Reductions
CIS 621 and the ex-622

There are many reductions - we will mention three which are polynomial time, and one that is below polynomial time.

**Definition 1** A set $A$ polynomial time Turing reduces to a set $B$, denoted $A \leq_{PT}^P B$, if $A \in P^B$. That is, if $A$ can be computed in polynomial time with an oracle for $B$.

**Definition 2** A set $A$ is polynomial time truth-table reducible to $B$, denoted $A \leq_{Ptt}^P B$ if, on input $x$, the following can be computed in time polynomial in $|x|$:  

- strings $y_1, y_2, \ldots, y_k$
- a predicate $R_x$ with arity $k$

with the property that $x \in A$ iff $R_x(y_1 \in B, y_2 \in B, \ldots, y_k \in B)$.

**Definition 3** A set $A$ is polynomial time many-one reducible to $B$, denoted $A \leq_{Pm}^P B$, if there is a polynomial time transducer $f$ such that for all $x$, 

$$x \in A \iff f(x) \in B.$$ 

The first is sometimes called a “Cook reduction” and the last a “Karp reduction”. This is because the original paper by Cook showing that SAT is NP-complete used $\leq_{PT}^P$, while a subsequent influential paper by Karp used $\leq_{Pm}^P$. The latter is the most common.

The following is quite easy to see.

**Fact** If $A \leq_{Pm}^P B$, then $A \leq_{Ptt}^P B$. If $A \leq_{Ptt}^P B$, then $A \leq_{PT}^P B$.

**Definition** A class $C$ is closed under a reduction $\leq$ if 

$$A \leq B \land B \in C \implies A \in C.$$ 

**Closure Theorem** $NP$ is closed under $\leq_{Pm}^P$. $P$ and $PSPACE$ are closed under $\leq_{Pm}^P$, $\leq_{Ptt}^P$, and $\leq_{PT}^P$.

**proof:** exercise?

**Transitivity Theorem** If $A \leq_{Pm}^P B$ and $B \leq_{Pm}^P C$, then $A \leq_{Pm}^P C$. The reductions $\leq_{Ptt}^P$ and $\leq_{PT}^P$ are also transitive.

**proof:** Let $A \leq_{Pm}^P B$ and $B \leq_{Pm}^P C$. By the definition, there are transducers $f$ and $g$, computable in time $p_f$ and $p_g$ respectively, such that $x \in A \iff f(x) \in B$ and $y \in B \iff g(y) \in C$. Clearly, then 

$$x \in A \iff g(f(x)) \in C.$$
Note that $|f(x)| \leq pf(|x|)$, so the time to compute $g(f(x))$ is bounded by $pf(|x|) + pg(pf(|x|))$. □

**Definition** Given a reduction $\leq$ and class $C$, a set $B$ is $\leq$-hard for $C$ if, for all $A \in C$, $A \leq B$. The set $B$ is $\leq$-complete for $C$ if $B$ is $\leq$-hard for $C$ and $B \in C$.

From this point on, let us only refer to reductions that are transitive and to classes that are closed under the reduction.

**Fact** If $B$ is $\leq$-hard for $C$ and $B \leq C$, then $C$ is $\leq$-hard for $C$.

**Fact** If $B$ is $\leq$-hard for $C$ and $B \in D$, where $D$ is closed under $\leq$, then $C \subseteq D$.

The first fact is useful in showing complete sets, and the second is why complete sets are interesting. Especially interesting is a consequence of the second fact:

**Fact** If $B$ is $\leq^P_m$-complete for $NP$ and $B \in P$, then $P = NP$. If $B$ is $\leq^P_m$-complete for $NP$ and $B \in coNP$, then $NP = coNP$.

It is not at all hard to create an $NP$-complete set. (However, it is very hard to show a natural complete set.) Let $M_1, M_2, \ldots$ be an enumeration of the NDTMs. It is easy to see (exercise) that the following set is $\leq^P_m$-complete for $NP$

$$\{ \langle i, x, 0^m \rangle | M_i \text{ accepts } x \text{ within } m \text{ steps} \}.$$  

Notice that the reductions above do not discriminate well within $P$:

**Fact** Let $B$ be any set. Then $B$ is $\leq^P_T$ complete for $P$. If $B \neq \{0,1\}^*$ and $B \neq \emptyset$, then $B$ is $\leq^P_m$ complete for $P$.

Therefore, we need a reduction more appropriate to $P$ - the standard one being the “log-space many-one” reduction, denoted $\leq^{log}_m$.

**Definition** $A \leq^{log}_m B$ if there is a function $f : \Sigma_A^* \rightarrow \Sigma_B^*$ such that

1. $\forall x \in \Sigma_A^*, x \in A \iff f(x) \in B$.

2. $f$ can be computed in log-space (by a machine with a read-only input tape and write-only output tape, not subject to the space bound).

**exercise** Show that $\leq^{log}_m$ is transitive.

Later, we will see a complete problem for $P$:

**Theorem** The circuit evaluation problem is $\leq^{log}_m$-complete for $P$. 

2