Introduction to Complexity Theory*
Corrections and Additions

Oded Goldreich

August 13, 2000

Following is a list of major corrections and additions to the lecture notes. Currently the list contains a single item.

1 PP versus $\#P$

The class PP as defined in Lecture 7 (cf., Def. 7.6), is computationally equivalent to the class $\#P$ as defined in Lecture 10 (cf., Def. 10.4) in the sense that each class is Cook-reducible to the other. Recall that the class PP was referred to in Lecture 7 as a probabilistic complexity class that allows "useless" algorithms (i.e., the difference in their behavior, on YES and NO-instances, may be negligible). What we forgot to mention is that PP is strongly related (as stated above) to the counting (complexity) class $\#P$.

Theorem 1 (computational equivalence of PP and $\#P$)

1. *PP is Cook-reducible to $\#P$.*
2. *$\#P$ is Cook-reducible to PP.*

Proof: Let $L \in PP$ and suppose that M is a probabilistic polynomial-time machine witnessing this fact as in Definition 7.6. For a suitable NP-relation, denoted R, and a suitable polynomial p, it follows that $\Pr[M(x)=1] = 2^{-p(|x|)} \cdot f_R(x)$, where $f_R(x) \stackrel{\rm def}{=} |\{y \in \{0,1\}^{p(|x|)} : (x,y) \in R\}|$ (as in Definition 10.3). Thus, $x \in L$ if and only if $f_R(x) > \frac{1}{2} \cdot 2^{p(|x|)}$. It follows that L is decidable by a polynomial-time machine with oracle access to f_R; that is, L is Cook-reducible to $\#P$.

On the other hand, for some NP-relation R, consider the function f_R in $\#P$. It suffices to show that the language $\#_R = \{(x,k) : k \leq f_R(x)\}$ (as in Definition 10.6) is Cook-reducible to PP. Letting p be an adequate polynomial so that $(x,y) \in R$ implies $|y| = p(|x|)$, we define a relation R' as follows:

$$R' \stackrel{\rm def}{=} \{((x,k),(1,y)) : (x,y) \in R\} \bigcup \left\{((x,k),(0,m)) : m \in \{1,...,2^{p(|x|)} - k\}\right\}$$

Consider a machine M' that on input (x,k), uniformly selects $z \in \{0,1\}^{p(|x|)+1}$, and accepts if and only if $((x,k),z) \in R'$. Note that if $(x,k) \in \#_R$ then $\Pr[M'(x,k)=1] \geq \frac{k+(2^{p(|x|)}-k)}{2^{p(|x|)+1}} = \frac{1}{2}$, whereas if $(x,k) \notin \#_R$ then $\Pr[M'(x,k)=1] < \frac{k+(2^{p(|x|)}-k)}{2^{p(|x|)+1}} = \frac{1}{2}$. By a minor modification (as in the proof of Fact 7.4.1), it follows that $\#_R$ is in PP. ■

---

* Lecture Notes for a course given in 1998 at the Weizmann Institute of Science, Israel.

Toda's Theorem: In Lecture 7, we showed that NP is contained in PP. It turns out that the entire Polynomial-Time Hierarchy (as defined in Lecture 9) is Cook-reducible to PP (or, equivalently, to $\#P$). The latter statement was proved by Toda [1].

Bibliographic Notes

1. S. Toda. On the computational power of PP and $\oplus$P. In *30th FOCS*, pages 514–519, 1989.