Algebraic Aspects of the Polynomial Littlewood–Offord Problem

Zhihan Jin

ISTA

Joint work with Matthew Kwan, Lisa Sauermann and Yiting Wang

Austrian Stochastics Days, Sept 29th, 2026

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

- Can be infinite.

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

- Can be infinite.
- Analytic number theory: how many zeros are in $\{-B, \ldots, -1, 0, 1, \ldots, B\}^n$, where B is large and n is fixed?

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

- Can be infinite.
- Analytic number theory: how many zeros are in $\{-B, \ldots, -1, 0, 1, \ldots, B\}^n$, where B is large and n is fixed?
- What if B is small while n is large?

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

- Can be infinite.
- Analytic number theory: how many zeros are in $\{-B, \ldots, -1, 0, 1, \ldots, B\}^n$, where B is large and n is fixed?
- What if B is small while n is large?
  - How many zeros of f are in $\{-1, 1\}^n$?

Counting solutions of a polynomial

Question

Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, how many zeros does it have?

- Can be infinite.
- Analytic number theory: how many zeros are in $\{-B, \ldots, -1, 0, 1, \ldots, B\}^n$, where B is large and n is fixed?
- What if B is small while n is large?
  - How many zeros of f are in $\{-1, 1\}^n$?
- Counting $\Leftrightarrow$ Probability.

Erdős–Littlewood–Offord theorem

Question

For independent Rademacher random variables $x_1, \ldots, x_n \in \{\pm 1\}$, how likely does $\sum_{i=1}^{n} a_i x_i + c = 0$ hold?

Erdős–Littlewood–Offord theorem

Question

For independent Rademacher random variables $x_1, \dots, x_n \in \{\pm 1\}$, how likely does $\sum_{i=1}^n a_i x_i + c = 0$ hold?

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^n a_i x_i + c = 0\right] \leq \binom{n}{n/2} / 2^n = O\big(1/\sqrt{n}\,\big).$$

Erdős–Littlewood–Offord theorem

Question

For independent Rademacher random variables $x_1, \dots, x_n \in \{\pm 1\}$, how likely does $\sum_{i=1}^n a_i x_i + c = 0$ hold?

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^n a_i x_i + c = 0\right] \le \binom{n}{n/2} / 2^n = O\big(1/\sqrt{n}\,\big).$$

- Foundational result in anti-concentration theory.

Linear Littlewood–Offord problems

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^{n} a_i x_i + c = 0\right] \leq \binom{n}{n/2} / 2^n = O\big(1/\sqrt{n}\,\big).$$

Linear Littlewood–Offord problems

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^{n} a_i x_i + c = 0\right] \le \binom{n}{n/2} / 2^n = O\big(1/\sqrt{n}\,\big).$$

- $\binom{n}{n/2}/2^n$ is the probability of $\sum_i x_i = 0$.

Linear Littlewood–Offord problems

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^{n} a_i x_i + c = 0\right] \leq \binom{n}{n/2}/2^n = O\big(1/\sqrt{n}\,\big).$$

- $\binom{n}{n/2}/2^n$ is the probability of $\sum_i x_i = 0$.
  - In this case, $a_1 = a_2 = \cdots = a_n$.

Linear Littlewood–Offord problems

Theorem (Erdős–Littlewood–Offord 1945)

If $a_1, \dots, a_n \in \mathbb{R} \setminus \{0\}, c \in \mathbb{R}$, *then*

$$\mathbb{P}\left[\sum_{i=1}^{n} a_i x_i + c = 0\right] \leq \binom{n}{n/2}/2^n = O\big(1/\sqrt{n}\,\big).$$

- $\binom{n}{n/2}/2^n$ is the probability of $\sum_i x_i = 0$.
  - In this case, $a_1 = a_2 = \cdots = a_n$.

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Linear Littlewood–Offord problems

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Linear Littlewood–Offord problems

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Theorem (Tao–Vu 2009)

If $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \gg n^{-C}$, *then almost all of the* a_i*s lie in a 'generalised arithmetic progression'.*

Linear Littlewood–Offord problems

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Theorem (Tao–Vu 2009)

If $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \gg n^{-C}$, *then almost all of the* a_i*s lie in a 'generalised arithmetic progression'.*

- In some sense, a tight characterisation of when $\mathbb{P}[\cdot]$ is large.

Linear Littlewood–Offord problems

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Theorem (Tao–Vu 2009)

If $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \gg n^{-C}$, *then almost all of the* a_i*s lie in a 'generalised arithmetic progression'.*

- In some sense, a tight characterisation of when $\mathbb{P}[\cdot]$ is large.
- $\hookrightarrow \mathbb{P}[\cdot] \approx n^{-1/2}$ implies almost all a_is are essentially the same.

Linear Littlewood–Offord problems

Question

Does $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \approx n^{-1/2}$ imply anything about the coefficients?

Theorem (Tao–Vu 2009)

If $\mathbb{P}\big[\sum_i a_i x_i + c = 0\big] \gg n^{-C}$, *then almost all of the* a_i*s lie in a 'generalised arithmetic progression'.*

- In some sense, a tight characterisation of when $\mathbb{P}[\cdot]$ is large.
- $\hookrightarrow \mathbb{P}[\cdot] \approx n^{-1/2}$ implies almost all a_is are essentially the same.
- Useful in random matrix theory etc.

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.

Polynomial Littlewood–Offord Problems

Setting: $x_1, \dots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \dots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \dots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?

Polynomial Littlewood–Offord Problems

Setting: $x_1, \dots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \dots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \dots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.

Polynomial Littlewood–Offord Problems

Setting: $x_1, \dots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \dots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \dots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2$

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2 \Rightarrow -10n \leq \boldsymbol{x}^T A \boldsymbol{x} \leq 10n$ whp.

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2 \Rightarrow -10n \leq \boldsymbol{x}^T A \boldsymbol{x} \leq 10n$ whp.
  - Expect anti-concentration $1/n$?

Polynomial Littlewood–Offord Problems

Setting: $x_1, \ldots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \ldots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2 \Rightarrow -10n \leq \boldsymbol{x}^T A \boldsymbol{x} \leq 10n$ whp.
  - Expect anti-concentration $1/n$?
- $\mathbb{P}\Big[\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big) = 0\Big] \geq \mathbb{P}\big[\sum_{i<n/2} x_i = 0\big] \approx 1/\sqrt{n}.$

Polynomial Littlewood–Offord Problems

Setting: $x_1, \dots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \dots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \dots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2 \Rightarrow -10n \leq \boldsymbol{x}^T A \boldsymbol{x} \leq 10n$ whp.
  - Expect anti-concentration $1/n$?
- $\mathbb{P}\Big[\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big) = 0\Big] \geq \mathbb{P}\big[\sum_{i<n/2} x_i = 0\big] \approx 1/\sqrt{n}.$
- Maybe $f \approx g \cdot h$ is the only obstruction to getting $1/n$?

Polynomial Littlewood–Offord Problems

Setting: $x_1, \dots, x_n \in \{\pm 1\}$ are i.i.d. Rademacher random variables.

Question

If $f(x_1, \dots, x_n)$ is a degree-d polynomial, how large is

$$\mathbb{P}\big[f(x_1, \dots, x_n) = 0\big]?$$

- E.g. $\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big)$, $\boldsymbol{x}^T A \boldsymbol{x}$ for $A \in \mathbb{R}^{n\times n}$.
- What anti-concentration do we expect?
- Consider $\boldsymbol{x}^T A \boldsymbol{x}$ for a generic $A \in \{0,1\}^{n\times n}$.
  - $\mathrm{Var}(\boldsymbol{x}^T A \boldsymbol{x}) \approx n^2 \Rightarrow -10n \leq \boldsymbol{x}^T A \boldsymbol{x} \leq 10n$ whp.
  - Expect anti-concentration $1/n$?
- $\mathbb{P}\Big[\big(\sum_{i<n/2} x_i\big)\big(\sum_{j\geq n/2} x_j\big) = 0\Big] \geq \mathbb{P}\big[\sum_{i<n/2} x_i = 0\big] \approx 1/\sqrt{n}$.
- Maybe $f \approx g \cdot h$ is the only obstruction to getting $1/n$?
  - Meka–Nguyen–Vu: as long as $f \not\approx 0$, $\mathbb{P}[f = 0] \leq n^{\varepsilon - 1/2}$.

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\ldots,x_n)=0\big] \leq n^{\varepsilon-1}$.

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\ldots,x_n)=0\big] \leq n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\ldots,x_n)=0\big] \le n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).
- Costello proved it for **bilinear** forms, i.e. $f = \boldsymbol{x}^T A \boldsymbol{y}$.

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).
- Costello proved it for **bilinear** forms, i.e. $f = \boldsymbol{x}^T A \boldsymbol{y}$.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Costello's conjecture holds for multilinear forms of any fixed degree.

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).
- Costello proved it for **bilinear** forms, i.e. $f = \boldsymbol{x}^T A \boldsymbol{y}$.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Costello's conjecture holds for multilinear forms of any fixed degree.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Suppose f is a quadratic form.

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).
- Costello proved it for **bilinear** forms, i.e. $f = \boldsymbol{x}^T A \boldsymbol{y}$.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Costello's conjecture holds for multilinear forms of any fixed degree.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Suppose f is a quadratic form.

- $\mathbb{P}[f=0] \le n^{-0.54}$ *if* $\deg(f)=2$ *and 'far' from being reducible.*

Corrected Costello's conjecture

Conjecture (Costello 2013, corrected)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon-1}$.

- Connected to counting integral points in varieties (e.g., the *affine dimension growth conjecture*).
- Costello proved it for **bilinear** forms, i.e. $f = \boldsymbol{x}^T A \boldsymbol{y}$.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Costello's conjecture holds for multilinear forms of any fixed degree.

Theorem (J., Kwan, Sauermann and Wang 2025+)

Suppose f is a quadratic form.

- $\mathbb{P}[f=0] \le n^{-0.54}$ *if* $\deg(f)=2$ *and 'far' from being reducible.*
- $\mathbb{P}[f=0] \le n^{\varepsilon-1}$ *if* $\deg(f)=2$ *and* $f \not\approx \sum_{i\le O(1)} g_i h_i$.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

$$A = \left[\begin{array}{c|c} A_{I,I} & A_{I,J} \\ \hline A_{I,J}^T & A_{J,J} \end{array}\right]$$

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

$$A = \left[\begin{array}{c|c} A_{I,I} & A_{I,J} \\ \hline A_{I,J}^T & A_{J,J} \end{array}\right] \qquad f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$$

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

$$A = \left[\begin{array}{c|c} A_{I,I} & A_{I,J} \\ \hline A_{I,J}^T & A_{J,J} \end{array}\right]$$

$$\begin{aligned} & f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J) \\ &= 2 \cdot \boldsymbol{x}_I^T A_{I,J} \big(\boldsymbol{x}_J^{(1)} - \boldsymbol{x}_J\big) + \varphi\big(\boldsymbol{x}_J, \boldsymbol{x}_J^{(1)}\big). \end{aligned}$$

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

- How to reduce it to the linear case?

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

$$A = \left[\begin{array}{c|c} A_{I,I} & A_{I,J} \\ \hline A_{I,J}^T & A_{J,J} \end{array}\right]$$

$$\begin{aligned} & f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J) \\ = \; & 2 \cdot \boldsymbol{x}_I^T A_{I,J} \big(\boldsymbol{x}_J^{(1)} - \boldsymbol{x}_J\big) + \varphi\big(\boldsymbol{x}_J, \boldsymbol{x}_J^{(1)}\big). \end{aligned}$$

It is linear in $\boldsymbol{x}_I$!

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - We wasted half of the equations. 

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - We wasted half of the equations. 
- Sample m independent copies $\boldsymbol{x}_J^{(1)}, \ldots, \boldsymbol{x}_J^{(m)}$ of $\boldsymbol{x}_J$.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - We wasted half of the equations. 
- Sample m independent copies $\boldsymbol{x}_J^{(1)}, \ldots, \boldsymbol{x}_J^{(m)}$ of $\boldsymbol{x}_J$.
  - Every $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(i)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.

Costello's conjecture for quadratic forms

Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - We wasted half of the equations. 
- Sample m independent copies $\boldsymbol{x}_J^{(1)}, \ldots, \boldsymbol{x}_J^{(m)}$ of $\boldsymbol{x}_J$.
  - Every $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(i)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - Make use of m out of $m + 1$ equations.

Costello's conjecture for quadratic forms

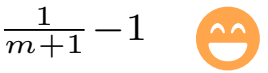
Setting: $f(x_1, \ldots, x_n) = f(\boldsymbol{x}) = \boldsymbol{x}^T A \boldsymbol{x}$ for symmetric $A \in \mathbb{C}^{n \times n}$.

Show: $\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] \leq n^{\varepsilon - 1}$ or A can be made low rank by changing $o(n^2)$ entries.

The decoupling trick

Partition $[n] = I \cup J$ and let $\boldsymbol{x}_J^{(1)}$ be an independent copy of $\boldsymbol{x}_J$.

$$\mathbb{P}\big[f(\boldsymbol{x}) = 0\big] = \mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = 0\big] \leq \sqrt{\mathbb{P}\big[f(\boldsymbol{x}_I, \boldsymbol{x}_J) = f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) = 0\big]}$$

- $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(1)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - We wasted half of the equations. 
- Sample m independent copies $\boldsymbol{x}_J^{(1)}, \ldots, \boldsymbol{x}_J^{(m)}$ of $\boldsymbol{x}_J$.
  - Every $f(\boldsymbol{x}_I, \boldsymbol{x}_J^{(i)}) - f(\boldsymbol{x}_I, \boldsymbol{x}_J)$ is linear in $\boldsymbol{x}_I$.
  - Make use of m out of $m+1$ equations.
  - Expect $\mathbb{P}[f(\boldsymbol{x}) = 0] \leq (n^{\varepsilon-1})^{m/(m+1)} \approx n^{\varepsilon + \frac{1}{m+1} - 1}$ 

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.
- Apply the inverse Littlewood–Offord theorem to $\boldsymbol{x}_I$.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.
- Apply the inverse Littlewood–Offord theorem to $\boldsymbol{x}_I$.
  - Almost all coefficients are very 'structured'.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.
- Apply the inverse Littlewood–Offord theorem to $\boldsymbol{x}_I$.
  - Almost all coefficients are very 'structured'.
- Almost all 1000×1000 submatrices of $A_{I,J}$ are degenerate.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.
- Apply the inverse Littlewood–Offord theorem to $\boldsymbol{x}_I$.
  - Almost all coefficients are very 'structured'.
- Almost all 1000×1000 submatrices of $A_{I,J}$ are degenerate.

  $\Rightarrow$ Almost all 1000×1000 of A are degenerate.

Costello's conjecture for quadratic forms

- After decoupling, we get m equations, linear in $\boldsymbol{x}_I$.
  - Each coefficient is given by a row of $A_{I,J}$ and $\boldsymbol{x}_J^{(i)} - \boldsymbol{x}_J$, $i \in [m]$.
- Suppose $\mathbb{P}[f(\boldsymbol{x}) = 0] \geq n^{\varepsilon - 1}$.
- Apply the inverse Littlewood–Offord theorem to $\boldsymbol{x}_I$.
  - Almost all coefficients are very 'structured'.
- Almost all 1000×1000 submatrices of $A_{I,J}$ are degenerate.

  $\Rightarrow$ Almost all 1000×1000 of A are degenerate.
- A local-to-global phenomenon on the rank: A can be made rank-$O(1)$ up to changing $o(n^2)$ entries.

Future Directions

- So far, the proofs have been mostly combinatorial. A more geometric method to study $\{-1,1\}^n \cap \{\boldsymbol{x} : f(x_1,\ldots,x_n) = 0\}$?

Future Directions

- So far, the proofs have been mostly combinatorial. A more geometric method to study $\{-1,1\}^n \cap \{\boldsymbol{x} : f(x_1,\ldots,x_n) = 0\}$?
- Prove Costello's conjecture (corrected).

Future Directions

- So far, the proofs have been mostly combinatorial. A more geometric method to study $\{-1,1\}^n \cap \{\boldsymbol{x} : f(x_1,\ldots,x_n) = 0\}$?
- Prove Costello's conjecture (corrected).
- What happens when $\mathbb{P}[f = 0] \gg n^{-100}$?

Thank you!

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1, \ldots, x_n) = 0\big] \leq n^{\varepsilon - d/2}$.

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\ldots,x_n)=0\big] \le n^{\varepsilon-d/2}$.

- Sah–Sawhney–Kwan: false for $d \ge 3$.

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon - d/2}$.

- Sah–Sawhney–Kwan: false for $d \ge 3$.



$L_1 = \sum_{i\in I_1} x_i$ $\quad\cdots\quad$ $L_6 = \sum_{i\in I_6} x_i$

$$f(x_1,\dots,x_n) = L_1L_2L_3 + L_4L_5L_6$$

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon - d/2}$.

- Sah–Sawhney–Kwan: false for $d \ge 3$.



$L_1 = \sum_{i\in I_1} x_i$ $\quad\cdots\quad$ $L_6 = \sum_{i\in I_6} x_i$

$$f(x_1,\dots,x_n) = L_1L_2L_3 + L_4L_5L_6$$

- $\mathbb{P}\big[f=0\big] \ge \mathbb{P}[L_1=0]\cdot\mathbb{P}[L_4=0] \succeq 1/n.$

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon - d/2}$.

- Sah–Sawhney–Kwan: false for $d \ge 3$.



$L_1 = \sum_{i\in I_1} x_i$ $\qquad \cdots \qquad$ $L_6 = \sum_{i\in I_6} x_i$

$$f(x_1,\dots,x_n) = L_1L_2L_3 + L_4L_5L_6$$

- $\mathbb{P}\big[f=0\big] \ge \mathbb{P}[L_1=0]\cdot\mathbb{P}[L_4=0] \succeq 1/n$.
- f is 'far' from being reducible.

A counterexample to Costello's original conjecture

Conjecture (Costello 2013)

Suppose f is a degree-d polynomial. If f is 'far' from being reducible, then $\mathbb{P}\big[f(x_1,\dots,x_n)=0\big] \le n^{\varepsilon-d/2}$.

- Sah–Sawhney–Kwan: false for $d \ge 3$.



$L_1 = \sum_{i\in I_1} x_i$ $\quad\cdots\quad$ $L_6 = \sum_{i\in I_6} x_i$

$$f(x_1,\dots,x_n) = L_1L_2L_3 + L_4L_5L_6$$

- $\mathbb{P}\big[f=0\big] \ge \mathbb{P}[L_1=0]\cdot\mathbb{P}[L_4=0] \succeq 1/n$.
- f is 'far' from being reducible.

Question

Does $\mathbb{P}[f=0] > n^{\varepsilon-d/2}$ imply that f is essentially determined by $O(1)$ polynomials of degree at most $d-1$?