Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity

ZEYU GUO[1] NITIN SAXENA[1] AMIT SINHABABU[1]

[1]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Outline

1. Approximate polynomials satisfiability

Outline

1. Approximate polynomials satisfiability
    - Application: verifying hitting-sets for $\overline{\mathsf{VP}}$

Outline

1. Approximate polynomials satisfiability
    - Application: verifying hitting-sets for $\overline{\mathsf{VP}}$
2. Algebraic independence testing over finite fields

Outline

1. Approximate polynomials satisfiability
    - Application: verifying hitting-sets for $\overline{\mathsf{VP}}$
2. Algebraic independence testing over finite fields

A common theme appeared in both problems is the study of the Zariski closure $\overline{\mathrm{Im}(\mathbf{f})}$ of the image of a polynomial map $\mathbf{f}$.

Approximate polynomials satisfiability

Introduction

Polynomials satisfiability is a well studied problem in computer science.

Introduction

Polynomials satisfiability is a well studied problem in computer science.

Polynomials satisfiability (PS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common solution over $\overline{\mathbb{F}}$.

Introduction

Polynomials satisfiability is a well studied problem in computer science.

Polynomials satisfiability (PS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common solution over $\overline{\mathbb{F}}$.

Known to be NP-hard and in PSPACE [Brownawell '87, Kollár '88].

Introduction

Polynomials satisfiability is a well studied problem in computer science.

Polynomials satisfiability (PS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common solution over $\overline{\mathbb{F}}$.

Known to be NP-hard and in PSPACE [Brownawell '87, Kollár '88].

Assuming GRH, PS is in PH when $\mathbb{F} = \mathbb{Q}$ [Koiran '96].

Introduction

A polynomial system with no solution may have an approximate solution.

Introduction

A polynomial system with no solution may have an approximate solution.

Example

The system $X = XY - 1 = 0$ has no solution.

Introduction

A polynomial system with no solution may have an approximate solution.

Example

The system $X = XY - 1 = 0$ has no solution. However, it has an approximate solution $\{X = \epsilon, Y = 1/\epsilon\}$ (let $\epsilon \to 0$).

Introduction

A polynomial system with no solution may have an approximate solution.

Example

The system $X = XY - 1 = 0$ has no solution. However, it has an approximate solution $\{X = \epsilon, Y = 1/\epsilon\}$ (let $\epsilon \to 0$).

Approximate polynomials satisfiability (APS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common approximate solution, i.e., $x_1, \ldots, x_n \in \overline{\mathbb{F}}[\epsilon, \epsilon^{-1}]$ such that $f_i(x_1, \ldots, x_n) \in \epsilon\overline{\mathbb{F}}[\epsilon]$ for $i = 1, \ldots, m$.

Introduction

A polynomial system with no solution may have an approximate solution.

Example

The system $X = XY - 1 = 0$ has no solution. However, it has an approximate solution $\{X = \epsilon, Y = 1/\epsilon\}$ (let $\epsilon \to 0$).

Approximate polynomials satisfiability (APS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common approximate solution, i.e., $x_1, \ldots, x_n \in \overline{\mathbb{F}}[\epsilon, \epsilon^{-1}]$ such that $f_i(x_1, \ldots, x_n) \in \epsilon\overline{\mathbb{F}}[\epsilon]$ for $i = 1, \ldots, m$.

Example

Deciding if the tensor rank of a tensor T over $\overline{\mathbb{F}}$ is $\leq k$ is a PS instance.

Introduction

A polynomial system with no solution may have an approximate solution.

Example

The system $X = XY - 1 = 0$ has no solution. However, it has an approximate solution $\{X = \epsilon, Y = 1/\epsilon\}$ (let $\epsilon \to 0$).

Approximate polynomials satisfiability (APS)

Given $f_1, f_2, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$, determine if $f_1 = f_2 = \cdots = f_m = 0$ have a common approximate solution, i.e., $x_1, \ldots, x_n \in \overline{\mathbb{F}}[\epsilon, \epsilon^{-1}]$ such that $f_i(x_1, \ldots, x_n) \in \epsilon\overline{\mathbb{F}}[\epsilon]$ for $i = 1, \ldots, m$.

Example

Deciding if the tensor rank of a tensor T over $\overline{\mathbb{F}}$ is $\leq k$ is a PS instance.
Deciding if the border rank of T over $\overline{\mathbb{F}}$ is $\leq k$ is an APS instance.

Previous results & our result

APS is NP-hard, but previously not known in PSPACE.

Previous results & our result

APS is NP-hard, but previously not known in PSPACE.

APS is in EXPSPACE by a Gröbner basis algorithm [Derksen-Kemper '02, Mulmuley '12].

Previous results & our result

APS is NP-hard, but previously not known in PSPACE.

APS is in EXPSPACE by a Gröbner basis algorithm [Derksen-Kemper '02, Mulmuley '12].

Theorem [GSS18]

APS $\in$ PSPACE.

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Let $V = \overline{\mathrm{Im}(\mathbf{f})}$, i.e., the Zariski closure of $\mathrm{Im}(\mathbf{f})$.

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Let $V = \overline{\mathrm{Im}(\mathbf{f})}$, i.e., the Zariski closure of $\mathrm{Im}(\mathbf{f})$.

Note $f_1 = \cdots = f_m = 0$ have a common solution in $\overline{\mathbb{F}}^n$ iff $\mathbf{0} \in \mathrm{Im}(\mathbf{f})$.

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Let $V = \overline{\mathrm{Im}(\mathbf{f})}$, i.e., the Zariski closure of $\mathrm{Im}(\mathbf{f})$.

Note $f_1 = \cdots = f_m = 0$ have a common solution in $\overline{\mathbb{F}}^n$ iff $\mathbf{0} \in \mathrm{Im}(\mathbf{f})$.

Lemma

$f_1 = \cdots = f_m = 0$ have a common approximate solution iff $\mathbf{0} \in \overline{\mathrm{Im}(\mathbf{f})}$.

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Let $V = \overline{\mathrm{Im}(\mathbf{f})}$, i.e., the Zariski closure of $\mathrm{Im}(\mathbf{f})$.

Note $f_1 = \cdots = f_m = 0$ have a common solution in $\overline{\mathbb{F}}^n$ iff $\mathbf{0} \in \mathrm{Im}(\mathbf{f})$.

Lemma

$f_1 = \cdots = f_m = 0$ have a common approximate solution iff $\mathbf{0} \in \overline{\mathrm{Im}(\mathbf{f})}$.

The proof follows Lehmkuhl & Lickteig's proof for border rank [LL89].

Geometric reformulation of APS

$f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ defines a polynomial map $\mathbf{f} : \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^m$.

Let $V = \overline{\mathrm{Im}(\mathbf{f})}$, i.e., the Zariski closure of $\mathrm{Im}(\mathbf{f})$.

Note $f_1 = \cdots = f_m = 0$ have a common solution in $\overline{\mathbb{F}}^n$ iff $\mathbf{0} \in \mathrm{Im}(\mathbf{f})$.

Lemma

$f_1 = \cdots = f_m = 0$ have a common approximate solution iff $\mathbf{0} \in \overline{\mathrm{Im}(\mathbf{f})}$.

The proof follows Lehmkuhl & Lickteig's proof for border rank [LL89].

So APS is equivalent to the problem of deciding if $\mathbf{0} \in V = \overline{\mathrm{Im}(\mathbf{f})}$.

Proof sketch

First compute $\dim V$ in PSPACE [Perron '27, Csanky '76].

Proof sketch

First compute $\dim V$ in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if $\operatorname{codim} V = 0$ or 1:

Proof sketch

First compute $\dim V$ in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if $\operatorname{codim} V = 0$ or 1:

If $\operatorname{codim} V = 0$, then $V = \overline{\mathbb{F}}^m \ni \mathbf{0}$.

Proof sketch

First compute $\dim V$ in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if $\operatorname{codim} V = 0$ or 1:

If $\operatorname{codim} V = 0$, then $V = \overline{\mathbb{F}}^m \ni \mathbf{0}$.

If $\operatorname{codim} V = 1$, we use the fact $\mathbf{0} \in V \Leftrightarrow \langle X_1, \ldots, X_m \rangle \supseteq I(V)$

Proof sketch

First compute dim V in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if codim $V = 0$ or 1:

If codim $V = 0$, then $V = \overline{\mathbb{F}}^m \ni \mathbf{0}$.

If codim $V = 1$, we use the fact $\mathbf{0} \in V \Leftrightarrow \langle X_1, \ldots, X_m \rangle \supseteq I(V)$
$\Leftrightarrow$ the polynomials in $I(V)$ have zero constant term.

Proof sketch

First compute $\dim V$ in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if $\operatorname{codim} V = 0$ or 1:

If $\operatorname{codim} V = 0$, then $V = \overline{\mathbb{F}}^m \ni \mathbf{0}$.

If $\operatorname{codim} V = 1$, we use the fact $\mathbf{0} \in V \Leftrightarrow \langle X_1, \ldots, X_m \rangle \supseteq I(V)$
$\Leftrightarrow$ the polynomials in $I(V)$ have zero constant term.

As $\operatorname{codim} V = 1$, $I(V)$ is a principal ideal, generated by a polynomial g of degree $\deg(V) \leq \prod_{i=1}^{m} \deg(f_i)$ [Perron '27].

Proof sketch

First compute dim V in PSPACE [Perron '27, Csanky '76].

Testing $\mathbf{0} \in V$ is easy if codim $V = 0$ or 1:

If codim $V = 0$, then $V = \overline{\mathbb{F}}^m \ni \mathbf{0}$.

If codim $V = 1$, we use the fact $\mathbf{0} \in V \Leftrightarrow \langle X_1, \dots, X_m \rangle \supseteq I(V)$
$\Leftrightarrow$ the polynomials in $I(V)$ have zero constant term.

As codim $V = 1$, $I(V)$ is a principal ideal, generated by a polynomial g of degree $\deg(V) \leq \prod_{i=1}^{m} \deg(f_i)$ [Perron '27].

Checking if g has zero constant term reduces to solving an exponential-size linear equation system, which is in PSPACE [Csanky '76].

Proof sketch

When codim $V > 1$, we reduce to the case codim $V = 1$.

Proof sketch

When $\operatorname{codim} V > 1$, we reduce to the case $\operatorname{codim} V = 1$.

Idea: replace $f_1, \ldots, f_m$ by $g_1, \ldots, g_k$, where $k = \dim V + 1$ and each g_i is a random linear combination of f_i's.

Proof sketch

When codim $V > 1$, we reduce to the case codim $V = 1$.

Idea: replace $f_1, \ldots, f_m$ by $g_1, \ldots, g_k$, where $k = \dim V + 1$ and each g_i is a random linear combination of f_i's.

Geometrically, replacing f_i's by g_i's corresponds to replacing $V \subseteq \overline{\mathbb{F}}^m$ by $V' := \overline{\pi(V)} \subseteq \overline{\mathbb{F}}^k$, where $\pi : \overline{\mathbb{F}}^m \to \overline{\mathbb{F}}^k$ is a random linear map.

Proof sketch

When codim $V > 1$, we reduce to the case codim $V = 1$.

Idea: replace $f_1, \ldots, f_m$ by $g_1, \ldots, g_k$, where $k = \dim V + 1$ and each g_i is a random linear combination of f_i's.

Geometrically, replacing f_i's by g_i's corresponds to replacing $V \subseteq \overline{\mathbb{F}}^m$ by $V' := \overline{\pi(V)} \subseteq \overline{\mathbb{F}}^k$, where $\pi : \overline{\mathbb{F}}^m \to \overline{\mathbb{F}}^k$ is a random linear map.

We show that w.h.p. $\dim V' = \dim V$, which implies

$$\text{codim } V' = k - \dim V = 1.$$

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

The weaker statement $\mathbf{0} \notin \pi(V)$ is equivalent to $\pi^{-1}(\mathbf{0}) \cap V = \emptyset$.

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

The weaker statement $\mathbf{0} \notin \pi(V)$ is equivalent to $\pi^{-1}(\mathbf{0}) \cap V = \emptyset$. This holds w.h.p since $\pi^{-1}(\mathbf{0})$ is the intersection of $k = \dim V + 1$ random hyperplanes.

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

The weaker statement $\mathbf{0} \notin \pi(V)$ is equivalent to $\pi^{-1}(\mathbf{0}) \cap V = \emptyset$. This holds w.h.p since $\pi^{-1}(\mathbf{0})$ is the intersection of $k = \dim V + 1$ random hyperplanes.

However, this does not guarantee $\mathbf{0} \notin \overline{\pi(V)}$, because $\pi^{-1}(\mathbf{0})$ and V can get "infinitesimally close" and "meet at infinity".

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

The weaker statement $\mathbf{0} \notin \pi(V)$ is equivalent to $\pi^{-1}(\mathbf{0}) \cap V = \emptyset$. This holds w.h.p since $\pi^{-1}(\mathbf{0})$ is the intersection of $k = \dim V + 1$ random hyperplanes.

However, this does not guarantee $\mathbf{0} \notin \overline{\pi(V)}$, because $\pi^{-1}(\mathbf{0})$ and V can get "infinitesimally close" and "meet at infinity".

Solution: replacing the affine space $\overline{\mathbb{F}}^m$ by the projective space $\mathbb{P}^m$.

Proof sketch

To prove that this is indeed a reduction, we also need to prove that $\mathbf{0} \in V'$ iff $\mathbf{0} \in V$.

The "if" part is trivial. For the "only if" part, we want to prove: assuming $\mathbf{0} \notin V$, then w.h.p $\mathbf{0} \notin \overline{\pi(V)}$.

The weaker statement $\mathbf{0} \notin \pi(V)$ is equivalent to $\pi^{-1}(\mathbf{0}) \cap V = \emptyset$. This holds w.h.p since $\pi^{-1}(\mathbf{0})$ is the intersection of $k = \dim V + 1$ random hyperplanes.

However, this does not guarantee $\mathbf{0} \notin \overline{\pi(V)}$, because $\pi^{-1}(\mathbf{0})$ and V can get "infinitesimally close" and "meet at infinity".

Solution: replacing the affine space $\overline{\mathbb{F}}^m$ by the projective space $\mathbb{P}^m$.

Lemma [GSS18]

Assume $\mathbf{0} \notin V$. Then $\mathbf{0} \notin \overline{\pi(V)}$ if the projective closure of $\pi^{-1}(\mathbf{0})$ and that of V are disjoint, which holds with high probability.

Verifying hitting-sets for $\overline{\mathsf{VP}}$

Hitting-sets for $\overline{\mathsf{VP}}$

Informally, $\overline{\mathsf{VP}}$ is the class of polynomials approximated by arithmetic circuits of polynomial size and polynomial degree.

Hitting-sets for $\overline{\mathsf{VP}}$

Informally, $\overline{\mathsf{VP}}$ is the class of polynomials approximated by arithmetic circuits of polynomial size and polynomial degree.

Mulmuley (FOCS'12, J.AMS'17) considered the problem of constructing small hitting-sets for $\overline{\mathsf{VP}}$.

Hitting-sets for $\overline{\mathsf{VP}}$

Informally, $\overline{\mathsf{VP}}$ is the class of polynomials approximated by arithmetic circuits of polynomial size and polynomial degree.

Mulmuley (FOCS'12, J.AMS'17) considered the problem of constructing small hitting-sets for $\overline{\mathsf{VP}}$.

Heintz & Schnorr [HS80] proved the existence of such small hitting sets.

Hitting-sets for $\overline{\mathsf{VP}}$

Informally, $\overline{\mathsf{VP}}$ is the class of polynomials approximated by arithmetic circuits of polynomial size and polynomial degree.

Mulmuley (FOCS'12, J.AMS'17) considered the problem of constructing small hitting-sets for $\overline{\mathsf{VP}}$.

Heintz & Schnorr [HS80] proved the existence of such small hitting sets.

While it is easy to enumerate the list of candidates for small hitting-sets, it is not obvious how to verify a candidate is a hitting-set in PSPACE.

Hitting-sets for $\overline{\text{VP}}$

Informally, $\overline{\text{VP}}$ is the class of polynomials approximated by arithmetic circuits of polynomial size and polynomial degree.

Mulmuley (FOCS'12, J.AMS'17) considered the problem of constructing small hitting-sets for $\overline{\text{VP}}$.

Heintz & Schnorr [HS80] proved the existence of such small hitting sets.

While it is easy to enumerate the list of candidates for small hitting-sets, it is not obvious how to verify a candidate is a hitting-set in PSPACE.

Mulmuley noted that it is in EXPSPACE.

Hitting-sets for $\overline{\mathsf{VP}}$

Recently, Forbes and Shpilka (STOC '18) showed that small hitting-sets for $\overline{\mathsf{VP}}_{\mathbb{C}}$ can be constructed in PSPACE.

Hitting-sets for $\overline{\mathsf{VP}}$

Recently, Forbes and Shpilka (STOC '18) showed that small hitting-sets for $\overline{\mathsf{VP}}_{\mathbb{C}}$ can be constructed in PSPACE.

Their proof uses classical topology of euclidean spaces and does not extend to positive characteristic.

Hitting-sets for $\overline{\mathsf{VP}}$

Recently, Forbes and Shpilka (STOC '18) showed that small hitting-sets for $\overline{\mathsf{VP}}_{\mathbb{C}}$ can be constructed in PSPACE.

Their proof uses classical topology of euclidean spaces and does not extend to positive characteristic.

Theorem [GSS18]

Verifying hitting-sets for $\overline{\mathsf{VP}}$ is in PSPACE, regardless of the base field $\mathbb{F}$. Therefore, constructing small hitting-sets for $\overline{\mathsf{VP}}$ is in PSPACE.

Previously, verifying hitting-sets in PSPACE was open even for $\mathbb{F} = \mathbb{C}$.

Proof sketch

We need the construction of a universal circuit $\Psi(\mathbf{x}, \mathbf{y})$ over a field $\mathbb{K}$ [Raz08]. It has the property that every small arithmetic circuit over $\mathbb{K}$ is simulated by $\Psi(\mathbf{x}, \beta)$ for some $\beta \in \mathbb{K}$.

Proof sketch

We need the construction of a universal circuit $\Psi(\mathbf{x}, \mathbf{y})$ over a field $\mathbb{K}$ [Raz08]. It has the property that every small arithmetic circuit over $\mathbb{K}$ is simulated by $\Psi(\mathbf{x}, \beta)$ for some $\beta \in \mathbb{K}$.

Let $\mathbb{K} = \overline{\mathbb{F}}(\epsilon)$. Then $\overline{\mathsf{VP}}$ consists of the arithmetic circuits C over $\overline{\mathbb{F}}$ satisfying $C(\mathbf{x}) \equiv \Psi(\mathbf{x}, \beta)|_{\epsilon=0}$ for some $\beta \in \mathbb{K}$.

Proof sketch

We need the construction of a universal circuit $\Psi(\mathbf{x}, \mathbf{y})$ over a field $\mathbb{K}$ [Raz08]. It has the property that every small arithmetic circuit over $\mathbb{K}$ is simulated by $\Psi(\mathbf{x}, \beta)$ for some $\beta \in \mathbb{K}$.

Let $\mathbb{K} = \overline{\mathbb{F}}(\epsilon)$. Then $\overline{\mathsf{VP}}$ consists of the arithmetic circuits C over $\overline{\mathbb{F}}$ satisfying $C(\mathbf{x}) \equiv \Psi(\mathbf{x}, \beta)|_{\epsilon=0}$ for some $\beta \in \mathbb{K}$.

Theorem [GSS18]

$\mathcal{H} = \{u_1, \ldots, u_k\}$ is not a hitting-set iff $\exists\ (\alpha, \beta) \in \mathbb{K}^n \times \mathbb{K}^m$ such that

- $\forall i \in [n]$, $\alpha_i^{r+1} - 1 \in \epsilon\overline{\mathbb{F}}[\epsilon]$
- $\Psi(\alpha, \beta) - 1 \in \epsilon\overline{\mathbb{F}}[\epsilon]$, and
- $\forall i \in [k]$, $\Psi(u_i, \beta) \in \epsilon\overline{\mathbb{F}}[\epsilon]$

Proof sketch

We need the construction of a universal circuit $\Psi(\mathbf{x}, \mathbf{y})$ over a field $\mathbb{K}$ [Raz08]. It has the property that every small arithmetic circuit over $\mathbb{K}$ is simulated by $\Psi(\mathbf{x}, \beta)$ for some $\beta \in \mathbb{K}$.

Let $\mathbb{K} = \overline{\mathbb{F}}(\epsilon)$. Then $\overline{\mathsf{VP}}$ consists of the arithmetic circuits C over $\overline{\mathbb{F}}$ satisfying $C(\mathbf{x}) \equiv \Psi(\mathbf{x}, \beta)|_{\epsilon=0}$ for some $\beta \in \mathbb{K}$.

Theorem [GSS18]

$\mathcal{H} = \{u_1, \ldots, u_k\}$ is not a hitting-set iff $\exists\ (\alpha, \beta) \in \mathbb{K}^n \times \mathbb{K}^m$ such that

- $\forall i \in [n]$, $\alpha_i^{r+1} - 1 \in \epsilon\overline{\mathbb{F}}[\epsilon]$
- $\Psi(\alpha, \beta) - 1 \in \epsilon\overline{\mathbb{F}}[\epsilon]$, and
- $\forall i \in [k]$, $\Psi(u_i, \beta) \in \epsilon\overline{\mathbb{F}}[\epsilon]$

This gives an APS characterization of hitting-sets for $\overline{\mathsf{VP}}$.

Algebraic independence testing over finite fields

Definition (algebraic independence)

Polynomials $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ are algebraically dependent if they satisfy a nontrivial polynomial relation $Q(f_1, \ldots, f_m) = 0$. Otherwise they are algebraically independent.

Introduction

Definition (algebraic independence)

Polynomials $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ are algebraically dependent if they satisfy a nontrivial polynomial relation $Q(f_1, \ldots, f_m) = 0$. Otherwise they are algebraically independent.

Example

$X + Y$ and $(X + Y)^2$ are algebraically dependent, while X and Y are algebraically independent.

Introduction

Algebraic independence is related to the transcendence degree of field extensions and the dimension of algebraic varieties.

Introduction

Algebraic independence is related to the transcendence degree of field extensions and the dimension of algebraic varieties.

It has also found applications in polynomial identity testing, construction of extractors, etc.

Introduction

Algebraic independence is related to the transcendence degree of field extensions and the dimension of algebraic varieties.

It has also found applications in polynomial identity testing, construction of extractors, etc.

Question: Can we test algebraic independence efficiently?

Jacobian criterion

Theorem (Jacobian criterion [Jac41])

Suppose $\mathrm{char}(\mathbb{F}) = 0$. Then $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ are algebraically independent iff the Jacobian matrix

$$J(f_1, \ldots, f_m) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_n} \end{pmatrix}$$

has full row rank over $\mathbb{F}(X_1, \ldots, X_n)$.

Jacobian criterion

Theorem (Jacobian criterion [Jac41])

Suppose $\text{char}(\mathbb{F}) = 0$. Then $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ are algebraically independent iff the Jacobian matrix

$$J(f_1, \ldots, f_m) = \begin{pmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_n} \end{pmatrix}$$

has full row rank over $\mathbb{F}(X_1, \ldots, X_n)$.

Corollary

Algebraic dependence testing is in coRP if $\text{char}(\mathbb{F}) = 0$.

Algebraic independence over finite fields

However, the Jacobian criterion may fail in positive characteristic.

Algebraic independence over finite fields

However, the Jacobian criterion may fail in positive characteristic.

Example: $f_1 = X, f_2 = Y^p$

Algebraic independence over finite fields

However, the Jacobian criterion may fail in positive characteristic.

Example: $f_1 = X, f_2 = Y^p$

$$J(f_1, f_2) = \begin{pmatrix} 1 & 0 \\ 0 & pY^{p-1} \end{pmatrix}$$

Algebraic independence over finite fields

However, the Jacobian criterion may fail in positive characteristic.

Example: $f_1 = X, f_2 = Y^p$

$$J(f_1, f_2) = \begin{pmatrix} 1 & 0 \\ 0 & pY^{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if } \mathrm{char}(\mathbb{F}) = p.$$

Algebraic independence over finite fields

However, the Jacobian criterion may fail in positive characteristic.

Example: $f_1 = X, f_2 = Y^p$

$$J(f_1, f_2) = \begin{pmatrix} 1 & 0 \\ 0 & pY^{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if } \mathrm{char}(\mathbb{F}) = p.$$

Previously, it was known that algebraic independence testing over finite fields is in $\mathsf{NP}^{\#\mathsf{P}}$ (Mittmann, Saxena, Scheiblechner, Trans. AMS'14).

Our result

Theorem [GSS18]

Algebraic independence testing over finite fields is in $\mathsf{AM} \cap \mathsf{coAM}$.

Our result

Theorem [GSS18]

Algebraic independence testing over finite fields is in $\mathsf{AM} \cap \mathsf{coAM}$.

Corollary

Algebraic independence testing over finite fields is not NP-hard (or coNP-hard) unless PH collapses to its second level.

Geometric reformulation

$f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ define polynomial map $\mathbf{f} : \overline{\mathbb{F}}_q^n \to \overline{\mathbb{F}}_q^m$.

Geometric reformulation

$f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ define polynomial map $\mathbf{f} : \overline{\mathbb{F}}_q^n \to \overline{\mathbb{F}}_q^m$.

Let $V := \overline{\mathrm{Im}(\mathbf{f})}$.

Geometric reformulation

$f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ define polynomial map $\mathbf{f} : \overline{\mathbb{F}}_q^n \to \overline{\mathbb{F}}_q^m$.

Let $V := \overline{\mathrm{Im}(\mathbf{f})}$.

Fact

$\dim V \leq m$, and equality holds iff $f_1, \ldots, f_m$ are algebraically independent.

Geometric reformulation

$f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ define polynomial map $\mathbf{f} : \overline{\mathbb{F}}_q^n \to \overline{\mathbb{F}}_q^m$.

Let $V := \overline{\mathrm{Im}(\mathbf{f})}$.

Fact

$\dim V \leq m$, and equality holds iff $f_1, \ldots, f_m$ are algebraically independent.

We want to distinguish the two cases $\dim V = m$ and $\dim V < m$.

Geometric reformulation

$f_1, \ldots, f_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ define polynomial map $\mathbf{f} : \overline{\mathbb{F}}_q^n \to \overline{\mathbb{F}}_q^m$.

Let $V := \overline{\mathrm{Im}(\mathbf{f})}$.

Fact

$\dim V \leq m$, and equality holds iff $f_1, \ldots, f_m$ are algebraically independent.

We want to distinguish the two cases $\dim V = m$ and $\dim V < m$.

We can reduce to the case that $n = m$ and q is large enough (Pandey, Saxena, Sinhababu, MFCS'16).

Proof sketch

How do we separate the two cases $\dim V = m$ and $\dim V < m$?

Proof sketch

How do we separate the two cases $\dim V = m$ and $\dim V < m$?

Idea: estimate the cardinality of $S := \operatorname{Im}(\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m) \subseteq V$.

Proof sketch

How do we separate the two cases $\dim V = m$ and $\dim V < m$?

Idea: estimate the cardinality of $S := \mathrm{Im}(\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m) \subseteq V$.

Lemma [GSS18]

We have $\begin{cases} |S| \leq \left(\prod_{i=1}^m \deg(f_i)\right) \cdot q^{m-1} & \text{if } \dim V < m, \\ |S| \geq \frac{(1-o(1))}{\prod_{i=1}^m \deg(f_i)} \cdot q^m & \text{if } \dim V = m. \end{cases}$

Proof sketch

How do we separate the two cases $\dim V = m$ and $\dim V < m$?

Idea: estimate the cardinality of $S := \mathrm{Im}(\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m) \subseteq V$.

Lemma [GSS18]

We have $$\begin{cases} |S| \leq \left(\prod_{i=1}^m \deg(f_i)\right) \cdot q^{m-1} & \text{if } \dim V < m, \\ |S| \geq \frac{(1-o(1))}{\prod_{i=1}^m \deg(f_i)} \cdot q^m & \text{if } \dim V = m. \end{cases}$$

Lemma (Goldwasser-Sipser [GS86])

Let S be a set whose membership is testable in NP, and either $|S| \leq k$ or $|S| \geq 2k$ for some given $k > 0$. Then deciding if $|S| \geq 2k$ is in AM.

Proof sketch

How do we separate the two cases $\dim V = m$ and $\dim V < m$?

Idea: estimate the cardinality of $S := \mathrm{Im}(\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m) \subseteq V$.

Lemma [GSS18]

We have
$$\begin{cases} |S| \le \left(\prod_{i=1}^m \deg(f_i)\right) \cdot q^{m-1} & \text{if } \dim V < m, \\ |S| \ge \frac{(1-o(1))}{\prod_{i=1}^m \deg(f_i)} \cdot q^m & \text{if } \dim V = m. \end{cases}$$

Lemma (Goldwasser-Sipser [GS86])

Let S be a set whose membership is testable in NP, and either $|S| \le k$ or $|S| \ge 2k$ for some given $k > 0$. Then deciding if $|S| \ge 2k$ is in AM.

$\Rightarrow$ algebraic independence testing is in AM.

Proof sketch

To prove the coAM result, we pick random $y \in S$, and estimate the cardinality N_y of the preimage of y under $\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Proof sketch

To prove the coAM result, we pick random $y \in S$, and estimate the cardinality N_y of the preimage of y under $\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Lemma [GSS18]

If $\dim V = m$, then w.h.p, $N_y \leq \prod_{i=1}^m \deg(f_i)$.
If $\dim V < m$, then for $k > 0$, $\Pr[N_y \geq k] \geq 1 - k \prod_{i=1}^m \deg(f_i)/q$.

Proof sketch

To prove the coAM result, we pick random $y \in S$, and estimate the cardinality N_y of the preimage of y under $\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Lemma [GSS18]

If $\dim V = m$, then w.h.p, $N_y \leq \prod_{i=1}^m \deg(f_i)$.
If $\dim V < m$, then for $k > 0$, $\Pr[N_y \geq k] \geq 1 - k \prod_{i=1}^m \deg(f_i)/q$.

Choose $2 \prod_{i=1}^m \deg(f_i) \leq k \ll q / \prod_{i=1}^m \deg(f_i)$, and apply the Goldwasser-Sipser Lemma to the preimage of y

Proof sketch

To prove the coAM result, we pick random $y \in S$, and estimate the cardinality N_y of the preimage of y under $\mathbf{f}|_{\mathbb{F}_q^n} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Lemma [GSS18]

If $\dim V = m$, then w.h.p, $N_y \leq \prod_{i=1}^{m} \deg(f_i)$.
If $\dim V < m$, then for $k > 0$, $\Pr[N_y \geq k] \geq 1 - k \prod_{i=1}^{m} \deg(f_i)/q$.

Choose $2 \prod_{i=1}^{m} \deg(f_i) \leq k \ll q / \prod_{i=1}^{m} \deg(f_i)$, and apply the Goldwasser-Sipser Lemma to the preimage of y

$\Rightarrow$ algebraic independence testing is in coAM.

Conclusion

Summary and open problems

We have shown

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.
- Verifying hitting-sets for $\overline{\mathrm{VP}}$ is in PSPACE.

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.
- Verifying hitting-sets for $\overline{\mathsf{VP}}$ is in PSPACE.
- Algebraic independence testing over finite fields is in $\mathsf{AM} \cap \mathsf{coAM}$.

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.
- Verifying hitting-sets for $\overline{\mathsf{VP}}$ is in PSPACE.
- Algebraic independence testing over finite fields is in $\mathsf{AM} \cap \mathsf{coAM}$.

Open problems:

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.
- Verifying hitting-sets for $\overline{\mathsf{VP}}$ is in PSPACE.
- Algebraic independence testing over finite fields is in AM $\cap$ coAM.

Open problems:

- When $f_1, \ldots, f_n$ are defined over $\mathbb{Q}$, it is known that PS $\in$ AM under GRH [Koiran '96]. Can we put APS in AM, or in any complexity class lower than PSPACE?

Summary and open problems

We have shown

- APS is NP-hard and is in PSPACE.
- Verifying hitting-sets for $\overline{\mathrm{VP}}$ is in PSPACE.
- Algebraic independence testing over finite fields is in $\mathrm{AM} \cap \mathrm{coAM}$.

Open problems:

- When $f_1, \ldots, f_n$ are defined over $\mathbb{Q}$, it is known that $\mathrm{PS} \in \mathrm{AM}$ under GRH [Koiran '96]. Can we put APS in AM, or in any complexity class lower than PSPACE?
- Subexponential-time algorithm for algebraic independence testing over finite fields?

Questions?