Testing membership in varieties, algebraic natural proofs, and geometric complexity theory

Markus Bläser

Saarland University

with Christian Ikenmeyer, Gorav Jindal, Vladimir Lysikov, Anurag Pandey, and Frank-Olaf Schreyer

Orbit closure containment problems

The minrank problem

Variety membership and natural proofs

Variety membership problem

Variety membership problem

- "Given" a variety V and
- given a point x in the ambient space
- decide whether $x \in V$!

What is the complexity of this problem?

$\longrightarrow$ depends on the encoding of V

Varieties given by circuits

Theorem

If V is given by a list of arithmetic circuits, then the membership problem is in coRP*.*

Proof:

- Let $C_1, \ldots, C_t$ computing $f_1, \ldots, f_t$ such that $V = V(f_1, \ldots, f_t)$.
- Test whether $f_1(x) = \cdots = f_t(x) = 0$ by evaluating C_τ at x. (Polynomial Identity Testing)

Remark

Can be realized as a many-one reduction to PIT.

PIT reduces to PIT for constant polynomials

Lemma

There is a many-one reduction from general PIT to PIT for constant polynomials.

Proof:

- Let C be a circuit of size s computing $f(X_1, \ldots, X_n)$.
- The degree and the bit size of the coefficients are exponentially bounded in s.
- f is not identically zero iff $f(2^{2^{s^2}}, \ldots, 2^{2^{ns^2}}) \neq 0$.

Remark

The proof yields a many-one reduction from PIT to hypersurface membership testing when the surface is given as a circuit.

Further ways to specify varieties

- Explicitely in the problem:
  Let $V = (V_n)$ and consider V-membership
- As an orbit closure:
  Let $G = (G_n)$ be a sequence of groups acting on an n-dimensional ambient space.
  Given (x, v) decide whether $x \in \overline{G_n v}$!
  (*Orbit containment problem*)
- By a dense subset:
  Given circuits computing a polynomial map, decide whether x lies in the closure of the image.

Tensor rank and matrix multiplication

Definition

$u \otimes v \otimes w \in U \otimes V \otimes W$ is called a rank-one tensor.

Definition (Rank)

$R(t)$ is the smallest r such that there are rank-one tensors $t_1, \ldots, t_r$ with $t = t_1 + \cdots + t_r$.

Lemma

Let $t \in U \otimes V \otimes W$ *and* $t' \in U' \otimes V' \otimes W'$.

- $R(t \oplus t') \leq R(t) + R(t')$
- $R(t \otimes t') \leq R(t)R(t')$

Strassen's algorithm and tensors

Observation: Tensor product $\cong$ Recursion

Strassen's algorithm:

- $\langle 2,2,2\rangle^{\otimes s} = \langle 2^s, 2^s, 2^s\rangle$
- $R(\langle 2,2,2\rangle^{\otimes s}) \leq 7^s$

Definition (Exponent of matrix multiplication)

$$\omega = \inf\{\tau \mid R(\langle n,n,n\rangle) = O(n^\tau)\}$$

Strassen: $\omega \leq \log_2 7 \leq 2.81$

Lemma

If $R(\langle k,m,n\rangle) \leq r$, *then* $\omega \leq 3 \cdot \frac{\log r}{\log kmn}$.

Restrictions

Definition

Let $A : U \to U'$, $B : V \to V'$, $C : W \to W'$ be homomorphism.

- $(A \otimes B \otimes C)(u \otimes v \otimes w) = A(u) \otimes B(v) \otimes C(w)$
- $(A \otimes B \otimes C)t = \sum_{i=1}^{r} A(u_i) \otimes B(v_i) \otimes C(w_i)$ for $t = \sum_{i=1}^{r} u_i \otimes v_i \otimes w_i$.
- $t' \leq t$ if there are A, B, C such that $t' = (A \otimes B \otimes C)t$. ("restriction").

Lemma

- *If* $t' \leq t$, *then* $R(t') \leq R(t)$
- $R(t) \leq r$ *iff* $t \leq \langle r \rangle$.
  ($\langle r \rangle$ "diagonal" of size r.*)*

Orbit problems

Let $(A, B, C) \in \mathrm{End}(U) \times \mathrm{End}(V) \times \mathrm{End}(W)$ act on $U \otimes V \otimes W$ by

$$(A, B, C)u \otimes v \otimes w = A(u) \otimes B(v) \otimes C(w).$$

and linearity.

We can interpret $t \in U' \otimes V' \otimes W'$ as an element of $U \otimes V \otimes W$ by embedding U' into U, V' into V, and W' into W.

Lemma

$R(t) \leq r$ *iff* $t \in (\mathrm{End}(U) \times \mathrm{End}(U) \times \mathrm{End}(U))\langle r \rangle$.

Border rank and orbit problems

- S_r be the set of all tensors of rank r.
- $X_r := \overline{S_r}$ is the set of tensors of *border rank* $\leq r$.

Lemma

If $\underline{R}(\langle k, m, n\rangle) \leq r$, *then* $\omega \leq 3 \cdot \frac{\log r}{\log kmn}$.

Lemma

$\underline{R}(t) \leq r$ *iff* $t \in \overline{(GL_r \times GL_r \times GL_r)\langle r\rangle}$.

Identity testing

Lemma (Valiant)

If a polynomial $f \in k[X_1, \dots, X_n]$ *can be computed by a formula of size* s*, then there is a matrix pencil of size* $m \times m$

$$A := A_0 + X_1 A_1 + \cdots + X_n A_n$$

such that $f = \det(A)$*. We have* $m = O(s)$*.*

Observation

f *is identically zero iff* A *does not have full rank.*

$\mathrm{SL}_m \times \mathrm{SL}_m$ acts on $(A_0, \dots, A_n)$ by

$$(S, T)(A_0, \dots, A_n) := (SA_0T, \dots, SA_nT).$$

Noncommutative identity testing

Definition

Let G act on V. The *null cone* are all vectors v such that $0 \in \overline{Gv}$.

One can define a noncommutative version of the rank of a matrix pencil.

Theorem (Bürgin–Draisma)

A does not have full noncommutative rank iff A is in the null cone of the left-right-SL-action.

Theorem (Garg–Gurvits–Oliviera–Wigderson)

This null-cone problem can be solved deterministically in polynomial time.

Projections as orbit problems

Definition

1. $f \in K[X]$ is a *projection* of $g \in K[X]$ if there is a substitution $r : X \to X \cup K$ such that $f = r(g)$. "$f \leq g$"
2. A p-family (f_n) is a *p-projection* of another p-family (g_n) if there is a p-bounded q such that $f_n \leq g_{q(n)}$. "$(f_n) \leq_p (g_n)$ "

- End_n acts on $k[X_1, \ldots, X_n]$ by $(gh)(x) = h(g^t x)$ for $g \in \mathrm{End}_n$, $h \in k[X_1, \ldots, X_n]$, $x \in k^n$.
- If $f \in \mathrm{End}_n\, h$ and h is homogeneous of degree d, then f is homogeneous of degree d
- If $f \leq h$, then $\deg f$ can be smaller than $\deg h$.
- Padding: Replace f by $X_1^{\deg h - \deg f} f$.
- If $f \leq h$, then $X_1^{\deg h - \deg f} f \in \mathrm{End}_n\, h$
- VP and $\mathrm{VP}_{\mathrm{ws}}$ are closed under End_n.

Valiant's conjecture

Conjecture (Valiant)

$\mathsf{VP} \neq \mathsf{VNP}$

- the weaker conjecture $\mathsf{VP}_{\mathrm{ws}} \neq \mathsf{VNP}$ is equivalent to $\mathrm{per} \not\leq_p \det$.

Conjecture (Mulmuley & Sohoni)

$\mathsf{VNP} \not\subseteq \overline{\mathsf{VP}_{\mathrm{ws}}}$

- equivalent to $X_{11}^{n-m}\,\mathrm{per}_m \notin \overline{\mathrm{GL}_{n^2}\det_n}$ for any $n = \mathrm{poly}(m)$.

Orbit closure containment problem

- We want to understand the complexity of deciding

$$x \in \overline{Gv}?$$

- We will focus on tensors.
- Tensor rank is NP-hard (Hastad).
- Very little is known about closures.
- In partcular, we do not know any hardness results for border rank.

The minrank problem

Definition

Let $A_1, \dots, A_k \in K^{m \times n}$. The *min-rank* of $A_1, \dots, A_k$ is the minimum number r such that there are scalars $\lambda_1, \dots, \lambda_m$, not all being 0, with

$$\mathrm{rk}(\lambda_1 A_1 + \cdots + \lambda_k A_k) \leq r.$$

We denote the min-rank by $\mathrm{minR}(A_1, \dots A_k)$.

- Can also be phrased in terms of a matrix pencil $X_1 A_1 + \cdots + X_k A_k$.
- Can be phrased in terms of tensors by stacking the matrices on top of each other.

Geometric description

Theorem

Let U, V, W be vector spaces over an algebraically closed field $\mathbb{F}$. The set of all tensors $T \in U \otimes V \otimes W$ with minrank at most r is Zariski closed.

Definition

We call the projective variety

$$\mathbb{P}\mathcal{M}_{U\otimes V\otimes W,r} = \{[T] \in \mathbb{P}(U \otimes V \otimes W) \mid \exists x \neq 0\colon \operatorname{rk}(Tx) \leq r\}$$

the *projective minrank variety*, and the corresponding affine cone

$$\mathcal{M}_{U\otimes V\otimes W,r} = \{T \in U \otimes V \otimes W \mid \exists x \neq 0\colon \operatorname{rk}(Tx) \leq r\}$$

the *affine minrank variety*, or just the *minrank variety*.

Simple properties

Lemma

Let V' and W' be subspaces of V and W respectively. Then

$$\mathcal{M}_{U\otimes V'\otimes W',r} = \mathcal{M}_{U\otimes V\otimes W,r} \cap (U \otimes V' \otimes W').$$

Lemma

Let $\dim U = k$, $\dim V = n$ and $\dim W > s = n(k-1) + r$. Then

$$\mathcal{M}_{U\otimes V\otimes W,r} = \bigcup_{\substack{W'\subset W \\ \dim W' = s}} \mathcal{M}_{U\otimes V\otimes W',r}.$$

Lemma

The variety $\mathcal{M}_{U\otimes V\otimes W,r}$ is invariant under the standard action of $\mathrm{GL}(U) \times \mathrm{GL}(V) \times \mathrm{GL}(W)$ on $U \otimes V \otimes W$.

Orbit problem

- Let $L = (F^n)^{\oplus(k-1)} \oplus F^r$, $\dim L = s := n(k-1) + r$.
- Let L_i be the i-th summand with standard basis e_{ij}, $1 \le j \le \dim L_i$.
- Let $U = F^k$ with standard basis e_i.

$$T_{k,n,r} = e_1 \otimes (\sum_{j=1}^{r} e_{1j} \otimes e_{1j}) + \sum_{i=2}^{k} e_i \otimes (\sum_{j=1}^{n} e_{ij} \otimes e_{ij}),$$

- The group $GL(U) \times GL(L) \times GL(L)$ acts on $U \otimes L \otimes L$.

Theorem

Suppose V and W are subspaces of L. Then

$$\mathcal{M}_{U\otimes V\otimes W,r} = \overline{(GL(U) \times GL(L) \times GL(L))T_{k,n,r}} \cap (U \otimes V \otimes W).$$

Symmetries

Theorem

If $r < n$*, then the stabilizer of* $T_{k,n,r}$ *in* $\mathrm{GL}_k \times \mathrm{GL}_s \times \mathrm{GL}_s$ *is isomorphic to* $(\mathrm{GL}_r \times \mathrm{GL}_1) \times (\mathrm{GL}_n \times \mathrm{GL}_1)^{k-1} \rtimes \mathfrak{S}_{k-1}$.

$$(Z_1, z_1, \dots, Z_k, z_k) \in (\mathrm{GL}_r \times \mathrm{GL}_1) \times (\mathrm{GL}_n \times \mathrm{GL}_1)^{k-1}$$

is embedded into $\mathrm{GL}_k \times \mathrm{GL}_s \times \mathrm{GL}_s$ *via*

$$(\mathrm{diag}(z_1, \dots, z_k), \mathrm{diag}(Z_1, \dots, Z_k), \mathrm{diag}((z_1 Z_1)^{-T}, \dots, (z_k Z_k)^{-T}))$$

and $\mathfrak{S}_{k-1}$ *permutes the last* $k-1$ *coordinates of* U *and the last* $k-1$ *summands of* L *simultaneously.*

Theorem

If $\mathrm{stab}\, T = \mathrm{stab}\, T_{k,n,r}$*, then* T *lies in* $\overline{(\mathrm{GL}_k \times \mathrm{GL}_s \times \mathrm{GL}_s) T_{k,n,r}}$.
If $\mathrm{stab}\, T \supset \mathrm{stab}\, T_{k,n,r}$*, then* $T \in \overline{(\mathrm{GL}_k \times \mathrm{GL}_s \times \mathrm{GL}_s) T_{k,n,r}}$

Complexity

Problem ($\mathrm{HMinRank}$)

Given matrices $(A_1, \dots, A_m)$ *and a number* r*,*
decide whether $\mathrm{minR}(A_1, \dots, A_m) \leq r$*.*

$\mathrm{HMinRank1}$*: special case when* $r = 1$*.*

Problem ($\mathrm{HQuad}_{S,F}$)

Given a set of quadratic forms represented by lists of coefficients from $S \subseteq F$*, determine if it has a common nontrivial zero over* F*.*

Theorem

$\mathrm{HQuad}_{\{0,1,-1\},F}$ *is* NP*-hard for any field* F*.*

Complexity (2)

Theorem

Let F be a field and K be an effective subfield of F. Then $\mathrm{HMinRank1}_{\mathrm{K},\mathrm{F}}$ is polynomial-time equivalent to $\mathrm{HQuad}_{\mathrm{K},\mathrm{F}}$.

Corollary

Let F be a field and K be an effective subfield of F. Then $\mathrm{HMinRank1}_{\mathrm{K},\mathrm{F}}$ is NP*-hard.*

Corollary

Given two tensors t and t', deciding whether the orbit closure of t is contained in the orbit closure of t' (under the usual $\mathrm{GL}_n \times \mathrm{GL}_n \times \mathrm{GL}_n$ action) is NP*-hard.*

Orbit closure containment problems

The minrank problem

Variety membership and natural proofs

How to prove lower bounds?

The generic GCT approach to proving lower bounds:

- Given a sequence of points x_n and
- a sequence of varieties V_n
- we want to prove that $x_n \notin V_n$
- by exhibiting a sequence f_n of polynomials such that
- $f_n(x_n) \neq 0$ anf f_n vanishes on V_n.

How to prove lower bounds?

The generic GCT approach to proving lower bounds:

- Given a sequence of points x_n and
- a sequence of varieties V_n
- we want to prove that $x_n \notin V_n$
- by exhibiting a sequence f_n of polynomials such that
- $f_n(x_n) \neq 0$ anf f_n vanishes on V_n.

What is the complexity of f_n?

How to prove lower bounds?

The generic GCT approach to proving lower bounds:

- Given a sequence of points x_n and
- a sequence of varieties V_n
- we want to prove that $x_n \notin V_n$
- by exhibiting a sequence f_n of polynomials such that
- $f_n(x_n) \neq 0$ anf f_n vanishes on V_n.

What is the complexity of f_n?

Superpolynomial, if membership testing is hard!

Properties of varieties

Definition

A p-family of varieties (V_n) is *polynomially definable*, if for each n, there are polynomials $f_1, \ldots, f_m$ such that V_n is the common zero set of these polynomials and $L(f_i)$ is polynomially bounded in n for all $1 \leq i \leq m$.

Definition

A p-family of varieties (V_n) with $V_n \subseteq F^{p(n)}$ is *uniformly generated* if for all n, there are polynomials $g_1, \ldots, g_{p(n)}$ over K such that

1. the image of $(g_1, \ldots, g_{p(n)})$ is dense in V_n,
2. each g_i has polynomial circuit complexity, and
3. there is a polynomial time bounded Turing machine M that given n in unary, outputs for each g_i an arithmetic circuit.

Barriers

Theorem

Let $\mathbb{F}$ be a field and $\mathbb{K}$ be an effective subfield. Let $V = (V_n)$ be a p-family of varieties such that V is polynomially definable over $\mathbb{K}$ and uniformly generated and the V-membership problem is NP*-hard. Then* coNP $\subseteq \exists$BPP*.*

1. Guess a circuit C of size polynomial in n.
2. Generate the circuits $D_1, \ldots, D_{p(n)}$ computing polynomials $g_1, \ldots, g_{p(n)}$ generating a dense subset.
3. Use polynomial identity testing to check whether $C(g_1, \ldots, g_{p(n)})$ is identically zero. If not, reject.
4. Otherwise, use polynomial identity testing to check whether $C(x_1, \ldots, x_{p(n)})$ is identically zero. If yes, reject. Otherwise accept.

Barriers (2)

Lemma

Let $(V_n) \subseteq F^{p(n)}$ *be a p-family of varieties. Let* (G_n) *be a sequence of groups and* (u_n) *be a sequence of vectors such that* V_n *is the* G_n*-orbit closure of* u_n*. If for a generic element* $g \in G_n$*, the coordinate functions* $(\gamma_1, \ldots, \gamma_{p(n)})$ *of* gu_n *can be described by polynomial size circuits* $(C_1, \ldots, C_{p(n)})$ *and the mapping* $1^n \mapsto (C_1, \ldots, C_{p(n)})$ *is polynomial time computable, then* (V_n) *is uniformly generated.*

Corollary

Let S *be an effective subfield of* F*. For infinitely many* n*, there is an* m*, a tensor* $t \in S^{m\times n\times n}$ *and a value* r *such that there is no algebraic* $\mathrm{poly}(n)$*-natural proof for the fact that the minrank of* t *is greater than* r *unless* $\mathsf{coNP} \subseteq \exists\mathsf{BPP}$*.*

Is this the end?

- We construct various equations for the minrank varieties using GCT methods, even “in the regime” where the membership problem is NP-hard.
- They have polynomial size descriptions in other models, for instance, they are given by:
  - succinctly represented exponential size determinants,
  - succinctly represented exponential sums, or
  - succinct representation-theoretic objects.
- Proving that these equations do not vanish on our points of interest becomes the hard problem.