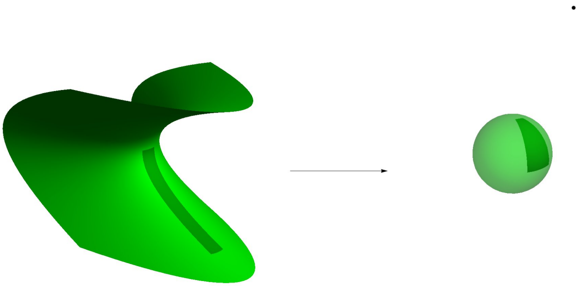
Complexity Theory and Geometry*

J.M. Landsberg

Texas A&M University



*color pictures by Jesko Hüttenhain

History: 1950's, Soviet Union- Is brute force search avoidable?

A traveling saleswoman visits 20 cities: Moscow, Leningrad, Stalingrad,...
Is there a route less than 50,000km?

Only known method: essentially brute force search

Number of paths to check grows exponentially.

Can routes be found more efficiently?

Cause for hope: it is very easy to check if a proposed route is less then 50,000km.

1970's: Cook, Karp, Levin: Precise conjecture

P: the class of problems that are "easy" to solve (e.g. determining existence of a perfect matching in a bipartite graph)

NP: the class of problems that are "easy" to verify (e.g., the traveling saleswoman)

Conjecture

$\mathbf{P} \neq \mathbf{NP}$.

Late 1970's: Valiant, computer science $\rightsquigarrow$ algebra

Problem: *count* the number of perfect matchings of a bipartite graph.

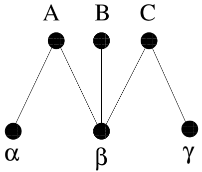


Figure: Amy is allergic to γrapes, Bob insists on βanana, Carol dislikes αpple.

Count by computing a polynomial. Let $X = (x^i_j)$: incidence matrix of the graph, where $x^i_j = 1$ if $\exists$ edge between vertices i and j and is otherwise zero.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Late 1970's: Valiant, computer science $\rightsquigarrow$ algebra

perfect matching $\leftrightarrow$ each row paired with a column such that corresponding matrix entry is 1

i.e., identity matrix or permutation of its columns.

$\mathfrak{S}_n$: permutations of $\{1, \ldots, n\}$.

The *permanent* of $X = (x^i_j)$ is

$$\mathrm{perm}_n(X) := \sum_{\sigma \in \mathfrak{S}_n} x^1_{\sigma(1)} x^2_{\sigma(2)} \cdots x^n_{\sigma(n)}.$$

$\mathrm{perm}_n(X) = \#$ perfect matchings, e.g. $\mathrm{perm}_3 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = 1$

Late 1970's: Valiant, computer science $\rightsquigarrow$ algebra

VNP: sequences of polynomials that are "easy" to write down.

For example, $(\mathrm{perm}_n) \in \mathbf{VNP}$.

VP: sequences of polynomials that are "easy" to compute.

For example, $(\det_n) \in \mathbf{VP}$ (Gaussian elimination).

Conjecture (Valiant (1979))

$\mathbf{VP} \neq \mathbf{VNP}$.

Permanents via determinants

$$perm_m(Y) := \sum_{\sigma \in \mathfrak{S}_m} y^1_{\sigma(1)} y^2_{\sigma(2)} \cdots y^m_{\sigma(m)}$$

$$det_n(X) := \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sign}(\sigma) x^1_{\sigma(1)} x^2_{\sigma(2)} \cdots x^n_{\sigma(n)}$$

For example

$$\det_2 \begin{pmatrix} x^1_1 & x^1_2 \\ x^2_1 & x^2_2 \end{pmatrix} = x^1_1 x^2_2 - x^1_1 x^2_1,$$

and

$$\mathrm{perm}_2 \begin{pmatrix} y^1_1 & y^1_2 \\ y^2_1 & y^2_2 \end{pmatrix} = y^1_1 y^2_2 + y^1_1 y^2_1 = \det_2 \begin{pmatrix} y^1_1 & -y^1_2 \\ y^2_1 & y^2_2 \end{pmatrix}$$

Permanents via small determinants?

[B. Grenet (2011)]:

$$\mathrm{perm}_3(Y) = \det_7 \begin{pmatrix} 0 & y_1^1 & y_1^2 & y_1^3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & y_3^3 & y_3^2 & 0 \\ 0 & 0 & 1 & 0 & 0 & y_3^1 & y_3^3 \\ 0 & 0 & 0 & 1 & y_3^1 & 0 & y_3^2 \\ y_2^2 & 0 & 0 & 0 & 1 & 0 & 0 \\ y_2^3 & 0 & 0 & 0 & 0 & 1 & 0 \\ y_2^1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

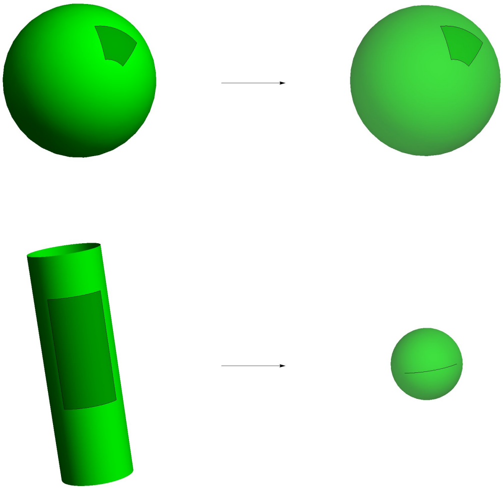
Question: Can every perm_m be expressed in this way for some n?
Valiant: Yes! In fact $n \sim 2^m$ works.

Conjecture (Valiant (1979))

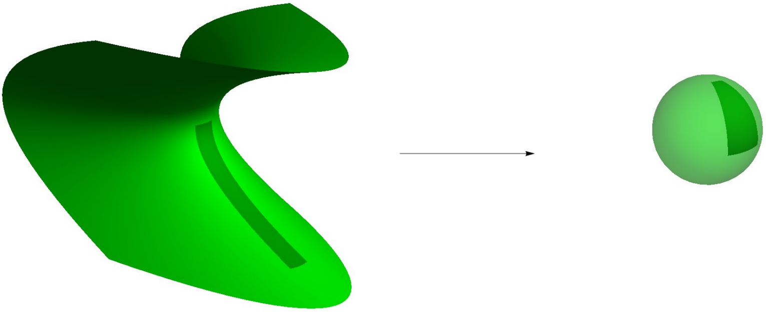
Let $n(m)$ be a polynomial. $\forall m \gg 0$, $\nexists$ affine linear functions $x_j^i(y_t^s)$ with $\mathrm{perm}_m(Y) = \det_{n(m)}(X(Y))$.

Differential Geometry detour

Given a surface in 3-space, its **Gauss image** in the two-sphere is the union of all unit normal vectors to the surface:



Differential Geometry detour

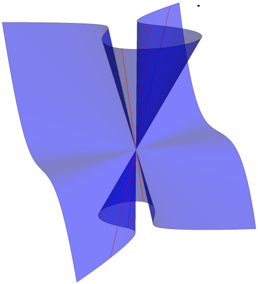


Can define the Gauss image without a distance function, via conormal lines.

Dimension of image still defined.

Classical Theorem: Surfaces with Gauss image a curve are:

- The union of tangent rays to a space curve.
- A generalized cone, i.e., the union of lines connecting a point to a plane curve. (Includes case of cylinders, where point is at infinity.)



Connection to complexity theory?

Gauss images are defined in higher dimensions.

The hypersurface

$$\{\det_n(X) = 0\} \subset \{n \times n \text{ matrices}\} = \mathbb{C}^{n^2}$$

has low dimensional Gauss image ($2n - 2$ v. expected $n^2 - 2$).

Under substitution $X = X(Y)$, Gauss image stays degenerate.

Theorem (Mignon-Ressayre (2004))

If $n(m) < \frac{m^2}{2}$, then $\nexists$ affine linear functions $x^i_j(y^s_t)$ such that $\mathrm{perm}_m(Y) = \det_n(X(Y))$.

Algebraic geometry: the study of zero sets of polynomials

Our situation: Polynomials on spaces of polynomials.

Let

$$P(x_1, \ldots, x_N) = \sum_{1 \leq i_1 \leq \cdots i_d \leq N} c_{i_1,\ldots,i_d} x_{i_1} \cdots x_{i_d}$$

homogeneous, degree d in N variables;

Study polynomials on the coefficients $c_{i_1,\ldots,i_d}$.

These coefficients are coordinates on the vector space $Sym^d\mathbb{C}^N = \mathbb{C}^{\binom{N+d-1}{d}}$.

Geometric Complexity Theory approach to Valiant's conjecture [Mulmuley-Sohoni (2001)]

Idea: Find a sequence of polynomials $\{P_m\}$ such that

- $P_m(q_m) = 0$ for all polynomials

$$q_m(Y) = \det_{n(m)}(X(Y))$$

  when $n(m)$ is a polynomial,
- $P_m(\mathrm{perm}_m) \neq 0$.

Use *representation theory* (systematic study of symmetries via linear algebra) to find $\{P_m\}$.

Algebraic geometry

Theorem (L-Manivel-Ressayre (2013))

An explicit $\{P_m\} \rightsquigarrow$ *strengthened Mignon-Ressayre Theorem.*

Bonus! solved a classical problem: find defining equations for the variety of hypersurfaces with degenerate Gauss images (dual varieties).

A practical problem: efficient linear algebra

Standard algorithm for matrix multiplication, row-column:

$$\begin{pmatrix} * & * & * \\ & & \\ & & \end{pmatrix} \begin{pmatrix} * & & \\ * & & \\ * & & \end{pmatrix} = \begin{pmatrix} * & & \\ & & \\ & & \end{pmatrix}$$

uses $O(n^3)$ arithmetic operations.

Strassen (1968) set out to prove this standard algorithm was indeed the best possible.

At least for 2×2 matrices.

He failed.

Strassen's algorithm

Let A, B be 2×2 matrices $A = \begin{pmatrix} a_1^1 & a_2^1 \\ a_1^2 & a_2^2 \end{pmatrix}, \quad B = \begin{pmatrix} b_1^1 & b_2^1 \\ b_1^2 & b_2^2 \end{pmatrix}$. Set

$$\begin{aligned} I &= (a_1^1 + a_2^2)(b_1^1 + b_2^2), \\ II &= (a_1^2 + a_2^2)b_1^1, \\ III &= a_1^1(b_2^1 - b_2^2) \\ IV &= a_2^2(-b_1^1 + b_1^2) \\ V &= (a_1^1 + a_2^1)b_2^2 \\ VI &= (-a_1^1 + a_1^2)(b_1^1 + b_2^1), \\ VII &= (a_2^1 - a_2^2)(b_1^2 + b_2^2), \end{aligned}$$

If $C = AB$, then

$$\begin{aligned} c_1^1 &= I + IV - V + VII, \\ c_1^2 &= II + IV, \\ c_2^1 &= III + V, \\ c_2^2 &= I + III - II + VI. \end{aligned}$$

Astounding conjecture

Iterate: $\rightsquigarrow 2^k \times 2^k$ matrices using $7^k \ll 8^k$ multiplications,

and $n \times n$ matrices with $O(n^{2.81})$ arithmetic operations.

Conjecture

For all $\epsilon > 0$, $n \times n$ matrices can be multiplied using $O(n^{2+\epsilon})$ arithmetic operations.

$\rightsquigarrow$ *asymptotically, multiplying matrices is nearly as easy as adding them!*

How to *disprove* astounding conjecture via algebraic geometry?

Study polynomials on spaces of *bilinear maps*.

Set $N = n^2$.
Matrix multiplication is a bilinear map

$$M_{\langle n \rangle} : \mathbb{C}^N \times \mathbb{C}^N \to \mathbb{C}^N.$$

$\{$bilinear maps $T : \mathbb{C}^N \times \mathbb{C}^N \to \mathbb{C}^N\}$: vector space of dim $= N^3$.

Idea: Look for polynomials P_n on $\mathbb{C}^{N^3}$ such that

- $P_n(T) = 0 \ \forall \ T$ computable with $O(N)$ arithmetic operations, and
- $P_n(M_{\langle n \rangle}) \neq 0$.

How to disprove? - Precise formulation

$$M_{\langle 1\rangle} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$$
$$(x, y) \mapsto xy$$

denotes scalar multiplication.

Set

$$M_{\langle 1\rangle}^{\oplus r} : \mathbb{C}^r \times \mathbb{C}^r \to \mathbb{C}^r$$
$$((x_1, \ldots, x_r), (y_1, \ldots, y_r)) \mapsto (x_1 y_1, \ldots, x_r y_r).$$

$\{$bilinear maps computable with r scalar multiplications$\}$
$=$ set of degenerations of $M_{\langle 1\rangle}^{\oplus r}$.
$= \mathrm{End}(\mathbb{C}^r) \times \mathrm{End}(\mathbb{C}^r) \times \mathrm{End}(\mathbb{C}^r) \cdot M_{\langle 1\rangle}^{\oplus r}$,
$=:$ $\mathbf{Arith}_r$

How to disprove?- Precise formulation

$T : \mathbb{C}^r \times \mathbb{C}^r \to \mathbb{C}^r$ has *tensor rank at most r* if $T \in \textbf{Arith}_r$, and write $\mathbf{R}(T) \leq r$.

Theorem (Strassen (1969))

$\mathbf{R}(M_{\langle n \rangle}) = O(n^\tau)$ *if and only if* $M_{\langle n \rangle}$ *can be computed with* $O(n^\tau)$ *arithmetic operations.*

How to *prove* the astounding conjecture?

Idea:Find collections $\{P_{j,n}\}$ such that

- $P_{j,n}(T_n) = 0$ for all j if and only if $T_n \in \mathbf{Arith}_{O(n^{2+\epsilon})}$
- Show $P_{j,n}(M_{\langle n \rangle}) = 0$ for all j.

Problem: The zero set of all polynomials vanishing on

$$S := \{(z, w) \mid z = 0,\ w \neq 0\} \subset \mathbb{C}^2,$$

is the line

$$\{(z, w) \mid z = 0\} \subset \mathbb{C}^2.$$

Good news: not a problem for matrix multiplication

For a set $X \subset \mathbb{C}^N$, let

$$\overline{X} := \{y \in \mathbb{C}^N \mid P(y) = 0 \ \forall P \ni P|_X \equiv 0\} \subset \mathbb{C}^N$$

the *Zariski closure* of X.

Polynomials can only detect membership in $\overline{\mathbf{Arith}_r} \subset \mathbb{C}^{r^3}$.

$\mathbf{Arith}_r \subsetneq \overline{\mathbf{Arith}_r}$.

$T \in \mathbb{C}^{r^3}$ has *tensor border rank at most r* if $T \in \overline{\mathbf{Arith}_r}$.
Write $\underline{\mathbf{R}}(T) \leq r$.

Theorem (Bini (1980))

$\underline{\mathbf{R}}(M_{\langle n \rangle}) = O(n^\tau)$ if and only if $M_{\langle n \rangle}$ can be computed with $O(n^\tau)$ arithmetic operations.

State of the art

- [Classical] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq n^2$
- [Strassen (1983)] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq \frac{3}{2}n^2$
- [Lickteig (1985)] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq \frac{3}{2}n^2 + \frac{n}{2} - 1$
- [L-Ottaviani (2012)] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq 2n^2 - n$

The classical result: proof by retreat to linear algebra

Write $A, B, C = \mathbb{C}^r$.

View a bilinear map

$$\begin{aligned} T : A \times B &\to C \\ (a, b) &\mapsto T(a, b) \end{aligned}$$

as a linear map

$$\begin{aligned} T_A : A &\to \{\text{linear maps } B \to C\} \\ a &\mapsto \{b \mapsto T(a, b)\} \end{aligned}$$

Then $\underline{\mathbf{R}}(T) \geq \operatorname{rank}(T_A)$.

Back to permanent v. determinant

Zariski closure is potentially serious difficulty:

Conjecture (Mulmuley (2014))

There are sequences in the closure of the degenerations of the determinant than are not in **VP**.

Algebraic geometry **disadvantage**: potentially wild sequences of polynomials.

Mignon-Ressayre: $n < \frac{m^2}{2} \implies \mathrm{perm}_m \notin \mathrm{End}(\mathbb{C}^{n^2}) \cdot \det_n$

L-Manivel-Ressayre: $n < \frac{m^2}{2} \implies \mathrm{perm}_m \notin \overline{\mathrm{End}(\mathbb{C}^{n^2}) \cdot \det_n}$

Algebraic geometry **advantage**

$$\overline{\mathrm{End}(\mathbb{C}^{n^2}) \cdot \det_n} = \overline{GL_{n^2} \cdot \det_n}$$

An orbit closure!

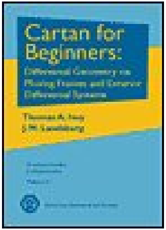
Peter-Weyl Theorem: In principle, modulo the boundary, representation theory describes the ideal of the orbit closure as a GL_{n^2}-module.

$\rightsquigarrow$ interesting questions regarding Kronecker v. plethysm coefficients

$\rightsquigarrow$ difficult extension problem.

Thank you for your attention

For more on **tensors**, their geometry and applications, resp. Gauss maps and local **differential geometry**:



Notes from a **fall 2014 class on geometry and complexity theory at UC Berkeley/Simons Inst. Theoretical computing**: www.math.tamu.edu/∼jml/alltmp.pdf

A **survey on GCT**: www.math.tamu.edu/∼jml/Lgctsurvey.pdf