# Recent progress on geometric complexity theory

Christian Ikenmeyer

UNIVERSITY OF LIVERPOOL

Oxford-Warwick Complexity Meeting
2020-Oct-15

# Agenda

# Agenda

## The quest for computational complexity lower bounds

- The separation of complexity classes such as P and NP is one of the most fundamental open problems at the intersection of theoretical computer science and mathematics.
- Progress has been very slow! Proving lower bounds seems very difficult!
- Valiant (1979) found a close connection between complexity questions and natural questions in algebra:

**Theorem (Valiant 1979)**

Every multivariate polynomial $f$ can be written as the determinant of a matrix whose entries are polynomials of degree $\leq 1$. The dimension of the matrix is at most the smallest number of arithmetic operations in a formula computing $f$.

Example: $$f := y + 2x + xz + 2xy - x^2z = \det \begin{pmatrix} x & y & 0 \\ -1 & z+y+2 & x \\ 1 & z & 1 \end{pmatrix}$$

Def.: Required dimension of the matrix is called the **determinantal complexity** $\mathrm{dc}(f)$.

In the example we have $\mathrm{dc}(f) \leq 3$.

The class VDET consists of all sequences of polynomials $f_m$ with polyn. bounded $\mathrm{dc}(f_m)$.

"VDET = easy to compute"

Examples: $\det_m \in \mathrm{VDET}$, $x_1 x_2 \cdots x_m \in \mathrm{VDET}$, $x_1^m + x_2^m + \cdots + x_m^m \in \mathrm{VDET}$

# The permanent polynomial and VNP

$\mathrm{per}_m(x_{1,1}, x_{1,2}, \ldots, x_{m,m}) := \sum_{\pi \in \mathfrak{S}_m} x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{m,\pi(m)}$

- Set all $x_{i,j}$ to 0 or 1: then $\mathrm{per}_m$ = number of perfect matchings in bipartite graph.
- Set all $x_{i,j}$ to 0 or 1: then $\mathrm{per}_m$ = number of cycle covers in directed graph.
- Applications in theor. physics: Wavefunctions describing identical bosons
- $\#P$-complete as a function

**Valiant's universality theorem holds also for the permanent:**

Every multivariate polynomial $f$ can be written as the permanent of a matrix whose entries are polynomials of degree $\leq 1$.

Def.: Required size of the matrix is called the **permanental complexity** $\mathrm{pc}(f)$.
The class VNP consists of all sequences of polynomials $f_m$ with polyn. bounded $\mathrm{pc}(f_m)$.

**Valiant's "Determinant vs Permanent" Conjecture (1979)**

- VDET $\neq$ VNP. Equivalently: $\mathrm{dc}(\mathrm{per}_m)$ is not polynomially bounded.

Remark: Over characteristic 2 we have $\mathrm{per}_m = \det_m$, so we replace $\mathrm{per}_m$ by the Hamiltonian cycle polynomial.

## Connections to Boolean complexity

Separating VDET $\neq$ VNP is "easier" than Boolean complexity (Bürgisser 1998):

- $\mathsf{P}/\mathrm{poly} \neq \mathsf{NP}/\mathrm{poly}$ implies VDET $\neq$ VNP over finite fields.
- $\mathsf{P}/\mathrm{poly} \neq \mathsf{NP}/\mathrm{poly}$ implies VDET $\neq$ VNP over $\mathbb{C}$, assuming the generalized Riemann hypothesis.

$\mathsf{P}/\mathrm{poly} \neq \mathsf{NP}/\mathrm{poly}$ is widely believed: If $\mathsf{NP} \subseteq \mathsf{P}/\mathrm{poly}$, then

- $\mathsf{PH} = \Sigma_2^{\mathsf{P}}$ (Karp-Lipton, 1980, Sipser) and
- AM $=$ MA (Arvind, Köbler, Schöning, 1995).

# Determinantal complexity of the permanent

Upper bound:

- $\mathrm{dc}(\mathrm{per}_m) \leq 2^m - 1$ [Grenet; 2011]

Lower bounds:

- $\mathrm{dc}(\mathrm{per}_m) \geq \frac{m^2}{2}$ over $\mathbb{C}$ [Mignon, Ressayre; 2004]
- $\mathrm{dc}(\mathrm{per}_m) \geq (m-1)^2 + 1$ over $\mathbb{R}$ [Yabe; 2015]
- $\mathrm{dc}(\mathrm{per}_3) = 7$ [Alper, Bogart, Velasco; 2015]
- $\mathrm{dc}(\mathrm{per}_4) \geq 9$ [Alper, Bogart, Velasco; 2015]

[Bringmann, I, Zuiddam; JACM 2018] **simplifies** the computational model:
Same as determinantal complexity, but the only allowed matrices are:

- Tridiagonal matrices with secondary diagonals only 1s.

$$\det\begin{pmatrix} x & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & x & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = x+1 \qquad \det\begin{pmatrix} \varepsilon^{-1}x & 1 & 0 & 0 & 0 \\ 1 & \varepsilon^2 & 1 & 0 & 0 \\ 0 & 1 & -\varepsilon^{-1}x & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & y \end{pmatrix} = \underbrace{x^2+y-\varepsilon xy}_{\overset{\varepsilon\to 0}{\longrightarrow} x^2+y}$$

The required matrix dimension is called the **continuantal complexity** $\mathrm{cc}(f)$.
(Name based on the continuant polynomial from the theory of continued fractions)
For some polynomials $\mathrm{cc}(f) = \infty$ (Allender, Wang 2011).

**Definition (border continuantal complexity)**

Let $\underline{\mathrm{cc}}(f)$ denote the smallest $n$ such that $f$ can be approx. arbitrarily closely by polynomials $f_\varepsilon$ with $\mathrm{cc}(f_\varepsilon) \leq n$.

**Theorem [Bringmann, I, Zuiddam]**

$\underline{\mathrm{cc}}(f) < \infty$. Moreover, if $\underline{\mathrm{cc}}(\mathrm{per}_m)$ grows superpolynomially, then $\mathrm{VF} \neq \mathrm{VNP}$
($\mathrm{VF} = \mathrm{VDET}$ up to quasipolynomial blowup).

$\to$ The definition of $\underline{\mathrm{cc}}$ is analogous to border Waring rank (fast matrix multiplication)!

# Waring rank

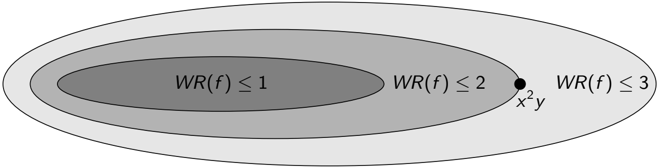
## Theorem (Waring rank is finite)

For every homogeneous degree $d$ polynomial $f$ there exists a decomposition $f = \sum_{i=1}^{r} (\ell_i)^d$, where each $\ell_i$ is a homogeneous linear polynomial. The smallest possible $r$ is called the **Waring rank** $WR(f)$ or **symmetric rank** of $f$.

Remark: Waring rank was used by Pratt [FOCS 2019] to obtain a faster algorithm for approximately counting subgraphs of bounded treewidth.

Example:

$6x^2y = (x+y)^3 + (y-x)^3 - 2x^3$, hence $\mathrm{WR}(x^2y) \le 3$. In fact, $\mathrm{WR}(x^2y) = 3$.




$3x^2y = \lim_{\varepsilon \to 0} \frac{1}{\varepsilon}\left((x+\varepsilon y)^3 - x^3\right)$

This makes determining $WR(W)$ subtle! Continuous methods cannot prove $WR(W) > 2$.

The **border Waring rank** $\underline{WR}(f)$ is defined as the smallest $r$ such that $f$ can be approximated arbitrarily closely by polynomials of Waring rank $\le r$.

# Border Waring rank of cubic polynomials: fast matrix multiplication

$$M_m := \sum_{i,j,k=1}^{m} x_{i,j} \cdot x_{j,k} \cdot x_{k,i} \in \mathbb{C}[x_1, \ldots, x_{m^2}]_3$$

$\omega :=$ smallest $k$ such that for all $\varepsilon > 0$ there exists an $O(n^{k+\varepsilon})$ time algorithm to multiply to $n \times n$ matrices.

**Theorem [Chiantini, Hauenstein, I., Landsberg, Ottaviani 2017]**

$\omega = \liminf\{\log_m WR(M_m)\} = \liminf\{\log_m \underline{WR}(M_m)\}$

Recent progress (Alman and Vassilevska Williams, SODA2021): $\omega \leq 2.3728639$

# Summary part I

- If NP $\not\subseteq$ P$/\mathrm{poly}$, then $\mathrm{dc}(\mathrm{per}_m)$ grows superpolynomially (assuming GRH).
- The study of $\mathrm{dc}(\mathrm{per}_m)$ is difficult. Continuantal complexity is a simpler model of computation, but it requires approximations.
- Such approximations are classically studied in the setting of fast matrix multiplication.

We will now see: These approximations are hard-wired into GCT

## Orbit closures and the padded permanent

Define $E(\mathrm{det}_n)$ := determinants of $n \times n$ matrices whose entries are homogeneous linear polynomials.

$$\det \begin{pmatrix} x_{1,1}+x_{1,2} & x_{1,2}-2x_{2,2} \\ x_{2,1} & x_{1,1}+x_{1,2} \end{pmatrix} = x_{1,1}^2 + 2x_{1,1}x_{1,2} + x_{1,2}^2 - x_{1,2}x_{2,1} + 2x_{2,1}x_{2,2} \in E(\mathrm{det}_2)$$

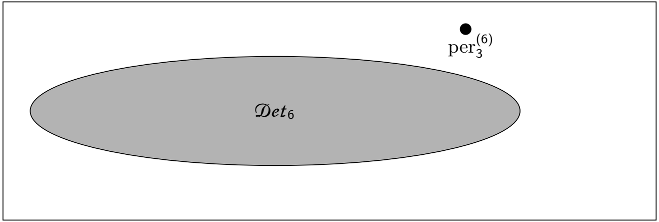
Using approximations can be naturally be phrased as the Euclidean closure (equivalent to Zariski closure here): $\mathcal{D}et_n := \overline{E(\mathrm{det}_n)}$.
[Hüttenhain, Lairez; 2016] classify all polynomials that are in $\mathcal{D}et_3$ but not in $E(\mathrm{det}_3)$. E.g.,
$x_1^2y_1 + x_2^2y_2 + x_3^2y_3 + x_1x_2z_3 + x_1z_2x_3 + z_1x_2x_3$

### Lower bound method [Mulmuley and Sohoni, 2001]

Define the **padded permanent**: $\mathrm{per}_m^{(n)} := x_{1,1}^{n-m}\mathrm{per}_m$.

$$\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n \quad \text{implies} \quad \mathrm{dc}(\mathrm{per}_m) > n.$$

With algebraic geometry one can show: $\mathcal{D}et_n$ is a **projective variety**.
This gives a lot of additional structure to $\mathcal{D}et_n$!
In particular, we "know in principle how to separate" $\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$



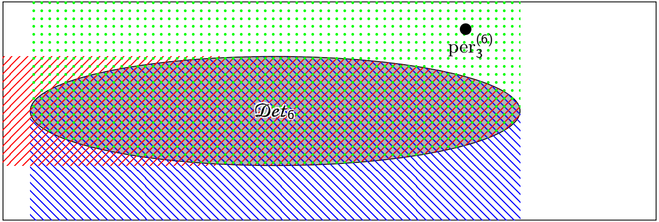

would imply $\mathrm{dc}(\mathrm{per}_3) > 6$

# $\mathcal{D}et_n$ is a projective variety

A subset $\mathcal{D} \subseteq \mathbb{C}^N$ is a **projective variety** if there exist finitely many homogeneous polynomials $\Delta_1, \ldots, \Delta_k$ such that

$$f \in \mathcal{D} \quad \text{iff} \quad \Delta_1(f) = \Delta_2(f) = \cdots = \Delta_k(f) = 0.$$

$\mathcal{D}et_n$ is a projective variety (by Chevalley's theorem).




would imply $\mathrm{dc}(\mathrm{per}_3) > 6$

## Consequence: Points can be separated from varieties via **polynomials**

$\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$ iff there exists a homogeneous polynomial $\Delta$ with

- $\Delta(f) = 0$ for all $f \in \mathcal{D}et_n$ and
- $\Delta(\mathrm{per}_m^{(n)}) \neq 0$.

Meta-complexity (algebraic natural proofs): What can be said about the complexity of the $\Delta_i$?

# Toy example (Waring rank)

$\mathbb{A} := \mathbb{C}[x,y]_2 = \langle x^2, xy, y^2 \rangle$.

Every element in $\mathbb{A}$ can be represented as $ax^2 + bxy + cy^2$.

- $\mathcal{D} := \{f \in \mathbb{A} \mid \exists \alpha, \beta \in \mathbb{C} : f = (\alpha x + \beta y)^2\}$ Waring rank 1 polynomials
- $f \in \mathcal{D}$ iff $\Delta(f) = b^2 - 4ac = 0$.
- To prove $f$ has $\mathrm{WR}(f) \geq 2$ we compute $\Delta(f) \neq 0$. For example, $\Delta(xy) = 1 \neq 0$, hence $\mathrm{WR}(xy) \geq 2$.
- We want to study these functions that behave like $\Delta$: **Representation theory**

For $f(x,y) \in \mathcal{D}$ we see that also $f(y,x) \in \mathcal{D}$.

What happens to $b^2 - 4ac$ is we switch the roles of $x$ and $y$?

- $\tau(x) = y$ and $\tau(y) = x$
- $\tau(x^2) = y^2$, $\tau(y^2) = x^2$, $\tau(xy) = xy$
- $\tau(a) = c$, $\tau(c) = a$, $\tau(b) = b$
- $\tau(b^2) = b^2$, $\tau(ac) = ac$
- $\tau(b^2 - 4ac) = b^2 - 4ac$

## Group actions

$\Delta := b^2 - 4ac$.

Switching the roles of $x$ and $y$ is denoted by a multiplication with the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Delta = \Delta.$

For any $2 \times 2$ matrix $A$: $A\Delta = \det(A)^2 \Delta$.

In particular

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \Delta = \Delta; \qquad \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \Delta = \alpha_1^2 \alpha_2^2 \Delta$$

Thus $\Delta$ is a **highest weight polynomial of weight (2,2).**

**Definition (highest weight polynomial)**

A function $\Delta$ is called a **highest weight polynomial** of weight $\lambda = (\lambda_1, \dots, \lambda_N)$, if

- $\Delta$ is invariant under the action of upper triangular matrices with 1s on the diagonal
- and $\Delta$ gets rescaled by $\alpha_1^{\lambda_1} \cdots \alpha_N^{\lambda_N}$ under the action of diagonal matrices $\mathrm{diag}(\alpha_1, \dots, \alpha_N)$.

# Complexity lower bounds via highest weight polynomials

## Definition (highest weight polynomial)

A function $\Delta$ is called a **highest weight polynomial** of weight $\lambda = (\lambda_1, \ldots, \lambda_N)$, if

- $\Delta$ is invariant under the action of upper triangular matrices with 1s on the diagonal
- and $\Delta$ gets rescaled by $\alpha_1^{\lambda_1} \cdots \alpha_N^{\lambda_N}$ under the action of diagonal matrices $\mathrm{diag}(\alpha_1, \ldots, \alpha_N)$.

Recall: Want $\Delta$ vanishing on $\mathcal{D}et_n$ and $\Delta(\mathrm{per}_m^{(n)}) \neq 0$.

## Theorem (representation theory)

If $\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$, then there exists a highest weight polynomial $\Delta$ such that $A\Delta$ vanishes on $\mathcal{D}et_n$ and $A\Delta(\mathrm{per}_m^{(n)}) \neq 0$ for a generic matrix $A$.

This works in high generality. We just need that $\mathcal{D}et_n$ is closed under the action of $\mathrm{GL}_{n^2}$.

## Crucial conclusion

If complexity lower bounds exist, then there exist highest weight polynomials proving them.

# Complexity of highest weight polynomials

**Crucial conclusion**

If complexity lower bounds exist, then there exist highest weight polynomials proving them.

**Theorem (Garg, I, Makam, Oliveira, Walter, Wigderson, CCC 2020)**

The hyperpfaffian, which is a highest weight polynomial, is VNP-complete.

**Theorem (Bläser, Dörfler, I, arXiv:2002.11594)**

If highest weight polynomials are encoded efficiently (not as a coefficient list, but as Young tableaux), then it is NP-hard to evaluate them at a point of Waring rank 3.
(Efficient evaluation is possible if the tableau has low treewidth.)

# Mulmuley and Sohoni's heuristic attempt: Occurrence Obstructions

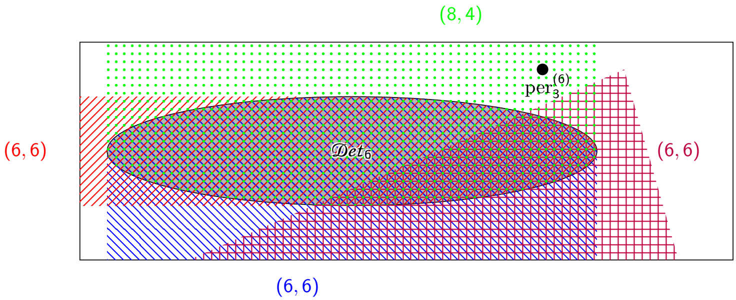
Consider the finite dimensional vector space of highest weight polynomials $\Delta$ of weight $\lambda$.

**Proposition (a coarse technique for finding complexity lower bounds)**

If there exists $\lambda$ such that for a generic matrix $A$ we have

- for **all (!)** highest weight polynomials $\Delta$ of weight $\lambda$: $A\Delta$ vanishes on $\mathcal{D}et_n$
- there exists a highest weight polynomial $\Delta$ of weight $\lambda$ such that $A\Delta(\mathrm{per}_m^{(n)}) \neq 0$

then $\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$.



# Mulmuley and Sohoni's heuristic attempt: Occurrence Obstructions

Consider the finite dimensional vector space of highest weight polynomials $\Delta$ of weight $\lambda$.

**Proposition (a coarse technique for finding complexity lower bounds)**

If there exists $\lambda$ such that for a generic matrix $A$ we have

- for **all (!)** highest weight polynomials $\Delta$ of weight $\lambda$: $A\Delta$ vanishes on $\mathcal{D}et_n$
- there exists a highest weight polynomial $\Delta$ of weight $\lambda$ such that $A\Delta(\mathrm{per}_m^{(n)}) \neq 0$

then $\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$.

- We used this approach to show nontrivial border rank lower bounds for the matrix multiplication tensor [Bürgisser, I; STOC 2011, STOC 2013].
- Mulmuley and Sohoni conjectured that this approach could show superpolynomial lower bounds on $\mathrm{dc}(\mathrm{per}_m)$. This was too optimistic:

> In [I, Panova; FOCS 2016] and later [Bürgisser, I, Panova; FOCS 2016, JAMS] we prove that this approach **cannot** give $\mathrm{dc}(\mathrm{per}_m) > m^{25}$.

Remark: The setting can be homogenized so that there is no known no-go result.

# More general heuristic attempt: "Multiplicities"

Mulmuley and Sohoni also proposed a more general approach based on **multiplicities**.

Analogously to $\mathcal{D}et_n := \overline{E(\det_n)}$ we define the **padded permanent orbit closure** $\mathcal{P}er_m^{(n)} := \overline{E(\mathrm{per}_m^{(n)})}$. Key property:

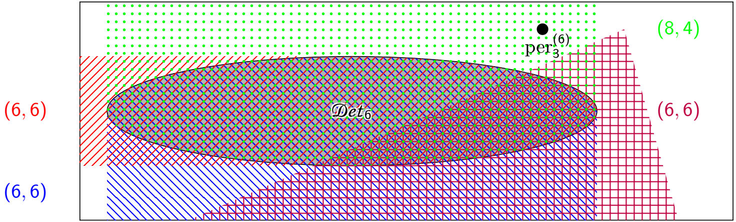
$$\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n \quad \Leftrightarrow \quad \mathcal{P}er_m^{(n)} \not\subseteq \mathcal{D}et_n$$

**Orbit closure containment** problem (NP-hard, [Bläser, I, Jindal, Lysikov STOC 2018]).

We compare **two** varieties. If $\dim \mathcal{P}er_m^{(n)} > \dim \mathcal{D}et_n$, then $\mathcal{P}er_m^{(n)} \not\subseteq \mathcal{D}et_n$.

Instead of $\dim \mathcal{D}et_n$ we can also take other properties:

Def.: The **multiplicity** $\mathrm{mult}_\lambda(\mathbb{C}[\mathcal{D}et_n])$ is defined as the dimension of the space of highest weight polynomials of weight $\lambda$ restricted to $\mathcal{D}et_n$.




If $\mathrm{mult}_\lambda(\mathbb{C}[\mathcal{P}er_m^{(n)}]) > \mathrm{mult}_\lambda(\mathbb{C}[\mathcal{D}et_n])$, then $\mathrm{per}_m^{(n)} \notin \mathcal{D}et_n$.

# Hope for multiplicities

**Theorem [Dörfler, I, Panova; ICALP 2019]**

There are situations where occurrences do **not** work, but multiplicities do.

(Cluster computation to rule out occurrence obstructions)

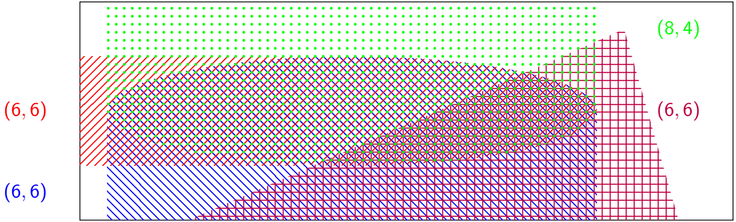
Recent work on dimension data ([Larsen, Pink; 1990], [Yu; 2016]) suggest that the method could be fine enough for separations.

Intuitively, the multiplicities $\mathrm{mult}_\lambda(\mathbb{C}[\mathcal{P}er_m^{(n)}])$ and $\mathrm{mult}_\lambda(\mathbb{C}[\mathcal{D}et_n])$ should be very different, because $\det$ and $\mathrm{per}$ have very different **symmetry groups**.

# Computation of representation theoretic multiplicities

Almost all multiplicities are $\#P$-hard to compute (in particular NP-hard), even in "simpler" cases:

- For the famous Kronecker coefficient even deciding positivity is NP-hard [I, Mulmuley, Walter; 2017].
- This is also true for plethysm coefficients, which is just the dim. of the highest weight polynomial space. [Fischer, I; 2020].



## Theorem [I, Kandasamy; STOC 2020]

Let $m \geq 3$. Let $\Pi_m := \overline{E(x_1 x_2 \cdots x_m)}$. Let $\Gamma_m := \overline{E(x_1^m + x_2^m + \cdots + x_m^m)}$. Let $\lambda := (4m, \underbrace{2m, 2m, 2m, \ldots, 2m}_{m-1 \text{ many}})$.

Then

$$\text{pleth. coeff.}(\lambda) \geq 3 > \text{mult}_\lambda(\mathbb{C}[\Gamma_m]) \geq 2 > 1 \geq \text{mult}_\lambda(\mathbb{C}[\Pi_m]) \overset{m=p\pm 1}{>} 0.$$

Therefore

- $\Gamma_m \not\subseteq \Pi_m$.

and hence $x_1^m + \cdots + x_m^m$ is not a product of homogeneous linear polynomials.

The bounds are derived from the **symmetry groups** of $x_1^m + \cdots + x_m^m$ and $x_1 \cdots x_m$.

This is the first time we get both lower and upper bounds from the symmetry groups.

# Algebraic natural proofs

**Definition [Forbes, Shpilka, Volk; 2017] and independently [Grochow, Kumar, Saks, Saraf; 2017]**

Given a sequence of varieties $(\mathcal{C}_n)_n$ (of polynomials of degree $n$ in poly($n$) variables), then a sequence $\Delta \in \text{VP}$ of nonzero polynomials is called a (VP-)**algebraic natural proof** against $\mathcal{C}$ if $\forall n : \Delta_n(\mathcal{C}_n) = \{0\}$.

This notion is dual to $\mathcal{C}$ being a hitting set for VP.
The sequence $\mathcal{C}_n = \{f \mid \mathrm{dc}(f) \leq n\}$ "captures VDET".

**Theorem [Bläser, I, Jindal, Lysikov; STOC 2018]**

If there are $\text{VP}^0$-algebraic natural proofs over char 0 against the set of matrices with permanent zero, then $\text{P}^{\#\text{P}} \subseteq \exists\text{BPP}$.

But this variety can be described with occurrence obstructions: very succinct encoding for hard functions.

**Theorem [Bläser, I, Jindal, Lysikov; STOC 2018] + [Bläser, I, Lysikov, Pandey, Schreyer SODA 2021]**

If $\text{coNP} \not\subseteq \text{NP}^{\text{BPP}}$, then no VP-algebraic natural proofs exist for minrank 1.

Generalization in [Bläser, I, Lysikov, Pandey, Schreyer SODA 2021] to arbitrary varieties that are efficiently sampleable and where membership testing is NP-hard, for example: slice rank.
Challenging open question: How hard it is to decide membership in $\{f \mid \mathrm{dc}(f) \leq n\}$?

## Summary

- If we allow approximations (=Euclidean closures) in algebraic complexity, then all complexity lower bounds can be proved via highest weight polynomials. Some are VNP-complete.
- Multiplicity obstructions use only the dimension of the vector space of highest weight polynomials. Occurrence obstructions even only use their occurrence.
- Even though computing multiplicities is NP-hard, sometimes enough information about the multiplicities can be extracted from the symmetry groups of the two polynomials. They might be good enough to prove strong lower bounds.
- GCT "breaks the algebraic natural proofs barrier“ in toy settings by encoding hard functions succinctly.
- Slice rank and related notions give new natural testbeds for GCT.

Thank you for your attention!