CS286.2 Lecture 4: Dinur's Proof of the PCP Theorem

Scribe: Thom Bohdanowicz

Previously, we have proven a weak version of the PCP theorem: NP $\subseteq$ PCP$_{1,1/2}(r = \text{poly}, q = O(1))$. With this result we have the desired constant completeness and soundness, but the proof is exponentially long. It takes difficult work to shorten the proof to get the full PCP theorem: NP $\subseteq$ PCP$_{1,1/2}(r = O(\log n), q = O(1))$.

Now we will see a different approach to the proof of the PCP theorem which was recently discovered (2006) by Irit Dinur. The approach here will be to take a result with a small soundness gap, NP $\subseteq$ PCP$_{1,1-\frac{1}{m}}(r = O(\log n), q = O(1))$, and gradually amplify the soundness to get the desired gap while keeping the length of the proof constant.

The proof can be understood using the CSP variant of the PCP theorem:

Theorem 1. *For any $L \in$ NP there is a polynomial-time mapping $x \in \{0,1\}^* \mapsto \varphi_x$ where φ_x is a q-CSP over $m = \text{poly}(n)$ clauses, $q \in O(1)$, such that:*

- $x \in L \implies \omega(\varphi_x) = 1$
- $x \notin L \implies \omega(\varphi_x) \leq 1/2$

The main Lemma facilitating Dinur's proof is the following:

Lemma 2. *There exists an efficient polynomial-time procedure mapping a 2-CSP $\varphi = \varphi^{(i)}$ to 2-CSP $\varphi' = \varphi^{(i+1)}$ as follows*

- $\varphi = \varphi^{(i)}$ *over* $\Sigma = \{0,1\} \implies \varphi' = \varphi^{(i+1)}$ *over* $\Sigma = \{0,1\}$
- $\varphi^{(i)}$ *has m constraints* $\implies \varphi^{(i+1)}$ *has $m' \leq Cm$ constraints where C is some universal constant*
- $\omega(\varphi^{(i)}) = 1 \implies \omega(\varphi^{(i+1)}) = 1$
- $\omega(\varphi^{(i)}) \leq 1 - \epsilon \implies \omega(\varphi^{(i+1)}) \leq 1 - 2\epsilon$

To see why this lemma implies the PCP theorem, here's the idea: take some NP-complete language like $3-$COLORING. By definition it is NP-hard to decide for the corresponding 2-CSP $\varphi^{(0)}$ whether $\omega(\varphi^{(0)}) = 1$ or $\omega(\varphi^{(0)}) \leq 1 - \frac{1}{m}$, where m is the number of constraints (which in the case of $3-$COLORING is the number of edges in the graph). Applying the above Lemma once brings us from $\{\omega(\varphi^{(0)}) = 1 \; or \; \omega(\varphi^{(0)}) \leq 1 - \frac{1}{m}\}$ to $\{\omega(\varphi^{(1)}) = 1 \; or \; \omega(\varphi^{(1)}) \leq 1 - \frac{2}{m}\}$, and so applying it t times brings us to $\{\omega(\varphi^{(t)}) = 1 \text{ } or \text{ } \omega(\varphi^{(t)}) \leq 1 - \frac{2^t}{m}\}$. Setting $t \sim \log m$, we're done, noting that $|\varphi^{(t)}| \leq C^t m \sim m^{\log_2 C+1}$ remains polynomial in the size of the original instance $\varphi^{(0)}$.

The proof of the Lemma has two main steps: gap amplification (GA) and alphabet reduction (AR). These steps operate as follows on our original 2-CSP instance:

- CSP: $\varphi = \varphi^{(i)}$ a 2-CSP $\mapsto_{GA}$ $\varphi' = \varphi^{(i)'}$ a 2-CSP $\mapsto_{AR}$ $\varphi'' = \varphi^{(i+1)}$ a 2-CSP
- Clauses: $m \mapsto_{GA} m' \leq Cm \mapsto_{AR} m'' \leq C'm'$
- Alphabet: $\Sigma = \{0,1\} \mapsto_{GA} \Sigma' = [w] = \{0,1,...,w-1\}$ where w is some larger integer $\mapsto_{AR} \Sigma'' = \{0,1\}$
- Completeness: $\omega(\varphi = \varphi^{(i)}) = 1 \mapsto_{GA} \omega(\varphi' = \varphi^{(i)'}) = 1 \mapsto_{AR} \omega(\varphi'' = \varphi^{(i+1)}) = 1$
- Soundness: $\omega(\varphi = \varphi^{(i)}) \leq 1 - \epsilon \mapsto_{GA} \omega(\varphi' = \varphi^{(i)'}) \leq 1 - 6\epsilon \mapsto_{AR} \omega(\varphi'' = \varphi^{(i+1)}) \leq 1 - 2\epsilon$

As noted above, repeating these steps $O(\log m)$ times gives a constant gap with only a polynomial blow-up in the number of constraints (since all clauses involve a constant number of variables, the same automatically holds for the number of variables). The harder part is constructing the gap amplification procedure, so that's what we will look at in this lecture. It requires the use of *expander graphs.*

Expander Graphs

An expander graph is a graph $G = (V, E)$ which has good 'expansion' properties. A loose definition would be that there is never a small subset of vertices that has a lot of edges 'inside', but connecting the subset to the rest of the graph with only a few edges. We focus on n-vertex d-regular graphs, and give the following definition.

Definition 3. *Let n, d be integers and $0 \leq \rho < 1$. An n-vertex d-regular graph G is called a (n, d, ρ)-expander if*

$$\forall\, S \subseteq [n] \text{ s.t. } |S| \leq \frac{n}{2}, \; |E(S, \overline{S})| \geq \rho d |S|. \tag{1}$$

Note that $d|S|$ is the maximum number of edges that we could talk about. Also, notice that we always have $\rho \leq \frac{1}{2}$.[1]). The following theorem states the existence of good expanders.

Theorem 4. $\forall\, \epsilon > 0$, $\exists\, d = d(\epsilon)$, $\exists\, N = N(\epsilon)$ *s.t.* $\forall\, n \geq N$, $\exists\, G$ *which is a* $(n, d, \frac{1}{2} - \epsilon)$-*expander.*

[1] To see this, for any graph G consider a randomly chosen S obtained by including every vertex independently with probability $1/2$. In expectation the set S will have exactly $dn/4$ edges going out, and so there must exist a set S having as many edges leaving it.

We will not prove it, but it is not too hard to show using the probabilistic method: a random graph works. Explicit constructions, on the other hand, are much harder. The following lemma about expanders states the key property that will be used in the analysis of Dinur's gap amplification procedure.

Lemma 5. *Suppose that G is an (n, d, ρ)-expander. Then for any set $S \subseteq [n]$ with $|S| \leq \frac{n}{2}$,*

$$\forall\ t,\ \Pr_{u \sim_t v}(u \in S, v \in S) \leq \frac{|S|}{n}\left(\frac{|S|}{n} + \left(\frac{1-\rho^2}{2}\right)^t\right) \tag{2}$$

where $u \sim_t v$ denotes choosing a uniformly random $u \in V$, making a t-step random walk starting there, and arriving at $v \in V$.

Proof. We'll prove it for $t = 1$. By definition of expansion,

$$\begin{aligned}
\Pr_{u \sim_t v}(u \in S, v \in S) &= \Pr(u \in S)\Pr(v \in S | u \in S) \\
&= \frac{|S|}{n}(1-\rho) \\
&\leq \frac{|S|}{n}\left(\frac{|S|}{n} + \frac{1}{2} - \rho\right) \\
&\leq \frac{|S|}{n}\left(\frac{|S|}{n} + \frac{1-\rho^2}{2}\right),
\end{aligned}$$

where the first inequality uses $|S|/n \leq 1/2$ and the last that $1 - 2\rho \leq 1 - \rho^2$ for $\rho \leq 2$. Note this is a bit of a wasteful bound. Alternatively there is an algebraic technique: ρ is related to the second largest eigenvalue $\lambda_2(G)$ of the adjacency matrix $A(G)$ as $\lambda_2(G) \leq 1 - \frac{\rho^2}{2}$ (this is called Cheeger's inequality). Then use $\lambda_2(G^t) = \lambda_2(G)^t$ and then use $\rho \geq \frac{1-\lambda_2}{2}$. G^t is a graph whose adjacency matrix specifies the paths of length t in G as edges, rather than the paths of length 1; applying the $t = 1$ case proven above to G^t would yield the lemma. We omit the details. □

Proof/Construction of Gap Amplification Step

We just want to get the main idea of this proof, and so we assume that the constraint graph G of φ is an (n, d, ρ)-expander for some $\rho < 1$. (An additional step in Dinur's proof shows that this can always be the case, without loss of generality.) Suppose $\omega(\varphi) \leq 1 - \epsilon$. Then any assignment to the vertices violates a fraction of at least ϵ of the constraints. These correspond to a 'bad' set of edges of G, which we can call S.

We want to figure out how to define φ' as specified for the gap amplification step. Fix a parameter t and define φ' as follows:

- φ''s variables are the same as φ's
- φ''s alphabet is $\Sigma' = \{0, 1\}^{1+d+d^2+\ldots+d^t}$. The idea is that each variable holds a value for itself, its nearest neighbors and etc... all the way to the t-th nearest neighbors.

- The constraints are "weighted" constraints; we can always go back to "unweighted" constraints by duplicating the "heavy" (higher probability) constraints as many times as required. The constraints are generated according to the following distribution: 1. Choose a random vertex u. 2. Make a t-step random walk in G from u to v. 3. Look at the values of the variables of φ', x'_u and x'_v, that are associated to the vertices u and v. Each of these variables provides an assignment of values in $\{0,1\}$ to all vertices at distance at most t from them. Check that the values provided by x'_u and x'_v agree on all vertices in the path $u \to v$, and that the common values satisfy all of φ's constraints along the path. The whole checking procedure makes a single constraint that is placed on an (u,v) edge for φ'.

Why does this work? The first thing to check would be that $\omega(\varphi) = 1 \implies \omega(\varphi') = 1$, which is clear: all variables x' in φ' can be assigned values consistent with a single satisfying assignment x for φ. Second and more importantly is to check that $\omega(\varphi) \leq 1 - \epsilon \implies \omega(\varphi') \leq 1 - 6\epsilon$. Let's take an assignment y to the variables for φ', such that y violates a fraction $(1 - \omega\varphi') = 1 - \delta$ of the clauses.

- What we'll show: there exists some x that violates a fraction at most $\frac{\delta}{6}$ of the constraints of φ.
- Since by assumption $\omega(\varphi) \leq 1 - \varepsilon$, we must have $\frac{\delta}{6} \geq \epsilon$ and so $\delta \geq 6\epsilon$, which will conclude the proof.

We make an important simplification. Assume that y is obtained in the "correct" way from some x for φ: when two y overlap (that is, they provide values for the same vertices of G) then their values match. If this simplifying assumption is not true, then the proof involves an additional step of amounting to a 'decoding' procedure which defines x at any vertex to be the majority value among those provided by all neighbouring y; it is then possible to show that there is always a "strong majority". Our simplifying assumption thus amounts to assuming that majority is unanimity! I

So, our goal is to show that $\delta \geq 6\epsilon$. We'll show that if y violates at most a fraction δ of the clauses, then x violates at most a fraction $\frac{\delta}{t}$ of clauses. But the best x violates at least a fraction ϵ of clauses.. so, $\frac{\delta}{t} \geq \epsilon$ and so $\delta \geq t\epsilon$ and we can take $t \leq 6$ to get what we want. (Note that we could get better for larger t but remember that the alphabet size for φ' increases very quickly with t...)

We need to show that a random constraint is violated with probability of at least $t\epsilon$. A random constraint is a whole bunch of constraints from φ. If these were chosen independently then the probability we completely avoid the 'bad' set S would be $(1-\epsilon)^t \simeq 1 - t\epsilon$, and so with probability at least $t\epsilon$ we see a violation.

However, constraints are *not independent*: they are selected from the random walk. The following lemma will let us complete the proof.

Lemma 6. *Let G be a (n,d,ρ) expander. Let S be a subset of edges of G such that $|S|/m = \varepsilon$, where m is the total number of edges. Let $t < 1/(d\varepsilon)$ be an integer. Then*

$$\Pr_{u \sim_t v}\left(\textit{at least one edge of the } t\textit{-walk is in } S\right) \geq \frac{\rho^2}{8d} t\varepsilon.$$

Applying the lemma with S the set of edges corresponding to constraints that are not satisfied by the assignment x, we obtain that $\delta \geq \rho^2/(8d)t\varepsilon$. Choosing $t = 48d/\rho^2$ (where ρ is the expansion factor of a good expander used in the construction, and can be taken to be a small constant, e.g. $\rho = 1/4$) then gives us $\delta \geq 6\varepsilon$ (as long as ε is not too large, in case we'd be done already), as desired.

Proof. For $i = 1, \ldots, t$ define indicator variables $X_i = 1$ if the i-th edge of the t-step random walk from u to v is in S, and $X_i = 0$ otherwise. Then $E[X_i] = |S|/m = \varepsilon$: since the first vertex u of the walk is chosen uniformly at random, any individual edge of the walk is also a uniformly random edge in G. By linearity of expectation, we deduce

$$E[X] = E\Big[\sum_i X_i\Big] = \sum_i E[X_i] = t\varepsilon,$$

where X is the number of edges along the walk that are in S. The probability in the lemma is $\Pr(X > 0)$. We will use a second moment bound

$$\Pr(X > 0) \geq \frac{E[X]^2}{E[X^2]}, \tag{3}$$

which holds for any random variable $X \geq 0$. For this it only remains to lower bound the second moment $E[X^2]$. Let $\overline{S}$ be the set of vertices in G that touch an edge in S. Write

$$\begin{aligned}
E[X^2] &= E\Big[\sum_{1\leq i,j\leq t} X_i X_j\Big] \\
&= \sum_{1\leq i,j\leq t} E[X_i X_j] \\
&= \sum_i E\big[X_i^2\big] + 2\sum_{1\leq i<j\leq t} E[X_i X_j] \\
&= t\varepsilon + 2\sum_{1\leq i<j\leq t} \Pr(i\text{-th edge in } S \text{ and } j\text{-th edge in } S) \\
&\leq t\varepsilon + 2\sum_{1\leq i<j\leq t} \Pr(i\text{-th vertex in } \overline{S} \text{ and } j\text{-th vertex in } \overline{S}) \\
&\leq t\varepsilon + 2\sum_{1\leq i<j\leq t} d\varepsilon\Big(d\varepsilon + \big((1-\rho^2)/2\big)^{j-i}\Big) \\
&\leq t\varepsilon + 2t^2(d\varepsilon)^2 + 2td\varepsilon 2/\rho^2 \\
&\leq (3 + 4d/\rho^2)t\varepsilon,
\end{aligned}$$

where the here the key step is given in the second inequality, in which we applied Lemma 5 (the factor $d\varepsilon$ comes from the fact that $|\overline{S}| \leq d|S|$). In the last inequality we used $td\varepsilon < 1$. Together with (3) this concludes the proof of the lemma. □