Combinatorial aspects of matrix multiplication

Kevin Pratt

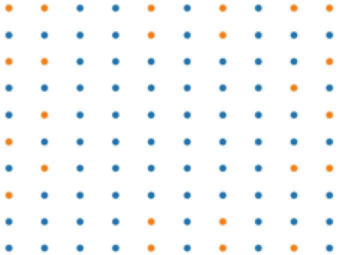
Courant Institute, NYU

Teaser problem

- *What is the size of the largest subset of $[n] \times [n]$ containing no three points of the form $(x, y), (x, y + d), (x + d, z)$, with $d \neq 0$?*

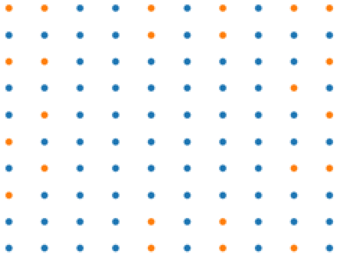
Teaser problem

- *What is the size of the largest subset of* $[n] \times [n]$ *containing no three points of the form* $(x, y), (x, y + d), (x + d, z)$, *with* $d \neq 0$?



Teaser problem

- *What is the size of the largest subset of $[n] \times [n]$ containing no three points of the form $(x, y), (x, y + d), (x + d, z)$, with $d \neq 0$?*



- **What does this have to do with algorithms for matrix multiplication?**

A billion dollar question

- [Str69]: $n \times n$ matrices can be multiplied using $O(n^{2.81})$ arithmetic operations

A billion dollar question

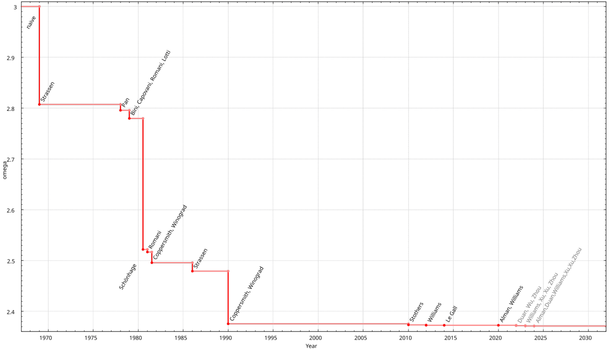
- [Str69]: $n \times n$ matrices can be multiplied using $O(n^{2.81})$ arithmetic operations
- **Can this be improved to $O(n^2)$?**

A billion dollar question

- [Str69]: $n \times n$ matrices can be multiplied using $O(n^{2.81})$ arithmetic operations
- **Can this be improved to $O(n^2)$?**
- $\omega := \inf\{\tau \in \mathbb{R} \mid n \times n$ matrices can be multiplied using $O(n^\tau)$ ops. in $\mathbb{F}\}$

A billion dollar question

- [Str69]: $n \times n$ matrices can be multiplied using $O(n^{2.81})$ arithmetic operations
- **Can this be improved to $O(n^2)$?**
- $\omega := \inf\{\tau \in \mathbb{R} \mid n \times n$ matrices can be multiplied using $O(n^\tau)$ ops. in $\mathbb{F}\}$



A billion dollar question

- [Str69]: $n \times n$ matrices can be multiplied using $O(n^{2.81})$ arithmetic operations
- **Can this be improved to $O(n^2)$?**
- $\omega := \inf\{\tau \in \mathbb{R} \mid n \times n$ matrices can be multiplied using $O(n^{\tau})$ ops. in $\mathbb{F}\}$
- $\omega < 2.372$ [ADW+24]

Overview

- The *group theoretic approach* of [CU03, CKSU05]

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers
- Intermediate questions towards $\omega = 2$ [Pra24]

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers
- Intermediate questions towards $\omega = 2$ [Pra24]
  - Trapezoid-free sets; skew-corner free sets

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers
- Intermediate questions towards $\omega = 2$ [Pra24]
  - Trapezoid-free sets; skew-corner free sets
  - Reasons to be optimistic?

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers
- Intermediate questions towards $\omega = 2$ [Pra24]
  - Trapezoid-free sets; skew-corner free sets
  - Reasons to be optimistic?
- Further questions

Overview

- The *group theoretic approach* of [CU03, CKSU05]
  - Summary of what's known; some nontrivial bounds
  - Potential approaches to $\omega = 2$; barriers
- Intermediate questions towards $\omega = 2$ [Pra24]
  - Trapezoid-free sets; skew-corner free sets
  - Reasons to be optimistic?
- Further questions

We know very little about the limits of current approaches!

A group-theoretic approach [CU03]

- Let G be a finite group

A group-theoretic approach [CU03]

- Let G be a finite group
- Say $X, Y, Z \subseteq G$ satisfy the *triple product property* (TPP) if

$$xx'^{-1}yy'^{-1}zz'^{-1} = 1_G \iff x = x', y = y', z = z'$$

A group-theoretic approach [CU03]

- Let G be a finite group
- Say $X, Y, Z \subseteq G$ satisfy the *triple product property* (TPP) if

$$xx'^{-1}yy'^{-1}zz'^{-1} = 1_G \iff x = x', y = y', z = z'$$

- Given $A \in \mathbb{F}^{|X|\times|Y|}$, $B \in \mathbb{F}^{|Y|\times|Z|}$, compute

$$\left(\sum A_{x,y}xy^{-1}\right)\left(\sum B_{y,z}yz^{-1}\right) \in \mathbb{F}[G]$$

A group-theoretic approach [CU03]

- Let G be a finite group
- Say $X, Y, Z \subseteq G$ satisfy the *triple product property* (TPP) if

$$xx'^{-1}yy'^{-1}zz'^{-1} = 1_G \iff x = x', y = y', z = z'$$

- Given $A \in \mathbb{F}^{|X| \times |Y|}, B \in \mathbb{F}^{|Y| \times |Z|}$, compute

$$\left(\sum A_{x,y} xy^{-1}\right)\left(\sum B_{y,z} yz^{-1}\right) \in \mathbb{F}[G]$$

- Coefficient of xz^{-1} = (row x of A) $\cdot$ (column z of B)

A group-theoretic approach [CU03]

- Let G be a finite group
- Say $X, Y, Z \subseteq G$ satisfy the *triple product property* (TPP) if

$$xx'^{-1}yy'^{-1}zz'^{-1} = 1_G \iff x = x', y = y', z = z'$$

- Given $A \in \mathbb{F}^{|X|\times|Y|}$, $B \in \mathbb{F}^{|Y|\times|Z|}$, compute

$$(\sum A_{x,y}xy^{-1})(\sum B_{y,z}yz^{-1}) \in \mathbb{F}[G]$$

- Coefficient of xz^{-1} = (row x of A) $\cdot$ (column z of B)

A group-theoretic approach [CU03]

- Let G be a finite group
- Say $X, Y, Z \subseteq G$ satisfy the *triple product property* (TPP) if

$$xx'^{-1}yy'^{-1}zz'^{-1} = 1_G \iff x = x', y = y', z = z'$$

- Given $A \in \mathbb{F}^{|X| \times |Y|}$, $B \in \mathbb{F}^{|Y| \times |Z|}$, compute

$$\left(\sum A_{x,y} xy^{-1}\right)\left(\sum B_{y,z} yz^{-1}\right) \in \mathbb{F}[G]$$

- Coefficient of xz^{-1} = (row x of A) $\cdot$ (column z of B)

Theorem

Suppose X, Y, Z satisfy the TPP. Then $(|X||Y||Z|)^{\omega/3} \leq \sum d_i^{\omega}$, where d_i are the dimensions of the irreducible representations of G.

A trivial bound

- For G abelian and $|X| = |Y| = |Z| = n$, this simplifies to $\omega \leq \log_n |G|$

A trivial bound

- For G abelian and $|X| = |Y| = |Z| = n$, this simplifies to $\omega \leq \log_n |G|$
- Intuition: reducing $n \times n$ matrix mult. to convolution in G, which takes $\approx |G| = n^{\log_n |G|}$-time

A trivial bound

- For G abelian and $|X| = |Y| = |Z| = n$, this simplifies to $\omega \leq \log_n |G|$
- Intuition: reducing $n \times n$ matrix mult. to convolution in G, which takes $\approx |G| = n^{\log_n |G|}$-time

A trivial bound

- For G abelian and $|X| = |Y| = |Z| = n$, this simplifies to $\omega \leq \log_n |G|$
- Intuition: reducing $n \times n$ matrix mult. to convolution in G, which takes $\approx |G| = n^{\log_n |G|}$-time

Example

Let $G = \mathbb{Z}_m^3$.

$$X = (\mathbb{Z}_m, 0, 0), Y = (0, \mathbb{Z}_m, 0), Z = (0, 0, \mathbb{Z}_m)$$

These satisfy the TPP, so $\omega \leq 3$.

A trivial bound

- For G abelian and $|X| = |Y| = |Z| = n$, this simplifies to $\omega \leq \log_n |G|$
- Intuition: reducing $n \times n$ matrix mult. to convolution in G, which takes $\approx |G| = n^{\log_n |G|}$-time

Example

Let $G = \mathbb{Z}_m^3$.

$$X = (\mathbb{Z}_m, 0, 0), Y = (0, \mathbb{Z}_m, 0), Z = (0, 0, \mathbb{Z}_m)$$

These satisfy the TPP, so $\omega \leq 3$.

- Optimal for abelian groups: addition map $(x, y, z) \to x + y + z$ injective, so $|G| \geq n^3$

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP
  - $(x_i - y_i') + (y_j - z_j') + (z_k - x_k') = 0 \iff i = j = k$

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP
  - $(x_i - y_i') + (y_j - z_j') + (z_k - x_k') = 0 \iff i = j = k$
- Embedding *independent* instances of matrix mult into $\mathbb{F}[G]$

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP
  - $(x_i - y_i') + (y_j - z_j') + (z_k - x_k') = 0 \iff i = j = k$
- Embedding *independent* instances of matrix mult into $\mathbb{F}[G]$

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP
  - $(x_i - y_i') + (y_j - z_j') + (z_k - x_k') = 0 \iff i = j = k$
- Embedding *independent* instances of matrix mult into $\mathbb{F}[G]$

Theorem

Suppose $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ *satisfy the STPP. Then* $\sum_{i=1}^r (|X_i||Y_i||Z_i|)^{\omega/3} \leq |G|$.

The simultaneous triple product property

- Best bounds on ω: *simultaneous triple product property* (STPP) in abelian groups
- Families $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ satisfy STPP if
  - For all i, X_i, Y_i, Z_i satisfy the TPP
  - $(x_i - y_i') + (y_j - z_j') + (z_k - x_k') = 0 \iff i = j = k$
- Embedding *independent* instances of matrix mult into $\mathbb{F}[G]$

Theorem

Suppose $(X_i)_{i=1}^r, (Y_i)_{i=1}^r, (Z_i)_{i=1}^r$ *satisfy the STPP. Then* $\sum_{i=1}^r (|X_i||Y_i||Z_i|)^{\omega/3} \leq |G|$.

- Intuition: if we can perform r independent instances of $n \times n$ matrix mult in time $|G|$, expect to perform 1 instance in time $|G|/r$

A nontrivial bound on ω

- In $\mathbb{Z}_m^3$, let

$$\begin{aligned} X_1 &= (*, 0, 0) & Y_1 &= (0, *, 0) & Z_1 &= (0, 0, *) \\ X_2 &= (0, *, 0) & Y_2 &= (0, 0, *) & Z_2 &= (*, 0, 0) \end{aligned}$$

where $*$ denotes a nonzero element of $\mathbb{Z}_m$

A nontrivial bound on ω

- In $\mathbb{Z}_m^3$, let

$$\begin{aligned} X_1 &= (*,0,0) & Y_1 &= (0,*,0) & Z_1 &= (0,0,*) \\ X_2 &= (0,*,0) & Y_2 &= (0,0,*) & Z_2 &= (*,0,0) \end{aligned}$$

  where $*$ denotes a nonzero element of $\mathbb{Z}_m$
- These satisfy the STPP:

$$\begin{aligned} X_1 - Y_1 &= (*,*,0) & Y_1 - Z_1 &= (0,*,*) & Z_1 - X_1 &= (*,0,*) \\ X_2 - Y_2 &= (0,*,*) & Y_2 - Z_2 &= (*,0,*) & Z_2 - X_2 &= (*,*,0) \end{aligned}$$

A nontrivial bound on ω

- In $\mathbb{Z}_m^3$, let

$$\begin{array}{lll} X_1 = (*,0,0) & Y_1 = (0,*,0) & Z_1 = (0,0,*) \\ X_2 = (0,*,0) & Y_2 = (0,0,*) & Z_2 = (*,0,0) \end{array}$$

  where $*$ denotes a nonzero element of $\mathbb{Z}_m$
- These satisfy the STPP:

$$\begin{array}{lll} X_1 - Y_1 = (*,*,0) & Y_1 - Z_1 = (0,*,*) & Z_1 - X_1 = (*,0,*) \\ X_2 - Y_2 = (0,*,*) & Y_2 - Z_2 = (*,0,*) & Z_2 - X_2 = (*,*,0) \end{array}$$

- Hence $\omega \leq \log_{m-1} m^3/2$. For $m = 16$, this gives $\omega \leq 2.816$

The simultaneous double product property [CKSU05]

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

- Open: can this yield $\omega = 2$? [Gre]

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

- Open: can this yield $\omega = 2$? [Gre]

The simultaneous double product property [CKSU05]

Definition

Set families $(A_i)_{i=1}^r, (B_i)_{i=1}^r$ satisfy the *simultaneous double product property* (SDPP) if:

- $|A_i + B_i| = |A_i||B_i|$ for all i
- $a_i + b_j \neq a_k + b_k$ whenever $i \neq j$

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

- Open: can this yield $\omega = 2$? [Gre]

Conjecture

For arbitrarily large n, there exists an abelian group G of order $n^{2+o(1)}$, and n pairs of subsets A_i, B_i with $|A_i||B_i| \geq n^{2-o(1)}$ satisfying the SDPP.

The best SDPP construction known

The best SDPP construction known

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

The best SDPP construction known

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

The best SDPP construction known

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

Example (The virus)

Let $G = \mathbb{Z}_m^{2\ell}$. For $S \subset [2\ell], |S| = \ell$, define

$$A_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i = 0 \text{ for } i \in S, x_i \neq 0 \text{ else}\}$$

$$B_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i \neq 0 \text{ for } i \in S, x_i = 0 \text{ else}\}$$

The best SDPP construction known

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

Example (The virus)

Let $G = \mathbb{Z}_m^{2\ell}$. For $S \subset [2\ell], |S| = \ell$, define

$$A_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i = 0 \text{ for } i \in S, x_i \neq 0 \text{ else}\}$$

$$B_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i \neq 0 \text{ for } i \in S, x_i = 0 \text{ else}\}$$

- $\binom{2\ell}{\ell} \cdot (m-1)^{\omega\ell} \leq m^{3\ell}$, so $\omega \leq \log_{m-1}(m^{3\ell}/\binom{2\ell}{\ell})/\ell$

The best SDPP construction known

Theorem

Suppose A_i, B_i satisfy the SDPP. Then $\sum(|A_i||B_i|)^{\omega/2} \leq |G|^{3/2}$.

Example (The virus)

Let $G = \mathbb{Z}_m^{2\ell}$. For $S \subset [2\ell], |S| = \ell$, define

$$A_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i = 0 \text{ for } i \in S, x_i \neq 0 \text{ else}\}$$

$$B_S = \{x \in \mathbb{Z}_m^{2\ell} : x_i \neq 0 \text{ for } i \in S, x_i = 0 \text{ else}\}$$

- $\binom{2\ell}{\ell} \cdot (m-1)^{\omega\ell} \leq m^{3\ell}$, so $\omega \leq \log_{m-1}(m^{3\ell}/\binom{2\ell}{\ell})/\ell$
- Taking $m = 6, \ell \to \infty$, this gives $\omega < 2.48$

Barriers

- Current algorithms: STPP's in $\mathbb{Z}_m^n$ with small m and growing n

Barriers

- Current algorithms: STPP's in $\mathbb{Z}_m^n$ with small m and growing n

Barriers

- Current algorithms: STPP's in $\mathbb{Z}_m^n$ with small m and growing n

Theorem ([BCC$^+$17])

For every m, there exists $c_m > 0$ such that no STPP in $\mathbb{Z}_m^n$ can yield a bound of $\omega \leq 2 + c_m$.

Barriers

- Current algorithms: STPP's in $\mathbb{Z}_m^n$ with small m and growing n

Theorem ([BCC+17])

For every m, there exists $c_m > 0$ such that no STPP in $\mathbb{Z}_m^n$ can yield a bound of $\omega \leq 2 + c_m$.

- $c_m \to 0$ as $m \to \infty$, so this says nothing for e.g. cyclic groups

Barriers

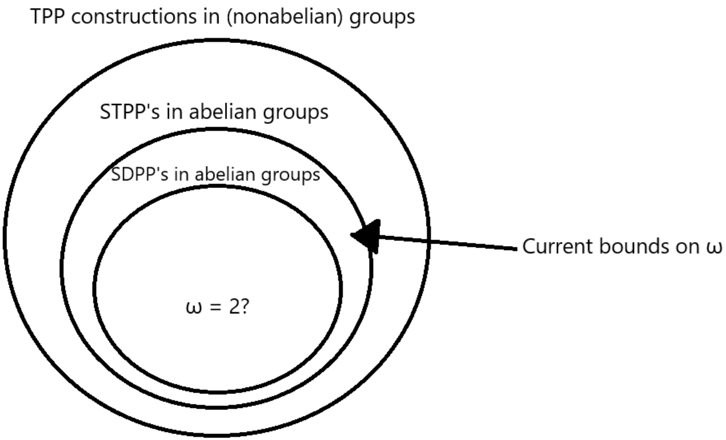
- Current algorithms: STPP's in $\mathbb{Z}_m^n$ with small m and growing n

Theorem ([BCC+17])

For every m, there exists $c_m > 0$ such that no STPP in $\mathbb{Z}_m^n$ can yield a bound of $\omega \leq 2 + c_m$.

- $c_m \to 0$ as $m \to \infty$, so this says nothing for e.g. cyclic groups
- **Can we rule out STPP's in arbitrary abelian groups, and in particular, cyclic groups?**

Summary


TPP constructions in (nonabelian) groups
STPP's in abelian groups
SDPP's in abelian groups
ω = 2?
Current bounds on ω

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$
- Let X_G be "group addition" hypergraph

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$
- Let X_G be "group addition" hypergraph
  - Vertex set $G \sqcup G \sqcup G$

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$
- Let X_G be "group addition" hypergraph
  - Vertex set $G \sqcup G \sqcup G$
  - Edges $(x,y,z), x+y+z=0$

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$
- Let X_G be "group addition" hypergraph
  - Vertex set $G \sqcup G \sqcup G$
  - Edges $(x,y,z), x+y+z=0$
- TPP: induced copy of M_n inside of X_G

A hypergraph view of STPPs

- Let M_n be "matrix multiplication" hypergraph
  - Vertex set $[n]^2 \sqcup [n]^2 \sqcup [n]^2$
  - Edges $((i,j),(j,k),(k,i))$
- Let X_G be "group addition" hypergraph
  - Vertex set $G \sqcup G \sqcup G$
  - Edges $(x,y,z), x+y+z=0$
- TPP: induced copy of M_n inside of X_G
- STPP: induced disjoint union of M_n's in X_G

M_n and trapezoids

M_n and trapezoids

Definition

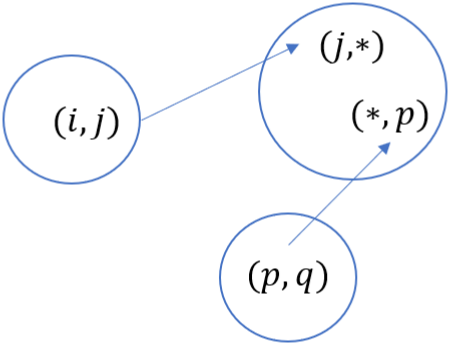
Call a hypergraph *trapezoid-free* if any two vertices in different parts have at most one common neighbor in the third part.

M_n and trapezoids

Definition

Call a hypergraph *trapezoid-free* if any two vertices in different parts have at most one common neighbor in the third part.

- M_n is trapezoid-free



M_n and trapezoids

Definition

Call a hypergraph *trapezoid-free* if any two vertices in different parts have at most one common neighbor in the third part.

- M_n is trapezoid-free

M_n and trapezoids

Definition

Call a hypergraph *trapezoid-free* if any two vertices in different parts have at most one common neighbor in the third part.

- M_n is trapezoid-free

Definition

Given a hypergraph X, let $Val(X)$ be the maximum number of hyperedges in any induced trapezoid-free subhypergraph of X.

M_n and trapezoids

Definition

Call a hypergraph *trapezoid-free* if any two vertices in different parts have at most one common neighbor in the third part.

- M_n is trapezoid-free

Definition

Given a hypergraph X, let $Val(X)$ be the maximum number of hyperedges in any induced trapezoid-free subhypergraph of X.

- $Val(M_n) = n^3$ (maximum possible!)

Why "trapezoids"?

- Let $Val(n) := Val(X_{\mathbb{Z}_n})$

Why "trapezoids"?

- Let $Val(n) := Val(X_{\mathbb{Z}_n})$
- Hypergraph induced by $X, Y, Z \subseteq \mathbb{Z}_n$ is trapezoid-free: any $x' \in X, y' \in Y$, there is at most one solution to

$$x' + y + z = 0$$
$$x + y' + z = 0$$

with $x \in X, y \in Y, z \in Z$ (and symmetrically)

Why "trapezoids"?

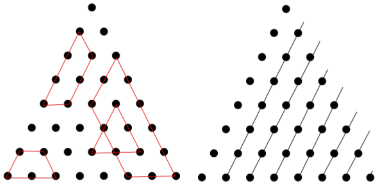
- Let $Val(n) := Val(X_{\mathbb{Z}_n})$
- Hypergraph induced by $X, Y, Z \subseteq \mathbb{Z}_n$ is trapezoid-free: any $x' \in X, y' \in Y$, there is at most one solution to

$$x' + y + z = 0$$
$$x + y' + z = 0$$

  with $x \in X, y \in Y, z \in Z$ (and symmetrically)
- Number of hyperedges = number of solutions to $x + y + z = 0$

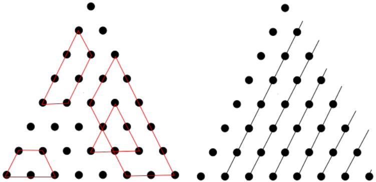
Why “trapezoids”?

- Pictorially: let $\Delta_n := \{(x,y,z) \in [n] : x+y+z=n\}$



Why "trapezoids"?

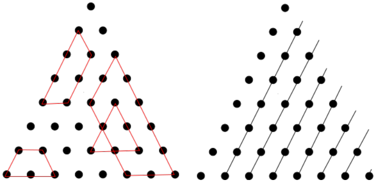
- Pictorially: let $\Delta_n := \{(x,y,z) \in [n] : x+y+z=n\}$



- Delete lines parallel parallel to sides to eliminate all vertices of equilateral trapezoids

Why "trapezoids"?

- Pictorially: let $\Delta_n := \{(x,y,z) \in [n] : x+y+z=n\}$



- Delete lines parallel parallel to sides to eliminate all vertices of equilateral trapezoids
- $Val(n)$: maximum number of points that can remain

Trapezoids

Trapezoids

Theorem ([Pra24])

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where q is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$, *where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Conjecture

$Val(n) < n^{1+o(1)}$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$*.*
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$*.*

Conjecture

$Val(n) < n^{1+o(1)}$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Conjecture

$Val(n) < n^{1+o(1)}$.

Proof idea.

Prior barriers reduce this to understanding if STPPs in $\mathbb{Z}_n$ can yield $\omega = 2$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Conjecture

$Val(n) < n^{1+o(1)}$.

Proof idea.

Prior barriers reduce this to understanding if STPPs in $\mathbb{Z}_n$ can yield $\omega = 2$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield* $\omega = 2$ *using the family of groups* $\mathbb{Z}_q^n$*, where* q *is a prime power, then* $Val(n) \geq n^{1+c}$ *for some absolute* $c > 0$.
- *If [CKSU05, Conjecture 4.7] is true, then* $Val(n) \geq n^{4/3-o(1)}$.

Conjecture

$Val(n) < n^{1+o(1)}$.

Proof idea.

Prior barriers reduce this to understanding if STPPs in $\mathbb{Z}_n$ can yield $\omega = 2$.

If $X \geq Y \implies Val(X) \geq Val(Y)$.

Trapezoids

Theorem ([Pra24])

- *If STPP constructions yield $\omega = 2$ using the family of groups $\mathbb{Z}_q^n$, where q is a prime power, then $Val(n) \geq n^{1+c}$ for some absolute $c > 0$.*
- *If [CKSU05, Conjecture 4.7] is true, then $Val(n) \geq n^{4/3-o(1)}$.*

Conjecture

$Val(n) < n^{1+o(1)}$.

Proof idea.

Prior barriers reduce this to understanding if STPPs in $\mathbb{Z}_n$ can yield $\omega = 2$.
If $X \geq Y \implies Val(X) \geq Val(Y)$. So, $X_{\mathbb{Z}_n} \geq \sqcup_{i=1}^{k} M_N \implies Val(n) \geq kN^3$. □

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free
- The projection of $(x, y, z) \in X \times Y \times Z : x + y + z = 0$ onto (x, y) coordinates contains no skew corners: $(x, y), (x, y + z), (x + z, w)$:

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free
- The projection of $(x, y, z) \in X \times Y \times Z : x + y + z = 0$ onto (x, y) coordinates contains no skew corners: $(x, y), (x, y + z), (x + z, w)$:

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free
- The projection of $(x, y, z) \in X \times Y \times Z : x + y + z = 0$ onto (x, y) coordinates contains no skew corners: $(x, y), (x, y + z), (x + z, w)$:

Conjecture

If $S \subseteq [n]^2$ is skew corner-free, then $|S| \leq n^{1+o(1)}$.

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free
- The projection of $(x, y, z) \in X \times Y \times Z : x + y + z = 0$ onto (x, y) coordinates contains no skew corners: $(x, y), (x, y + z), (x + z, w)$:

Conjecture

If $S \subseteq [n]^2$ is skew corner-free, then $|S| \leq n^{1+o(1)}$.

- Traditional corners: $(x, y), (x, y + d), (x + d, y)$

A relaxation: skew corner-free sets

- Let $X, Y, Z \subseteq \mathbb{Z}_n$ be trapezoid-free
- The projection of $(x, y, z) \in X \times Y \times Z : x + y + z = 0$ onto (x, y) coordinates contains no skew corners: $(x, y), (x, y + z), (x + z, w)$:

Conjecture

If $S \subseteq [n]^2$ is skew corner-free, then $|S| \leq n^{1+o(1)}$.

- Traditional corners: $(x, y), (x, y + d), (x + d, y)$
- Exist corner-free subsets of $[n]^2$ as big as $n^{2-o(1)}$ [AS74]

Large skew-corner free sets exist!

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ of size $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x, y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x, y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x,y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

If $(x,y), (x,y+z) \in A_{r,t}$, then $x \cdot z = 0$.

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x, y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

If $(x, y), (x, y + z) \in A_{r,t}$, then $x \cdot z = 0$. So there can be no point $(w, x + z) \notin A_{r,t}$ as $||y + x||^2 > r$. Hence $A_{r,t}$ contains no skew corners.

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ *of size* $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x, y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

If $(x, y), (x, y + z) \in A_{r,t}$, then $x \cdot z = 0$. So there can be no point $(w, x + z) \notin A_{r,t}$ as $||y + x||^2 > r$. Hence $A_{r,t}$ contains no skew corners.
By pigeonhole, can choose r, t so that $|A_{r,t}| \geq m^{2d} / (dm^2)^2$.

Large skew-corner free sets exist!

Theorem ([Bek24])

There exist skew corner-free subset of $[n]^2$ of size $n^{2-o(1)}$.

Proof sketch.

Let $B = [m]^d$. Consider the set

$$A_{r,t} = \{(x, y) \in B^2 : ||x||^2 = ||y||^2 = r, x \cdot y = t\}.$$

If $(x, y), (x, y + z) \in A_{r,t}$, then $x \cdot z = 0$. So there can be no point $(w, x + z) \notin A_{r,t}$ as $||y + x||^2 > r$. Hence $A_{r,t}$ contains no skew corners.
By pigeonhole, can choose r, t so that $|A_{r,t}| \geq m^{2d} / (dm^2)^2$.
Embed into $[(2m)^d]$ via base $2m$ expansion. □

Conclusion

- Know that $n \leq Val(n) < o(n^{3/2})$. Is $Val(n) = n^{3/2-o(1)}$?

Conclusion

- Know that $n \leq Val(n) < o(n^{3/2})$. Is $Val(n) = n^{3/2-o(1)}$?
  - Would this imply that $\omega = 2$?

Conclusion

- Know that $n \leq Val(n) < o(n^{3/2})$. Is $Val(n) = n^{3/2-o(1)}$?
  - Would this imply that $\omega = 2$?
- Is “the virus” the best SDPP construction? Nikodym sets?

Thank you!

Thank you!

Questions?

References I

- Josh Alman, Ran Duan, Virginia Vassilevska Williams, Yinzhan Xu, Zixuan Xu, and Renfei Zhou, *More asymmetry yields faster matrix multiplication*, arXiv preprint arXiv:2404.16349 (2024).
- Miklós Ajtai and Endre Szemerédi, *Sets of lattice points that form no squares*, Stud. Sci. Math. Hungar **9** (1974), no. 1975, 9–11.
- Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans, *On cap sets and the group-theoretic approach to matrix multiplication*, Discrete Anal. (2017), Paper No. 3, 1–27.
- Adrian Beker, *Improved bounds for skew corner-free sets*, arXiv preprint arXiv:2402.19169 (2024).

References II

- Henry Cohn, Robert Kleinberg, Balázs Szegedy, and Christopher Umans, *Group-theoretic algorithms for matrix multiplication*, Proceedings of the 46th Annual Symposium on Foundations of Computer Science (FOCS 2005), IEEE Computer Society, 2005, pp. 379–388.
- Henry Cohn and Christopher Umans, *A group-theoretic approach to fast matrix multiplication*, Proceedings of the 44th Annual Symposium on Foundations of Computer Science (FOCS 2003), IEEE Computer Society, 2003, pp. 438–449.
- Ben Green, *100 open problems*, Available at `https://people.maths.ox.ac.uk/greenbj/papers/open-problems.pdf`.

References III

- Kevin Pratt, *On generalized corners and matrix multiplication*, 15th Innovations in Theoretical Computer Science Conference (ITCS 2024), Schloss-Dagstuhl-Leibniz Zentrum für Informatik, 2024.
- Volker Strassen, *Gaussian elimination is not optimal*, Numerische mathematik **13** (1969), no. 4, 354–356.