Diagonalization is a technique we use to show a set S is smaller than a set R. The principle is simple even when the execution can be difficult to understand. In short, we find a way to index every element of S and construct an element in R that doesn't match any indexed element of S.

Ex) Let $S = \{\frac{n}{6} \mid n \in \mathbb{Z}^+\}$. Let $R = \mathbb{Q}$. Prove $|S| < |R|$.

Clearly $S \subset R$, but we can use diagonalization for this toy example.

For i, j, let $S_i(j)$ be the j^{th} digit of the i^{th} element of S.
Similarly, let $q(j)$ be the j^{th} digit of $q \in \mathbb{Q}$.

i \ j	0	1	2	3	4	5	6	7	8	...
0	[0]	0	0	0	0	0	0	0	0	
1	0	[1]	6	6	6	6	6	6	6	
2	0	3	[3]	3	3	3	3	3	3	
3	0	5	0	[0]	0	0	0	0	0	
4	0	6	6	6	[6]	6	6	6	6	
5	0	8	3	3	3	[3]	3	3	3	
6	1	0	0	0	0	0	[0]	0	0	

Pick $q \in \mathbb{Q}$ such that $\forall 0 \le i \le |S|, S_i(i) \neq q(i)$. In other words q matches no element of S along the diagonal, thus q cannot be in S, therefore $S \subset R$ and $|S| < |R|$.

Here we can pick $q = 1.201005$, which is rational and satisfies the above requirement.

□

Ex) Prove $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Since $\forall n$, $\{n\} \in \mathcal{P}(\mathbb{N})$, it's clear that $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$.

To show that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, it suffices to show that there is no surjection $f: \mathbb{N} \to \mathcal{P}(\mathbb{N})$. For the sake of contradiction, assume there *is* such a surjection f. Then we can enumerate the values f takes.

i	$f(i)$	$0 \in f(i)$	$1 \in f(i)$	$2 \in f(i)$	$3 \in f(i)$	.....
0	$\mathbb{N}$	✓	✓	✓	✓	...
1	$\emptyset$	X	X	X	X	...
2	odds	X	✓	X	✓	...
3	evens	✓	X	✓	X	...
4	multiples of 3	✓	X	X	✓	...
⋮	⋮	⋮	⋮	⋮	⋮	⋱

We now construct a bad actor set in $\mathcal{P}(\mathbb{N})$ that matches no $f(i)$. If we can do that, then f is not surjective, which is nonsense because it is, so this contradiction implies no such f exists and $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Let $R = \{i \in \mathbb{N} \mid i \notin f(i)\}$.

Then for $i \in \mathbb{N}$, we have the following cases.

If $i \in f(i)$, then $i \notin R$, hence $R \neq f(i)$.

If $i \notin f(i)$, then $i \in R$, hence $R \neq f(i)$.

But i was arbitrary, so $\forall i \in \mathbb{N}$, $R \neq f(i)$.

□

This argument generalizes to any arbitrary set S.

Ex) Let S be a set. Prove $|S| < |\mathcal{P}(S)|$.

As before, $\forall s \in S$, $\{s\} \in \mathcal{P}(S)$, so $|S| \leq |\mathcal{P}(S)|$.

It remains to show that $|S| \neq |\mathcal{P}(S)|$. To do so, it suffices to show that there is surjection $f: S \to \mathcal{P}(S)$.

For the sake of contradiction, assume a surjection $f: S \to \mathcal{P}(S)$ exists.

Now define the set $R = \{s \in S \mid s \notin f(s)\}$.

Since f is a surjection, $\exists s_0 \in S$ for which $R = f(s_0)$.

This gives us the following two cases.

If $s_0 \in f(s_0)$, then $s_0 \notin R$, thus $R \neq f(s_0)$.

If $s_0 \notin f(s_0)$, then $s_0 \in R$, thus $R \neq f(s_0)$.

But then $R = f(s_0)$ and $R \neq f(s_0)$, which is absurd.

Thus no such f exists.

Therefore $|S| < |\mathcal{P}(S)|$.

□

At the beginning of this course, we used diagonalization to show there are more real numbers than naturals. We reproduce this proof here (which has a number of useful consequences).

Ex) Prove $|\mathbb{N}| < |\mathbb{R}|$.

$\mathbb{N} \subset \mathbb{R}$, so clearly $|\mathbb{N}| \leq |\mathbb{R}|$. To show $|\mathbb{N}| \neq |\mathbb{R}|$, it suffices to show there is no surjection $f: \mathbb{N} \to \mathbb{R}$.

For the sake of contradiction, assume there is such an f.

Then if $f(i)(j) = r_i(j)$ is the j^{th} digit of the i^{th} real, we can enumerate them as follows.

i \ j	0	1	2	3	4	5	...
0	1	3	1	4	1	5	9
1	2	2	2	2	2	2	2
2	4	1	2	7	3	1	9
3	1	0	0	0	0	0	0
4	3	4	1	2	2	3	9
5	1	1	1	1	1	1	1
⋮							

An example enumeration of $\mathbb{R}$ with f. The actual values of f are not under our control.

Pick $r \in \mathbb{R}$ that we define as follows, for $i \in \mathbb{N}$.

$$r(i) = \begin{cases} 0 & r_i(i) \neq 0 \\ 1 & r_i(i) = 0. \end{cases}$$

Then for any $i \in \mathbb{N}$, we have $r(i) \neq r_i(i)$, so $r \neq r_i$ for any i. Thus f is not a surjection.

$\rightarrow\leftarrow$

$\therefore$ No such f exists and thus $|\mathbb{N}| < |\mathbb{R}|$. □

This size disparity between countable sets and uncountable sets (particularly countable sets and their power sets) has many interesting consequences.

Ex) There exists a language which is not recognizable.

pf) We can encode a TM into a string in Σ^*.
However, the set of all languages is $\mathcal{P}(\Sigma^*)$.
Since $|\Sigma^*| < |\mathcal{P}(\Sigma^*)|$, there is some language L for which no TM M satisfies $L(M) = L$.
Thus L is not recognizable.

We can actually extend this proof with a measure to show almost all languages are not recognizable, but such is beyond the scope of this course.

The set of all languages $\mathcal{L} = \mathcal{P}(\Sigma^*)$ is uncountable, whereas the set of all TM encodings (and thus TMs) is $\mathcal{M} \in \mathcal{L}$. In other words $|\mathcal{M}| < |\mathcal{L}|$.

This garantees we can perform a number of interesting diagonalizations.

Let $M_i \in \mathcal{M}$ be the i^{th} TM.

Let $w_i \in \Sigma^*$ be the i^{th} string.

Prove That

$$A_{TM} = \{ \langle M_i, w_j \rangle \mid i, j \in \mathbb{N} \text{ and } M_i \text{ accepts } w_j \}$$

is recognizable. Then prove that it is not decidable.

Hint: Try giving a decider for D_{TM} using a decider for A_{TM}.

$$D_{TM} = \{ \langle M_i, \langle M_i \rangle \rangle \mid i \in \mathbb{N} \text{ and } M_i \text{ rejects } \langle M_i \rangle \}$$

Prove that if

$$EQ_{TM} = \{ \langle M_i, M_j \rangle \mid i, j \in \mathbb{N} \text{ and } L(M_i) = L(M_j) \},$$

then either EQ_{TM} is recognizable or $\overline{EQ_{TM}}$ is recognizable.

Now show that EQ_{TM} is not decidable.

Hint: Assume that EQ_{TM} is decidable and show that A_{TM} is as well.

This leads into our discussion of reducability and co-RE.

Use diagonalization to show that the language

$A_{TM} = \{\langle M, w\rangle \mid M \text{ is a TM and } M(w) \text{ accepts}\}$

is not decidable (Hint: the set of all TMs is enumerable, so consider running $M_i(\langle M_j\rangle)$). In addition, show that A_{TM} is recognizable.

To show A_{TM} is recognizable, we give a TM N for which $L(N) = A_{TM}$.

N = "On input $\langle M, w\rangle$, ← If the input isn't of this format, we reject immediately.

1) Run $M(w)$.
2) If $M(w)$ accepted, accept
3) Otherwise reject"

Now to show A_{TM} is not decidable, suppose for the sake of contradiction that it is. Then there is a decider D with $L(D) = A_{TM}$.

Consider the following TM B.

B = "On input $\langle M\rangle$,

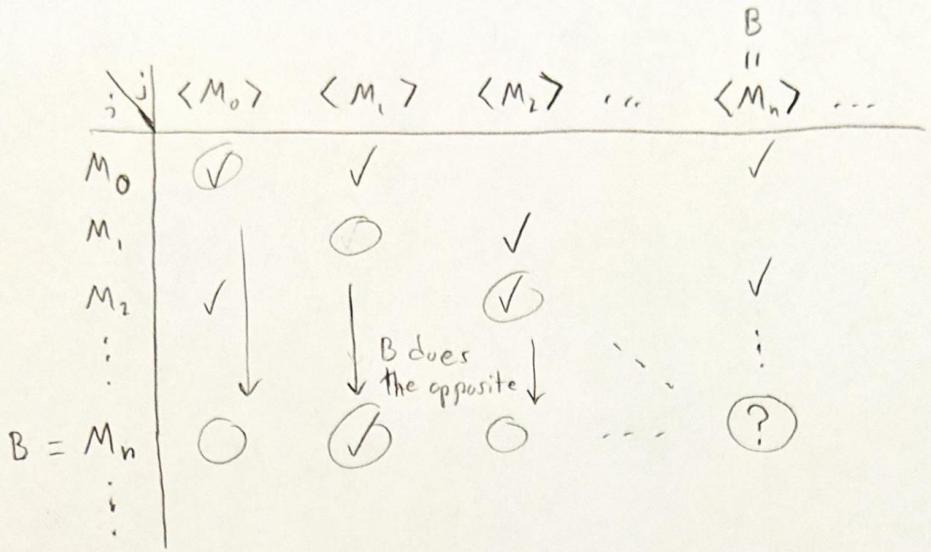
1) Run $D(\langle M, \langle M\rangle\rangle)$
2) If D accepts $\langle M, \langle M\rangle\rangle$, reject
3) Otherwise accept."

What is the language of B? It's

$L(B) = \{\langle M\rangle \mid M \text{ is a TM and } M(\langle M\rangle) \text{ rejects}\}$.

Why does this matter?

Let's draw the behavior of D as a table. D accepts $\langle M_i, \langle M_j\rangle\rangle$ iff $M_i(\langle M_j\rangle)$ accepts (we leave an entry blank if $M_i(\langle M_j\rangle)$ loops or rejects).



n is the index of B in the enumeration of all TMs, which must exist.

D accepts whevever there is a ✓ and rejects otherwise

So if D exists, B must also exist and is a decider. But when we consider B(⟨B⟩), we end up in the awkward situation where:

If B accepts ⟨B⟩, then B(⟨B⟩) rejects ⇒ B does not accept ⟨B⟩.

If B rejects ⟨B⟩, then B(⟨B⟩) accepts ⇒ B accepts ⟨B⟩.

In either case we have a contradiction, so no such D can exist.

Thus A_{TM} is not decidable.

□

Prove EQ_{TM} is co-RE.

We give a TM M for $\overline{EQ_{TM}}$.

M = "On input ⟨M_i, M_j⟩, ← reject if not formatted properly

1) For k = 1 to ∞

a) Run M_i and M_j on strings $w_1, \dots, w_k$ for k steps

b) If M_i and M_j disagree on any string, accept"

Clearly, $L(M) = \overline{EQ_{TM}}$.

Now assume EQ_{TM} is decidable. Then there is a TM D which decider it

Define the TMs $N_{M,w}$ and A

$N_{M,w}$ = " On input x,

1) Run $M(w)$
2) Accept if $M(w)$ accepts
3) Reject "

A = " On input w,
1) Accept "

Notice that $L(N_w) = \begin{cases} \Sigma^* & M(w) \text{ accepts} \\ \varnothing & \text{otherwise} \end{cases}$ and $L(A) = \Sigma^*$.

Hence $L(N_w) = L(A)$ iff $M(w)$ accepts. Then the following TM D' will decide A_{TM}, which is undecidable. As such, no such D exists, and thus EQ_{TM} is not decidable.

D' = " On input $\langle M, w \rangle$,
1) Run $D(\langle N_{M,w}, A \rangle)$
2) If D accepts, accept
3) If D rejects, reject."

D' always halts since D is a decider. Moreover, clearly D' accepts iff $M(w)$ accepts.

□