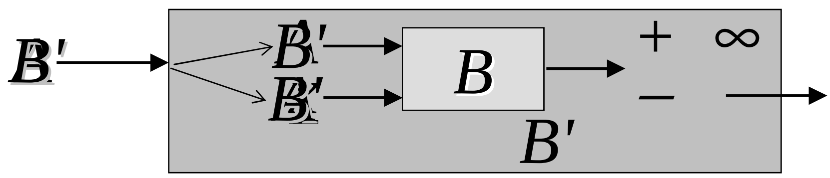
I. Recap on the discrete Theory of Computation

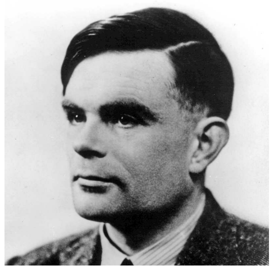
- un-/computability, Halting Problem
- oracle computation
- Asymptotic runtime and memory
- Machine models: unit vs. bit cost
- $\mathcal{L}$, $\mathcal{P}$, $\mathcal{NP}_1$, $\mathcal{NP}$, $\#\mathcal{P}$, $\mathcal{PSPACE}$, $\mathcal{EXP}$
- Reduction and completeness
- Parameterized complexity

Alan M. Turing 1936

•first scientific calculations on digital computers

•*What are its fundamental limitations?*





•Undecidable Halting Problem *H*: **No** algorithm *B* can always correctly ans ~~simulator/interpreter *B* ?~~

Given ⟨A,x⟩, does algorithm A terminate on input x?

Proof by contradiction: Consider algorithm *B*' that, on input *A*, executes *B* on ⟨*A*,*A*⟩ and, upon a positive answer, loops infinitely. How does *B*' behave on *B*' ?

Un-/Semi-/Decidability I

Definition: a) An 'algorithm' $\mathcal{A}$ computes a partial function $f{:\subseteq}\{0,1\}^* \to \{0,1\}^*$ if it

- on inputs $\underline{x}\in\mathrm{dom}(f)$ prints $f(\underline{x})$ and terminates,
- on inputs $\underline{x}\notin\mathrm{dom}(f)$ does not terminate.

Injective string pairing function ("*Hilbert Hotel*")

$$\langle x_1,\ldots,x_n\,;\,y_1,\ldots,y_m\rangle := 0\,x_1\,0\,x_2\,0\ldots 0\,x_n\,1\,y_1\ldots y_m$$

b) $\mathcal{A}$ decides set $L\subseteq\{0,1\}^*$ if it computes its total char. function: $\mathrm{cf}_L(\underline{x}):=1$ for $\underline{x}\in L$, $\mathrm{cf}_L(\underline{x}):=0$ for $\underline{x}\notin L$.

c) $\mathcal{A}$ semi-decides L if terminates precisely on $\underline{x}\in L$

d) $\mathcal{A}$ enumerates L if it computes some total bijection $f{:}\{0,1\}^*{=}\mathbb{N}\to L$.

Un-/Semi-/Decidability II

Example: The Halting problem H, considered as subset of $\{0,1\}^*$, is semi-decidable, not decidable.

Theorem: a) Every finite L is decidable.

b) L is decidable iff its complement $\overline{L}$ is.

c) L is decidable iff both L, $\overline{L}$ are semi-decidable.

d) L is enumerable iff infinite and semi-decidable.

b) $\mathcal{A}$ decides set $L\subseteq\{0,1\}^*$ if it computes its total char. function: $\mathrm{cf}_L(\underline{x}):=1$ for $\underline{x}\in L$, $\mathrm{cf}_L(\underline{x}):=0$ for $\underline{x}\notin L$.

c) $\mathcal{A}$ semi-decides L if terminates precisely on $\underline{x}\in L$

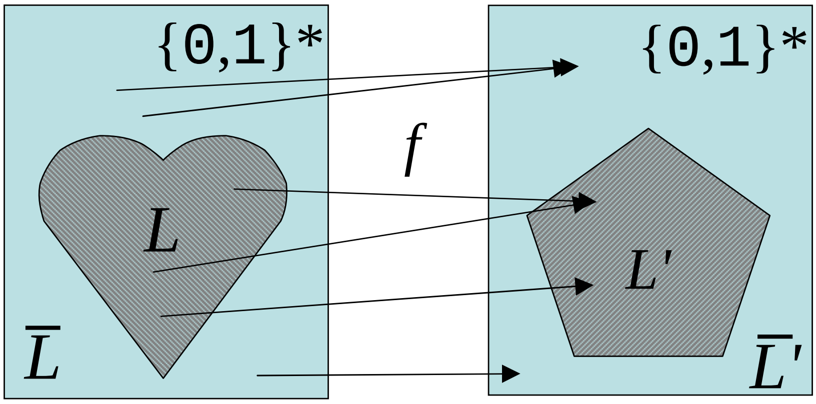
d) $\mathcal{A}$ enumerates L if it computes some total bijection $f{:}\{0,1\}^*{=}\mathbb{N}\to L$.

Comparing Decision Problems

Halting problem $H = \{ \langle \mathcal{A}, \underline{x} \rangle : \mathcal{A}(\underline{x}) \text{ terminates } \}$

Nontriviality $N = \{ \langle \mathcal{A} \rangle : \exists \underline{y}\ \mathcal{A}(\underline{y}) \text{ terminates } \}$

Totality problem $T = \{ \langle \mathcal{A} \rangle : \forall \underline{z}\ \mathcal{A}(\underline{z}) \text{ terminates} \}$



- $H \leqslant N$ undecidable
- $H \leqslant T$ undecidable
- $N \leqslant H \not\leqslant \overline{H}$
- $\overline{H} \leqslant T \Rightarrow T \not\leqslant H$

For $L, L' \subseteq \{0,1\}^*$ write $L \leqslant L'$ if there is a computable $f: \{0,1\}^* \to \{0,1\}^*$ such that $\forall \underline{x}: \ \underline{x} \in L \Leftrightarrow f(\underline{x}) \in L'$.
a) $\overline{L'}$ semi-/decidable $\Rightarrow$ so $\overline{L}$. b) $L \leqslant L' \leqslant L'' \Rightarrow L \leqslant L''$

Examples of Undecidability

KAIST CS700 M. Ziegler

Universes $\mathcal{U}$ other than {0,1}* (e.g. $\mathbb{N}$): encode.

Halting problem: $H = \{ \langle \mathcal{A}, \underline{x} \rangle : A \text{ terminates on } \underline{x} \}$

Hilbert's 10th: The following set is undecidable:

$\{ \langle p \rangle \mid p \in \mathbb{N}[X_1, \ldots X_n], n \in \mathbb{N}, \exists x_1 \ldots x_n \in \mathbb{N}\ \ p(x_1, \ldots x_n) = 0 \}$

Word Problem for finitely presented groups

Mortality Problem for two 21×21 matrices

Homeomorphy of two finite simplicial complexes

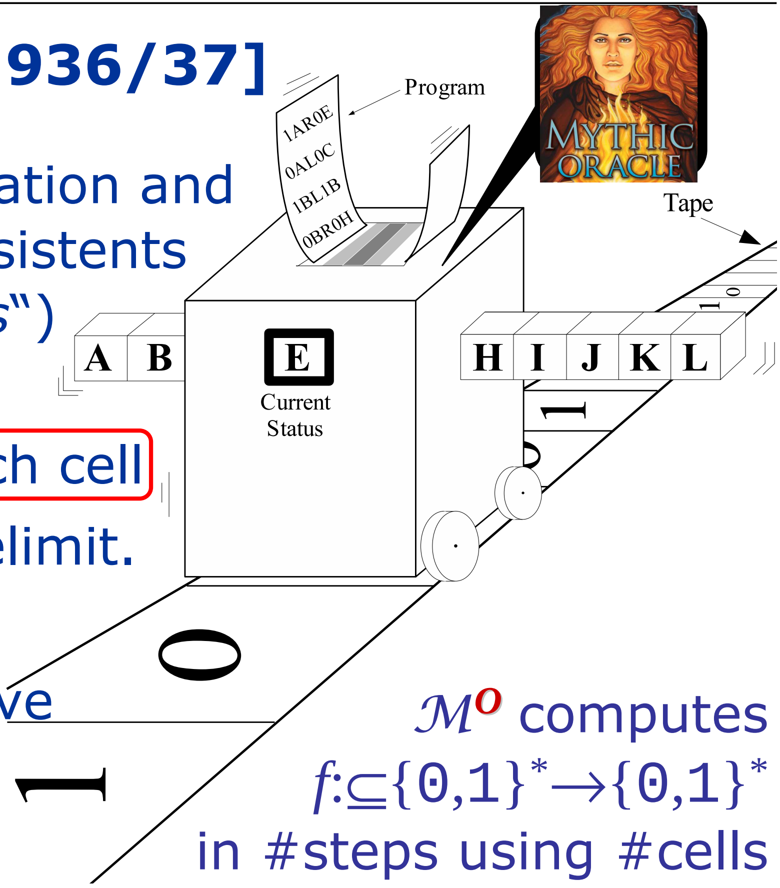
For $L, L' \subseteq \{0,1\}^*$ write $L \leqslant L'$ if there is a computable $f: \{0,1\}^* \to \{0,1\}^*$ such that $\forall \underline{x}: \ \underline{x} \in L \Leftrightarrow f(\underline{x}) \in L'$.
a) L' semi-/decidable $\Rightarrow$ so L. b) $L \leqslant L' \leqslant L'' \Rightarrow L \leqslant L''$

Bit Model: Turing Machine

Alan M. Turing [1936/37]

Mathematical idealization and abstraction of his assistents (profess. „*computers*")

- unbounded tape
- one bit (0/1) in each cell
- initially: input + delimit.
- finite program
- one read/write/move operation per step
- until stop: output.



$\mathcal{M}^{\mathcal{O}}$ computes $f{:\subseteq}\{0,1\}^*\to\{0,1\}^*$ in #steps using #cells

Bit Model: Turing Machine

KAIST
CS700 M. Ziegler

$\mathcal{M} = (Q,q_0,q_+,q_-,\delta)$, where Q is a finite set of states,

$\delta{:\subseteq}\{0,1\}\times Q\to\{L,R\}\times\{0,1\}\times Q$ transition table,

$q_0\in Q$ initial, $q_+\in Q$ accepting, $q_-\in Q$ rejecting state.

A configuration of $\mathcal{M}$ is a triple $(\underline{v},q,\underline{w})$, with $q\in Q$ and $\underline{v},\underline{w}\in\{0,1\}^*$. The initial configuration on input $\underline{w}$ is $(\ ,q_0,\underline{w})$. A successor configuration to $(\underline{v}, q, b\ \underline{w})$ is • $(\underline{v}\ b', p, \underline{w})$ for $\delta(b,q)=(R,b',p)$, • $\delta(b,q)=(L,b',p)$

Shoenfield's Limit Lemma: A partial $f{:\subseteq}\mathbb{N}\to\mathbb{N}$ is computable relative to H iff $f(n)=\lim_j g(n,j)$ for some total (oracle-free) computable $g{:}\mathbb{N}\times\mathbb{N}\to\mathbb{N}$.