Complexity Reading Group 11/12/2015

1 Oracles

Definition 1: An *Oracle Turing Machine* M has:

- Read/Write Tape (Oracle Tape)
- Special states (q_{query}, q_{yes}, q_{no})
- Need to specify the Oracle itself, O, that is, which language O decides.

Execution of M^O:

1. Move to state query
2. If $q \in O$, then next state is q_{yes}.
3. If $q \notin O$, then next state is q_{no}.

M^O is a complete machine, meaning it specifies a full computation.

Definition 2: An *Oracle Complexity Class* C:

$$C = \{L(M) \mid M \text{ is a } TM \text{ satisfying } P(M)\} \tag{1}$$

Where $P(\cdot)$ is an arbitrary complexity class.

$$C^O = \{L(M^O) \mid M^O \text{ is an Oracle } TM \text{ satisfying } P(M^O)\} \tag{2}$$

If C and D are complexity classes, then:

$$C^D = \cup_{o \in D} C^O \tag{3}$$

1.1 Examples

Recall the polynomial hierarchy:

$$\Sigma_{i+1}^P = NP^{QSAT_i} = NP^{\Sigma_i^P} = NP^{\Pi_i^P}$$
$$\Pi_{i+1}^P = (coNP)^{QSAT_i} = (coNP)^{\Sigma_i^P}$$

2 Relativization

Definition 3: An inclusion $C \subseteq D$ is said to relativize if:

$$\forall_O : C^O \subseteq D^O \tag{4}$$

The notion is also (informally) extended to proofs of inclusions.

2.1 Some properties

1. True or False: $C = D \rightarrow \forall_A C^A = D^A$. [**False**]
2. True or False: $C \neq D \rightarrow \forall_A C^A \neq D^A$. [**False**]
3. Some properties:
   - $C \subseteq C^O$
   - $P^O \subset NP^O$
4. $D = PH$, then $P^D = NP^D$
5. Choose a random oracle O s.t. $P(x \in O) = \frac{1}{2}$, what is the probability that $P^O \subset$ *Recursive*? Since there are uncountably many undecidable languages and only countably many decidable languages, with probability 1 we get an oracle that decides an undecidable language, so with probability O $P^O \subseteq$ *Recursive*.

3 Relativization Barrier

Theorem 1 (Baker Gill Solvoy): There are oracles A, B, s.t. $P^A = NP^A$, but $P^B \neq NP^B$

Proof:

$\boxed{\text{Part A:}}$ $A = EC : \{(M, x, 1^n) \mid M(x) = 1 \text{ in } 2^n \text{ steps}\}$ (note: n is an arbitrary parameter).

Therefore $EXP \subseteq P^A$, since you can fix n to be whatever. So $NP^A \subseteq EXP$.

Therefore $P^A = NP^A$. $\square$

$\boxed{\text{Part B:}}$ Given an artbitrary B, we know for $U_B = \{1^n \mid \exists x \in B : |X| = n\}$, $U_B \in NP^B$

Now we want B s.t. $U_B \notin P^B$.

<u>Diagonlization Argument</u>

$\{M_i\} : OTM$.

Sort of an inductive gig on i. At the 'previous' stage we have determined a finite set of strings $\{x\}$ of whether $x \in B$ or not.

For step i: run M_i with input 1^{n_i}, where $n_i > |x| \forall_x$: s.t. x is determined, for $\frac{2^n}{10}$ steps.

Query: (q)

- If q is determined before, answer consistently.
- If q is new, answer false.

After this execution, we get some result:

- If $M_i(1^{n_i}) = 1$, then $x \notin B, \forall_x : |x| = n_i$
- If $M_i(1^{n_i}) = 0$, then choose some unqueried $x : |x| = n$ and make $x \in B$.

$\therefore$ We know that $U_B \notin DTIME^B(\frac{2^n}{10})$

$\therefore U_B \notin P^B$ □

4 Other Results

Proposition: Draw a random oracle O s.t. for all n, $P($ no $|x| = n \in O) = 1/2$, $P(a$ uniformly random $x \in O) = 1/2$.

With probability 1 $P^O \neq NP^O$.

Theorem 2 (Bennett and Gill): Draw a random oracle O s.t. $Pr(x \in O) = \frac{1}{2}$. With probability 1, $P^O \neq NP^O$.

(False) Hypothesis 1 (Random Oracle Hypothesis): Let S be a complexity theoretic statement. Then S is true iff, with probability 1, S^A is also true, where A is draw as above ($Pr(x \in O) = \frac{1}{2}$).

Note: The above was disproven!

Theorem 3 (Chang et. al. 1994): With probability 1, $IP^A \neq PSPACE^A$