# Encoding First-Order Data

We are building towards the famously undecidable Halting Problem.

Intuitively,

Consider the following machines:

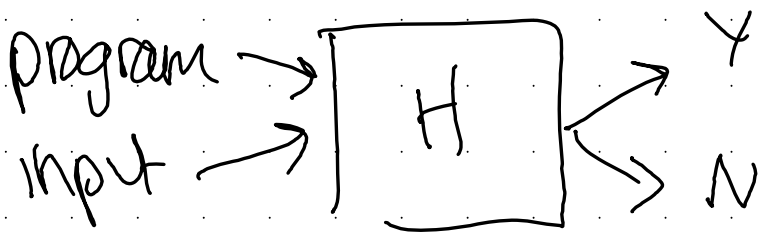




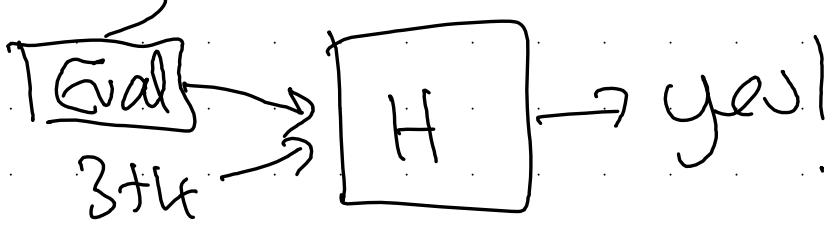


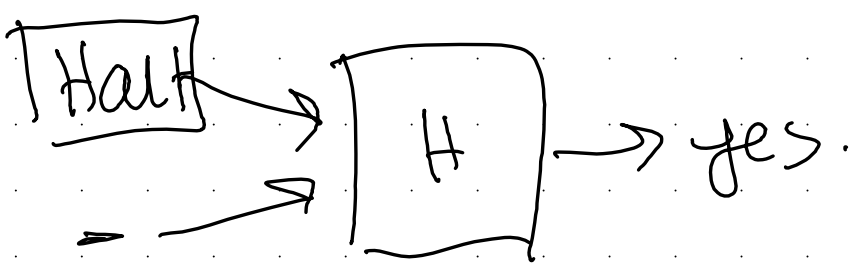


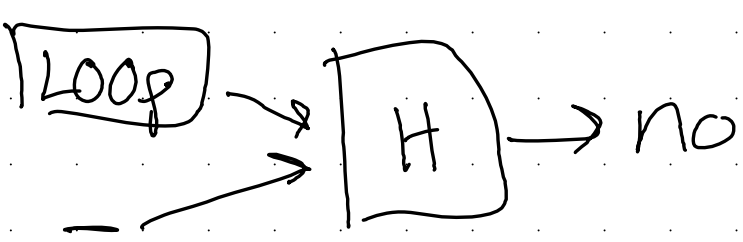

The Halting Problem states that the following machine cannot be created:

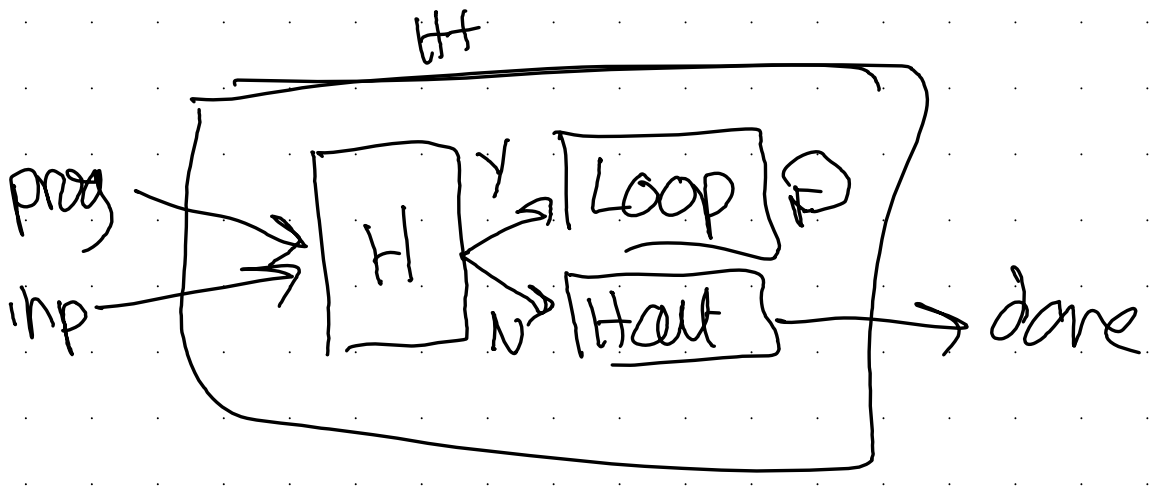



e.g.




If H says yes, then it will loop forever
... so we should have said no

If H says no, then it will halt
... so we should have said Y

This is a proof by contradiction showing that the Halting Problem is undecidable.

As part of this course, we will show this formally

⇒ we need to be able to encode whole programs as natural numbers

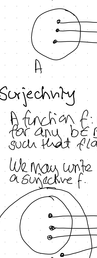
# Mathematical Tools

## Bijections
- Then two defs
  - via injectivity + surjectivity
  - via isomorphism
- example: $\mathbb{Z} \cong \mathbb{N}$

## Injectivity:

A function $f: A \to B$ is injective just if for any $a_1, a_2 \in A$, we have that $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

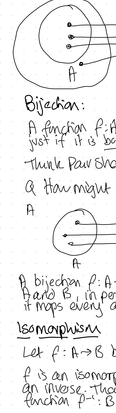
We may write $f: A \rightarrowtail B$ for an injective f.




## Surjectivity

A function $f: A \to B$ is surjective just if for any $b \in B$ there exists $a \in A$ such that $f(a) = b$.

We may write $f: A \twoheadrightarrow B$ for a surjective f.

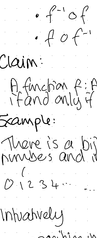



## Bijection:

A function $f: A \to B$ is a bijection just if it is both injective and surjective.

Think Pair Share:

Q How might I draw a bijection




A bijection $f: A \to B$ puts the two sets, A and B, in perfect correspondence: it maps every $a \in A$ uniquely to a $b \in B$.

## Isomorphism

Let $f: A \to B$ be a function.

f is an isomorphism just if it has an inverse. That is, there exists a function $f^{-1}: B \to A$ such that

- for all $a \in A$ we have $f^{-1}(f(a)) = a$
- for all $b \in B$, we have $f(f^{-1}(b)) = b$

Alternative:

- $f^{-1} \circ f = id_A$
- $f \circ f^{-1} = id_B$

## Claim:

A function $f: A \to B$ is a bijection if and only if it is an isomorphism

## Example:

There is a bijection between natural numbers and integers:

0 1 2 3 4 ⋯ ⋯ −2 −1 0 1 2 ⋯

Intuitively

- positive ints to even nats
- negative ints to odd nats

Formally

We define

$$\beta: \mathbb{Z} \to \mathbb{N}$$

$$\beta(x) = \begin{cases} 2x & x \geq 0 \\ -2x - 1 & x < 0 \end{cases}$$

Claim: $\beta$ is a bijection

Proof (inj + surj)

① $\beta$ is injective

GOAL = for all $k_1, k_2 \in \mathbb{Z}$, $\beta(k_1) = \beta(k_2)$ implies $k_1 = k_2$

Fix $k_1, k_2 \in \mathbb{Z}$

Assume $P: \beta(k_1) = \beta(k_2)$

GOAL': $k_1 = k_2$

Case on $k_1, k_2$ neg/pos:

i) $k_1, k_2$ are both positive:

$$\begin{aligned} P: \beta(k_1) &= \beta(k_2) \\ 2k_1 &= 2k_2 \\ k_1 &= k_2 \end{aligned}$$

ii) $k_1, k_2$ are both negative

$$\begin{aligned} P: \beta(k_1) &= \beta(k_2) \\ -2k_1 - 1 &= -2k_2 - 1 \\ k_1 &= k_2 \end{aligned}$$

iii) $k_1$ pos, $k_2$ neg

$$\begin{aligned} P: \beta(k_1) &= \beta(k_2) \\ 2k_1 &= -2k_2 - 1 \\ 2k_1 + 2k_2 &= -1 \\ 2(k_1 + k_2) &= -1 \\ k_1 + k_2 &= -1/2 \end{aligned}$$

Integers are whole numbers, so this cannot occur.

iv) Analogous to (iii)

I forgot to also show $\beta$ is be surjective! Here is the proof:

② $\beta$ is surjective

GOAL = for all $n \in \mathbb{N}$, there exists a $k \in \mathbb{Z}$ such that $\beta(k) = n$.

Fix $n \in \mathbb{N}$

GOAL' = provide $k \in \mathbb{Z}$ such that $\beta(k) = n$

We will case on the parity of n.

i) n even:

Here we can combine the general form of even numbers with the definition of $\beta$ to find a suitable k.

If we write it as $n = 2n'$, we can use $k = n'$, which fulfils the condition:

$$\beta(n') = 2n'$$
$$= n \text{ as desired}$$

ii) n odd:

Same process, but it is maybe a tad less obvious for odd numbers. From $\beta$ and our odd number form, we get two equations for n:

$$n = -2k - 1 \qquad n = 2n' + 1$$

We can equate these and solve for k:

$$\begin{aligned} 2n' + 1 &= -2k - 1 \\ 2n' + 2 &= -2k \\ \longrightarrow \quad k &= -n' - 1 \end{aligned}$$

This process guarantees that k fulfils the condition

If we write it as $n = 2n' + 1$, then $k = -n' - 1$, which fulfils our condition

$$\begin{aligned} \beta(-n' - 1) &= -2(-n' - 1) - 1 \\ &= 2n' + 2 - 1 \\ &= 2n' + 1 \\ &= n \text{ as desired} \end{aligned}$$

Proof (isomorphism):

To prove this

- Define $\beta^{-1}: \mathbb{N} \to \mathbb{Z}$
- Prove the round hopping

$$\beta^{-1}(n) = \begin{cases} n/2 & \text{if } n \text{ is even} \\ -(n+1)/2 & \text{if } n \text{ is odd} \end{cases}$$

$$\begin{aligned} n &= -2i - 1 \\ n + 1 &= -2i \\ i &= -(n+1)/2 \end{aligned}$$