Simple Use of Oracles

CIS 622, Computational Complexity

An oracle is a set of strings to which we have instant access during a computation. That is, if we are using the set B as an oracle, then we get to ask questions of the form \( y \in B \) during a computation. We receive an answer yes/no in one step. This computation is said to be relative to B.

For example, consider the following deterministic algorithm for TAUT using oracle SAT:

```
input: formula F
if ( (not F) is in SAT )
    then REJECT
else ACCEPT
```

This shows that \( TAUT \in P^{SAT} \). In words, \( TAUT \) can be computed in (deterministic) polynomial time relative to \( SAT \). (By the way, this also shows that \( TAUT \leq_P SAT \).

If C is a complexity class, we say that \( P^C = \bigcup_{B \in C} P^B \). Thus, \( TAUT \in P^{NP} \).

Looking ahead, we define \( \Delta_2^P = P^{NP} \) and \( \Sigma_2^P = NP^{NP} \).

In class, we were starting to look at \( P^{NP\cap\text{coNP}} \), with the goal of showing that \( P^{NP\cap\text{coNP}} \subseteq \text{NP} \). So let \( A \in P^B \), where \( B \in \text{NP} \cap \text{coNP} \). Thus, there is a poly-time DTM \( M \) accepting \( A \) which operates relative to \( B \). There are also poly-time NDTMs \( M_0 \) accepting \( \overline{B} \) and \( M_1 \) accepting \( B \).

The following nondeterministic algorithm (with no oracle) will accept \( A \):

```
input: x
Simulate M on x.
When a query of the form "y in B" is made
    Non-deterministically guess the answer Y or N to "y in B"
    If the answer guessed was Y
        then simulate M_1 on y
            if M_1 reaches accepting state
                then return to simulation of M on x with answer Y
            if M_1 reaches rejecting state
                then halt and REJECT
    If the answer guessed was N
```

1
then simulate $M_0$ on $y$
  if $M_0$ reaches accepting state
    then return to simulation of $M$ on $x$ with answer $N$
  if $M_0$ reaches rejecting state
    then halt and REJECT

When the simulation of $M$ on $x$ halts, if $M$ accepts
  then ACCEPT
else REJECT

Note that both $P$ and $P^C$ are closed under complementation. Thus, $P^{NP\cap coNP} \subseteq NP$ implies $P^{NP\cap coNP} \subseteq coNP$. Therefore, $P^{NP\cap coNP} \subseteq NP \cap coNP$.

Trivially $NP \cap coNP \subseteq P^{NP\cap coNP}$. So we have shown that

$$P^{NP\cap coNP} = NP \cap coNP.$$