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 2012 by Grant Schoenebeck
- Large parts of these slides were copied or modified from a previous years' course given by 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.

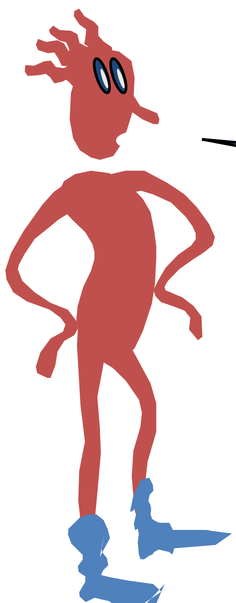
Ideal Computers and Computable Numbers

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.



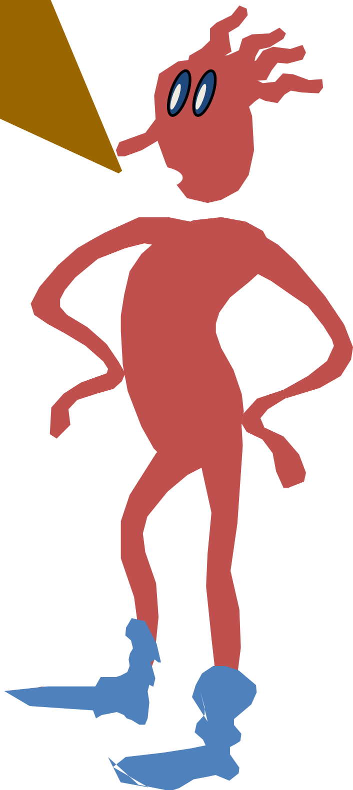
Are all real numbers computable?

Describable Numbers

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

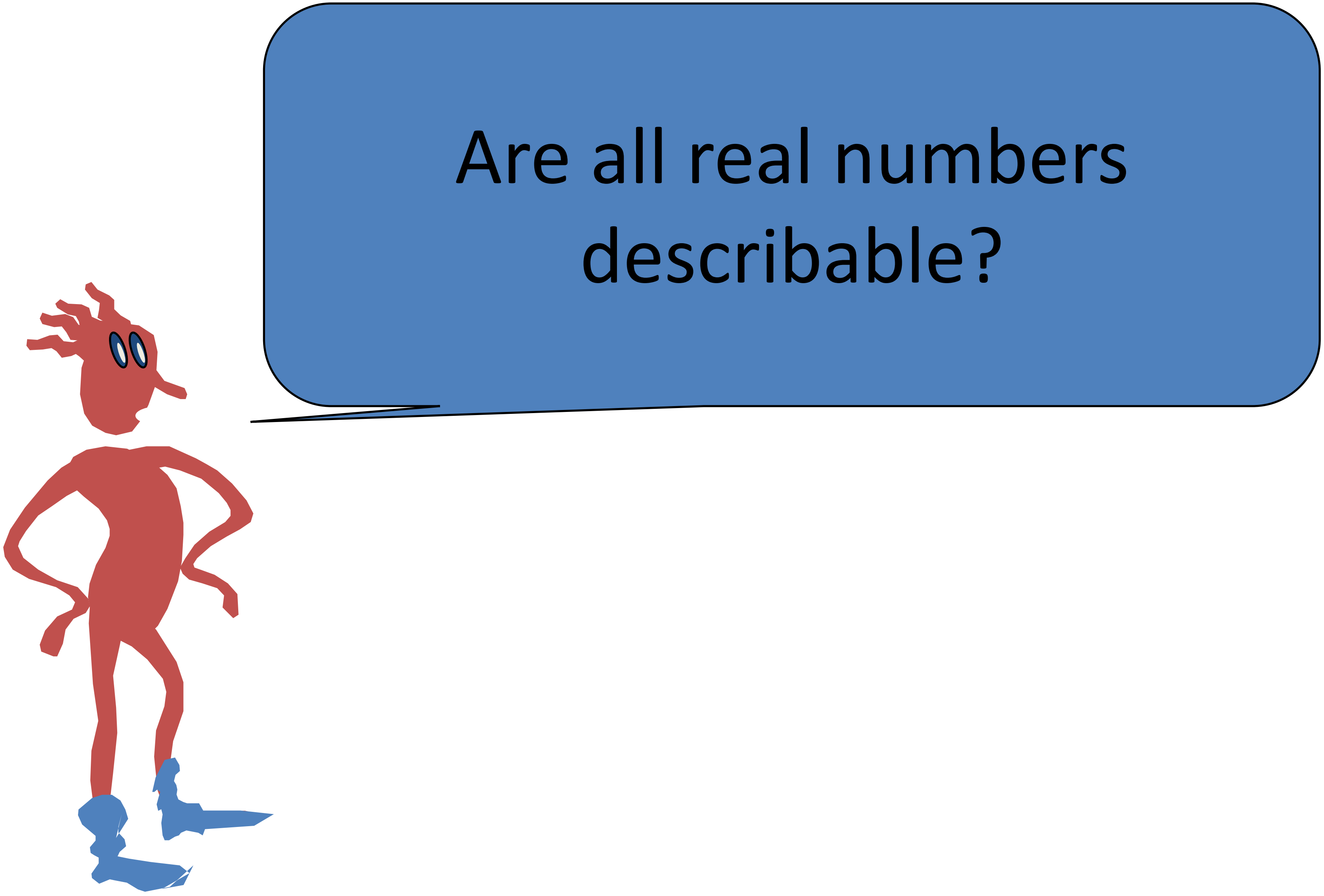
- 2: “Two.”
- π: “The area of a circle of radius one.”

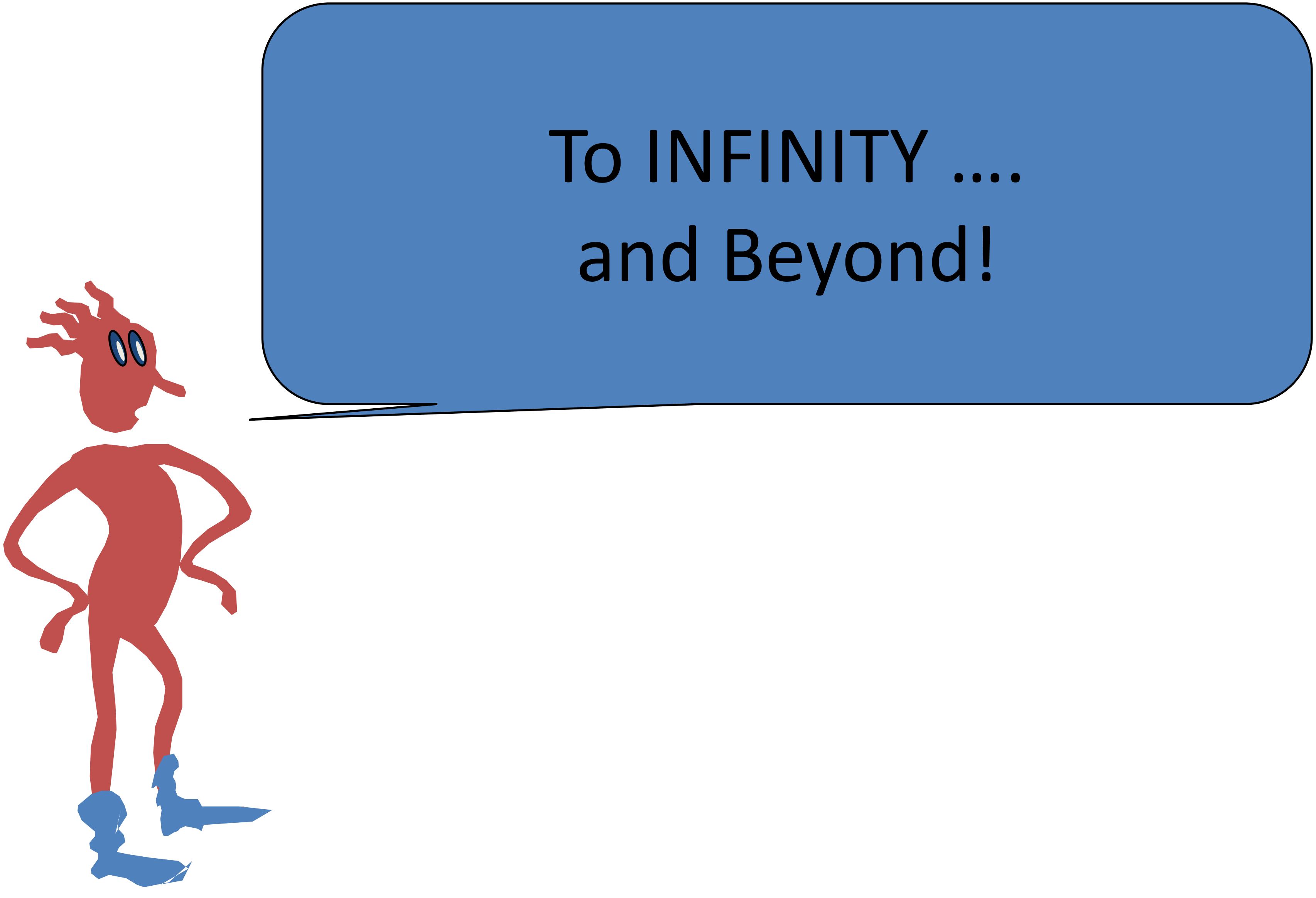
Is every computable real number,
also a describable real number?



Computable r: some program outputs r

Describable r: some sentence denotes r


Are all real numbers describable?


To INFINITY ….
and Beyond!

Bijections

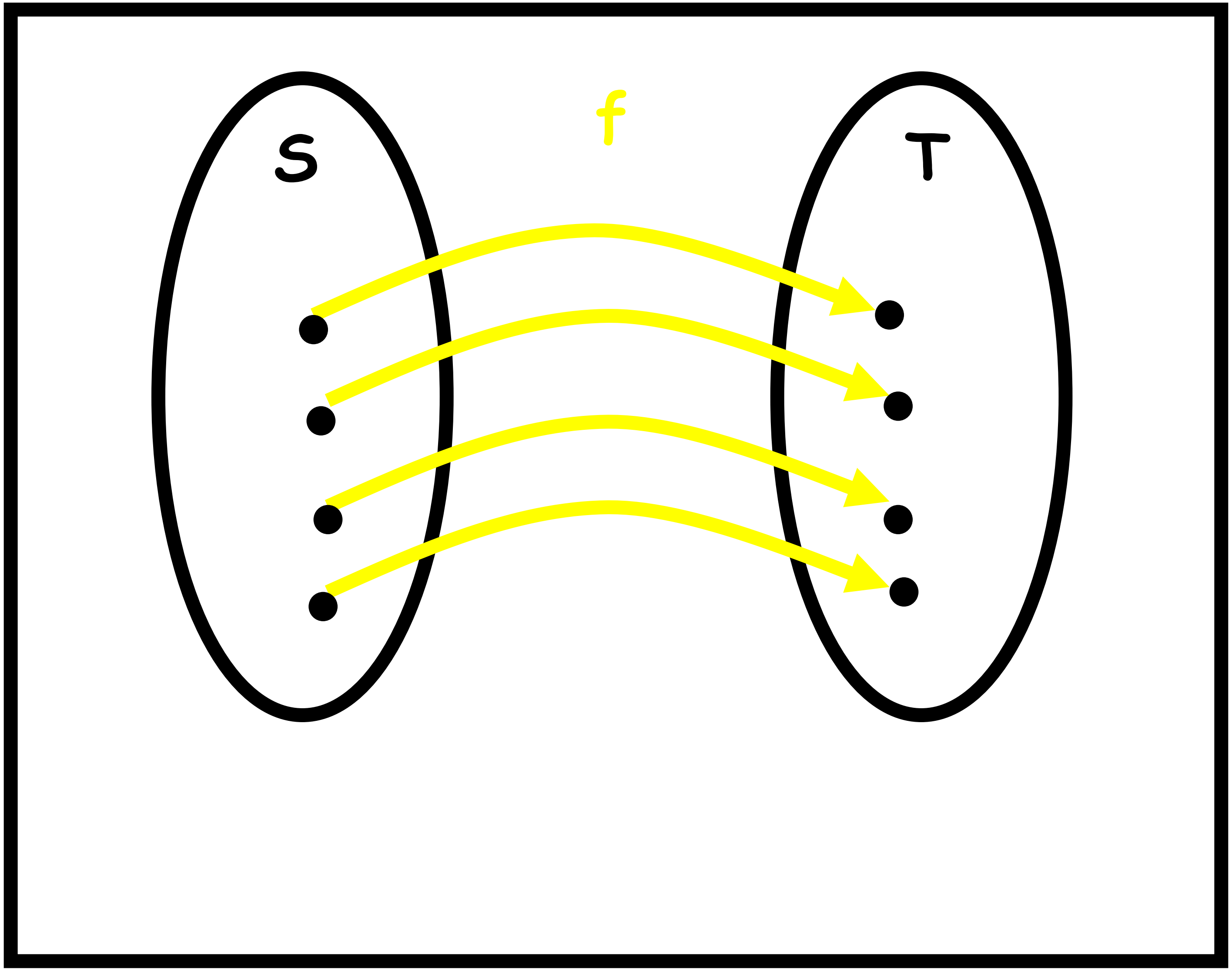
Let S and T be sets.

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

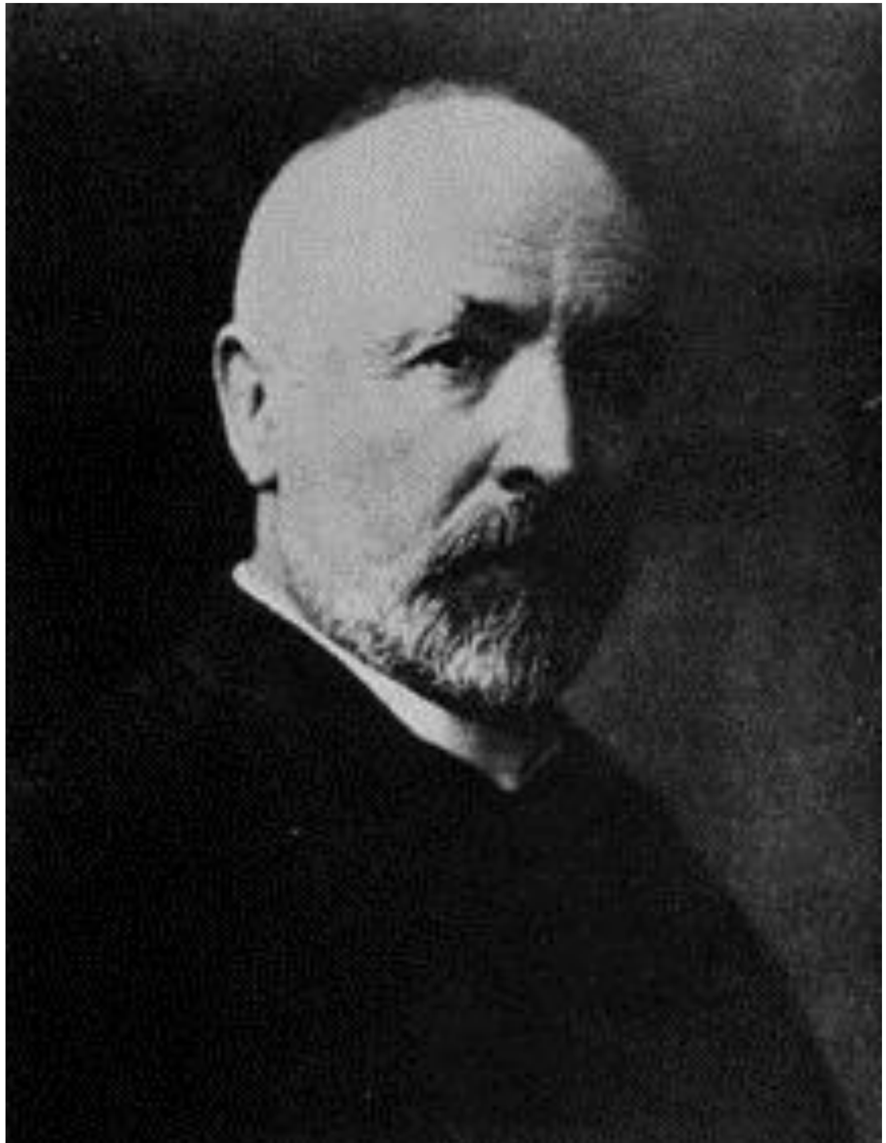


Note: if there is a bijection from S to T
then there is a bijection from T to S!
So it makes sense to say "bijection between A and B"

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.

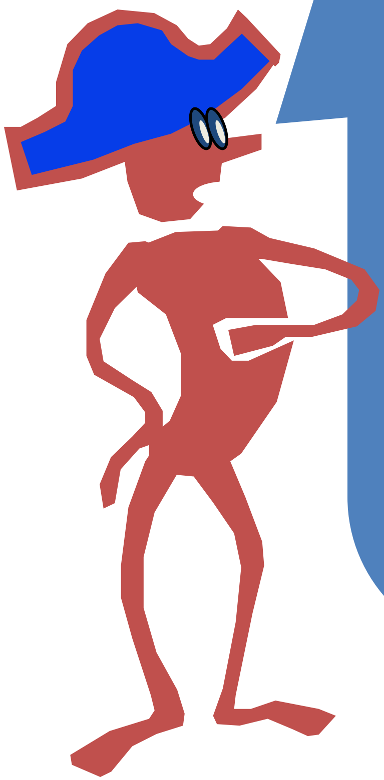
Cantor's Definition (1874)

- 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!

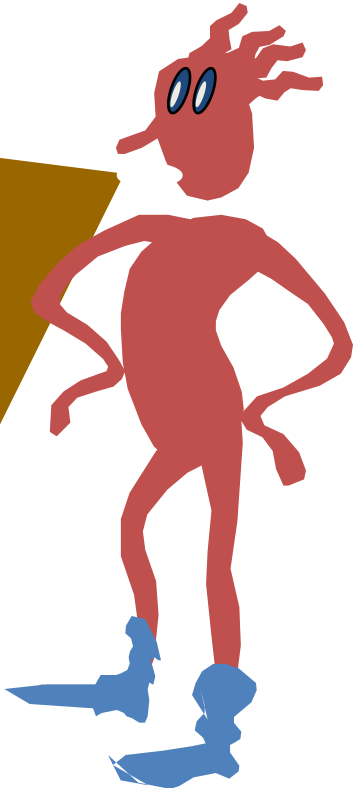
E is a proper subset of **N** with plenty left over.

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

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

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

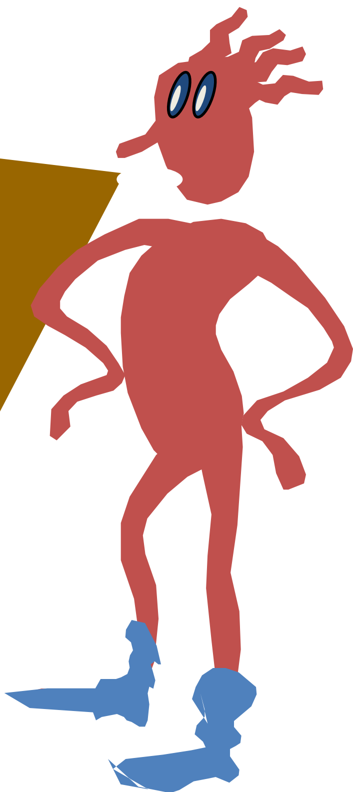
$f(x) = 2x$ is a bijection from **N** to **E**!



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



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.

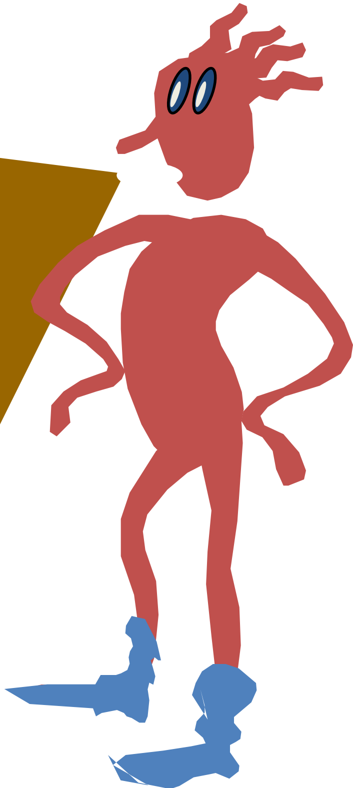
Actually, no…

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

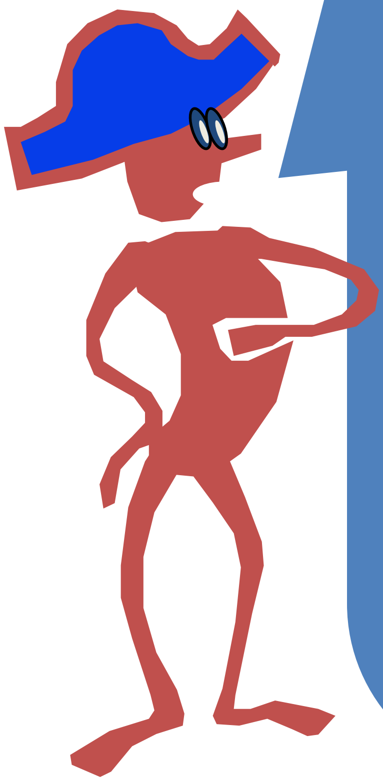
- If $f: A \rightarrow B$ and $g: B \rightarrow C$ are bijections,
- Then
  $h(x) = g(f(x))$ is a bijection from $A \rightarrow C$

- **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!)



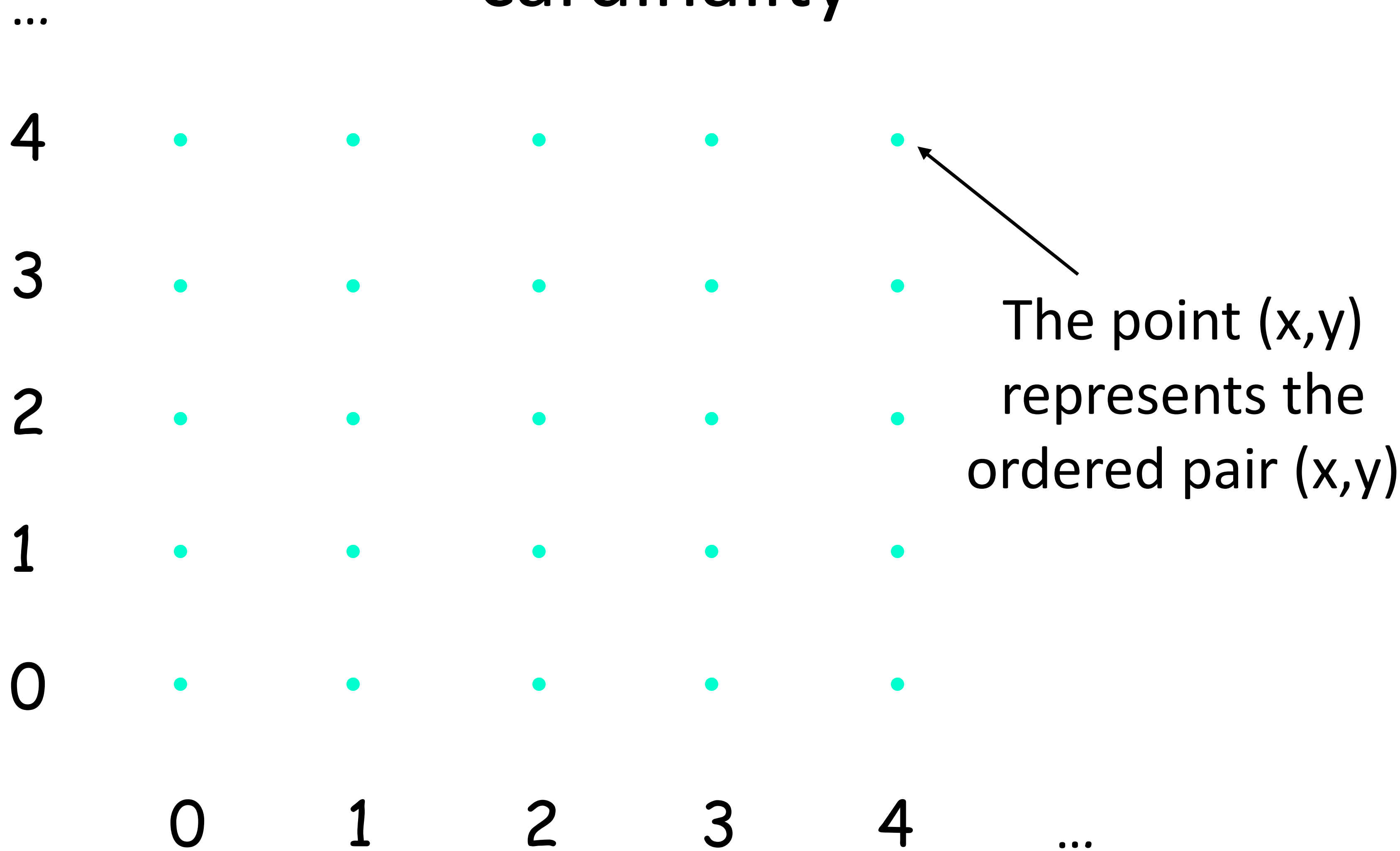
No way!
The rationals are dense: between any two there is a third. You can’t list them one by one without leaving out an infinite number of them.

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

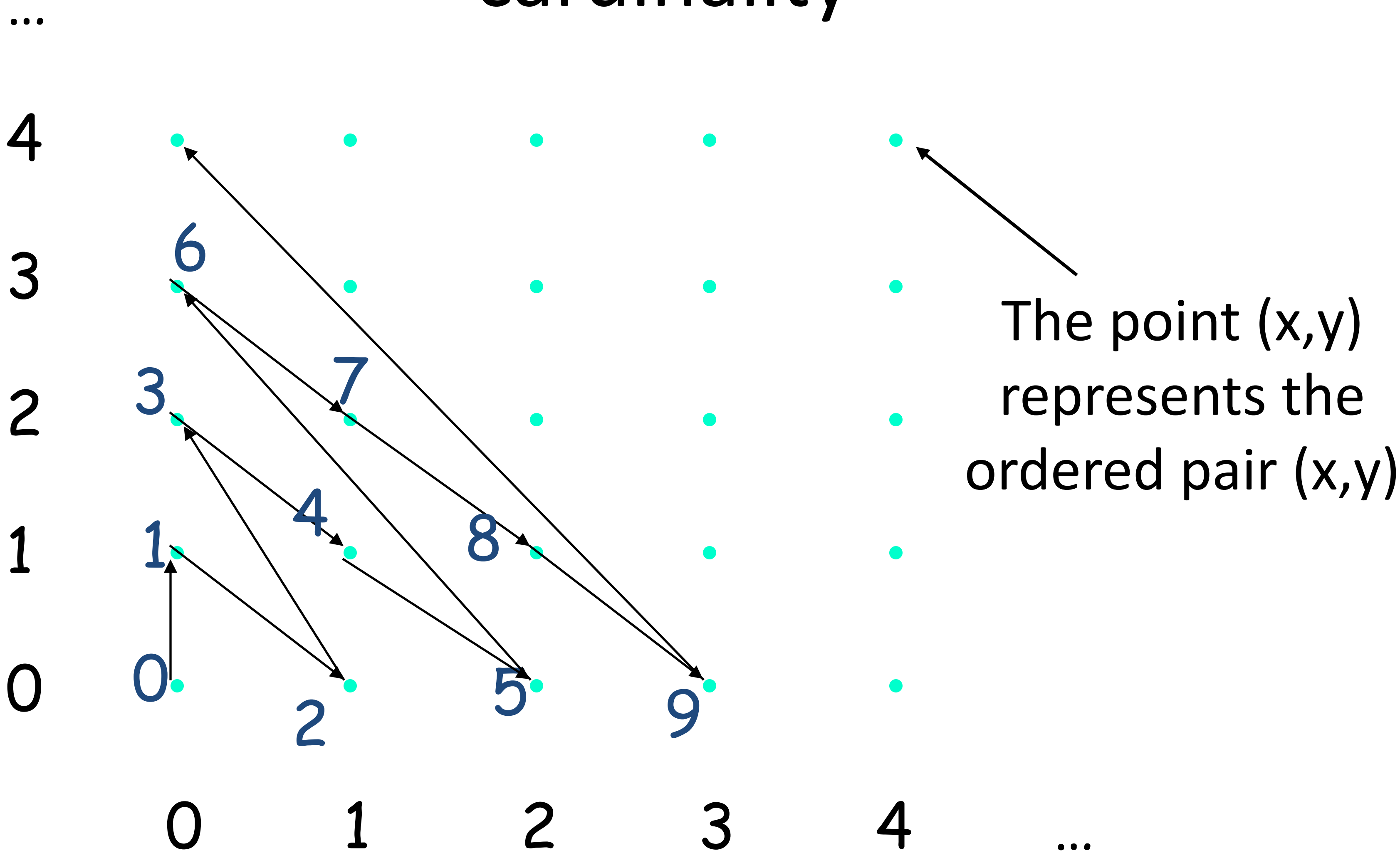
First, let’s warm up with another interesting one:

N can be paired with **NxN**

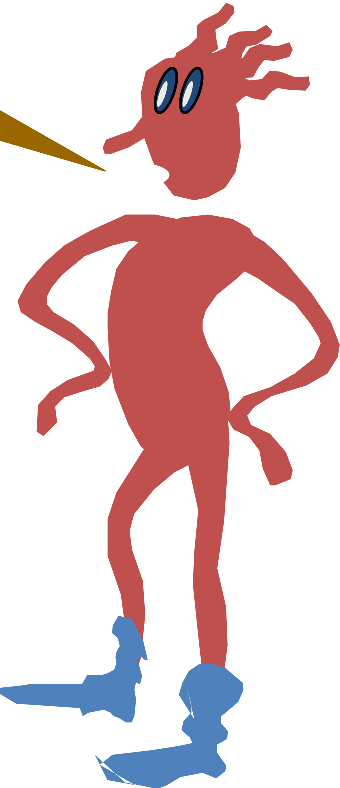
Theorem: **N** and **N** x **N** have the same cardinality

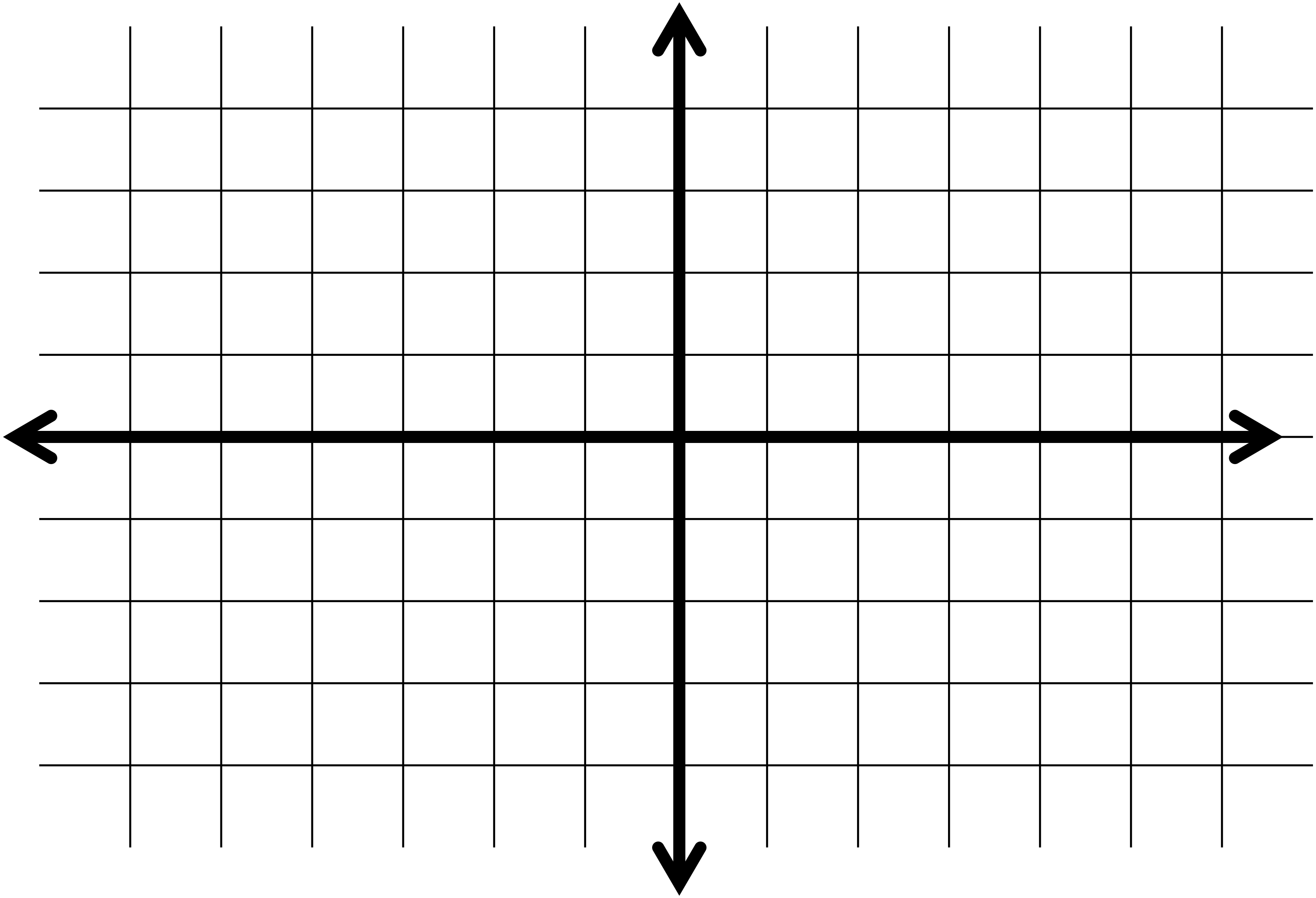


Theorem: **N** and **N** x **N** have the same cardinality

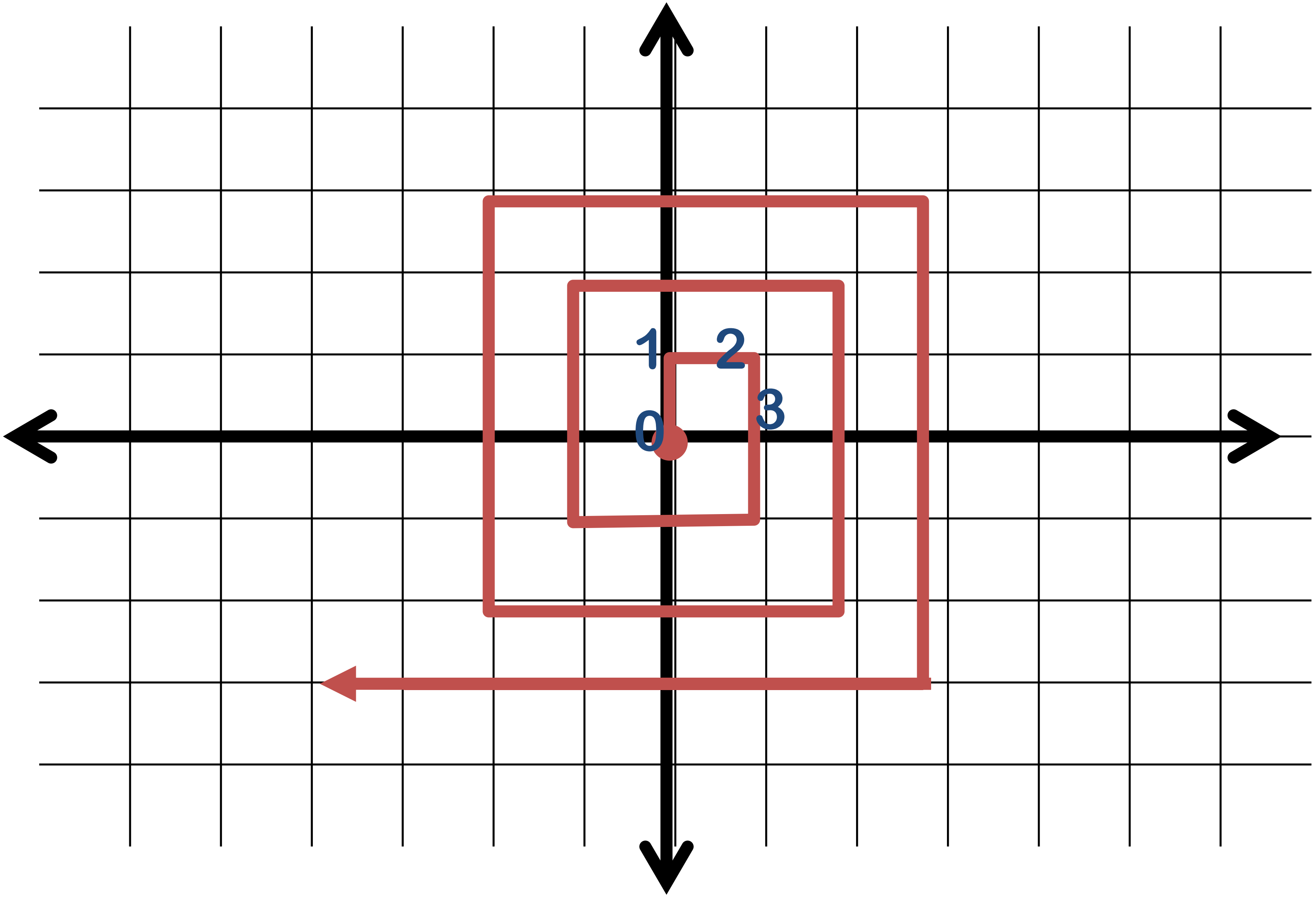


On to the Rationals!





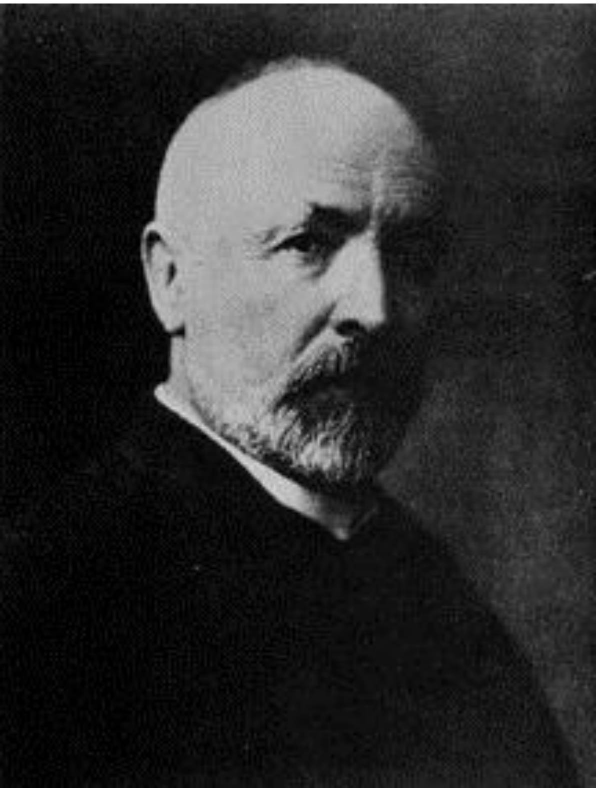
The point at x,y represents x/y



The point at x,y represents x/y

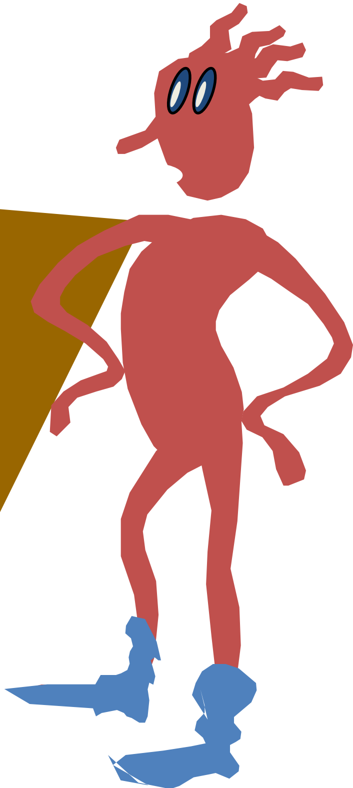
- *1877 letter to Dedekind:*

  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.



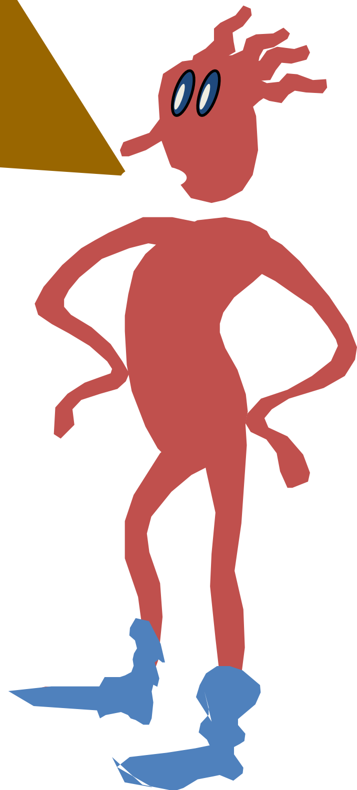
Do **N** and **R** have the same cardinality?

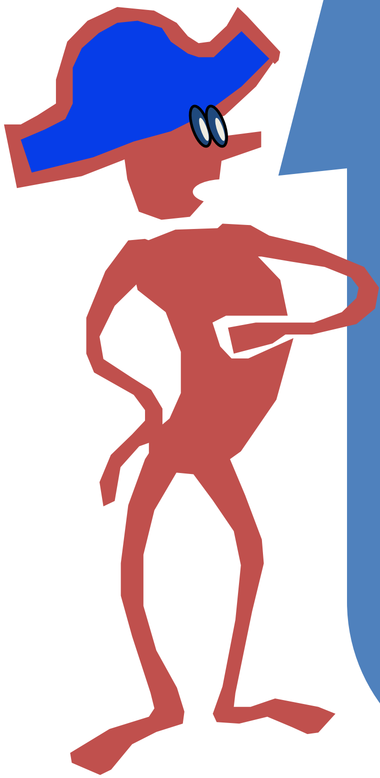
N = { 0, 1, 2, 3, 4, 5, 6, 7, …. }

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: .3333333333333333333333…

1: .31415926565783959385949 82..

…

k: .345322214243555345221123235..

…

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	
...					...

...

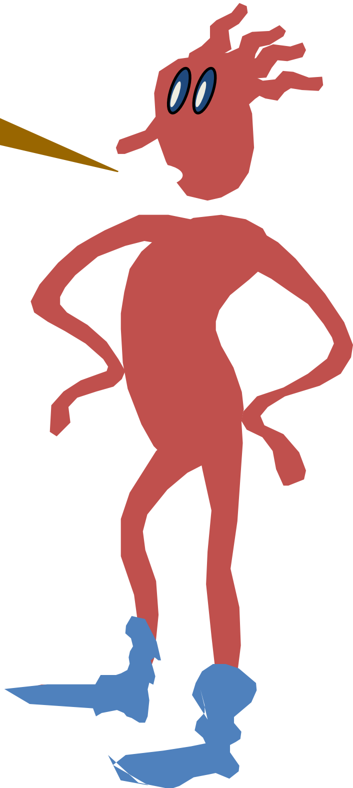
$$C_k = \begin{cases} 1, \text{ if } d_k = 2 \\ 2, \text{ otherwise} \end{cases}$$

Claim:

$Confuse_L$ is not in the list L!

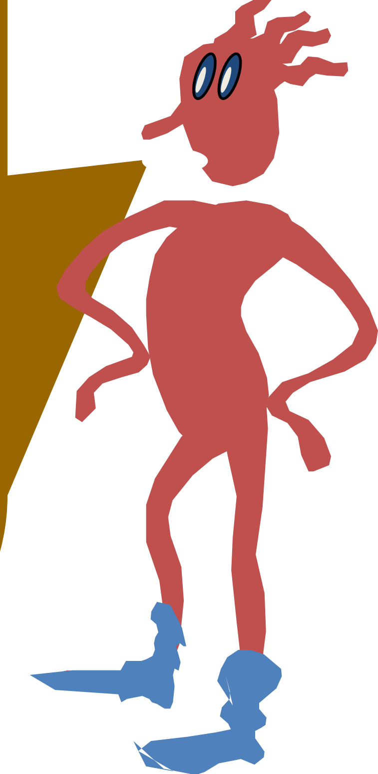
$Confuse_L$ differs from the k^{th} element of L in the k^{th} position. This contradicts our assumption that list L has all reals in I.

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

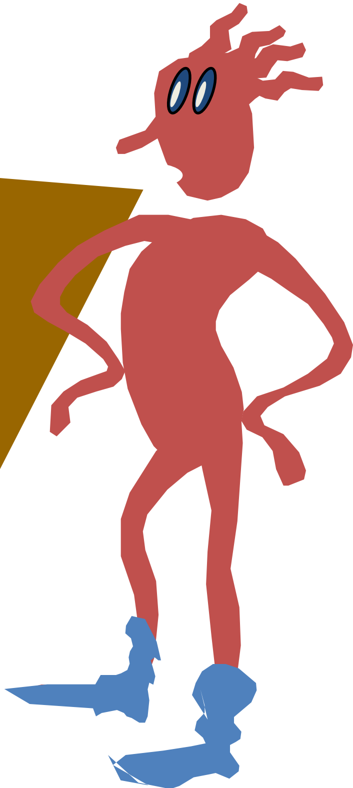
The set of all possible Java programs is a subset of Σ^*

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.

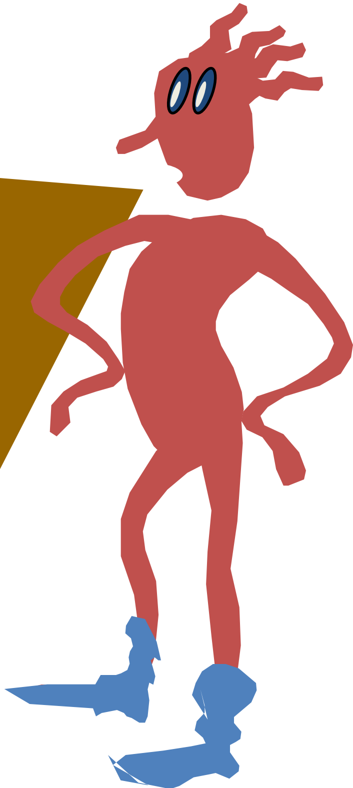
The set of all possible finite length pieces of English text is countable.

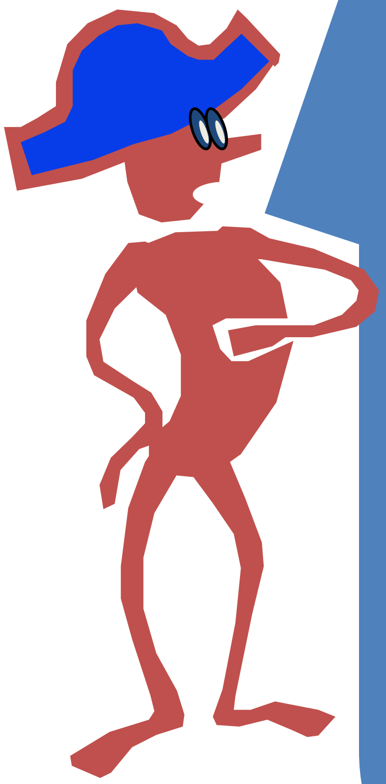


There are countably many Java programs and uncountably many reals.

HENCE:

MOST REALS ARE NOT COMPUTABLE.





There are countably many descriptions and uncountably many reals.

Hence:

MOST REAL NUMBERS ARE NOT DESCRIBABLE IN ENGLISH!

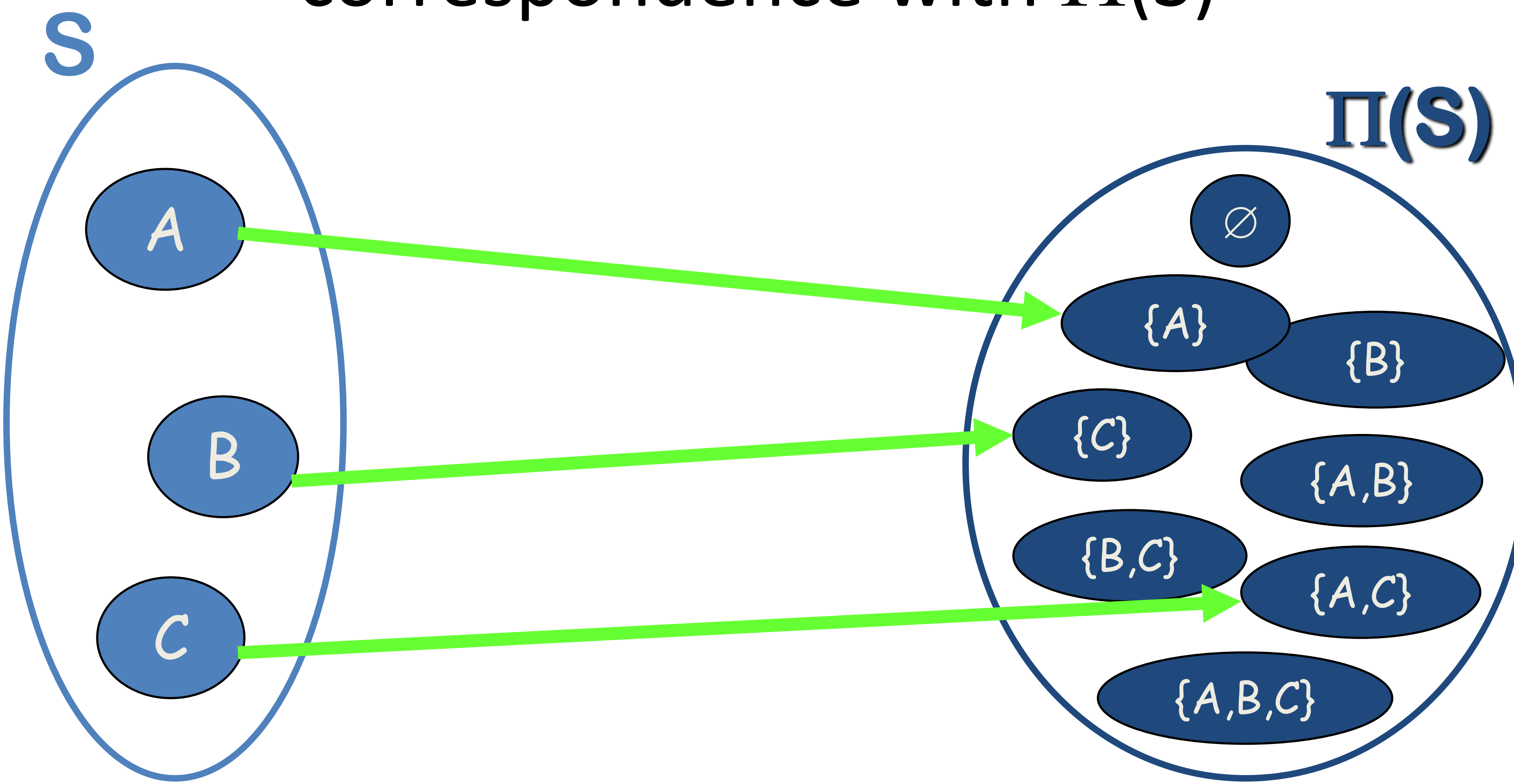
Is there a real number that can be described, but not computed by any program?

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 $\Pi(S)$.
- Proposition: If S is finite, the power set of S has cardinality $2^{|S|}$

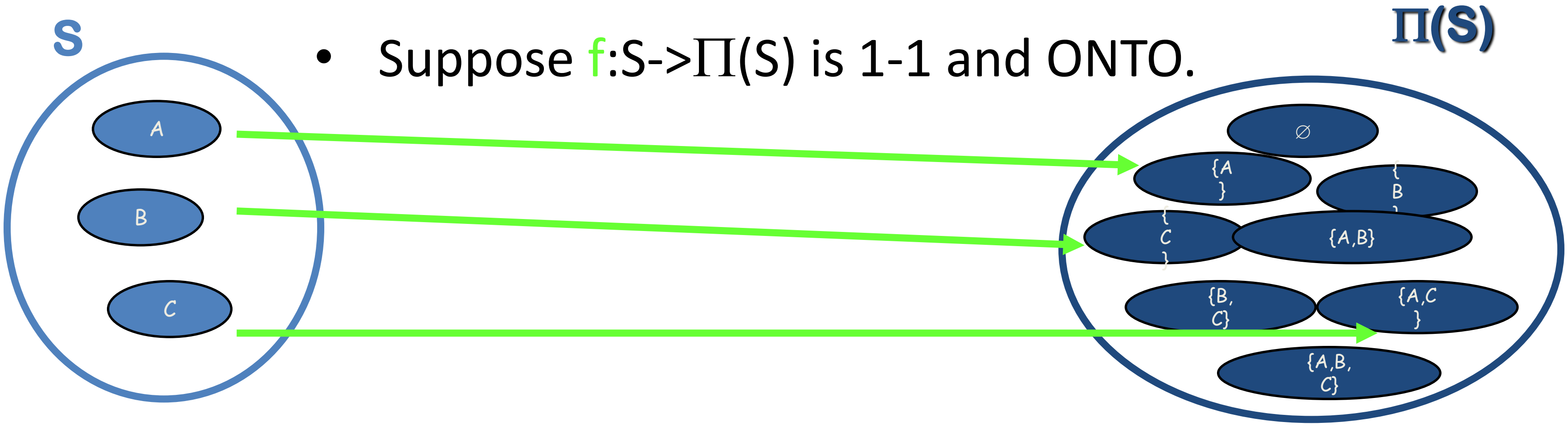
Theorem: S can't be put into 1-1 correspondence with Π(S)



- 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->Π(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?

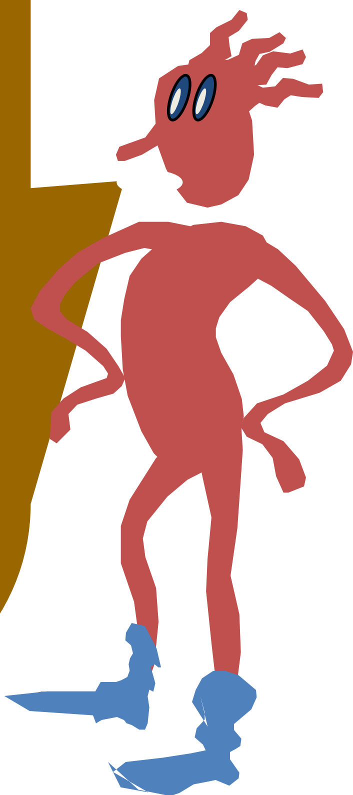
YES: Definition of CONFUSE implies no

NO: Definition of CONFUSE implies yes

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

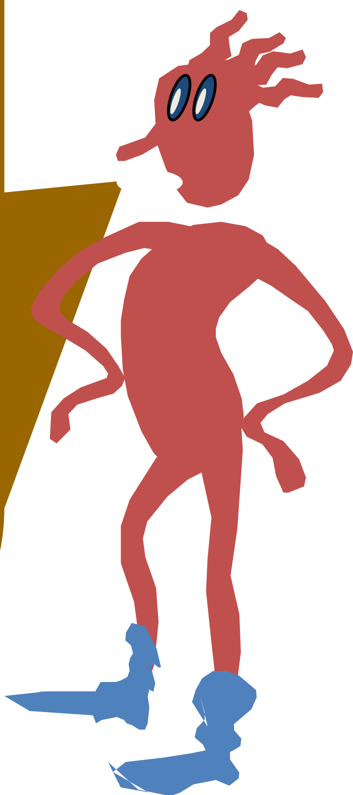
The first infinity is called:

$$\aleph_0$$



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

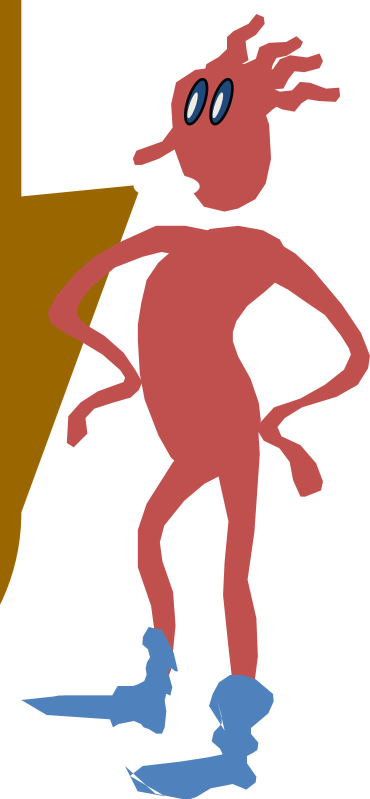
Are there any more infinities?



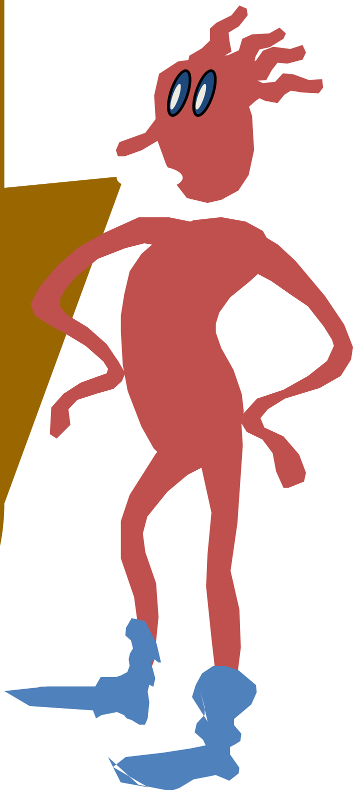
$$\aleph_0, \aleph_1, \aleph_2, \ldots$$

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

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

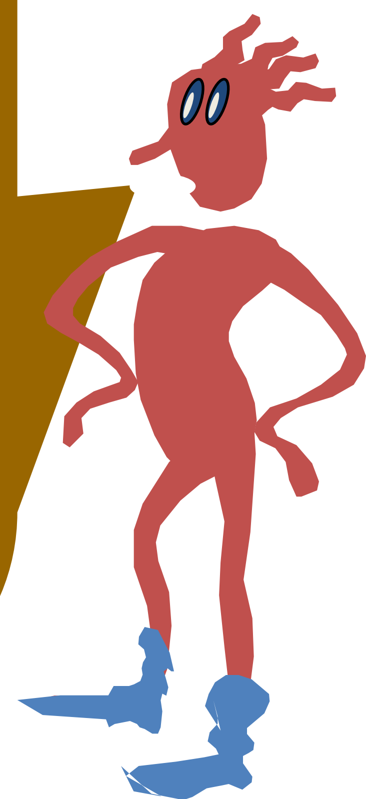


In fact, the same argument can be used to show that no single infinity is big enough to count the number of infinities!

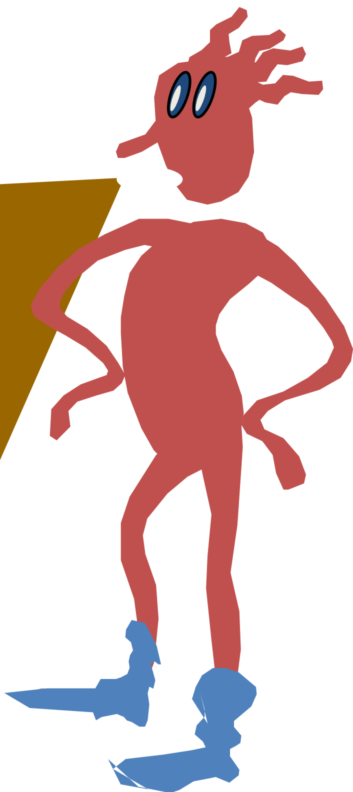


$\aleph_0, \aleph_1, \aleph_2, \ldots$

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!

David Hilbert (1862-1943)

- *Who among us would not be happy to lift the veil behind which is hidden the future; to gaze at the coming developments of our science and at the secrets of its development in the centuries to come? What will be the ends toward which the spirit of future generations of mathematicians will tend? What methods, what new facts will the new century reveal in the vast and rich field of mathematical thought?*

- In mathematics there is no ignorabimus.

The HELLO WORLD assignment

- Suppose your teacher tells you:
- **Write a JAVA program to output the word “HELLO WORLD” on the screen and halt.**

- Space and time are not an issue.
The program is for an ideal computer.

- PASS for any working HELLO program, no partial credit.

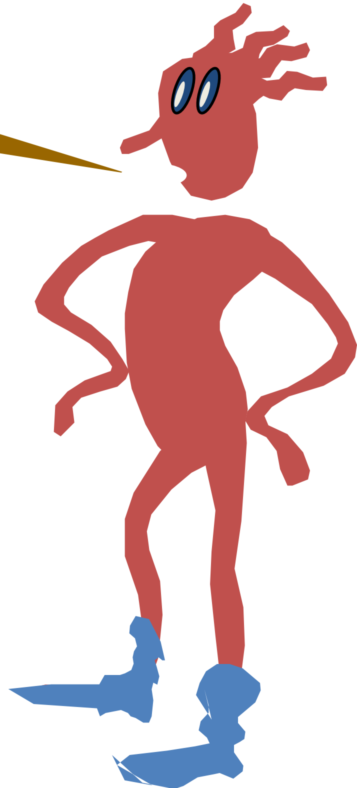
Teacher's Grading Program

- The grading program G must be able to take any Java program P and grade it.

$$G(P) = \begin{cases} \text{Pass, if P prints "HELLO WORLD"} \\ \text{Fail, otherwise.} \end{cases}$$

How exactly might such a script work?

What kind of program could a student who hated his/her teacher hand in?



Nasty Program

- n:=2;
- While (the number 2n can be written as the sum of two primes)
- n++;
- Print "HELLO WORLD";

- The nasty program is a PASS if and only if the Goldbach conjecture is false.

Despite the simplicity of the HELLO WORLD assignment, there is no program to correctly grade it!

This can be proved.

The theory of what can and can't be computed by an ideal computer is called Computability Theory or Recursion Theory.

The Ideal Memory Model

- Σ = finite alphabet of symbols
- Each memory location holds one element of Σ

- “Abstract” Version: One memory location for each natural number 0, 1, 2, …

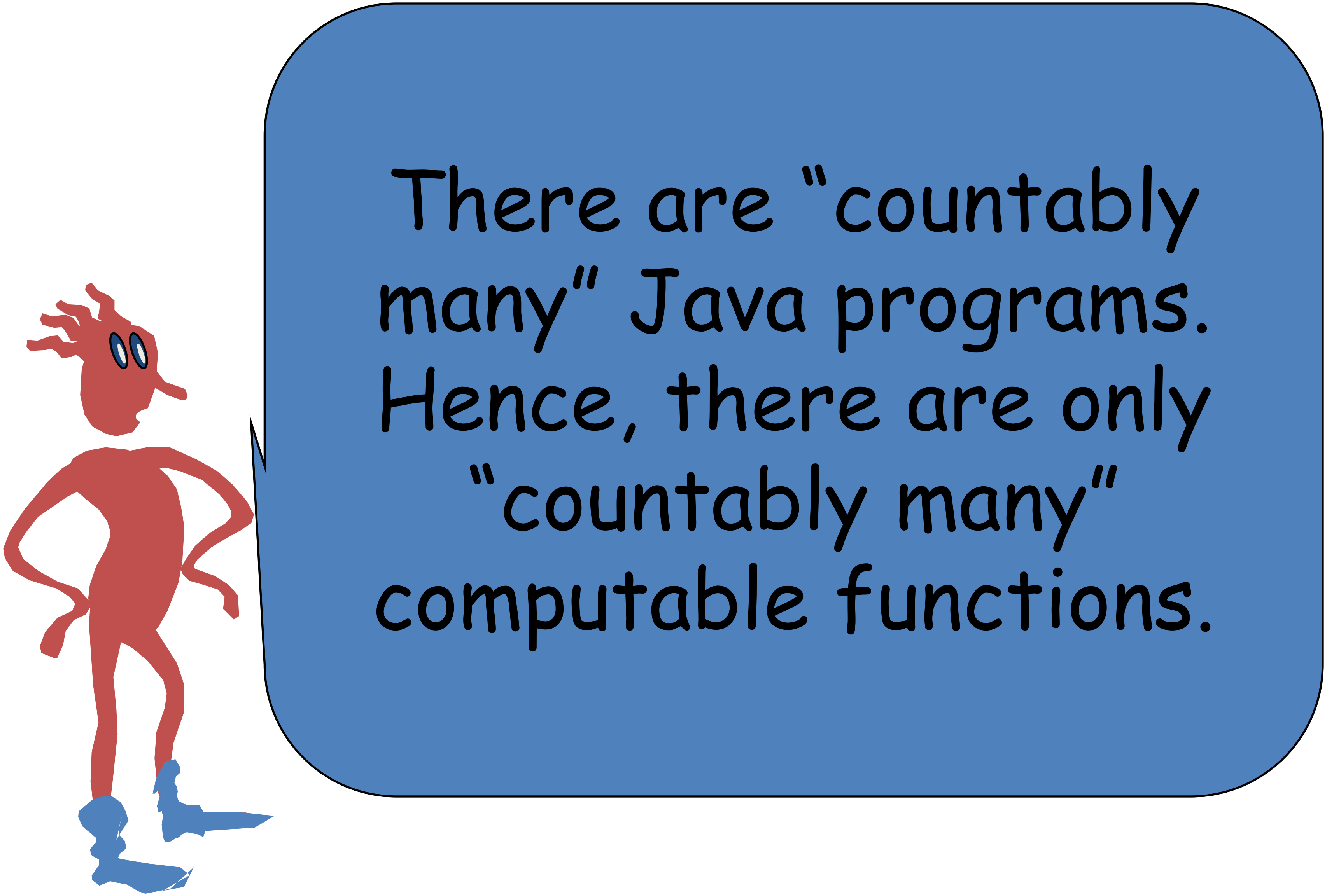
- “Practical” Version: Any time you start to run out of memory, the computer contacts the factory. A maintenance person is flown by helicopter and attaches 100 Terabytes of RAM to the computer.

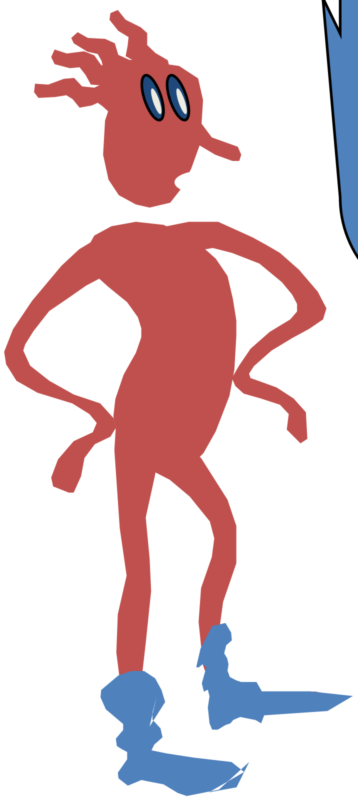
Computable Functions

- Fix any precise programming language, i.e., Java.
- A program is any finite string of symbols from Σ that a Java interpreter will run (won't give a syntax error)

- Recall Σ^* is the set of all strings of symbols.

- A function $f : \Sigma^* \to \Sigma^*$ is <u>computable</u> if there is a program P that computes f, when P is executed on a computer with ideal memory.
- That is, for all strings x in Σ^*, $P(x) = f(x)$.


There are “countably many” Java programs. Hence, there are only “countably many” computable functions.



Are there countably many functions from Σ^* to Σ^* ?

Theorem: There are uncountably many functions!

- There is a bijection between
  - The set of all subsets of Σ^* (the powerset of Σ^*)
  - The set of all functions f: Σ^* -> {0,1}

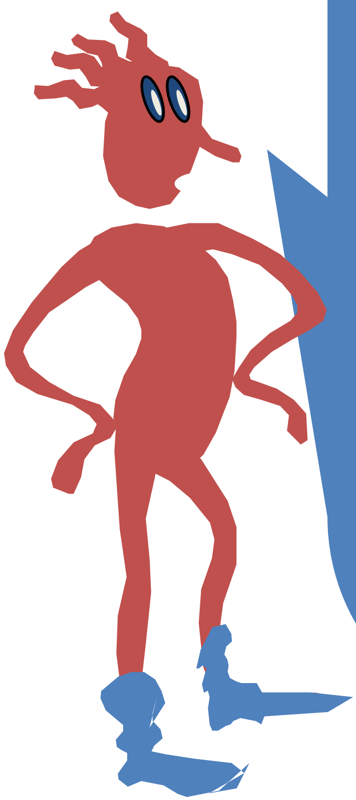
- Take a subset S of Σ^*, we map it to the function f where:
- f(x) = 1 x in S
- f(x) = 0 x not in S

Uncountably many functions.

- There is a bijection between

  - The set of all subsets of Σ^* (the powerset of Σ^*)
  - The set of all functions f: Σ^* - > {0,1}

- So the set of all f: Σ^* -> {0,1} has the same size as the powerset of Σ^*
- But Σ^* is countable, so the powerset of Σ^* is uncountable!
- (No bijection between Σ^* and Power(Σ^*)!)



So there are functions from Σ^* to $\{0,1\}$ that are not computable.

Can we describe an incomputable one?
Can we describe an interesting, incomputable function?

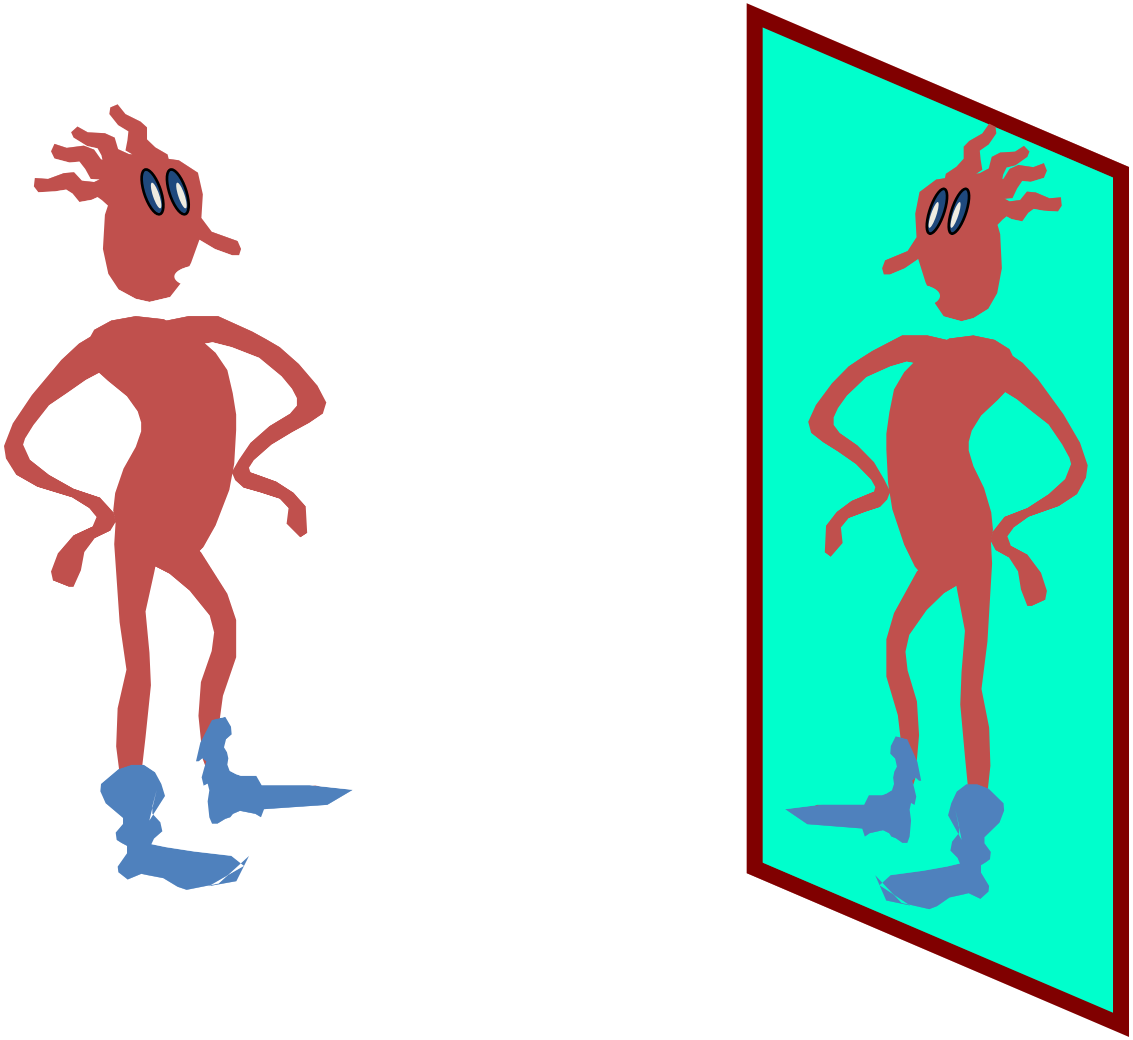
Notation And Conventions

- Fix any programming language
- When we refer to "program P" we mean the text of the source code for P
- P(x) is the final output of program P on input x, assuming that P eventually halts

P(P)

- It follows from our conventions that P(P) is the output obtained when we run P on the text of its own source code.

P(P) … So that’s what I look like



The Famous Halting Set: K

- K is the set of all programs P such that P(P) halts.

- $K = \{ \text{Program } P \mid P(P) \text{ halts}\}$

The Halting Problem

- Is there a program HALT such that:

- HALT(P) = yes, if P(P) halts
- HALT(P) = no, if P(P) does not halt

The Halting Problem
$K = \{P \mid P(P) \text{ halts }\}$

- Is there a program HALT such that:

- HALT(P) = yes, if $P \in K$
- HALT(P) = no, if $P \notin K$

- HALTS decides whether or not any given program is in K.

- Suppose a program HALT, solving the halting problem, existed:

- HALT(P) = yes, if P(P) halts
- HALT(P) = no, if P(P) does not halt

- We will call HALT as a subroutine in a new program called WEIRD.

- THEOREM: There is no program that can solve the halting problem! (Alan Turing 1937)

- The Program WEIRD(P):
- If HALT(P) then go into an infinite loop.
- Else stop.
- <Put text of subroutine HALT here>

- Does WEIRD(WEIRD) halt or not?

- YES implies HALT(WEIRD) = yes
- but then, WEIRD(WEIRD) will infinite loop

CONTRADICTION

- NO implies HALT(WEIRD) = no
- but then, WEIRD(WEIRD) halts

Turing's argument is just like the DIAGONALIZATION argument from the theory of infinities.

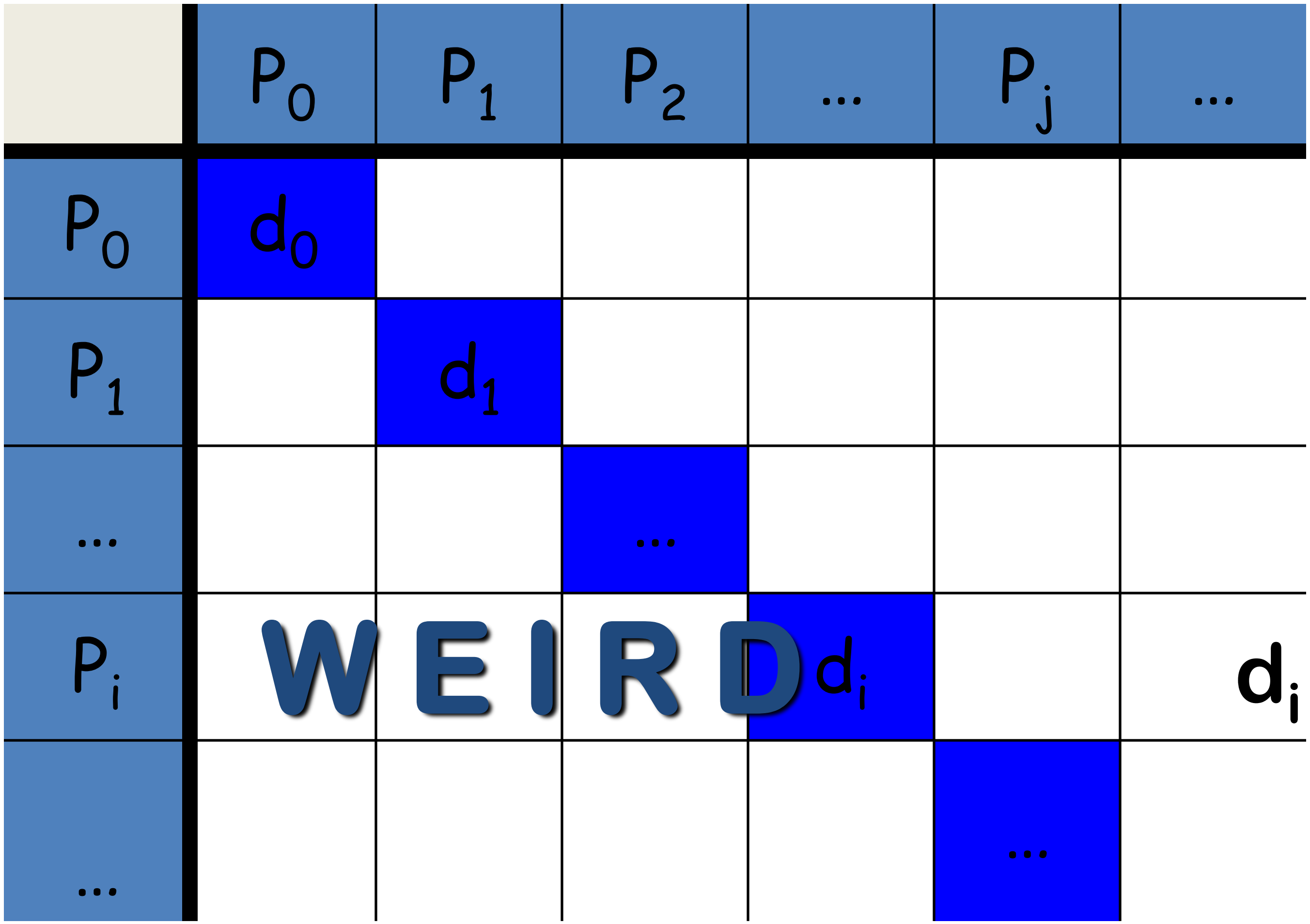
	P_0	P_1	P_2	...	P_j	...
P_0						
P_1						
...						
P_i						
...						

YES, if $P_i(P_j)$ halts
NO, otherwise

	P_0	P_1	P_2	...	P_j	...
P_0	d_0					
P_1		d_1				
...			...			
P_i				d_i		
...					...	

d_i = HALT(P_i)

YES, if $P_i(P_j)$ halts
NO, otherwise

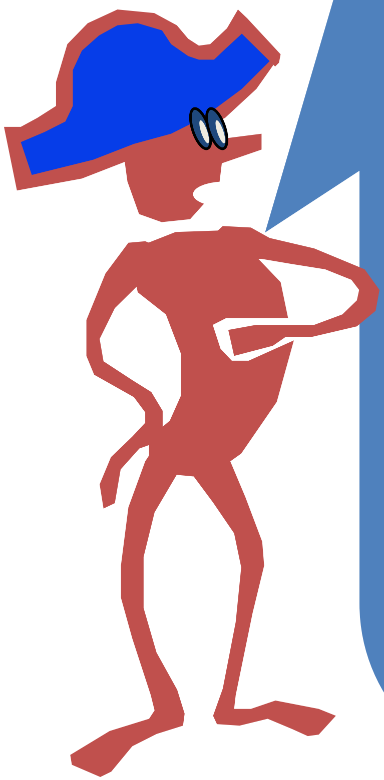


$d_i = \mathrm{HALT}(P_i)$

WEIRD(P_i) halts iff d_i = NO
The WEIRD row contains the opposite of the diagonal…

Alan Turing (1912-1954)

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



Consider the real number between 0 and 1, which has a 1 in the i^{th} decimal place if P_i **is in** K, and 0 otherwise

Computability Theory: Vocabulary Lesson

- We call a set $S \subseteq \Sigma^*$ decidable

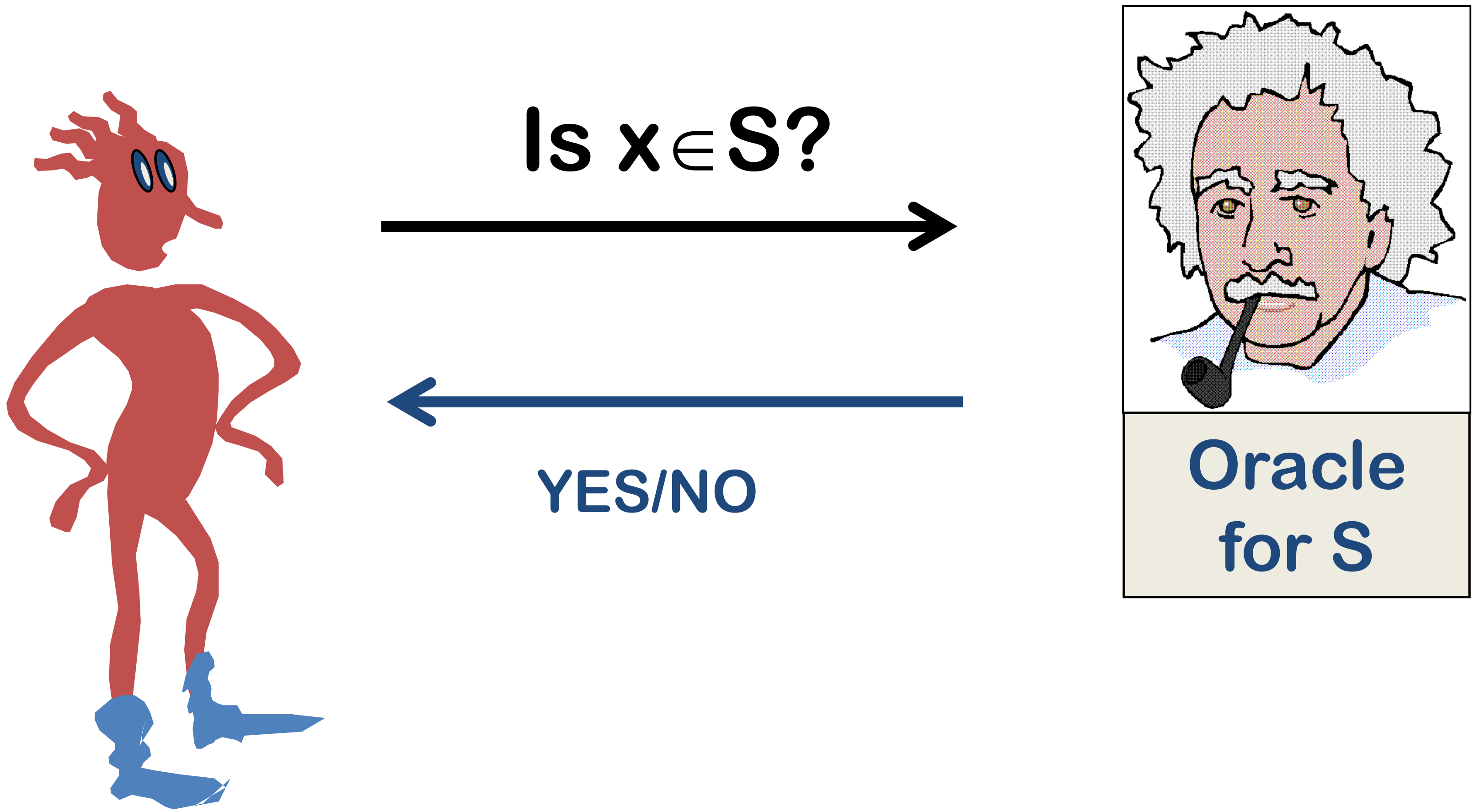
if there is a program P such that:

- P(x) = yes, if $x \in S$
- P(x) = no, if $x \notin S$

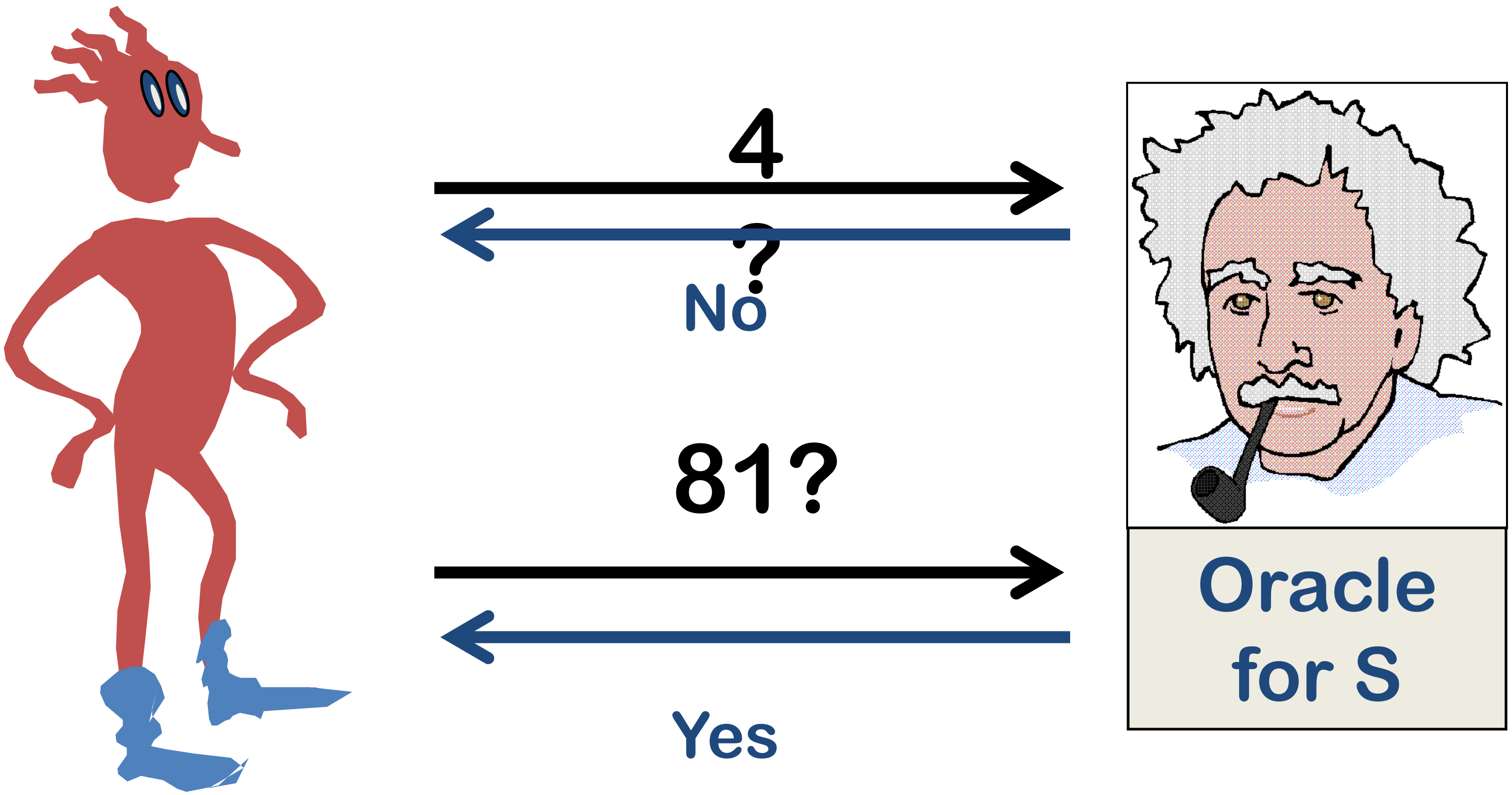
- We already know: K is **undecidable**

Now that we have established that the Halting Set K is undecidable, we can use it as a starting point for more “natural” undecidability results.

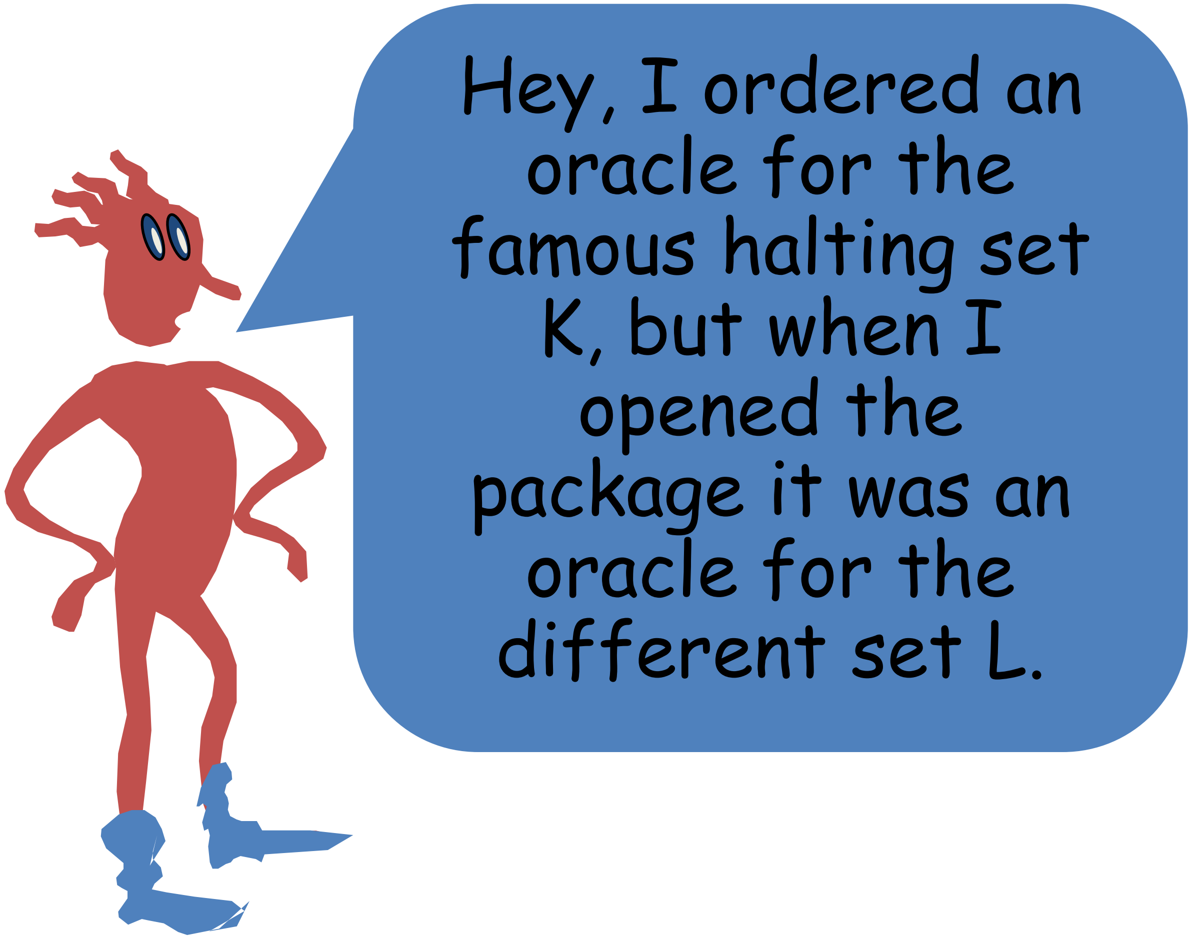
Oracle For Set S



Example Oracle
S = Odd Naturals



L = the set of programs that take no input and halt

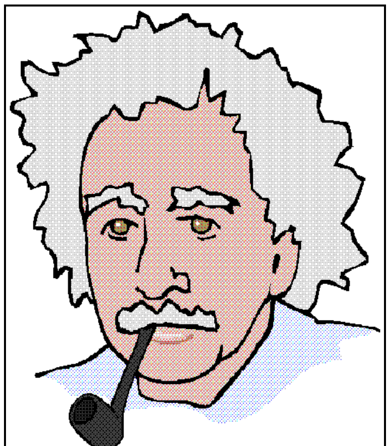


GIVEN: Oracle for L

L = the set of programs that take no input and halt

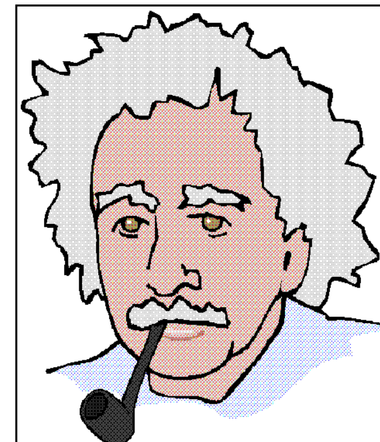
P ; Q $\equiv$ simulates P using P as input

Does P(P) halt?



BUILD:
Oracle for K

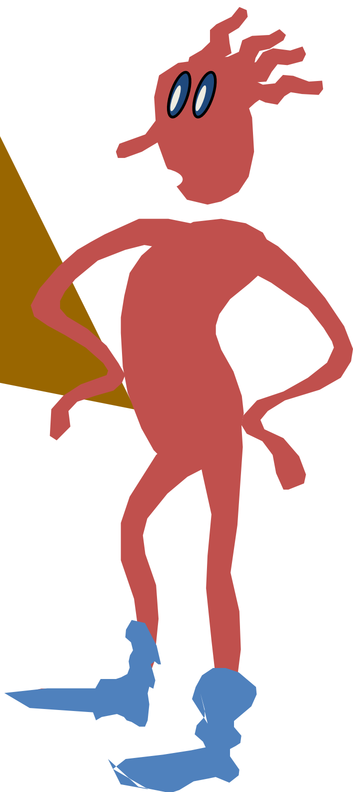
Does the program Q halt?



GIVEN:
Oracle for L

Thus, if L were decidable then K would be as well. (If there were a program for L, there'd be one for K, too!)

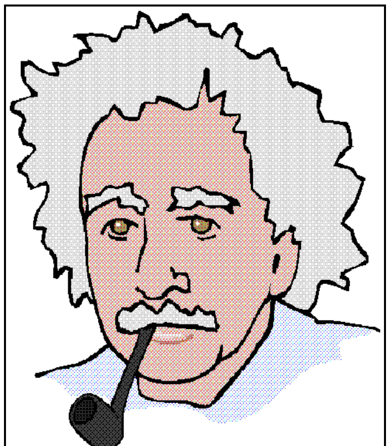
We already know K is not decidable. Therefore L is also not decidable!



HELLO = the set of programs that print HELLO and hal

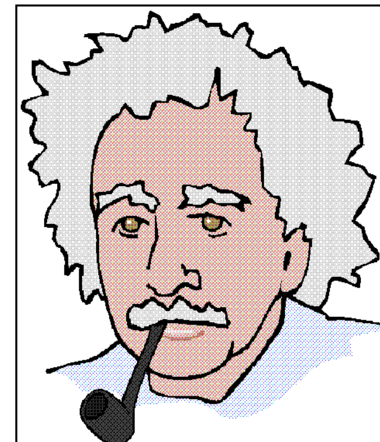
Does P halt?

Let P’ be P with all print statements removed.



BUILD:
Oracle for L

Does [P’; Print HELLO] ever print HELLO?

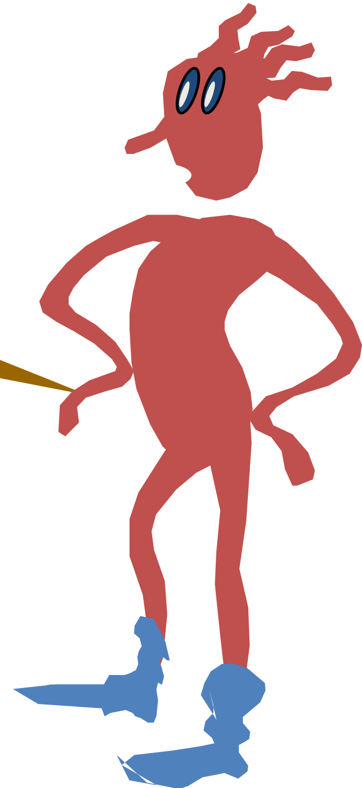


GIVEN:
HELLO Oracle

If there were a program for HELLO, then there'd be a program for L.

But L is not decidable.

So HELLO is not decidable.



EQUAL = All <P,Q> such that P and Q have identical outputs on all inputs

Does P equal HELLO ?

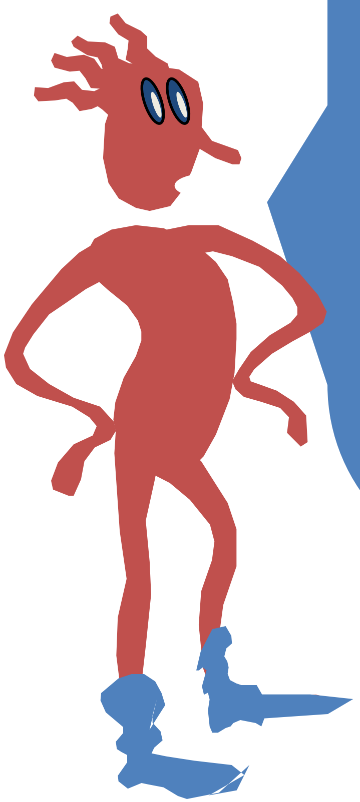
Let H = [Print HELLO]

Are P and H equal?

BUILD:
HELLO
Oracle

GIVEN:
EQUAL
Oracle

Halting with input, Halting without input, The “Hello World” assignment, and EQUAL are not decidable.



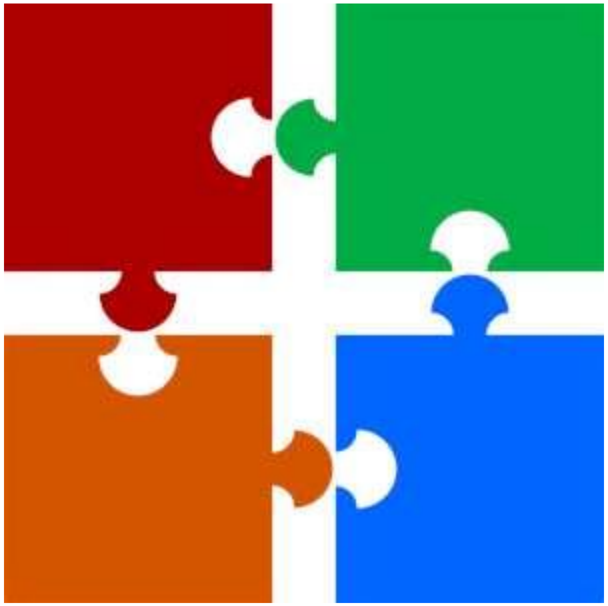
What about problems that have no obvious relation to halting, or even to computation can encode the Halting Problem is non-obvious ways?

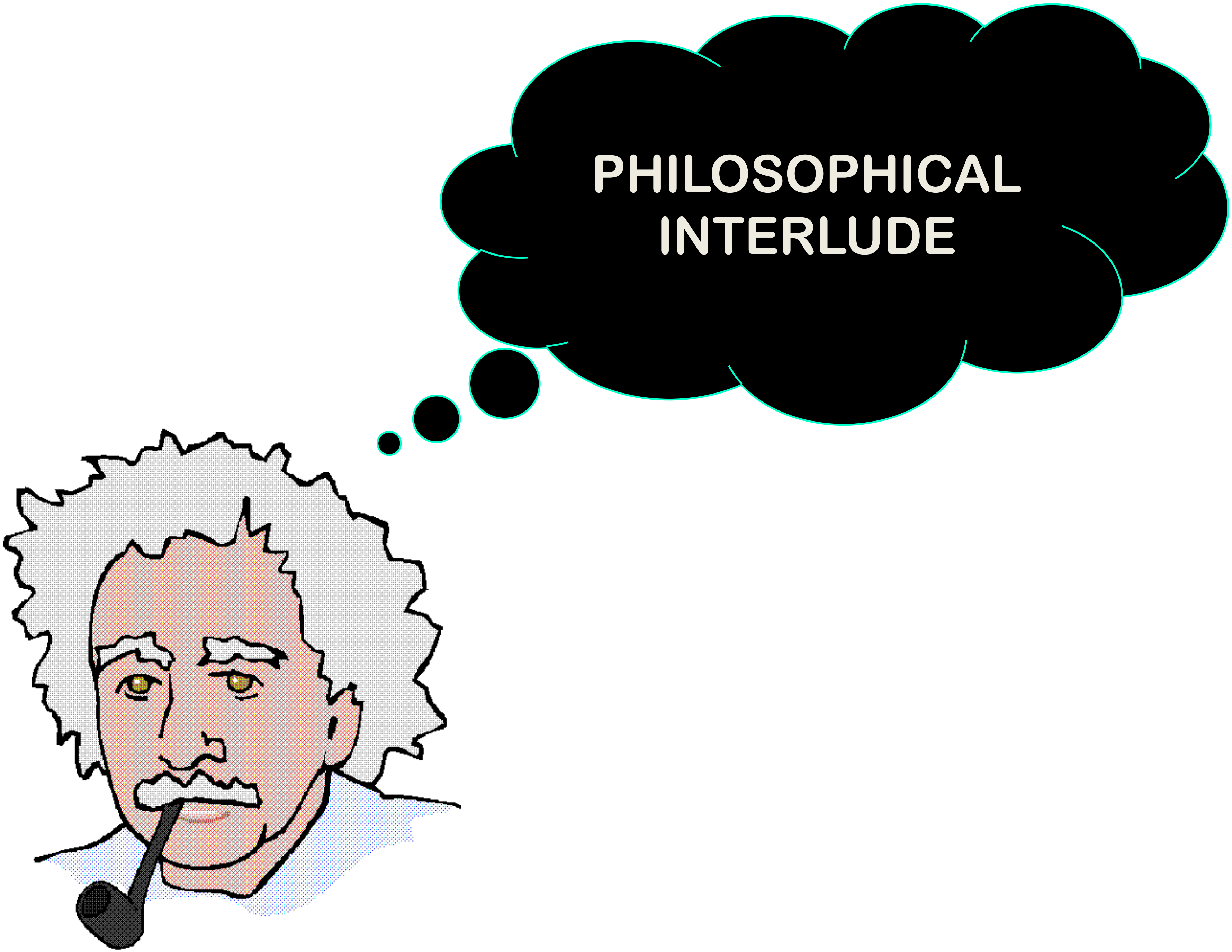
Diophantine equations

- $a^k + b^k = c^k$
- $xy^2 - xz = p$
- Hilberts 10^{th} problem was to find a solution to such equations.

Puzzle Pieces

- Given a finite set of puzzle pieces, can you tile the plane (you are allowed to use each piece arbitrarily often)?




PHILOSOPHICAL
INTERLUDE

CHURCH-TURING THESIS

- Any well-defined procedure that can be grasped and performed by the human mind and pencil/paper, can be computed on a conventional digital computer with no bound on its memory.

The Church-Turing Thesis is NOT a theorem. It is a statement of belief about the universe we live in.

- Your opinion will be influenced by your religious, scientific, and philosophical beliefs.

Empirical Intuition

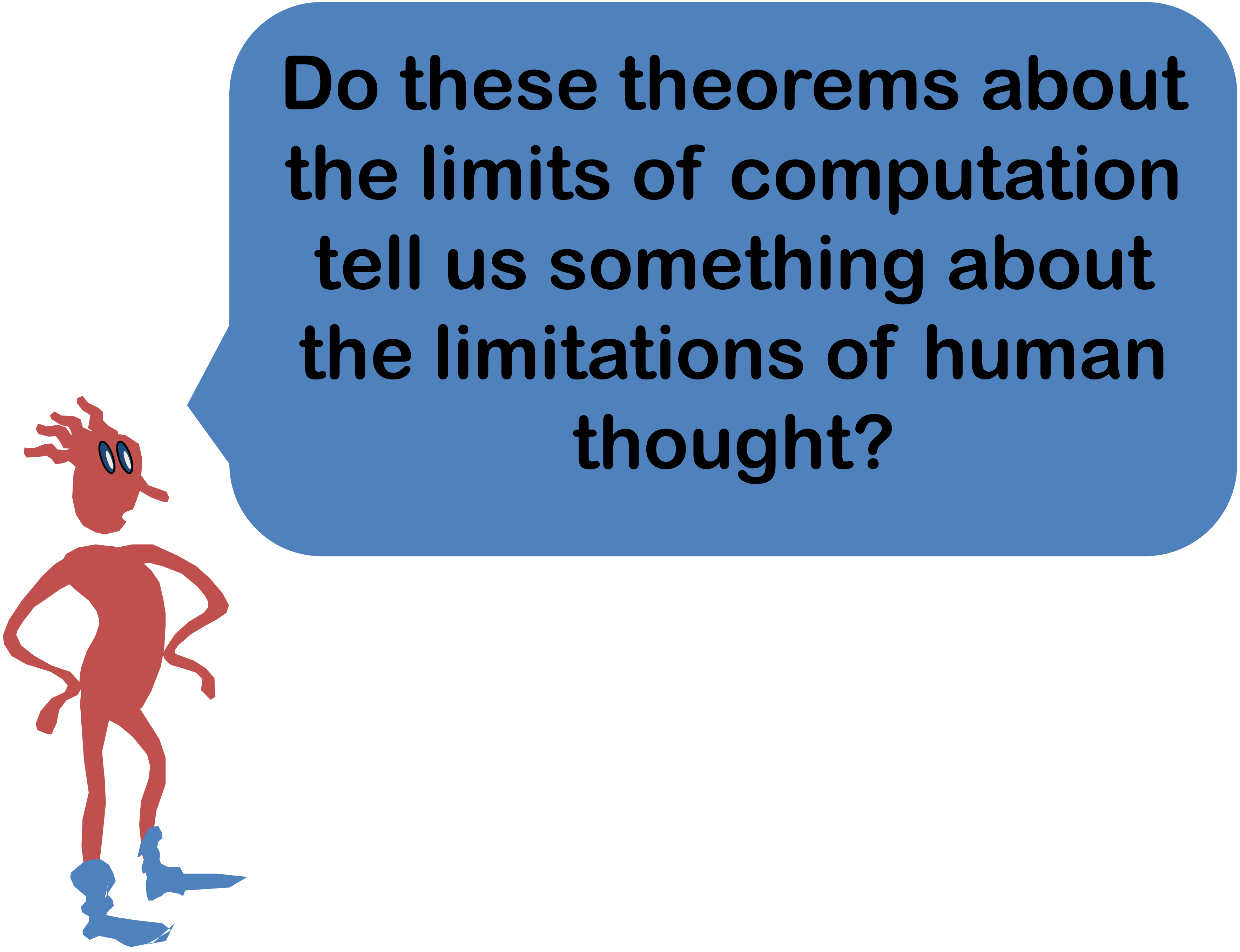
- No one has ever given a counter-example to the Church-Turing thesis. That is, no one has given a concrete example of something that humans can compute in a consistent and well defined way, that also can't be programmed on a computer.
- The thesis is true.

Mechanical Intuition

- The brain is a machine. The components of the machine obey physical laws.
- In principle, an entire brain can be simulated step by step on a digital computer. Thus, any thoughts of such a brain can be computed by a simulating computer. The thesis is true.

Spiritual Intuition

- The mind consists of part matter and also part soul. Soul, by its very nature, cannot be reduced to physical laws. Thus, the action and thoughts of the brain cannot be simulated or reduced to simple components and rules. The thesis is false.


Do these theorems about the limits of computation tell us something about the limitations of human thought?