Computational Complexity

Handout – Lecture 10

Definition 1 (val(φ)). Let φ be a propositional formula in CNF. Then val(φ) is the maximum ratio of clauses of φ that can be satisfied simultaneously by any truth assignment.

Thus, if φ is satisfiable, then $\text{val}(\varphi) = 1$, and if φ is not satisfiable, then $\text{val}(\varphi) < 1$.

Definition 2 (PCP verifier). Let $L \subseteq \{0,1\}^*$ be a language and let $q, r : \mathbb{N} \to \mathbb{N}$ be functions. We say that L has an $(r(n), q(n))$-PCP verifier if there is a polynomial-time probabilistic algorithm V that satisfies:

- *(Efficiency)* When given as input a string $x \in \{0,1\}^n$ and when given random access to a string $\pi \in \{0,1\}^*$ of length at most $q(n)2^{r(n)}$ (which we call the *proof*), V uses at most $r(n)$ random coin flips and makes at most $q(n)$ nonadaptive queries to locations of π.
  - Random access: V can query an oracle that gives the i-th bit of π.
  - Nonadaptive queries: the queries do not depend on the answers for previous queries.
- V always outputs either 0 or 1.
- *(Completeness)* If $x \in L$, then there exists a proof $\pi \in \{0,1\}^*$ of length at most $q(n)2^{r(n)}$ such that $\Pr[V^\pi(x) = 1] = 1$. This string is called the *correct proof* for x.
- *(Soundness)* If $x \notin L$, then for every proof $\pi \in \{0,1\}^*$ of length at most $q(n)2^{r(n)}$, it holds that $\Pr[V^\pi(x) = 1] \leq 1/2$.

Definition 3 (PCP($r(n), q(n)$)). Let $q, r : \mathbb{N} \to \mathbb{N}$ be functions. The class PCP($r(n), q(n)$) consists of all languages $L \subseteq \{0,1\}^*$ for which there exist constants $c, d > 0$ such that L has a $(c \cdot r(n), d \cdot q(n))$-PCP verifier.