Math 261C: Randomized Algorithms

Lecture topic: PCP Theorem, Introduction

Lecturer: Sam Buss
Scribe notes by: Udbhav Singh
Date: June 2, 2014

The lecture will follow the paper by Irit Dinur [1].

1. Preliminary Definitions

Definition 1 (NP-completeness)**.** *A language L is NP-complete under many-one reduction if for any language in NP there is a polynomial time many-one reduction to L. Examples include SAT, 3-SAT, 3-colorability.*

The 3-colorability problem is defined by the following input, output structure
Input: A graph G
Output: "Yes" iff the vertices of G can be assigned one of three colors such that no two vertices of any edge get the same color.

2. PCP Theorem

We present the prosaic form of the PCP version first.

Definition 2. *Let ϕ be an instance of SAT. For τ a truth assignment, we define $UNSAT_\tau(\phi)$ = fraction of ϕ's clauses false under τ. We define $UNSAT(\phi) = \min_\tau UNSAT_\tau(\phi)$.*

Theorem 1 (PCP Version 1: Prosaic Form)**.** *There is a constant $\delta < 1$ and $k \geq 3$ (in fact $k = 3$ works too) such that if L satisfies the following conditions then L is NP-complete.*

1. *If ϕ is an instance of $k-SAT$ and if ϕ is satisfiable, then $\phi \in L$.*
2. *If ϕ is an instance of k-SAT and ϕ is unsatisfiable, then $UNSAT(\phi) \geq \delta \implies \phi \in L$.*

Loosely speaking, this implies that approximating the number of ϕ's clauses that can be simultaneously satisfied is NP hard.

Definition 3. *A language L is in $PCP(r(n), q(n))$, iff*

1. *there is a polynomial time verifier* $V = V(x, \pi)$ *which choses* $\leq r(n)$ *bits at random, examines only* $q(n)$ *bits of* π *and either accepts or rejects.*
2. *"Completeness": For* $x \in L, \exists \pi$ *s.t.* $\mathbf{Pr}[V(x, \pi)$ *accepts*$] = 1$.
   "Soundness": For $x \notin L, \forall \pi, \mathbf{Pr}[V(x, \pi)$ *accepts*$] \leq 1/2$

Theorem 2 (PCP Version 2)**.** $SAT \subseteq PCP(O(\log n), O(1))$

This version of the PCP theorem, justifies the name Probabilistically Checkable Proofs.

The proof π is supplied by the Prover. The verifier V choses some $O(\log n)$ random bits and accepts/rejects by seeing $O(1)$ bits of π.

Without loss of generality, it can be assumed that π has at most $q(n)2^{r(n)}$ many bits. In particular, for PCP, $|\pi| = n^{O(1)}$. In this lecture, we will prove the equivalence of the two versions of the PCP theorem. The actual proof of the PCP theorem will be presented in the subsequent lectures.

3. Equivalence of versions of PCP

Theorem 3. *The two versions of the PCP theorem are equivalent*

Proof. **Case 1: Version 1 implies Version 2.**

Suppose SAT is many-one polynomial-time reducible to any language L of version 1. Then we have a poly time function $f(x)$ such that $\forall x \in \{0,1\}^*$, if $x \in SAT$, then $f(x) \in SAT$), if $x \notin SAT$, then $UNSAT(f(x)) \geq \delta$. The PCP protocol for SAT is as follows. □

Input: x
Output: Decide if $x \in SAT$
Algorithm:
Step 1: Compute $\phi = f(x)$
Step 2: Repeat N times:
    Choose a clause of ϕ at random.
    For each literal x_j inϕ
        look up its value as j^{th} bit of π.
        If clause is not satisfied, Reject
Step 3: Accept

Algorithm 1: PCP protocol for SAT

N is chosen large enough so that $(1 - \delta)^N < 1/2$.

This shows that $SAT \subseteq PCP(O(\log n), O(1))$ which implies that $NP \subseteq PCP(O(\log n), O(1))$.

Case 2: Version 2 implies Version 1.

Assume SAT has a $PCP(c_1 \log n, c_2)$ protocol V where c_1, c_2 are constants.

We want to form a many-one reduction $f(x)$.

The reduction $f(x)$ works as follows.

1. For each choice r of the $c_1 \log n$ random bits (there are $2^{c_1 \log n} = n^{O(1)}$ many r's): Run $V(x, \pi, r)$ which examines c_2 of the bits of π. Form an instance of SAT, ϕ_r where
   (a) Variables of ϕ_r are bits of π examined.
   (b) Values of ϕ_r is true iff $V(x, \pi, r)$ accepts.

   (Size of ϕ_r is $O(1)$).
2. Let $f(x) = \bigwedge \phi_r$ (ϕ_r's are CNF formulas).
   Since this was a PCP reduction, either there is a π that satisfies all ϕ_r's or every π has at least fraction $1/2$ of the ϕ_r's false. If each ϕ_r has $\leq k$ ($k = k(c_2)$), then $UNSAT(f(x)) \geq \frac{1}{k}\frac{1}{2}$. We can then take $\delta = 1/2k$.

This completes the proof.

References

[1] Irit Dinur *The PCP Theorem by Gap Amplification*, J. ACM 54, 3, June 2007,Issue No. 0004-5411, Article 12 doi = 10.1145/1236457.1236459 http://doi.acm.org/10.1145/1236457.1236459