Combinatorial Nullstellensatz and the Erdős box problem

Alexey Gordeev

Department of Mathematics and Mathematical Statistics, Umeå University, Sweden

August 19, 2024

Combinatorial Nullstellensatz

- $\mathbb{F}$ — any field, $f \in \mathbb{F}[x_1, \ldots, x_r]$
- $x_1^{d_1} \ldots x_r^{d_r}$ is a *monomial of f* if its coefficient in f is non-zero

Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

Combinatorial Nullstellensatz

- $\mathbb{F}$ — any field, $f \in \mathbb{F}[x_1, \ldots, x_r]$
- $x_1^{d_1} \ldots x_r^{d_r}$ is a *monomial of f* if its coefficient in f is non-zero

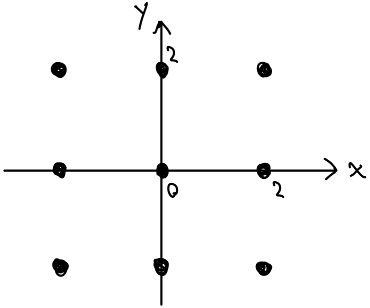
Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

◇ *Example*: $\deg f(x, y) = 4$

$f(x, y) = \cdots + cx^2y^2$

$A_1 = A_2 = \{-2, 0, 2\}$



Combinatorial Nullstellensatz

- $\mathbb{F}$ — any field, $f \in \mathbb{F}[x_1, \dots, x_r]$
- $x_1^{d_1} \dots x_r^{d_r}$ is a *monomial of f* if its coefficient in f is non-zero

Combinatorial Nullstellensatz (Alon, 1999)

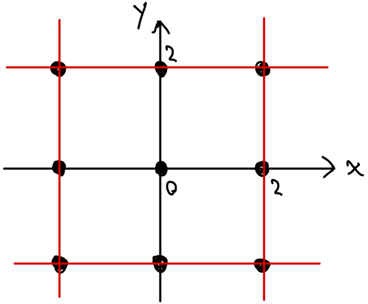
If $x_1^{d_1} \dots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \dots + d_r$, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \dots \times A_r$.

◇ *Example*: $\deg f(x, y) = 4$

$f(x, y) = \dots + cx^2y^2$

$A_1 = A_2 = \{-2, 0, 2\}$

◇ $(x-2)(x+2)(y-2)(y+2)$



Combinatorial Nullstellensatz

- $\mathbb{F}$ — any field, $f \in \mathbb{F}[x_1, \ldots, x_r]$
- $x_1^{d_1} \ldots x_r^{d_r}$ is a *monomial of f* if its coefficient in f is non-zero

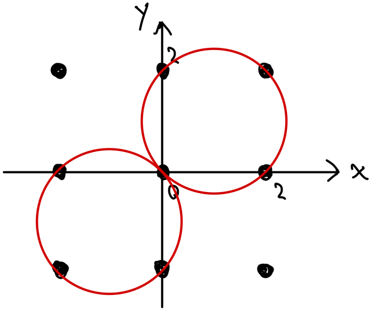
Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

- ◇ *Example*: $\deg f(x,y) = 4$

  $f(x,y) = \cdots + cx^2y^2$

  $A_1 = A_2 = \{-2, 0, 2\}$
- ◇ $((x-1)^2 + (y-1)^2 - 2) \cdot ((x+1)^2 + (y+1)^2 - 2)$



Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A + B| \geq \min(p, |A| + |B| - 1)$.

Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A+B| \geq \min(p, |A|+|B|-1)$.

1. If $|A|+|B|>p$, then $A \cap (x-B) \neq \emptyset$ for every $x \in \mathbb{Z}_p$, so $A+B=\mathbb{Z}_p$.

Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A+B| \geq \min(p, |A|+|B|-1)$.

1. If $|A|+|B|>p$, then $A \cap (x-B) \neq \emptyset$ for every $x \in \mathbb{Z}_p$, so $A+B=\mathbb{Z}_p$.
2. Otherwise, suppose $|A+B| \leq |A|+|B|-2 < p$ and define

$$f(x,y) := \prod_{c \in A+B} (x+y-c).$$

Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A + B| \geq \min(p, |A| + |B| - 1)$.

1. If $|A| + |B| > p$, then $A \cap (x - B) \neq \emptyset$ for every $x \in \mathbb{Z}_p$, so $A + B = \mathbb{Z}_p$.
2. Otherwise, suppose $|A + B| \leq |A| + |B| - 2 < p$ and define

$$f(x, y) := \prod_{c \in A+B} (x + y - c).$$

3. $f(a, b) = 0$ for any $a \in A$, $b \in B$, i.e. f vanishes on $A \times B$.

Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A+B| \geq \min(p, |A|+|B|-1)$.

1. If $|A|+|B|>p$, then $A \cap (x-B) \neq \emptyset$ for every $x \in \mathbb{Z}_p$, so $A+B=\mathbb{Z}_p$.
2. Otherwise, suppose $|A+B| \leq |A|+|B|-2<p$ and define

$$f(x,y) := \prod_{c \in A+B} (x+y-c).$$

3. $f(a,b)=0$ for any $a \in A$, $b \in B$, i.e. f vanishes on $A \times B$.
4. The coefficient of $x^{|A|-1} y^{|A+B|-|A|+1}$ in f is $\binom{|A+B|}{|A|-1} \neq 0 \pmod p$,

Example: a proof of Cauchy-Davenport theorem

Cauchy-Davenport theorem

If p is a prime, $\emptyset \neq A, B \subset \mathbb{Z}_p$, then $|A+B| \geq \min(p, |A|+|B|-1)$.

1. If $|A|+|B| > p$, then $A \cap (x-B) \neq \emptyset$ for every $x \in \mathbb{Z}_p$, so $A+B = \mathbb{Z}_p$.
2. Otherwise, suppose $|A+B| \leq |A|+|B|-2 < p$ and define

$$f(x,y) := \prod_{c \in A+B} (x+y-c).$$

3. $f(a,b) = 0$ for any $a \in A$, $b \in B$, i.e. f vanishes on $A \times B$.
4. The coefficient of $x^{|A|-1}y^{|A+B|-|A|+1}$ in f is $\binom{|A+B|}{|A|-1} \neq 0 \pmod{p}$, $|A+B|-|A|+1 \leq |B|-1$, thus, by **CN**, f does not vanish on $A \times B$.

Generalized Combinatorial Nullstellensatz

Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \dots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

Generalized Combinatorial Nullstellensatz

Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \dots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

- $x_1^{d_1} \dots x_r^{d_r}$ is a *maximal monomial* of f if it does not divide any other monomial of f

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

Generalized Combinatorial Nullstellensatz

Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

- $x_1^{d_1} \ldots x_r^{d_r}$ is a *maximal monomial* of f if it does not divide any other monomial of f

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

◇ *Example*: $f(x, y) = x^{100} + xy + y^{100}$

Generalized Combinatorial Nullstellensatz

Combinatorial Nullstellensatz (Alon, 1999)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a monomial of f and $\deg f = d_1 + \cdots + d_r$, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

- $x_1^{d_1} \ldots x_r^{d_r}$ is a *maximal monomial* of f if it does not divide any other monomial of f

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

- ◇ *Example*: $f(x, y) = x^{100} + xy + y^{100}$
- ◇ **Schauz, 2008**: even more general theorem
- ◇ in practically all known applications the degree condition is sufficient

Turán numbers

- G — graph; *Turán number* (or *extremal number*) $\mathrm{ex}(n, G)$ — maximum number of edges in a graph on n vertices containing no copies of G

Theorem (Turán, 1941)

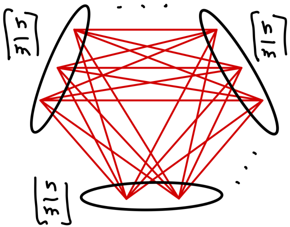
$\mathrm{ex}(n, K_{m+1}) = \left(1 - \frac{1}{m} + o(1)\right)\binom{n}{2}$.

Turán numbers

- G — graph; *Turán number* (or *extremal number*) $\mathrm{ex}(n,G)$ — maximum number of edges in a graph on n vertices containing no copies of G

Theorem (Turán, 1941)

$\mathrm{ex}(n,K_{m+1}) = \left(1-\frac{1}{m}+o(1)\right)\binom{n}{2}$.

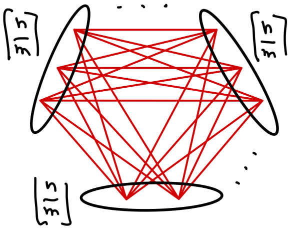


Turán numbers

- G — graph; *Turán number* (or *extremal number*) $\mathrm{ex}(n, G)$ — maximum number of edges in a graph on n vertices containing no copies of G

Theorem (Turán, 1941)

$$\mathrm{ex}(n, K_{m+1}) = \left(1 - \tfrac{1}{m} + o(1)\right)\binom{n}{2}.$$



Theorem (Erdős–Stone, 1946)

$$\mathrm{ex}(n, G) = \left(1 - \frac{1}{\chi(G)-1} + o(1)\right)\binom{n}{2}.$$

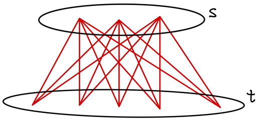
◇ determines $\mathrm{ex}(n, G)$ asymptotically when G is not bipartite ($\chi(G) > 2$)

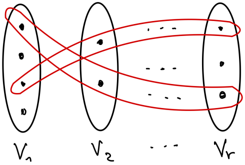
Hypergraph Turán numbers and r-partite r-graphs

- *hypergraph* $H = (V, E)$: V — set of vertices, $E \subset 2^V$ — set of edges
- *r-graph* (or *r-uniform hypergraph*): every edge contains r vertices
- H — r-graph; *Turán number* $\mathrm{ex}(n, H)$ — maximum number of edges in an r-graph on n vertices containing no copies of H

Hypergraph Turán numbers and r-partite r-graphs

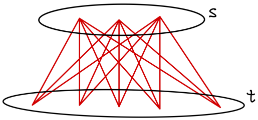
- *hypergraph* $H = (V, E)$: V — set of vertices, $E \subset 2^V$ — set of edges
- *r-graph* (or *r-uniform hypergraph*): every edge contains r vertices
- H — r-graph; *Turán number* $\mathrm{ex}(n, H)$ — maximum number of edges in an r-graph on n vertices containing no copies of H
- *r-partite* r-graph $H = (V_1 \sqcup \cdots \sqcup V_r, E)$: each edge intersects each V_i
- *complete r-partite r-graph* $K^{(r)}_{s_1,\ldots,s_r}$: $|V_i| = s_i$, all $s_1 \ldots s_r$ possible edges

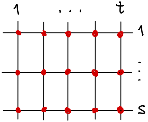


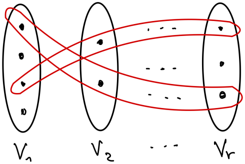


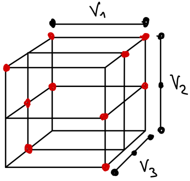
Hypergraph Turán numbers and r-partite r-graphs

- *hypergraph* $H = (V, E)$: V — set of vertices, $E \subset 2^V$ — set of edges
- *r-graph* (or *r-uniform hypergraph*): every edge contains r vertices
- H — r-graph; *Turán number* $\mathrm{ex}(n, H)$ — maximum number of edges in an r-graph on n vertices containing no copies of H
- *r-partite* r-graph $H = (V_1 \sqcup \cdots \sqcup V_r, E)$: each edge intersects each V_i
- *complete r-partite r-graph* $K^{(r)}_{s_1,\ldots,s_r}$: $|V_i| = s_i$, all $s_1 \ldots s_r$ possible edges

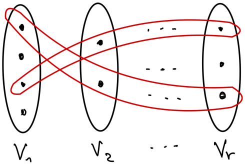


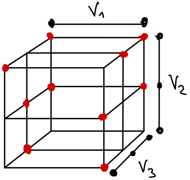






Turán numbers of complete r-partite r-graphs

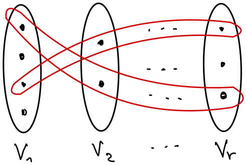


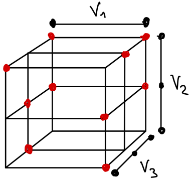


Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\ldots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \leq \cdots \leq s_r$.

Turán numbers of complete r-partite r-graphs



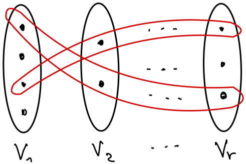


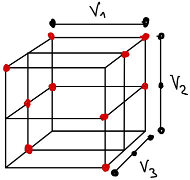
Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\ldots,s_r}) = O\left(n^{r - \frac{1}{s_1 \cdots s_{r-1}}}\right)$ for $s_1 \leq \cdots \leq s_r$.

- **Conjecture:** is asymptotically tight **Mubayi, 2002**

Turán numbers of complete r-partite r-graphs



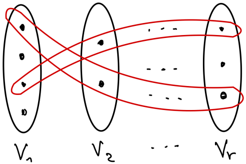


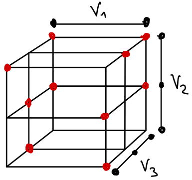
Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\dots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \leq \cdots \leq s_r$.

- **Conjecture:** is asymptotically tight — **Mubayi, 2002**
- **True for:** $K_{2,2}$ and $K_{3,3}$ — **E.Klein, 1934 and Brown, 1966**

Turán numbers of complete r-partite r-graphs





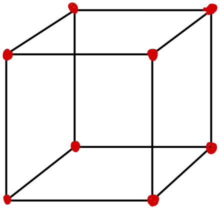
Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

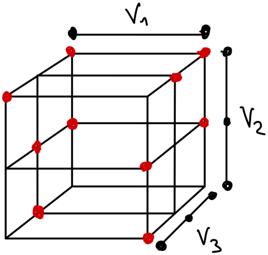
$\mathrm{ex}(n, K^{(r)}_{s_1,\dots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \le \cdots \le s_r$.

◇ **Conjecture:** is asymptotically tight **Mubayi, 2002**

- **True for:** $K_{2,2}$ and $K_{3,3}$ **E.Klein, 1934 and Brown, 1966**
- $s_i \ge 2$ and $s_r \ge C(s_1, \dots, s_{r-1})$ **Ma–Yuan–Zhang, 2018**
  (for graphs: **Blagojević–Bukh–Karasev, 2013**, **Bukh, 2015**)
- $s_i \ge 2$ and $s_r > ((r-1)(s_1 \dots s_{r-1} - 1))!$ **Pohoata–Zakharov, 2021+**
  (for graphs: **Kollár–Rónyai–Szabó, 1996**, **Alon–Rónyai–Szabó, 1999**)

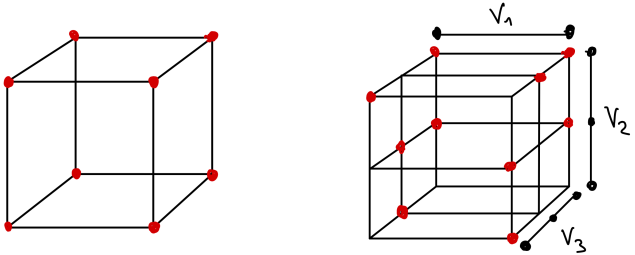
Erdős box problem





- $\mathrm{ex}(n, K^{(r)}_{2,\ldots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**

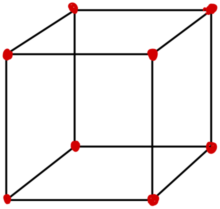
Erdős box problem

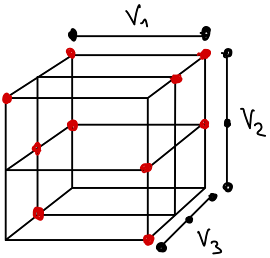


- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K_{2,2}) = \Theta(n^{3/2})$ **E.Klein, 1934**

◇ no matching lower bound for $r > 2$ is known

Erdős box problem



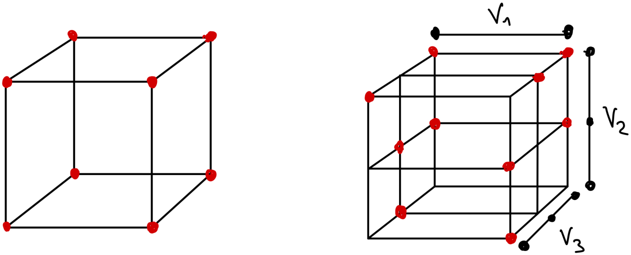


- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K_{2,2}) = \Theta(n^{3/2})$ **E.Klein, 1934**

◇ no matching lower bound for $r > 2$ is known

- $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$ **Katz–Krop–Maggioni, 2002**

Erdős box problem



- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K_{2,2}) = \Theta(n^{3/2})$ **E.Klein, 1934**

◇ no matching lower bound for $r > 2$ is known

- $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$ **Katz–Krop–Maggioni, 2002**
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\lceil\frac{2^r-1}{r}\rceil^{-1}}\right)$ **Conlon–Pohoata–Zakharov, 2021**
  (improving on **Gunderson–Rödl–Sidorenko, 1999**)

Erdős box problem

- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\lceil\frac{2^r-1}{r}\rceil^{-1}}\right)$ **Conlon–Pohoata–Zakharov, 2021**
    - algebraic structure + random multilinear maps

Erdős box problem

- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\lceil \frac{2^r-1}{r} \rceil^{-1}}\right)$ **Conlon–Pohoata–Zakharov, 2021**
  - algebraic structure + random multilinear maps
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right)$ **G., 2024**
  - an application of a new method using Combinatorial Nullstellensatz
  - explicit construction, simple proof

Erdős box problem

- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\lceil\frac{2^r-1}{r}\rceil^{-1}}\right)$ **Conlon–Pohoata–Zakharov, 2021**
  - ◇ algebraic structure + random multilinear maps
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right)$ **G., 2024**
  - ◇ an application of a new method using Combinatorial Nullstellensatz
  - ◇ explicit construction, simple proof

r	2	3	4	5	6
$r - \frac{1}{2^{r-1}}$	1.5	2.75	3.875	4.9375	5.96875
$r - \lceil\frac{2^r-1}{r}\rceil^{-1}$	1.5	2.(6)	3.75	4.(857142)	5.(90)
$r - \frac{1}{r}$	1.5	2.(6)	3.75	4.8	5.8(3)

Erdős box problem

- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = O\left(n^{r-\frac{1}{2^{r-1}}}\right)$ for $r \geq 2$ **Erdős, 1964**
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\lceil\frac{2^r-1}{r}\rceil^{-1}}\right)$ **Conlon–Pohoata–Zakharov, 2021**
  - algebraic structure + random multilinear maps
- $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right)$ **G., 2024**
  - an application of a new method using Combinatorial Nullstellensatz
  - explicit construction, simple proof

r	2	3	4	5	6
$r - \frac{1}{2^{r-1}}$	1.5	2.75	3.875	4.9375	5.96875
$r - \lceil\frac{2^r-1}{r}\rceil^{-1}$	1.5	2.(6)	3.75	4.(857142)	5.(90)
$r - \frac{1}{r}$	1.5	2.(6)	3.75	4.8	5.8(3)

- $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$ **Katz–Krop–Maggioni, 2002**

  $\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right)$ **Yang, 2021, PhD thesis**
  - proof is much more complicated

The framework

- *The Generalized Combinatorial Lasoń–Alon–Zippel–Schwartz Nullstellensatz Lemma, arxiv:2305.10900* **Rote, 2023**

The framework

◇ *The Generalized Combinatorial Lasoń–Alon–Zippel–Schwartz Nullstellensatz Lemma, arxiv:2305.10900* **Rote, 2023**

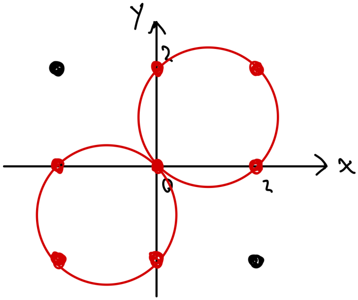
- $\mathbb{F}$ — field, $f \in \mathbb{F}[x_1, \ldots, x_r]$, $B_1, \ldots, B_r \subset \mathbb{F}$, $B = B_1 \times \cdots \times B_r$
- $Z(f, B) := \{(a_1, \ldots, a_r) \in B \mid f(a_1, \ldots, a_r) = 0\}$

The framework

◇ *The Generalized Combinatorial Lasoń–Alon–Zippel–Schwartz Nullstellensatz Lemma, arxiv:2305.10900* **Rote, 2023**

- $\mathbb{F}$ — field, $f \in \mathbb{F}[x_1, \ldots, x_r]$, $B_1, \ldots, B_r \subset \mathbb{F}$, $B = B_1 \times \cdots \times B_r$
- $Z(f, B) := \{(a_1, \ldots, a_r) \in B \mid f(a_1, \ldots, a_r) = 0\}$
- $H(f, B) := (V, E)$ is an r-partite r-graph, where

$$V := B_1 \sqcup \cdots \sqcup B_r, \quad E := Z(f, B)$$

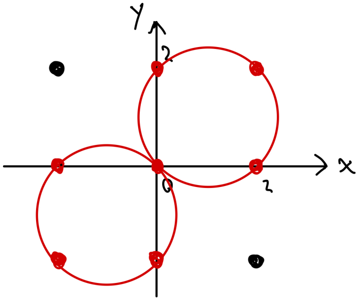


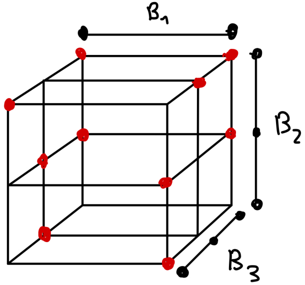
The framework

◇ *The Generalized Combinatorial Lasoń–Alon–Zippel–Schwartz Nullstellensatz Lemma, arxiv:2305.10900* **Rote, 2023**

- $\mathbb{F}$ — field, $f \in \mathbb{F}[x_1, \ldots, x_r]$, $B_1, \ldots, B_r \subset \mathbb{F}$, $B = B_1 \times \cdots \times B_r$
- $Z(f, B) := \{(a_1, \ldots, a_r) \in B \mid f(a_1, \ldots, a_r) = 0\}$
- $H(f, B) := (V, E)$ is an r-partite r-graph, where

$$V := B_1 \sqcup \cdots \sqcup B_r, \quad E := Z(f, B)$$





The framework

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \ldots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \ldots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \ldots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

The framework

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

Key Lemma

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \cdots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

The framework

Generalized Combinatorial Nullstellensatz (Lasoń, 2010)

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, then for any $A_1, \dots, A_r \subset \mathbb{F}$ with $|A_i| \geq d_i + 1$, $f(a_1, \dots, a_r) \neq 0$ for some $a_i \in A_i$. In other words, f does not vanish on $A_1 \times \cdots \times A_r$.

Key Lemma

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \cdots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Key Lemma (general)

If for every $\pi \in \mathcal{S}_r$ there exists a maximal monomial of f which divides $x_{\pi_1}^{d_1} \dots x_{\pi_r}^{d_r}$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \cdots \times B_r)$ is free of copies of $K^{(r)}_{d_1+1,\dots,d_r+1}$.

Schwartz–Zippel type corollary

Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\dots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \le \cdots \le s_r$.

Key Lemma

If $x_1^{d_1}\dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1,\dots,d_r)$, then for any $B_1,\dots,B_r \subset \mathbb{F}$, $H(f, B_1 \times \cdots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Schwartz–Zippel type corollary

Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\ldots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \le \cdots \le s_r$.

Key Lemma

If $x_1^{d_1}\ldots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1,\ldots,d_r)$, then for any $B_1,\ldots,B_r \subset \mathbb{F}$, $H(f, B_1\times\cdots\times B_r)$ is free of copies of $K^{(r)}_{d+1,\ldots,d+1}$.

Corollary

If $x_1^{d_1}\ldots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1,\ldots,d_r)$, then for any $B_1,\ldots,B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1\times\cdots\times B_r)| = O\left(n^{r-\frac{1}{(d+1)^{r-1}}}\right).$$

Schwartz–Zippel type corollary

Theorem (Erdős, 1964; for graphs: Kővári–Sós–Turán, 1954)

$\mathrm{ex}(n, K^{(r)}_{s_1,\dots,s_r}) = O\left(n^{r-\frac{1}{s_1\cdots s_{r-1}}}\right)$ for $s_1 \le \cdots \le s_r$.

Key Lemma

If $x_1^{d_1}\dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1,\dots,d_r)$, then for any $B_1,\dots,B_r \subset \mathbb{F}$, $H(f, B_1\times\cdots\times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Corollary

If $x_1^{d_1}\dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1,\dots,d_r)$, then for any $B_1,\dots,B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1\times\cdots\times B_r)| = O\left(n^{r-\frac{1}{(d+1)^{r-1}}}\right).$$

- *Example*: $|Z(x^n + xy + y^n, B_1\times B_2)| = O(n^{3/2})$ for any B_i, $|B_i| = n$

Construction

Key Lemma

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \cdots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Construction

Key Lemma

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \dots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Lemma (G., 2024)

Let $\mathbb{F}_{p^r}$ be the finite field of size p^r, $\mathbb{F}^*_{p^r} = \mathbb{F}_{p^r} \setminus \{0\}$, and

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j},$$

where $x_{r+1} = x_1$ and so on. Then $|Z(f, (\mathbb{F}^*_{p^r})^r| = p^{r-1}(p^r - 1)^{r-1}$.

Construction

Key Lemma

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $H(f, B_1 \times \dots \times B_r)$ is free of copies of $K^{(r)}_{d+1,\dots,d+1}$.

Lemma (G., 2024)

Let $\mathbb{F}_{p^r}$ be the finite field of size p^r, $\mathbb{F}^*_{p^r} = \mathbb{F}_{p^r} \setminus \{0\}$, and

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j},$$

where $x_{r+1} = x_1$ and so on. Then $|Z(f, (\mathbb{F}^*_{p^r})^r| = p^{r-1}(p^r - 1)^{r-1}$.

Theorem (G., 2024)

$$\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r - \frac{1}{r}}\right).$$

Proof of Theorem

Theorem (G., 2024)

$$\mathrm{ex}(n, K^{(r)}_{2,\ldots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right).$$

$$f(x_1, \ldots, x_r) = x_1 \ldots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

Proof of Theorem

Theorem (G., 2024)

$$\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right).$$

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. $x_1 \dots x_r$ is maximal in f, thus $H(f, (\mathbb{F}^*_{p^r})^r)$ is free of copies of $K^{(r)}_{2,\dots,2}$.

Proof of Theorem

Theorem (G., 2024)

$$\mathrm{ex}(n, K_{2,\dots,2}^{(r)}) = \Omega\left(n^{r-\frac{1}{r}}\right).$$

$$f(x_1,\dots,x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. $x_1 \dots x_r$ is maximal in f, thus $H(f, (\mathbb{F}_{p^r}^*)^r)$ is free of copies of $K_{2,\dots,2}^{(r)}$.

◇ Classical Combinatorial Nullstellensatz would be useless here!

Proof of Theorem

Theorem (G., 2024)

$$\mathrm{ex}(n, K_{2,\dots,2}^{(r)}) = \Omega\left(n^{r-\frac{1}{r}}\right).$$

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. $x_1 \dots x_r$ is maximal in f, thus $H(f, (\mathbb{F}_{p^r}^*)^r)$ is free of copies of $K_{2,\dots,2}^{(r)}$.

◇ Classical Combinatorial Nullstellensatz would be useless here!

2. $H(f, (\mathbb{F}_{p^r}^*)^r)$ has $n = r(p^r - 1)$ vertices.

Proof of Theorem

Theorem (G., 2024)

$$\mathrm{ex}(n, K^{(r)}_{2,\dots,2}) = \Omega\left(n^{r-\frac{1}{r}}\right).$$

$$f(x_1,\dots,x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. $x_1 \dots x_r$ is maximal in f, thus $H(f, (\mathbb{F}^*_{p^r})^r)$ is free of copies of $K^{(r)}_{2,\dots,2}$.
   - ◇ Classical Combinatorial Nullstellensatz would be useless here!
2. $H(f, (\mathbb{F}^*_{p^r})^r)$ has $n = r(p^r - 1)$ vertices.
3. $H(f, (\mathbb{F}^*_{p^r})^r)$ has $|Z(f, (\mathbb{F}^*_{p^r})^r| = p^{r-1}(p^r-1)^{r-1} = \Omega\left(n^{r-\frac{1}{r}}\right)$ edges.

Proof of Lemma

$$f(x_1, \ldots, x_r) = x_1 \ldots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. For any $a_1, \ldots, a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$

Proof of Lemma

$$f(x_1,\ldots,x_r) = x_1\ldots x_r + \sum_{i=1}^{r}\prod_{j=1}^{r-1} x_{i+j}^{p^r-p^j}$$

1. For any $a_1,\ldots,a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$, so

$$f(a_1,\ldots,a_r) = a_1\ldots a_r\Big(1 + \sum_{i=1}^{r}\prod_{j=0}^{r-1} a_{i+j}^{-p^j}\Big)$$

Proof of Lemma

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. For any $a_1, \dots, a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$, so

$$\begin{aligned} f(a_1, \dots, a_r) &= a_1 \dots a_r \Big(1 + \sum_{i=1}^{r} \prod_{j=0}^{r-1} a_{i+j}^{-p^j} \Big) \\ &= a_1 \dots a_r \left(1 + \mathrm{Tr}\left(a_1^{-1} a_2^{-p} \dots a_r^{-p^{r-1}} \right) \right), \end{aligned}$$

where $\mathrm{Tr}(a) = a + a^p + \dots + a^{p^{r-1}}$ — trace of the field extension $\mathbb{F}_{p^r}/\mathbb{F}_p$.

Proof of Lemma

$$f(x_1, \ldots, x_r) = x_1 \ldots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. For any $a_1, \ldots, a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$, so

$$\begin{aligned} f(a_1, \ldots, a_r) &= a_1 \ldots a_r \Big(1 + \sum_{i=1}^{r} \prod_{j=0}^{r-1} a_{i+j}^{-p^j} \Big) \\ &= a_1 \ldots a_r \left(1 + \mathrm{Tr} \left(a_1^{-1} a_2^{-p} \ldots a_r^{-p^{r-1}} \right) \right), \end{aligned}$$

   where $\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{r-1}}$ — trace of the field extension $\mathbb{F}_{p^r}/\mathbb{F}_p$.
2. $\mathrm{Tr}(a) = -1$ for exactly p^{r-1} elements $a \in \mathbb{F}_{p^r}^*$.

Proof of Lemma

$$f(x_1, \ldots, x_r) = x_1 \ldots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. For any $a_1, \ldots, a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$, so

$$f(a_1, \ldots, a_r) = a_1 \ldots a_r \Big(1 + \sum_{i=1}^{r} \prod_{j=0}^{r-1} a_{i+j}^{-p^j}\Big)$$
$$= a_1 \ldots a_r \left(1 + \mathrm{Tr}\left(a_1^{-1} a_2^{-p} \ldots a_r^{-p^{r-1}}\right)\right),$$

   where $\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{r-1}}$ — trace of the field extension $\mathbb{F}_{p^r}/\mathbb{F}_p$.
2. $\mathrm{Tr}(a) = -1$ for exactly p^{r-1} elements $a \in \mathbb{F}_{p^r}^*$.
3. Fix $a_2, \ldots, a_r$; there are exactly p^{r-1} values of a_1: $f(a_1, \ldots, a_r) = 0$.

Proof of Lemma

$$f(x_1, \dots, x_r) = x_1 \dots x_r + \sum_{i=1}^{r} \prod_{j=1}^{r-1} x_{i+j}^{p^r - p^j}$$

1. For any $a_1, \dots, a_r \in \mathbb{F}_{p^r}^*$ we have $a_i^{p^r} = a_i$, so

$$\begin{aligned} f(a_1, \dots, a_r) &= a_1 \dots a_r \Big(1 + \sum_{i=1}^{r} \prod_{j=0}^{r-1} a_{i+j}^{-p^j} \Big) \\ &= a_1 \dots a_r \left(1 + \mathrm{Tr}\left(a_1^{-1} a_2^{-p} \dots a_r^{-p^{r-1}} \right) \right), \end{aligned}$$

   where $\mathrm{Tr}(a) = a + a^p + \dots + a^{p^{r-1}}$ — trace of the field extension $\mathbb{F}_{p^r}/\mathbb{F}_p$.
2. $\mathrm{Tr}(a) = -1$ for exactly p^{r-1} elements $a \in \mathbb{F}_{p^r}^*$.
3. Fix $a_2, \dots, a_r$; there are exactly p^{r-1} values of a_1: $f(a_1, \dots, a_r) = 0$.
4. $|Z(f, (\mathbb{F}_{p^r}^*)^r| = p^{r-1}(p^r - 1)^{r-1}$.

Further questions

- Find more constructions using this framework

Further questions

- Find more constructions using this framework
  - Find a way to add randomization to this algebraic method

Further questions

- Find more constructions using this framework
  - Find a way to add randomization to this algebraic method
  - $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$, **Katz–Krop–Maggioni, 2002** seems structurally similar to our construction
  - Can other known constructions be "translated" into this language?

Further questions

- Find more constructions using this framework
  - ◇ Find a way to add randomization to this algebraic method
  - ◇ $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$, **Katz–Krop–Maggioni, 2002** seems structurally similar to our construction
  - ◇ Can other known constructions be "translated" into this language?

Corollary

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1 \times \cdots \times B_r)| = O\left(n^{r - \frac{1}{(d+1)^{r-1}}}\right).$$

Further questions

- Find more constructions using this framework
  - Find a way to add randomization to this algebraic method
  - $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$, **Katz–Krop–Maggioni, 2002** seems structurally similar to our construction
  - Can other known constructions be "translated" into this language?

Corollary

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1 \times \cdots \times B_r)| = O\left(n^{r - \frac{1}{(d+1)^{r-1}}}\right).$$

- When is the bound from the corollary not optimal?
  - It is tight for $f(x, y) = xy + P(x) + Q(y)$, $\mathbb{F} = \mathbb{F}_{p^2}$

Further questions

- Find more constructions using this framework
  - ◇ Find a way to add randomization to this algebraic method
  - ◇ $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$, **Katz–Krop–Maggioni, 2002** seems structurally similar to our construction
  - ◇ Can other known constructions be "translated" into this language?

Corollary

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1 \times \cdots \times B_r)| = O\left(n^{r - \frac{1}{(d+1)^{r-1}}}\right).$$

- When is the bound from the corollary not optimal?
  - ◇ It is tight for $f(x,y) = xy + P(x) + Q(y)$, $\mathbb{F} = \mathbb{F}_{p^2}$
  - ◇ Can the upper bound be improved for a particular $\mathbb{F}$?
  - ◇ **Rote, 2023**: How large can the set $Z(f, B_1 \times B_2)$ be for $f(x,y) = xy + P(x) + Q(y)$, $B_i \subset \mathbb{Z}$, $|B_i| = n$?

Further questions

- Find more constructions using this framework
  - ◇ Find a way to add randomization to this algebraic method
  - ◇ $\mathrm{ex}(n, K^{(3)}_{2,2,2}) = \Omega(n^{8/3})$, **Katz–Krop–Maggioni, 2002** seems structurally similar to our construction
  - ◇ Can other known constructions be "translated" into this language?

Corollary

If $x_1^{d_1} \dots x_r^{d_r}$ is a maximal monomial of f, $d = \max(d_1, \dots, d_r)$, then for any $B_1, \dots, B_r \subset \mathbb{F}$, $|B_i| = n$,

$$|Z(f, B_1 \times \cdots \times B_r)| = O\left(n^{r - \frac{1}{(d+1)^{r-1}}}\right).$$

- When is the bound from the corollary not optimal?
  - ◇ It is tight for $f(x, y) = xy + P(x) + Q(y)$, $\mathbb{F} = \mathbb{F}_{p^2}$
  - ◇ Can the upper bound be improved for a particular $\mathbb{F}$?
  - ◇ **Rote, 2023**: How large can the set $Z(f, B_1 \times B_2)$ be for $f(x, y) = xy + P(x) + Q(y)$, $B_i \subset \mathbb{Z}$, $|B_i| = n$?
- Find more applications of Lasoń's Combinatorial Nullstellensatz