Lecture 6

Wednesday, 7 June 2023 12:48

Last Lecture ① Dimension of Gauss image of perm_m hypersurface is full, i.e. m^2-2

② Need to show that dim. of Gauss image of det hypersurface is $2n-2$.

③ Degeneracy is preserved under substitution, so

$$m^2-2 \leq 2n-2$$

Zeros$(\det_n)$:

$$\left(SL_n(\mathbb{C}) \times SL_n(\mathbb{C})\right) \big/ \mu_n \rtimes \mathbb{Z}_2 \longleftarrow \text{stabilizer of det } G_{\det_n}$$

μ_n: Kernel of the product map

$$\mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$\det(AXB) = \det A \det B \det X, \quad \det(X^T) = \det X.$$

✱ Any pt. on det. hypersurface in the $G_{\det_n}$ orbit of

① $P_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \qquad r \leq n-1$

② The hypersurface is singular at $G_{\det_n} \cdot P_r$ where $r < n-1$

Recall

$$\sigma_1 = Seg(\mathbb{P}A_1 \times \cdots \times \mathbb{P}A_n)$$
$$:= \mathbb{P}\{T \in A_1 \otimes \cdots \otimes A_n \,/\, R(T) = 1\} \subseteq \mathbb{P}(A_1 \otimes \cdots \otimes A_n)$$

Prop Recall $\sigma_r^0(Seg(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}))$ is the space of matrices of rank r

$\hat{\ } \ 0 \ldots \mathbb{P}^{n-1} \ \mathbb{P}^{n-1}) \quad \{ \ldots \mid x \ \mathrm{Ker}(M) \subset \mathrm{Im}(M)\}$

Prop Recall $\sigma_r(Seg(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}))$ is the space ...

① $\hat{T}_M \sigma_r^0 (Seg(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})) = \{ X \in Mat_{n \times n} \mid X \,Ker(M) \subseteq Im(M) \}$

② $N^*_m \sigma_r^0 (Seg(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})) = Ker\, M \otimes (Image\ M)^{\perp} \cong Ker\, M \otimes Ker\, M^T$

Lemma $\dim Zeros(\det_n)^{\vee} = 2n-2$

Proof Smooth pts are in the $G_{\det_n}$ orbit of P_{n-1}

$$P_{n-1} = \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}$$

Ker Ker^T

Also $N^*_{P_{n-1}} Zeros(\det_n) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ * \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & \cdots & * \end{pmatrix}$

Ker $P_{n-1} \otimes$ Ker P^T_{n-1}

$$= \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & 0 & \vdots \\ 0 & \cdots & * \end{bmatrix}$$

rank 1 matrix

Thus tangent hyperplanes to $Z(\det_n)$ are parameterized by rank 1 matrices $\sigma_1^0(Seg(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}))$, which has dimension $2n-2$

$\boxtimes$

Thm [Mignon-Ressayre] ① rank of Hessian of $\det_n$ at smooth pts is

$2n-2+2 = 2n$

② Rank of Hessian of $perm_m$ at some pt is m^2

$\Rightarrow m^2 \leq 2n \Rightarrow n \geq \frac{m^2}{2}$

Grenet's u.b. on $dc(perm_m)$

Proof 1 [Combinatorial] ① Construct a digraph whose vertices are subsets of

Proof 1 [Combinatorial] ① Construct a digraph whose vertices are subsets of $[m] := \{1, \dots, m\}$, but identify ϕ & $[m]$. There are thus a total of $2^m - 1$ vertices.

② Place a directed edge from S to T with weight $x_{i,j}$ if

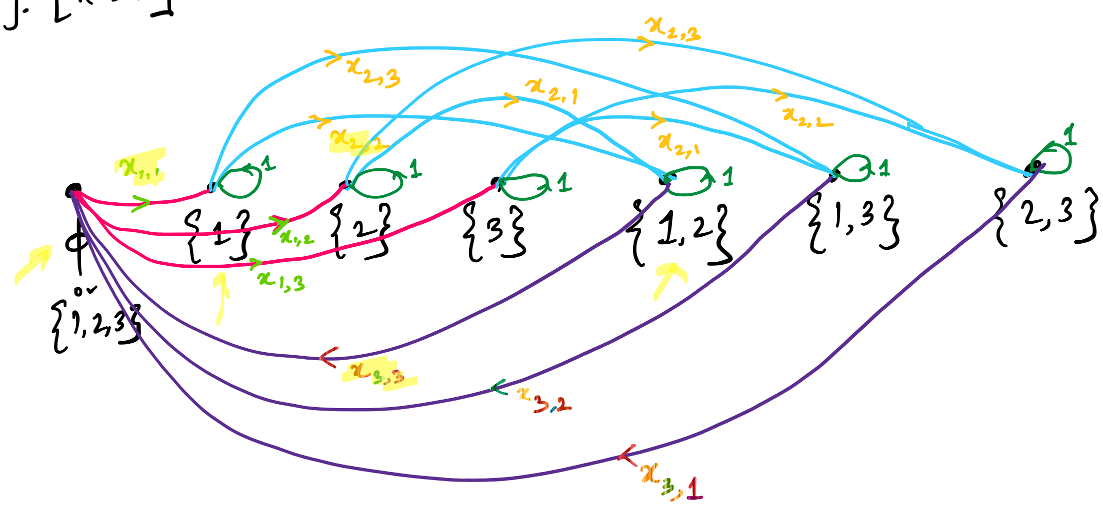
$$|S| = i-1, \; j \notin S, \; T = S \cup \{j\}$$

(a) Node ϕ will thus have outgoing edges of wt. $x_{1,j}$ to all nodes $\{j\}$ $j \in [m]$

(b) Since ϕ & $[m]$ are identified, ϕ has incoming edges of wt. $x_{n,j}$ from $[m] \setminus \{j\}$.

③ All nodes except $\phi / [m]$ get a self loop of weight 1.

e.g. $[n=3]$



Observe Vertex cycle covers are in bijective correspondence with permutations in S_m

This is because cycle covers have a specific structure in the above graph:-

① Any non-self loop has to pass through ϕ. This means a vertex cover has exactly 1 non-self loop and $2^m - 1 - m$ self loops.

② non-self loop corresponds to any order of $\{1, \dots m\}$.

③ Thus vertex cycle covers $\Longleftrightarrow$ elems of S_m

③ Thus vertex cycle covers $\Longleftrightarrow$ elems of S_m

Perm of the adj matrix of G is going to be $\text{perm}(X)$.

The cycle covers all have the same sign, so

$\text{Perm}(X) = \text{Perm}(G) = \pm \det(G)$

size of $G = 2^m - 1$

$\boxtimes$

<u>Defn</u> R- comm ring. E be a free R-module of rank r. Given an R-linear map $s: E \to R$, the Koszul complex associated to s.

$$K_\bullet(s): 0 \to \bigwedge^r E \xrightarrow{d_r} \bigwedge^{r-1} E \to \cdots \to \bigwedge^1 E \xrightarrow{d_1 (= s)} R \to 0$$

$$d_k(e_1 \wedge \cdots \wedge e_k) = \sum_{i=1}^{k} (-1)^{i+1} s(e_i)\, \underbrace{e_1 \wedge \cdots \wedge \hat{e}_i \wedge \cdots \wedge e_k}$$

$\hat{e}_i \leftarrow$ means you are omitting e_i

Definition implies

① $d_k \circ d_{k+1} = 0$, thus $K_\bullet(s)$ is a chain complex

② If $s: E = R^n \xrightarrow{[x_1 \ldots x_n]} R$, then $K_\bullet(s)$ is a free resolution of $R/\langle x_1 \ldots x_n \rangle$

free module on R generated by a regular sequence $x_1 \ldots x_n$

Proof 2 [Algebraic] Let ϕ_i denote the matrix of d_i of the Koszul complex of $(x_{i,1} \ldots x_{i,n})$. Let $\tilde{\phi}_i$ be the matrix ϕ_i but with "$-$" signs removed

Let ψ be the direct sum of $\tilde{\phi}_i$, and define

$$M_m = \psi + J_n$$

$$M_{nn} = \psi + J_n$$

$n \times n$ nilpotent matrix

+ Jordan matrix with 1's on the subdiagonal

Verify that the det of M is the perm (X) up to a $\pm$ sign

```
i1 : R = QQ[x_11,x_12,x_13,x_21,x_22,x_23,x_31,x_32,x_33]

o1 = R

o1 : PolynomialRing

i2 : C = koszul matrix{{x_11,x_12,x_13}}

      1      3      3      1
o2 = R  <-- R  <-- R  <-- R

     0      1      2      3

o2 : ChainComplex

i3 : C.dd

          1                                 3
o3 = 0 : R  <---------------------- R  : 1
               | x_11 x_12 x_13 |

          3                                 3
     1 : R  <--------------------------- R  : 2
               {1} | -x_12 -x_13 0     |
               {1} | x_11  0     -x_13 |
               {1} | 0     x_11  x_12  |

          3                  1
     2 : R  <---------------- R  : 3
               {2} | x_13  |
               {2} | -x_12 |
               {2} | x_11  |
```

Stabilizer of the permanent :$\rightarrow$

$$G_{perm} \quad \left[\left(T(SL_m(\mathbb{C})) \times T(SL_m(\mathbb{C}))\right) \rtimes (S_m \times S_m)\right]/\mu_n \rtimes \mathbb{Z}_2$$

maximal torus

(*) $\tilde{A}_{grent} : \mathbb{C}^{m^2} \longrightarrow \mathbb{C}^{n^2} \quad (n = 2^m - 1)$

Satisfies a nice equivariance property :

There is an injective homomorphism

$\psi : T(SL_m(\mathbb{C})) \rightarrow G_{det_n}$ s.t.

There is an injective ...

$$\psi : T(SL_m(\mathbb{C})) \to G_{\det_n} \quad \text{s.t.}$$

$$\tilde{A}_{\text{Grenet}}(gY) = \psi(g)\left(\tilde{A}_{\text{Grenet}}(Y)\right)$$

$g \in T(SL_m(\mathbb{C}))$

* If you impose the restriction that your embedding has the above equivariance property, then Grenet's embedding is optimal.

$$edc(\text{perm}_m) = 2^m - 1$$

We have an exponential seperation b/w perm & det in a restricted model of computation.

* If we can show an equivariant expression for perm_m of size $dc(\text{perm}_m)^c$ then $VP_{\mathbb{C}} \neq VNP_{\mathbb{C}}$

Restricted models of computation

Defn [Depth] the no. of edges in the longest path from an i/p node to its o/p

Defn [fanin] no. of edges coming into the gate

Waring Rank $\quad \Sigma\Lambda\Sigma$- Circuits

Defn [Waring Rank] $P \in \mathbb{C}[\bar{x}]_{(d)}$. The smallest r s.t we can write

$$P = l_1^d + \cdots \, l_r^d \qquad l_i \to \text{linear forms}$$

Defn [$\Sigma\Lambda^\delta\Sigma$ - Circuit] Consists of three layers: first addn gates. second - powering gate third is just a single addn gate.

$$l \longmapsto l^\delta,$$

Prop $P \in \mathrm{Sym}^d \mathbb{C}^n$, Waring rank $(P) = r$

① $\Rightarrow$ P admits a $\Sigma \Lambda^d \Sigma$-circuit of size $r(n+2)$

② $dc(P) \leq d r + 1$

Waring rank can be studied by looking at Secant varieties of the Veronese variety.

Shallow circuits for $VP \neq VNP$

depth 3, depth 4 & depth 5

$\Sigma\Pi\Sigma \qquad \Sigma\Pi\Sigma\Pi \qquad \Sigma\Lambda^{\alpha}\Sigma\Lambda^{\beta}\Sigma$

Defn A circuit is homogeneous if for each + gate, inputs have the same degree

Thm $N = N(d)$ be a poly in d. Let (P_d) $\in \mathrm{Sym}^d \mathbb{C}^N$ be a sequence of polys that can be computed by circuits of size $s = s(d)$ (poly in d). Let $\theta(d) = 2^{O(\sqrt{d \log ds \log N})}$. Then (P_d) is computable

(a) by a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit of size $\theta(d)$

(b) by a $\Sigma\Pi\Sigma$ circuit of size $\theta(d)$

(c) by a homogeneous $\Sigma\Lambda^{O(\sqrt{d})}\Sigma\Lambda^{O(\sqrt{d})}\Sigma$ circuit of size $\theta(d)$

Cor if (Perm_m) is not computable by any of the above circuits of size $2^{\omega(\sqrt{m} \log^{3/2} m)}$, then $VP \neq VNP$.

Prop [Geom intepration of above]

① $d = N^{O(1)}$, $P \in \mathrm{Sym}^d \mathbb{C}^N$ has a circuit of size s. then $[\ell^{n-d}p]$ belongs to the r^{th} secant variety of the Chow variety of degree n in $\mathbb{C}^{N+1}$ with $rn \sim s^{\sqrt{d}}$

Chow variety of degree n in $\mathbb{C}^{N+1}$ with ...

(2) If $[\ell^{n-m} \mathrm{perm}_m] \notin$ r^{th} secant variety of the degree n Chow variety in $\mathbb{C}^{m^2+1}$, then $VP \neq VNP$.

Thm [Gupta et al. "Method of Shifted partial derivatives"] ←

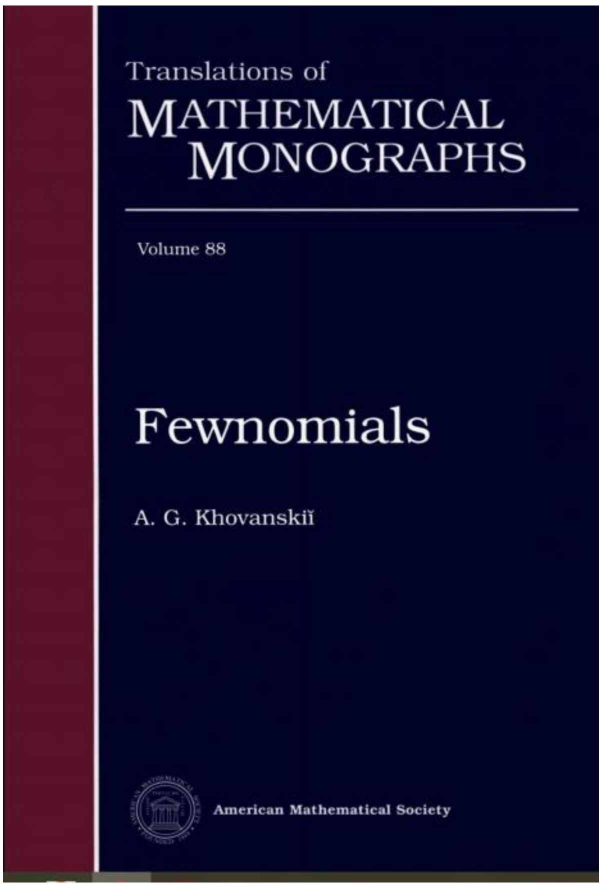
Any $\Sigma\Pi^{O(\sqrt{m})}\Sigma\Pi^{O(\sqrt{m})}$ circuit that computes Perm_m must have top fanin at least $2^{\Omega(\sqrt{m})}$.

Came very close to $VP \neq VNP$

Fewnomials & Real-Tau conjecture

Thm [Descartes' Rule of signs] $P \in \mathbb{R}[x]$ of any arbit. degree, but only t monomials, it has $\sim 2t$ roots (counted with multiplicities)

(8) Fewnomials



Conjecture [Real-Tau conjecture]

Conjecture [Real-Tau conjecture]

$\sum_{i=1}^{K} \prod_{j=1}^{m} f_{i,j}(x)$, where $f_{i,j}$ are t-sparse. No. of zeros is $\mathrm{Poly}(K, t, 2^m)$

$\Sigma\Pi$

Thm Real-Tau Conj $\Rightarrow$ $VP_{\mathbb{C}} \neq VNP_{\mathbb{C}}$

Mathematical problems for the next century

Steve Smale

The Mathematical Intelligencer **20**, 7–15 (1998) | Cite this article

4th	Shub–Smale tau-conjecture on the integer zeros of a polynomial of one variable[6][7]	Unresolved.

Thm [Briquel-Buergisser] If $f_{i,j}$ are chosen as follows:

① fix support of $f_{i,j}$ of t.

② Let the coeff of $f_{i,j}$ be indepent $\mathcal{N}(0,1)$.

Then $\mathbb{E}[\text{real zeros}] = O(k m^2 t)$

Real-Tau conj is true with prob ~ 1

Thm [Koiran et al.] ① It is true that

$\sum_{i=1}^{K} \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ have $O\left(t^{O(k^2 m)}\right)$ roots.

(without counting multiplicity)

② Restricted classes of depth 4-circuits (poly sizes) cannot compute the permanent.

e.g. $fg + 1$, f, g t-sparse $\rightarrow$ Descartes gives $\sim t^2$ (improve this!!)

MAIN TECHNICAL TOOL (WRONSKIAN)

Defn Given $f_1 \ldots f_k$, define

<u>Defn</u> Given $f_1 \ldots f_k$, define

$$W(f_1 \ldots f_k) = \det \left[\left(f_j^{(i-1)} \right)_{i,j \in [k]} \right]$$

<u>Prop</u> If $f_1 \ldots f_k$ are analytic functions, then:

$$\{f_i\} \text{ are linearly indep} \iff W(f_1 \ldots f_k) \neq 0.$$

<u>Thm</u> [Voorhoeve & Van der Poorten] $f_1 \ldots f_k$ are real analytic functions over an interval I. Then

$$N(f_1 + \cdots + f_k) \leq k-1 + \sum_{j=1}^{k-2} N(W(f_1 \ldots f_j)) + \sum_{j=1}^{k} N(W(f_1 \ldots f_j))$$

zeros with multiplicity.

<u>Thm</u> [Koiran et al.] Same bound holds on zeros of polynomials without multiplicity if f_i's are linearly indep. on I.

Main thm uses this tool + $W(f_1^{\alpha} \ldots f_k^{\alpha})$