COS 522: Complexity Theory : Boaz Barak
Handout 8: PCP Theorem I: Outline and Alphabet Reduction

Reading: Chapter 18

Two views of the PCP Theorem:

Approximation Algorithms	**Probabilistically Checkable Proofs**
Def: A ρ-approximates $\mathsf{3SAT}$ if for every 3CNF φ, $A(\varphi)$ is an assignment satisfying a $\rho\mathsf{val}(\varphi)$ fraction of φ's clauses.	**Def:** $L \in \mathbf{PCP}(r,q)$ if there's a random-access verifier with r random bits and q queries satisfying **Completeness:** $x \in L \implies \exists\pi \Pr[V^\pi(x)=1]=1$ and **Soundness:** $x \notin L \implies \forall\pi \Pr[V^\pi(x)=1] \leq 1/2$.
Thm 1: If $\exists$ ptime 0.999 approx alg for $\mathsf{3SAT}$ then $\mathbf{P}=\mathbf{NP}$. In fact, $\exists$ ptime R such that **(1)** $\varphi \in \mathsf{3SAT} \implies \mathsf{val}(R(\varphi))=1$ **(2)** $\varphi \notin \mathsf{3SAT} \implies \mathsf{val}(R(\varphi))<0.999$.	**Thm 2:** $\mathbf{NP} \subseteq \mathbf{PCP}(O(\log n), 100)$

Can change 0.999 to $7/8+\epsilon$ and 100 to 3 by a slight relaxation of completeness (1 changes to $1-\epsilon$) and soundness (1/2 changes to $1/2+\epsilon$).

Equivalence of two views: Definition of CSP, ρ-$\mathsf{GAP}\,q\mathsf{CSP}$.

Thm 3: $\exists q$ ρ-$\mathsf{GAP}\,q\mathsf{CSP}$ is $\mathbf{NP}$-hard.

Thm 1 $\implies$ Thm 2 $\implies$ Thm 3 $\implies$ Thm 1.

Summary of notations:

Approx view		PCP view
CSP instance (φ)	$\longleftrightarrow$	**PCP** verifier (V)
Assignment to variables ($\mathbf{u}$)	$\longleftrightarrow$	**PCP** proof (π)
Number of variables (n)	$\longleftrightarrow$	Length of proof
Arity of constraints (q)	$\longleftrightarrow$	Number of queries (q)
Logarithm of number of constraints ($\log m$)	$\longleftrightarrow$	Number of random bits (r)
Maximum of $\mathsf{val}(\varphi)$ for a NO instance	$\longleftrightarrow$	Soundness parameter
Thms 2,3 (ρ-$\mathsf{GAP}\,q\mathsf{CSP}$ is $\mathbf{NP}$-hard)	$\longleftrightarrow$	Thm 1 ($\mathbf{NP} \subseteq \mathbf{PCP}(\log n, O(1))$)

Hardness of approximation for independent set

$\mathbf{NP} \subseteq \mathbf{PCP}(poly(n), 1)$ Exponential-sized PCP for quadratic equations.

Outline of proof of PCP Theorem

CSP problems with larger alphabet

Main Lemma: Def of CL Reductions.

	Arity	Alphabet	Constraints	Value
Original	q_0	binary	m	$1-\epsilon$
	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
Main Lemma	q_0	binary	Cm	$1-2\epsilon$

Gap amplification and Alphabet Reduction Lemmas

	Arity	Alphabet	Constraints	Value
Original	q_0	binary	m	$1-\epsilon$
	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
Gap Amplification	2	W	Cm	$1-6\epsilon$
	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
Alphabet Reduction	q_0	binary	$C'Cm$	$1-2\epsilon$

Proof of Alphabet Reduction

Homework Assignments

§1 (30 points) Using the PCP Theorem as a black-box, show that for every constant $\rho > 0$, the independent set problem is hard to approximate within a factor of ρ *without* using expander graphs.

§2 (30 points) Exercise 18.15 (10ϵ there should be changed to 10δ)

§3 (50 points) Exercise 18.16