How to find hay in a haystack?

Joseph (J.M.) Landsberg

Owen Professor of Mathematics, Texas A&M University

Supported by NSF grant AF-2203618

The problem

A random polynomial (or tensor, i.e., multi-linear map) is difficult to evaluate.

The problem: Write down *explicit* polynomials (tensors) that are difficult to evaluate.

More precisely: write down explicit sequences of polynomials (tensors) that are difficult to evaluate.

This talk is about explicit polynomials (tensors) that behave like random ones as far as their complexity is concerned.

Non-example: $\det_n$: homogeneous polynomial of degree n in n^2 variables,
$\det_n(X) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$
explicit, each term easy to describe (coeffs $0, \pm 1$). Despite $n!$ terms, easy to evalulate (Gaussian elimination)

Warning

Classical text: Computational Complexity (Arora and Barak)

Chapter 14: Circuit lower bounds: Complexity theory's Waterloo

General strategy

Prove lower bounds for polynomials (tensors) with symmetry.

Example of polynomial with a lot of symmetry: $\det_n$
as $\det_n(X) = \det_n(gXh)$, g, h: matrices with $\det = 1$
$\dim(G_{\det_n}) \sim 2n^2 - 2$.

Others?

The most famous version (L. Valiant 1978)

Conjecture (Valiant, algebraic version of P v. NP) There exist explicit sequences of polynomials that are nearly as difficult to evaluate as random ones.

More precise version:

Thm. (Valiant) Any polynomial $p(x_1, \ldots, x_M)$ may be expressed as the determinant of an $N \times N$ matrix whose entries are affine linear forms in the x_i, for some N.

Moreover, the smallest N that works, denoted $dc(p)$, captures the complexity of evaluating p.

Conjecture: Let $\mathrm{perm}_m \in S^m(\mathbb{C}^{m^2})$ denote the permanent. Then $dc(\mathrm{perm}_m)$ grows faster than any polynomial in m.

Note perm_m has symmetry:
$\mathrm{perm}_m(Y) = \mathrm{perm}_m(gYh)$ where g, h either permutation matrices or diagonal with determinant one.
$\dim(G_{\mathrm{perm}_m}) = 2m - 2$

Example (B. Grenet 2011)

$$\mathrm{perm}_3 \begin{pmatrix} y_1^1 & y_2^1 & y_3^1 \\ y_1^2 & y_2^2 & y_3^2 \\ y_1^3 & y_2^3 & y_3^3 \end{pmatrix} = \det{}_7 \begin{pmatrix} 0 & 0 & 0 & 0 & y_3^3 & y_2^3 & y_1^3 \\ y_1^1 & 1 & & & & & \\ y_2^1 & & 1 & & & & \\ y_3^1 & & & 1 & & & \\ & y_2^2 & y_1^2 & 0 & 1 & & \\ & y_3^2 & 0 & y_1^2 & & 1 & \\ & 0 & y_3^2 & y_2^2 & & & 1 \end{pmatrix}$$

So $dc(\mathrm{perm}_3) \leq 7$. Known $= 7$, moreover (Mignon-Ressayre 2004) $dc(\mathrm{perm}_m) \geq \frac{m^2}{2}$. Proof via local differential geometry.
Still state of the art.

Grenet's example in general

Grenet:

$$dc(\text{perm}_m) \leq 2^m - 1$$

Prop. (L-Ressayre 2017): Grenet's example has symmetry. $(\mathfrak{S}_m \times \mathbb{T}_m)$, about half the symmetries of perm_m.

More precisely: map $\mathbb{C}^{m^2} \to \mathbb{C}^{(2^m-1)^2}$ is equivariant for $\mathfrak{S}_m \times \mathbb{T}_m$.

Theorem (L-Ressayre 2017): If insist on expressions with symmetry, Grenet's example is optimal.

Allowing a small error

Example: $p(x, y) = x^2 y$ cannot be written as a sum of two cubes $\ell_1^3 + \ell_2^3$.

But $p(x, y) = \lim_{\epsilon \to 0} \frac{1}{3\epsilon}[(x + \epsilon y)^3 - x^3]$

Let $\overline{dc}(p)$ be smallest N such that p may be expressed as a determinant with error at most ϵ, any $\epsilon > 0$.

Theorem (L-Manivel-Ressayre 2013) $\overline{dc}(\mathrm{perm}_3) \geq \frac{m^2}{2}$.

To solve, had to solve a 100 year old question in algebraic geometry about dual varieties.

Notation

$A = \mathbb{C}^{\mathbf{a}}$: column vectors,
$GL(A)$: group of invertible linear maps $A \to A$ i.e., group of changes of bases.

A^*: row vectors = space of linear maps $A \to \mathbb{C}$, where $\alpha \in A^*$, $v \in A$, $\alpha(v) = \alpha v$, row-column mult.

$\mathbf{a} \times \mathbf{b}$ matrix M

Could represent
$M : B \to A$ linear map
$w \mapsto Mw$.
Or bilinear form
$M : A^* \times B \to \mathbb{C}$
$(\alpha, w) \mapsto \alpha M w$
Both cases: Same group action $GL(A) \times GL(B)$
Normal forms $\begin{pmatrix} \mathrm{Id}_k & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$
$0 \leq k \leq \min\{\mathbf{a}, \mathbf{b}\}$: finite number of orbits

Group actions

Bilinear forms: $GL(A) \times GL(B)$ acts on $A \otimes B$, finite number of orbits, simple normal form for each.

Use: efficient algorithm to solve systems of linear equations (ancient China, rediscovered by Gauss) or to compute determinant

Exploit (part of) group action to put system in easy form.

Tensors

Now consider $T \in A \otimes B \otimes C$. (or $T \in A_1 \otimes \cdots \otimes A_k$)

Trilinear form $A^* \times B^* \times C^* \to \mathbb{C}$.

Bilinear map $A^* \times B^* \to C$.

Linear map $T_A : A^* \to B \otimes C$

Note
$\dim(\mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m) = m^3 >> 3m^2 = \dim(GL_m \times GL_m \times GL_m)$, no hope for normal forms in general.

Example: $A^*, B^*, C = \mathcal{A}$ algebra, $T = T_{\mathcal{A}}$ structure tensor. i.e., $T_{\mathcal{A}}(a_1, a_2) := a_1 a_2$.
In particular, A, B, C space of $n \times n$ matrices $T = M_{\langle n \rangle}$ structure tensor of matrix multiplication.

Complexity of Tensors

Def. $T \in A \otimes B \otimes C$ has *rank one* if $\exists\ a \in A,\ b \in B,\ c \in C$ such that $T = a \otimes b \otimes c$.

rank $\mathbf{R}(T)$: smallest r such that T is a sum of r rank one tensors

border rank $\underline{\mathbf{R}}(T)$: The smallest r such that T is a limit of rank r tensors.

Both $\mathbf{R}(T)$ and $\underline{\mathbf{R}}(T)$ measure the complexity of evaluating the bilinear map associated to T.
Thm. (Essentially Terracini 1911, Precise version Lickteig 1985): Let $T \in \mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$. If T is random, (and $m \neq 3$) then

$$\underline{\mathbf{R}}(T) = \mathbf{R}(T) = \lceil \frac{m^3}{3m-2} \rceil \sim m^2/3$$

Hay in a haystack problem for tensors: find an explicit tensor with rank or border rank of a random tensor, or at least large border rank (complexity).

Hay in a haystack for tensors (embarassing state of the art)

Have explicit $T \in \mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$
(resp. explicit sequence $T_m \in \mathbb{C}^m \otimes \mathbb{C}^m \otimes \mathbb{C}^m$) with:

Classical $\underline{\mathbf{R}}(T_m) \geq m$.

Strassen (1983) $\underline{\mathbf{R}}(T_m) \geq \frac{3}{2}m$. In particular $m = 3$, explicit with random border rank 5.

Lickteig (1985) $\underline{\mathbf{R}}(T_m) \geq \frac{3}{2}m + \frac{1}{2}\sqrt{m} - 1$.

L (2005) $m = 4$, $\underline{\mathbf{R}}(M_{\langle 2 \rangle}) = 7$, random border rank.

L-Ottaviani (2010) $\underline{\mathbf{R}}(M_{\langle n \rangle}) \geq 2n^2 - n$, i.e., explicit sequence with $\underline{\mathbf{R}}(T_m) \geq 2m - \sqrt{m}$

L (2015) explicit sequence with $\underline{\mathbf{R}}(T_m) \geq 2m - 2$
Other than trivial cases, $\mathbf{a} = \mathbf{b} = \mathbf{c} \leq 4$, in 2023 only cases with explicit tensor of random border rank.

Theorem (D. Wu 2024) Explicit tensor in $\mathbb{C}^3 \otimes \mathbb{C}^6 \otimes \mathbb{C}^8$ with border rank of a random tensor (namely 10).
largest case where hay in a haystack problem is solved.

Idea of proofs: retreat to linear algebra

Choose linear map $f : A{\otimes}B{\otimes}C \to U{\otimes}V$.

Say $\mathrm{rank}(f(a{\otimes}b{\otimes}c)) \leq s$ for all rank one tensors.

Then if $\mathrm{rank}(f(T)) > sr$, conclude $\underline{\mathbf{R}}(T) > r$.

Choice of f made with aid of representation theory.

Example: $U = \Lambda^p A^*{\otimes}B$ and $V = \Lambda^{p+1}A{\otimes}C$, judiciously chosen p.

Rem: this gives rise to best bounds, but ~ 1 year to implement for $M_{\langle n\rangle}$.

Theorem (Efremenko-Garg-Oliviera-Wigderson 2017) Game (almost) over for these methods.

A phyrric victory

Idea: use tensors with special symmetry and Borel fixed point theorem to prove non-existence of border rank decompositions.

More precisely: if can show that restricting T to any $\mathbb{B}_T$-fixed hyperplane has border rank at least k, then $\underline{\mathbf{R}}(T) \geq k+1$. Here $\mathbb{B}_T \subset G_T$ is a Borel subgroup. "border substitution method"

$\rightsquigarrow$
(L-Michalek 2022): Explicit sequence with $\underline{\mathbf{R}}(T_m) \geq (2.02)m$.

A path to breaking the barriers: Buczynska-Buczynski 2022

Classical v. Modern algebraic geometry: shift in perspective from the geometric object to its ideal.

To prove lower bounds for T, prove there does not exist a curve of ideals. Sufficient to prove there does not exist a Borel fixed limit point.

Conner-Harper-L (2023): used to prove many new lower bounds, in particular $\underline{\mathbf{R}}(M_{\langle 3\rangle}) \geq 17$, $\underline{\mathbf{R}}(\det_3) \geq 17$, in fact $= 17$, and (C-Huang-L 2023) $\underline{\mathbf{R}}(\mathrm{perm}_3) = 16$.

The problem of univited guests: not all Borel fixed limit points come from an admissible curve. Similar barrier.

Work in progress (with Conner, Huang, Mandziuk): use deformation theory to get rid of uninvited guests, i.e. to overcome barrier. So far: small test cases. Stay tuned!

Thank you for your attention

For more on **tensors**, their geometry and applications, resp. **geometry and complexity**, resp. **asymptotic geometry**, resp. **quantum computation and information**: