Cardinality revisited

- A set is finite (has finite cardinality) if its cardinality is some (finite) integer n.
- Two sets A,B have the same cardinality iff there is a one-to-one correspondence from A to B
- E.g. alphabet (lower case)
- a b c …..
- 1 2 3 …..

Infinite sets

- Why do we care?
- Cardinality of infinite sets
- Do all infinite sets have the same cardinality?

Countable sets

Defn: Is finite OR has the same cardinality as the positive integers.

- Why do we care?

E.g.

- The algorithm works for "any n"
- Induction!

A special countable set

- The set of all binary strings

- Therefore the set of all Java programs is countable!

Countable sets – contd.

- Proving this involves (usually) constructing an explicit bijection with positive integers.
- Fact (Will not prove): Any subset of a countable set is countable.

Will prove that

- The rationals are countable!
- The reals are not countable

Countably Infinite Sets

A set S is <u>infinite</u> if there exists a surjective function $F: S \rightarrow \mathrm{N}$.
"The set N has no more elements than S."

A set S is <u>countable</u> if there exists a surjective function $F: \mathrm{N} \rightarrow S$
"The set S has not more elements than N."

A set S is <u>countably infinite</u> if there exists a bijective function $F: \mathrm{N} \rightarrow S$.
"The sets N and S are of equal size."

The integers are countable

- Write them as

  0, 1, -1, 2, -2, 3, -3, 4, -4, ……
- Find a bijection between this sequence

  and 1,2,3,4,…..

  Notice the pattern:

  $1 \to 0$ $2 \to 1$ So $f(n) = n/2$ if n even

  $3 \to -1$ $4 \to 2$ $-(n-1)/2$ o.w.

  $5 \to -2$ $6 \to 3$

Other simple bijections

- Odd positive integers

  $1 \rightarrow 1 \quad 2 \rightarrow 3 \quad 3 \rightarrow 5 \quad 4 \rightarrow 7$ ….

- Union of two countable sets A, B is countable:

  Say $f: N \rightarrow A$, $g: N \rightarrow B$ are bijections

  New bijection $h: N \rightarrow A \cup B$

  $h(n) = f(n/2)$ if n is even

  $= g((n-1)/2)$ if n is odd.

The rationals are countable

- Show that $Z^+ \times Z^+$ is countable.
- Trivial injection between Q^+, $Z^+ \times Z^+$.
- To go from Q^+ to Q, use the trick used to construct a bijection from Z to Z^+.
- Details on the board.

Facts to note

- Note that the ordering of Q is not in increasing order or decreasing order of value.
- In proofs, you CANNOT assume that an ordering has to be in increasing or decreasing order.
- So cannot use ideas like "between any two real numbers x, y, there exists a real number 0.5(x+y)" to prove uncountability.

The reals are not countable

- Wrong proof strategy:
- Suppose it is countable
- Write them down in increasing order
- Prove that there is a real number between any two successive reals.

- WHY is this incorrect?

(Note that the above “proof” would show that the rationals are not countable!!)

The reals are not countable - 2

- Cantor diagonalization argument (1879)
- VERY powerful, important technique.
- Proof by contradiction.
- Strategy
  - Assume countable
  - look at all numbers in the interval [0,1)
  - list them in ANY order
  - show that there is some number not listed

Uncountable Sets

There are infinite sets that are not countable.

Typical examples are R, P (N) and P ({0,1}*)

We prove this by a diagonalization argument.
In short, if S is countable, then you can make a list $s_1, s_2, \ldots$ of all elements of S.

Diagonalization shows that given such a list, there will always be an element x of S that does not occur in $s_1, s_2, \ldots$

Uncountability of $\mathcal{P}$ (N)

The set $\mathcal{P}$ (N) contains all the subsets of {1,2,…}.
Each subset $X \subseteq N$ can be identified by an infinite string of bits x_1x_2... such that $x_j=1$ iff $j \in X$.

There is a bijection between $\mathcal{P}$ (N) and $\{0,1\}^N$.

Proof by contradiction: Assume $\mathcal{P}$ (N) countable.
Hence there must exist a surjection F from N to the set of infinite bit strings.
"There is a list of *all* infinite bit strings."

Diagonalization

Try to list all possible infinite bit strings:

0	0	0	0	0	0	…
1	1	1	1	1	1	…
2	1	0	0	0	0	…
3	0	1	0	1	0	…
⋮						⋱

Look at the bit string on the diagonal of this table: 0101… The negation of this string (“1010…”) does not appear in the table.

No Surjection $N \rightarrow \{0,1\}^N$

Let F be a function $N \rightarrow \{0,1\}^N$.
F(1),F(2),… are all infinite bit strings.

Define the infinite string $Y=Y_1Y_2\ldots$ by
Y_j = **NOT**(j-th bit of F(j))

On the one hand $Y \in \{0,1\}^N$, but on the other hand: for every $j \in N$ we know that $F(j) \neq Y$ because F(j) and Y differ in the j-th bit.

F cannot be a surjection: $\{0,1\}^N$ is uncountable.

The set of all functions

- ....is therefore uncountable!

- So there must exist problems for which there do not exist Java programs (or pseudocode, or algorithms!)

Generalization

- We proved that $\mathcal{P}(\{0,1\}^*)$ is uncountably infinite.
- Can be generalized to $\mathcal{P}(\Sigma^*)$ for any finite Σ.

R is uncountable

- Similar diagonalization proof. We will prove [0,1) uncountable
- Let F be a function N $\rightarrow$ R
  F(1),F(2),… are all infinite digit strings (padded with zeroes if required).
- Define the infinite string of digits $Y=Y_1Y_2\ldots$ by
  $Y_j = \mathbf{F(i)}_i + 1$ **if** $\mathbf{F(i)}_i < 8$
  7 **if** $\mathbf{F(i)}_i \geq 8$

Q: Where does this proof fail on N?

Other infinities

- We proved 2^N uncountable. We can show that this set has the same cardinality as P (N) and R.
- What if we take P (R)?
- Can we build bigger and bigger infinities this way?
- Cantor: Continuum hypothesis – YES!

Notes

- The cardinality of neither the reals nor the integers are finite, yet one set is countable, the other is not.
- Q: Is there a set whose cardinality is “in-between”?
- Q: Is the cardinality of R the same as that of [0,1) ?