TESTING SPARSE POLYNOMIAL IDENTITIES OVER SMALL FIELDS

Simon Grünbacher, Erhard Aichinger and Paul Hametner
Institute for Algebra
Austrian Science Fund FWF P33878

JOHANNES KEPLER
UNIVERSITY LINZ

FWF
Der Wissenschaftsfonds.

THE QUESTION

The Question

Let $\mathbb{K}$ be a field and let $S \subseteq \mathbb{K}$ be a finite set.
We are interested in the following question:
Given: Black-box access to a sparse polynomial $p \in \mathbb{K}[X_1, \ldots, X_n]$.
Asked: Does $p(x) = 0$ hold for all $x \in S^n$?
Example: Does $p = 1 + X^2 + 2XY + XYZ$ vanish on $\{-1, 1\}^3$?
Goal: Decide by testing only some points $x \in S^n$.

Why sparsity might help

Example

- Let $S = \{-1, 1\}$.
- Let $a \in S^n$ and let $p := \prod_{i=1}^{n}(X_i - a_i)$.
- We have $\{x \in S^n \mid p(x) \neq 0\} = \{(-a_1, \ldots, -a_n)\}$.
- Given only black-box access, we would have to test all 2^n points to decide $\forall x \in S^n : p(x) = 0$.
- However, p has $M(p) = 2^n$ monomials and is therefore not sparse.
- Perhaps testing sparse identities is easier.

What happened before

Theorem [Clausen, Dress, Grabmeier, Karpinski '91]

Let $n \in \mathbb{N}, \mathbb{K} = S = GF(q)$ and let $m \geq 2$. There exists a testing set $T \subseteq S^n$ with $|T| \leq (n(q-1))^{\log_2(m)}$ with the following property:
For all $p \in \mathbb{K}[X_1, \ldots, X_n]$ with $M(p) \leq m$ monomials and $\deg_{X_i} p < q$ we have

$$(\forall x \in S^n : p(x) = 0) \iff (\forall x \in T : p(x) = 0).$$

$\Longrightarrow$ Test at most $(n(q-1))^{\log_2(M(p))}$ points.

What happened before

Theorem [Kiltz, Winterhof '04]

Let $n \in \mathbb{N}$, let $\mathbb{K} = GF(q)$, let $\gamma \in \mathbb{K}$ be an element of order d and let $S = \{\gamma^i \mid 1 \leq i \leq d\}$. Let $p \in \mathbb{K}[X_1, \ldots, X_n]$ with $p \neq 0$ and $\deg_{X_i} p < d$ and let $W := \{x \in S^n \mid p(x) \neq 0\}$. Then $|W| \geq \frac{d^n}{M(p)}$.

$\Longrightarrow$ Test $10 \cdot M(p)$ random points and find a non-zero with high probability.

What we did

Theorem [EA, SG, PH]

Let $\mathbb{K} := GF(q)$ be the field with $q > 2$ elements, let $t := \frac{q-1}{q-2}$, let $m \in \mathbb{N}$ and let $S \subseteq \mathbb{K} \setminus \{0\}$. There is a testing set $T \subseteq S^n$ of size at most $(n \cdot |S|)^{\log_t(m)}$ with the following property:
For all $p \in \mathbb{K}[X_1, \ldots, X_n]$ with $M(p) \leq m$, we have

$$(\forall x \in S^n : p(x) = 0) \iff (\forall x \in T : p(x) = 0).$$

$\Longrightarrow$ Similar bounds for more general S.

THE PROOF

Absorbing Polynomials

Definition

Let K be an integral domain, let $S \subseteq K$ be a set, let $n \in \mathbb{N}$ and let $s \in S^n$. A polynomial $p \in K[X_1, \ldots, X_n]$ is called absorbing at s for S^n if for all $x \in S^n$ with $\exists i \in \underline{n} : x_i = s_i$, we have $p(x) = 0$.

Absorbing Polynomials

Definition

Let K be an integral domain, let $S \subseteq K$ be a set, let $n \in \mathbb{N}$ and let $s \in S^n$. A polynomial $p \in K[X_1, \ldots, X_n]$ is called absorbing at s for S^n if for all $x \in S^n$ with $\exists i \in \underline{n} : x_i = s_i$, we have $p(x) = 0$.

Example

Let $S = \{-1, 0, 1\} \subseteq \mathbb{R}$ and $p := (X_1 - 1)(X_2 + 1)$. Then p is absorbing at $(1, -1)$.

X_2			
1	-4	-2	0
0	-2	-1	0
-1	0	0	0
	-1	0	1 X_1

Goal: Find lower bound on the number of monomials of absorbing polynomials.

Absorbing Polynomials

Question: Does every absorbing polynomial p that is nonzero on S^n satisfy $M(p) \geq 2^n$?

Absorbing Polynomials

Question: Does every absorbing polynomial p that is nonzero on S^n satisfy $M(p) \geq 2^n$?

Example

The polynomial $p_1 := X_1 \dots X_n$ is absorbing at $s = (0, \dots, 0)$ and $M(p_1) = 1$.

Absorbing Polynomials

Question: Does every absorbing polynomial p that is nonzero on S^n satisfy $M(p) \geq 2^n$?

Example

The polynomial $p_1 := X_1 \dots X_n$ is absorbing at $s = (0, \dots, 0)$ and $M(p_1) = 1$.

Example

- Let $r \geq 2$ and let $S = \{1, \alpha\} \subseteq \mathbb{C}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- Let $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{C}[X_1, \dots, X_{r-1}]$.
- The polynomial p_2 is nonzero at $(1, \dots, 1)$ and absorbing at $s = (\alpha, \dots, \alpha)$.
- Note that $M(p_2) = r$.
- Multiplying such polynomials yields nonzero absorbing polynomials q_n on $S^{n(r-1)}$ of size $M(q_n) = r^n = 2^{\log_2(r)n}$.

Absorbing Polynomials

Lemma

Assume the following:

- K integral domain, $S \subseteq K \setminus \{0\}$
- $p = \sum_{e \in E} c(e) X^e \in K[X_1, \ldots, X_n]$ with $c(e) \neq 0$ for all $e \in E$
- p absorbing at $s \in S^n$ and there exists a $t \in S^n$ such that $p(t) \neq 0$
- $r \in \mathbb{N}$ such that X^r is constant on S

Then for all $d \in \{0, \ldots, r-1\}^n$ there exists an $e \in E$ such that for all $1 \leq i \leq n$, we have $d_i \not\equiv_r e_i$.

Absorbing Polynomials

Proof.

- Seeking a contradiction, let $d \in \{0, \ldots, r-1\}^n$ be a counterexample.
- Let $g := X_1^{r-d_1} \ldots X_n^{r-d_n} p$. The polynomial g is also absorbing at s and $g(t) \neq 0$.
- On S^n, every monomial of g is constant in at least one argument by our choice of d.
- Therefore $0 \neq g(t) = \sum_{u \in \{0,1\}^n} (-1)^{u_1 + \cdots + u_n} g(s_1^{u_1} t_1^{1-u_1}, \ldots, s_n^{u_n} t_n^{1-u_n}) = 0$, a contradiction.

□

Remote points

Definition

Let $n, r \in \mathbb{N}$. We say that $E \subseteq \underline{r}^n$ has remote points if for all $d \in \underline{r}^n$, we have $e \in E$ such that $e_i \neq d_i$ for all $i \in \underline{n}$.

Lemma

Let $n \in \mathbb{N}, r \geq 2$. Then every $E \subseteq \underline{r}^n$ that has remote points satisfies $|E| \geq (\frac{r}{r-1})^n$.

Proof.

- For $e \in E$ let $D(e) := \{d \in \underline{r}^n \mid \forall i \in \underline{n} : d_i \neq e_i\}$.
- We have $|D(e)| = (r-1)^n$ for all $e \in E$.
- We have $\underline{r}^n = \bigcup_{e \in E} D(e)$.
- Therefore $r^n = |\bigcup_{e \in E} D(e)| \leq \sum_{e \in E} |D(e)| = |E| \cdot (r-1)^n$.

□

Monomials of absorbing polynomials

Lemma

Let K be an integral domain, let $S \subseteq K \setminus \{0\}$ and let $r \in \mathbb{N}$ such that X^r is constant on S. Let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ with $p(t) \neq 0$. Then $M(p) \geq (\frac{r}{r-1})^n$.

Monomials of absorbing polynomials

Lemma

Let K be an integral domain, let $S \subseteq K \setminus \{0\}$ and let $r \in \mathbb{N}$ such that X^r is constant on S. Let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ with $p(t) \neq 0$. Then $M(p) \geq (\frac{r}{r-1})^n$.

Proof.

- If $p = \sum_{e \in E} c(e) X^e$, where $E \subseteq \mathbb{N}^n$ is the set of exponents, then

$$E' := \{(e_1 \mod r, \ldots, e_n \mod r) \mid e \in E\} \subseteq \{0, \ldots r-1\}^n$$

  must have remote points.
- Therefore $|E| \geq |E'| \geq (\frac{r}{r-1})^n$.

□

Barrington's trick

Lemma

Let K be an integral domain, let $S \subseteq K \setminus \{0\}$ and let $r \in \mathbb{N}$ such that $\forall x \in S : x^r = 1$. Let $t = \frac{r}{r-1}$. Let $p \in K[X_1, \ldots, X_n]$ be a polynomial that does not vanish on S^n. Then for all $a \in S^n$ there exists a $b \in S^n$ with $p(b) \neq 0$ and $d(a, b) := |\{i \mid a_i \neq b_i\}| \leq \log_t(M(p))$.

Barrington's trick

Lemma

Let K be an integral domain, let $S \subseteq K \setminus \{0\}$ and let $r \in \mathbb{N}$ such that $\forall x \in S : x^r = 1$. Let $t = \frac{r}{r-1}$. Let $p \in K[X_1, \ldots, X_n]$ be a polynomial that does not vanish on S^n. Then for all $a \in S^n$ there exists a $b \in S^n$ with $p(b) \neq 0$ and $d(a, b) := |\{i \mid a_i \neq b_i\}| \leq \log_t(M(p))$.

Proof.

- Choose $b \in S^n$ with $p(b) \neq 0$ such that $\{i \mid a_i \neq b_i\} = \{i_1, \ldots, i_k\}$ has minimal size.
- Let h be the polynomial obtained from setting $x_i = b_i$ for all $i \in \underline{n}$ with $a_i = b_i$.
- Now h depends on the k remaining variables and is absorbing on $\{a_{i_1}, b_{i_1}\} \times \cdots \times \{a_{i_k}, b_{i_k}\}$ by minimality.
- Hence $M(p) \geq M(h) \geq t^k$ and therefore $\log_t(M(p)) \geq k$.

□

Barrington's trick

Theorem

Let $\mathbb{K} = GF(q)$ be a finite field, let $S \subseteq K \setminus \{0\}$ and let $t = \frac{q-1}{q-2}$. Let $a \in S^n$. For $m \geq 2$ let $T_m := \{x \in S^n \mid \log_t(m) \geq d(a,x)\}$. Let $p \in K[X_1, \ldots, X_n]$ with $M(p) \leq m$. Then $|T_m| \leq (n|S|)^{\log_t(m)}$ and

$$\forall x \in S^n : p(x) = 0 \iff \forall x \in T_m : p(x) = 0.$$

Proof.

- The property $\forall x \in S^n : p(x) = 0 \iff \forall x \in T_m : p(x) = 0$ follows from the last lemma because $x^{q-1} = 1$ on S.
- Size bound: We make $\log_t(m)$ choices for $i \in \underline{n}$ and $x_i \in S$.

□

How did we get here?

Our results about absorbing polynomials can be used to prove the following:

Lemma

Let t be a term in n variables over the alternating group $(A_4, \cdot, (\cdot)^{-1})$. Assume that the term function t^{A_4} satisfies $1 \in \{x_1, \ldots, x_n\} \Rightarrow t^{A_4}(x_1, \ldots, x_n) = 1$ and that t^{A_4} is not always 1. Then t has length at least 2^{n-2}.

How did we get here?

Our results about absorbing polynomials can be used to prove the following:

Lemma

Let t be a term in n variables over the alternating group $(A_4, \cdot, (\cdot)^{-1})$. Assume that the term function t^{A_4} satisfies $1 \in \{x_1, \ldots, x_n\} \Rightarrow t^{A_4}(x_1, \ldots, x_n) = 1$ and that t^{A_4} is not always 1. Then t has length at least 2^{n-2}.

Example

The term $t(x_1, x_2) = [x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2$ satisfies these properties.

How did we get here?

Our results about absorbing polynomials can be used to prove the following:

Lemma

Let t be a term in n variables over the alternating group $(A_4, \cdot, (\cdot)^{-1})$. Assume that the term function t^{A_4} satisfies $1 \in \{x_1, \ldots, x_n\} \Rightarrow t^{A_4}(x_1, \ldots, x_n) = 1$ and that t^{A_4} is not always 1. Then t has length at least 2^{n-2}.

Example

The term $t(x_1, x_2) = [x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2$ satisfies these properties.

Note: It is known that identity testing over $(A_4, \cdot, (\cdot)^{-1})$ (but not over $(A_4, \cdot, (\cdot)^{-1}, [\cdot, \cdot])$) can be done in polynomial time. This does not yield a better algorithm, but it might guide the way towards identity testing over $(S_4, \cdot, (\cdot)^{-1})$.