Symmetry versus Optimality

J.M. Landsberg

Texas A&M University

July 31 2017

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?

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

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

i.e., an element of

$$\mathbb{C}^N \otimes \mathbb{C}^N \otimes \mathbb{C}^N$$

Idea: Look for polynomials P_n on $\mathbb{C}^N \otimes \mathbb{C}^N \otimes \mathbb{C}^N$ 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? - Geometric detour

Let $X \subset \mathbb{CP}^M$ be a projective variety. Stratify $\mathbb{CP}^M$ by a sequence of nested spaces

$$X \subset \sigma_2(X) \subset \sigma_3(X) \subset \cdots \subset \sigma_f(X) = \mathbb{CP}^M$$

where

$$\sigma_r(X) = \overline{\cup_{x_1,\ldots,x_r \in X} \mathrm{span}\{x_1, \ldots, x_r\}}$$

is the variety of secant $\mathbb{P}^{r-1}$'s to X.

How to disprove?- Precise formulation

Let
$X = Seg(\mathbb{P}^{N-1} \times \mathbb{P}^{N-1} \times \mathbb{P}^{N-1}) \subset \mathbb{P}(\mathbb{C}^N \otimes \mathbb{C}^N \otimes \mathbb{C}^N) = \mathbb{CP}^{N^3-1}$ be the Segre variety of rank one tensors.

For $p \in \mathbb{CP}^{N^3-1}$, Let $\underline{\mathbf{R}}(p)$ denote the smallest r such that $p \in \sigma_r(X)$, called the *border rank of p*.

• [Bini, 1980] $\underline{\mathbf{R}}(M_{\langle n \rangle}) = O(n^\tau) \Leftrightarrow n \times n$ matrices can be multiplied using $O(n^\tau)$ arithmetic operations. .

• [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)] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq \frac{3}{2} n^2 + \frac{n}{2} - 1$

2010- state of the art $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq \frac{3}{2} n^2 + \frac{n}{2} - 1$, except it was shown $\underline{\mathbf{R}}(M_{\langle 2 \rangle}) = 7$ (L, 2006, Hauenstein-Ikenmeyer-L, 2013)

How to find equations for $\sigma_r(X)$?- representation theory

$Seg(\mathbb{P}A \times \mathbb{P}B \times \mathbb{P}C)$ is homogeneous for $G = GL(A) \times GL(B) \times GL(C)$.

For any G-variety $X \subset \mathbb{P}V_\lambda$, its ideal will be a G-module, so one should not look for individual polynomials, but modules of polynomials.

Can do systematically in small cases (Hauenstein-Ikenmeyer-L, 2013)

Determinantal equations

Idea: look for G-modules V_μ, V_ν where there exists a G-module inclusion $i : V_\lambda \to V_\mu \otimes V_\nu$. Then

$$\underline{\mathbf{R}}(p) \geq \frac{\operatorname{rank}(i(p))}{\operatorname{rank}(i(x))}.$$

$\rightsquigarrow$

- [L-Ottaviani (2012)] $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq 2n^2 - n$

Limit of the method is $\underline{\mathbf{R}}(p) \geq 2n^2 - 1$.

More symmetry and lower bounds

$M_{\langle n\rangle}$ also has symmetry:
As a trilinear map

$$M_{\langle n\rangle}(X,Y,Z)=\mathrm{trace}(XYZ)$$

and

$$\mathrm{trace}(XYZ)=$$
$$\mathrm{trace}(YZX)=\mathrm{trace}(Z^TY^TX^T)=\mathrm{trace}((gX)Y(Zg^{-1}))=\mathrm{etc}...$$

for $g\in GL_n$.

$$G_{M_{\langle n\rangle}}=PGL_n^{\times 3}\rtimes(\mathbb{Z}_3\rtimes\mathbb{Z}_2)$$

Symmetry combined with "border substitution method" (normal forms and specializations)

$$\rightsquigarrow$$

- [L-Michalek (2016)] $\underline{\mathbf{R}}(M_{\langle n\rangle})\geq 2n^2-\log_2(n)-1$

Game over?

Work of Bernardi-Ranestad (cactus variety fills fast)

and Buczynski-Galazka (determinantal equations are equations for the cactus variety)

$\rightsquigarrow$

Determinantal techniques will never prove $\underline{\mathbf{R}}(M_{\langle n \rangle}) > 6n^2$.

Perhaps try to prove conjecture?

Valiant's conjecture

Gödel, Nash, Soviet Union researchers in 1950's $\rightsquigarrow$

1970's: Cook, Karp, Levin: $\mathbf{P} \neq \mathbf{NP}$: The class of problems that can be solved in polynomial time is smaller than the class of problems whose proposed solutions can be verified in polynomial time.

Valiant: algebraic version: Is a polynomial sequence that can be written down efficiently necessarily efficiently computable?
Conjecture: NO
Example: y: $m \times m$ matrix.

$$\mathrm{perm}_m(y) = \sum_{\sigma \in \mathfrak{S}_m} y_{1,\sigma(1)} \cdots y_{m,\sigma(m)} \in S^m \mathbb{C}^{m^2}$$

Easy to write down. Conjecture: difficult to evaluate

Valiant's conjecture: precise meaning of "difficult"

Theorem (Valiant)

Let P be a homogeneous polynomial of degree m in M variables. Then there exists an n and $n \times n$ matrices $A_0, A_1, \ldots, A_M$ such that

$$P(y^1, \ldots, y^M) = \det_n(A_0 + y^1 A_1 + \cdots + y^M A_M).$$

Write $P(y) = \det_n(A(y))$.

Let $\mathrm{dc}(P)$ be the smallest n that works.

Conjecture (Valiant)

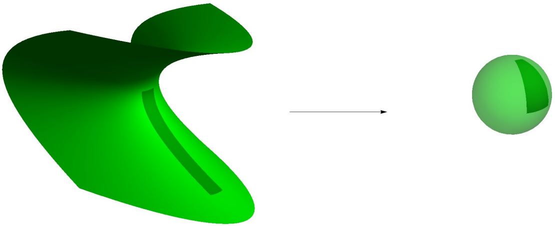
$\mathrm{dc}(\mathrm{perm}_m)$ *grows faster than any polynomial in m.*

State of the art

• $\mathrm{dc}(\mathrm{perm}_2) = 2$ (classical)

$$\mathrm{perm}_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det{}_2 \begin{pmatrix} a & -b \\ c & d \end{pmatrix}$$

• $\mathrm{dc}(\mathrm{perm}_m) \geq \frac{m^2}{2}$ (Mignon-Ressayre, 2005) Proof via differential geometry: Gauss maps.



Zariski closed version: Mulmuley-Sohoni

Idea: translate problem to an orbit closure containment problem by allowing limits. Let $\overline{\mathrm{dc}}(\mathrm{perm}_m)$ smallest n in this enlarged category of degenerations.

• $\overline{\mathrm{dc}}(\mathrm{perm}_m) \geq \frac{m^2}{2}$ (L-Manivel-Ressayre, 2013)

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

Paths towards Valiant's conjecture

Restricted models: solve the conjecture assuming extra hypotheses.
• [Nisan, 1991]: Exponential lower bound assuming non-commutative multiplication. Defect: same exponential lower bound holds for the determinant. Other similar results with same defect.

Occurance obstructions [Mulmuley-Sohoni 2001] Use representation theory to separate permanent from determinant by finding a module that does not occur in the orbit closure of the determinant that could occur in the orbit closure of the permanent.
• [Ikenmeyer-Panova 2016, Bürgiser-Ikenmeyer-Panova 2016, Gesmundo-Ikenmeyer-Panova 2017] This cannot work.

Shifted partial derivatives [Gupta, Kamath, Kayal, Saptharishi, 2013]: Use Hilbert functions of Jacobian varieties.
• [Efremenko-L-Schenck-Weyman 2015, Gesmundo-L 2017] This cannot work.

Upper bounds?

- [Grenet 2011] $\mathrm{dc}(\mathrm{perm}_m) \leq 2^m - 1$, via explicit expressions

- [Alper-Bogart-Velasco 2015] $\mathrm{dc}(\mathrm{perm}_3) = 7$. In particular, Grenet's representation for perm_3:

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

is optimal.

- [L-Ressayre 2015]: Grenet's expressions have symmetry

Symmetry v. Optimality

Main question of talk:

If a tensor or polynomial has symmetry, does it admit an optimal expression with (some) symmetry?

Strassen's algorithm revisited

• [Burichenko 2014]: Strassen's optimal decomposition has $\mathfrak{S}_3 \rtimes (\mathbb{Z}_3 \rtimes \mathbb{Z}_2)$ symmetry, where $\mathfrak{S}_3 \subset PGL_2 \subset PGL_2^{\times 3}$.

$$M_{\langle 2\rangle} = \mathrm{Id}_2^{\otimes 3} + \mathbb{Z}_3 \rtimes \mathbb{Z}_2 \cdot \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \right).$$

Work in progress (Ballard-Conner-Ikenmeyer-L-Ryder): look for matrix multiplication decompositions with symmetry.

In particular, cyclic $\mathbb{Z}_3$ symmetry.

Symmetry v. Optimality

The smallest known decomposition of $M_{\langle 3 \rangle}$ is of size 23.

We found rank 23 decompositions with extra symmetry.

A decomposition with $\mathbb{Z}_4 \times \mathbb{Z}_3$-symmetry

$$
\begin{aligned}
M_{\langle 3\rangle} = &- \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}^{\otimes 3} \\
&+ \mathbb{Z}_4 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}^{\otimes 3} \\
&+ \mathbb{Z}_4 \cdot \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}^{\otimes 3} \\
&+ \mathbb{Z}_2 \cdot \begin{pmatrix} 0 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}^{\otimes 3} \\
&+ \mathbb{Z}_3 \times \mathbb{Z}_4 \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ 0 & 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

What next?

Bad news: standard numerical search for $\mathbb{Z}_3$-invariant decompositions still to large for $M_{\langle 4 \rangle}$.

Good news: method extends using geometric building blocks. (Work in progress.)

Symmetry and permanent v. determinant

Geometric complexity theory (GCT) principle: perm_m and $\det_n$ are special because they are determined by their *symmetry groups*:

A, B: $n \times n$ matrices with determinant one, then $\det_n(AXB) = \det_n(X)$, and $\det_n(X^T) = \det_n(X)$.

$G_{\det_n}$ is the subgroup of GL_{n^2} generated by such.

σ, τ: $m \times m$ permutation matrices or diagonal matrices with determinant one, then $\mathrm{perm}_m(\sigma y \tau) = \mathrm{perm}_m(y)$, and $\mathrm{perm}_m(y^T) = \mathrm{perm}_m(y)$.

G_{perm_m} is the subgroup of GL_{m^2} generated by such.

Let $G^L_{\mathrm{perm}_m}$ be the subgroup of G_{perm_m} generated by the σ's.

Equivariance

Let $G \subseteq G_P$. A determinantal expression $A : \mathbb{C}^M \to \mathbb{C}^{n^2}$ for $P \in S^m\mathbb{C}^M$ is *G-equivariant* if given $g \in G$, there exist $(B, C) \in GL_n \times GL_n \subset G_{det_n}$ such that

$$A(g \cdot y) = BA(y)C$$

or $A(g \cdot y) = BA(y)^T C$.

In other words, there exists an injective group homomorphism $\psi : G \to G_{\mathrm{det}_n}$ such that $A(y) = \psi(g) \cdot (A(g \cdot y))$.

•[L-Ressayre, 2015]: Grenet's expressions $A_{Grenet} : \mathbb{C}^{m^2} \to \mathbb{C}^{n^2}$ such that $\mathrm{perm}_m(y) = \mathrm{det}_n(A_{Grenet}(y))$ are $G^L_{\mathrm{perm}_m}$-equivariant.

Example

Let

$$g(t) = \begin{pmatrix} t_1 & & \\ & t_2 & \\ & & t_3 \end{pmatrix}.$$

Then $A_{Grenet,3}(g(t)y) = B(t)A_{Grenet,3}(y)C(t)$, where

$$B(t) = \begin{pmatrix} t_3 & & & & & & \\ & t_1 t_3 & & & & & \\ & & t_1 t_3 & & & & \\ & & & t_1 t_3 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix} \quad \text{and} \quad C(t) = B(t)^{-1}.$$

Invariant description of Grenet's expressions

Let $E, F = \mathbb{C}^m$. The space $S^k E$ is an irreducible $GL(E)$-module but it is is not in general irreducible as a $G^L_{\mathrm{perm}_m}$-module. Let

$e_1, \ldots, e_m$ be a basis of E, and let $(S^k E)_{reg} \subset S^k E$ denote the span of the square-free monomials: $(S^k E)_{reg}$ is an irreducible $G^L_{\mathrm{perm}_m}$-submodule of $S^k E$. There exists a unique

$G^L_{\mathrm{perm}_m}$-equivariant projection π_k from $S^k E$ to $(S^k E)_{reg}$.

For $v \in E$, define $s_k(v) : (S^k E)_{reg} \to (S^{k+1} E)_{reg}$ to be multiplication by v followed by π_{k+1}.

Fix a basis $f_1, \ldots, f_m$ of F^*. If $y = (y_1, \ldots, y_m) \in E \otimes F$, let $(s_k \otimes f_j)(y) := s_k(y_j)$.

Invariant description of Grenet's expressions

•[L-Ressayre, 2015] The following is Grenet's determinantal representation of perm_m. Let $\mathbb{C}^n = \bigoplus_{k=0}^{m-1} (S^k E)_{reg}$, so $n = 2^m - 1$, and identify $S^0 E \simeq (S^m E)_{reg}$. Set

$$A_0 = \sum_{k=1}^{m-1} \mathrm{Id}_{(S^k E)_{reg}}$$

and define

$$A = A_0 + \sum_{k=0}^{m-1} s_k \otimes f_{k+1}. \tag{1}$$

Then $(-1)^{m+1} \mathrm{perm}_m = \det_n \circ A$. To obtain the permanent exactly, replace $\mathrm{Id}_{(S^1 E)_{reg}}$ by $(-1)^{m+1} \mathrm{Id}_{(S^1 E)_{reg}}$ in the formula for A_0.

Remark: the s_k's give the dual complex to the Koszul under the Howe-Young endofunctor induced by the involution on symmetric functions.

Results

•[L-Ressayre, 2015] Among $G^L_{\mathrm{perm}_m}$-equivariant determinatal expressions for perm_m, Grenet's expressions are optimal and unique up to trivialities.

•[L-Ressayre, 2015] There exists a G_{perm_m}-equivariant determinantal expression for perm_m of size $\binom{2m}{m} - 1$.

•[L-Ressayre, 2015] Among G_{perm_m}-equivariant determinatal expressions for perm_m, the size $\binom{2m}{m} - 1$ expressions are optimal and unique up to trivialities.

Let $\mathrm{edc}(P)$ denote the smallest size equivariant determinantal expression for a polynomial P. For P generic, $\mathrm{edc}(P) = \mathrm{dc}(P)$ and $\mathrm{edc}(\det_m) = \mathrm{dc}(\det_m) = m$. Define the restricted model of equivariant determinantal expressions. Valiant's conjecture holds in this restricted model.

To my knowledge, equivariant determinantal complexity is the only restricted model with an exponential separation of the permanent from the determinant.

Thank you for your attention

For more on geometry and complexity: