Function f mapping CSPs to CSPs is a COMPLETE LINEAR-BLOWUP (CL-) REDUCTION if

(i) f polynomial-time computable

(ii) $val(\varphi) = 1 \Rightarrow val(f(\varphi)) = 1$

(iii) If φ has m constraints, then $f(\varphi)$ has at most Cm constraints and alphabet size W. C and W do not depend on #constraints or #variables in φ

PCP theorem follows from 2 lemmas:

LEMMA 22.5 (GAP AMPLIFICATION)

$\forall \ell, q \in \mathbb{N}^+ \; \exists W \in \mathbb{N}^+, \varepsilon_0 \in (0,1)$, CL-reduction $g_{\ell,q}$ such that

(i) $g_{\ell,q}$ maps $q\mathrm{CSP}_2$ instances to $2\mathrm{CSP}_W$ instances

(ii) $val(\varphi) \leq 1-\varepsilon$ for $\varepsilon < \varepsilon_0 \Rightarrow$
$val(g_{\ell,q}(\varphi)) \leq 1 - \ell\varepsilon$

That is, gap between satisfiable and unsatisfiable instances blows up by factor ℓ.
But alphabet size also increases (a lot).

LEMMA 22.6 (ALPHABET REDUCTION)

$\exists q_0 \in \mathbb{N}^+$ and CL-reduction h such that

(i) h maps $2\mathrm{CSP}_W$ instances to $q_0\mathrm{CSP}_2$ instances

(ii) $val(\varphi) \leq 1-\varepsilon \Rightarrow val(h(\varphi)) \leq 1 - \varepsilon/3$

A d-regular undirected graph $G=(V,E)$ over n vertices (possibly with multi-edges and self-loops) is an (n,d,λ)-spectral expander if the second largest eigenvalue in absolute value of the normalized adjacency matrix A_G of G is at most λ

Quick facts: $\lambda < 1$ if G connected and non-bipartite

$\lambda \gtrsim 2/\sqrt{d}$ always

The smaller the λ, the better the connectivity properties of the graph

CONSTRAINT GRAPH $G(\varphi)$ for $2CSP_W$ instance φ

$V(G(\varphi)) = [n] \longleftrightarrow$ identify with variables $u_1, \ldots, u_n$

Add edge (i,j) for every constraint over variables u_i, u_j

Say that a $qCSP_W$ instance φ is "nice" if

- Property 1: $q=2$
- Property 2: $G(\varphi)$ is d-regular for some (even) constant d; at every vertex half of edges are self-loops
- Property 3: $G(\varphi)$ is an (n,d,λ)-expander for, say, $\lambda = 0.9$

In Lemma 22.5, can preprocess $qCSP_2$ instance φ to $2CSP_W$ instance φ' such that $G(\varphi')$ is nice. So Lemma 22.5 follows if we can prove the following:

We skipped the details. Not too hard, but not enlightening...

LEMMA 22.9 (POWERING)

There is an algorithm A that given

- nice $2CSP_W$ instance ψ
- parameter $t \in \mathbb{N}^+$

produces $2CSP_{W'}$ instance $A(\psi, t) = \psi^t$ such that

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

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

(3) If $val(\psi) \leq 1 - \varepsilon$, $\varepsilon < \frac{1}{d\sqrt{t}}$, then
$val(\psi^t) \leq 1 - \varepsilon'$, $\varepsilon' = \frac{\sqrt{t}}{10^5 d W^4} \varepsilon$

(4) A runs in time polynomial in n, m and W^{d^t}

scales like $\Omega(\sqrt{t}\,\varepsilon)$ is what's important

Recall that unless stated otherwise

n = # variables in CSP instance

m = # constraints in CSP instance

CONSTRUCTION

"New variable" y_i encodes value of u_i PLUS all u_j at distance $\leq t + \sqrt{t}$ from u_i in $G(\psi)$

y_i "claims" all these variables
"has an opinion" about their value

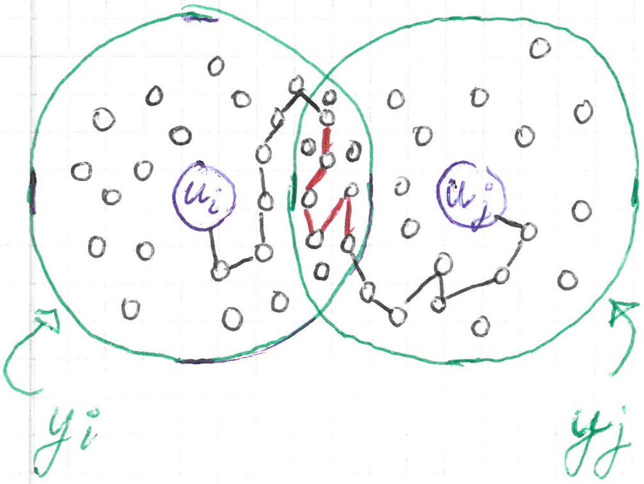
Graph terminology

Walk sequence of vertices $(v_1, v_2, v_3, \dots)$
such that $\forall i$ (v_i, v_{i+1}) edge
(sometimes called path)

Path walk without repeating vertices
(sometimes called a simple path)
Arora-Barak seems to use walk and path
as synonyms.

One constraint C_p for every walk with
$2t+1$ steps in $G(\Psi)$ $\langle i_1, i_2, \dots, i_{2t+2} \rangle$

$i = i_1$
$j = i_{2t+2}$



$\Psi_s(u_{i_k}, u_{i_{k+1}})$

C_p checks all constraints in Ψ such that
1) y_i has an opinion about u_{i_k}, say v_1
(i.e., u_{i_k} within distance $t + \sqrt{t}$ from u_i)
2) y_j has opinion about $u_{i_{k+1}}$, say v_2
(i.e., $u_{i_{k+1}}$ within distance $t + \sqrt{t}$ from u_j)

C_p accepts iff $\Psi_s(v_1, v_2)$ satisfied for
all such Ψ_s.

We skip proof of properties $\mathcal{L}1$ & $\mathcal{L}4$

$\mathcal{L}2$ (completeness) is straightforward
If ψ is satisfiable, then fix some satisfying assignment to u_i-variables
Let every y_i encode this assignment to variables in its neighbourhood

The hard part is $\mathcal{L}4$ - the soundness / gap

<u>Proof idea</u>: Take assignment to y_i:s of ψ^t violating not too many constraints. "Decode" to assignment of u_i:s of ψ violating very few constraints.

Or in the other direction: We know any assignment to ψ violates ε-fraction of constraints
Every constraint C_p in ψ^t has two nodes y_i & y_j checking $\Omega(\sqrt{t})$ constraints $\psi_i \in \psi$ about which both y_i and y_j have opinions. In the best of worlds, should have probability $\Omega(\sqrt{t}\,\varepsilon)$ of picking up at least <u>one</u> violated constraint. But y_i of course need not assign values to u_i:s consistently.

<u>PLURALITY ASSIGNMENT</u>

overloading variable names and their values

Fix an arbitrary assignment $y = y_1, \ldots, y_n$

For every u_i, define random variable Z_i as follows:

1) Start at vertex i
2) Take t-step random walk in $G(\psi)$, ending at, say j
3) Output the value that y_j claims for u_i

For every i, let $\boxed{z_i} = \underset{w \in [0, W-1]}{\operatorname{argmax}} \Pr[Z_i = w]$
(splitting ties arbitrarily)

$$\boxed{\Pr[Z_i = z_i] \geq 1/W}$$

Plurality assignment to $u = (u_1, \ldots, u_n)$

i's $= \boxed{(z_1, \ldots, z_n)}$

Any assignment to ψ violates
$\varepsilon m = \varepsilon nd/2$ constraints

Exists a set F of at least $\varepsilon nd/2$ failed
constraints violated by $z = (z_1, \ldots, z_n)$
$\equiv$ edges in $G(\psi)$

Use this set to show at least ε' fraction
of constraints C_p of ψ^t are violated
by assignment $y = (y_1, \ldots, y_n)$; $\varepsilon' = \Omega(\sqrt{t}\,\varepsilon)$

Pick a random walk $p = \langle i_1, \ldots, i_{2t+2} \rangle$ in
G of length $2t+1$, corresponding to a
constraint C_p (i.e., uniformly randomly
chosen)

For $j \in [2t+1]$, say that jth edge in
p (i_j, i_{j+1}) is TRUTHFUL if

y_{i_1} claims $u_{i_j} = z_{i_j}$
$y_{i_{2t+2}}$ claims $u_{i_{j+1}} = z_{i_{j+1}}$

i.e., new variables for end points of p claim that
u_{i_j} and $u_{i_{j+1}}$ agree with the plurality values

OBSERVATION (SIMPLE BUT CRUCIAL)
If the walk p has a truthful edge that lies in F, then C_p is violated

Proof By parsing the definitions.

So, we want to prove that ε'-fraction of constraints C_p / walks p contains a truthful edge in F

Game plan (which we won't have time to carry out):

(1) Fix any position j in walk.
Then jth edge of random walk p is a uniformly random edge (not hard)

(2) ~~Midpoint~~ edge of walk (distance t from both endpoints (i_{t+1}, i_{t+2}) has y_{i_1} taking part in plurality vote for $u_{i_{t+1}}$

$y_{i_{2t+2}}$ — " — $u_{i_{t+2}}$

$\Rightarrow$ Edge is truthful with probability $\geq \frac{1}{W} \cdot \frac{1}{W}$ (pretty much by definition)

(3) For edges in interval $[t - \sqrt{t}, t + \sqrt{t}]$ both y_{i_1} and $y_{i_{2t+2}}$ have opinions about endpoints "middle edges"
If we are sufficiently close to midpoint — at most $\delta\sqrt{t}$ away for small δ — then

opinions likely to agree with opinions about midpoints of walks $\Longrightarrow$ edges in interval $[t-\delta\sqrt{t}, t+\delta\sqrt{t}]$ are truthful with probability

$$\Omega(1/W^2)$$

Uses argument about statistical distance of distributions — not so obvious

(4) By (1) and (3) for any edge e and any fixed $j \in [t-\delta\sqrt{t}, t+\delta\sqrt{t}]$ it holds for a random walk p that

$$\Pr[e \text{ truthful} \mid e\ j\text{th edge}] = \Omega\left(\frac{1}{W^2}\right)$$

$$\Pr[e \text{ is } j\text{th edge}] = \frac{1}{|E|}$$

Let $\boxed{V = V(p) = \#\{\text{middle edges both truthful and in } F\}}$

By linearity of expectation we have

$$E[V] = \sum_{j=t-\delta\sqrt{t}}^{t+\delta\sqrt{t}} \Pr[j\text{th edge truthful and in } F]$$

$$= \sum_j \sum_{e \in F} \Pr[e \text{ is } j\text{th edge and is truthful}]$$

$$= 2\delta\sqrt{t} \cdot |F| \cdot \frac{1}{|E|} \cdot \Omega\left(\frac{1}{W^2}\right)$$

$$= \Omega\left(\frac{\delta\sqrt{t}\,\varepsilon}{W^2}\right)$$

This is straightforward

This looks quite similar to the kind of expression we are shooting for! Except...

Except we need to bound
$Pr[C_p \text{ violated}] \geq Pr[V>0]$,
not $E[V]$!

(5) In general, $E[V]$ says nothing about $Pr[V>0]$.
Unless we can prove that V is likely to be concentrated around its expectation.

Follows if variance $Var(V)$ small

Follows if second moment $E[V^2]$ not too large

(6) How could $E[V]$ be far off from $Pr[V>0]$? Most of the time no truthful middle edges in F, but when there are, then there are tons of them! Want to rule this out.

Look at $V' = \#$ middle edges in F

clearly $V' \geq V$

So sufficient to upper-bound

$$E[(V')^2]$$

This is where we are going to use that $G(\varphi)$ is an expander graph.

Recall from last lecture the claim that for an (n, d, λ)-spectral expander $G = (V, E)$ and any $S \subseteq V$, $|S| \leq n/2$

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

If we instead sample length-r walks with endpoints u, v (say), we get corollary

$$\Pr_{\substack{u \rightsquigarrow v \\ \text{length-}r \text{ walk}}}\left[u \in S \wedge v \in S\right] \leq \frac{|S|}{n} \cdot \frac{1+\lambda^r}{2}$$

because G^r is an (n, d^r, λ^r)-spectral expander. And by assumption, F is a very small set of edges, covering very few vertices.

Since $G(\varphi)$ is an expander, it is very unlikely that a random walk will cluster inside vertex set touched by F.

Doing the calculations, we get

Calculations, estimations...

$$E[V^2] \leq E[(V')^2] = O(\varepsilon \delta \sqrt{t} d) \quad (**)$$

(7) For a non-negative random variable V it holds that

$$\boxed{\Pr[V > 0] \geq \frac{E[V]^2}{E[V^2]}} \qquad (***)$$

[Useful exercise to prove this]

Plugging (*) and (**) into (***) we get

$$\Pr[\,C_p \text{ violated}\,] \geq \Pr[\,V>0\,] \geq$$

$$\geq \Omega\left(\frac{\sqrt{t}}{dW^4}\varepsilon\right) \qquad \text{as required.}$$

We dont have time to do the details, but given the intuition above you could hopefully follow the proofs on pages 468 - 470 in Arora-Barak (and bugfix the details if and when needed...)

So, modulo all the details skipped, this establishes Lemma 22.9, which modulo even more details skipped, establishes the Gap Amplification Lemma 22.5.

[But to be fair, we did cover all the important and interesting ingredients of the proof.]

LEMMA 22.6 (ALPHABET REDUCTION)
$\exists\, q_0 \in \mathbb{N}^+$ and CL-reduction h such that

(i) h maps $2CSP_W$ instances to $q_0\,CSP_2$ instances
(ii) $\mathrm{val}(\varphi) \le 1-\varepsilon \Rightarrow \mathrm{val}(h(\varphi)) \le 1 - \varepsilon/3$

We will use the PCP verifier in our proof of $\text{QUADEQ} \in PCP_{1,1/2}(\mathrm{poly}(n), 1)$

PROPOSITION
There is a poly-time reduction f from CIRCUITSAT to QUADEQ such that if C is a circuit of size ℓ with k inputs, then $f(C)$ is a set of quadratic equations with $O(\ell)$ equations over ℓ variables. Furthermore, in a witness for $f(C)$ the first k variables encode a satisfying input for C

Proof Exercise — not hard.

We also need to remember correspondence:

ρ-GAP $q\,CSP_2$ problem of size S $\Longleftrightarrow$ PCP verifier with q queries, completeness 1, soundness error ρ, randomness $\log S$

Start with $2CSP_W$ instance
Variables $u_1, \ldots, u_n$ taking values in $[W]$
Constraints $C_1, \ldots, C_m$

Encode variables as binary strings
in $\{0,1\}^k$ for $k = \log W$
Then C_i is function $C_i : \{0,1\}^{2k} \to \{0,1\}$
Can be encoded as circuit of
size $\leq 2^{2k} = W^2$

Each such circuit has PCP verifier
reading $O(1)$ bits (universal constant)
and using poly(W) randomness

Proof is Walsh-Hadamard encoding
of string of length $\leq W^2$, first k
bits of which is satisfying assignment

Idea

Require proofs for all circuits/constraints
$C_1, \ldots, C_m$

Write down separately Walsh-Hadamard
encodings of $u_1, \ldots, u_n \in \{0,1\}^{\log W}$

Verifier: 1) Pick $C_s(u_{i_{s,1}}, u_{i_{s,2}})$ randomly

2) check proof π_s for circuit C_s using
PCP verifier from a couple of lectures ago

3) Run concatenation test to check that

$\pi_S = WH(\mathcal{U})$ for some $\mathcal{U}$ such that

$$\mathcal{U} = u_{i_S,1} \circ u_{i_S,2} \circ z \qquad (+)$$

1) & 2) is exactly as in our proof of QUADEQ $\in PCP_{1,1/2}(\text{poly}(n),1)$

For 3), we have (thanks to previous testing)

$$f = WH(u_{i_S,1})$$

$$g = WH(u_{i_S,2})$$

$$h = WH(\mathcal{U})$$

Pick random $x, y \in \{0,1\}^k$

Check if

$$h(x \circ y \circ \vec{0}) = f(x) + g(y)$$

This detects violation of $(+)$ with probability $1/2$ by the random subsum principle

If we fix circuit C_S and look at proofs f, g, h above, the argument yields the following theorem (or, rather, <u>corollary</u> of $NP \subseteq PCP_{1,1/2}(\text{poly}(n),1)$ theorem)

COROLLARY 22.13 (PCP of proximity)

There is a verifier V that given any circuit C_s of size ℓ with $2k$ inputs has the following properties

1) if $u_1, u_2 \in \{0,1\}^k$ are such that $u_1 \circ u_2$ is a satisfying assignment for C_s, then $\exists\ \pi_3$ of size $2^{poly(\ell)}$ such that V accepts $WH(u_1) \circ WH(u_2) \circ \pi_{s,3}$ with probability 1

2) For every triple of strings π_1, π_2, π_3, $\pi_1, \pi_2 \in \{0,1\}^{2^k}$, if V accepts $\pi_1 \circ \pi_2 \circ \pi_3$ with probability 1/2, then π_1, π_2 are 0.01-close to $WH(u_1), WH(u_2)$ for $u_1, u_2 \in \{0,1\}^k$ s.t. $u_1 \circ u_2$ satisfies C_s

3) V runs in poly(ℓ) time, uses poly(ℓ) random bits, and queries only $O(1)$ bits

Consider now a verifier that (given $\varphi = \{C_1, \ldots, C_m\}$) asks for $WH(u_i)$, $i \in [n]$, as well as $\pi_{s,3}$ for all C_s.

It then picks a random s and runs verifier above for C_s and decides accordingly.

The tests for a given C_s is a qCSP$_2$ instance $\mathcal{C}_s$

The full verifier is a qCSP$_2$ instance

$$\Psi = \bigcup_{s=1}^{m} \mathcal{C}_s$$

We claim that if $\bigcup_{s=1}^{m} \mathcal{C}_s$ has assignment satisfying $(1-\delta)$-fraction of constraints, then we can construct assignment to original $2CSP_W$ instance φ satisfying $(1-2\delta)$ fraction of constraints

[Here we get factor 2 while Arora-Barak get 3 for some reason ...]

Suppose we have assignment to Ψ falsifying only δ constraints.

Clearly, $\exists$ at most 2δ $s' \in [m]$ s.t. 50% of constraints in $\mathcal{C}_{s'}$ falsified

Look at all other $\mathcal{C}_s$. Since acceptance probability $\geq 50\%$, we have Walsh-Hadamard encodings of assignments $a_{i_{s,1}}, a_{i_{s,2}} \in \{0,1\}^{\log W}$ such that $C_s(a_{i_{s,1}}, a_{i_{s,2}}) = 1$

(always unique)

For all u_i that do not get values from such C_s, let u_i = arbitrary value in $[W]$

Then the assignment $(a_1, \ldots, a_n) \in [W]^n$ satisfies all but a fraction 2δ of the constraints in the original $2CSP_W$ instance φ.

The Alphabet Reduction Lemma 22.6 follows. $\boxed{/\!/\!/}$

[And for this lemma we didn't really cheat in the proof]

AND NOW THE COURSE IS OVER — WRAP-UP

- Basic computational complexity theory
- Selection of "advanced" topics:
  - distributed algorithms
  - proof complexity
  - PCPs and hardness of approximation
- Hope that course gave you
  - general ~~overview~~ view of complexity theory (though by necessity biased)
  - opportunity to practise expository skills
  - mental gymnastics!
- We have (what we think are) interesting topics for MSc theses
- We are always interested in sharp PhD students (though competition is stiff)

THANKS FOR TAKING THE COURSE — HOPE YOU ENJOYED IT!