

Approaches to bounding the exponent of matrix multiplication

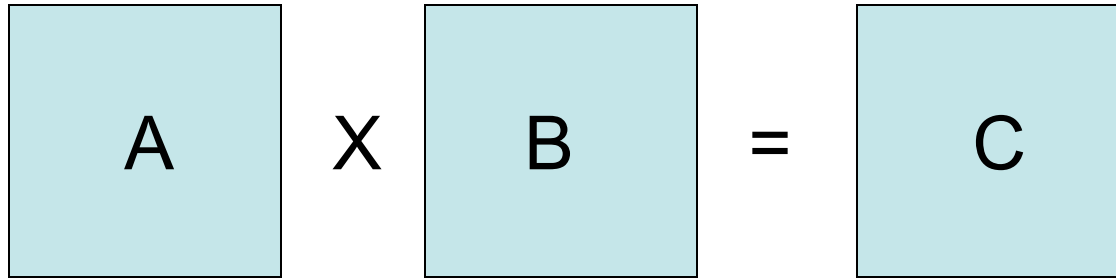
Chris Umans

Caltech

Based on joint work with Noga Alon, Henry Cohn, Bobby Kleinberg, Amir Shpilka, Balazs Szegedy

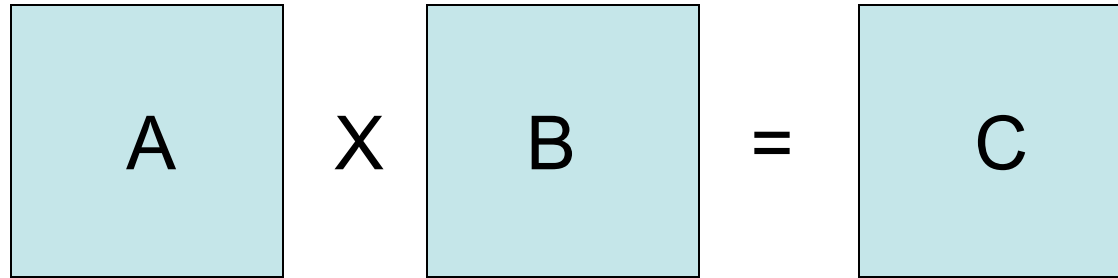
Simons Institute Sept. 17, 2014

Introduction



- Standard method: $O(n^3)$ operations
- Strassen (1969): $O(n^{2.81})$ operations

Introduction


$$A \times B = C$$

- Standard method: $O(n^3)$ operations
- Strassen (1969): $O(n^{2.81})$ operations

The exponent of matrix multiplication:
smallest number ω such that for all $\varepsilon > 0$
 $O(n^{\omega + \varepsilon})$ operations suffice

History

- Standard algorithm $\omega \leq 3$
- Strassen (1969) $\omega < 2.81$
- Pan (1978) $\omega < 2.79$
- Bini; Bini et al. (1979) $\omega < 2.78$
- Schönhage (1981) $\omega < 2.55$
- Pan; Romani; Coppersmith
+ Winograd (1981-1982) $\omega < 2.50$
- Strassen (1987) $\omega < 2.48$
- Coppersmith + Winograd (1987) $\omega < 2.375$
- Stothers (2010) $\omega < 2.3737$
- Williams (2011) $\omega < 2.3729$
- Le Gall (2014) $\omega < 2.37286$

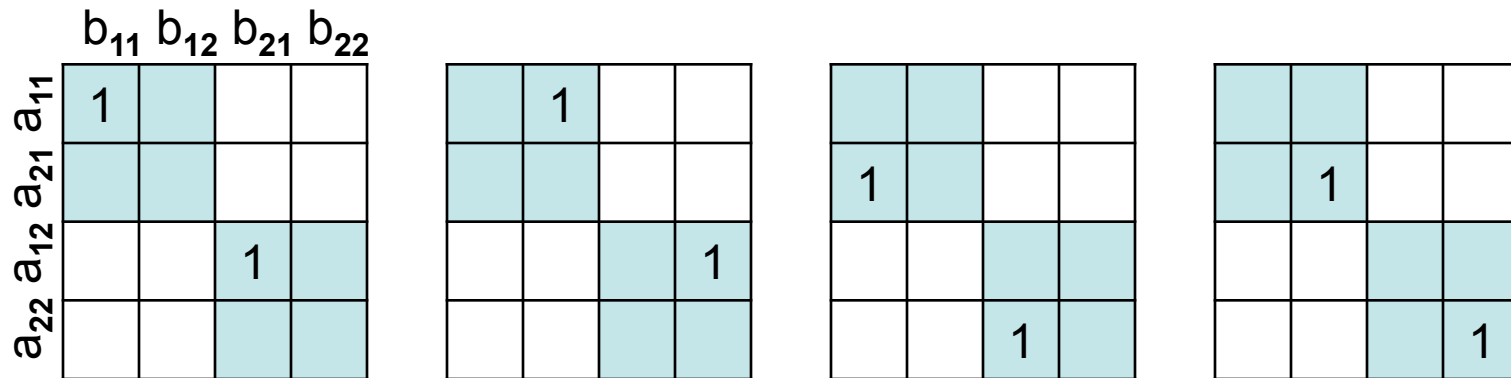
Outline

1. main ideas from **Strassen 1969** through **Le Gall 2014**
2. approach via embedding into **semi-simple algebra multiplication**
 - groups
 - coherent configurations/association schemes

The matrix multiplication tensor

$\langle n, n, n \rangle$ is a $n^2 \times n^2 \times n^2$ tensor described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

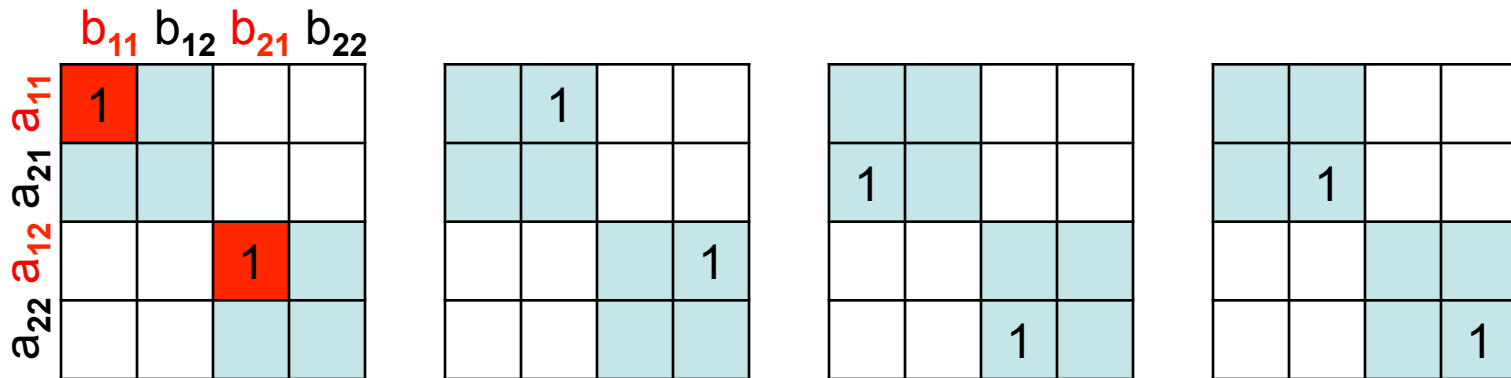
$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline c_{11} & c_{12} \\ \hline c_{21} & c_{22} \\ \hline \end{array}$$



The matrix multiplication tensor

$\langle n, n, n \rangle$ is a $n^2 \times n^2 \times n^2$ tensor described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

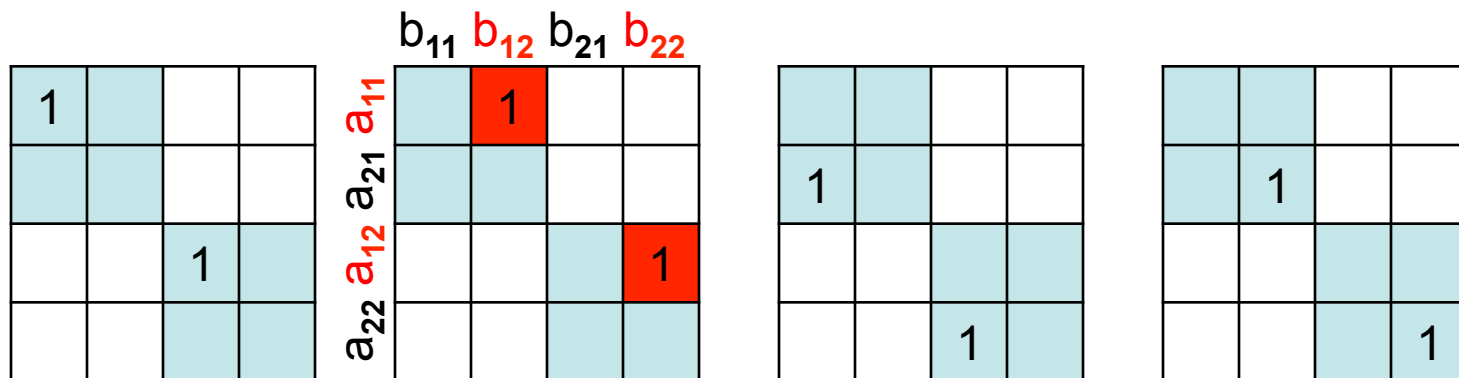
$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline c_{11} & c_{12} \\ \hline c_{21} & c_{22} \\ \hline \end{array}$$



The matrix multiplication tensor

$\langle n, n, n \rangle$ is a $n^2 \times n^2 \times n^2$ tensor described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

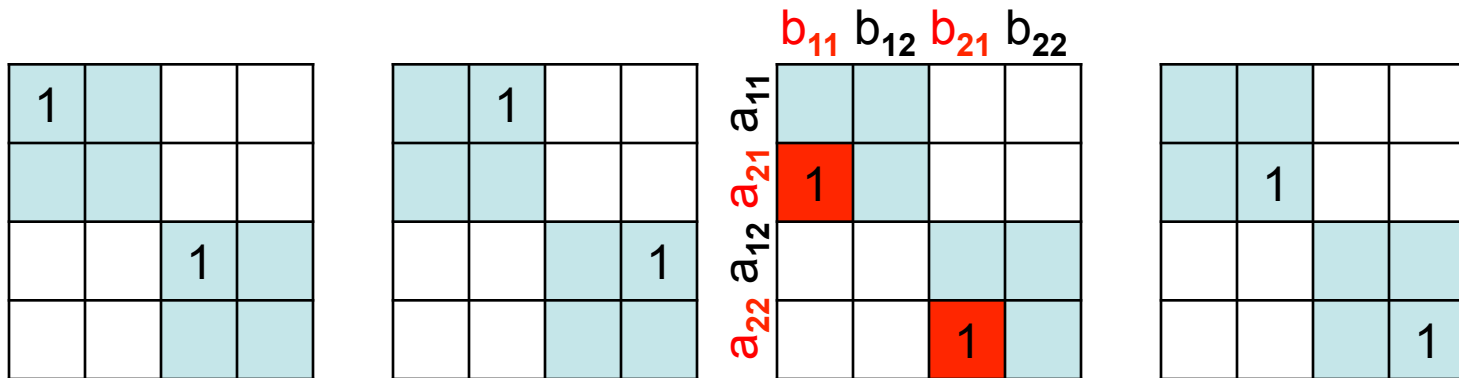
$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline c_{11} & c_{12} \\ \hline c_{21} & c_{22} \\ \hline \end{array}$$



The matrix multiplication tensor

$\langle n, n, n \rangle$ is a $n^2 \times n^2 \times n^2$ tensor described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

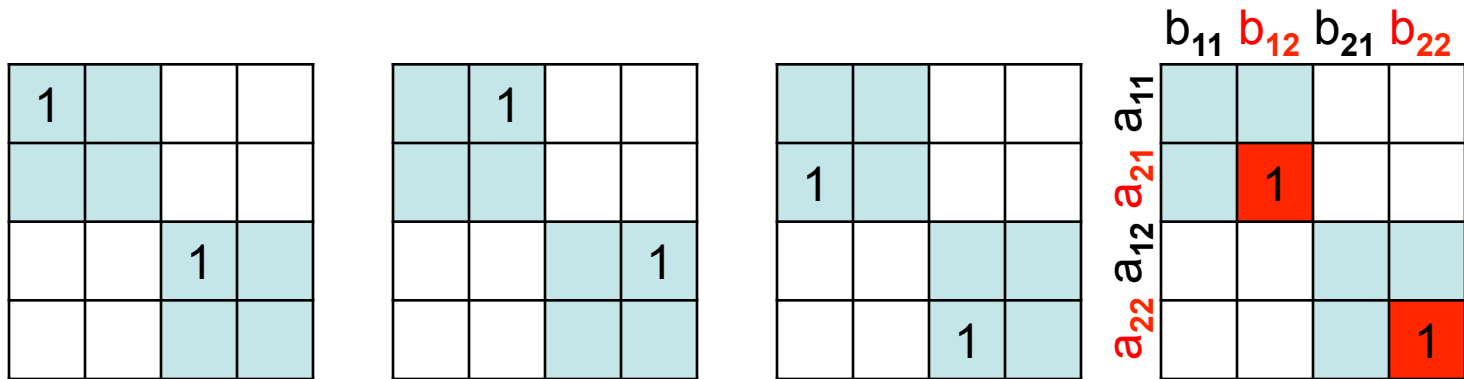
$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline c_{11} & c_{12} \\ \hline c_{21} & c_{22} \\ \hline \end{array}$$



The matrix multiplication tensor

$\langle n, n, n \rangle$ is a $n^2 \times n^2 \times n^2$ tensor described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline c_{11} & c_{12} \\ \hline c_{21} & c_{22} \\ \hline \end{array}$$

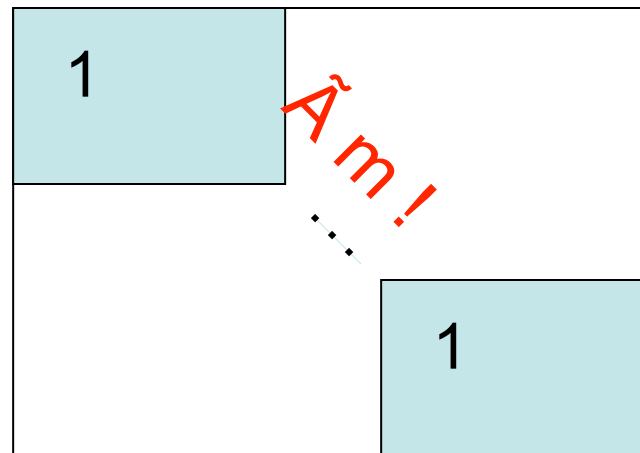


The matrix multiplication tensor

$\langle n, m, p \rangle$ is a $nm \times mp \times pn$ tensor
 described by trilinear form $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$

$$\begin{array}{c} m \\ \square \\ n \quad A \end{array} \times \begin{array}{c} m \\ \square \\ p \quad B \end{array} = \begin{array}{c} \square \\ n \quad C \\ p \end{array}$$

Each of
 np slices of
 $\langle n, m, p \rangle$:



Strategies
for upper bounding the rank
of the
matrix multiplication tensor

Upper bounds on rank

- Observation: $\langle n, n, n \rangle^{-i} = \langle n^i, n^i, n^i \rangle$
) $R(\langle n^i, n^i, n^i \rangle) \cdot R(\langle n, n, n \rangle)^i$
- **Strategy I:** bound rank for small n by hand
 - $R(\langle 2, 2, 2 \rangle) = 7$! < 2.81
 - $R(\langle 3, 3, 3 \rangle) \geq 2$ [19..23] (worse bound)
 - even computer search infeasible...

Upper bounds on rank

- **Border rank** = rank of sequence of tensors approaching target tensor **entrywise**

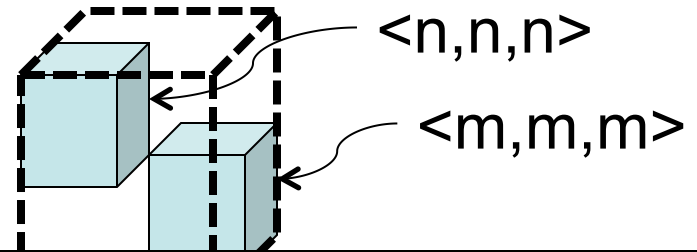
1		1	rank = 3	2-1	1	1
		1		border rank = 2:	1	2

- **Strategy II**: bound *border rank* for small n

- Lemma: $\underline{R}(\langle n, n, n \rangle) < r) ! < \log_n r$
 – $\underline{R}(\langle 2, 2, 3 \rangle) \cdot 10$ $! < 2.79$

Upper bounds on rank

- Direct sum of tensors
 $\langle n, n, n \rangle \oplus \langle m, m, m \rangle$



(multiple matrix multi

“Asymptotic Sum Inequality” and example (Schönhage 1981)

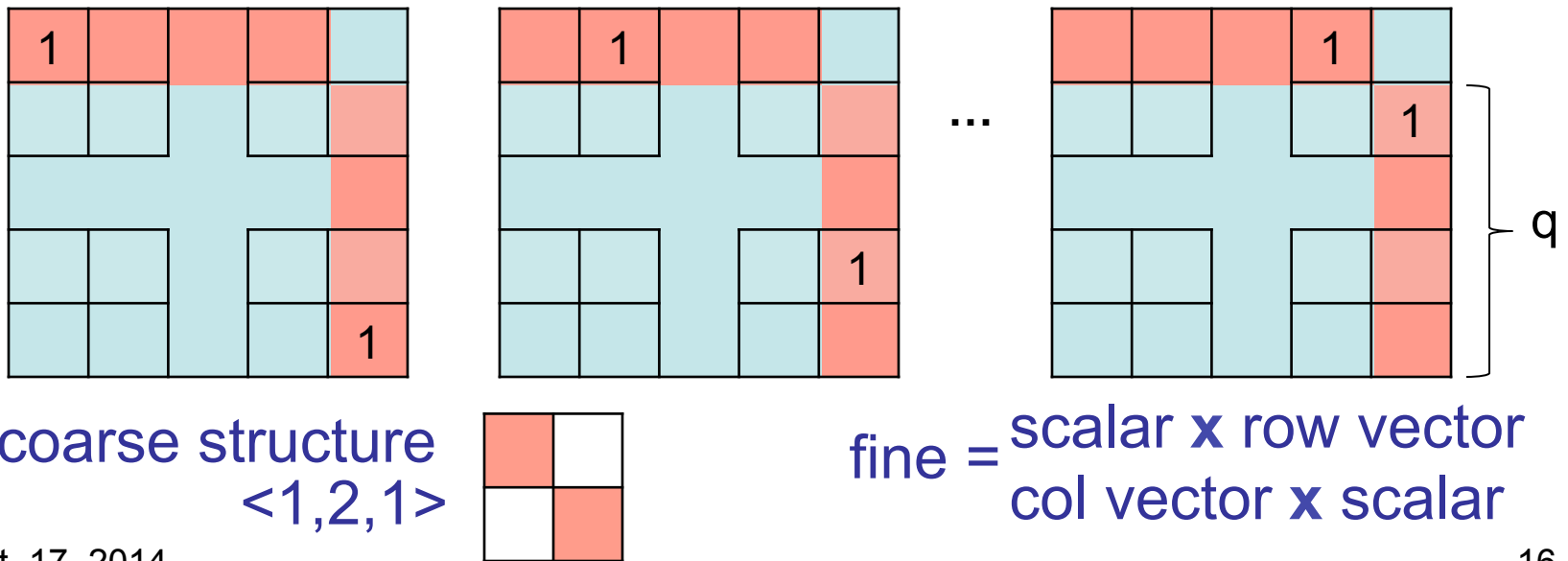
- **Strategy III**: bound (border) rank of *direct sums* of small matrix multiplication tensors

$$\underline{R}(\langle n_1, n_1, n_1 \rangle \oplus \dots \oplus \langle n_k, n_k, n_k \rangle) < r \implies \sum_i n_i! < r$$

$$\underline{R}(\langle 4, 1, 3 \rangle \oplus \langle 1, 6, 1 \rangle) \cdot 13 \quad ! < 2.55$$

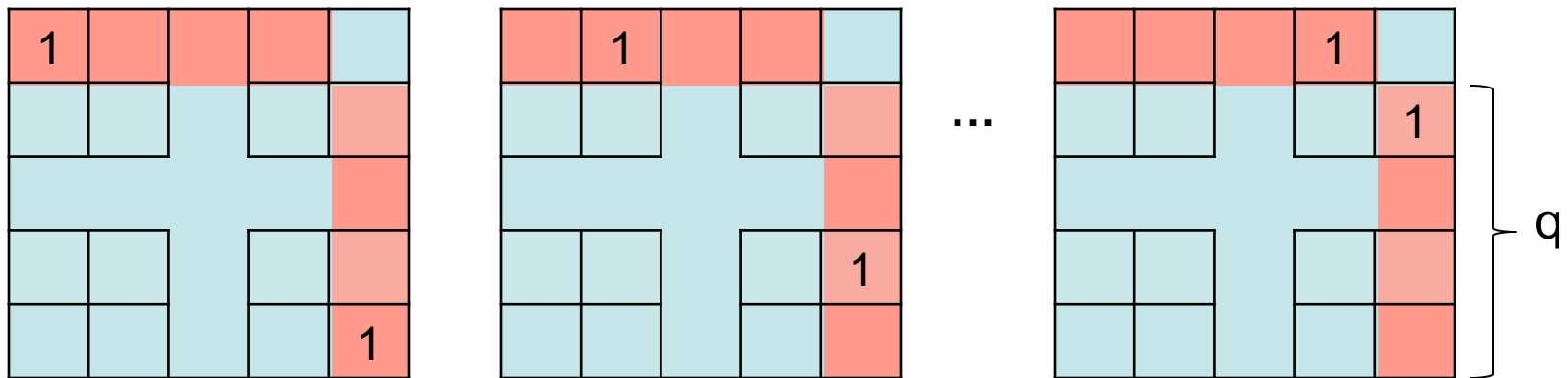
Upper bounds on rank

- **Strategy IV:** Strassen “laser method”
 - tensor with “coarse structure” of MM and “fine structure” components **isomorphic** to MM
(many independent MMs in high tensor powers)



Upper bounds on rank

- **Strategy IV**: Strassen “laser method”
 - tensor with “coarse structure” of MM and “fine structure” components **isomorphic** to MM
(many independent MMs in high tensor powers)



border rank = $q + 1$;

$q = 5$ yields $! < 2.48$

Upper bounds on rank

- Coppersmith-Winograd and beyond:
border rank of this tensor is $q+2$:

$$\sum_{i=1 \dots q} X_0 Y_i Z_i + X_i Y_0 Z_i + X_i Y_i Z_0 + \\ X_0 Y_0 Z_{q+1} + X_0 Y_{q+1} Z_0 + X_{q+1} Y_0 Z_0$$

- 6 “pieces”: target proportions in high tensor power affect # and size of independent MMs
- $q = 6$ yields $! < 2.388$

Upper bounds on rank

- **Coppersmith-Winograd and beyond:** analyze tensor powers of this tensor

$$T_q = \sum_{i=1 \dots q} X_0 Y_i Z_i + X_i Y_0 Z_i + X_i Y_i Z_0 + X_0 Y_0 Z_{q+1} + X_0 Y_{q+1} Z_0 + X_{q+1} Y_0 Z_0$$

Tensor power	# "pieces"	bound	reference
2	36	2.375	C-W
4	1296	2.3737	Stothers
8	1679616	2.3729	Williams
16	2.82×10^{12}	2.3728640	Le Gall
32	7.95×10^{24}	2.3728639	Le Gall

Upper bounds on rank

- Coppersmith-Winograd and beyond

Tensor power	# pieces	bound	reference
2	36	2.375	C-W
4	1296	2.3737	Stothers
8	1679616	2.3729	Williams
16	2.82×10^{12}	2.3728640	Le Gall
32	7.95×10^{24}	2.3728639	Le Gall

- **Ambainis-Filmus 2014:** N-th tensor power cannot beat bound of **2.3078**

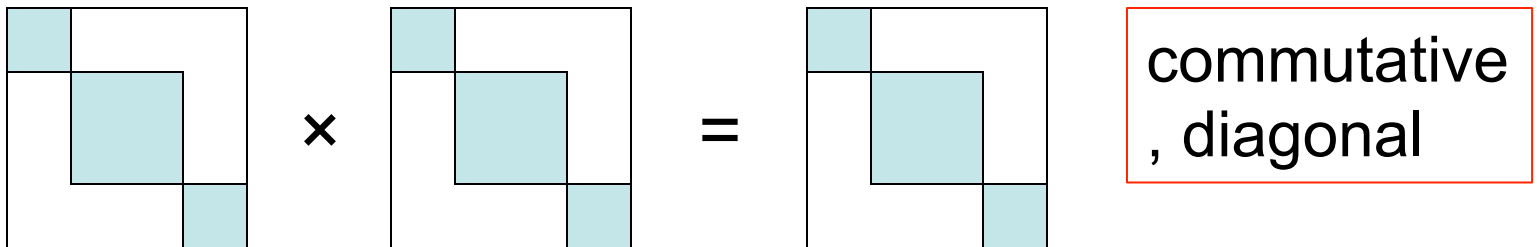
A different approach

- So far...
 - bound border rank of small tensor (by hand)
 - asymptotic bound from high tensor powers
- Disadvantages
 - limited universe of “starting” tensors
 - high tensor powers hard to analyze

matrix multiplication
via **groups** and
coherent configurations /
association schemes

The general approach

- Cohn-Umans 2003, 2012:
 - *embed* $n \times n$ matrix multiplication into **semi-simple algebra** multiplication
 - semi-simple: isomorphic to **block-diagonal MM**



- key hope: “nice basis” w/ combinatorial structure
- reduce $n \times n$ MM to smaller MMs; recurse

The Group Algebra

- given finite group G , **group algebra** $C[G]$ has elements $\sum_g a_g g$ with multiplication

$$\left(\sum_g a_g g\right)\left(\sum_h b_h h\right) = \sum_f \left(\sum_{gh=f} a_g b_h\right) f$$

- structure: $C[G] \cong (C^{d_1 \times d_1}) \times \dots \times (C^{d_k \times d_k})$
- **group elements** are “nice basis”

“Nice basis” embedding:

Subgroups X, Y, Z of G satisfy the
triple product property

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

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

The embedding:

$$Q(S) = \{s^{-1}t : s, t \in S\}$$

Subsets X, Y, Z of G satisfy the
triple product property

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

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

$$\underline{\mathbf{A}} = \sum a_{x,y} (x y^{-1})$$

$$\underline{\mathbf{B}} = \sum b_{y,z} (y z^{-1})$$

Claim: $(\underline{\mathbf{A}}\underline{\mathbf{B}})_{x,z} = \text{coeff. on } (x z^{-1}) \text{ in } \underline{\mathbf{A}}^* \underline{\mathbf{B}}.$

The embedding:

$$Q(S) = \{s^{-1}t : s, t \in S\}$$

Subsets X, Y, Z of G satisfy the
triple product property

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

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

$$\underline{\mathbf{A}} = \sum a_{x_1, y_1} (x_1 y_1^{-1})$$

$$\underline{\mathbf{B}} = \sum b_{y_2, z_2} (y_2 z_2^{-1})$$

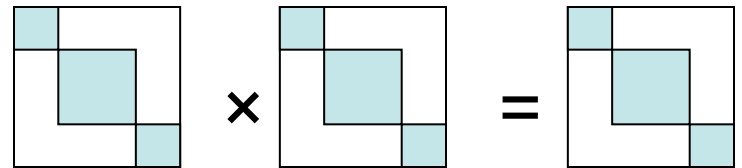
Claim: $(\underline{\mathbf{A}}\underline{\mathbf{B}})_{x_3, z_3} = \text{coeff. on } (x_3 z_3^{-1}) \text{ in } \underline{\mathbf{A}}^* \underline{\mathbf{B}}.$

$$(x_1 y_1^{-1})(y_2 z_2^{-1}) = x_3 z_3^{-1} \quad) \quad x_3^{-1} x_1 y_1^{-1} y_2 z_2^{-1} z_3 = 1$$

How many multiplications?

Embedding + structure of $C[G]$ yields bound on rank (\approx # multiplications):

- we use $m \leq \sum d_i^3$ mults
- really $m = \sum d_i!$ mults
- *at least* $m \geq \sum d_i^2 = |G|$ mults



First Challenge: embed $k \times k$ matrix multiplication in group of size $\frac{1}{4} k^2$

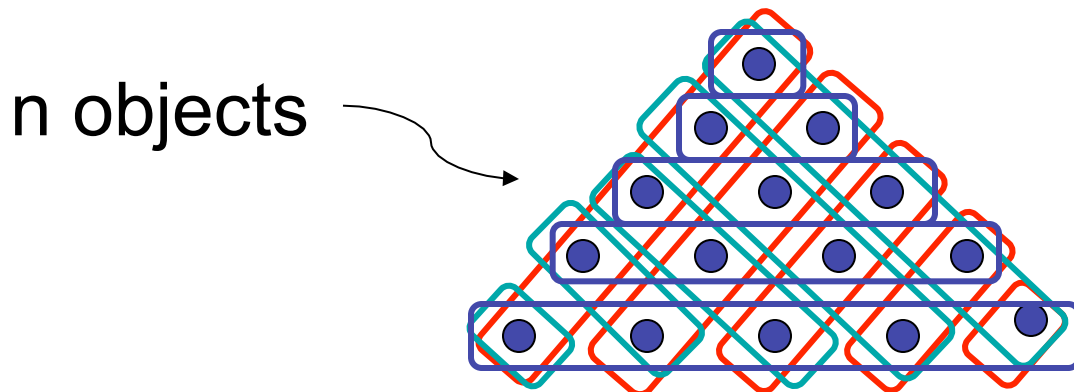
The embedding

First Challenge: embed $k \times k$ matrix multiplication in group of size $\frac{1}{4} k^2$

- simple pigeonhole argument:
 - embedding in an **abelian** group requires group to have size k^3

The triangle construction

Theorem: can embed $k \times k$ matrix multiplication in **symmetric group** of size $k^{2 + o(1)}$

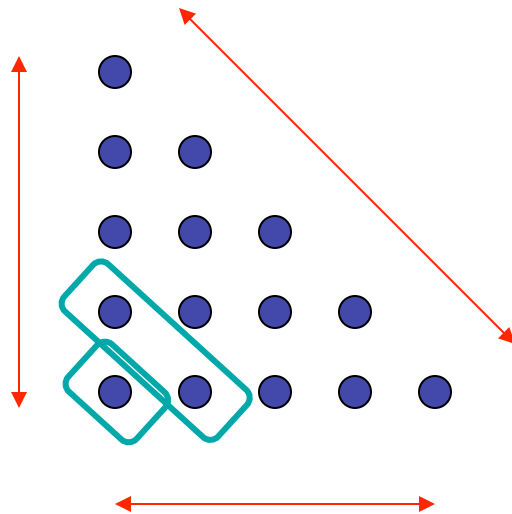


- subgroup **X**
- subgroup **Y**
- subgroup **Z**

need X, Y, Z in S_n all with size $\approx |S_n|^{1/2}$

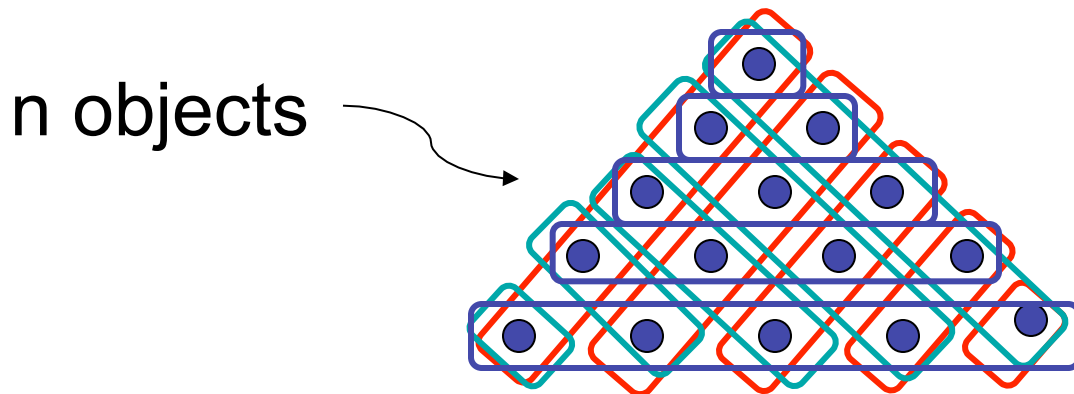
The triangle construction

- X moves points within rows
- Y moves points within columns
- Z moves points within diagonals
- want: $xyz = 1 \Rightarrow x = y = z = 1$



The triangle construction

Theorem: can embed $k \times k$ matrix multiplication in **symmetric group** of size $k^{2 + o(1)}$



- subgroup X
- subgroup Y
- subgroup Z

unfortunately, $d_{\max} > |X| (= |Y| = |Z|)$

What should we be aiming for?

Theorem: in group G supporting $k \times k$ matrix multiplication with character degrees d_1, d_2, d_3, \dots , we obtain:

$$k^\omega \cdot \sum_i d_i^\omega$$

- If $X, Y, Z \in G$ satisfy T.P.P. and

$$- (|X| \phi |Y| \phi |Z|)^{1/3} = k, |G|^{1/2 - o(1)}$$

$$- d_{\max} \cdot |G|^{1/2 - \epsilon}$$

then $\epsilon = 2$

$$\frac{\sum_i d_i!}{d_{\max}! - 2|G|}$$

Constructions in linear groups

- Good candidate family:
 - $SL(n, q)$ for fixed dimension n
 - In $SL(n, \mathbb{R})$ these three subgroups satisfy the triple product property:
 - upper-triangular with ones on the diagonal
 - lower-triangular with ones on the diagonal
 - the special orthogonal group $SO(n, \mathbb{R})$
- and dim. of each is $\frac{1}{2}$ dim. of G as $n \neq 1$

Group algebra approach

- [CKSU 2005] wreath product groups yield :
 - $! < 2.48, ! < 2.41$
 - key part of construction is combinatorial
 - two conjectures implying $! = 2$
- Main disadvantage:
 - non-trivial results *require* non-abelian groups
 - most ideas foiled by too-large char. degrees

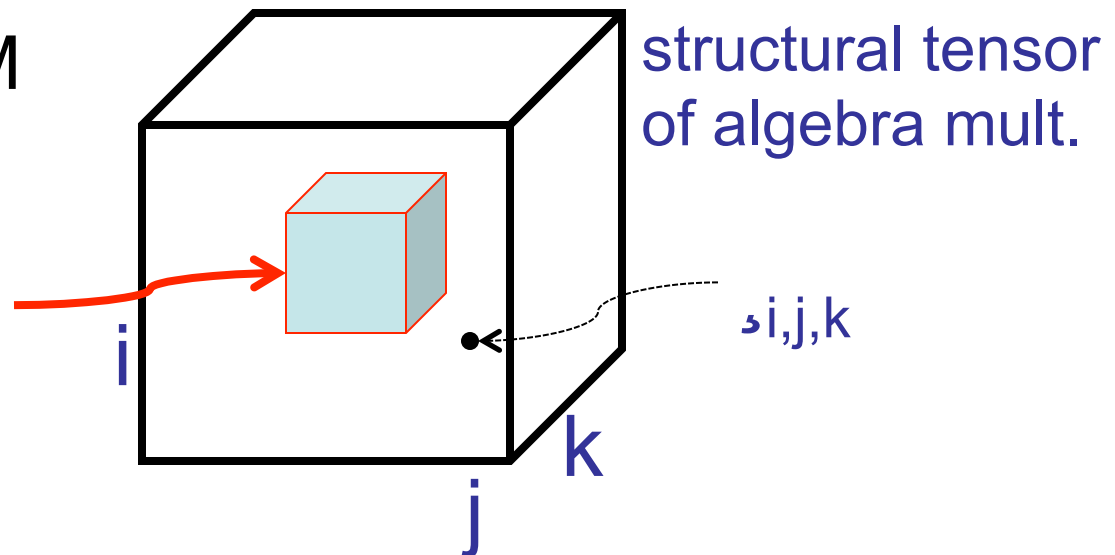
General semi-simple algebras

- (finite dimensional, complex) algebra specified by
 - “nice basis” e_1, e_2, \dots, e_r
 - structure constants $\alpha_{i,j,k}$ satisfying

$$e_i e_j = \sum_k \alpha_{i,j,k} e_k$$

“realizes” MM
if contains*:

MM tensor
 $\langle n, n, n \rangle$



Weighted vs. unweighted MM

- Technical problem:
 - MM tensor $\langle n, n, n \rangle$ given by $\sum_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$
 - embedding into algebra bounds rank of tensor given by

$$\sum_{i,j,k} \alpha_{i,j,k} X_{i,j} Y_{j,k} Z_{k,i}$$

(with $\alpha_{i,j,k} \neq 0$)

- group algebra: $\alpha_{i,j,k}$ always 0 or 1

Weighted vs. unweighted MM

s-rank of tensor T : minimum rank of tensor with same support as T

Does upper bound on s-rank of MM tensor imply upper bound on ordinary rank?

Example:

$$\begin{array}{|c|c|} \hline a_{11} & a_{12} \\ \hline a_{21} & a_{22} \\ \hline \end{array} \times \begin{array}{|c|c|} \hline b_{11} & b_{12} \\ \hline b_{21} & b_{22} \\ \hline \end{array} = \begin{array}{|c|c|} \hline a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ \hline a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \\ \hline \end{array}$$

Weighted vs. unweighted MM

s-rank of tensor T: minimum rank of tensor with same support as T

Does upper bound on s-rank of MM tensor imply upper bound on ordinary rank?

Example:

a_{11}	a_{12}
a_{21}	a_{22}

\times

b_{11}	b_{12}
b_{21}	b_{22}

!

$a_{11}b_{11} +$ $a_{12}b_{21}$	$a_{11}b_{12} +$ $a_{12}b_{22}$
$a_{21}b_{11} +$ $a_{22}b_{21}$	$a_{21}b_{12} +$ $2\phi a_{22}b_{22}$

does it help if can compute this in 6 multiplications?

Weighted vs. unweighted MM

- s-rank can be much smaller than rank:

$\mathbb{R} = n\text{-th root of unity}$

0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	0

rank n

same support:

\mathbb{R}_0	\mathbb{R}_1	\mathbb{R}_2	\mathbb{R}_3
\mathbb{R}_3	\mathbb{R}_0	\mathbb{R}_1	\mathbb{R}_2
\mathbb{R}_2	\mathbb{R}_3	\mathbb{R}_0	\mathbb{R}_1
\mathbb{R}_1	\mathbb{R}_2	\mathbb{R}_3	\mathbb{R}_0

rank 1

-

1	1	1	1
1	1	1	1
1	1	1	1
1	1	1	1

rank 1

maybe it's easy to show s-rank of $n \times n$ matrix multiplication is n^2 (!!)

Weighted vs. unweighted MM

$$\alpha = \inf \{ \beta : \text{rank}(\langle n, n, n \rangle) \cdot O(n^\beta) \}$$

$$\alpha_s = \inf \{ \beta : \text{s-rank}(\langle n, n, n \rangle) \cdot O(n^\beta) \}$$

Theorem: $\alpha = (3\alpha_s - 2)/2$

in particular, $\alpha_s = 2 + \frac{2}{3} \Rightarrow \alpha = 2 + (3/2)^2$

- Proof idea:
 - find $\frac{1}{4} n^2$ copies of $\langle n, n, n \rangle$ in 3^{rd} tensor power
 - when broken up this way, can rescale

A promising family of
semisimple algebras

Coherent configurations

“group theory without groups”

- points X , partition R_1, R_2, \dots, R_r of X^2

– diagonal $\{(x,x) : x \in X\}$ is union of some classes

if one class:
“association scheme”

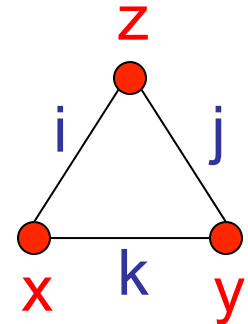
– for each i , there is i^*

$p_{i,j}^k = p_{j,i}^k$: commutative

$$R_i^* = \{(y,x) : (x,y) \in R_i\}$$

– exist integers $p_{i,j}^k$ such that for all $(x,y) \in R_k$:

$$\#\{z : (x,z) \in R_i \text{ and } (z,y) \in R_j\} = p_{i,j}^k$$



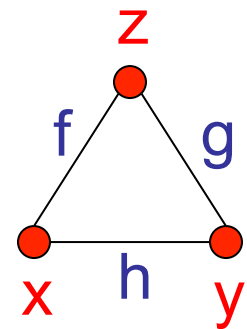
Coherent configs: examples

- Hamming scheme:
 - points 0/1 vectors
 - classes determined by hamming distance
- distance-regular graph:
 - points = vertices
 - classes determined by distance in graph metric

Coherent configs: examples

- scheme based on finite group G
 - set $X =$ finite group G
 - classes $R_g = \{(x, xg) : x \in X\}$

$$p_{f,g}^h = 1 \text{ if } fg=h, 0 \text{ otherwise}$$



- “Schurian”:
 - group G acts on set X
 - classes = orbits of (diagonal) G -action on X^2

Coherent configs: examples

- “Schurian”:
 - group G acts on set X
 - classes = orbits of (diagonal) G -action on X^2
- one Schurian scheme: “group scheme”
 - group $G \times G$ acts on G via $(g,h) \cdot x = gxh^{-1}$
 - orbits all of the form $\{(x,y): xy^{-1} \in C_i\}$ for conjugacy class C_i
 - always commutative!

Adjacency algebra

CC: points X , partition R_1, R_2, \dots, R_r of X^2

- for each class R_i , matrix A_i with

$$A_i[x,y] = 1 \text{ iff } (x,y) \in R_i$$

- 3 CC axioms)

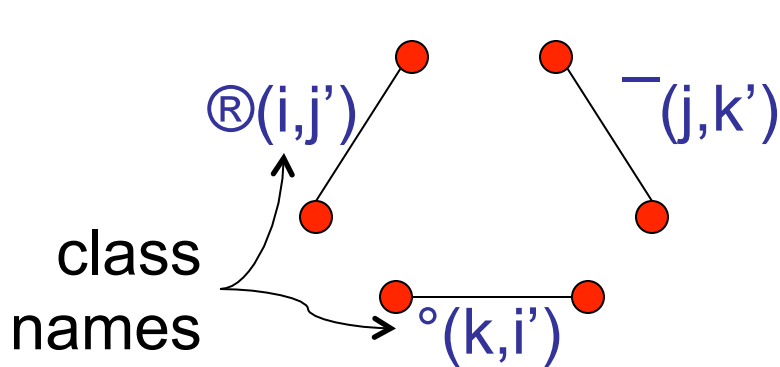
$\{A_i\}$ generate a semisimple algebra

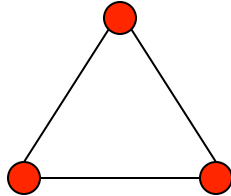
– e.g., 3rd axiom implies $A_i A_j = \sum_k p_{ij}^k A_k$

– if the CC based on group G , algebra is $C[G]$

Nice basis conditions

- group algebra $C[G]$: “nice basis” yields **triple product property**
- adjacency algebras of CCs: “nice basis” yields **triangle condition**:

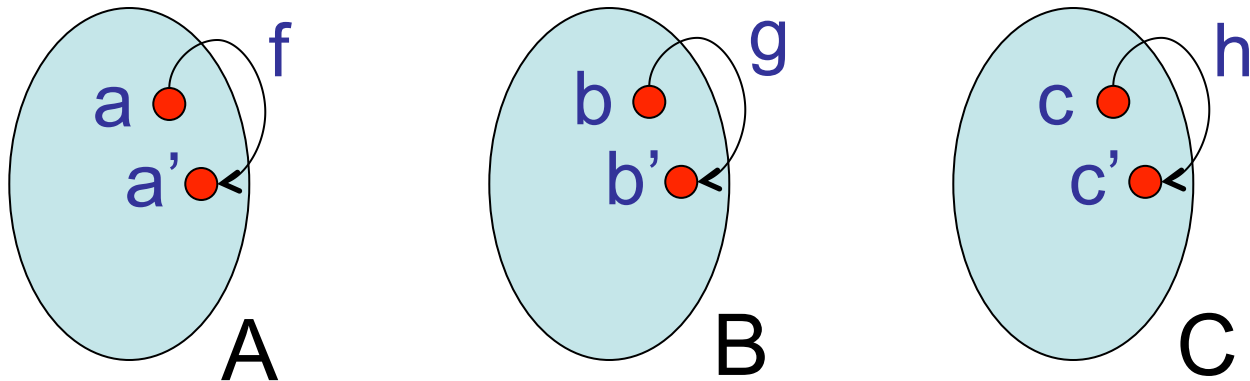


can look like 

iff $i = i', j = j', k = k'$

Nice basis conditions

- Schurian CCs: “nice basis” yields
 - group G acts on set X
 - subsets A, B, C of X realize $\langle |A|, |B|, |C| \rangle$ if:



$fgh = 1$ implies $a = a'$, $b = b'$, $c = c'$

Coherent configs vs. groups

Generalization for generalization's sake?

- recall group framework:
 - **non-commutative** necessary

Theorem: in group G realizing $n \times n$ matrix multiplication, with **character degrees** d_1, d_2, d_3, \dots , we obtain:

$$R(\langle n, n, n \rangle) \cdot \sum_i d_i^\omega \cdot d_{\max}^{\omega-2} \leq |G|$$

goals: $|G| \geq \frac{1}{4} n^2$ **and small** d_{\max}

Coherent configs vs. groups

Generalization for generalization's sake?

- coherent configuration framework:

- commutative suffices!

- combinatorial constructions from old setting yield

$$!_s < 2.48, !_s < 2.41$$

- conjectures from old setting (if true) would imply $!_s = 2$

in commutative
Schurian CC's
even group
schemes

even symmetric

Proof idea

we prove a general transformation:

if can realize **several independent matrix multiplications** in CC...

- can do this in abelian groups
- conjectures: can “pack optimally”

... then high **symmetric power** of CC realizes *single* matrix multiplication

– reproves Schönhage’s

Asymptotic Sum Inequality

preserves
commutativity

Commutative CCs suffice

Main point

embedding $n \times n$ matrix multiplication
into a commutative coherent configuration
of rank $\frac{1}{4} n^2$ is a viable route to !
= 2

(no representation theory needed)

Open problems

- find a construction in new framework that
 - proves non-trivial bound on $!_s$
 - is not based on constructions from old setting
- is the (border) s-rank of $\langle 2, 2, 2 \rangle = 6$?
- embed $n \times n$ MM into commutative coherent configuration of rank $\frac{1}{4} n^2$