RECAP OF LAST LECTURE

Proof of $NP \subseteq PCP_{1,1/2}(poly(n), 1)$

QUADEQ quadratic equations over $\{0,1\}$

Given $m \times n^2$ matrix A $\quad \mathcal{E} = \{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$

m-dim vector b

Find n^2-dim U such that

(1) $A \cdot U = b$

(2) $U = u \otimes u$

$= (u_1 \cdot u, u_2 \cdot u, \ldots, u_n \cdot u)$

for $u \in \{0,1\}^n$

Proof π: Write down Walsh-Hadamard encodings $WH(u)$, $WH(U)$

$WH(u) = \{u \cdot x \mid x \in \{0,1\}^n\}$

- Can test efficiently whether string close to $WH(u)$
- If so, can evaluate $u \cdot x$ at any x, even if position x corrupted

PCP verifier test for $\pi = f, g$

1) Test f close to $WH(u)$
   g close to $WH(U)$
2) Test $U = u \otimes u$
3) Read off sum of random subset $\mathcal{E}_i$, $i \in S$ of equations from $WH(U)$ and check satisfied

So far, all of our PCP constructions and CSP problems were over the binary alphabet.

For some problems, more natural to encode over larger, non binary alphabets of size W for some $W \in \mathbb{N}^+$

We will think of this alphabet as

$$\{0, 1, 2, \ldots, W-2, W-1\} \qquad (i)$$

or

$$\{1, 2, 3, \ldots, W-1, W\} \qquad (ii)$$

depending on what seems most natural (definitely always variant (i) when $W = 2$, not seldom variant (ii) when $W > 2$).

DEFINITION (a bit sloppy)
For integers $q, W \in \mathbb{N}^+$, the $q\text{CSP}_W$ problem is defined analogously to the qCSP problem in Def 11.11 except that the underlying alphabet is of size W and constraints are encoded in terms of functions $f_i : [W]^q \to \{0,1\}$

Examples

3SAT subcase of qCSP$_W$ where $q = 3$, $W = 2$, constraints are disjunctions over literals over variables

3COL subcase of qCSP$_W$ where $q = 2$, $W = 3$, and for every edge (i,j) there is a constraint $u_i \neq u_j$

Want to prove version C of PCP Theorem:

There are constants $q \in \mathbb{N}^+$, $\rho \in (0,1)$ s.t. ρ-GAP qCSP is NP-hard.

Let us consider $\rho = 1 - \varepsilon$ for ε not a constant but a function of # constraints m

For unsatisfiable instance φ,

$$val(\varphi) \leq 1 - 1/m$$

Hence, we have NP-hard "gap problems" for gap $\rho = 1 - 1/m$

Want to use this to build iteratively NP-hard $(1-\varepsilon)$-GAP qCSP problems for larger and larger $\varepsilon = \varepsilon(m)$ until we get absolute constant ε independent of m

DEFINITION 22.3

A function f mapping CSP instances to CSP instances is a COMPLETE LINEAR-BLOWUP REDUCTION (or CL-reduction, for short) if it is polynomial-time computable and for every instance φ it holds that:

COMPLETENESS If $val(\varphi) = 1$, then $val(f(\varphi)) = 1$

LINEAR BLOWUP If m is the number of constraints in φ, then $f(\varphi)$ has at most Cm constraints and alphabet size W, where C and W can depend on the arity and alphabet size of φ, but <u>not</u> on the number of constraints or variables of φ.

LEMMA 22.4 (PCP MAIN LEMMA)

There exists constants $q_0 \geq 3$, $\varepsilon_0 > 0$, and a CL-reduction f such that for every q_0 CSP_2-instance φ and every $\varepsilon < \varepsilon_0$ it holds that $\psi = f(\varphi)$ is a q_0 CSP_2-instance satisfying

$$val(\varphi) \leq 1 - \varepsilon \Rightarrow val(\psi) \leq 1 - 2\varepsilon$$

Given this lemma, (version C of) the PCP Theorem immediately follows.

Just take an NP-hard q_0 CSP <u>decision</u> problem and apply f to it sufficiently many times. (Proof on next page for completeness.)

Proof of PCP Theorem assuming Lemma 22.4

Fix $g_0 \geq 3$. The decision problem g_0-CSP is NP-complete (since it contains e.g. g_0-SAT).
Let φ be an instance with m constraints
We have $val(\varphi) = 1$ or $val(\varphi) \leq 1 - 1/m$.

Let $\varphi^{(1)} = f(\varphi)$, $\varphi^{(2)} = f(\varphi^{(1)})$, ...,
$\varphi^{(i)} = f(\varphi^{(i-1)})$ for $i = 1, \ldots, \lceil \log m \rceil$

If $val(\varphi) = 1$, then $val(\varphi^{(i)}) = 1 \quad \forall i$

If $val(\varphi) \leq 1 - 1/m$, then

$$val(\varphi^{(i)}) \leq 1 - 2^i/m$$

as long as $2^{i-1}/m < \varepsilon_0$, and hence

$$val(\varphi^{(\lceil \log m \rceil)}) \leq 1 - \min\{2\varepsilon_0, 2^{\lceil \log m \rceil}/m\}$$

$$= 1 - 2\varepsilon_0$$

$\varphi^{(\lceil \log m \rceil)}$ has size $\leq C^{\lceil \log m \rceil} \cdot m = poly(m)$

This gives a reduction from an NP-complete problem to a $(1-2\varepsilon_0)$-GAP g_0 CSP problem, which establishes (version C of) the PCP Theorem

$\square$

Lemma 22.4 is proven in 2 steps

(1) Take $g\text{CSP}_2$ with small gap and transform to 2CSP_W with large gap but also large alphabet W
(GAP AMPLIFICATION)

(2) Take 2CSP_W with large gap and transform to $g\text{CSP}_2$ with still decent gap
(ALPHABET REDUCTION)

Let us state these steps as formal lemmas.

LEMMA 22.5 (GAP AMPLIFICATION)
For every $\ell, g \in \mathbb{N}^+$ there exist $W \in \mathbb{N}^+$, $\varepsilon_0 > 0$, and a CL-reduction $g_{\ell,g}$ such that for every $g\text{CSP}_2$-instance φ it holds that $\psi = g_{\ell,g}(\varphi)$ is a 2CSP_W-instance such that

$$\text{val}(\varphi) \leq 1-\varepsilon \text{ for } \varepsilon < \varepsilon_0 \Rightarrow \text{val}(\psi) \leq 1 - \ell\varepsilon.$$

LEMMA 22.6 (ALPHABET REDUCTION)
There exists a constant $g_0 \in \mathbb{N}^+$ and a CL-reduction h such that if φ is a 2CSP_W-instance, then ψ is a $g_0\text{CSP}_2$-instance such that

$$\text{val}(\varphi) \leq 1-\varepsilon \Rightarrow \text{val}(\psi) \leq 1 - \varepsilon/3$$

Lemma 22.4 follows by composing g in Lemma 22.5 with h in Lemma 22.6.

	Arity	Alphabet size	# constraints	Value
Original	g_0	2	m	$1-\varepsilon$
	⇓	⇓	⇓	⇓
Lemma 22.5 g	2	W	Cm	$1-6\varepsilon$
$\ell=6$, $q=g_0$	⇓	⇓	⇓	⇓
Lemma 22.6	g_0	2	$C'Cm$	$1-2\varepsilon$

OVERVIEW OF IDEAS

Gap amplification = drive down soundness error

Know how to do this = repeat verifier test K times

Problem: Gives arity $g_0 K$ – we want arity 2!

Solution:
- Look at graph structure of ψ
- Ask about whole neighbourhoods of assignments – check consistency
- Make sure graph structure is very well-connected – EXPANDER GRAPHS

Alphabet reduction Now we have 2CSP problem with large gap.

Require
a) encoding of good assignment to CSP instance
b) encoding of proof that verifier should accept assignment

Use PCP verifier from $NP \subseteq PCP_{1,1/2}(\text{poly}(n), 1)$

to check that verifier for 2CSP$_W$ instance would have accepted - VERIFIER COMPOSITION

A CRASH COURSE ON EXPANDER GRAPHS

G undirected d-regular graph on n vertices from now on.

$G=(V,E)$ is an (n,d,ρ)-edge expander if

(i) $|V(G)| = n$

(ii) G is d-regular

(iii) $\forall S \subseteq V$, $|S| \leq n/2$, it holds that

$$|E(S,\bar{S})| = |\{(u,v) \mid u \in S, v \in \bar{S}\}| \geq \rho d |S|$$

Intuition: G is very well-connected - every set S has lots of edges to rest of graph

Let $A_G = \{a_{ij}\}_{i,j \in [n]}$ normalized adjacency matrix

a_{ij} = # edges (i,j) / d

μ is an eigenvalue of A_G if $\exists v \in \mathbb{R}^n$, $v \neq 0$,

$$Av = \mu v$$

FACT A_G has n real eigenvalues (counted with multiplicities)

[and the corresponding eigenvectors form a basis of $\mathbb{R}^n$, but we don't need that]

This follows from the Spectral theorem (A_G is real and symmetric)

Let $\lambda_i = |\mu_i|$ for eigenvalues sorted in decreasing order w.r.t. absolute value

i.e. $|\mu_1| \geq |\mu_2| \geq \ldots \geq |\mu_n|$

Eigenvalues of A_G give us information about connectivity properties of G

For instance:

1) Max eigenvalue $\mu_1 = 1$ (always) and $\mu_2 \neq 1$ iff G is connected

2) A connected graph is bipartite iff $\mu_2 = -1$

3) Expansion properties of G are governed by how far λ_2 is from 1

λ_2 also denoted $\lambda(G)$

Hence the following definition:

G is an (n, d, λ)-spectral expander if

(i) $|V(G)| = n$

(ii) G is d-regular

(iii) $\lambda(G) \leq \lambda$

THEOREM (JUST FYI)
If G is an (n, d, λ)-spectral expander then G is also an $(n, d, (1-\lambda)/2)$-edge expander (and there is also a kind of converse, although the bounds are not exactly right).

There are explicit (i.e., polynomial-time computable) constructions of expander graphs for quite good parameters (but in practice, just randomly sampling a d-regular graph is very likely to give much better parameters, although it's hard to know for sure)

Expander graphs are ubiquitous in TCS and we could give a whole course on them...

We will just need two properties of (spectral) expander graphs

PROPOSITION α

For any (n, d, λ) - spectral expander $G = (V, E)$ and any $S \subseteq V$, $|S| \leq n/2$, sampling a uniformly random edge $(u, v) \in E$ it holds that

$$\Pr_{(u,v) \in E}\left[u \in S \text{ and } v \in S\right] \leq \frac{|S|}{|V|}\left(\frac{1}{2} + \frac{\lambda}{2}\right)$$

Proof

Exercise (but see hints in Arora-Barak)

Let G^ℓ be the graph on V s.t. $(u, v) \in E(G^\ell)$ if there is a length-ℓ walk from u to v in G

Not hard to see $A_{G^\ell} = (A_G)^\ell$

PROPOSITION β

If G is an (n, d, λ) - spectral expander, then G^ℓ is an $(n, d^\ell, \lambda^\ell)$ - spectral expander.

Proof

This follows by the definition above and that if μ is an eigenvalue of A, then μ^ℓ is an eigenvalue of A^ℓ.

We will also need a technical condition on $gCSP_W$ - instances

CONSTRAINT GRAPH $G(\varphi)$ of φ

$V(G(\varphi)) = [n]$ — identify i with variable u_i

For every constraint $\varphi(u) = f(u_{i_1}, \ldots, u_{i_2}, \ldots, u_{i_j}, \ldots, u_{i_q})$ there is an edge (i,j) for every pair of variables u_i, u_j appearing in f.

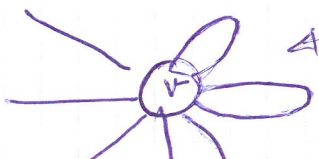
Allow $G(\varphi)$ to have - self-loops
- parallel edges

Actually, will only use this for binary constraints

$qCSP_W$ instance is "nice" if

Property 1: $q = 2$ (but no condition on W)

Property 2: $G(\varphi)$ is d-regular for some constant d (independent of W) and at every vertex half of the edges are self-loops



Example for $d = 6$

Property 3: $G(\varphi)$ is (n, d, λ)-spectral expander, $\lambda \leq 0.9$

CLAIM W.l.o.o.g. the instance φ in (say) Lemma 2.5 is nice.

That is, there is a boring, technical reduction that maps arbitrary $qCSP_W$-instances into nice $2CSP_{f(q)}$-instances (without really screwing up soundness too much) — details in Sec 22.A on pages 491-493.

[At some point, we were going to start skipping details. Well, it is happening now...]

Given a nice $2CSP_W$ instance, we apply a "powering" operation to improve the soundness error = increase the fraction of violated constraints

LEMMA 22.9 (Powering)
There is an algorithm A that given a nice $2CSP_W$ instance ψ and $t \in \mathbb{N}^+$ produces a $2CSP_{W'}$ instance $A(\psi, t) = \psi^t$ such that

1) $W' < W^{d^{5t}}$ where d = degree of $G(\psi)$ and ψ^t has $\frac{n d^{2t+1}}{2}$ constraints

2) $val(\psi) = 1 \Rightarrow val(\psi^t) = 1$

3) For every $\varepsilon < \frac{1}{d\sqrt{t}}$ it holds that if $val(\psi) \leq 1-\varepsilon$, then $val(\psi^t) \leq 1-\varepsilon'$ for $\varepsilon' = \frac{\sqrt{t}}{10^5 d W^4}\varepsilon$

4) A runs in time polynomial in $\sqrt{m_\psi}$ and W^{d^t}

Given this lemma, the gap amplification step is done. Let us describe the construction and sketch the proof (which we won't finish today).

Construction of ψ^t

ψ is over "old variables" $u_1, \ldots, u_n$ taking values in $[0, W-1]$

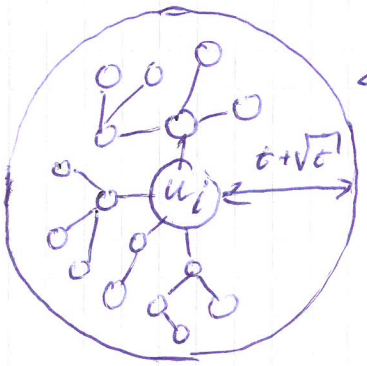
ψ^t will contain "new variables" $y_1, \ldots, y_n$

y_i encodes value of u_i plus every u_j that can be reached from u_i via at most $t+\sqrt{t}$ steps in $G(\psi)$

$$\#\text{ such vertices} \leq 1 + d + d^2 + \ldots + d^{t+\sqrt{t}} \leq$$
$$\leq d^{t+\sqrt{t}+1} \leq d^{5t}$$

Values = tuple in $[0, W-1]^{d^{5t}}$ = less than

$$= \text{single symbol in alphabet of size} \leq W' < W^{d^{5t}}$$



y_i

y_i "claims" all u_j in ball of radius $t+\sqrt{t}$ centered at u_i

Since all u_j appearing in constraints with u_i are neighbours in $G(\psi)$, can set values in y_i to satisfy many constraints. But other y_k far away might want to set some of its old variables u_j differently to satisfy

other constraints. If y_i and y_j claim overlapping vertices, then we will have inconsistency.

What we want:

(i) Show such inconsistencies must be frequent if $val(\Psi) \leq 1-\varepsilon$

(ii) Design binary constraints to detect such inconsistencies.

Sidenote

Arora-Barak talk interchangeably about paths (usually: vertices cannot repeat) and walks (vertices can repeat). I think they mean walks pretty much all the time.

Add constraint C_p for every $2t+1$ step path/walk $\langle i_1, i_2, \ldots, i_{2t+2} \rangle$.

C_p depends on y_{i_1} and $y_{i_{2t+2}}$ (arity 2)

C_p is violated if (and only if) there exists some j such that

1. i_j is in $t+\sqrt{t}$ radius ball around i_1
2. i_{j+1} is in $t+\sqrt{t}$ radius ball around i_{2t+2}
3. Let w = value of u_{i_j} claimed by y_{i_1}
   w' = value of $u_{i_{j+1}}$ claimed by $y_{i_{2t+2}}$
   (w, w') violates binary constraint in Ψ depending on $u_{i_j}, u_{i_{j+1}}$

Observations / Claims

Lemma 22.9, property 1)

Already checked alphabet size

constraints d^{2t+1}

Property 4)

Construction of ψ^t can be made to run in time polynomial in W^{dt} and m.

Property 2)

If ψ is satisfiable, then we obtain satisfying assignment to ψ^t by fixing an assignment to the old variables and letting all y_i pick values according to this assignment.

Property 3)

This is the hard part...

Philosophical aside: Why are we using graph $G_1(\varphi)$? Why not just pick uniformly random sets?

Requires too much randomness for PCP verifier.

But taking a local random walk in an expander graph is almost as good as true randomness, but much cheaper!