Hardness of Approximation

Thodoris Lykouris

National Technical University of Athens

February 7, 2012

Contents

Characterization of NP

Hardness of approximation

NP prover-verifier

For every language $L \in NP$, there is a prover P and a polynomial verifier V such that the verifier reads:

- an input x
- a proof y

satisfying the following

- Completeness: If $x \in L$ then P produces a proof y that $V^y(x)$ always accepts
- Soundness: If $x \notin L$, $V^y(x)$ rejects every proof

$PCP_{c(n),s(n)}[p(n), q(n)]$ (Arora-Safra 92)

A language $L \in PCP_{c(n),s(n)}[p(n), q(n)]$, there exists a prover P and a polynomial verifier V such that the verifier the verifier reads:

- an input x of length n
- a random input r of length $p(n)$
- randomly chosen $q(n)$ bit from a proof y

satisfying the following

- Completeness: If $x \in L$ then P produces a proof y that $V^y(x)$ accepts with probability $\geq c(n)$.
- Soundness: If $x \notin L$, $V^y(x)$ rejects the proof with probability $< s(n)$.

$PCP[O(logn), O((1))]$

A language $L \in PCP[O(logn, O(1)]$, there exists a prover P and a polynomial verifier V such that the verifier the verifier reads:

- an input x of length n
- a random input r of length $clogn$
- randomly chosen k bit from a proof y

satisfying the following

- Completeness: If $x \in L$ then P produces a proof y that $V^y(x)$ accepts with probability 1.
- Soundness: If $x \notin L$, $V^y(x)$ rejects the proof with probability $< \frac{1}{2}$.

PCP Theorem (Arora,Lund, Motwani, Sudan, Szegedy 92)

PCP Theorem

$$NP = PCP[O(logn), O(1)]$$

Let's flip the coin

The coin

For every language $L \in NP$ there is always a way to write proofs such that for every instance x:

- If $x \in L$ then there is a correct proof
- If $x \notin L$ then every proof has a lot of errors

Two sides of the coin

- PCP theorem
- Hardness of approximation

Contents

Characterization of NP

Hardness of approximation

Approximability of NP-hard problems

Decision problem

NP-hard

Optimization problem

- no approximation
- $O(poly(n))$-approximation
- $O(logn)$-approximation
- $O(1)$-approximation
- PTAS-FPTAS,$(1+\epsilon)$-approximation

Approximability of Max SAT

Theorem

The PCP Theorem implies that there is an $\epsilon_1 > 0$ *such that there is no polynomial time* $(1 + \epsilon_1)$*-approximate algorithm for MAX-3SAT, unless* $P = NP$.

Proof: The reduction

- We check for any random string r and any input x: 2^k different possible bits on the proof
- Hence, the verifier is a boolean function $f_r^x = C_{r,1} \wedge C_{r,2} \cdots \wedge C_{r,2^k}$
- Each of these clause has k litterals: replaced by $(k-2)$ clauses with 3 litterals.

The proof: No PTAS for the MAX 3SAT

- At least half of the random inputs reject the proof (at least one of their clauses is unsatisfied) due to Soundness
- Size of random input: $clogn$
- Number of random inputs: $2^{clogn} = n^c$
- At least $\frac{n^c}{2}$ clauses unsatisfied.
- Total number of clauses: $(k-2)2^k n^c$
- At least $\frac{n^c/2}{(k-2)2^k n^c} = \frac{1}{(k-2)2^{k+1}}$ unsatisfied.
- Unless P=NP, no better approximation than $1 - \frac{1}{(k-2)2^{k+1}}$-approx.

Tight inapproximability for MAX-3SAT

Theorem (Hastad 01)

For every $\epsilon > 0$, $NP = PCP_{1-\epsilon,1/2+\epsilon}[O(\log n), 3]$. *Furthermore the verifier behaves as follows: it uses randomness to pick three entries* i, j, k *in the witness and a bit* b*, and it accepts iff* $w_i \oplus w_j \oplus w_k = b$.

- Hence, 4 clauses instead of $(k-2)2^k$ for every random string.
- Unless P=NP, no better approximation than $(1 - \frac{1}{4\times 2)-} = \frac{7}{8} - \delta$-approx, for every δ.

Approximability of Independent Set

Theorem

There is a constant $c > 1$ such that if there is a polynomial time n^c-approximate algorithm for Independent Set then $P = NP$

Reduction

- For every random string and different possible bits on the proof, we create a node
- All the nodes of the same random string have an edge between them
- All the nodes that refer to the same bit but have different "'opinion"' for the bit have an edge between them

Inapproximability of Independent Set

- If $x \in L$, then there exists an independent set of size n^c.
- If $x \notin L$, from soundness at most half of the random string can have compatible "'opinions"' for the same bits: $\frac{n^c}{2}$
- PCP one-side error: There exists some constant t s.t. no better than n^t-approximation

More inapproximability results

- TSP : no-approximation
- Univeral scheduling: $3/2-\epsilon$
- Disjoint paths: $m^{-1/2+\epsilon}$
- Steiner Tree: no-approximation scheme
- UFL: 1.463
- Set Cover: $c \log n$
- Max-E3SAT: $7/8+\epsilon$
- Independent Set: no $n^{-1+\epsilon}$