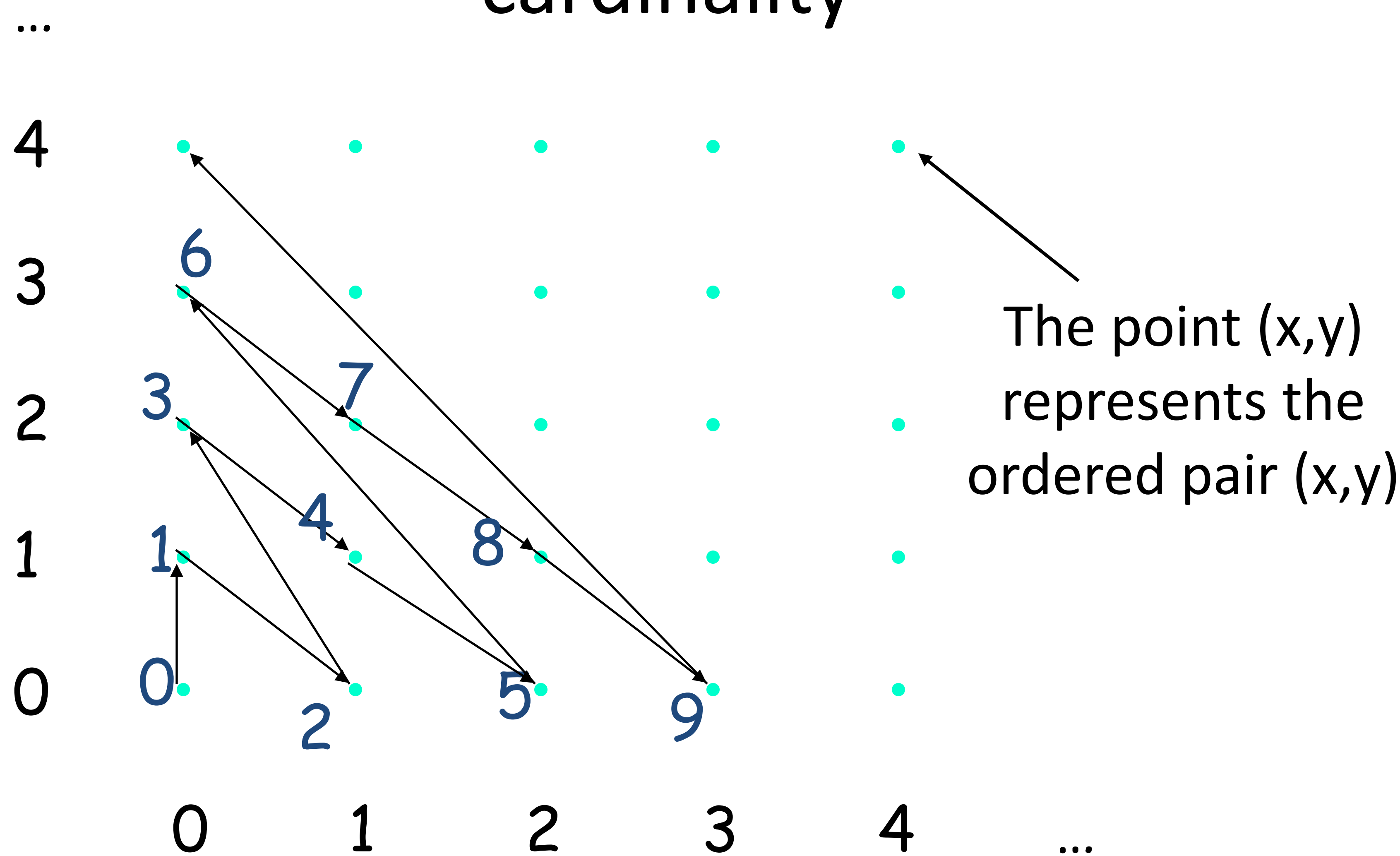
First, let’s warm up with another interesting one:

N can be paired with **NxN**

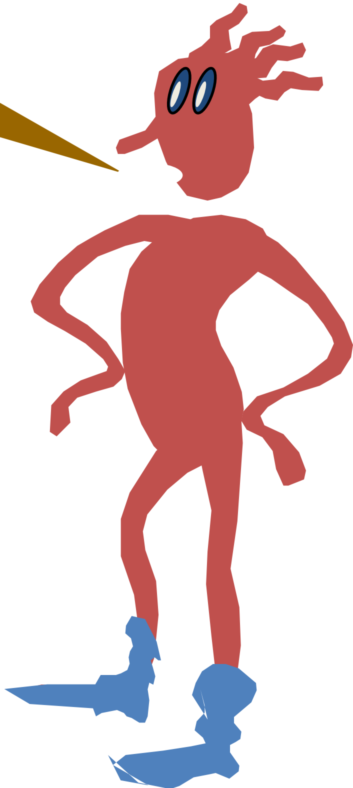
Theorem: **N** and **N** x **N** have the same cardinality

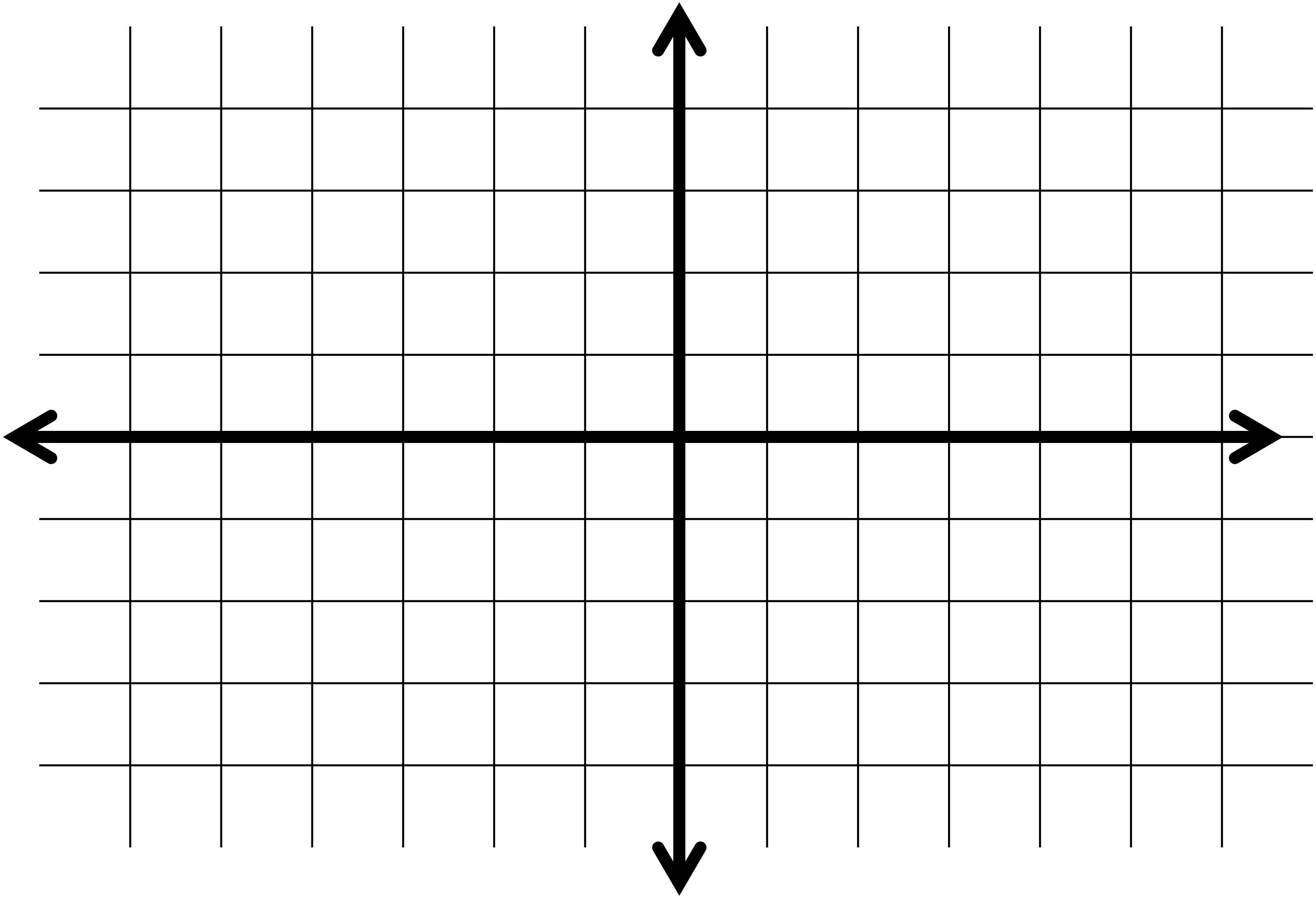


Theorem: **N** and **N** x **N** have the same cardinality

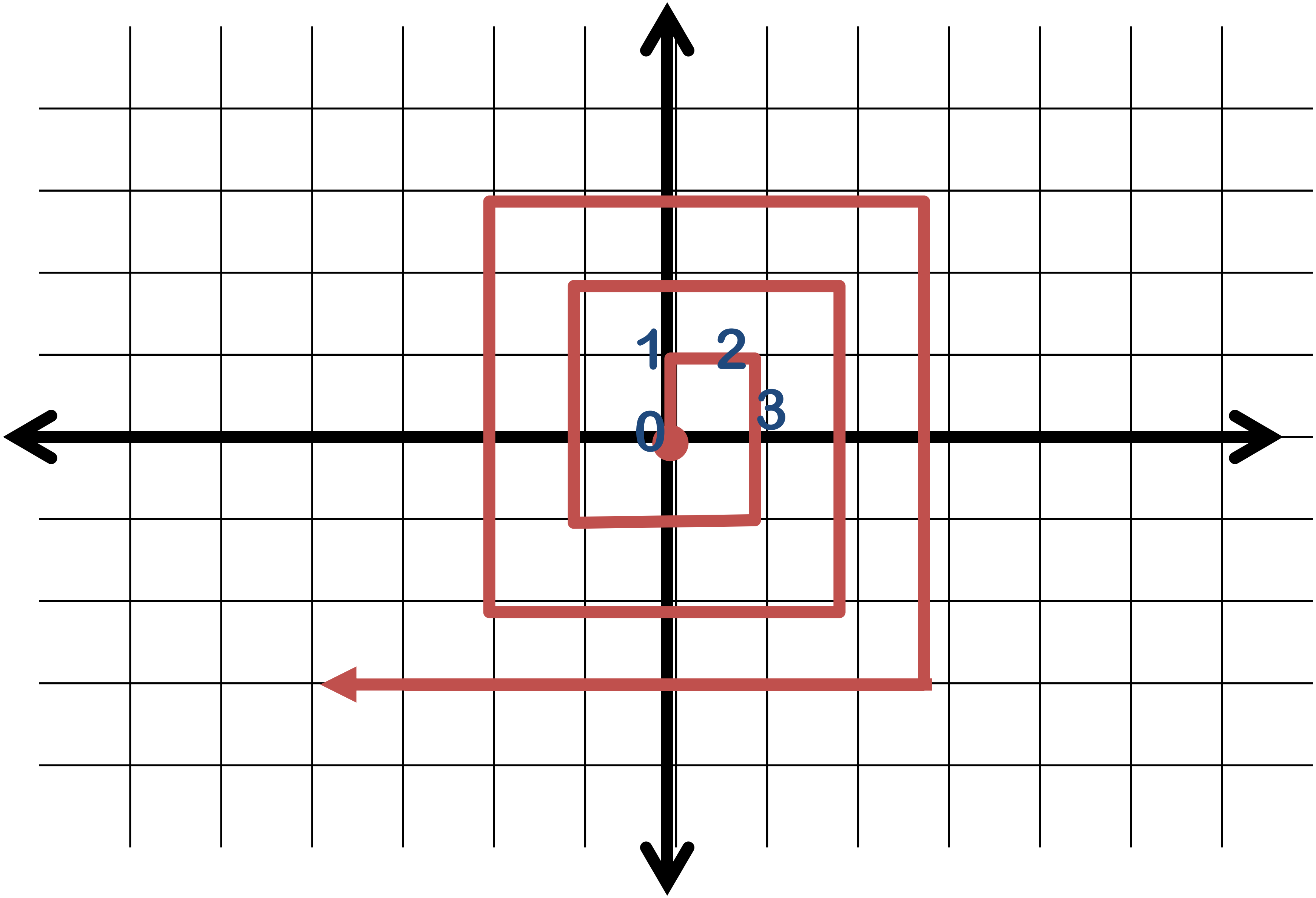


On to the Rationals!





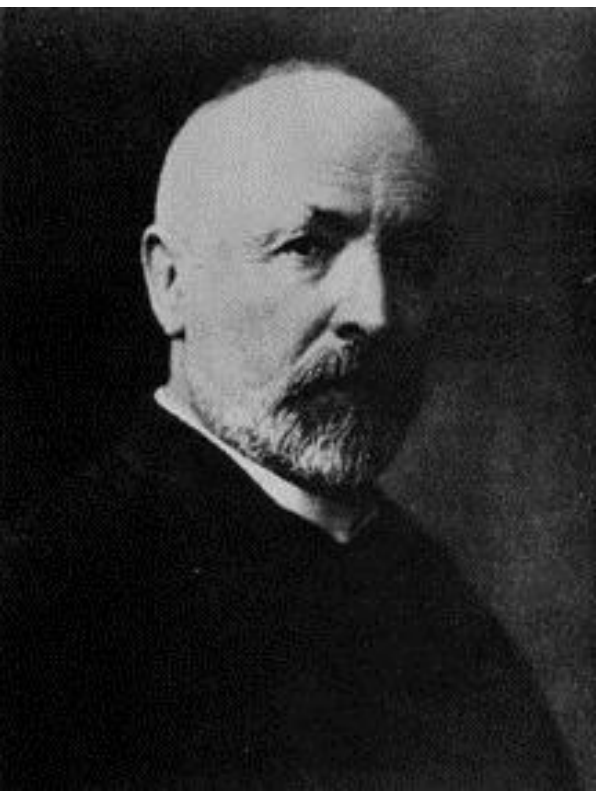
The point at x,y represents x/y



The point at x,y represents x/y

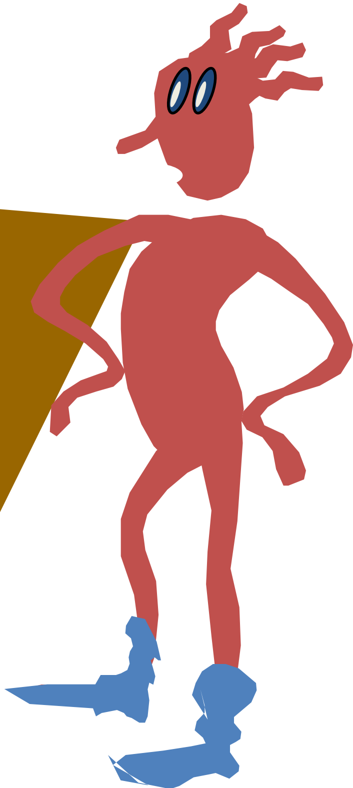
- *1877 letter to Dedekind:*

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



We call a set countable if it has a bijection with the natural numbers.

So far we know that N, E, Z, and Q are countable.

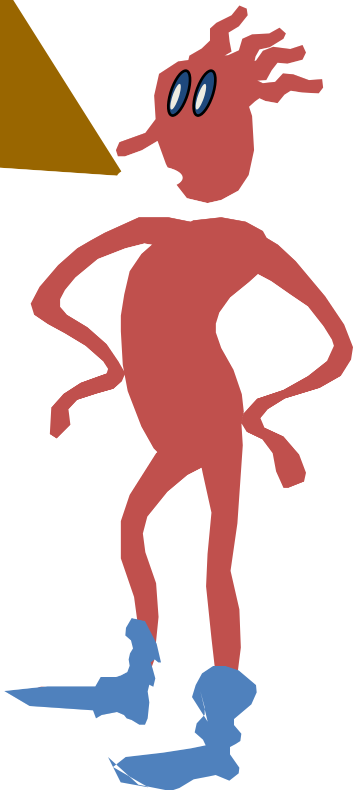


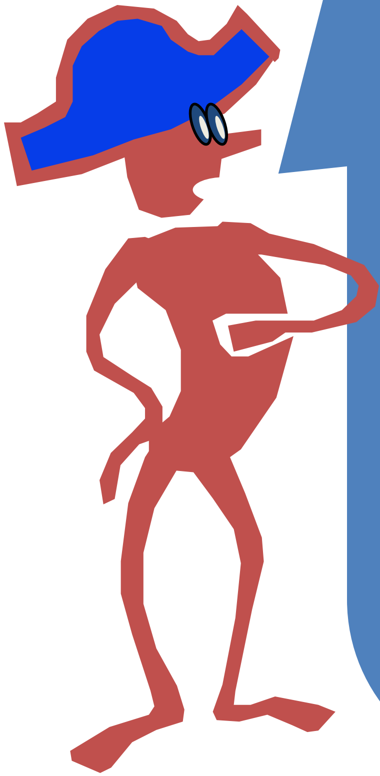
Do **N** and **R** have the same cardinality?

N = { 0, 1, 2, 3, 4, 5, 6, 7, …. }

R = The Real Numbers

No way!
You will run out of natural numbers long before you match up every real.





Don’t jump to conclusions!

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.

He invented a very important technique called “DIAGONALIZATION”

Theorem: The set **I** of reals between 0 and 1 is not countable.

- **Proof by contradiction:**
- Suppose **I** is countable.
- Let f be the bijection from **N** to **I**. 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 **I** of reals between 0 and 1 is not countable.

Proof by contradiction:

Suppose **I** is countable.

Let f be the bijection from **N** to **I**. Make a list L as follows:

(This must be a complete list of **I**)

0: .33333333333333333333333…
1: .31415926565783959385949 82..

…

k: .34532221424355534522112 3235..

…

L	0	1	2	3	4	...
0	3	3	3	3	3	3
1	3	1	4	5	9	2
2	...					
3						
...						

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

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

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

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

$$C_k = \begin{cases} 1, \text{ if } d_k = 2 \\ 2, \text{ otherwise} \end{cases}$$

Claim:
Confuse$_L$ is
not in the list L!

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

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

…

$$c_k = \begin{cases} 1, \text{ if } d_k = 2 \\ 2, \text{ otherwise} \end{cases}$$

Claim:

Confuse_L is not in the list L!

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		
…					…	

$$C_k = \begin{cases} 1, & \text{if } d_k = 2 \\ 2, & \text{otherwise} \end{cases}$$

Claim:

Confuse_L is not in the list L!

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	
...					...

…

$$C_k = \begin{cases} 1, \text{ if } d_k = 2 \\ 2, \text{ otherwise} \end{cases}$$

Claim:

$Confuse_L$ is not in the list L!

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	
…					…

…

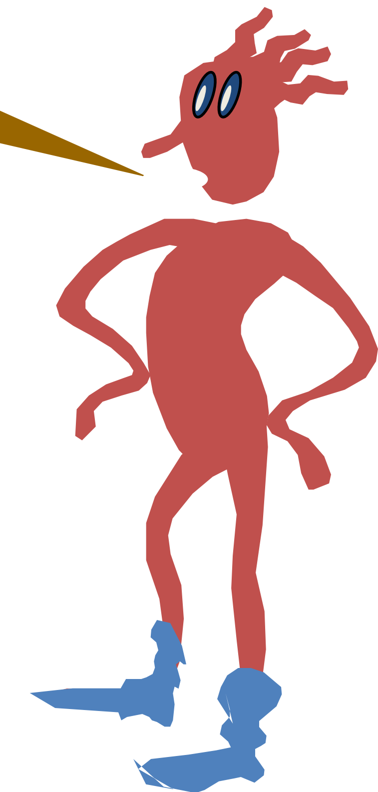
$$C_k = \begin{cases} 1, \text{ if } d_k = 2 \\ 2, \text{ otherwise} \end{cases}$$

Claim:

Confuse_L is not in the list L!

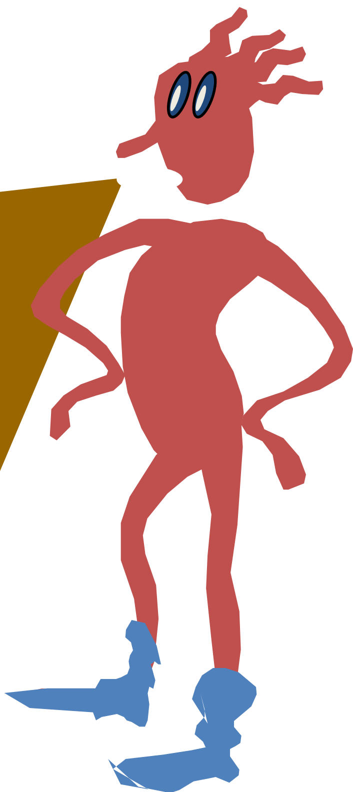
Confuse_L differs from the k^{th} element of L in the k^{th} position. This contradicts our assumption that list L has all reals in I.

The set of reals is uncountable!



Hold it!
Why can't the same argument be used to show that Q is uncountable?

The argument works the same for Q until the very end. Confuse_L is not necessarily a rational number, so there is no contradiction from the fact that it is missing from list L.



Standard Notation

Σ = Any finite alphabet

Example: {a,b,c,d,e,…,z}

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

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

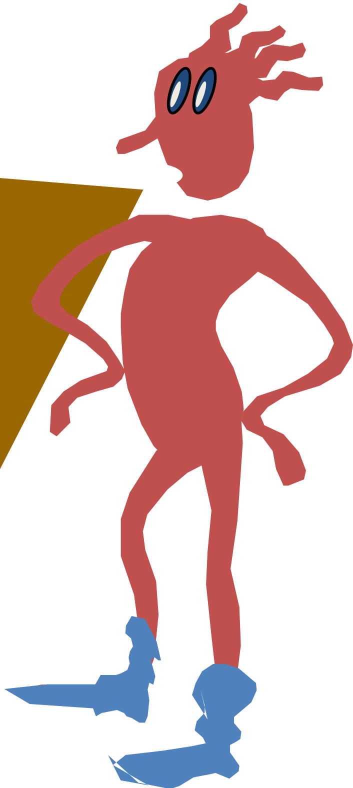
The set of all possible Java programs is a subset of Σ^*

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.

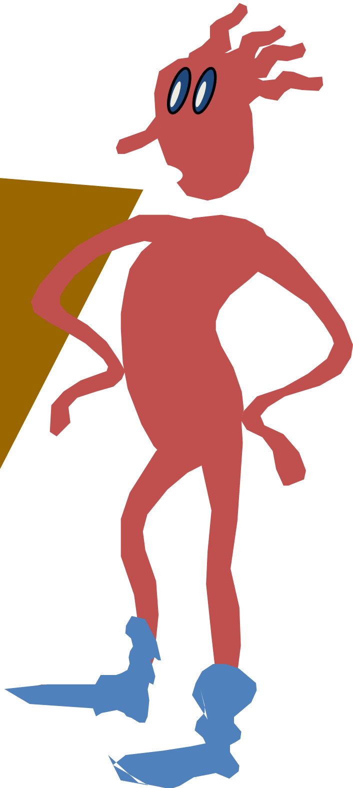
The set of all possible finite length pieces of English text is countable.

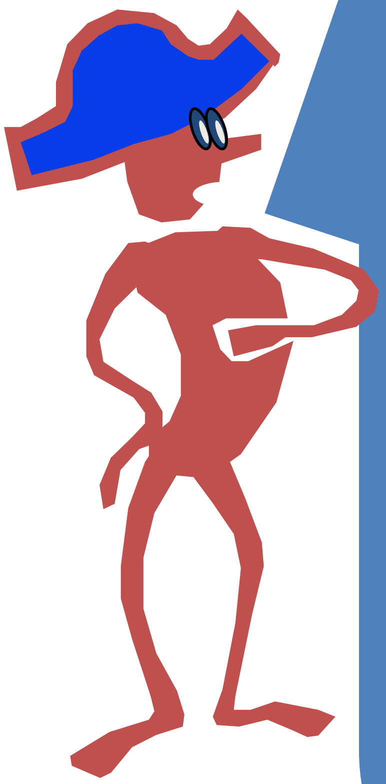


There are countably many Java programs and uncountably many reals.

HENCE:

MOST REALS ARE NOT COMPUTABLE.





There are countably many descriptions and uncountably many reals.

Hence:

MOST REAL NUMBERS ARE NOT DESCRIBABLE IN ENGLISH!

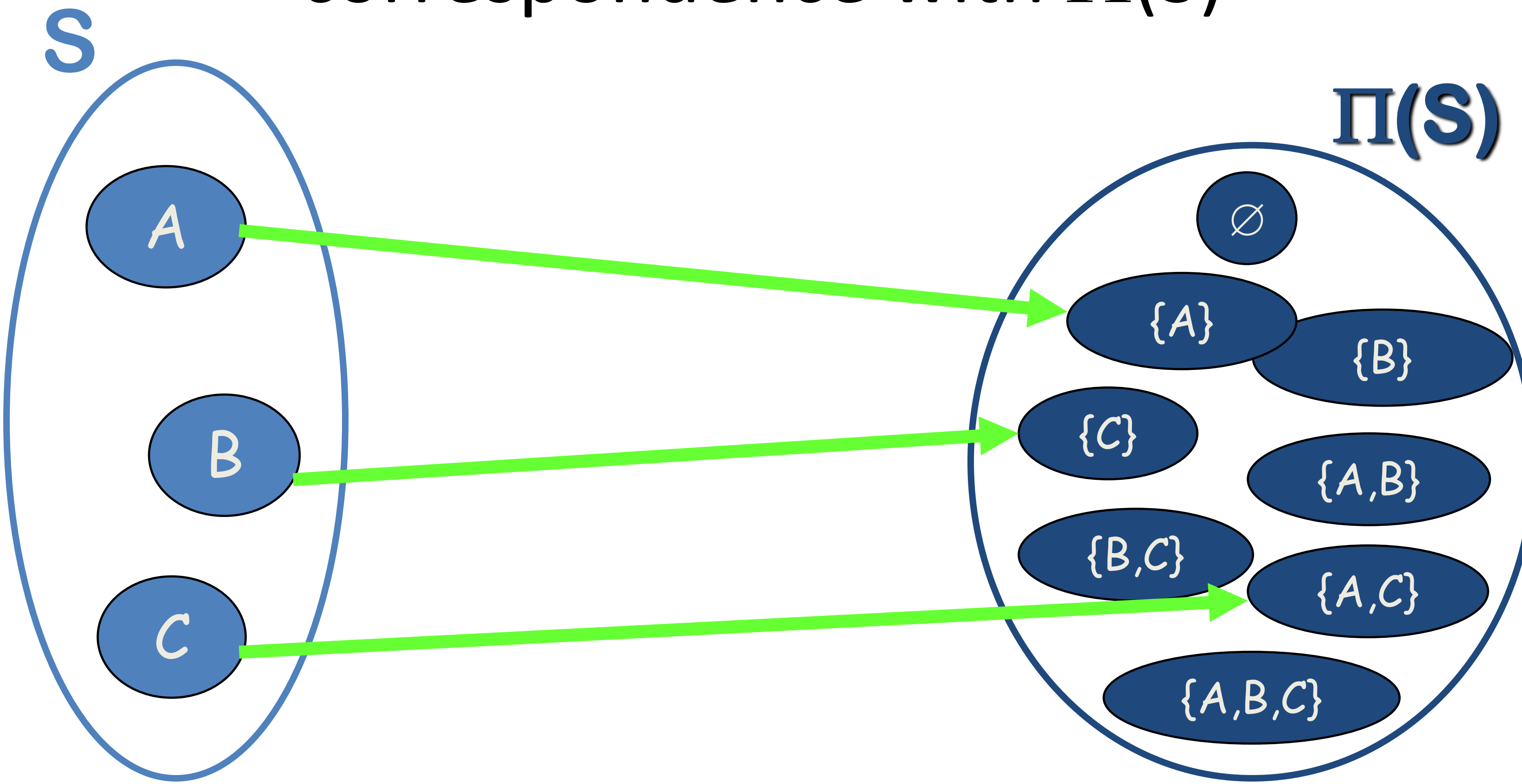
Is there a real number that can be described, but not computed by any program?

We know there are at least 2 infinities. Are there more?

Power Set

- The power set of S is the set of all subsets of S.
- The power set is denoted Π(S).
- Proposition: If S is finite, the power set of S has cardinality $2^{|S|}$

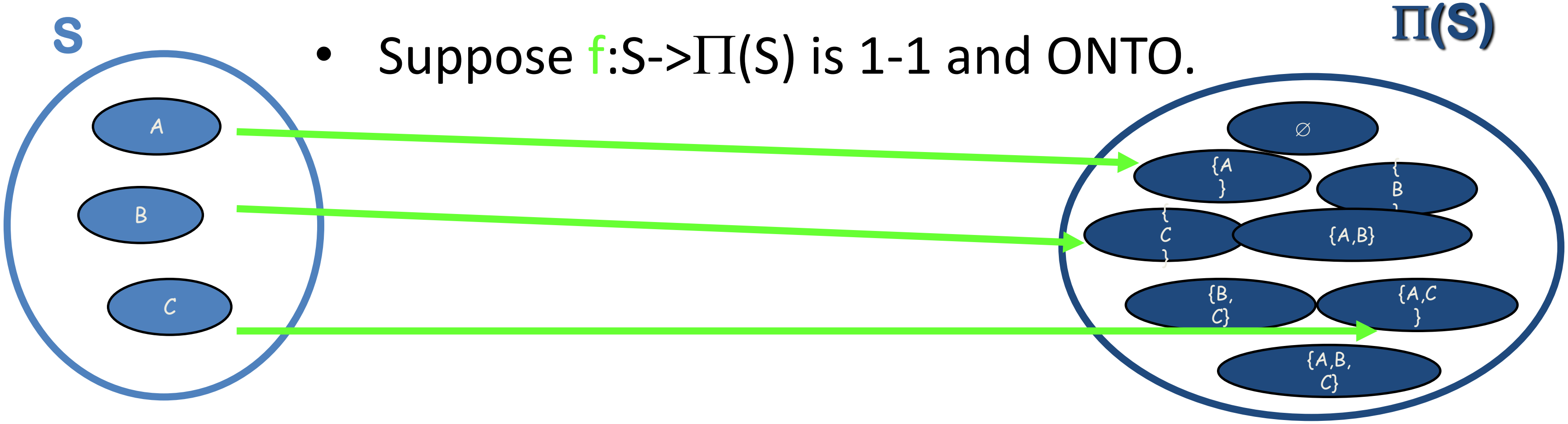
Theorem: S can't be put into 1-1 correspondence with $\Pi(S)$



- Suppose f:S->Π(S) is 1-1 and ONTO.

Theorem: S can't be put into 1-1 correspondence with $\Pi(S)$

- Suppose f:S->$\Pi(S)$ is 1-1 and ONTO.



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

There is some y such that f(y)=CONFUSE

Is y in CONFUSE?

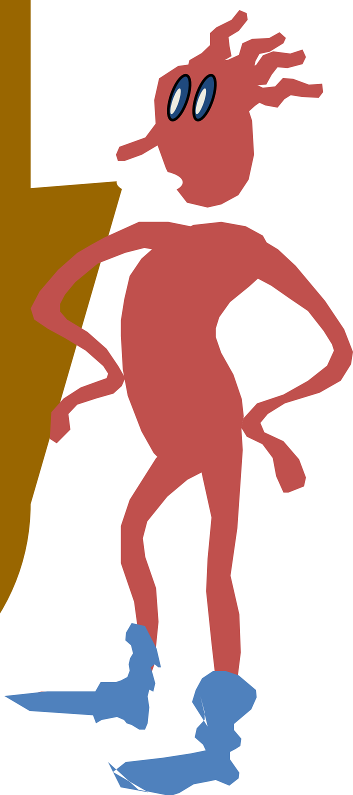
YES: Definition of CONFUSE implies no

NO: Definition of CONFUSE implies yes

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

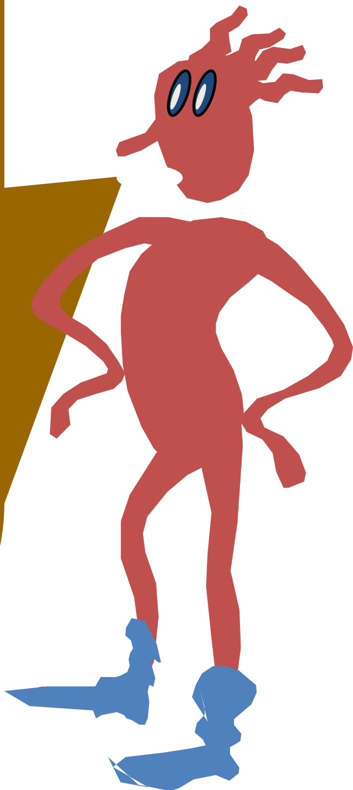
The first infinity is called:

$$\aleph_0$$



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

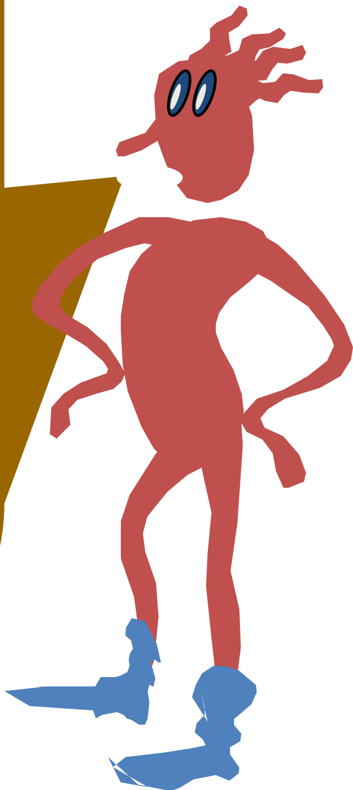
Are there any more infinities?



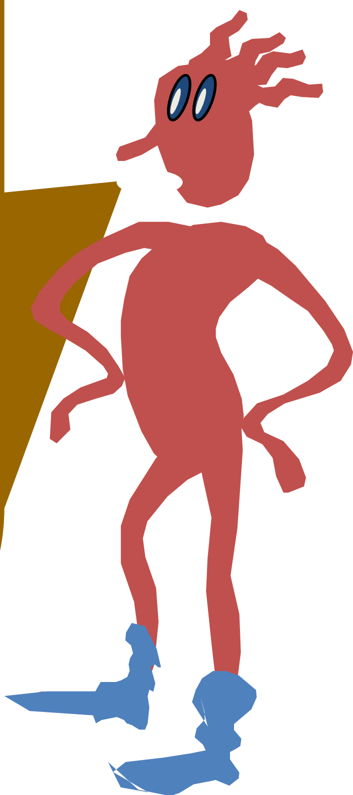
$$\aleph_0, \aleph_1, \aleph_2, \ldots$$

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

$\Pi(S)$ is provably larger than any of them.

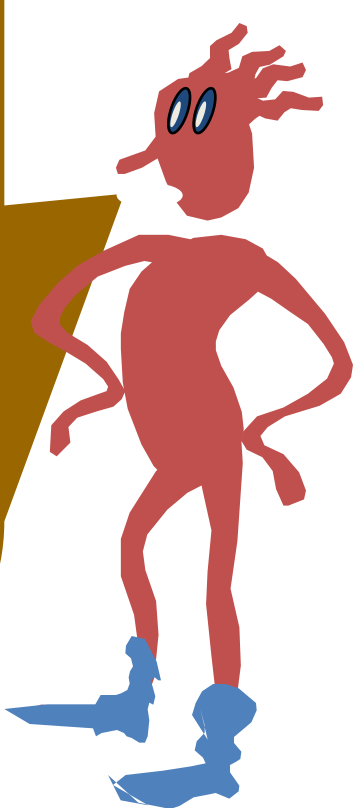


In fact, the same argument can be used to show that no single infinity is big enough to count the number of infinities!

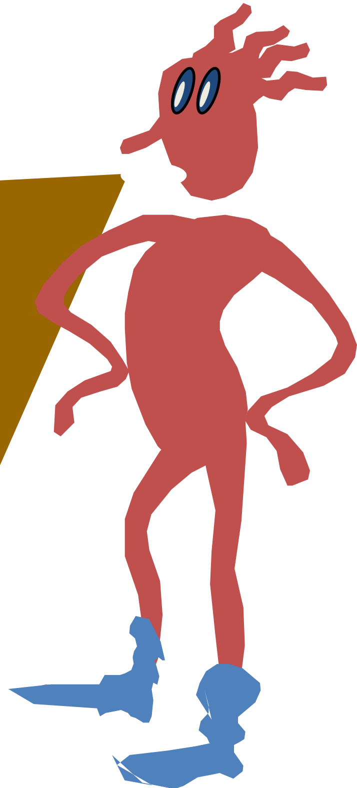


$\aleph_0, \aleph_1, \aleph_2, \ldots$

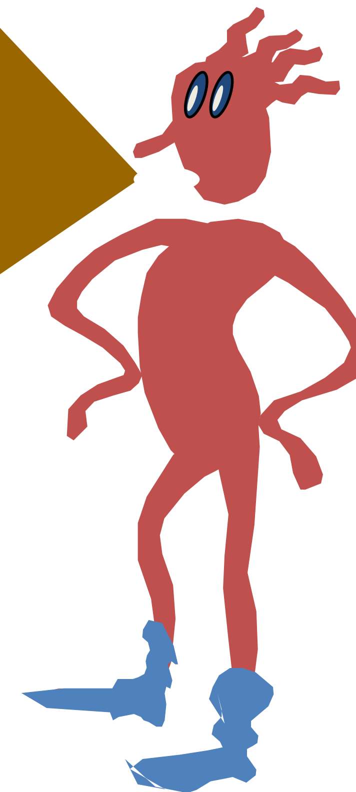
Cantor wanted to show that the number of reals was $\aleph_1$



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!



In fact it was proved here in New Jersey, by professors at the Institute for Advanced Study!