Infinite sets

Adam Wyner

CS3518, Spring 2017

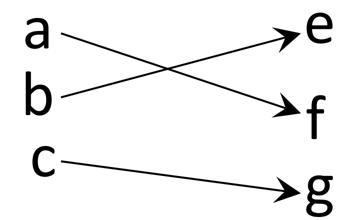
University of Aberdeen

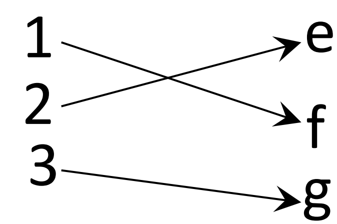
Cardinality (informal)

- The cardinality of a finite set is its number of elements
- E.g., card({a,b,c}) = card({e,f,g}) = 3
- Note: for finite sets X and Y, card(X) = card(Y) if and only if there exists a bijection between X and Y.
- There are different, but related notions here:
  - what is the 'size' of a set?
  - is there a bijection between the sets?
  - if there is a bijection, what are the elements (in the sets) that are being related?
  - what is the bijective function?

Cardinality (informal)

- For these sets {a,b,c} and {e,f,g}, we could make a function:
- This is a bijection (one-to-one and onto).
- The elements being related are letters.
- It isn't clear what the bijective function is other than what is given.
- We could also have the domain as natural numbers, which is similarly a bijection; in which case, we have a way to determine the cardinality.
- We can call this an enumeration.





Enumeration

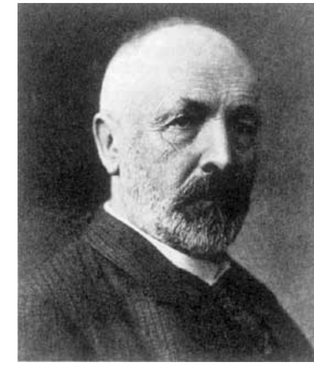
- What can and what cannot be enumerated?
- This is related to a basic idea running through the course – where we have more problems than solutions.
- In turn, can we make a bijective function (a program) from solutions to the problems they solve.
- Hard to answer in a general way. At least we can enumerate the problems, leaving the actual function as a number. Thus, we will try to understand what problems we can and cannot solve “in principle” with a program.
- Enumerated sets are computable; if some set is not enumerable, it is not computable.

Infinity

- We can determine the cardinality of a set if the set has 0 or 1 or 2 or … n (i.e. any natural number) elements.
- But what if the set has an infinite number of elements? Some examples:
  - The set of all natural numbers
  - The set of all even natural numbers
  - L(1*) = 1, 11,111,1111,11111, etc.
  - L(0*1*) = 01,001,011,0001,0011, etc

  - * is the Kleene Star, meaning zero or more

The diagonalisation method



- Georg Cantor (1873): What's the size of an infinite set?
- e.g., is card(L(1^*)) = card(L(0^*1^*))?
  - Both are infinite
  - But is one larger than the other?
- Cantor's idea:
  - The size (cardinality) of a set should not depend on the *identity* of its elements
  - Two finite sets *A* and *B* have the same size if we can pair the elements of *A* with elements of *B, that is, the elements correspond.*
  - Formally: there exists a **bijection** between A and B

Correspondences

n	$f(n)$
1	2
2	4
3	6
$\vdots$	$\vdots$

- Example: Let
  - $\mathcal{N}$ be the set of pos. natural numbers {1, 2, 3, …}
  - $\mathcal{E}$ the set of even pos. natural numbers {2, 4, 6, …}
- Using Cantor's definition of size, we can show that $\mathcal{N}$ and $\mathcal{E}$ have the same size:
  - Bijection (!): $f(n) = 2n$
- Intuitively, $\mathcal{E}$ is smaller than $\mathcal{N}$, but
  - Pairing each element of $\mathcal{N}$ with its corresponding element in $\mathcal{E}$ is possible,
  - So we declare these two sets to be the same size
  - This even though $\mathcal{E} \subset \mathcal{N}$ ($\mathcal{E}$ is a real subset of $\mathcal{N}$)
- Strange but true!

Countable (enumerable) sets

- A set X is finite if it has n elements, for some n in $\mathcal{N}$.
- A set is countable if either
  - It is finite or
  - It has the same size as $\mathcal{N}$, the natural numbers
- For example,
  - $\mathcal{N}$ (natural numbers) is countable, and so are all its subsets
  - $\mathcal{E}$ (even numbers) is countable
  - {0,1,2,3} is countable
  - $\emptyset$ is countable (it is a finite set!)
- How about supersets of $\mathcal{N}$?

An even stranger example…

- Let $\mathcal{Q}$ be the set of positive rational numbers

$$\mathcal{Q} = \{ m/n \mid m, n \in \mathcal{N} \}$$

- Just like $\mathcal{E}$, the set $\mathcal{Q}$ has the same size as $\mathcal{N}$!
  - We show this giving a bijection from $\mathcal{Q}$ to $\mathcal{N}$
  - $\mathcal{Q}$ is thus countable
- One way is to enumerate (i.e., to list) Q's elements.
  - Pair the first element of Q with 1 (first element of $\mathcal{N}$)
  - And so on, making sure every member of $\mathcal{Q}$ appears only once in the list

An even stranger example… (Cont’d)

- To build a list with the elements of Q
  - make infinite matrix with all positive rational numbers
  - *i*-th row contains all numbers with numerator *i*
  - *j*-th column has all numbers with denominator *j*
  - *i*/*j* is in *i*-th row and *j*-th column

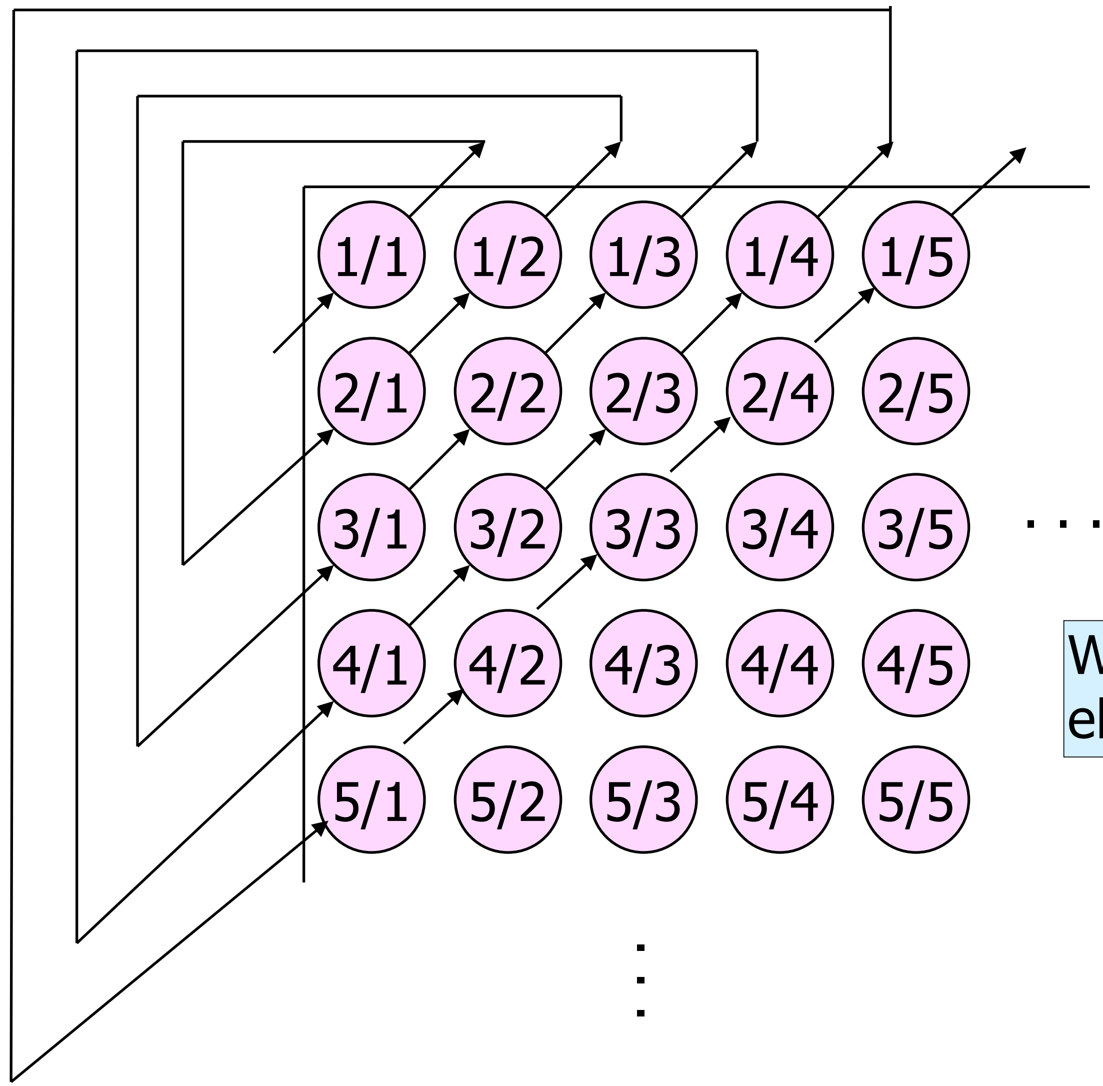
$$\begin{array}{cccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \\ 5/1 & 5/2 & 5/3 & 5/4 & 5/5 & \\ & & \vdots & & & \end{array}$$

An even stranger example… (Cont'd)

- Now we turn the previous matrix into a list
- A bad way: begin list with first row
  - Since rows are infinite, we will never get to 2^{nd} row!

An even stranger example… (Cont'd)

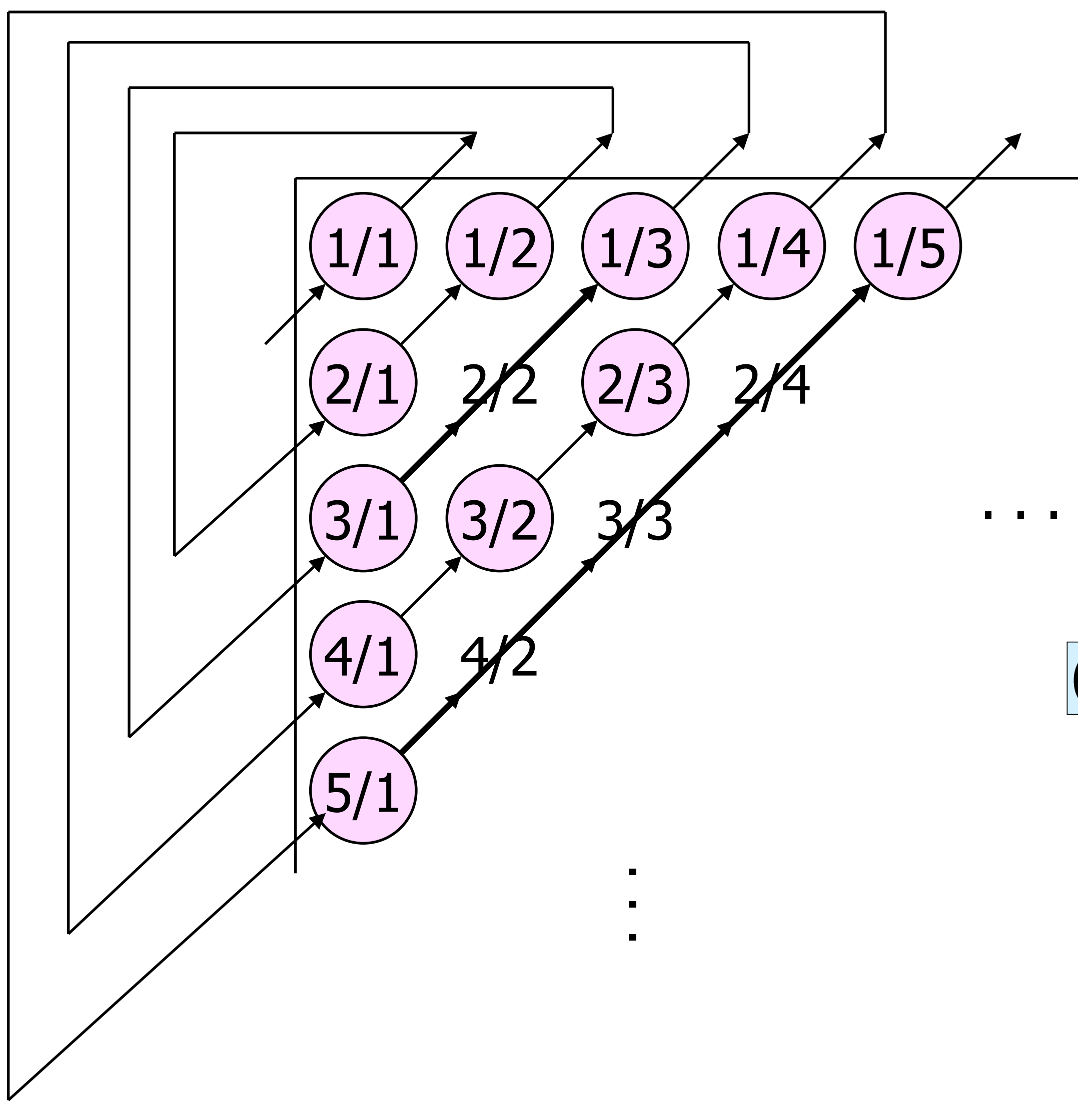
- Instead, we list the elements along diagonals:



We should, however, eliminate repeated elements

An even stranger example… (Cont'd)

- We list elements along diagonals without repetitions:



We make an enumerable list:

(1/1, 2/1, 1/2, 3/1, 1/3, …)

Why does diagonalisation work?

- While each of the ‘axes’ are infinite, the diagonal is finite – ‘bouncing off the bumpers’.
- Enumeration by example.
- It is a bijective function from $\mathcal{Q}$ to $\mathcal{N}$

1/1	1/2	1/3	1/4	1/5	
2/1	2/2	2/3	2/4	2/5	
3/1	3/2	3/3	3/4	3/5	. . .
4/1	4/2	4/3	4/4	4/5	
5/1	5/2	5/3	5/4	5/5	
		⋮			

What is the bijective function between Q and N?

- Can we provide not just the enumerated list, but more `content' to the function f: Q $\rightarrow$ N such that f(q) = n is a bijective function, e.g. f(x) = 2n.
- Can we prove it is bijective?
- This is, apparently, more complex....

Uncountable sets

- Some sets have no correspondence with $\mathcal{N}$
- These sets are simply too big!
  - They are not countable: we say <u>uncountable</u>
- Theorem:
  - The set of real numbers between 0 and 1 (e.g., 0.244, 0.3141592323....) is uncountable
    Call this set $R_{0,1}$
- Strange but true!
- Some sets are even larger. “Serious” set theory is all about theorems that concern infinite sets, most of which is irrelevant for this course.

Proof about uncountability of reals

- Theorem: | $R_{0,1}$ | > |N|. Proof strategy:
- | $R_{0,1}$ |>=|N|. Suppose | $R_{0,1}$ |=|N| and derive a contradiction.
- Each member of $R_{0,1}$ can be written as a zero followed by a dot and a countable sequence of digits.
- Suppose there existed a complete enumeration of R, (using *whatever* order) <e1,e2,e3,...>.

Proof about uncountability of reals

An arbitrary list might start this way:

e1. 0.0000000000000000000000....

e2. 0.0100000000000000000000....

e3. 0.8200000000000000000000....

e4. 0.1710000000000000000000....

...

Now construct a real number *n* that's <u>not</u> in the enumeration:

n's first digit (after the dot) =
[e1's first digit] + 1

n's second digit = [e2's second digit] + 1 ...

<u>General</u>: *n*'s i-th digit = [e-i's i-th digit] + 1

∀i: *n* differs from e-i in its i-th digit

Contradiction: <e1,e2,e3,...> is not a (complete) enumeration after all because we can always create a real number not in the previous enumeration. QED

Point

- This proof of the non-countability of the set of real numbers is known as Cantor's *diagonalisation* argument
- We have something that cannot be enumerated
- It proved to be the start of a large new area of set theory, involving the cardinalities of infinite sets

The Russell Paradox

Rosen 5th ed., §1.6
especially ex. 30 on p. 86

Basic Set Notations

- Set enumeration {a, b, c} and set-builder $\{x \mid P(x)\}$.
- $\in$ relation, and the empty set $\varnothing$.
- Set relations =, $\subseteq$, $\subseteq$, $\subset$, $\supset$, $\not\subset$, etc.
- Venn diagrams.
- Cardinality $|S|$ and infinite sets **N**, **Z**, **R**.
- Power sets P(S).

Axiomatic set theory

- Various axioms, e.g., saying that the union of a set of sets is a set; the intersection of a set of sets is a set; etc.
- **One key axiom "The Comprehension Principle":**

  Given a Predicate P, one can construct a set. It consists of all those elements x such that P(x) is true (recall the characteristic function). Alternatively, given any property P there exists a set containing all objects that have that property.

Axiomatic set theory

- But, the resulting theory turns out to be *logically inconsistent*! (more detail soon)
  - This means, there exists a set theoretic proposition p such that both p and $\neg p$ follow logically from the axioms of the theory!
  - $\therefore$ The conjunction of the axioms leads to a contradiction.
  - This makes the theory fundamentally uninteresting, because *any* possible statement in it can be (very trivially) proven!

Prove:

Theorem: Given a contradiction, any statement can be proven

Proof: Let your contradiction be $p \,\&\neg p$ (assuming you have proven it before)

Suppose you want to prove an arbitrary q

($p \,\&\neg p$) --> q is a tautology of propositional logic
(Check truth table of the formula, given $p \,\&\neg p$ is false)
Since you have proven $p \,\&\neg p$, q follows with Modus Ponens.

This version of set theory is inconsistent

Russell's paradox:

- Background: can have "The set A of all sets is a set, so A is a member of itself." Not generally true since "The set B of all teapots is not a teapot, so B is not a member of itself."
- But, this leads to a problem. Consider the set that corresponds with the predicate S, where elements in S are not elements of themselves; alternatively, the set of all sets which don't contain themselves i.e. $x \notin x$, *where x is a set:*

  $S = \{x \mid x \notin x\}$
- Now ask: is $S \in S$?

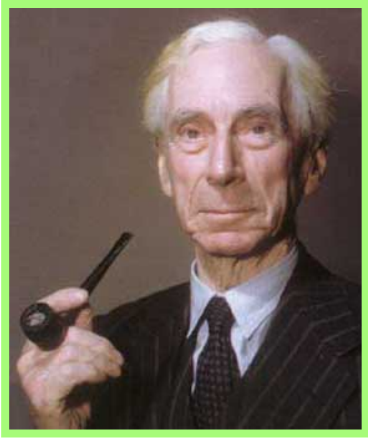
Russell's paradox

- *L*et $S = \{x \mid x \notin x\}$. Is $S \in S$?
- If $S \in S$, then S is one of those x for which $x \notin x$. In other words, $S \notin S$. The assumption and the conclusion are a contradiction.
- If $S \notin S$, then S is not one of those x for which $x \notin x$. If this is so, i.e. S is not an element of the set of sets that are not elements of themselves, then $S \in S$. The assumption and the conclusion are a contradiction.
- We conclude that both $S \in S$ nor $S \notin S$
- Paradox!

What to do?

- To avoid inconsistency, set theory had reject the Comprehension Principle and use an alternative set of axioms.
- A consistent axiomatic set theory is Zermelo-Fraenkel set theory with the axiom of choice, though we don't discuss this further here.

Bertrand Russell
1872-1970



One technique to avoid the problem:

- *Given a* ***set*** *S* and a predicate P, construct a new set, consisting of those elements x of S such that P(x) is true.
- You will see this technique in use when we get to the programming language Haskell, where we can write something like:

$$\{x \mid x \in \{1..\}, \text{even } x\}$$

but not

$$\{ x \mid \text{even } x\}$$

Notice that the definition of the set restricts the domain of x.

Another technique to avoid the problem:

- Russell's paradox arises from the fact that we can write funny things like $x \notin x$ (or x $\in$ x, for that matter).
- One solution: use types to forbid such expressions.
- You'll see this technique in Haskell's use of typing.

Our focus: computability

- We shall not worry about “saving” set theory from paradoxes like Russell’s
- Instead, we shall use the Russell paradox in a different setting
- But first we need to talk about Formal Languages, Haskell, and Turing Machines