

# Matrix multiplication algorithms from infinite groups

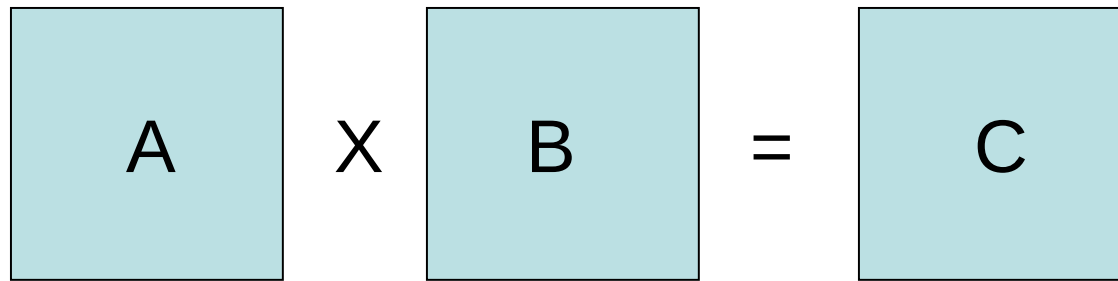
**Chris Umans**

Caltech

Joint work with: Jonah Blasiak, Henry Cohn, Josh Grochow, Kevin Pratt

WACT 2025

# Group theory approach [CU03]


$$\boxed{A} \times \boxed{B} = \boxed{C}$$

Idea: reduce **matrix multiplication** to **group algebra multiplication**

- group algebra:  $\mathbb{C}[G]$  has elements  $\sum_g a_g g$
- $\mathbb{C}[G] \simeq (\mathbb{C}^{d_1 \times d_1}) \times (\mathbb{C}^{d_2 \times d_2}) \times \dots \times (\mathbb{C}^{d_k \times d_k})$

# The basic idea

Find a group  $G$  that permits an embedding

matrix  $A \rightarrow \underline{A} \in C[G]$ , matrix  $B \rightarrow \underline{B} \in C[G]$

so that can read off entries of  $AB$  from  $\underline{A} \cdot \underline{B}$

# Reduction via 3 subgroups:

Subgroups  $X, Y, Z$  of  $G$  satisfy the  
**triple product property (TPP)**

if for all  $x \in X, y \in Y, z \in Z$ :

$$xyz = 1 \quad \text{iff} \quad x = y = z = 1.$$

$$\underline{A} = \sum_{x,y} A[x,y](xy^{-1})$$

$$\underline{B} = \sum_{y,z} B[y,z](yz^{-1})$$

When does

$$(x'y^{-1})(y'z'^{-1}) = xz^{-1} ?$$

$$(AB)[x,z] = \text{coefficient on } xz^{-1} \text{ in } \underline{A} \cdot \underline{B}$$

# Irrep dimensions govern bound

- if  $|X|=|Y|=|Z|=k$ , this is *reduction* from  $k \times k$  mat. mult. to *block-diagonal mat. mult.*

**Theorem:** in finite group  $G$  with irrep dimensions  $d_1, d_2, d_3, \dots$ , we obtain:

$$k^\omega \leq \sum_i d_i^\omega$$

need  $k > d_{\max}$   
want  $k \approx |G|^{1/2}$

- Usually use:  $k^\omega \leq d_{\max}^{\omega-2} \cdot |G|$

If  $d_{\max} \approx |G|^{1/2}$ , prove nothing until prove  $\omega = 2$ .

# Example TPP

- In  $G = \text{SL}_2(F_p)$ :

$$X = \left\{ \begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} : x \in F_p \right\} \quad Y = \left\{ \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} : y \in F_p \right\}$$

$$Z = \left\{ \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} : z \in F_p \right\}$$

$$\begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

# Example TPP

- In  $G = \text{SL}_2(F_p)$ :

$$X = \left\{ \begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} : x \in F_p \right\} \quad Y = \left\{ \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} : y \in F_p \right\}$$

$$Z = \left\{ \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} : z \in F_p \right\}$$

$$\begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

# Example TPP

- In  $G = \text{SL}_2(F_p)$ :

$$X = \left\{ \begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} : x \in F_p \right\} \quad Y = \left\{ \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} : y \in F_p \right\}$$

$$Z = \left\{ \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} : z \in F_p \right\}$$

$$\begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$



# Example TPP

- In  $G = \text{SL}_2(F_p)$ :

$$X = \left\{ \begin{bmatrix} 1 & \\ x & 1 \end{bmatrix} : x \in F_p \right\} \quad Y = \left\{ \begin{bmatrix} 1+y & y \\ -y & 1-y \end{bmatrix} : y \in F_p \right\}$$

$$Z = \left\{ \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} : z \in F_p \right\}$$

$$\begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}$$

Nontrivial:  $|G| = p^3 - p$ ;  $|X| = |Y| = |Z| = p$

# Which groups can prove $\omega = 2$ ?

- no abelian group
- no group  $G$  with  $|G|^\epsilon$ -size **abelian normal subgroup** with bounded exponent [BCCGNSU 2017]
- no group  $G$  with  $|G|^\epsilon$ -size **normal p-subgroup** with mild extra conditions [BCCGU 2017]
- simple groups:
  - no 3 Young subgroups in alt. group [BCCGU 2017]
  - **no matrix group (finite of Lie Type)** [BCGPU 2023]

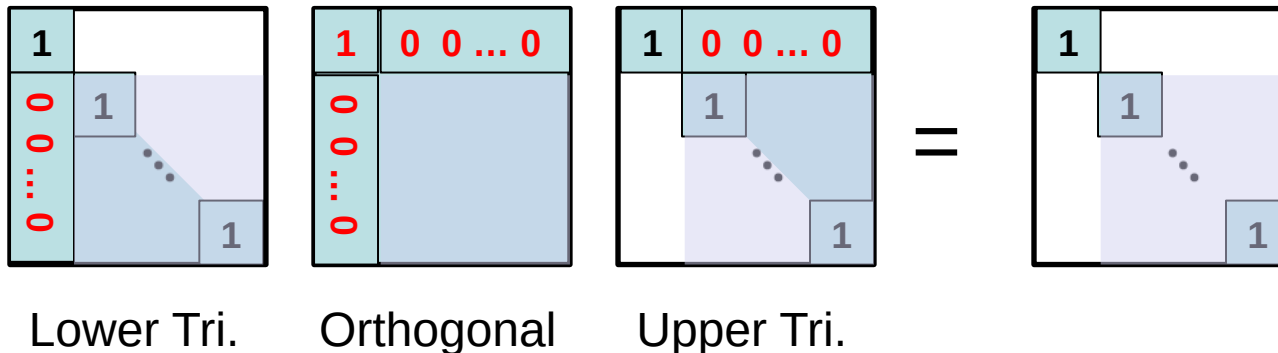
# Analog in infinite matrix groups

- e.g.  $GL(n, F)$ ,  $SL(n, F)$ ,  $O(n, F)$ 
  - $F = \mathbf{C}$  or  $\mathbf{R}$
  - also unitary, symplectic...
- These groups, and nice subgroups of them, have a notion of dimension:
  - e.g.  $\dim$  of  $GL_n$  is  $n^2$ ,  $\dim$  of subgroup of lower-unitriangular matrices is  $(n^2 - n)/2$

Analog TPP goal: subgroups of **sqrt size**  
 $\Leftrightarrow$  subgroups of **half dimension**

# Example construction

- Three subgroups in  $GL(n, \mathbf{R})$ :
  - lower uni-triangular, orthogonal, upper uni-tri.



“sum of squares = 0  $\Rightarrow$  each summand = 0”  
is powerful and enables good constructions

# Finite algorithms from from infinite group TPP constructions

# Original framework: computing $AB$

- Given  $X, Y, Z$  in **finite  $G$** , satisfying TPP:
  - for each irrep  $\rho: G \rightarrow \mathbb{C}^{d \times d}$  compute:

$$\begin{aligned} \rho \left( \sum_{x,y} A[x,y] (xy^{-1}) \right) \cdot \rho \left( \sum_{y',z} B[y',z] (y'z^{-1}) \right) \\ = \sum_{x,y,y',z} A[x,y] B[y',z] \rho(xy^{-1}y'z^{-1}) \end{aligned}$$

- the  $\rho_{i,j}: G \rightarrow \mathbb{C}$  form a basis for *all*  $f: G \rightarrow \mathbb{C}$ .
- “read off  $AB[x,z]$ ” means take the linear combination for fn.  $f$  that is 1 only on  $xz^{-1}$

# New framework for infinite grps

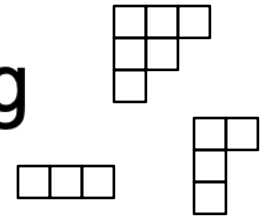
- Given **finite** subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$  in **infinite group**  $\mathbf{G}$ , satisfying TPP:
  - for **some irreps**  $\rho: \mathbf{G} \rightarrow \mathbb{C}^{d \times d}$  compute

$$\begin{aligned} & \rho \left( \sum_{x,y} A[x,y] (xy^{-1}) \right) \cdot \rho \left( \sum_{y',z} B[y',z] (y'z^{-1}) \right) \\ &= \sum_{x,y,y',z} A[x,y] B[y',z] \rho(\underbrace{xy^{-1}y'z^{-1}}_M) \end{aligned}$$

- “read off  $AB[x,z]$ ” means: find lin. combo of  $\rho_{i,j}$  equal to  $f_{x,z}(M) = 1$  if  $M = xz^{-1}$   
 $= 0$  if  $M = \text{any other } xy^{-1}y'z^{-1}$

# Separating polynomials

- Irreps of  $GL(n, \mathbf{R})$  indexed by Young diagrams.



- the  $\rho_{i,j}$  for irreps up to size  $D$  span exactly the set of total-degree  $D$  polynomials
- **cut off at size  $D$** ; now to “read off  $AB[x,z]$ ”:
- find “**separating polynomial of deg  $D$** ”:

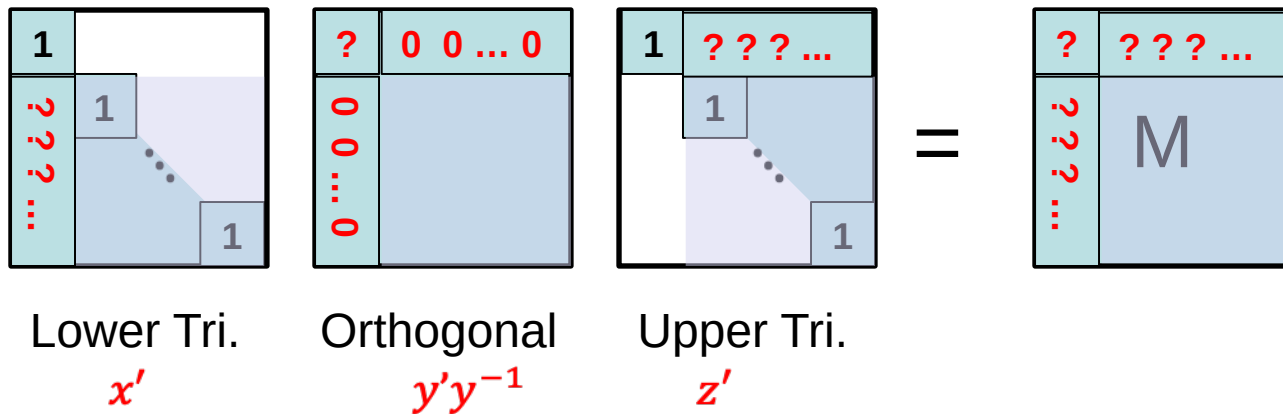
$$f_{x,z}(M) = 1 \text{ if } M = xz^{-1}$$

$$0 \text{ if } M = \text{any other } xy^{-1}y'z^{-1}$$



# Separating polynomials example

- Three subgroups in  $GL(n, \mathbf{R})$ :



$$f_{x,z}(M) = \delta_1(M[1,1])$$

$$\cdot \delta_{(z_1, z_2, \dots)}(M[\text{top row}])$$

$$\cdot \delta_{(x_1, x_2, \dots)}(M[\text{left col}]) \dots$$

ind. degree equals #  
possible values in  
each entry of  $M$

# Target degree and dimension

- Given finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$  in  $GL_n$ , satisfying TPP:
  - each of size  $q^{\text{dim of subgroup}}$
  - separating polynomials of total degree  $O(q)$
  - $\dim(\mathbf{X}) = \dim(\mathbf{Y}) = \dim(\mathbf{Z}) = \frac{n^2}{2} - o(n)$
- This would prove  $\omega = 2$ .

target  
degree

# Target degree and dimension

- Given finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$  in  $GL_n$ , satisfying TPP:
  - each of size  $q^{\text{dim of subgroup}}$
  - separating polynomials of total degree  $O(q)$
  - $\dim(\mathbf{X}) = \dim(\mathbf{Y}) = \dim(\mathbf{Z}) = \frac{n^2}{2} - o(n)$
- This would prove  $\omega = 2$ . Previous slide:
  - degree  $O(q^2)$
  - $\dim(\mathbf{X}) = \dim(\mathbf{Y}) = \dim(\mathbf{Z}) = \frac{n^2}{2} - \Theta(n)$

target  
degree

# Getting the right degree

**Theorem** [BCGPU2025]: In  $U_{\{\frac{n}{2}, \frac{n}{2}\}}$  (dimension  $\frac{n^2}{2}$ ) there are three subgroups  $X, Y, Z$ , each of dimension  $\frac{n^2}{4} - \Theta(n)$  satisfying the TPP, and finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$  each of size  $q^{\dim \text{ of subgroup}}$  with separating polynomials of degree  $O(q)$ .

(proof sketch at end of talk)

# Two ideas for designing separating polynomials

# Setup so far

- $X, Y, Z$  subgroups in  $GL_n$  satisfying the Triple Product Property
- **design** finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$ 
  - each of size  $q^{\text{dim of subgroup}}$
- **design** separating polynomials of deg  $O(q)$ 
  - argument  $M = xy^{-1}y'z^{-1}$

$$\begin{aligned} f_{x,z}(M) &= 1 \text{ if } M = xz^{-1} \\ &= 0 \text{ if } M = \text{any other } xy^{-1}y'z^{-1} \end{aligned}$$

# Setup so far

- **design** finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$ 
  - each of size  $q^{\text{dim of subgroup}}$
- **design** separating polynomials of deg  $O(q)$ 
  - argument  $M = xy^{-1}y'z^{-1}$

$$\begin{aligned} f_{x,z}(M) &= 1 \text{ if } M = xz^{-1} \\ &= 0 \text{ if } M = \text{any other } xy^{-1}y'z^{-1} \end{aligned}$$

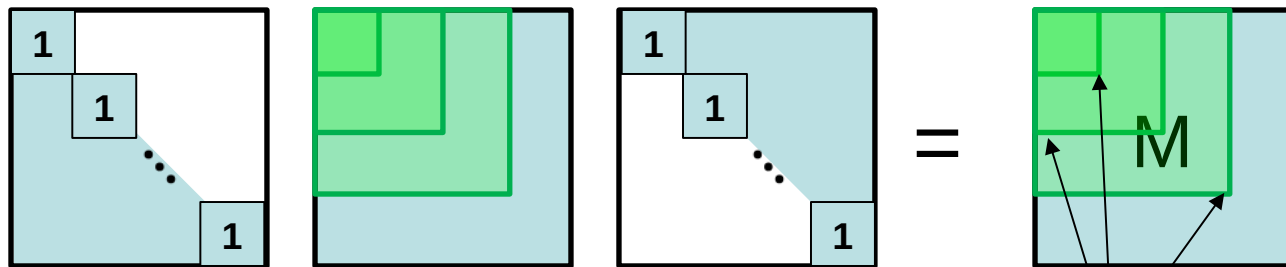
Idea #1: 
$$\begin{aligned} \text{design } f_0(xy^{-1}y'z^{-1}) &= 1 \text{ if } y^{-1}y' = I \\ &= 0 \text{ if } y^{-1}y' \neq I \end{aligned}$$

# Invariant polynomials

Select  $f_0$  from ring of invariant polynomials

- under left-multiplication by  $X$
- under right-multiplication by  $Z$

- Example: subgroups in  $GL(n, \mathbf{R})$



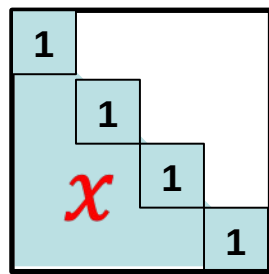
- can adapt sep. polys. in earlier e invariant ring

leading principle minors are **invariant**

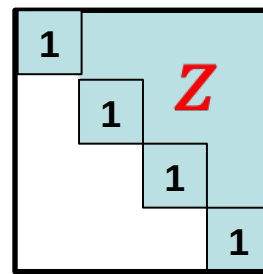
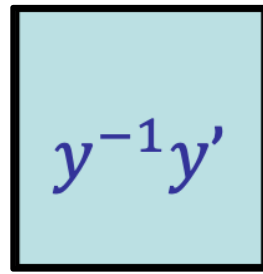


# Remaining task:

- finite subsets of 2 subgroups in  $GL(n, \mathbf{R})$ :

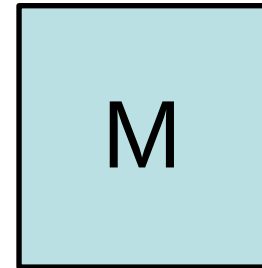


Lower Tri.



Upper Tri.

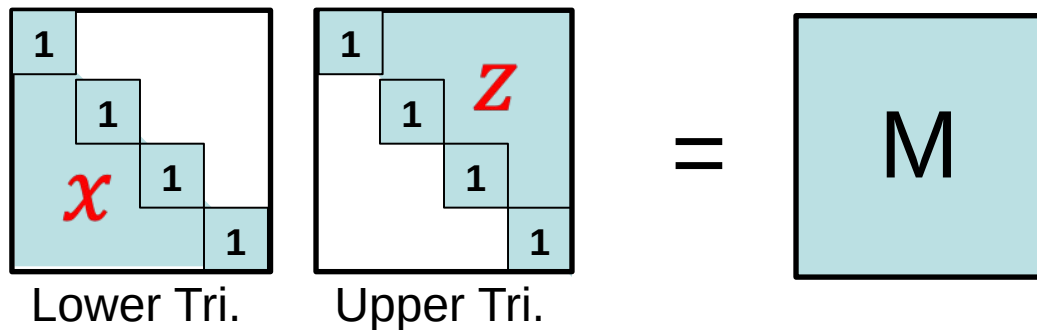
=



$f_0(M)$  vanishes unless this is the identity matrix

# Remaining task:

- finite subsets of 2 subgroups in  $GL(n, \mathbf{R})$ :



- find “**separating polynomials**” (to be multiplied with  $f_0$ )

$$f_{x,z}(M) = 1 \text{ if } M = xz^{-1}$$

$$0 \text{ if } M = \text{any other } x'z'^{-1}$$

$q$  values in entries of  $x, z \Rightarrow O(q^2)$  values in entries of  $M$

# Idea #2: use Lie algebra

- Lie Group  $G$  has associated Lie Algebra  $\mathfrak{g}$ 
  - $\mathfrak{g}$  is a vectorspace
  - for any  $A \in \mathfrak{g}$ , we have  $\exp(\epsilon A) \in G$   
(e.g. Orthogonal Group  $\Rightarrow$  skew-symmetric matrices)
- finite subsets of  $X, Y, Z$  can be defined via finite subsets of associated Lie algebras
  - the matrices have  $\epsilon$ 's in their entries, which in turn means the irreps have  $\epsilon$ 's in their entries
  - final bound is on border-rank rather than rank

# Remaining task now easier

$$\exp(\epsilon \cdot \begin{array}{|c|c|c|c|} \hline 0 & & & \\ \hline & 0 & & \\ \hline & & 0 & \\ \hline & & & 0 \\ \hline \end{array}) \exp(\epsilon \cdot \begin{array}{|c|c|c|c|} \hline 0 & & & \\ \hline & 0 & & -B \\ \hline & & 0 & \\ \hline & & & 0 \\ \hline \end{array}) = \begin{array}{|c|c|c|c|} \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline \end{array} M$$

$$M = I + \epsilon(A - B) + O(\epsilon^2)$$

- choose entries of A, B in  $\{0, 1, 2, \dots, q\}$
- $O(q)$  values in entries of  $(M - I)/\epsilon$ , up to  $O(\epsilon)$
- separating polynomials of deg.  $O(q)$ :

$$f_{x,z}(M) = h_{A,B} \left( \frac{M - I}{\epsilon} \right), \text{ where}$$

$$h_{A,B}(M') = 1 \text{ if } M' = A - B; \text{ otherwise } 0$$

# Lie algebra trick works in general

**Theorem** [BCGPU2025]: Given  $X, Y \subseteq Y, Z$  with  $|Y| = q^{\dim \text{ of subgroup}}$  and polynomial  $p$  in  $\text{Inv}_{X,Z}$  for which

- $p(M) = 1$  if  $M = I$ ,
- $p(M) = 0$  for any other  $M$  in  $yy^{-1}$

If  $X \cap Z = \{I\}$  then there exist finite subsets  $X \subseteq X, Y \subseteq Y, Z \subseteq Z$  satisfying TPP, each of size  $q^{\dim \text{ of subgroup}}$  with separating polynomials of total degree  $O(q + \deg(p))$ .

# Design task: putting it all together

- $X, Y, Z$  subgroups in  $GL_n$  satisfying the Triple Product Property
- **determine** the ring of polynomials invariant under left-mult. by  $X$ , right-mult by  $Z$
- **design** subset  $Y \subseteq Y$  of size  $q^{\text{dim of subgroup}}$
- **design** sep. poly in inv. ring, of deg  $O(q)$

$$\begin{aligned} f_0(y^{-1}y') &= 1 \text{ if } y^{-1}y' = I \\ &= 0 \text{ if } y^{-1}y' \neq I \end{aligned}$$

# Getting the right degree

# Getting the right degree: proof

**Theorem** [BCGPU2025]: In  $U_{\{\frac{n}{2}, \frac{n}{2}\}}$  (dimension  $\frac{n^2}{2}$ ) there are three subgroups  $X, Y, Z$ , each of dimension  $\frac{n^2}{4} - \Theta(n)$  satisfying the TPP, and finite subsets  $\mathbf{X} \subseteq X, \mathbf{Y} \subseteq Y, \mathbf{Z} \subseteq Z$  each of size  $q^{\dim \text{ of subgroup}}$  with separating polynomials of degree  $O(q)$ .



# Getting the right degree: proof

## Proof sketch:

- start with a construction in  $GL_n(\mathbb{C})$
- $Inv_{X,Y} \ni$  “complex-Frobenius-squared”

$$p(M) = \sum_{i,j} |M_{i,j}|^2$$

- compose with a polynomial: separating **function**  $f_0$  of correct “degree”, but not a polynomial
- restrict entire construction to unitary group
- $M_{i,j}^*$  is now an entry of  $M^{-1}$
- $p$  is now a **polynomial** in entries of  $M$

# Conclusions

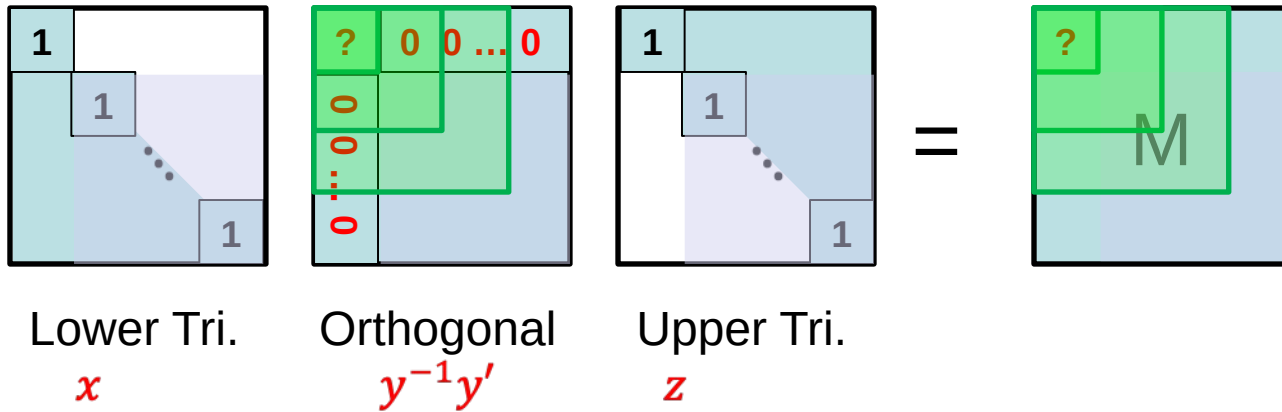
- find a Triple Product Property construction
  - in  $GL_n$ 
    - we know several constructions
  - subgroups of dimension  $n^2/2 - o(n)$ 
    - we know how to do this but in an affine group
  - finite subsets of size  $q^{\dim \text{ of subgroup}}$  with separating polys of degree  $O(q)$ 
    - we know how to do this but in a unitary group
- Then  $\omega = 2$ .

Thank you!

# Invariant polynomials

- subgroups in  $GL(n, \mathbf{R})$ :

leading principle minors are **invariant**



$$f_0(M) = \delta_1(lpm_1(M)) \cdot \delta_1(lpm_2(M)) \cdots$$

**Claim:**  $f_0(xy^{-1}y'z^{-1}) = f_0(y^{-1}y') = 1$   
 implies  $y^{-1}y' = I$