Warm-Up Problem

Please fill out your Teaching Evaluation Survey!

Warm up: Given a program P that accepts input and input I, does P run forever on I?

Theorem: The Looping Problem is undecidable.

Beyond CS 245

Carmen Bruni

Lecture 24

Based on slides by Jonathan Buss, Lila Kari, Anna Lubiw and Steve Wolfman with thanks to B. Bonakdarpour, A. Gao, D. Maftuleac, C. Roberts, R. Trefler, and P. Van Beek

Last Time

- Prove that the Halting Problem is Undecidable
- Prove other problems are undecidable based on reductions to the Halting Problem.

Email

Correction: I thought we could be sloppy with the words“array assignment” - apparently not all instructors agreed with this this term - please always add the word “array” when annotating array assignments.

The Technique: “Diagonalization”

The technique used in the proof of the undecidability of the halting problem is called **diagonalization**.

It was originally devised by Georg Cantor (in 1873) for a different purpose.

Cantor was concerned with the problem of measuring the sizes of infinite sets. Are some infinite sets larger than others?

Example. The set of even natural numbers is the same size (!!) as the set of all natural numbers.

Example. The set of all infinite sequences over $\{0, 1\}$ is larger than the set of natural numbers.

(Idea of proof: (A) Assume that each sequence has a number. (B) find a sequence that is different from every numbered sequence.)

Countable sets

A set S is **countable** if there is a one-to-one correspondence between S and the set of natural numbers ($\mathbb{N}$).

How do we prove that a set is **uncountable**?

Cantor's diagonal argument

Consider an infinite sequence $S = (s_1, s_2, ...)$, where each element s_i is an infinite sequence of 1s or 0s (s_i is a binary string of infinite length).

$$\begin{aligned}
s_1 &= (0,0,0,0,0,0,...)\\
s_2 &= (1,1,1,1,1,1,...)\\
s_3 &= (0,1,0,1,0,1,...)\\
s_4 &= (1,0,1,0,1,0,...)\\
s_5 &= (1,1,0,0,1,1,...)\\
s_6 &= (0,0,1,1,0,0,...)\\
&...
\end{aligned}$$

Cantor's diagonal argument

There is a sequence $\overline{s}$ such that if $s_{n,n} = 1$, then $\overline{s}_n = 0$, and otherwise $\overline{s}_n = 1$.

$$
\begin{aligned}
s_1 &= (\mathbf{0}, 0, 0, 0, 0, 0, \ldots) \\
s_2 &= (1, \mathbf{1}, 1, 1, 1, 1, \ldots) \\
s_3 &= (0, 1, \mathbf{0}, 1, 0, 1, \ldots) \\
s_4 &= (1, 0, 1, \mathbf{0}, 1, 0, \ldots) \\
s_5 &= (1, 1, 0, 0, \mathbf{1}, 1, \ldots) \\
s_6 &= (0, 0, 1, 1, 0, \mathbf{0}, \ldots) \\
&\ldots
\end{aligned}
$$

Define $\overline{s} = (1, 0, 1, 1, 0, 1, \ldots)$.

Then $\overline{s}$ is not any of the sequences s_i on the list S.

Cantor's diagonal argument

By construction, $\overline{s}$ is not contained in the countable sequence S.

Let T be a set consisting of all infinite sequences of 0s and 1s. By definition, T must contain S and $\overline{s}$.

Since $\overline{s}$ is not in S, the set T cannot coincide with S.

Therefore, T is uncountable; it cannot be placed in one-to-one correspondence with $\mathbb{N}$.

Cantor's diagonal argument

Therefore, the set of even integers is smaller than the set of all infinite sequences over $\{0, 1\}$.

$\mathbb{R}$ is Uncountable

We will show that a subset of $\mathbb{R}$, per example $(0,1)$, is uncountable.

Let S be the following countable sequence of elements from $(0,1)$:
$e_1 = 0.3245890172245\ldots$
$e_2 = 0.1478562003640\ldots$
$e_3 = 0.7129601400235\ldots$
$e_4 = 0.0024533889974\ldots$
$e_5 = 0.5364578912235\ldots$
$e_6 = 0.8581488004222\ldots$
$\ldots$

$\mathbb{R}$ is Uncountable

It is possible to build a new number $\overline{e} = (0.\overline{e}_1\overline{e}_2\overline{e}_3\ldots)$ in such a way that if $e_{n,n} = k$, where k is one digit natural number, then $\overline{e}_n$ is an one-digit natural number different than k.

$e_1 = 0.\mathbf{3}245890172245\ldots$
$e_2 = 0.1\mathbf{4}78562003640\ldots$
$e_3 = 0.71\mathbf{2}9601400235\ldots$
$e_4 = 0.002\mathbf{4}533889974\ldots$
$e_5 = 0.5364\mathbf{5}78912235\ldots$
$e_6 = 0.85814\mathbf{8}8004222\ldots$
$\ldots$

$\overline{e} = (0.580135\ldots)$

$\mathbb{R}$ is Uncountable

By the construction, $\overline{e} \in (0,1)$ is not contained in the countable set S.

Therefore the countable set S cannot coincide with $(0,1)$.
We obtain that $(0,1)$ is uncountable.

$\mathbb{R}$ is Uncountable (long proof)

We build an one-to-one correspondence between the set T and a subset of $\mathbb{R}$.

Let function $f(t) = 0.t$, where t is a string in T.
Reworded, $f(x_1 ... x_n ...) = \sum_{i=1}^{\infty} \frac{x_i}{2^i}$
For example, $f(0111\,...) = 0.0111\,....$

Observe that $f(1000\,...) = 0.1000\,... = 1/2$, and
$f(0111\,...) = 0.0111\,... = 1/4 + 1/8 + 1/16 + ... = \sum_{n=2}^{\infty} \frac{1}{2^n} = 1/2$.

Hence, f is not a bijection.

Cantor's diagonal argument (long proof)

To produce a bijection from T to the interval $(0,1) \subset \mathbb{R}$:

- From $(0,1)$ remove the numbers having two binary expansions and form $a = (1/2, 1/4, 3/4, 1/8, 3/8, 5/8, 7/8, ...)$.
- From T, remove the strings appearing after the binary point in the binary expansions of 0, 1, and the numbers in sequence a and form $b = (000\ldots, 111\ldots, 1000\ldots, 0111\ldots, 01000\ldots, 00111\ldots, ...)$.

$g(t)$ from T to $(0,1)$ is defined by: If t is the nth string in sequence b, let $g(t)$ be the nth number in sequence a; otherwise, let $g(t) = 0.t$.

Cantor's diagonal argument (long proof)

To build a bijection from T to $\mathbb{R}$, we use $tan(x)$, a bijection from $(\pi/2, \pi/2)$ to $\mathbb{R}$.

The linear function $h(x) = \pi.x - \pi/2$ provides a bijection from $(0, 1)$ to $(-\pi/2, \pi/2)$.

The composite function $tan(h(x))$ provides a bijection from $(0, 1)$ to $\mathbb{R}$.

The function $tan(h(g(t)))$ is a bijection from T to $\mathbb{R}$.

Cantor's diagonal argument

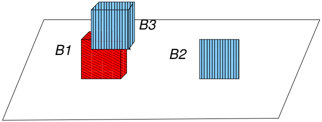
Using diagonalization, one can show that (for example):

- $|\mathbb{Q}| = |\mathbb{N}| = |\mathbb{Z}|$
- $|\mathbb{N}| < |2^{\mathbb{N}}|$
- The set of all functions from $\mathbb{N}$ to $\mathbb{N}$ is uncountable.

A Classic AI Example: Blocks Worlds

A “blocks world” consists of a set of blocks, and a table.

- Each block may be on the table, or on one of the other blocks.
- Each block may have a colour.



In the picture, there are three blocks.

Two of them are blue (vertical stripes) and one is red (diagonal stripes).

Set of objects: $\{B1, B2, B3\}$.

We can describe the world with relations: *On*, *OnTable*, *Red*, *Blue*, ...

Describing a Blocks World

The domain $\{B1, B2, B3\}$ is a finite set.

Therefore, we can list all of the properties, in various ways:

- *OnTable*$(B1)$, *OnTable*$(B2)$, $\neg$*OnTable*$(B3)$.
- *On*:

	B1	B2	B3
B1	F	F	F
B2	F	F	F
B3	T	F	F

- The set $\{\, b \mid \textit{Blue}(b) \,\}$ of blue blocks is $\{B2, B3\}$.

Properties in the Blocks World

Some properties are fundamental to the world.

"No box is on itself" $\big(\forall x\,(\neg \mathit{On}(x,x))\big)$.

"A box on the table is not on any box":

$$\Big(\forall x\,\Big(\mathit{OnTable}(x) \to (\neg(\exists y\ \mathit{On}(x,y)))\Big)\Big)\ .$$

Some properties depend on the situation.

"Every red box has a box on it": $\Big(\forall x\,\Big(\mathit{Red}(x) \to \exists y\ \mathit{On}(y,x)\Big)\Big)$.

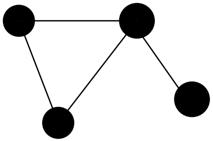
"Some box is on a box that is on the table":

$$\big(\exists x\ \exists y\,(\mathit{On}(x,y) \wedge \mathit{OnTable}(y))\big)\ .$$

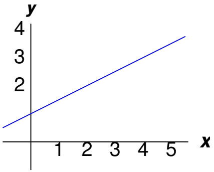
Graphs

A *graph* is a binary relation.

A finite graph:



An infinite graph:



(The set $\{ \langle x, y \rangle \mid y = 1 + x/2 \}$).

A graph is *undirected* if the relation is symmetric; i.e., the formula

$$\forall x \; \forall y \left(E(x, y) \rightarrow E(y, x) \right)$$

holds.

Relational Databases

A *relational database* is a listing of one or more relations.

Example:

- *Person*: The people (or their names).
- *NumberOf*: An association between people and their phone numbers.

Here the domain contains both people and phone numbers — the objects about which we have relations.

A sample statement: “Somebody has no phone number.”

$$\exists x \left(\mathit{Person}(x) \wedge (\neg(\exists y\, (\mathit{NumberOf}(x,y)))) \right) .$$

Automation

- https://proofs.openlogicproject.org/
- https://github.com/StephanieMcIntyre/cs245-verification/blob/master/Assignments/simple.dfy
- https://rise4fun.com/dafny

Axioms on One Slide and Equality

- PA1: $\big(\forall x\,(\neg(s(x) = 0))\big)$
- PA2: $\Big(\forall x\,\big(\forall y\,((s(x) = s(y)) \to (x = y))\big)\Big)$
- PA3: $\big(\forall x\,((x + 0) = x)\big)$
- PA4: $\Big(\forall x\,\big(\forall y\,((x + s(y)) = s((x + y)))\big)\Big)$
- PA5: $\big(\forall x\,((x \times 0) = 0)\big)$
- PA6: $\Big(\forall x\,\big(\forall y\,((x \times s(y)) = ((x \times y) + x))\big)\Big)$
- PA7: $\Big(\varphi[0/v] \to \big((\forall v\,(\varphi \to \varphi[s(v)/v])) \to (\forall v\ \varphi)\big)\Big)$
- EQsymm: $\Big(\forall x\,\big(\forall y\,((x = y) \to (y = x))\big)\Big)$
- EQtrans(k): $\dfrac{(t_1 = t_2) \quad (t_2 = t_3) \quad \cdots \quad (t_k = t_{k+1})}{(t_1 = t_{k+1})}$
- EQsubs(r): $\dfrac{(t_1 = t_2)}{(r[t_1/z] = r[t_2/z])}$