COMP4141 Theory of Computation

Oracle machines & Turing Reducibility

Ron van der Meyden

CSE, UNSW

Revision: 2015/05/13

(Credits: K. Engelhardt, M Sipser, C Papadimitriou, R. van Glabbeek, P Hofner)

Definition

An *oracle* for a language B is an external device that is capable of deciding B.

An *oracle TM* is a modified TM $M^?$ that has the additional capability of querying an oracle.

If an oracle TM $M^?$ with an oracle for B decides A then we say that A is *decidable relative to* B.

Language A is *Turing reducible* to language B (or $A \leq_\mathsf{T} B$) if A is decidable relative to B.

$\leq_P$ vs $\leq_m$ vs $\leq_T$

$$A \leq_L B \quad \Rightarrow \quad A \leq_P B \quad \Rightarrow \quad A \leq_m B \quad \Rightarrow \quad A \leq_T B$$

As for the other two notions of reduction we have

Theorem

If $A \leq_T B$ and B is decidable, then A is decidable.

Corollary

If $A \leq_T B$ and A is undecidable, then B is undecidable.

but whereas $\leq_m$ also transferred r.e. this is not the case for $\leq_T$.

Example

Recall that A_{TM} is r.e. but $\overline{A_{TM}}$ isn't. But $A_{TM} \leq_T \overline{A_{TM}}$ and $\overline{A_{TM}} \leq_T A_{TM}$ by simply reversing the oracles' answers.

Definition

Let $\mathbf{P}^{O}$ be the class of languages decided by a polynomial-time oracle TM using oracle O. (Similar for $\mathbf{NP}^{O}$.)

Example

$\mathbf{NP} \subseteq \mathbf{P}^{SAT}$ and $\mathbf{coNP} \subseteq \mathbf{P}^{SAT}$.

Example

A formula of propositional logic ϕ is *minimal* if there does not exist a shorter formula ψ such that $\phi \Leftrightarrow \psi$ is valid (true for all assignments).

It is not known whether $\overline{\mathit{MIN\text{-}F}} \in \mathbf{NP}$ where

$$\mathit{MIN\text{-}F} = \{ \langle \phi \rangle \mid \phi \text{ is a minimal Boolean formula } \}$$

but $\overline{\mathit{MIN\text{-}F}} \in \mathbf{NP}^{\mathit{SAT}}$ as witnessed by the oracle NTM
$M^{?}$ = "On input $\langle \phi \rangle$

1. Non-deterministically guess a smaller formula ψ.
2. Ask the oracle whether $\langle \phi \Leftrightarrow \neg\psi \rangle \in \mathit{SAT}$ and if it accepts, *reject*; otherwise *accept*."

This problem is not known to be in NP, nor in co-NP.

$\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ and Diagonalisation

Any theorem proved about TMs by using only methods based on

I string representations of TMs

II simulation of one TM by another without much overhead in time/space

lifts to oracle machines.

That the resolution of $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ can not be such a theorem follows from:

Theorem (Baker, Gill, Solovay 1975)

Oracles A and B exist whereby $\mathbf{P}^A = \mathbf{NP}^A$ and $\mathbf{P}^B \neq \mathbf{NP}^B$.

Proof of $\exists A \left(\mathbf{P}^A = \mathbf{NP}^A\right)$

A could be QBF:

$$\begin{aligned}
\mathbf{NP}^{QBF} &\subseteq \mathbf{NPSPACE} && \text{by } QBF \in \mathbf{PSPACE} \\
&= \mathbf{PSPACE} && \text{by Savitch's theorem} \\
&\subseteq \mathbf{P}^{QBF} && QBF \text{ is } \mathbf{PSPACE}\text{-complete} \\
&\subseteq \mathbf{NP}^{QBF} && \text{by } \mathbf{P} \subseteq \mathbf{NP}
\end{aligned}$$

$\square$

Proof of $\exists B \left(\mathbf{P}^B \neq \mathbf{NP}^B\right)$

Iteratively construct a B (and its complement B') such that in the end $U_B \in \mathbf{NP}^B \setminus \mathbf{P}^B$ where

$$U_B = \{\, 1^n \mid \Sigma^n \cap B \neq \emptyset \,\} \quad .$$

That $U_B \in \mathbf{NP}^B$ is easy:

“On input 1^n guess $x \in \Sigma^n$ and *accept* iff the oracle confirms $x \in B$.”

Proof of $\exists B\,(\mathbf{P}^B \neq \mathbf{NP}^B)$ cont.

Initially, $B = B' = \emptyset$. For stage i of the construction, let $M_i^?$ be the i'th polynomial-time oracle TM running in w.l.o.g. in time n^i.

Let m exceed the length of all strings in $B \cup B'$ so far, and also $m^i < 2^m$.

We'll ensure that U_B and M_i^B disagree on 1^m.

1. Simulate $M_i^?$ on 1^m by answering queries x to the oracle with "yes" if $x \in B$, "no" if $x \in B'$, otherwise we also answer "no" and add x to B'.
2. If $M_i^?$ accepts 1^m then we put all strings of length m into B'; otherwise, we add the first string of length m neither in B nor in B' to B. Such a string exists because $M_i^?$ can have queried at most $m^i < 2^m$ strings of length m and none were queried ever before.

It follows that no M_i^B will decide U_B and thus $U_B \notin \mathbf{P}^B$. $\square$