

## 9. Graph Isomorphism and the Lasserre Hierarchy.

Lecturer: Massimo Lauria

Let  $G$  and  $H$  be two graphs, we say that two graphs are *isomorphic*, denoted as  $G \cong H$ , if there is a bijection  $\pi : V(G) \rightarrow V(H)$ , such that  $\{u, v\} \in E(G)$  if and only if  $\{\pi(u), \pi(v)\} \in E(H)$ . In this lecture, we discuss a recent paper by O’Donnell, Wright, Wu and Zhou<sup>1</sup> which proved the following theorem.

**Theorem 1.** *For infinitely many  $n$ , there exist graphs  $G$  and  $H$ , such that*

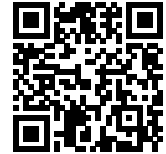
- $|V(G)| = |V(H)| = n$ .
- $|E(G)| = |E(H)| = O(n)$ .
- $G$  and  $H$  are “far from” being isomorphic.
- Any  $PC_{>}$  refutation of  $G \cong H$  has degree  $\Omega(n)$ .

We will define what we mean by “far from” isomorphic shortly. First, we give a (very) high level overview of the proof. The reduction starts by taking a 3XOR formula, and generate two graphs  $G$  and  $H$ , such that if the 3XOR formula is satisfiable, then  $G \cong H$ , and if the 3XOR formula is far from being satisfiable, then  $G$  and  $H$  are far from being isomorphic. Now remember from previous lectures that if we pick a random 3XOR formula, then with high probability it is unsatisfiable and the 3XOR refutation of it in  $PC_{>}$  will have degree  $\Omega(n)$ . This implies that the  $PC_{>}$  refutation for  $G \cong H$  will have degree  $\Omega(n)$ , otherwise one can convert this refutation to a refutation for the satisfiability of the 3XOR formula we started with without blowing up the degree.

### Background

Before we describe the reduction, let us start with some practical algorithm for solving graph isomorphism. One class of algorithms is known as “color refinement algorithm”, studied by McKay<sup>2</sup> and McKay-Piperno<sup>3</sup> The basic algorithm starts by giving all vertices in the two graphs with the same color. Then, in each step, replace the colors of the vertices with the multiset containing the colors of their neighbors. Repeat until the coloring in both graphs converge, or for some coloring, the numbers of vertices with that color in the two graphs are different, in which case return that the two graphs are not isomorphic. An example of a run of the algorithm is given in Figure 1 and Figure 2.

There are easy examples where the above color refinement algorithm does not work. In particular, consider any pair of  $d$ -regular graphs, that is, graphs where all vertices have exactly  $d$  neighbors. The coloring will essentially converge to the degree of the vertices.



<sup>1</sup> <http://www.soc.kth.se/~lauria/cos14/>  
R. O’Donnell, J. Wright, C. Wu, and Y. Zhou. *Hardness of Robust Graph Isomorphism, Lasserre Gaps, and Asymmetry of Random Graphs*, chapter 120, pages 1659–1677. 2014

<sup>2</sup> Brendan D. McKay. Practical graph isomorphism. In *Proceedings of the 1981 International Symposium on Mathematics*, pages 187–190. 1981.  
<sup>3</sup> Brendan D. McKay and Andrew Piperno. Practical graph isomorphism, ii. *J. Symb. Comput.*, 60:94–112, 2014

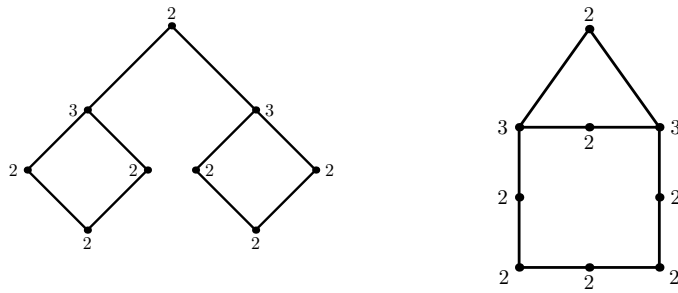


Figure 1: The first step of the color refinement algorithm, where vertices are labeled essentially with their degrees.

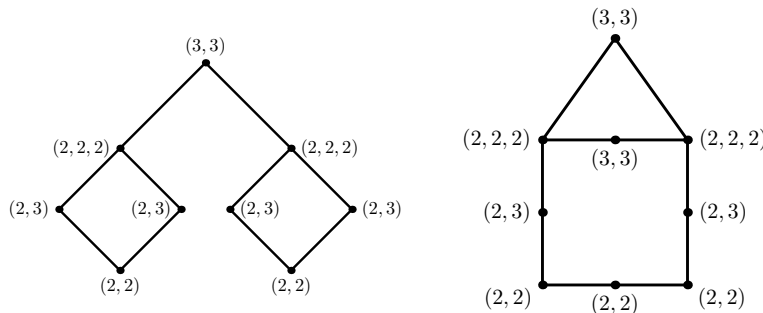


Figure 2: The second step of the color refinement algorithm. Observe that the number of vertices labeled (3,3) is different, and therefore the two graphs are not isomorphic.

The Weisfeiler-Lehman algorithm is an improvement of the basic color refinement algorithm. The algorithm takes a parameter  $k$ , and we denote the algorithm as  $WL^k$ . We could view it as running the color refinement algorithm on graph  $G^{(k)}$  and  $H^{(k)}$ , where for any graph  $G$ , define  $V(G^{(k)}) = V^k$ , and for all  $\{u, w\} \in E(G)$  and  $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k \in V(G)$ , we add the following edge to  $E(G^{(k)})$

$$\{(v_1, \dots, v_{i-1}, u, v_{i+1}, \dots, v_k), (v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_k)\}.$$

Instead of constructing the power graphs  $G^{(k)}$  and  $H^{(k)}$ , we could think of the algorithm as coloring subsets of  $k$  vertices.

For any  $k$ ,  $WL^k$  runs in time  $n^{k+O(1)}$ . It is known that for some constant  $k$ ,  $WL^k$  can distinguish random non-isomorphic graphs with high probability. Also, Grohe <sup>4</sup> proved that for every class of graphs with excluded minors, there is a  $k$  such that  $WL^k$  decides isomorphism of graphs in the class in polynomial time.

On the other hand, Atserias and Maneva <sup>5</sup> proved that

$$SA_k \leq WL^k \leq SA_{k+1}.$$

That is, the power of the  $k$ -level Weisfeiler-Lehman algorithm is sandwiched between neighboring levels of the canonical Sherali-Adams relaxation. Moreover, when  $k = 1$ , the Weisfeiler-Lehman algorithm is exactly the same power as the linear programming relaxation of the graph isomorphism problem.

It was also proved by Cai, Fürer and Immerman <sup>6</sup> that there are graphs for

<sup>4</sup> Martin Grohe. Fixed-point definability and polynomial time on graphs with excluded minors. *J. ACM*, 59(5):27:1–27:64, November 2012

<sup>5</sup> Albert Atserias and Elitza N. Maneva. Sherali-adams relaxations and indistinguishability in counting logics. *SIAM J. Comput.*, 42(1):112–137, 2013

<sup>6</sup> J.Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992. Scribe: Sangxia Huang

which distinguishing isomorphism with  $WL^k$  requires  $k = \Omega(n)$ .

We now define the meaning of two graphs being “far from” isomorphic.

**Definition 2.** For any  $0 \leq \alpha \leq 1$ , graphs  $G$  and  $H$  on  $n$  vertices, we say that a bijection  $\pi : V(G) \rightarrow V(H)$  is an  $\alpha$ -isomorphism if

$$\frac{|\{\{u, v\} \in E(G) \mid \{\pi(u), \pi(v)\} \in E(H)\}|}{\max\{|E(G)|, |E(H)|\}} \geq \alpha.$$

We say that  $G$  and  $H$  are  $\alpha$ -isomorphic if there is a bijection  $\pi$  such that  $\pi$  is an  $\alpha$ -isomorphism.

**Remark 3.** Note that since  $\pi$  is a bijection, the notion of  $\alpha$ -isomorphism of  $G$  and  $H$  is well defined.

For Theorem 1, we set  $\alpha = 1 - 10^{-18}$ , that is, we say that  $G$  and  $H$  are far from being isomorphic if they are at most  $(1 - 10^{-18})$ -isomorphic. In other words, any bijection between  $V(G)$  and  $V(H)$  must violate at least a fraction  $10^{-18}$  of the edges.

### The Reduction

We now define the reduction. We consider a random formula from  $3XOR(n, m)$  where we take  $m := cn$ , that is, a random  $3XOR$  formula with  $n$  variables and  $m$  equations.

For a given system of  $m$   $3XOR$  equations over  $n$  variables, the following process produces a graph on  $4m + 2n$  vertices with  $18m + n$  edges. The vertex set of the graph consists of two types of vertices: two variable vertices for each variable, labeled  $(x_i \leftarrow 0)$  and  $(x_i \leftarrow 1)$ , and for each clause  $x_{j_1} + x_{j_2} + x_{j_3} \equiv b_j \pmod{2}$ , 4 vertices corresponding to the 4 assignments to  $(x_{j_1}, x_{j_2}, x_{j_3})$  that satisfies the equation, labeled

$$C_j(x_{j_1} = a_{j_1}, x_{j_2} = a_{j_2}, x_{j_3} = a_{j_3}).$$

There is an edge between each pair of  $(x_i \leftarrow 0)$  and  $(x_i \leftarrow 1)$ . There are edges between clause variables corresponding to the same clause, so the 4 vertices corresponding to the same clause form a clique. And for each variable  $x_i$  that appears in clause  $j$  and a bit  $b \in \{0, 1\}$ , connect  $(x_i \leftarrow b)$  with  $C_j(x_{j_1} = a_{j_1}, x_{j_2} = a_{j_2}, x_{j_3} = a_{j_3})$  such that in clause  $j$  variable  $x_i$  is assigned value  $b$ .

The reduction uses the above process to produce two graphs: one from a random  $3XOR$  formula  $Ax = b$ , denoted as  $G_{Ax=b}$ , and another from the homogeneous version of it,  $Ax = 0$ , denoted as  $G_{Ax=0}$ .

The completeness of the reduction is given by the following lemma.

**Lemma 4.** If  $Ax = b$  has an assignment that satisfies  $(1 - \varepsilon)$ -fraction of the equations, then there exists a bijection  $\pi$  that is a  $(1 - \frac{2}{3}\varepsilon)$ -isomorphism between  $G_{Ax=b}$  and  $G_{Ax=0}$ .

*Proof.* Let  $y$  be an assignment that satisfies  $(1 - \varepsilon)$ -fraction of the equations in  $Ax = b$ . We define a bijection  $\pi$  as follows. For variable vertex  $(x_i \leftarrow b)$  in  $Ax = b$ ,  $\pi$  maps it to  $(x \leftarrow b \oplus y_i)$  in  $Ax = 0$ . For a clause  $C_j(x_{i_1} + x_{i_2} + x_{i_3} = b)$  satisfied by assignment  $y$ ,  $\pi$  maps  $C_j(x_{i_1} = b_1, x_{i_2} = b_2, x_{i_3} = b_3)$  to  $C_j(x_{i_1} = b_1 \oplus y_{i_1}, x_{i_2} = b_2 \oplus y_{i_2}, x_{i_3} = b_3 \oplus y_{i_3})$ . Note that since  $(b_1, b_2, b_3)$  is

a satisfying assignment for  $C_j$ , we have that  $b_1 + b_2 + b_3 = b = y_{i_1} + y_{i_2} + y_{i_3}$ , therefore this part of the mapping is well-defined. For an unsatisfied clause  $C_j$ , we map the 4 vertices corresponding to  $C_j$  in  $G_{Ax=b}$  to those corresponding to  $C_j$  in  $G_{Ax=0}$  in an arbitrary way.

Now we calculate the number of edges that are violated. The edges between variable vertices and the edges between clause vertices of a same clause is always preserved. The edges between variable vertices and clause vertices of satisfied clauses are also preserved. Therefore, at least  $n + 6m + (1 - \varepsilon)m \cdot 12 = n + 18m - 12\varepsilon m$  edges are satisfied by  $\pi$ .  $\square$

### Soundness of the Reduction

Recall that in previous lectures we studied the following  $PC_{>}$  refutation lower-bound.

**Lemma 5.** *For any  $c > 1$ , there exists  $\alpha > 0$ , such that with high probability  $3XOR(n, cn)$  requires  $\alpha n$ -degree  $PC_{>}$  refutation.*

To complete the reduction, we use the following two lemmas.

**Lemma 6.** *Let  $Ax = b$  be random formula from  $3XOR(n, cn)$ . If there is a refutation of  $G_{Ax=b} \cong G_{Ax=0}$  in degree  $r$ , then we can refute  $Ax = b$  in degree  $3r$ .*

**Lemma 7.** *Let  $c \geq 10^8$ . Then with high probability,  $G_{Ax=b}$  and  $G_{Ax=0}$  are not  $(1 - \frac{1}{95c^2})$ -isomorphic.*

In the rest of the lecture we prove Lemma 6. We will study Lemma 7 in the next lecture.

Now we formally define the axiom from which we derive refutation. For  $3XOR$ , we use the following encoding that we are already familiar with.

$$\begin{array}{ll} \forall i \in [n] & x_i^2 - x_i = 0 \\ \text{for constraint } x_{i_1} + x_{i_2} + x_{i_3} = b & \prod_{k=1}^3 (1 - 2x_{i_k}) = (-1)^b. \end{array}$$

We use the following natural encoding for graph isomorphism. The variables are  $\pi_{uv}$  for  $u \in V(G)$ ,  $v \in V(H)$ . The axioms are the following.

$$\begin{array}{ll} \forall u, v & \pi_{uv}^2 - \pi_{uv} = 0 \\ \forall u \in V(G) & \sum_{v \in V(H)} \pi_{uv} = 1 \\ \forall v \in V(H) & \sum_{u \in V(G)} \pi_{uv} = 1 \\ \forall \{u, u'\} \in E(G) & \sum_{\{u, v\} \in E(H)} \pi_{uv} \pi_{u'v} = 1 \end{array}$$

Suppose now that we have a degree  $r$  refutation for “ $G_{Ax=b} \cong G_{Ax=0}$ ”. To get a refutation for  $Ax = b$ , the main idea is to substitute  $\pi_{uv}$  with polynomials of  $x_i$ 's of degree 3. We then argue that we can derive the axioms of graph isomorphism after substitution from the axioms of  $3XOR$ . This proves Lemma 6 because we can take the refutation for “ $G_{Ax=b} \cong G_{Ax=0}$ ”, substitute the  $\pi_{uv}$ 's in each line with  $x_i$ 's and get a proof starting from the  $3XOR$  axioms, and since in the end we have  $-1 \geq 0$  which remains the same after substitution, this gives a refutation for  $Ax = b$ . And because we are substituting each  $\pi_{uv}$  with a polynomial of degree at most 3, the total degree of the refutation for  $Ax = b$  is no more than  $3r$ .

The substitution is in fact rather straightforward and intuitively similar to that in Lemma 4. We consider mappings between different types of vertices. For simplicity of notation, for any bits  $b, b' \in \{0, 1\}$  and 3XOR variable  $x$ , define  $I[b, b', x]$  as

$$I[b, b', x] = \begin{cases} x & \text{if } b \neq b' \\ 1 - x & \text{if } b = b' \end{cases}$$

For two variable vertices  $(x_i \leftarrow b)$  and  $(x_i \leftarrow b')$ , we define

$$\pi_{(x_i \leftarrow b)(x_i \leftarrow b')} = I[b, b', x_i].$$

For clause variables  $u = C_j(x_{i_1} = b_1, x_{i_2} = b_2, x_{i_3} = b_3)$ ,  $v = C_j(x_{i_1} = b'_1, x_{i_2} = b'_2, x_{i_3} = b'_3)$ , define

$$\pi_{uv} = I[b_1, b'_1, x_{i_1}] \cdot I[b_2, b'_2, x_{i_2}] \cdot I[b_3, b'_3, x_{i_3}].$$

All other variables are substituted with 0.

Now we verify that the graph isomorphism axioms after substitution are derivable from the 3XOR axioms.

$\pi_{uv}^2 - \pi_{uv} = 0$ . This is easy since either  $\pi_{uv}$  is substituted by 0, or by a product of  $I[b, b', x]$ 's, which is 0/1-valued.

$\sum_{v \in V(H)} \pi_{uv} = 1$  for any  $u \in V(G)$ . We consider two cases, when  $u$  is a variable vertex, and when  $u$  is a clause vertex.

Suppose that  $u = (x_i \leftarrow b)$ . Then only  $\pi_{(x_i \leftarrow b)(x_i \leftarrow b)}$  and  $\pi_{(x_i \leftarrow b)(x_i \leftarrow 1-b)}$  is not substituted by 0, and it is clear that they sum to 1.

Suppose now that  $u = C_j(x_{i_1} = b_1, x_{i_2} = b_2, x_{i_3} = b_3)$ . For  $\pi_{uv}$  to be nonzero, it must be that  $v$  is also a clause variable of  $C_j$ . Observe that if we expand the following

$$\sum_{b'_1 \oplus b'_2 \oplus b'_3 = b_1 \oplus b_2 \oplus b_3} \pi_{uv} = 1,$$

we get exactly the XOR constraint (multiplied by a constant factor).

$\sum_{u \in V(G)} \pi_{uv} = 1$  for any  $v \in V(H)$ . Similar to the case above.

For any  $\{u, u'\} \in E(G)$ ,  $\sum_{\{v, v'\} \in E(H)} \pi_{uv} \pi_{u'v'} = 1$ . We need to consider different types of edges in  $E(G)$ .

The edges between variable vertices are easy and the details are left as an exercise.

If  $\{u, u'\}$  is an edge between clause variables of the same clause  $C_j$  on variable  $x_{i_1}, x_{i_2}, x_{i_3}$ , then the only  $v, v'$ 's for which  $\pi_{uv} \pi_{u'v'}$  is nonzero are those corresponding to clause  $C_j$  in  $Ax = 0$ . Suppose  $u$  assigns  $(a_1, a_2, a_3)$  to  $(x_{i_1}, x_{i_2}, x_{i_3})$ , and  $u'$  assigns  $(a'_1, a'_2, a'_3)$ . Similarly, suppose that  $v$  assigns  $(b_1, b_2, b_3)$  and  $v'$  assigns  $(b'_1, b'_2, b'_3)$ . We must have that  $a_j \oplus b_j = a'_j \oplus b'_j$ , otherwise  $\pi_{uv} \pi_{u'v'}$  contains the factor  $x_{i_j}(1 - x_{i_j})$  which can be proved to be zero from the basic axioms. Otherwise, we will just get  $\pi_{uv} \pi_{u'v'} = \pi_{uv}^2 = \pi_{uv}$  and we just use the conclusion from above.

Finally we need to consider when  $u$  is a variable vertex  $(x_i \leftarrow a)$ , and  $u'$  is a clause vertex in  $Ax = b$ , denoted as  $C_j(x_{i_1} = a_1, x_{i_2} = a_2, x_{i_3} = a_3)$  and

without loss of generality assume that  $i = i_1$ . Then in the summation, the only non-zero terms are those where  $v$  is a variable vertex ( $x_i \leftarrow b$ ), and  $v'$  is a clause variable in  $Ax = 0$ , denoted as  $C_j(x_{i_1} = b_1, x_{i_2} = b_2, x_{i_3} = b_3)$ . Similar as in the previous case, we need to have  $a \oplus b = a_1 \oplus b_1$ , and therefore we can think of the summation as over the assignments that satisfies  $x_{i_1} + x_{i_2} + x_{i_3} = 0$ , and we have

$$\begin{aligned}
 & \sum_{\{v,v'\} \in E(H)} \pi_{uv} \pi_{u'v'} \\
 = & \sum_{b_1, b_2, b_3} I[a, a \oplus a_1 \oplus b_1, x_{i_1}] I[a_1, b_1, x_{i_1}] I[a_2, b_2, x_{i_2}] I[a_3, b_3, x_{i_3}] \\
 = & \sum_{b_1, b_2, b_3} I[a_1, b_1, x_{i_1}] I[a_2, b_2, x_{i_2}] I[a_3, b_3, x_{i_3}] \\
 = & \sum_{u'v'} \pi_{u'v'} = 1.
 \end{aligned}$$

## References

- [ ] Albert Atserias and Elitza N. Maneva. Sherali-adams relaxations and indistinguishability in counting logics. *SIAM J. Comput.*, 42(1):112–137, 2013.
- [ ] J.Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.
- [ ] Martin Grohe. Fixed-point definability and polynomial time on graphs with excluded minors. *J. ACM*, 59(5):27:1–27:64, November 2012.
- [ ] Brendan D. McKay. Practical graph isomorphism. *Congressus Numerantium*, 30:45–87, 1981.
- [ ] Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, ii. *J. Symb. Comput.*, 60:94–112, 2014.
- [ ] R. O’Donnell, J. Wright, C. Wu, and Y. Zhou. *Hardness of Robust Graph Isomorphism, Lasserre Gaps, and Asymmetry of Random Graphs*, chapter 120, pages 1659–1677. 2014.