10. Graph Isomorphism and the Lasserre Hierarchy

Lecturer: Massimo Lauria

We complete the technical part of the proof that refuting Graph Isomorphism requires linear degree in the Positivstellensatz proof system even for graphs that are far from isomorphic.

http://www.csc.kth.se/~lauria/sos14/

Recap

Recall that in the last lecture we started proving that refuting Graph Isomorphism is hard for SOS proof systems.

Theorem 1. [1] *For infinitely many n, there exist graphs G, H with $|V(G)| = |V(H)| = n$ and $|E(G) = E(H) = O(n)|$ that are not 10^{-18}-isomorphic and such that any $\mathrm{PC}_>$ refutation of $G \cong H$ requires degree $\Omega(n)$.*

[1]

Our plan was to reduce random 3-XOR to Graph Isomorphism, and it only remained to show one missing piece, namely that the graphs $G_{Ax=b}$ and $G_{Ax=0}$ resulting from our construction are far from isomorphic.

Lemma 2. *Fix a constant $c \geq 10^8$. Then w.h.p. $G_{Ax=b}$ and $G_{Ax=0}$ are not $(1 - 1/95c^2)$-isomorphic.*

We spend the rest of the lecture proving this lemma.

Auxiliary results

First we need to introduce some definitions and properties. The concept of almost-asymmetry is a generalization of asymmetry. Recall that an object is asymmetric if its group of automorphisms is trivial.

Definition 3. *A (hyper)graph G is* (β, γ)-asymmetric *if any $(1-\gamma)$-automorphism has at least a $(1-\beta)$ fraction of fixed points.*

Observe that, in particular, a $(0,0)$-asymmetric graph is the same as an asymmetric graph and that every graph is $(\beta, 1)$-asymmetric.

In other words, this definition means that if an almost-automorphism permutes many vertices then it has large error, or that the graph may have local but not global symmetries.

Theorem 4. *Let H be a random 3-uniform hypergraph with n variables and cn edges for some constant $c \geq 10^4$. Fix a constant $e^{-c/6} < \beta < 1$. Then w.h.p. H is $(\beta, \beta/240)$-asymmetric.*

Observe that the parameter loss in Theorem 4 is only constant.

Now we bound the average degree of large sets of random graphs.

Definition 5. *A (hyper)graph G is* (ϵ, D)-degree-bounded *if every set of $\epsilon|V(G)|$ vertices has average degree less than D.*

Definition 5 is equivalent to imposing that every fraction of *at least* ϵ vertices has average degree less than D. Observe that for $\epsilon = 1$ the definition is equivalent to average degree, and that for $\epsilon = 1/n$ the definition is equivalent to (maximum) degree.

Lemma 6. *If a (hyper)graph G is (ϵ, D)-degree-bounded then every set of βn vertices is incident to at most $(\beta + \epsilon)Dn$ edges.*

Proof. Add ϵn vertices to the original set. □

We can extract the underlying 3-uniform hypergraph from a 3-XOR by identifying vertices with variables and constraints by sets of variables, disregarding any information about signs. In particular, $Ax = b$ and $Ax = 0$ have the same underlying hypergraph, and the distribution of hypergraphs over random 3-XOR is very close to the distribution of random 3-uniform hypergraphs of the appropriate parameters.

Lemma 7. *Let $Ax = b$ be a random (n, cn)-3-XOR for some constant $c \geq 3$. Then w.h.p. the hypergraph of A is $(1/c, 100c)$-degree-bounded.*

The following is an instantiation of a theorem we discussed in the lecture proving lower bounds for random 3-SAT with concrete parameters.

Lemma 8. *Let $Ax = b$ be a random (n, cn)-3-XOR for some constant $c > 10^5$. Then at most a 0.51 fraction of constraints can be satisfied simultaneously.*

We have all the ingredients needed to state our main technical lemma, which we will prove in the next section.

Lemma 9. *Let $Ax = b$ be a random (n, cn)-3-XOR such that its underlying hypergraph H satisfies that:*

- *H is $(\epsilon, 100c)$-degree-bounded,*
- *H is (β, γ)-asymmetric,*

with $200\epsilon \leq \gamma$, and let $\delta = \min\{1/200, \gamma/48, \epsilon/95c\}$. If there is a $(1-\delta)$-isomorphism between $G_{Ax=b}$ and $G_{Ax=0}$, then it is possible to satisfy a $0.9 - 100(\epsilon + \beta)$ fraction of constraints of $Ax = b$ simultaneously.

We now set the appropriate parameters to Lemma 9 and complete the proof.

Proof of Lemma 2. Let $Ax = b$ be a random (n, cn)-3-XOR and let H be its underlying hypergraph. We choose the parameters $\epsilon = 1/c$, $\gamma = 200\epsilon = 200/c$, and $\beta = 240\gamma = 48000/c$. By Theorem 4, H is (β, γ)-asymmetric w.h.p.. By Lemma 7, H is $(\epsilon, 100c)$-degree-bounded w.h.p.. Let $\delta = \epsilon/95c = 1/95c^2$. Assume for the sake of contradiction that there is a $(1-\delta)$-isomorphism between $G_{Ax=b}$ and $G_{Ax=0}$. Then by Lemma 9 we can satisfy a fraction $0.9 - 100(1/c + 48000/c) \geq 0.8$ of the constraints of $Ax = b$ simultaneously. But this contradicts Lemma 8, therefore such almost-isomorphism does not exist. □

Proof of technical lemma

We next sketch the proof of Lemma 9, giving the intuition behind the claims but not making the calculations to establish them.

Let us assume that there is a $(1-\delta)$-isomorhpism π between $G_{Ax=b}$ and $G_{Ax=0}$. We will show that this isomorphism must be close to the almost-isomorphism induced by some assignment τ using the construction we saw in the last lecture and that the assignment τ satisfies a large fraction of constraints.

First we show that the almost-isomorphism π respects the structure in constraints versus variables of the graph. Let $\mathcal{A}$ be the set of constraint indices $j \in [cn]$ such that the four vertices of C_j are mapped to the four vertices of some other constraint $C^0_{j'}$. Intuitively, 4-cliques are mapped to 4-cliques or commit an error, so most constraints are mapped to constraints.

Claim 10. $|\mathcal{A}| \geq (1-19\delta)m$.

Let $\mathcal{B}$ be the set of variable indices $i \in [n]$ such that the two vertices of x_i are mapped to the two vertices of some other variable $x_{i'}$. Since most constraint nodes are already mapped to, most variable nodes are mapped to variable nodes and most pairs with an edge are mapped to pairs with an edge to avoid errors, thus most variables are mapped to variables.

Claim 11. $|\mathcal{B}| \geq (1-95c\delta)n$.

We now study how variables are mapped among themselves. Let $\sigma : [n] \longrightarrow [n]$ be the automorphism of variables induced by π in the following way. If $i \in \mathcal{B}$ and $\pi(x_i \to 0) = x_{i'} \to b$, then $\sigma(i) = i'$. Extend it arbitrarily to $[n] \setminus \mathcal{B}$. Again, in order to avoid errors, if (i_1, i_2, i_3) are a constraint then the edges joining constraints and variables are mapped to edges, which means that $(\sigma i_1, \sigma i_2, \sigma i_3)$ is also a constraint.

Claim 12. *σ is a $(1-100\epsilon-24\delta)$-automorphism of H, the underlying hypergraph of $Ax = b$.*

But we assumed that H is asymmetric, so by Definition 3 most of the domain of σ are fixed points. There is one degree of freedom left for each variable, though: whether we mapped the two nodes identically of we flipped them. We define an assignment using this information.

$$\tau(x_i) = \begin{cases} b & \text{if } \sigma(i) = i \text{ and } \pi(x_i \to 0) = x_i \to b \\ \text{arbitrary} & \text{otherwise} \end{cases} \tag{1}$$

The following claim finishes the proof of Lemma 9.

Claim 13. *$A\tau = b$ is correct in at least a $0.9 - 100(\epsilon+\beta)$ fraction of the entries.*

Proof sketch of Claim 13. We already argued that most variables are fixed points. It follows that most constraint nodes connected to fixed variables are either fixed or map to a constraint node in the same clique. In any case, most constraints are fixed points too.

This implies that π respects most constraints in the following sense: assume that C_j is a constraint over the variables x_1, x_2, x_3 and that they are fixed with respect to π. Let (b_1, b_2, b_3) be a constraint node of C_j in $G_{Ax=b}$, therefore adjacent to the vertex nodes $x_1 \to b_1$, $x_2 \to b_2$, $x_3 \to b_3$. Since

we assume that π fixes the involved variables and constraints, it maps the variable nodes $x_i \to b_i$ to $x_i \to b'_i$, and the constraint node to (b'_1, b'_2, b'_3).

By construction of $G_{Ax=0}$, $b'_1 + b'_2 + b'_3 = 0$, and by construction of τ, $\tau(x_i) = (b_i + b'_i)$. Finally, $\tau(x_1) + \tau(x_2) + \tau(x_3) = b_1 + b'_1 + b_2 + b'_2 + b_3 + b'_3 = b_1 + b_2 + b_3$ so τ satisfies the constraint C_j.

□

References