

Every NPC language is Self Reducible

Chris Calabro

May 10, 2004

A *relation* (not a language, contrary to the title) $R \subseteq (\Sigma^*)^2$ is poly-time *self reducible* iff \exists poly-time Turing machine M such that

$$\forall x \in L = \text{dom } R \quad (x, M^L(x)) \in R.$$

If L is NPC, then there is a poly-time (in its first input) Turing machine V deciding a relation R such that $L = \text{dom } R$. We now show that R is self reducible.

First construct the auxiliary relation

$$R' = \{((x, \alpha), w) \mid (x, \alpha w) \in R\}.$$

Then $L' = \text{dom } R' \in \text{NP}$ and so $L' \leq_p L$. So \exists poly-time $f : \Sigma^* \rightarrow \Sigma^*$ such that

$$\forall x \in \Sigma^* \quad (x \in L' \leftrightarrow f(x) \in L).$$

The following machine, given oracle access to L , can find a witness for a given $x \in L$ in poly-time, thus showing that R is self reducible.

```
 $M^L(x)\{$   
  if  $x \notin L$   
    return 'not in  $L$ '  
   $w \leftarrow \epsilon$   
  while  $\neg V(x, w)$   
    if  $f(x, w0) \in L$   
       $w \leftarrow w0$   
    else  
       $w \leftarrow w1$   
  return  $w$   
}
```

This is not necessarily a *downward* self reduction since we may be reducing the problem instance x to a more complex problem instance after f is applied.