Lecture 12: "random 3-XOR and Res(k)" - part II -

recap: In the last lecture we proved (modulo some claims and a lemma) that given a random 3-XOR formula $F = \bigwedge_{i=1}^{\Delta n} L_i$ in n variables, for Δ large enough G_F will be an $(\gamma_n, .8)$-boundary expander and from this it follows that the size needed in Res(k) to refute F is at least

$$2^{\frac{n}{2}^{\Omega(k^2)}},$$

which is of the form $2^{n^{\varepsilon}}$ for some $\varepsilon > 0$ whenever $k < \sqrt{\log n}$.

In this lecture we are going to fill the missing details. That is given F as above the following things are left to prove.

Lemma 1: Let F as above and let D the max degree of G_F, then there exists a distribution $\mathcal{D}$ on partial assignments s.t. for each k-DNF φ in normal form,

$$\Pr_{\alpha \in \mathcal{D}}\left[\varphi|_\alpha \neq 1\right] \leq 3 \cdot e^{-\frac{cov(\varphi)}{D^{\Omega(k)}}},$$

where $cov(\varphi)$ is (as in the last lectures) the covering number of φ.

Claim 1: Let F as above, there exists a restriction ρ s.t.

(i) $G_{F|_\rho}$ is an $(\frac{\gamma_n}{2}, .4)$-boundary expander

(ii) max degree $G_{F|_\rho}$ is $\leq$ constant $c\Delta$.

Claim 2: Let F as above, ρ as in claim 1 and $\mathcal{D}$ as in Lemma 1, for every $\sigma \in \mathcal{D}$ we have that $G_{F|_{\rho\sigma}}$ is an $(\frac{\gamma_n}{4}, .2)$-boundary expander.

All the constructions needed to prove the above results rely on an extension of the notion of support. So we start with this notion and some properties of it.

-Supp*-

We are going to define the support* for generic expander graphs although we are going to use it just for the graph G_F (or sub-graphs of it).

Def: (support*) Let $G=(L\cup R, E)$ be a finite bipartite graph s.t. G is an (r,c)-boundary expander. Let $J\subseteq R$ and let $I=(I_k)_{k\leq \bar{k}}$ a sequence of subsets of L s.t.

(i) $\emptyset = I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_{\bar{k}}$

(ii) $|I_{k+1}\setminus I_k| \leq \frac{r}{2}$

(iii) $|\partial(I_{k+1}\setminus I_k)\setminus(N(I_k)\cup J)| < \frac{c}{2}|I_{k+1}\setminus I_k|$

A sequence $I=(I_k)_{k\leq \bar{k}}$ satisf. the properties (i)→(iii) above and it is maximal is called J-valid*. Given such a sequence we define $\text{supp}^*_I(J) = I_{\bar{k}}$.

exercise 1: Given any J-valid* sequence $I=(I_k)_{k\leq \bar{k}}$, for any $k\leq \bar{k}$ we have that $|\partial I_k \setminus J| < \frac{c}{2}|I_k|$.

Hint: by induction on k.

obs 1: if $|J| \leq \frac{cr}{4}$ then for every J-valid* sequence I, we have that

$$|\text{supp}^*_I(J)| < \frac{2}{c}|J|$$

pf: Let $I=(I_k)_{k\leq \bar{k}}$. By contradiction suppose that $|\text{supp}^*_I(J)| \geq \frac{2}{c}|J|$, let $i\leq \bar{k}$ be the first index s.t. $|I_i| \geq \frac{2}{c}|J|$, then

$$|\partial I_i \setminus J| \geq |\partial I_i| - |J| \overset{(*)}{\geq} c|I_i| - |J| \geq c|I_i| - \frac{c}{2}|I_i| = \frac{c}{2}|I_i|$$

contradicting exercise 1.

the inequality (*) holds since $|I_i| = |I_i \setminus I_{i-1}| + |I_{i-1}| \leq \frac{r}{2} + \frac{2}{c}|J| \leq \frac{r}{2}+\frac{r}{2} = r$ so to I_i we can apply the fact that the graph is an (r,c)-boundary expander

□

The crucial property we want from $supp^*$ is the following.

obs 2: Let $G=(L \cup R, E)$ be an (r,c)-boundary expander and with left-degree d, let $J \subseteq R$ and I a J-valid* sequence. The sub-graph of G induced by removing from the vertices of G all the vertices in $J \cup supp^*_I(J) \cup N(supp^*_I(J))$ is an $(\frac{r}{2}, \frac{c}{2})$-boundary expander. Moreover if we take as J all the vertices of R of largest degree, the subgraph we obtain has degree at most $\max\{d, \frac{d|L|}{|J|}\}$.

pf: Let $A \subseteq L \setminus supp^*_I(J)$. Consider $\emptyset \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_{\bar{u}}$ be the sequence I used to define $supp^*_I(J)$. By maximality $\emptyset \subsetneq I_1 \subsetneq \dots \subsetneq I_{\bar{u}} \subsetneq I_{\bar{u}} \cup A$ is not a J-valid* chain. So if $|A| \leq \frac{r}{2}$ it must be that

$$|\partial A \setminus (N(supp^*_I(J)) \cup J)| \geq \frac{c}{2}|A|.$$

So this means exactly that the subgraph we built is an $(\frac{r}{2}, \frac{c}{2})$-boundary expander.

For the degree part just observe that if a vertex in R survives and it has degree d', then all vertices in J must have degree $\geq d'$ so the total degree in the graph G, $d|L|$, must be s.t.

$$d|L| > d'|J|.$$

So the bound on d' follows.

Proof of Claim ①: $F = \bigwedge_{i \in [\Delta_W]} L_i$ is an (r,c)-boundary expander with $r = \gamma_W$ and $c = 0.8$.

Choose J as the set of all $\frac{cr}{4}$ largest degree vertexes on the right part of G_F. Let I a J-valid* sequence computing $supp^*_I(J)$. By observation 1 $|supp^*_I(J)| < \frac{2}{c}|J| \leq \frac{r}{2}$ so $\bigwedge_{i \in supp^*_I(J)} L_i$ is satisfiable. Take ρ' any minimal size partial assigment satisfying such set of lin. equations. Since ρ' is of minimal size $dom\,\rho' \subseteq N(supp^*_I(J))$. Extend (arbitrarily) ρ' to a ρ with domain $J \cup N(supp^*_I(J))$. By construction $F|_\rho$ will have as constraint-variables graph $G_{F|_\rho}$ exactly the one from obs 2 - and the degree of $G_{F|_\rho}$ is $\leq \max\{3, \frac{3\Delta_K}{0.4\gamma_K}\} =$ constant.

□

The distribution $\mathcal{D}$

Let $F = \bigwedge_{i=1}^{\Delta n} L_i$ a 3-XOR formula in n variables s.t. G_F is an (r,c)-boundary expander. The partial assignment $\sigma \in \mathcal{D}$ is chosen according to the following experiment:

(i) for each variable x_i indip. w/p $\frac{cr}{8n}$ add it to a set Y

(i bis) choose a Y-valid* sequence I

(ii) choose σ unif. at random among the assignments s.t.

(a) σ satisfies $\bigwedge_{i \in \text{supp}_I^*(Y)} L_i$

(b) $\text{dom}\,\sigma = Y \cup N(\text{supp}_I^*(Y))$

N.B.: If there is no such σ we restart but the expected size of Y is $\frac{cr}{8}$ so it is very likely that there exists some σ s.t. σ satisfies $\bigwedge_{i \in \text{supp}_I^*(Y)} L_i$.

exercise: show that for this choice of $\mathcal{D}$, claim 2 holds.

Lemma 2: for any $\sigma \in \mathcal{D}$ and any k-term s.t. $\text{var}(t) \subseteq \text{dom}\,\sigma$ it holds that $\Pr_{\sigma \in \mathcal{D}}[t|_\sigma = 1] = 0$ or $\Pr_{\sigma \in \mathcal{D}}[t|_\sigma = 1] \geq 2^{-k}$. (*)

This is also true if we condition on σ assuming some particular values on some variables of $\text{dom}\,\sigma$. (**)

proof sketch: $\sigma \in \mathcal{D}$ means that σ satisfies $\bigwedge_{i \in \text{supp}_I^*(Y)} L_i$ and it is chosen unif at random among the p.a. with this property, but $\bigwedge_{i \in \text{supp}_I^*(Y)} L_i$ represents an affine subspace A of $\{0,1\}^n$ (remember that the L_is are 3-XORs). Consider any subset of coordinates S st all bitstrings $\{0,1\}^S$ are supported by A. Then $\sigma \in \mathcal{D}$ yields uniformly random and independent bits when restricted to $\{0,1\}^S$.

Consider as S a set of coordinates s.t. all variables in $\text{var}(t)$ are fully determined by the variables in $S \cap \text{var}(t)$. (why this S exists?)

then $\Pr_{\sigma \in \mathcal{D}}[t|_\sigma = 1] = \underbrace{\frac{1}{2} \cdot \ldots \cdot \frac{1}{2}}_{|S \cap \text{var}(t)|} \cdot \underbrace{\qquad}_{\leq \text{sent fully determ.}}$ So the bounds in (*) follows. For (**) it is the same (roughly) ~□

Proof of Lemma 1:

we are going to use some fairly basic probabilistic bounds and a weak version of Chernoff bounds. The following

(A) for every event A, B, C it holds that $\Pr[A] \le \Pr[A \mid B \wedge C] + \Pr[\neg B] + \Pr[\neg C]$

(B) let $X_1, \dots, X_n$ be independent random variables taking values in $\{0,1\}$, let $\mu = \mathbb{E}\left[\sum_{i=1}^{n} X_i\right]$ then $\Pr\left[\sum_{i=1}^{n} X_i < \frac{\mu}{2}\right] \le e^{-\mu/8}$ and

$$\Pr\left[\sum_{i=1}^{n} X_i > 2\mu\right] \le e^{-\frac{\mu}{4}}$$

Suppose we are given a K-DNF φ and $\sigma \in \mathcal{D}$, from the construction of σ we defined also a set of variables Y, to remind its connection with σ let's call it Y_σ. Let I_σ be the Y_σ-valid* sequence chosen. For simplicity we write $\text{supp}^*(Y_\sigma)$ for $\text{supp}^*_{I_\sigma}(Y_\sigma)$

We say that σ is good if $|Y_\sigma| \le \frac{cr}{4}$, since $\mathbb{E}[|Y_\sigma|] = \frac{cr}{8}$ then by Chernoff (B above)

$$\Pr_{\sigma \in \mathcal{D}}\left[\underbrace{|Y_\sigma| > \frac{cr}{4}}_{\sigma \text{ not good}}\right] \le e^{-\frac{cr}{32}} = e^{-\Omega\left(\frac{n}{D}\right)}$$

Moreover in φ we can always find $\ge \frac{\text{cov}(\varphi)}{K}$ variable disjoint terms and for each of them the probability that all the variables appear in Y_σ is $\left(\frac{cr}{8n}\right)^K = D^{-O(K)}$ since $r = \Omega\left(\frac{n}{D}\right)$. So the expected number of terms of φ variable-disjoint and with all the variables in Y_ρ is $\ge \frac{\text{cov}(\varphi)}{K} \cdot \frac{1}{D^{O(K)}}$. We say that φ is good (wrt σ) if φ has at least $\frac{\text{cov}(\varphi)}{2K\, D^{O(K)}}$ variable-disjoint terms each with variables in Y_σ.

By Chernoff, $\Pr_{\sigma \in \mathcal{D}}\left[\varphi \text{ is not good wrt } \sigma\right] \le e^{-\frac{\text{cov}(\varphi)}{8K D^{O(K)}}}$

So

$$\Pr_{\sigma \in \mathcal{D}}\left[\varphi|_\sigma \neq 1\right] = \Pr_{\sigma}\left[\bigwedge_{t \in \varphi}(t|_\sigma \neq 1)\right] \le \Pr_{\sigma}\left[\bigwedge_{t \in \varphi}(t|_\sigma \neq 1) \,\middle|\, \varphi \text{ good} \wedge \sigma \text{ good}\right] + \Pr_{\sigma}[\varphi \text{ not good}] + \Pr[\sigma \text{ not good}]$$

$$\le \underbrace{\Pr\left[\bigwedge_{t \in \tilde{\varphi}}(t|_\sigma \neq 1) \,\middle|\, \varphi \text{ good} \wedge \sigma \text{ good}\right]}_{(*)} + e^{-\Omega\left(\frac{n}{D}\right)} + e^{-\frac{\text{cov}(\varphi)}{8K D^{O(K)}}}$$

$\tilde{\varphi}$ is a sub-DNF of φ coming from the fact that φ is good

So now we just have to focus on the first term of the previous expression. To upper-bound it, it is enough to find some terms $t_1, \dots, t_T$ in $\tilde{\varphi}$ s.t. if we call E_i the event "σ satisfies t_i", then

$$\left.\begin{aligned} &\Pr_{\sigma \in \mathcal{D}}[E_1] \geq 2^{-k} \\ &\Pr_{\sigma \in \mathcal{D}}[E_i \mid \neg E_1 \wedge \dots \wedge \neg E_{i-1}] \geq 2^{-k} \end{aligned}\right\} (1)$$

Then, by the chain rule ($\Pr[A \wedge B] \leq \Pr[A \mid B] \cdot \Pr[B]$) we get

$(*) \leq (1-2^{-k})^T \leq e^{-\frac{T}{2^k}}$. So we just need to find $t_1, \dots, t_T$ s.t. the property (1) above holds and T is large enough. We use the fact that φ (and hence also $\tilde{\varphi}$) is in normal-form.

Let t_1 be any term in $\tilde{\varphi}$, since $\tilde{\varphi}$ is in normal form then

$$t_1 \wedge \bigwedge_{i \in \mathrm{supp}(t)} L_i \quad \text{is satisfiable.}$$

Since σ is good, i.e. $|Y_\sigma| \leq \frac{cr}{4}$ then by exercise 2, $|\mathrm{supp}^*(Y_\sigma)| \leq \frac{2}{c}|Y_\sigma| \leq \frac{r}{2}$

then by the observation 2 from last lecture

$$t_1 \wedge \bigwedge_{i \in \mathrm{supp}^*(Y_\sigma)} L_i \quad \text{is satisfiable.}$$

But $t_1 \in \tilde{\varphi}$ so by construction $\mathrm{var}(t_1) \subseteq Y_\sigma$ so $\Pr_\sigma[t_1|_\sigma = 1] \neq 0$ and hence by Lemma 2, $\Pr_\sigma[t_1|_\sigma = 1] \geq 2^{-k}$.

Now, intuitively, we are able to repeat this construction for terms that are "far" from previously constructed terms. More precisely the construction goes as follows: suppose we built $t_1, \dots, t_i$ and suppose the event $\neg E_1 \wedge \dots \wedge \neg E_i$ happened, we want to find t_{i+1} or stop the construction.

Let $V_i = \mathrm{var}(t_1) \cup \dots \cup \mathrm{var}(t_i)$, since $\tilde{\varphi}$ is a k-DNF of variable-disjoint terms then $|V_i| = ki$. Let Z_i be the set of all variables in $Y_\sigma \cup N(\mathrm{supp}^*(Y_\sigma))$ that are at distance $\leq \frac{4k}{c}$ from some element of $V_i \cup \mathrm{supp}^*(V_i)$.

If Z_i covers $\tilde{\varphi}$ we conclude the process and let $T = i$.

Otherwise let $t_{i+1} \in \tilde{\varphi}$ be a term s.t. t_{i+1} doesn't contain variables from Z_i, i.e. $var(t_{i+1})$ has distance from $V_i \cup supp^*(V_i)$ strictly bigger than $\frac{4K}{c}$.

Claim 3: $\Pr_{\sigma \in \mathcal{D}}\left[t_{i+1}\restriction_\sigma = 1 \mid \neg E_1 \wedge \cdots \wedge \neg E_i\right] \geq 2^{-K}$

So, given for granted for a moment this claim, it follows that

$$\Pr_\sigma[\varphi\restriction_\sigma \neq 1] \leq e^{-\frac{T}{2^K}} + e^{-\frac{cov(\varphi)}{K D^{\omega(K)}}} + e^{-\Omega\left(\frac{u}{D}\right)} \qquad (\star)$$

So let's l.b. T: CASE 1: $KT \leq \frac{cr}{4}$. So $|V_T| = KT \leq \frac{cr}{4}$ and hence $|supp^*(V_T)| \leq \frac{2}{c}|V_T| \leq \frac{2KT}{c}$

Let's give an upper and a lower bound for Z_T:

$$(\bullet)\ |Z_T| \geq |cov(\tilde{\varphi})| = |\tilde{\varphi}| \geq \frac{cov(\varphi)}{K D^{\omega(K)}}$$

(by def.; terms in $\tilde{\varphi}$ var. disj)

$$(\bullet\bullet)\ |Z_T| \leq \left(|V_T| + |supp^*(V_T)|\right) \cdot D^{\frac{4K}{c}+1} \leq \left(KT + \frac{2KT}{c}\right) \cdot D^{\frac{4K}{c}+1}$$

from $(\bullet)$ and $(\bullet\bullet)$ it follows immediately that

$$T \geq \frac{cov(\varphi)}{K D^{\omega(K)}}$$

CASE 2: $KT > \frac{cr}{4}$, so $T > \frac{cr}{4K} = \Omega\left(\frac{u}{KD}\right)$

Since $cov(\varphi) \leq u$ then we can upper bound $(\star)$ as

$$\Pr_\sigma[\varphi\restriction_\sigma \neq 1] \leq 3 \cdot e^{-\frac{cov(\varphi)}{D^{\omega(K)}}}$$

So it is remained only to prove Claim 3.

proof of Claim 3: by Lemma 2 it is enough to prove that $\Pr_\sigma\left[t_{i+1}\restriction_\sigma = 1 \mid \neg E_1 \wedge \cdots \wedge \neg E_i\right] \neq 0$. So let $\sigma \in \mathcal{D}$ s.t. $\neg E_1 \wedge \cdots \wedge \neg E_i$ holds and let $t_\sigma^{(i)}$ be a term expressing σ restricted to V_i, e.g.

if $\sigma = \{x=0, y=1, z=0\}$, $t_\sigma = \bar{x} \wedge y \wedge \bar{z}$.

Clearly $t_\sigma^{(i)} \wedge \bigwedge_{i \in supp^*(Y_\sigma)} L_i$ is satisfiable.

Also $t_{i+1} \wedge \bigwedge_{i \in supp^*(Y_\sigma)} L_i$ is satisfiable since t_{i+1} is locally consistent and $|supp^*(Y_\sigma)| \leq \frac{r}{2}$. We show that we have that

$$t_{i+1} \wedge t_\sigma^{(i)} \wedge \bigwedge_{i \in supp^*(Y_\sigma)} L_i \quad \text{is satisfiable.} \quad (*)$$

Hence we will have that

$$\Pr_\sigma[t_{i+1}\restriction_\sigma = 1 \mid \neg E_1 \wedge \dots \wedge \neg E_i] \geq \Pr_\sigma\left[t_{i+1}\restriction_\sigma = 1 \;\middle|\; \sigma\restriction_{V_i} = t_\sigma^{(i)} \text{ for some specific } t_\sigma^{(i)}\right] \neq 0$$

So by lemma 2 this probability is $\geq 2^{-k}$.

Let's focus on the equation $(*)$ then: suppose, by contradiction it is UNSAT, let then $\tilde{t}_{i+1} \subseteq t_i$, $\tilde{t}_\sigma^{(i)} \subseteq t_\sigma^{(i)}$ and $A \subseteq supp^*(Y_\sigma)$ s.t. $\tilde{t}_{i+1} \wedge \tilde{t}_\sigma^{(i)} \wedge \underbrace{\bigwedge_{i \in A} L_i}_{= F'}$ is minimally unsat.

We hence have that (i) $G_{F'}$ is connected

(ii) $\partial A \subseteq var(\tilde{t}_{i+1}) \cup var(\tilde{t}_\sigma^{(i)})$ and by what observed before it must be that both $var(\tilde{t}_{i+1})$ and $var(\tilde{t}_\sigma^{(i)})$ are non-empty.

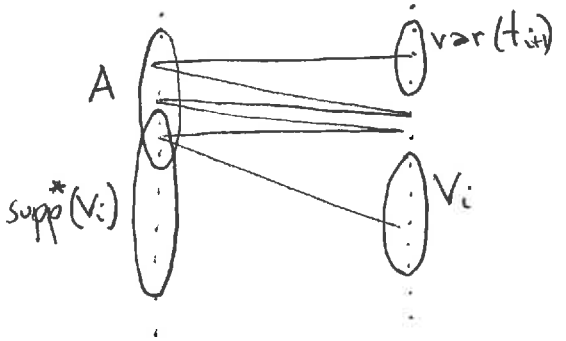
CASE 1: $|A \setminus supp^*(V_i)| > \frac{2k}{c}$ then

$$\left|\partial(A \setminus supp^*(V_i)) \setminus (V_i \cup supp^*(V_i))\right| \leq k < \frac{c}{2}\,|A \setminus supp^*(V_i)|$$

$\partial A \subseteq \underbrace{var(\tilde{t}_{i+1})}_{\text{size} \leq k} \cup \underbrace{var(\tilde{t}_\sigma^{(i)})}_{\subseteq V_i}$

so by a maximality argument we saw before (enlarging a chain...) we must have that $A \subseteq supp^*(V_i)$. ↯

CASE 2: $|A \setminus supp^*(V_i)| \leq \frac{2k}{c}$



Since $G_{F'}$ is connected and $var(\tilde{t}_i)$ and $var(\tilde{t}_\sigma^{(i)})$ are non-empty then there exists a path connecting those two sets using only left vertices in A.

Clearly the lenght of such path is $\leq 2|A \setminus supp^*(V_i)|$ (from that path we can build another one connecting $V_i \cup supp^*(V_i)$ to $var(t_{i+1})$.)

$\leq \frac{4k}{c} + 1$ (+1)

□