Lecture 7 (Ulrich Complexity)

Wednesday, 14 June 2023 12:43

How do you resolve VP vs VNP (so far):

① Prove you cannot or can compute the perm in poly time, or analyze circuit size of the perm.

② Either a polynomial u.b. or superpoly l.b on dc(perm)

③ Specific bounds on the size of bounded depth circuits

④ Bounding no. of zeros of "fewnomials"

Today we will see Ulrich Complexity → Can prove VP = VNP
→ can be thought of in Co-ordinate free way

Defn [Ulrich Complexity (Bläser. Eisenbud. Schreyer)] The Ulrich complexity of a hom. poly $f \in k[X_0 \ldots X_n]$ of degree d is the smallest 'r' s.t there is a matrix M of linear forms s.t.

$$\det(M) = f^r, \text{ and}$$

$$\exists N \quad M.N = f.Id_{dr}$$

notice $\underset{d}{\text{degree } f} \times r = \text{size}(M)$, so instead of size(M), you might as well study $\text{size}(M)/d = r$.

(*) The second condition brings us into the domain of Ulrich modules & Ulrich sheaves

(*) $uc(\det) = 1$ [N is the matrix of co-factors]

Conjecture $uc(f) \geq 2^{(\lceil \operatorname{codim} \underbrace{\operatorname{sing}}_{\text{Singular locus}} f/2 \rceil - 2)}$ for all f.

(*) Fact $\operatorname{codim} \operatorname{sing} \det_n = 4$, so above predicts

(*) Fact codim sing $\det_n = 4$, so above predicts
$uc(\det_n) \geq 1$ ✓

(*) Conjectured codim sing $\mathrm{per}_n = 2n$. This gives:

Conjecture $uc(\mathrm{perm}_n) \geq 2^{n-2}$ (true for $n=2$ & $n=3$)

Thm Poly(n) u.b. on $uc(\mathrm{perm}_n) \implies VP = VNP$
"over all fields"

errata: in the original paper, it was stated as sub-exponential

Defn [Ulrich bundles] Let $X \subseteq \mathbb{P}^n$ be a smooth proj. variety, of degree d.
A rank r vector bundle E on X is Ulrich if any of the foll. equiv. conds are satisfied
① The cohomology $H^{\cdot}(X, E(-p))$ vanish $1 \leq p \leq \dim(X)$
② If $\pi : X \to \mathbb{P}^{\dim(X)}$ is a finite linear proj., then $\pi_* E$ is trivial.

Defn [Ulrich Complexity] $f \in k[X_0, \ldots X_n]$ homogeneous defining $X \subseteq \mathbb{P}^n$. The Ulrich complexity of f is the min 'r' s.t there exists a rank r Ulrich bundle on X.

Defn [linear matrix factorization] $f \in k[X_0 \ldots X_n]$ hom of degree $d \geq 2$. 'f' has a matrix factorization of size 'm' if $\exists\, \alpha_1 \ldots \alpha_d \in M_m(k)$ with entries as linear forms

$$f I_m = \alpha_1 \cdots \alpha_d$$

Defn [Waring rank, Chow rank] $f \in k[X_0 \ldots X_n]$ of degree d
wr(f) is the min s.t there exists

$$f = \sum_{i=1}^{wr(f)} l_i^d \quad ; l_i \text{ linear forms}$$

Chow rank, denoted ch(f) is the min s.t there exists an expression

$$f = \sum^{ch(f)} l_{i_1} \cdots l_{i_d}$$

Chow rank, ...

$$f = \sum_{i=1}^{Ch(f)} l_{i,1} \cdots l_{i,d}$$

<u>Thm</u> ① f has a linear matrix factorization of size $d^{Ch(f)-1}$, and of size $d^{Ch(f)-1}$

② f has linear mat. fact. of size $m \implies$ hyp supports an Ul. bundle of rank $\leq \frac{m}{d}$

U.C. Can be studied by looking at secant varieties of Veronese/Chow varieties

Lecture 7 (GCT)

Wednesday, 14 June 2023 12:45

"String theory of Comp science"

GCT publications:

Overviews of GCT

- The GCT program toward the P vs. NP problem, CACM, vol. 55, issue 6, June 2012, pp. 98-107.
- On P vs. NP, and Geometric Complexity Theory, JACM, vol. 58, issue 2, April 2011.
- FOCS 2010 Tutorial based on this overview.

GCT Papers

- Lower Bounds in a Parallel Model without bit operations, SIAM J. Comput., 28, (1999), pp. 1460-1509.
- Geometric complexity theory I: An approach to the P vs. NP and related problems (with M. Sohoni), SIAM J. Comput., vol 31, no. 2, pp. 496-526, (2001).
- Geometric complexity theory II: Towards explicit obstructions for embeddings among class varieties (with M. Sohoni) , SIAM J. Comput., Vol. 38, Issue 3, June 2008.
- Geometric complexity theory, P vs. NP and explicit obstructions (with M. Sohoni), in "Advances in Algebra and Geometry", Edited by C. Musili, the proceedings of the International Conference on Algebra and Geometry, Hyderabad, 2001.
- Geometric complexity theory III: on deciding nonvanishing of a Littlewood-Richardson coefficient (with H. Narayanan and M. Sohoni), Journal of Algebraic Combinatorics, pages 1-8, November, 2011.
- Geometric complexity theory IV: nonstandard quantum group for the Kronecker problem (with J. Blasiak and M. Sohoni), to appear in Memoirs of American Mathematical Society. Preprint available as arXiv:cs/0703110[cs.CC], June 2013.
- Geometric Complexity Theory V: Efficient algorithms for Noether normalization, to appear in the Journal of the AMS.
- Explicit Proofs and The Flip, Technical Report, Computer Science Department, The University of Chicago, September 2010.
- Geometric Complexity Theory VI: the flip via positivity, Technical Report, computer science department, The University of Chicago, January 2011.
- Geometric Complexity Theory VII: Nonstandard quantum group for the plethysm problem, Technical Report TR-2007-14, computer science department, The University of Chicago, September, 2007.
- Geometric Complexity Theory VIII: On canonical bases for the nonstandard quantum groups, Technical Report TR-2007-15, computer science department, The University of Chicago, September, 2007.

Lecture notes on GCT

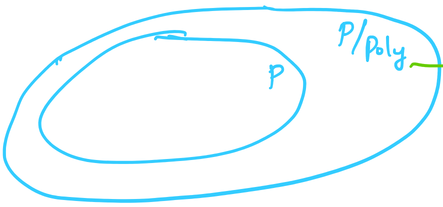
- On P vs. NP, Geometric Complexity Theory, and the Riemann Hypothesis, Technical Report, Computer Science department, The University of Chicago, August, 2009. cs.ArXiv preprint cs.CC/0908.1936

This overview is based on a series of three lectures. Video lectures in this series are available here.

- Geometric Complexity Theory: Introduction (with M. Sohoni), Technical Report TR-2007-16, computer science department, The University of Chicago, September, 2007. Lecture notes for an introductory graduate course on geometric complexity theory in the computer science department, the university of Chicago.
- On P vs. NP, Geometric Complexity Theory, and The Flip I: a high-level view, Technical Report TR-2007-13, computer science department, The University of Chicago, September, 2007.

Introduced by Mulmuley - Sohoni

* GCT-ish approach viable P vs NP



→ non-uniform $P \subsetneq P/poly$

Thus if $NP \not\subseteq P/poly \Rightarrow P \neq NP$

Example of an alg. in P/poly (Miller-Rabin primality test)

1. ^ a b Miller, Gary L. (1976), "Riemann's Hypothesis and Tests for Primality", *Journal of Computer and System Sciences*, **13** (3): 300–317, doi:10.1145/800116.803773, S2CID 10690396
2. ^ a b Rabin, Michael O. (1980), "Probabilistic algorithm for testing primality", *Journal of Number Theory*, **12** (1): 128–138, doi:10.1016/0022-314X(80)90084-0

Testing against small sets of bases [edit]

When the number n to be tested is small, trying all $a < 2(\ln n)^2$ is not necessary, as much smaller sets of potential witnesses are known to suffice. example, Pomerance, Selfridge, Wagstaff[4] and Jaeschke[11] have verified that

- if n < 2,047, it is enough to test a = 2;
- if n < 1,373,653, it is enough to test a = 2 and 3;
- if n < 9,080,191, it is enough to test a = 31 and 73;
- if n < 25,326,001, it is enough to test a = 2, 3, and 5;
- if n < 3,215,031,751, it is enough to test a = 2, 3, 5, and 7;
- if n < 4,759,123,141, it is enough to test a = 2, 7, and 61;
- if n < 1,122,004,669,633, it is enough to test a = 2, 13, 23, and 1662803;
- if n < 2,152,302,898,747, it is enough to test a = 2, 3, 5, 7, and 11;
- if n < 3,474,749,660,383, it is enough to test a = 2, 3, 5, 7, 11, and 13;
- if n < 341,550,071,728,321, it is enough to test a = 2, 3, 5, 7, 11, 13, and 17.

Using the work of Feitsma and Galway enumerating all base 2 pseudoprimes in 2010, this was extended (see OEIS: A014233), with the first result shown using different methods in Jiang and Deng:[12]

- if n < 3,825,123,056,546,413,051, it is enough to test a = 2, 3, 5, 7, 11, 13, 17, 19, and 23.
- if n < 18,446,744,073,709,551,616 = 2^{64}, it is enough to test a = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37.

Sorenson and Webster[13] verify the above and calculate precise results for these larger than 64-bit results:

- if n < 318,665,857,834,031,151,167,461, it is enough to test a = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, and 37.

high-level overview of GCT: Consider NP vs P/Poly as a means towards P vs NP. Construct, for each n, alg. varieties

$$X_{NP,n} \quad \& \quad X_{P,n}, \quad \text{such that}$$

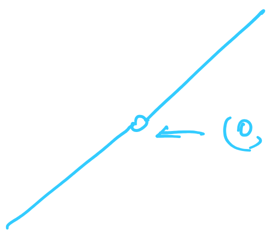
$$P \geq NP \iff X_{NP,n} \subseteq X_{P,n^k} \quad \forall\, n \geq n_0 \text{ \& some } k$$

Make sure $X_{NP,n}$ & $X_{P,n}$ are symmetric under the action of GL_n, so use tools from representation theory

Orbit closures Consider the action of $\mathbb{R}^\times$ on $\mathbb{R}^2$.

$$\underset{\substack{\cap \\ \mathbb{R}^\times}}{a} . (x,y) = (ax, ay).$$

What is the orbit of $(1,1)$



(0,0) is excluded

Orbit is not an alg. set.

CLASSICAL COMPLEXITY	GCT
A problem/funct. to be computed	pt. on an alg. variety

A problem/funct. to be computed	
$f \sim g$	pt_f & pt_g lie in the same GL-orbit
$\Downarrow$ Reduction b/w f & g	$\Downarrow$ action of a group element
Reduction b/w arbitrary elems	actions of limits of group elements
$\Downarrow$ $f \leq g$	$\Downarrow$ f lies in $\overline{G.g}$ → orbit closure

$V = (\mathbb{C}^{m^2})^*$, $\mathrm{End}(V)$ acts on $\mathrm{Sym}^m(V)$ ← degree m hom. poly in m^2 vars.

$$L.\, p(x) = p(L^T x)$$

End(V) is not a group!

<u>Defn</u> [Padded n-perm] $\quad z^{m-n}\,\mathrm{perm}_n \in \mathrm{Sym}^m(V)$

<u>Prop</u> $\quad dc(\mathrm{perm}_n) \leq m = n^{O(1)} \iff \mathrm{End}(V).\det_m \ni z^{m-n}\,\mathrm{perm}_n$

$GL(V)$ ← group of invertible linear transformations $\subseteq \mathrm{End}(V)$, dense in $\mathrm{End}(V)$, i.e. $\overline{GL(V)} = \mathrm{End}(V)$

$\Downarrow$

$A \in \mathrm{End}(V) \setminus GL(V)$, there exists $(A_i)_{\in GL(V)}$ s.t.

$$\lim_{i \to \infty} A_i = A$$

$GL(V).\det_m$ is dense in $\mathrm{End}(V).\det_m$

↑ group orbit

$$DET_m := \overline{GL(V).\det_m} = \overline{\mathrm{End}(V).\det_m}$$

$$PER_m^n := \overline{GL(V).\, z^{m-n}\,\mathrm{perm}_n}$$

<u>Conjecture</u> [Strengthening of Valiant's Conjecture] when $m = n^{O(1)}$, then

$$z^{m-n}.\,\mathrm{perm}_n \notin DET_m \iff PER_m^n \nsubseteq DET_m$$

Fact: This conjecture implies Valiant's Conjecture

Fact This conjecture implies Valiant's Conjecture

Q Orbit closures why?

Ans (1) They are closures of group orbits

(2) By defn, they are alg. varieties

(LATER) We can use any two fns. complete for any complexity classes and ask inclusion b/w orbit closures

helps us talk about actual P vs NP in GCT

Why is "orbit closures" inviting?

because:-

(1) Perm & det are special.. "characterized by their symmetries"

(2) Perm & det satisfy a notion called "partial stability"

$\Downarrow$ + Luna's étale slice thm

You can look at multiplicities of irreps in the isotypic decomp of $GL(X)$ action on the representations obtained by considering the co-ordinate rings of the orbit closure of the determinant & the Padded permanent.

---

examples to see how representation theory comes up

Consider the poly x^2y.

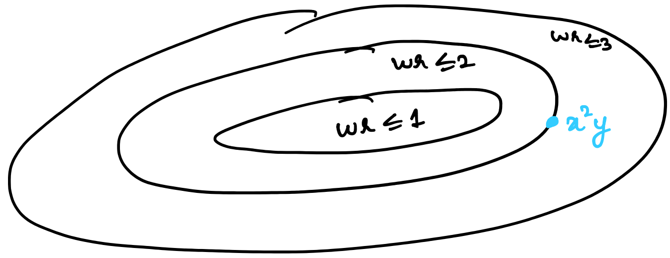
$$x^2y = \frac{1}{6}\left[(x+y)^3 + (y-x)^3 - 2y^3\right] \implies \mathrm{wr}(x^2y) \le 3$$

In fact $\mathrm{wr}(x^2y) = 3$

Check that: $\frac{1}{3\varepsilon}\left((x+\varepsilon y)^3 - x^3\right) = x^2y + \varepsilon xy^2 + \frac{\varepsilon^2}{3}y^2$

$$\Big\downarrow \varepsilon \to 0$$

$$x^2y$$



Because of continuity, any poly that vanishes on $wr \le 2$ must also vanish at x^2y. Thus we define border waring rank, denoted $\underline{wr}$

$$\underline{wr}(x^2y) = 2$$

① We can define border * → any complexity measure

② Border complexity measure are convenient to work with because the corresponding sets are closed (Euclidean & Zariski), thus finding a GCT-style seperating polynomial is feasible. Also GL acts on such sets.

$$x^2y = \lim_{\varepsilon \to 0} \frac{1}{3\varepsilon}\left((x+\varepsilon y)^3 - x^3\right).$$ $S_\varepsilon = \left(\frac{1}{3\varepsilon}\right)^{1/3}$, $\omega^3 = -1$, then

$$x^2y = \lim_{\varepsilon \to 0}\left[(S_\varepsilon x + \varepsilon S_\varepsilon y)^3 + (\omega S_\varepsilon x)^3\right]$$

This can be thought of as evaluating the polynomial x^3+y^3 at the pt $(x \;\; y)\begin{pmatrix} S_\varepsilon & \omega S_\varepsilon \\ \varepsilon S_\varepsilon & 0 \end{pmatrix}$

Generalising, we can say

$M_2(\mathbb{C}) \circ (x^3+y^3)$ ← exactly the set of poly of $wr \le 2$

monoid orbit

$$x^2y \in \overline{M_2(\mathbb{C}) \circ (x^3+y^3)} = \overline{GL_2(\mathbb{C}) \circ (x^3+y^3)}$$

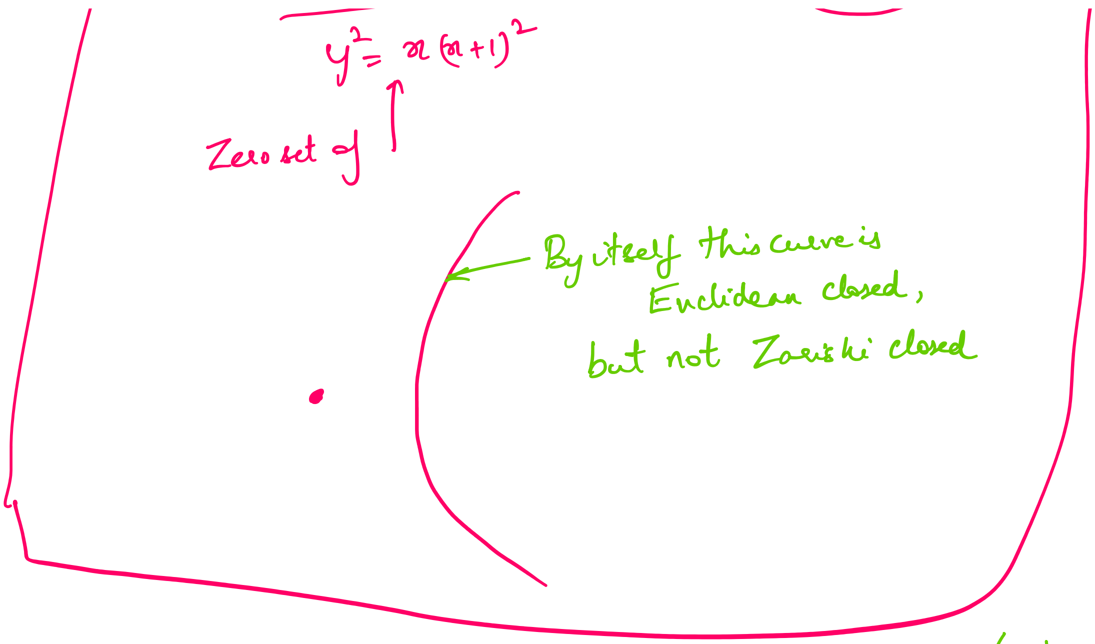
Proof sketch that such closures are alg. varieties

$$\overline{Y}^Z \supseteq \overline{Y} \supseteq Y$$

$\overline{Y}^Z \supsetneq \overline{Y}$ over Reals

aside

$$y^2 = x(x+1)^2$$



Chevalley's thm tells that orbit closures (alg. closed fields) are varieties $\boxtimes$

Concrete example for vanishing polynomials.

$\mathrm{Sym}^2(\mathbb{C}^2) \rightarrow$ 3 dim space with basis x^2, xy, y^2
(degree 2 homogeneous polys in 2 vars)

$$X_1 := \left\{ h \in \mathbb{C}[X,Y]_2 \;\middle|\; \mathrm{wr}(h) = 1 \right\}$$

$$\downarrow$$

$$h = (\alpha x + \beta y)^2$$

$$\Longleftrightarrow \quad X_1 := \left\{ ax^2 + bxy + cy^2 \;\middle|\; b^2 - 4ac = 0 \right\}$$

$b^2 - 4ac \in \mathrm{Sym}^2\left(\mathrm{Sym}^2(\mathbb{C}^2)\right)$ is a seperating polynomial

Claim $\mathrm{wr}(xy) > 1$

Proof $\quad xy = \underset{a}{0}\, x^2 + \underset{b}{1}\, xy + \underset{c}{0}\, y^2$

$$b^2 - 4ac \neq 0 \qquad \boxtimes$$

— Can define border complexity for any measure

— Can define border complexity for any measure

— We can define $\overline{VP}$

— Strengthening of Valiant conjecture : $\overline{VP} \neq VNP$

— We don't even know if $\overline{VP}$ & VP are diff.

$\overline{VP} \supseteq VP$, but we don't know if containment is strict

— $VP \subseteq VNP$ but don't know $\overline{VP} \subseteq VNP$

Recap
1. vec. space of polys, has GL-action
2. We have a Zariski closed X inside v.s.
3. need suitable funcs that help test membership in X
4. GL_n action on X carries over to funcs on X, so it is a representation of GL_n
5. Use multiplicities

e.g. Consider $Sym^2(\mathbb{C}^2)$ and action of S_2 $\quad e \neq \underset{S_2}{\rho} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$

Thus $Sym^2(\mathbb{C}^2)$ is a 3-dim representation of S_2

$\downarrow$ basis

$\{x^2, y^2, xy\}$ or $\{x^2+y^2, x^2-y^2, xy\}$

$\underbrace{\rho(x^2+y^2) = x^2+y^2, \ \rho(xy) = xy}_{\text{invariants under } S_2}, \ \underbrace{\rho(x^2-y^2) = -(x^2-y^2)}_{\text{skew-invariant under } S_2}$

$Sym^2(\mathbb{C}^2) = \langle xy, x^2+y^2 \rangle \oplus \langle x^2-y^2 \rangle$

this subspace is closed under action of S_2

Called a subrepresentation

$\dim_{inv}(Sym^2(\mathbb{C}^2)) = 2 \quad \& \quad \dim_{skew\text{-}inv}(Sym^2(\mathbb{C}^2)) = 1$

$\dim_{inv}(Sym^2(\mathbb{C}^2)) = 2$ & $\dim_{skew\text{-}inv}(Sym^2(\mathbb{C}^2)$

e.g. 2 Representations of S_2 ($Sym^2(Sym^2(\mathbb{C}^2))$)

Basis for $Sym^2(Sym^2(\mathbb{C}^2))$ is

$$\{a^2, ab, ac, b^2, bc, c^2\}$$

Action of S_2 on $Sym^2(\mathbb{C}^2)$ gives action on $Sym^2(Sym^2(\mathbb{C}^2))$

$$Sym^2(Sym^2(\mathbb{C}^2)) = \underbrace{\langle ac, b^2, a^2+c^2, ab+bc \rangle}_{\text{invariants under } S_2} \oplus \underbrace{\langle a^2-c^2, ab-bc \rangle}_{\text{skew-invariants}}$$

$$\underset{\substack{\cap \\ GL_2}}{g} \circ (b^2-4ac) = (\det(g))^2 (b^2-4ac)$$