A short section on Counting (Section 4.2 of text)

How do we capture the size of sets (cardinality)?

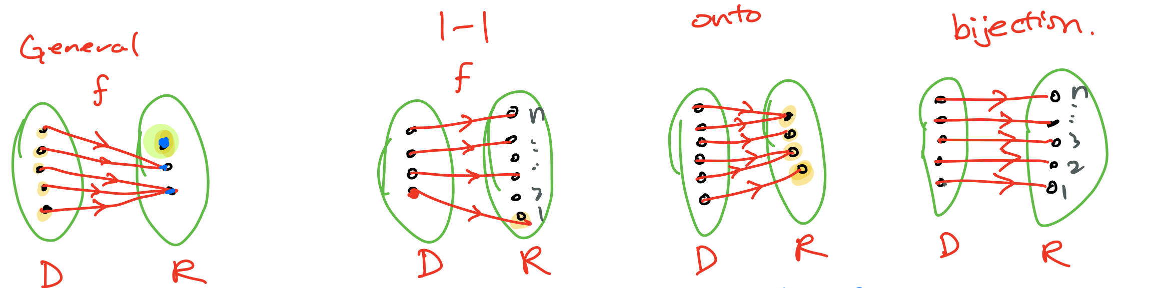
- when the set is finite
- when the set is infinite?

Recap about functions: 1-1 — injective

onto — surjective

correspondence — bijective.

function : $\underbrace{\text{Domain}}_{\text{set}} \to \underbrace{\text{Range}}_{\text{set}}$ $\qquad f : \mathbb{N} \to \mathbb{R}$



General	1-1	onto	1-1 and onto (bijection)
degree can be 0, 1, 2, ...	degree = 0 or 1	degree ≥ 1	degree = 1
	$\lvert D\rvert \leq \lvert R\rvert$	$\lvert D\rvert \geq \lvert R\rvert$	$\lvert D\rvert = \lvert R\rvert$

Defn A set S is $\boxed{\text{finite}}$ if $\exists$ integer n s.t. $\exists$ an 1-1 function from S to $\{1, 2, \ldots, n\}$ — $[n]$

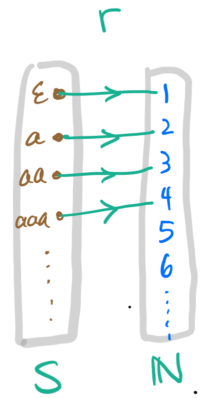
Defn If $\exists$ a bijection from S to $[n]$, then $\boxed{|S| = n}$ (the $\boxed{\text{cardinality}}$ of S)

Defn A set is $\boxed{\text{infinite}}$ if it is not finite.

Eg. $\mathbb{N} = \{1, 2, 3, \ldots\}$ is infinite set.

Def^n A set S is $\boxed{\text{countably infinite}}$ if $\exists$ a bijection r from S to $\mathbb{N}$. (alternatively W)

(In other words, S is countably infinite if we can $\boxed{\text{enumerate}}$ its elements via a $\boxed{\text{ranking function}}$ r.)



rank(aaa) = 4 $\qquad$ $r(aaa) = 4$

unrank(4) = aaa $\qquad$ $r^{-1}(4) = aaa$

In an enumeration of S, every $x \in S$ has finite rank.

Def^n A set is countable if it is either finite or countably infinite.

Def^n An enumeration of S is a bijection from S to $\mathbb{N}$.

Def^n A loose enumeration of S is a 1-1 function from S to $\mathbb{N}$.

Eg. $L((aa)^*)$

enumeration:

1. ε
2. aa
3. aaaa
4. aaaaaa

⋮

tighten $\Longleftarrow$

loose enumeration

0. ε
1.
2. aa
3.
4. aaaa

Each loose enumeration can be "tightened" into an enumeration that starts at 1.

Claim: $L(a^*)$ is countably infinite.

Proof: 0. ε
1. a
2. aa
3. aaa.

in general, string a^i has rank i in our enumeration.

is aaaaaaa in the listing?

Claim: $L((a+b)^*)$ is countably infinite.

Proof: attempt: alpha order

1. ε
2. a
3. aa
4. aaa
5. aaaa ...

Problem $\exists$ an infinite # of strings before b in the "enumeration".

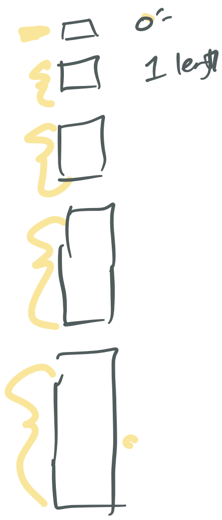
2nd attempt. $\boxed{\text{Shortlex order.}}$

- first ordering principle length
- within a length, alpha order.

1. ε
2. a
3. b.
4. a a
5. a b
6. b a
7. b b

⋮

abbab



This enumeration scheme works because for each string, $\exists$ a finite # of strings that precede it in the enumeration.

see proof later. $\square$

Claim: $\mathbb{Q}^+$, the set of positive rationals, is countably infinite.

Proof: Clearly it is infinite, since it contains $\mathbb{N}$. ie $\mathbb{N} \subseteq \mathbb{Q}^+$

How can we enumerate the rationals?

1st attempt (doomed)

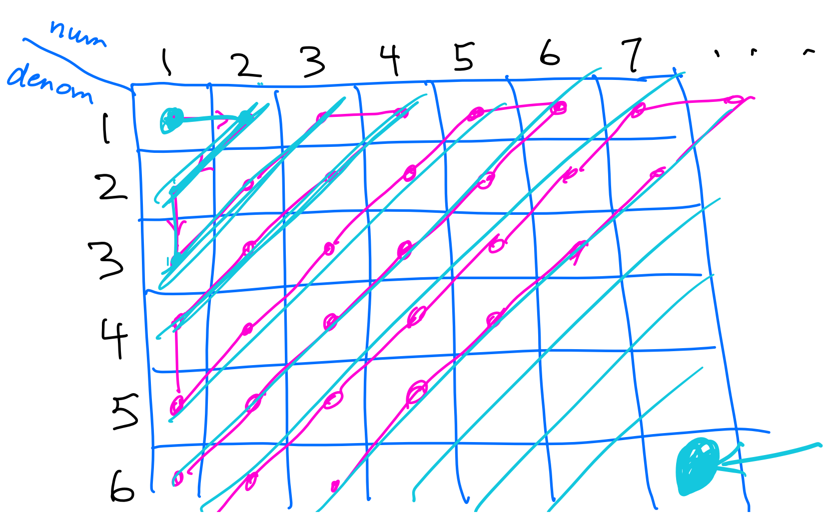
1. $1/1$
2. $1/2$
3. $1/3$
4. $1/4$

⋮

Problem: never get to $2/3$.

2nd attempt – in order of size – but what is the smallest positive rational?

3rd attempt. – A pos rational is a pos int numerator and a pos int denominator.



1. $\frac{1}{1}$ ✓
2. $\frac{2}{1}$ ✓
3. $\frac{1}{2}$ ✓
4. $\frac{1}{3}$ ✓

⋮

$\cancel{\frac{2}{2}}$ $\frac{2}{1}$

$\cancel{\frac{4}{2}}$

$\cancel{\frac{3}{3}}$ $\cancel{\frac{6}{2}}$

This is not a diagonalization proof – just a nice method for enumerating the cross product of two countably infinite sets.

Going back to our shortlex enumeration .. of strings over Σ.

Claim: $\forall$ length i, $\exists$ $|\Sigma|^i$ strings of that length.

$i = 3$, $\Sigma = \{\underbrace{a,b}_{2}\}$

$2 \times 2 \times 2$

Shortlex:

1. ε
2. a
3. b

⋮

596. aabbbb

Claim: $\forall$ strings w $\exists$ a finite number of strings over Σ that precede it in shortlex order.

Proof: Let $|w| = i$.

$\exists$ a finite # of lengths j such that $j < i$

Each length has a finite # of strings of that length.

Also, $\exists$ a finite # of strings of same length as w. ∎

Note: Shortlex works on any alphabet

If $\nexists$ an implicit ordering on the symbols of the alphabet, you can impose one arbitrarily.

eg $\{\triangle, \bigcirc, \square\}$ $\quad$ $\triangle < \bigcirc < \square$

$\{0, 1\}$ $\quad$ $0 < 1$

Is every set countable?

How about the set of infinite bit strings?

0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 0 1 0 0 0 ....

Madelaine says "YES", she has an enumeration.

I say: I can construct an infinite bitstring that is NOT in your enumeration.

Madelaine's enumeration:

T	1	2	3	4				
1	0	1	0	1	1	0	0	1
2	1	0	1	0	0	1	1	1
3	0	0	0	0	0	0	0	0
4	1	1	1	1	0	1	0	1
5	1	1	1	0	1	0	1	1
6	0	1	1	0	0	0	1	0
7	1	0	1	0	0	1	0	1

$\bar{D} = 1110011$

D = the diagonal bitstring.

$D[i] = T[i][i]$

$\bar{D}$ is the "flip" of the diagonal ie

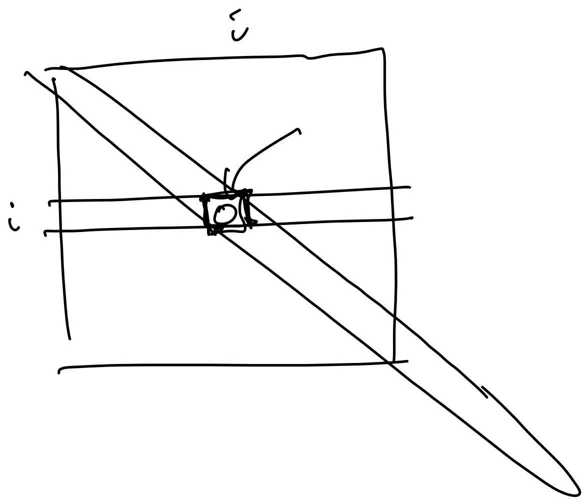
$$\bar{D}[i] = 1 - D[i] = 1 - T[i][i]$$

Claim: $\bar{D}$ is <u>not</u> enumerated.

Proof: If $\bar{D}$ is enumerated, then it has a rank r.

Then $\bar{D}[r] = \underbrace{T[r][r]}_{\bar{D}}$

But $\bar{D}[r] = 1 - T[r][r]$. $\Rightarrow\Leftarrow$



Georg Cantor

$|\mathbb{N}| = \aleph_0$

Aleph nought

$\therefore$ No enumeration can exist for infinite bitstrings.

$\therefore$ inf bitstrings are uncountably infinite. $\blacksquare$

$\mathbb{R}$ = the set of real numbers. $\mathbb{R}_{[0,1)} = \mathbb{R} \cap [0 \ldots 1)$

Claim: $\mathbb{R}_{[0,1)}$'s not countable.

Proof: BWOC. $\mathbb{S}$ $\mathbb{R}_{[0,1)}$ is countable. Then $\exists$ an enumeration:

1	.0^{1}	1	9	0	1	3	4	8	7	6	...
2	.9	2^{3}	1	2	2	3	7	9	1	0	...
3	.3	9	2^{3}	2	2	9	3	4	1	6	...
4	.2	2	2	2^{3}	0	0	0	0	0	0	...
5	.5	0	0	0	0^{1}	0	0	0	0	0	...
6	.7	6	0	1	9	2^{3}	8	7	8	7	...
7	.0	0	0	1	4	1	6^{7}	2	6	6	...
8	.1	0	0	1	9	2	1	9^{0}	3	4	
⋮											

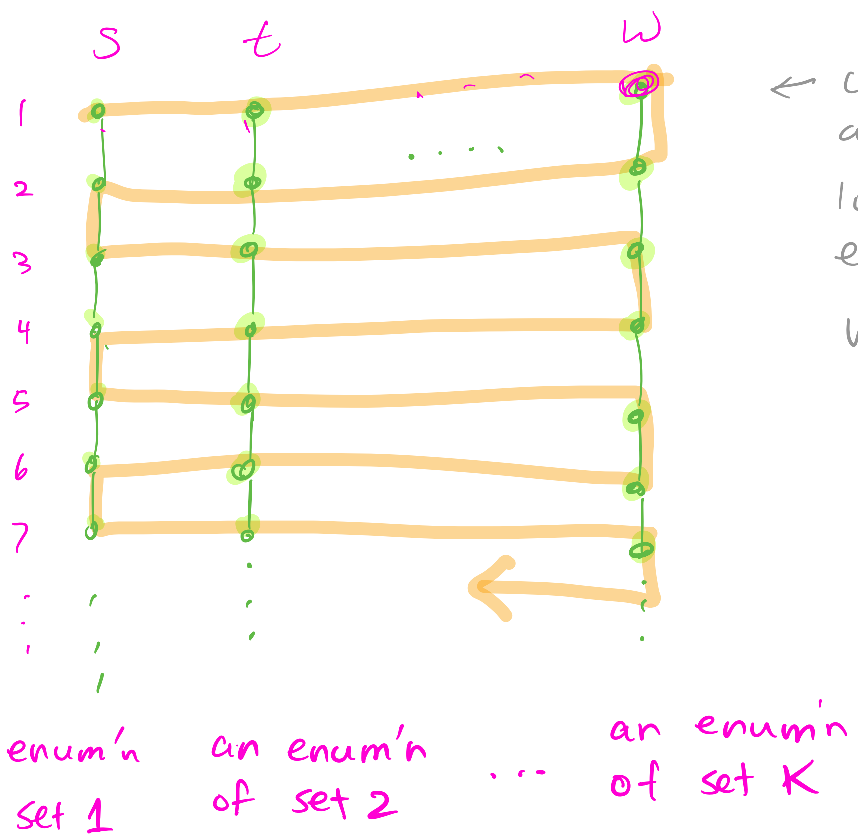
Then the number 0.13331370 . . . . , constructed by taking each digit along the diagonal and adding 1 to it (mod 10) is not in the enumeration!

$\Rightarrow$ it is not an enumeration.

Furthermore, $\forall$ proposed enumerations, you can always construct a real number that is not enumerated. ∎

Claim: The union of K countably infinite sets is also countably infinite.

Proof:



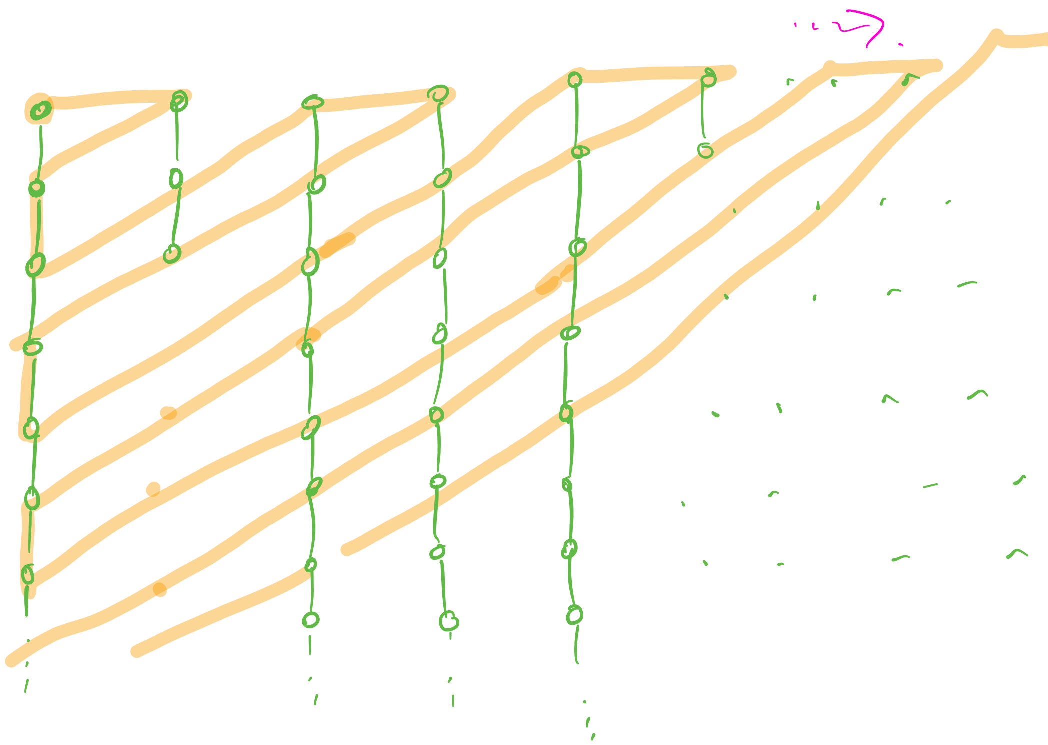
← construct a loose enumeration.

What makes it loose?

∎

Claim: The union of a countably infinite number of countable sets is countable.

Proof:



It is "loose" because:

- Some of the sets may "end early" (be finite).

But a loose enumeration is OK. $\blacksquare$

Warning: If a problem (on assignment or test) asks you to show something is countably infinite by giving an enum. scheme, I want to see the enumeration scheme, not the application of one of the theorems above.