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

Algebraic natural proofs

Natural proofs

Orbit closure containment problems

Variety membership and natural proofs

Natural proofs

Definition (Razborov & Rudich)

A property $\mathcal{P}$ of Boolean functions is *natural* if it has the following properties:

- **Usefulness:** If $f : \{0,1\}^n \to \{0,1\}$ has $\mathrm{poly}(n)$-sized circuits, then $f \in \mathcal{P}$.
- **Constructivity:** Given f by a truthtable of size $N = 2^n$, we can decide $f \in \mathcal{P}$ in time $\mathrm{poly}(N)$.
- **Largeness:** A random function is not in $\mathcal{P}$ with probability at least $1/\mathrm{poly}(N) = 2^{-O(n)}$.

The Razborov–Rudich barrier

- A function $f : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}$ is *pseudorandom* if when sampling the key $k \in \{0,1\}^\ell$ uniformly at random, the resulting distribution $f(\,.\,,k)$ is computationally indistinguishable from a truly random function.
- If oneway functions exists, so do pseudorandom functions.

Theorem (Razborov & Rudich)

A natural property $\mathcal{P}$ distinguishes a pseudorandom function having $\mathrm{poly}(n)$-size circuits from a truly random function in time $2^{O(n)}$.

Conclusion

If you believe in private key cryptography, then no natural proof will show superpolynomial circuit lower bounds.

Algebraic natural proofs

Definition (Forbes, Shpilka & Volk, Grochow, Kumar, Saks & Saraf)

Let $M \subseteq K[X]$ be a set of monomials.
Let $\mathcal{C} \subseteq \langle M \rangle$ and let $\mathcal{D} \subseteq K[T_m : m \in M]$.

A polynomial $D \in \mathcal{D}$ is an *algebraic $\mathcal{D}$-natural proof against $\mathcal{C}$*, if

1. D is a nonzero polynomial and
2. for all $f \in \mathcal{C}$, $D(f) = 0$, that is, D vanishes on the coefficient vectors of all polynomials in $\mathcal{C}$.

Remark:

- D defines a hypersurface.
- How hard is it to check $D(f) = 0$?
- Largeness comes for free.

Succinct hitting sets

Definition

A *hitting set* for $\mathcal{P} \subseteq K[X_1, \ldots, X_\mu]$ is a set $\mathcal{H} \subseteq K^\mu$ such that for all $p \in \mathcal{P}$, there is an $h \in \mathcal{H}$ such that $p(h) \neq 0$.

Definition (Succinct hitting sets)

Let $M \subseteq K[X]$ be a set of monomials.
Let $\mathcal{C} \subseteq \langle M \rangle$ and let $\mathcal{D} \subseteq K[T_m : m \in M]$.

H is a *$\mathcal{C}$-succinct hitting set for $\mathcal{D}$* if

- $H \subseteq \mathcal{C}$ and
- H viewed as a set of vectors of coefficients of length $|M|$ is a hitting set for $\mathcal{D}$.

The succinct hitting set barrier

Theorem

Let $M \subseteq K[X]$ *be a set of monomials.*
Let $\mathcal{C} \subseteq \langle M \rangle$ *and let* $\mathcal{D} \subseteq K[T_m : m \in M]$.
There are algebraic $\mathcal{D}$*-natural proofs against* $\mathcal{C}$ *iff there are no* $\mathcal{C}$*-succinct hitting set for* $\mathcal{D}$.

Corollary

Let $\mathcal{C} \subseteq K[X_1, \dots, X_n]$ *with degree* $\leq d$ *and computable by* $\mathrm{poly}(n, d)$*-size circuits.*
Then there is an algebraic $\mathrm{poly}(N_{n,d})$*-natural proof against* $\mathcal{C}$ *iff there is no* $\mathrm{poly}(n, d)$*-succinct hitting set for* $\mathrm{poly}(N_{n,d})$*-size circuits in* $N_{n,d}$ *variables.*

$$N_{n,d} = \binom{n+d}{d}$$

The succinct hitting set barrier (2)

Typical regime:

- $N_{n,d} = \binom{n+d}{d}$
- $d = \mathrm{poly}(n) \longrightarrow \mathrm{poly}(n) = \mathrm{poly}\log(N_{n,d})$

Conjecture/Wish/Fear

There are $\mathrm{poly}\log(N)$-succinct hitting sets for $\mathrm{poly}(N)$-size circuits.

Remark:

- Forbes, Shpilka, and Volk show that most known proof methods are natural.

Tensor rank

Definition

1. A tensor $t \in K^{k\times m\times n}$ has rank-one if
   $t = u \otimes v \otimes w := (u_h v_i w_j)$ for $u \in K^k$, $v \in K^m$, and $w \in K^n$.
2. The rank $R(t)$ of a tensor $t \in K^{k\times m\times n}$ is the smallest number r of rank-one tensors $s_1, \dots, s_r$ such that $t = s_1 + \cdots + s_r$.
3. S_r denotes the set of all tensors of rank $\leq r$.

Definition

$D \in K[X_1, \dots, X_{kmn}]$ is a $\mathrm{poly}(k, m, n)$-natural proof against S_r if

- D is nonzero,
- D vanishes on S_r, and
- D is computed by circuits of size $\mathrm{poly}(k, m, n)$.

Tensor rank (2)

Good news:

Theorem (Håstad)

Tensor rank is NP*-hard.*

Theorem (Shitov, Schaefer & Stefankovic)

Tensor rank is as hard as the existential theory over $\mathbb{K}$.

Bad news:

- S_r is not the zero set of a set of polynomials.
- When D vanishes on S_r, it also vanishes on its closure $\overline{S_r}$.
- $X_r := \overline{S_r}$ is the set of tensors of *border rank* $\leq r$.
- X_r contains tensors of rank $> r$.

Algebraic natural proofs

Natural proofs

Orbit closure containment problems

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

- Explicitly 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.

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

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

Identity testing

Lemma (Valiant)

If a polynomial $f \in k[X_1, \ldots, X_n]$ *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.*

$SL_m \times SL_m$ acts on $(A_0, \ldots, A_n)$ by

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

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

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 $k[X_1, \dots, X_n]$ by $(gh)(x) = h(g^t x)$ for $g \in \mathrm{End}_n$, $h \in k[X_1, \dots, X_n]$, $x \in k^n$.
- 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 $n = \mathrm{poly}(m)$.

$\longrightarrow$ **geometric complexity theory (GCT)**

Orbit closure containment problem

- We want to understand the complexity of deciding

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

- Here we will focus on tensors.
- Tensor rank is NP-hard. (Border rank is unknown.)
- Border minrank is NP-hard.
- We are just beginning to understand closures.
- In particular, we do not know any hardness results for border rank.

Algebraic natural proofs

Natural proofs

Orbit closure containment problems

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
- $f_n(x_n) \neq 0$ and 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
- $f_n(x_n) \neq 0$ and 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
- $f_n(x_n) \neq 0$ and 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 $f_1, \dots, f_m$ 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 $g_1, \dots, g_{p(n)}$ over K such that

1. the image of $(g_1, \dots, g_{p(n)})$ 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.

Ingredients

- **polynomially definability:**
  assumption
  lower bound
- **uniformly generated:**
  hitting set generator
  typically easy to achieve for tensors
  e.g. for tensor rank r: sum of r generic rank-1-tensors
- **hardness of membership problem:**
  needs individual proof
  minimum circuit size problem

Minrank

- There is a variant of rank called minrank.
- Border minrank can be defined as an orbit closure.
- Deciding border minrank is NP-hard.

Corollary

Let S be an effective subfield of $\mathbb{F}$. 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 border minrank of t is greater than r unless coNP $\subseteq$ $\exists$BPP*.*

Is this the end?

- We can 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.