# Identity testing for sparse polynomials on rectangular domains

joint work with Erhard Aichinger and Paul Hametner

Simon Grünbacher

June 15, 2023

# 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:

# 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 $p \in \mathbb{K}[X_1, \ldots, X_n]$.

# 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 $x \in S^n$?

# 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 $\{-1, 1\}^3$?

# 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 $S = \{-1, 1\}$

# Why sparsity might help

## Example

- Let $S = \{-1, 1\}$
- Let $a \in S^n$ and let $p := \prod_{i=1}^{n}(X_i - a_i)$.

# 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 $\{x \in S^n \mid p(x) \neq 0\} = \{(-a_1, \ldots, -a_n)\}$.

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

# 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.

# 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 all difficult cases are non-sparse.

# What Happened Before

# 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* $|T| \leq (n(q-1))^{\log_2(m)}$ *such that 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*

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

# 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* $|T| \leq (n(q-1))^{\log_2(m)}$ *such that 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 (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 $|T| \leq (n(q-1))^{\log_2(m)}$ such that 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*

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

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

**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 $|W| \geq \frac{d^n}{M(p)}$.*

# 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 $|T| \leq (n(q-1))^{\log_2(m)}$ such that 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.

**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 random points and find a non-zero with probability $1 - (1 - \frac{1}{M(p)})^{M(p)} \approx 1 - \frac{1}{e}$ after $M(p)$ evaluations.

# Our contribution

# Our contribution

## Theorem (EA, SG, PH)

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

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

# Our contribution

## Theorem (EA, SG, PH)

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

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

## Theorem (EA, SG, PH)

*Let $n \in \mathbb{N}$, let $K$ be an integral domain, let $a_1, b_1, \ldots, a_n, b_n \in K \setminus \{0\}$ with $a_i \neq b_i$ for all $i \in \underline{n}$. We assume that there is $r \in \mathbb{N}$ such that for each $i \in \underline{n}$, we have $a_i^r = b_i^r$. Let $t := \frac{r}{r-1}$, let $Q := \{a_1, b_1\} \times \cdots \times \{a_n, b_n\}$, let $p \in K[X_1, \ldots, X_n]$, and let $W := \{c \in Q \mid p(c) \neq 0\}$. If $W \neq \emptyset$, then $|W| \geq 2^{n - \log_t(M(p))}$.*

# 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 $p \in K[X_1, \dots, X_n]$ 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 $(1, -1)$

| | | |
|---|---|---|
| -4 | -2 | 0 |
| -2 | -1 | 0 |
| 0 | 0 | 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 $p \in K[X_1, \dots, X_n]$ 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 $(1, -1)$

| | | |
|---|---|---|
| -4 | -2 | 0 |
| -2 | -1 | 0 |
| 0 | 0 | 0 |

**Goal:** Find lower bound on the number of monomials of absorbing polynomials, based on $S$, $K$ and $n$.

# Absorbing Polynomials

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

# Absorbing Polynomials

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

## Example

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

# Absorbing Polynomials

**Question:** Does every polynomial $p$ that is nonzero on $S^n$ and absorbing for $S^n$ 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 $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.

# Absorbing Polynomials

**Question:** Does every polynomial $p$ that is nonzero on $S^n$ and absorbing for $S^n$ 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 $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- The polynomial $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{R}[X_1, \dots, X_{r-1}]$ is nonzero at $(1, \dots, 1)$ and absorbing at $s = (\alpha, \dots, \alpha)$ :

# Absorbing Polynomials

**Question:** Does every polynomial $p$ that is nonzero on $S^n$ and absorbing for $S^n$ 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 $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- The polynomial $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{R}[X_1, \dots, X_{r-1}]$ is nonzero at $(1, \dots, 1)$ and absorbing at $s = (\alpha, \dots, \alpha)$ :
- If $x \in S^n$ satisfies $\exists i : x_i = \alpha$, then we have $1 \leq u \leq r-1$ with $x_1 \dots x_{r-1} = \alpha^u$.

# Absorbing Polynomials

**Question:** Does every polynomial $p$ that is nonzero on $S^n$ and absorbing for $S^n$ 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 $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- The polynomial $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{R}[X_1, \dots, X_{r-1}]$ is nonzero at $(1, \dots, 1)$ and absorbing at $s = (\alpha, \dots, \alpha)$ :
- If $x \in S^n$ satisfies $\exists i : x_i = \alpha$, then we have $1 \leq u \leq r-1$ with $x_1 \dots x_{r-1} = \alpha^u$.
- Therefore $p_2(x) = \sum_{k=0}^{r-1} \alpha^{uk} = 0$

# Absorbing Polynomials

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

## Example

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

## Example

- Let $r \geq 2$ and let $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- The polynomial $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{R}[X_1, \ldots, X_{r-1}]$ is nonzero at $(1, \ldots, 1)$ and absorbing at $s = (\alpha, \ldots, \alpha)$ :
- If $x \in S^n$ satisfies $\exists i : x_i = \alpha$, then we have $1 \leq u \leq r-1$ with $x_1 \ldots x_{r-1} = \alpha^u$.
- Therefore $p_2(x) = \sum_{k=0}^{r-1} \alpha^{uk} = 0$
- Note that $M(p_2) = r$

# Absorbing Polynomials

**Question:** Does every polynomial $p$ that is nonzero on $S^n$ and absorbing for $S^n$ 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 $S = \{1, \alpha\} \subseteq \mathbb{R}$ with $\alpha = \exp(\frac{2i\pi}{r})$.
- The polynomial $p_2 := \sum_{k=0}^{r-1} (\prod_{j=1}^{r-1} X_j)^k \in \mathbb{R}[X_1, \dots, X_{r-1}]$ is nonzero at $(1, \dots, 1)$ and absorbing at $s = (\alpha, \dots, \alpha)$ :
- If $x \in S^n$ satisfies $\exists i : x_i = \alpha$, then we have $1 \leq u \leq r-1$ with $x_1 \dots x_{r-1} = \alpha^u$.
- Therefore $p_2(x) = \sum_{k=0}^{r-1} \alpha^{uk} = 0$
- 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

*Let $K$ be an integral domain and let $S \subseteq K \setminus \{0\}$, let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ such that $p(t) \neq 0$. Let $r \in \mathbb{N}$ such that $X^r$ is constant on $S$. Assume $p = \sum_{e \in E} c(e) X^e$. Let $d \in \{0, \ldots, r-1\}^n$. Then 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

## Lemma

*Let $K$ be an integral domain and let $S \subseteq K \setminus \{0\}$, let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ such that $p(t) \neq 0$. Let $r \in \mathbb{N}$ such that $X^r$ is constant on $S$. Assume $p = \sum_{e \in E} c(e)X^e$. Let $d \in \{0, \ldots, r-1\}^n$. Then there exists an $e \in E$ such that for all $1 \leq i \leq n$, we have $d_i \not\equiv_r e_i$.*

## Proof.

- Seeking a contradiction, let $d \in \{0, \ldots, r-1\}^n$ be a counterexample.

$\square$

# Absorbing Polynomials

**Lemma**

*Let $K$ be an integral domain and let $S \subseteq K \setminus \{0\}$, let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ such that $p(t) \neq 0$. Let $r \in \mathbb{N}$ such that $X^r$ is constant on $S$. Assume $p = \sum_{e \in E} c(e) X^e$. Let $d \in \{0, \ldots, r-1\}^n$. Then there exists an $e \in E$ such that for all $1 \leq i \leq n$, we have $d_i \not\equiv_r e_i$.*

**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 $g(t) \neq 0$.

$\square$

# Absorbing Polynomials

## Lemma

*Let $K$ be an integral domain and let $S \subseteq K \setminus \{0\}$, let $p \in K[X_1, \dots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ such that $p(t) \neq 0$. Let $r \in \mathbb{N}$ such that $X^r$ is constant on $S$. Assume $p = \sum_{e \in E} c(e)X^e$. Let $d \in \{0, \dots, r-1\}^n$. Then there exists an $e \in E$ such that for all $1 \leq i \leq n$, we have $d_i \not\equiv_r e_i$.*

## Proof.

- Seeking a contradiction, let $d \in \{0, \dots, r-1\}^n$ be a counterexample.
- Let $g := X_1^{r-d_1} \dots X_n^{r-d_n} p$. 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 $d$.

$\square$

# Absorbing Polynomials

## Lemma

*Let $K$ be an integral domain and let $S \subseteq K \setminus \{0\}$, let $p \in K[X_1, \ldots, X_n]$ be absorbing at $s \in S^n$ and let $t \in S^n$ such that $p(t) \neq 0$. Let $r \in \mathbb{N}$ such that $X^r$ is constant on $S$. Assume $p = \sum_{e \in E} c(e) X^e$. Let $d \in \{0, \ldots, r-1\}^n$. Then there exists an $e \in E$ such that for all $1 \leq i \leq n$, we have $d_i \not\equiv_r e_i$.*

## 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.

$\square$

# Patterns

**Definition**

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* if for all $d \in \underline{r}^n$, we have $e \in E$ such that $e_i \neq d_i$ for all $i \in \underline{n}$.

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

## Proof.

- For $e \in E$ let $D(e) := \{d \in \underline{r}^n \mid \forall i \in \underline{n} : d_i \neq e_i\}$.

$\square$

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

## 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 $e \in E$.

$\square$

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

## 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 $\underline{r}^n = \bigcup_{e \in E} D(e)$.

$\square$

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

## 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 $r^n = |\bigcup_{e \in E} D(e)| \leq \sum_{e \in E} |D(e)| = |E| \cdot (r-1)^n$.

$\square$

# Patterns

## Definition

Let $n, r \in \mathbb{N}$. We call $E \subseteq \underline{r}^n$ *pattern-avoiding* 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 $n \in \mathbb{N}, r \geq 2$ and let $E \subseteq \underline{r}^n$ be pattern-avoiding. Then $|E| \geq (\frac{r}{r-1})^n$.*

## 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 $r^n = |\bigcup_{e \in E} D(e)| \leq \sum_{e \in E} |D(e)| = |E| \cdot (r-1)^n$.
- Hence $(\frac{r}{r-1})^n \leq |E|$

$\square$

# 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 $p \in K[X_1, \dots, X_n]$ 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 be pattern-avioding.

$\square$

# 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 be pattern-avioding.
- Therefore $|E| \geq |E'| \geq (\frac{r}{r-1})^n$.

$\square$

# Rectangles containing zero

**Theorem**

*Let* $n \in \mathbb{N}$*, let* $\mathbb{K}$ *be a field and let* $S_1, \ldots, S_n \subseteq \mathbb{K}$ *be finite. Let* $s \in (S_1 \setminus \{0\}) \times \cdots \times (S_n \setminus \{0\})$ *and let* $p \in \mathbb{K}[X_1, \ldots, X_n]$ *be absorbing at* $s$ *for* $Q := S_1 \times \cdots \times S_n$*. Assume that* $\deg_{X_i} p < |S_i|$ *for all* $i \in \underline{n}$ *and that* $p$ *is nonzero on* $Q$*. Then* $M(p) \geq 2^n$*.*

# Rectangles containing zero

## Theorem

*Let $n \in \mathbb{N}$, let $\mathbb{K}$ be a field and let $S_1, \dots, S_n \subseteq \mathbb{K}$ be finite. Let $s \in (S_1 \setminus \{0\}) \times \dots \times (S_n \setminus \{0\})$ and let $p \in \mathbb{K}[X_1, \dots, X_n]$ be absorbing at $s$ for $Q := S_1 \times \dots \times S_n$. Assume that $\deg_{X_i} p < |S_i|$ for all $i \in \underline{n}$ and that $p$ is nonzero on $Q$. Then $M(p) \geq 2^n$.*

**Sketch of proof:**

- Special case: $S := S_1 = \dots = S_n$.

# Rectangles containing zero

**Theorem**

*Let $n \in \mathbb{N}$, let $\mathbb{K}$ be a field and let $S_1, \ldots, S_n \subseteq \mathbb{K}$ be finite. Let $s \in (S_1 \setminus \{0\}) \times \cdots \times (S_n \setminus \{0\})$ and let $p \in \mathbb{K}[X_1, \ldots, X_n]$ be absorbing at $s$ for $Q := S_1 \times \cdots \times S_n$. Assume that $\deg_{X_i} p < |S_i|$ for all $i \in \underline{n}$ and that $p$ is nonzero on $Q$. Then $M(p) \geq 2^n$.*

**Sketch of proof:**

- Special case: $S := S_1 = \cdots = S_n$.
- Let $r := |S|$ and let $p = \sum_{e \in E} c(e) X^e$.

# Rectangles containing zero

**Theorem**

*Let $n \in \mathbb{N}$, let $\mathbb{K}$ be a field and let $S_1, \ldots, S_n \subseteq \mathbb{K}$ be finite. Let $s \in (S_1 \setminus \{0\}) \times \cdots \times (S_n \setminus \{0\})$ and let $p \in \mathbb{K}[X_1, \ldots, X_n]$ be absorbing at $s$ for $Q := S_1 \times \cdots \times S_n$. Assume that $\deg_{X_i} p < |S_i|$ for all $i \in \underline{n}$ and that $p$ is nonzero on $Q$. Then $M(p) \geq 2^n$.*

**Sketch of proof:**

- Special case: $S := S_1 = \cdots = S_n$.
- Let $r := |S|$ and let $p = \sum_{e \in E} c(e) X^e$.
- Use the degree bound to show that the set $E \subseteq \{0, \ldots, r-1\}^n$ has the following property:

# Rectangles containing zero

## Theorem

*Let $n \in \mathbb{N}$, let $\mathbb{K}$ be a field and let $S_1, \ldots, S_n \subseteq \mathbb{K}$ be finite. Let $s \in (S_1 \setminus \{0\}) \times \cdots \times (S_n \setminus \{0\})$ and let $p \in \mathbb{K}[X_1, \ldots, X_n]$ be absorbing at $s$ for $Q := S_1 \times \cdots \times S_n$. Assume that $\deg_{X_i} p < |S_i|$ for all $i \in \underline{n}$ and that $p$ is nonzero on $Q$. Then $M(p) \geq 2^n$.*

**Sketch of proof:**

- Special case: $S := S_1 = \cdots = S_n$.
- Let $r := |S|$ and let $p = \sum_{e \in E} c(e) X^e$.
- Use the degree bound to show that the set $E \subseteq \{0, \ldots, r-1\}^n$ has the following property:
- For all $d \in E$ and $i \in \underline{n}$, we have $e \in E$ such that $d_i \neq e_i$ and $d_j = e_j$ for all $j \neq i$.

# Rectangles containing zero

**Theorem**

*Let $n \in \mathbb{N}$, let $\mathbb{K}$ be a field and let $S_1, \ldots, S_n \subseteq \mathbb{K}$ be finite. Let $s \in (S_1 \setminus \{0\}) \times \cdots \times (S_n \setminus \{0\})$ and let $p \in \mathbb{K}[X_1, \ldots, X_n]$ be absorbing at $s$ for $Q := S_1 \times \cdots \times S_n$. Assume that $\deg_{X_i} p < |S_i|$ for all $i \in \underline{n}$ and that $p$ is nonzero on $Q$. Then $M(p) \geq 2^n$.*

**Sketch of proof:**

- Special case: $S := S_1 = \cdots = S_n$.
- Let $r := |S|$ and let $p = \sum_{e \in E} c(e) X^e$.
- Use the degree bound to show that the set $E \subseteq \{0, \ldots, r-1\}^n$ has the following property:
- For all $d \in E$ and $i \in \underline{n}$, we have $e \in E$ such that $d_i \neq e_i$ and $d_j = e_j$ for all $j \neq i$.
- Show that every nonempty set $E$ with this property satisfies $|E| \geq 2^n$.

# Density of non-zeros

**Theorem**

*Let $K$ be an integral domain. Let $Q = \{a_1, b_1\} \times \cdots \times \{a_n, b_n\} \subseteq (K \setminus \{0\})^n$ with $a_i \neq b_i$ and let $r \in \mathbb{N}$ such that $a_i^r = b_i^r$ for all $i \in \underline{n}$. Let $t = \frac{r}{r-1}$. Let $p \in K[X_1, \ldots, X_n]$ and let $W := \{x \in Q \mid p(x) \neq 0\}$. If $W \neq \emptyset$, then $|W| \geq 2^{n - \log_t(M(p))}$.*

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.

$\square$

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n - \log_t(M(p))}$ by induction on $|W|$ :

$\square$

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n-\log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n-\log_t(M(p))} \leq 1 = |W|$.

$\square$

# Density of non-zeros

## Proof.

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n-\log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n-\log_t(M(p))} \leq 1 = |W|$.
- If $|W| > 1$, choose $u \neq v \in W$ and $i \in \underline{n}$ with $a = u_i$ and $v_i = b$.

$\square$

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n - \log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n - \log_t(M(p))} \leq 1 = |W|$.
- If $|W| > 1$, choose $u \neq v \in W$ and $i \in \underline{n}$ with $a = u_i$ and $v_i = b$.
- Let $Q' := \{a, b\}^{n-1}$

$\square$

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n - \log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n - \log_t(M(p))} \leq 1 = |W|$.
- If $|W| > 1$, choose $u \neq v \in W$ and $i \in \underline{n}$ with $a = u_i$ and $v_i = b$.
- Let $Q' := \{a, b\}^{n-1}$
- Let $p_a := p_{x_i = a}, p_b := p_{x_i = b}$ and let $W_a := \{w \in Q' \mid p_a(w) \neq 0\}, W_b := \{w \in Q' \mid p_b(w) \neq 0\}$.

$\square$

# Density of non-zeros

**Proof.**

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n-\log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n-\log_t(M(p))} \leq 1 = |W|$.
- If $|W| > 1$, choose $u \neq v \in W$ and $i \in \underline{n}$ with $a = u_i$ and $v_i = b$.
- Let $Q' := \{a, b\}^{n-1}$
- Let $p_a := p_{x_i=a}, p_b := p_{x_i=b}$ and let $W_a := \{w \in Q' \mid p_a(w) \neq 0\}, W_b := \{w \in Q' \mid p_b(w) \neq 0\}$.
- We have $|W_a| \leq |W_b|$ without loss.

$\square$

# Density of non-zeros

## Proof.

- We prove only the case $a := a_1 = \cdots = a_n, b := b_1 = \cdots = b_n$.
- We prove $|W| \geq 2^{n-\log_t(M(p))}$ by induction on $|W|$ :
- If $|W| = 1$, then $p$ is absorbing and therefore $M(p) \geq t^n$, hence $\log_t(M(p)) \geq n$, so $2^{n-\log_t(M(p))} \leq 1 = |W|$.
- If $|W| > 1$, choose $u \neq v \in W$ and $i \in \underline{n}$ with $a = u_i$ and $v_i = b$.
- Let $Q' := \{a, b\}^{n-1}$
- Let $p_a := p_{x_i=a}, p_b := p_{x_i=b}$ and let $W_a := \{w \in Q' \mid p_a(w) \neq 0\}, W_b := \{w \in Q' \mid p_b(w) \neq 0\}$.
- We have $|W_a| \leq |W_b|$ without loss.
- Use the induction hypothesis on $p_a$ to get $|W| = |W_a| + |W_b| \geq 2|W_a| \geq 2 \cdot 2^{(n-1)-\log_t(M(p_a))} \geq 2^{n-\log_t(M(p))}$

□

# 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 $S^n$. Let $a \in S^n$. Then 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 $p \in K[X_1, \dots, X_n]$ be a polynomial that does not vanish on $S^n$. Let $a \in S^n$. Then 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 $\{i \mid a_i \neq b_i\} = \{i_1, \dots, i_k\}$ has minimal size.

$\square$

# 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 $S^n$. Let $a \in S^n$. Then 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 $a_i = b_i$.

$\square$

# 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 $S^n$. Let $a \in S^n$. Then 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.

$\square$

# 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 $S^n$. Let $a \in S^n$. Then 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 $\log_t(M(p)) \geq k$.

$\square$

# 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 $s \in S^n$. For $m \geq 2$ let $T_m := \{x \in S^n \mid \log_t(m) \geq d(s,x)\}$. 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 $S$.

$\square$

# 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 $s \in S^n$. For $m \geq 2$ let $T_m := \{x \in S^n \mid \log_t(m) \geq d(s,x)\}$. 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 $S$.
- The bound $|T_m| \leq (n|S|)^{\log_t(m)}$ can be seen as follows:

□

# 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 $s \in S^n$. For $m \geq 2$ let $T_m := \{x \in S^n \mid \log_t(m) \geq d(s,x)\}$. 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 $S$.
- The bound $|T_m| \leq (n|S|)^{\log_t(m)}$ can be seen as follows:
- Let $k = \lfloor \log_t(m) \rfloor$. Every $t \in T_m$ can be identified with at least one pair $(I, v)$ where $v \in S^k$ and $I \subseteq \underline{n}$ with $|I| = k$.

$\square$

# 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* $s \in S^n$*. For* $m \geq 2$ *let* $T_m := \{x \in S^n \mid \log_t(m) \geq d(s,x)\}$*. 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 $S$.
- The bound $|T_m| \leq (n|S|)^{\log_t(m)}$ can be seen as follows:
- Let $k = \lfloor \log_t(m) \rfloor$. Every $t \in T_m$ can be identified with at least one pair $(I, v)$ where $v \in S^k$ and $I \subseteq \underline{n}$ with $|I| = k$.
- Therefore $|T_m| \leq |S|^k \cdot \binom{n}{k} \leq (n \cdot |S|)^k$.

$\square$

# How did we get here?

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

# 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 $(A_4, \cdot, (-)^{-1})$. 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 $(A_4, \cdot, (-)^{-1})$. Assume that the term function $t^{A_4}$ satisfies $1 \in \{x_1, \dots, x_n\} \Rightarrow t^{A_4}(x_1, \dots, x_n) = 1$ and that $t^{A_4}$ is not always 1. Then $t$ has length at least $2^{n-2}$.*

**Example**

The term $t(x_1, x_2) = [x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$ 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 $(A_4, \cdot, (-)^{-1})$. 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 $(A_4, \cdot, (-)^{-1})$ (but not over $(A_4, \cdot, (-)^{-1}, [\cdot, \cdot]))$ can be done in polynomial time. This does not yield a better algorithm, but it might guide the way towards identity testing over $(S_4, \cdot, (-)^{-1})$.

# Problem 1

To get a quasipolynomial-time algorithm for identity testing over $(S_4, \cdot)$, we would need to prove the following conjecture:

# Problem 1

To get a quasipolynomial-time algorithm for identity testing over $(S_4, \cdot)$, we would need to prove the following conjecture:

## Conjecture

*Let* $\alpha \in \mathbb{K} = GF(4)$ *be an element of order* $3$. *Let* $u(x) := \alpha^x$ *for* $x \in \mathbb{Z}_3$. *Let* $n, k \in \mathbb{N}$. *Let* $E \subseteq \{0,1\}^n$ *and let* $c : E \times \underline{k} \to \mathbb{Z}_3$. *Let* $f : \{1, -1\}^n \to \mathbb{K}$ *be defined by*

$$f(x) = \sum_{i \in \underline{k}} u\Big(\sum_{e \in E} c(e,i) x^e\Big).$$

*Assume that* $f(x)$ *is nonzero for a unique* $x \in \{-1,1\}^n$. *Then*

$$|\{(e,i) \in E \times \underline{k} \mid c(e,i) \neq 0\}| \geq 2^{c\sqrt{n}}.$$

*for some universal* $c > 0$.