PROOF COMPLEXITY AS A COMPUTATIONAL LENS
LECTURE 11: GRAPH COLOURING

Graph $G = (V, E)$ Finite, undirected, no self-loops or multi-edges

Valid **k-COLOURING** of G is $\chi : V \to [k]$ s.t. $\chi(u) \neq \chi(v)$ for all edges $(u,v) \in E$

One of the classic 21 NP-complete problems considered by [Karp '72]:

GRAPH COLOURING: Given $G = (V,E)$ and $k \in \mathbb{N}^+$, does G have a valid k-colouring?

NP-complete for fixed $k \geq 3$

$\chi(G)$ **CHROMATIC NUMBER**: Min k such that G has valid k-colouring

Best approximation algorithm computes $\chi(G)$ to within factor $O(n (\log \log n)^2 / (\log n)^3)$ [Halldórsson '93]

Approximating to within factor $n^{1-\varepsilon}$ is NP-hard [Zuckerman '07]

Given promise that graph G is 3-colourable, best polynomial-time algorithm needs $O(n^{0.19996})$ colours [Kawarabayashi & Thorup '17]

Lower bounds: NP-hard to $(2k-1)$-colour a k-colourable graph. Open whether colouring 3-colourable graphs with 6 colours is NP-hard

What about unconditional lower bounds?
[McDiarmid '84] developed method that covers many algorithms used for random graphs
[Beame, Culberson, Mitchell, Moore '05]:
- This is captured by resolution proof system
- Average-case exponential resolution size lower bounds for proofs of non-k-colourability for random graphs that are not k-colourable asymptotically almost surely (a.a.s.)

Algebraic approaches based on Nullstellensatz and Gröbner bases: Very good results in papers by De Loera, Margulies, et al ['08, '09, '11, '15]

[De Loera, Lee, Margulies, Onn '09]
Often constant-degree Nullstellensatz proofs!

For a long time best degree lower bound $k+1$ for k-colouring [De Loera et al. '15]

Optimal $\Omega(n)$ degree lower bounds for polynomial calculus in [Lauria & Nordström '17] via reduction from FPHP(G)

More general reduction framework by [Atserias & Ochremiak '19] — works also for Sherali-Adams and sum-of-squares
But only worst-case bounds for specific constructions of graphs

Can we get average-case lower bound as for resolution in [BCMM '05]?

Sum of squares only needs degree 2 to show that random d-regular graphs are not k-colourable a.a.s. when $d \geq 4k^2$
[Banks, Kleinberg, & Moore '19]

Topic of today's lecture:

THEOREM [Conneryd, de Rezende, Nordström, Pang, Risse '23]
For any $d \geq 6$, polynomial calculus requires degree $\Omega(n)$ a.a.s. to show that random d-regular graphs $\sim G_{n,d}$ and Erdős-Rényi random graphs $\sim G(n, d/n)$ are not 3-colourable.

In today's lecture:
- lower bounds for 4-colouring, not 3-colouring
- hold only for random regular graphs

Just to avoid some technical complications — all the main ingredients are there

Lower bounds hold in any field

But we need to make precise what encoding we are considering

Work in multilinear setting

$$\mathbb{F}[\vec{x}] / \{ x_j^2 - x_j \mid j \in [n] \}$$

Variables $x_{v,i}$ $v \in V$, $i \in [k]$

$x_{v,i} = 1 \iff$ "vertex v has colour i"

System of polynomials $Col(G,k)$ consists of

$$\sum_{i=1}^{k} x_{v,i} - 1 \qquad v \in V \qquad \text{COLOUR AXIOM}$$

$$x_{v,i} \cdot x_{v,i'} \qquad v \in V,\ i \neq i' \in [k] \qquad \text{FUNCTIONALITY AXIOM}$$

$$x_{u,i} \cdot x_{v,i} \qquad (u,v) \in E,\ i \in [k] \qquad \text{EDGE AXIOM}$$

(Results also hold for CNF encoding)

(Note that today we have $1 = \text{true}$
Doesn't really matter, but makes encoding simpler ...)

Another encoding popular in computational algebra by [Bayer '82]

Suppose field $\mathbb{F}$ contains primitive kth root of unity ω

$\{1, \omega, \omega^2, \ldots, \omega^{k-1}\}$ all distinct

$\omega^k = 1$

Variable y_v for $v \in V$

$y_v = \omega^j \iff$ "vertex v has colour j"

$$y_v^k - 1$$

$$\sum_{j=0}^{k-1} (y_u)^j (y_v)^{k-1-j} \qquad (u,v) \in E$$

$\mathbb{F}$ must contain kth root of unity
$\text{char}(\mathbb{F}) = 0$ or $\text{char}(\mathbb{F}) \nmid k$.

Focus on $\{0,1\}$-encoding

Degree lower bounds $\Rightarrow$ size lower bounds [IPS'99]

Degree lower bounds also hold for Bayer's encoding

$\{0,1\}$-degree $\leq d \Rightarrow$ Bayer degree $\leq \max\{k, d\}$

[Lauria & Nordström '17]

Prove degree lower bounds by designing pseudo-reduction operator

LEMMA [Razborov '98]

Let $\mathcal{P}$ set of multilinear polynomials, $D \in \mathbb{N}^+$

If there exists a degree-D pseudo-reduction operator R, i.e., an $\mathbb{F}$-linear operator over multilinear polynomials such that

(1) $R(f) = 0$ for $f \in \mathcal{P}$;

(2) for term t of degree $< D$ and any x

$R(xt) = R(xR(t))$;

(3) $R(1) \neq 0$;

then $\mathrm{Deg}_{PC}(\mathcal{P} \vdash 1) > D$

The lemma is true since for any PC derivation in degree $\leq D$, it is straightforward to show that R maps all derived polynomials p to $R(p) = 0$, so no such derivation can reach contradiction 1.

How to construct pseudoreduction operator?

For every monomial m, construct subset $S(m) \subseteq P$ and define

$$R(m) = R_{\langle S(m) \rangle}(m)$$

+ extend by linearity

Recall that we can define admissible order on monomials, e.g., degree-lex

$$x_4 x_5 \prec x_2 x_3 x_4 \prec x_2 x_3 x_5 \prec x_1 x_2 x_3 x_4$$

$LT(p)$ = largest term in p LEADING TERM

t is reducible mod ideal I if $\exists\, g \in I$ s.t. $t = LT(g)$

Any p can be written uniquely as

$$p = g + r$$

for $g \in I$ and r sum of irreducible terms mod I

$$R_I(p) = r$$

Construct $S(m)$ so that two lemmas hold

SIZE LEMMA If $\deg(t)$ is not too large, then $|S(m)|$ is not too large

"Heart of the proof lemma"

REDUCTION LEMMA If $u \in S(m)$ and $|u|$ not too large, then m is reducible mod $\langle u \rangle$ iff m is reducible mod $\langle S(m) \rangle$

The proof that R is a pseudo-reduction operator then goes like this

Template proof

(3) $\underline{R(1) \neq 0}$ 1 has small degree $\Rightarrow$

$S(1)$ is not too large $\Rightarrow$

$S(1)$ is satisfiable $\Leftrightarrow$

$1 \notin \langle S(1) \rangle$ $\Leftrightarrow$

$R_{\langle S(1) \rangle}(1) = 1 \neq 0$

(1) $\underline{R(f) = 0 \text{ for } f \in P}$

Let $m_f^* = \prod_{x \in Vars(f)} x$

$Deg(m_f^*)$ not too large

For $f = \sum_i t_i$ we get

$$\begin{aligned} R(f) &= R\left(\sum_i t_i\right) \\ &= \sum_i R(t_i) && [\text{linearity}] \\ &= \sum_i R_{\langle S(t_i) \rangle}(t_i) && [\text{definition}] \\ &= \sum_i R_{\langle S(m_f^*) \rangle}(t_i) && [\text{Repeated use of reduction lemma}] \\ &= R_{\langle S(m_f^*) \rangle}\left(\sum_i t_i\right) && [\text{linearity}] \\ &= R_{\langle S(m_f^*) \rangle}(f) \\ &= 0 \end{aligned}$$

since we argue that $f \in S(m_f^*)$.

② $R(xt) = R(xR(t))$

Start with right-hand side and write

$$R(xR(t)) = R\left(x \sum_{t' \in R(t)} t'\right) \quad \text{[unpacking]}$$

$$= \sum_{t' \in R(t)} R(xt') \quad \text{[linearity]}$$

$$= \sum_{t' \in R(t)} R_{\langle S(xt') \rangle}(xt') \quad \text{[definition]}$$

$$= \sum_{t' \in R(t)} R_{\langle S(xt) \rangle}(xt') \quad \text{[Reduction lemma plus some technicalities]}$$

$$= R_{\langle S(xt) \rangle}\left(\sum_{t' \in R(t)} xt'\right) \quad \text{[linearity]}$$

$$= R_{\langle S(xt) \rangle}\left(x \cdot R(t)\right) \quad \text{[packing]}$$

$$= R_{\langle S(xt) \rangle}\left(x \cdot R_{\langle S(t) \rangle}(t)\right) \quad \text{[definition]}$$

$$= R_{\langle S(xt) \rangle}(x \cdot t)$$

by properties of ideal reductions since $\langle S(xt) \rangle \supseteq \langle S(t) \rangle$

So all we need to do is to associate ~~m~~ with set $\subseteq Col(G,k)$ and show size & reduction lemmas

Natural to take $S(m) = Col(G[V(m)], k)$

$G[U]$ subgraph of G induced on U

Why did reduction lemma work before?

Imprecise proof sketch:

Take $\mathcal{U}' \supseteq S(m)$. Suppose m reducible mod $\mathcal{U}$

Write

$$m = \sum_{p \in S(m)} c_p \cdot p + \sum_{q \in \mathcal{U}' \setminus S(m)} c_q \cdot q + \sum r_k \qquad (\dagger)$$

Find ρ such that

- $\mathrm{dom}(\rho) \cap (\mathrm{Vars}(m) \cup S(m)) = \emptyset$
- $\rho(q) = 0$ for $q \in \mathcal{U}' \setminus S(m)$
- $r_k \downarrow \rho$ still irreducible (automatic)

Apply ρ to $(\dagger)$ to get

$$m = \sum_{p \in S(m)} c_p \downarrow \rho \cdot p + \sum_k r_k \downarrow \rho$$

So m reducible mod $S(m)$.

Problem: For colouring, $\mathcal{U}$ can contain neighbours of $V(m)$

If ρ colours neighbours of $V(m)$, then constraints on $V(m)$ affected

Solution: ρ doesn't have to be assignment.

Can be affine substitution as long as

- $q \downarrow \rho$ either $= 0$ or $\in \langle S(m) \rangle$
- ρ maps terms t to smaller terms $\in \downarrow \rho$

Recall also for multilinear polynomial q and polynomial set Q

col XL

$$Q \vdash q \iff q \in \langle Q \rangle$$

We need to choose ordering very carefully

Idea from [Romero & Tunçel '24] (arXiv '22)

- Colour G with $\chi(G)$ colours $\leq d$ for d-regular random graph
- Order vertices w.r.t. colour classes $u \prec v$ if $\chi(u) \prec \chi(v)$

Order variables $x_{v,1} \prec x_{v,2} \prec x_{v,3} \prec \dots$ and $x_{u,i} \prec x_{v,j}$ iff $u \prec v$

Path $(v_1, v_2, \dots, v_\ell)$ is INCREASING [DECREASING] if $v_i \prec v_{i+1}$ [$v_i \succ v_{i+1}$] for all i.

v is DESCENDANT of u if $\exists$ decreasing path $u \rightsquigarrow v$

$D_u = \{$ all descendants of $u \in U \}$

$\mathrm{Desc}(U)$ = DESCENDANTS GRAPH of U = induced subgraph $G[U \cup D_U]$

A τ-HOP w.r.t $U \subseteq V$ is simple path/cycle (No repetitions) of length τ such that
- both endpoints in U
- all other vertices of path in $V \setminus U$

τ-hop w.r.t $G[U]$ = τ-hop w.r.t U

$G[U] = (U, E \cap U \times U)$

No i-hops	Structure of $N(U)$
$i=2$	Every $v \in N(U)$ has single neighbour in U
$i=3$	$N(U)$ is independent set

To find $S(m) \leq Col(G,k)$, do following
- start with $V(m) = \{v \mid x_{v,i} \in Vars(m)\}$
- include all descendants
- make vertex set $\{2,3\}$-hop-free

DEFINITION 1: CLOSURE [Romero & Tunçel]
Given $U \subseteq V(G)$, do the following

$i := 0$
$H_0 := Desc(U)$
while exists $\{2,3\}$-hop Q_{i+1} w.r.t. H_i
  $H_{i+1} := Desc(V(H_i) \cup V(Q_{i+1}))$
  $i := i+1$
$CL(U) := V(H_i)$

This defines the CLOSURE $CL(U)$ of U

LEMMA 2
For any graph $G=(V,E)$ with linear order on V:
(1) $CL(U)$ is uniquely defined
(2) $U \subseteq CL(U)$
(3) $U \subseteq U' \Rightarrow CL(U) \subseteq CL(U')$ MONOTONICITY
(4) $CL(CL(U)) = CL(U)$ IDEMPOTENCY

Proof of Lemma 2

(2) & (4) immediate. Exercise to prove (1) & (3) by induction

□

The closure of a monomial m is

$$\boxed{Cl(m) := Cl(V(m))}$$

(For term $t = \alpha \cdot m$, $Cl(t) = Cl(m)$)

Our subset $S(m) \subseteq Col(G, k)$ is going to be $Col(G[Cl(m)], k)$

For brevity, let us write for $U \subseteq V$

$$I(U) = \langle Col(G[U], k) \rangle$$

Then we define

$$\boxed{R(m) = R_{I(Cl(m))}(m)}$$

($R(\alpha m) = \alpha \cdot R(m)$)

We now need to prove size and reduction lemmas. The following observation makes the size lemma believable

OBSERVATION 3

If $G = (V, E)$ has V ordered by a valid colouring $\chi : V \to [c]$, then every increasing/decreasing path has length $\leq c - 1$

If G has max degree d, then

$$\boxed{|V(Desc(U))| \leq 2 d^{c-1} |U|}$$

We also need to argue that adding $\{2,3\}$-hops doesn't increase the closure too much. For this, we need to use that

(a) random graphs are sparse

(b) adding $\{2,3\}$-hops rapidly increases density.

Some graph notation

$E(U,W) = \{(u,w) \mid u \in U, w \in W, (u,w) \in E\}$

$E(U) = E(U,U)$

For Tseitin we had $s = |V|/2$

Say that $G=(V,E)$ is an (s,δ)-EDGE EXPANDER if $\forall U \subseteq V, |U| \leq s \mid E(U, V \setminus U)| \geq \delta |U|$

Say that $G=(V,E)$ is (s,ε)-SPARSE if $\forall U \subseteq V, |U| \leq s \mid E(U)| \leq (1+\varepsilon)|U|$

For d-regular graphs, the two notions are equivalent

$$(s,\varepsilon)\text{-sparse} \iff (s, d-2(1+\varepsilon))\text{-expander}$$

We want to use

- random graphs are sparse
- small subgraphs of sparse graphs are 3-colorable
- small subsets of sparse graphs have small closures

LEMMA 4 (SPARSITY LEMMA)
$\exists$ constant $\delta > 0$ s.t. for $n, d \geq 3$,
$\varepsilon > \delta d^2 / \log n$ s.t. $\varepsilon = \omega(1/\log n)$,
if $G \sim G_{n,d}$ or $G \sim G(n, d/n)$, then
G is $(d^{-30(1+\varepsilon)/\varepsilon} \cdot n, \varepsilon)$-sparse
asymptotically almost surely

Proof Calculations.

LEMMA 5
If $G = (V, E)$ is (s, ε)-sparse for $\varepsilon < 1/2$,
then $\forall U \subseteq V$, $|U| \leq s$, it holds that
$G[U]$ is 3-colourable.

Proof
By induction on $|U|$.
Base case $|U| = 1$ obvious.
Consider U s.t. $|U| \leq s$
Average degree in $G[U]$ is
$$\frac{2|E(U)|}{|U|} \leq 2(1+\varepsilon) < 3 \quad \text{by sparsity}$$
so $\exists u$ of degree < 3
Colour $U \setminus \{u\}$ by induction, then colour u. ∎

But the chromatic number of random G is large, though not too large

LEMMA 6 [Kemkes, Pérez-Giménez, & Wormald '10]
[Achlioptas & Naor '05]
For $G \sim G_{n,d}$ or $G \sim G(n, d/n)$, it holds asymptotically almost surely that:
- $\chi(G) \leq 2d / \log d$
- if $d \geq 10$, then $\chi(G) \geq 5$

THEOREM 7

There exists constant $\delta > 0$ such that for all integers n and d satisfying $\delta d^3 / \log d < \log n$ it holds for $G \sim G_{n,d}$ and integer $k \geq 4$ that

$$\mathrm{Deg}_{PC}(\mathrm{col}(G,k) \vdash \bot) \geq 2^{-O(d)} \cdot n$$

Constant $d \Rightarrow$ degree $\Omega(n) \Rightarrow$ size $\exp(\Omega(n))$

LEMMA 8 (SIZE LEMMA)

Suppose for $G = (V,E)$ that
- max vertex degree $\leq d$
- $\chi(G) \leq c$
- G is $(s, 1/4c)$-sparse.

Then $\forall U \subseteq V$, $|U| \leq s/20c$, it holds that $|CL(U)| \leq 40 d^{c-1} |U|$

Proof sketch

Descendant graph is not too large by Observation 3

Adding 2-hops / 3-hops increases density

G is sparse. (Otherwise get small set that contradicts sparsity)

Iterative procedure to construct closure terminates after $O(|U|)$ steps △ □

Given that we believe the Size Lemma, all that remains to prove is the Reduction Lemma with associated technicalities.