VP, VNP, determinantal complexity of permanent

Wednesday, 31 May 2023 12:29

Last lecture:-

We defined VP, VNP, showed $(\text{perm}_n) \in VNP$

Prop $(\det_n) \in VP$

Proof Let S_n act on $\mathbb{C}[x_1, \ldots, x_n]$ naturally, and let $\mathbb{C}[x_1, \ldots, x_n]^{S_n}$ the invariant subspace.

Fact 1 The elementary symmetric funcs

$$e_r = \sum_{\substack{J \subseteq [n] \\ |J| = r}} x_{j_1} \cdots x_{j_r}$$ are a basis of $\mathbb{C}[x_1, \ldots, x_n]^{S_n}$

Fact 2 The power sum polynomials

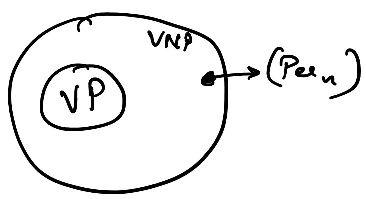
$$P_r = x_1^r + \cdots + x_n^r$$ are also a basis of $\mathbb{C}[x_1, \ldots x_n]^{S_n}$

(*) The determinant of $f : V \to V$ is the product of the e values $\lambda_1, \ldots, \lambda_n$

(*) $\text{Trace}(f) = \sum_{i=1}^{n} \lambda_i$, $\text{trace}(f^k) = \sum_{i=1}^{n} \lambda_i^k$

f^k can be computed with small circuits, so $\det(f)$ also can be computed using small circuits $\boxtimes$

Thm [Valiant] (Per_n) is VNP-complete. ($\text{char}\ K \neq 2$)



Conjecture [Valiant] $VP \subsetneq VNP$

Thm [Burgisser] $VP = VNP \implies \underbrace{P/\text{Poly}}_{\text{non-uniform Polynomial time}} = \underbrace{NP/\text{Poly}}_{\text{non-uniform NP}}$ (assuming Gen. Riemann Hyp.)

Class of decision problems

Class of decision problems Solvable by a family of polynomial size boolean circuits + the circuit family can be non-uniform, i.e., the could be a completely diff. circuit for each input length.

Polynomial time

NP

- VP vs VNP "arithmetic circuit complexity"
- P/Poly vs NP/Poly " boolean circuit complexity"
- P vs NP "uniform complexity"

* VP vs VNP has strong impact on what is called the polynomial hierarchy.

* Graph G with adj matrix A, the permanent of A counts the no. of perfect matchings. Checking for presence of perfect matching $\in$ P, but enumerator is hard.

Determinantal Complexity

Defn $I : \mathbb{C} \cup \{x_1, \dots x_n\}$.

- Every elem of I is an expression
- $expr_1 * expr_2$ & $expr_1 + expr_2$ are also expressions

The size of an expression is defined as the no. of +'s or *'s

Thus every expression is a polynomial in $\mathbb{C}[x_1, \dots x_n]$. For $f \in \mathbb{C}[x_1 \dots x_n]$,

expression size of f = $\min_{\phi \text{ computes } f} |\phi|$.

Thm [Universality of the determinant & permanent]

$\forall f \in \mathbb{C}[x_1 \dots x_n]$ of expr size u, there is a matrix M of size $(u+2)\times(u+2)$

entries of M are linear forms in $x_1, \dots x_n$

s.t $\det M = f$

(also true for permanent)

forms" in $x_1, \dots x_n$

(also true for permanent)

Def min size of matrix in above thm is called the determinantal complexity of f, denoted $dc(f)$

Thm $dc(perm_m) \le O(m^c)$, c is a const. $\Longrightarrow VP = VNP$

Proof by defn $\boxtimes$

$$\boxed{\text{Goal: } \frac{m^2}{2} \le dc(perm_m) \le 2^m - 1}$$

$dc(perm_m) \ge \frac{m^2}{2}$

Overview
1. Define Gauss maps
2. Notion of degeneracy of Gauss images
3. Show that – perm does not have degenerate Gauss images
   – det has "strongly" degenerate Gauss images

   lower bound follows from a dimension count

GAUSS MAPS

Maps points in 3 space to its unit normal vector on the unit sphere $\subseteq \mathbb{R}^3$

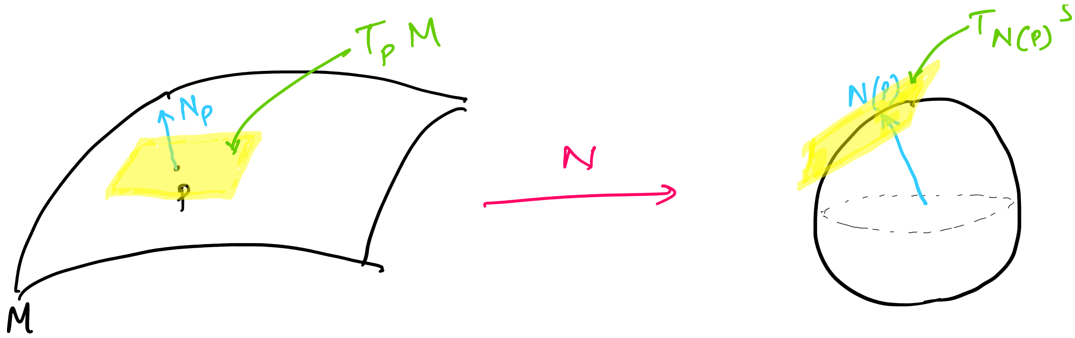
Defn [Gauss map for surfaces in $\mathbb{R}^3$] $M \subseteq \mathbb{R}^3$ is an oriented surface. N is the Gauss map of M

unit sphere

(Continuous)

$$N: M \longrightarrow S^2 (\subseteq \mathbb{R}^3)$$
$$p \longmapsto N_p \text{ (oriented unit normal vector at point } p)$$

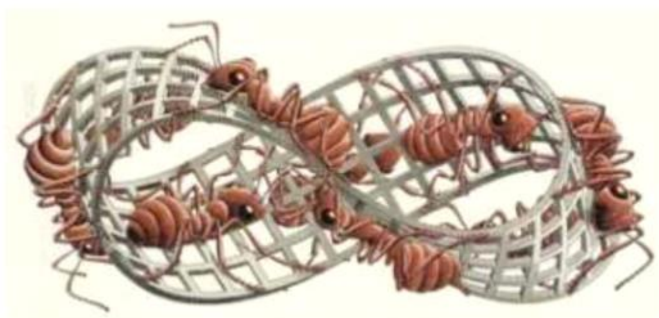
$(\|N_p\| = 1, \ \langle N_p, \vec{v} \rangle = 0 \ \ \forall \vec{v} \in T_p M)$



$$T_p M \cong T_{N(p)} S^2$$

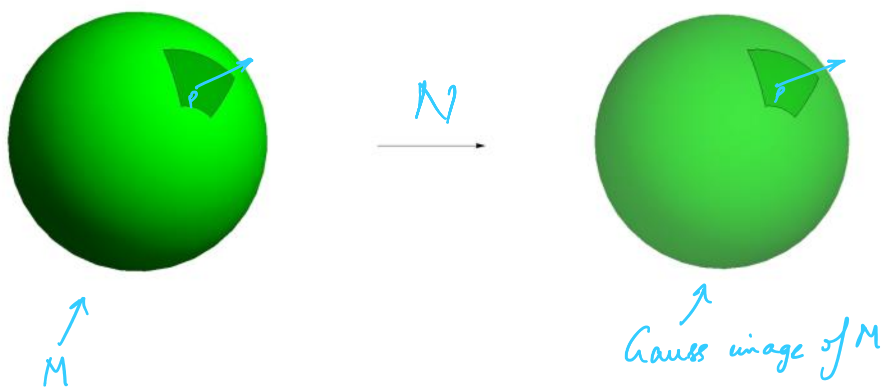
① Most surfaces have two choices for the direction of normal vector

② N need to be cont., so some surfaces do not have a Gauss map
e.g. Mobius strip

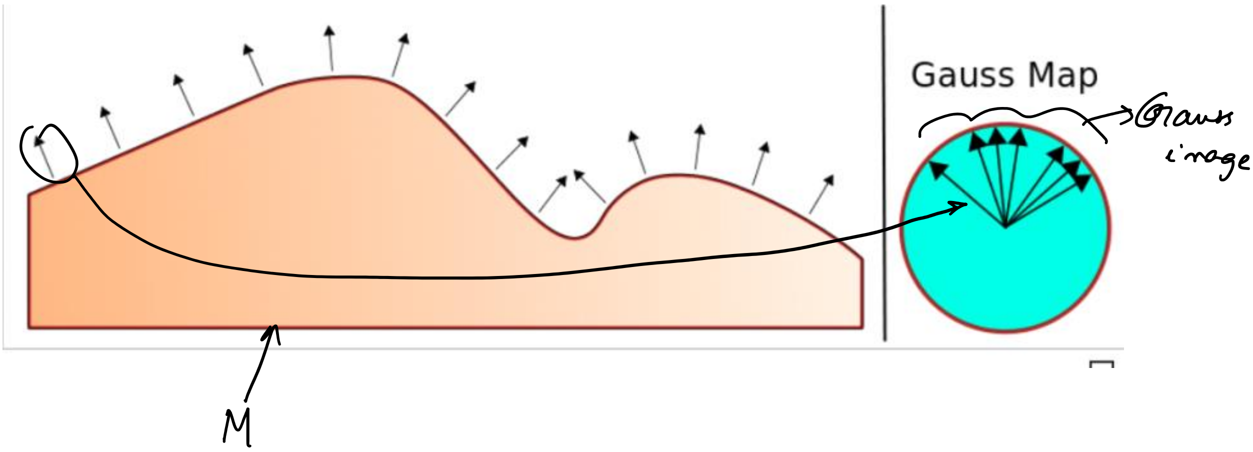


Mobius Band

Example ①



②



(3) Gauss image has lower dim. than M.

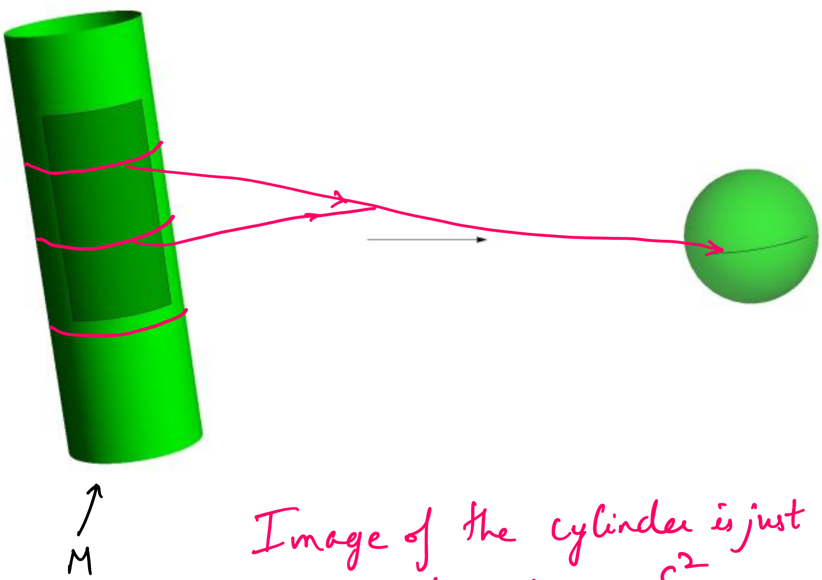


Image of the cylinder is just a great circle on S^2

$2 = \dim(M) > \dim(\text{great circle}) = 1$

(4) Gauss image of a plane in $\mathbb{R}^3$ (2 dim) is just a point (0-dim)

Thm [Segre 1910] Let $M \subseteq \mathbb{P}^3$ be a surface with degenerate Gauss image. Then it is one of

1. A linearly embedded $\mathbb{P}^2$
2. A cone over a curve C
3. A tangential variety to a curve C.

③ A tangential variety to a curve C.

"Having a degenerate Gauss image is a pathology"

Notation ① V - vector space $\quad \pi : V \setminus \{0\} \to \mathbb{P}V$

$y \longmapsto [y]$

② $X \subseteq \mathbb{P}V$, define

$$(V \supseteq) \hat{X} := \pi^{-1}(X) \cup \{0\}$$

③ If $\hat{X}$ is a variety, $X \subseteq \mathbb{P}V$ will also be called a variety.

Defn $X \subseteq \mathbb{P}V$ be an irred. proj. variety.

[Affine Tangent Space at $[x] \in X$] $\hat{T}_{[x]}X$ is just $T_x \hat{X} = \hat{T}_{[x]} X$

any pt. in V representing $[x] \in \mathbb{P}V$

[Projective tangent space] $\mathbb{P}(T_x \hat{X})$

Defn [Conormal space] $X \subseteq \mathbb{P}V$ (proj. variety). The conormal space at $[x] \in X$, denoted $N^*_{[x]}X \subseteq V^*$ is just the annihilator of $\hat{T}_{[x]}X$, i.e.

$$N^*_{[x]}X = \left(\hat{T}_{[x]}X\right)^{\perp}$$

Defn [Gauss image in general] $X \subseteq \mathbb{P}V$ be an irred. hypersurface. Define the Gauss image / Dual variety of X

$$X^\vee := \overline{\left\{ H \in \mathbb{P}V^* \;\middle|\; \exists\, [x] \in X_{\text{smooth}},\ \hat{T}_{[x]}X \subseteq \hat{H} \right\}}$$

$$= \overline{\left\{ H \in \mathbb{P}V^* \;\middle|\; \exists\, [x] \in X_{\text{smooth}},\ H \in \mathbb{P}N^*_{[x]}X \right\}}$$

Points

hyperplanes in $\mathbb{P}V^*$ determined by H

Union of all conormal lines in $\mathbb{P}V^*$

If $X^\vee$ is not a hypersurface, we say X has a degenerate Gauss image

* Perm hypersurface does not have a degenerate dual variety

* det hypersurface has a degenerate dual variety.

$(\det_n \text{ hypersurface})^\vee$ has low dimension. $\simeq n$

$(\text{Perm}_m \text{ hyp})^\vee$ has high dimension $\simeq m^2$

$$m^2 \lesssim n$$

— Let V be a v.s. over field k.

Ring of polynomial function V is denoted $k[V]$.

— $k[V]$ consists of polynomials in t_i, where t_i form a basis of V.

— If k is infinite, $k[V]$ is the symmetric algebra on V^*, i.e. $\mathrm{Sym}(V^*)$

→ $\mathrm{Sym}^q(V^*)$ — V.S. of multilinear functionals. (symmetric)

$$\lambda : \prod_{i=1}^{q} V \to k$$

→ Any $\lambda \in \mathrm{Sym}^q(V^*)$ gives you a homogeneous poly func of degree q.

$$f(v) = \lambda(v, \ldots, v)$$

Thus $\mathrm{Sym}^q(V^*) \longrightarrow k[V]_{(q)}$ is an isomorphism

Elems of $\mathrm{Sym}^q(\mathbb{C}^M)$ (a) hom. poly. of deg q on $(\mathbb{C}^M)^*$

(b) a symmetric tensor

(c) a homogeneous differential operator of order d on the

(b) a symmetric tensor

(c) a homogeneous differential operator of order d on the space of Polynomials, i.e. $\mathrm{Sym}((\mathbb{C}^N)^*)$

Idea:- $k[x_1 \dots x_n]$ is a vector space

$\frac{\partial}{\partial x_i}$ maps an elem of $k[x_1 \dots x_n]_{(q)} \cong \mathrm{Sym}^q(V^*)$

to an elem of

$k[x_1 \dots x_n]_{(q-1)} \cong \mathrm{Sym}^{q-1}(V^*)$

Defn Let $r \geq t$

$$\mathrm{Sym}^r(V^*) \otimes \mathrm{Sym}^t(V) \longrightarrow \mathrm{Sym}^{r-t}(V^*)$$

[Contraction map]

$\downarrow$

homogeneous diff operators of order t

Let $P \in \mathrm{Sym}^n \mathbb{C}^N$. $(\mathbb{C}^N)^*$ can be considered as the space of first order homogeneous diff. operators on $\mathrm{Sym}^n \mathbb{C}^N$. Define

$$P_{1,n-1} : (\mathbb{C}^N)^* \longrightarrow \mathrm{Sym}^{n-1}(\mathbb{C}^N)$$
$$\frac{\partial}{\partial x_j} \longmapsto \frac{\partial P}{\partial x_j}$$

[Co-ord free $\mathrm{Sym}^n V \subseteq V \otimes \mathrm{Sym}^{n-1} V = \mathrm{Hom}(V^*, \mathrm{Sym}^{n-1} V)$
$P \in \mathrm{Sym}^n V$, $P_{1,n-1} \in \mathrm{Hom}(V^*, \mathrm{Sym}^{n-1} V)$]

Define $P_{2,n-2} : \mathrm{Sym}^2((\mathbb{C}^N)^*) \longrightarrow \mathrm{Sym}^{n-2} \mathbb{C}^N$

$$\frac{\partial^2}{\partial x_i \partial x_j} \longmapsto \frac{\partial^2 P}{\partial x_i \partial x_j}$$

$$P_{k,n-k} : \mathrm{Sym}^k((\mathbb{C}^N)^*) \longrightarrow \mathrm{Sym}^{n-k} \mathbb{C}^N$$
$$D \longmapsto D(P)$$

Defn Let $P \in \mathrm{Sym}^d V^*$ be irreducible. Let $[x] \in Z(P)$ be

Prop Let $P \in \mathrm{Sym}^d V^*$ be irreducible. Let $[x] \in Z(P)$ be a general pt. Then

$$\dim Z(P)^\vee = \mathrm{rank}\left(P_{d-2,2}(x) \right) - 2$$

$\Longrightarrow$ $P_{d-2,2}(x) \in \mathrm{Sym}^2 V^*$, a symmetric matrix,

$P_{d-2,2}(x)$ is the Hessian of P.

Prop Let $Q \in \mathrm{Sym}^m \mathbb{C}^M$, $\tilde{A} : \mathbb{C}^M \to \mathbb{C}^N$ be such that

$Q(y) = P(\tilde{A}(y))$ $\forall\, y \in (\mathbb{C}^M)^*$, then

$(*)$ $\mathrm{rank}\left(Q_{n-2,2}(y) \right) \leq \mathrm{rank}\left(P_{n-2,2}(\tilde{A}(y)) \right)$

Remaining

1. $\mathrm{rank}\left((\mathrm{Perm}_m)_{m-2,2}(x) \right)$ for general $[x] \in Z(\mathrm{Perm}_m)$ is full, i.e. there is a pt. where the matrix has rank $\underline{m^2}$
2. $\dim Z(\det_n)^\vee = 2n-2$
   $\Longrightarrow \mathrm{rank}\left((\det_n)_{n-2,2}(x) \right) = \underline{2n}$ for general $[x] \in Z(\det_n)$
3. By $(*)$ Gauss image of $\{ \det(f(x)) = 0 \}$, for $f : \mathbb{C}^{m^2} \to \mathbb{C}^{n^2}$ is as degenerate as the Gauss map of $\{ \det(x) = 0 \}$, we have $m^2 \leq 2n$
   $\Rightarrow n \geq \frac{m^2}{2}$

To show that a hypersurface has non-degenerate Gauss image, find a pt. where Hessian of its defining eqn. has max. rank.

Lemma There exists such a pt. for perm_m

Proof Consider

$$y_0 = \begin{pmatrix} 1-m & 1 & \cdots & 1 \\ 1 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 1 & \cdots & \cdots & 1 \end{pmatrix}.$$

Easy to check $\mathrm{Perm}(y_0) = 0$

$$y_0 \in Z(\mathrm{Perm}_m)$$

To compute $(\mathrm{Perm}_m)_{m-2,2}(y_0)$, note

$$\frac{\partial^2}{\partial y_{i,j}\,\partial y_{k,l}} \mathrm{Perm}_m \underbrace{\begin{bmatrix} y_{1,1} & \cdots & y_{1,m} \\ \vdots & & \\ y_{m,1} & \cdots & y_{m,m} \end{bmatrix}}_{Y} = \begin{cases} 0 & \text{if } i=k \text{ or } j=l \\ \mathrm{Perm}_{m-2}\left(Y_{(\hat{i},\hat{j}),(\hat{k},\hat{l})}\right) & \text{otherwise} \end{cases}$$

rows i,k & cols j,l removed

$$M = \begin{pmatrix} 0 & Q & Q & \cdots & Q \\ Q & 0 & R & \cdots & R \\ Q & R & 0 & R \cdots & R \\ \vdots & \vdots & & \ddots & \vdots \\ Q & R & & R & 0 \end{pmatrix} \in \mathbb{C}^{m^2 \times m^2}, \text{ where}$$

$$Q = m-2\begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & & \vdots \\ 1 & 1 & \cdots & & 0 \end{pmatrix}, \text{ and}$$

$m \times m$

$$R = \begin{pmatrix} 0 & m-2 & \cdots & \cdots & m-2 \\ m-2 & 0 & -2 & \cdots & -2 \\ \vdots & -2 & 0 & \cdots & -2 \\ \vdots & \vdots & & \ddots & \vdots \\ m-2 & -2 & \cdots & \cdots & 0 \end{pmatrix}$$

$m \times m$

NTS M is invertible. WLOG $Q = Id_m$

Let $v = (v_{1,1} \quad v_{1,m} \quad v_{2,1} \cdots v_{2,m} \cdots v_{m,1} \cdots v_{m,m})$

NTS M is invertible.

Let $\underset{\substack{\uparrow \\ \ker M}}{V} = (\underbrace{v_{1,1} \cdots v_{1,m}}_{\tilde{V}_1}, \underbrace{v_{2,1} \cdots v_{2,m}}_{\tilde{V}_2} \cdots \underbrace{v_{m,1} \cdots v_{m,m}}_{\tilde{V}_m})$

$MV = 0$

$$\begin{aligned} &\tilde{V}_2 + \cdots + \tilde{V}_m = 0 \\ &\tilde{V}_1 + R\tilde{V}_3 + \cdots R\tilde{V}_m = 0 \\ &\vdots \\ &\tilde{V}_1 + R\tilde{V}_2 + \cdots R\tilde{V}_{m-1} = 0 \end{aligned} \iff \begin{aligned} &\tilde{V}_2 + \cdots + \tilde{V}_m = 0 \\ &\tilde{V}_1 - R\tilde{V}_2 = 0 \\ &\tilde{V}_1 - R\tilde{V}_3 = 0 \\ &\vdots \\ &\tilde{V}_1 - R\tilde{V}_m = 0 \end{aligned}$$

$(m-1)\tilde{V}_1 = 0 \Rightarrow \tilde{V}_1 = 0$ & $\tilde{V}_2 \cdots \tilde{V}_m = 0$

Thus $\ker M$ is trivial $\boxtimes$