Group-theoretical Method of Matrix Multiplication

Jiayue Qi

2018.11.29

Contents

ω

The greatest lower bound for the exponent of matrix multiplication algorithm is generally called ω.

It is clear: $2 \leq \omega \leq 3$

A Major Conjecture: $\omega = 2$.

Strassen's algorithm

Let $A, B, C \in R^{2^n \times 2^n}$.

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}, C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix} \tag{1}$$

Let

$$\begin{aligned} M_1 &:= (A_{11} + A_{22})(B_{11} + B_{22}) \\ M_2 &:= (A_{21} + A_{22})B_{11} \\ M_3 &:= A_{11}(B_{12} - B_{22}) \\ M_4 &:= A_{22}(B_{21} - B_{11}) \\ M_5 &:= (A_{11} + A_{12})B_{22} \\ M_6 &:= (A_{21} - A_{11})(B_{11} + B_{12}) \\ M_7 &:= (A_{12} - A_{22})(B_{21} + B_{22}) \end{aligned} \tag{2}$$

Strassen's algorithm

$C_{11}, C_{12}, C_{21}, C_{22}$ can be obtained from M_i by additions.

$$\begin{aligned} C_{11} &= M_1 + M_4 - M_5 + M_7 \\ C_{12} &= M_3 + M_5 \\ C_{21} &= M_2 + M_4 \\ C_{22} &= M_1 - M_2 + M_3 + M_6 \end{aligned} \tag{3}$$

Then we only need 7 multiplication operations in each step!
We repeat this step n times till the sub-matrix becomes number.

Denote $f(n)$ as the total number of calculations for multiplying two $2^n \times 2^n$ matrices.

$$f(n+1) = 7f(n) + s \cdot 4^n,$$

where s is the number of additions in one step of the algorithm.
Thus,

$$f(n) = (7 + o(1))^n,$$

then for multiplying two $N \times N$ ($N = 2^n$) matrices, the asymptotic complexity of Strassen's algorithm is:

$$O([7 + o(1)]^n) = O(N^{\log_2 7 + o(1)}) \approx O(N^{2.8074}).$$

History

- Volker Strassen, 1969, $\omega \leq 2.8074$.
- Don Coppersmith, Shmuel Winograd, 1990, tensor algorithm $\omega \leq 2.375477$. (CW1990)
- Andrew Stothers, 2010, improve CW1990 algorithm, $\omega \leq 2.374$.
- Virginia Williams, 2011, $\omega \leq 2.3728642$.
- Francois Le Gall, 2014, simplify Williams' algorithm, $\omega \leq 2.3728639$.

History of the complexity of matrix multiplication

- Henry Cohn, Robert Kleinberg, Balazs Szegedy, Chris Umans, 2005, the Group-theoretical Method of Matrix Multiplication, two conjectures $\implies \omega = 2$, best bound: $\omega \leq 2.41$.
- Andris Ambainis, Yuval Filmus, Francois Le Gall, 2015, "the framework of analyzing higher and higher tensor powers of a certain identity of Coppersmith and Winograd cannot result in an algorithm within running time $O(n^{2.3725})$ thus cannot prove $\omega = 2$".
- The main topic of this talk is the group-theoretical method of matrix multiplication.

Contents

Group Method of Matrix Multiplication: Notions

$\mathbb{C}$: the field of complex numbers.

- The group algebra $\mathbb{C}[G]$ of a finite group G decomposes as the direct product $\mathbb{C}[G] \cong \mathbb{C}^{d_1 \times d_1} \times \ldots \times \mathbb{C}^{d_k \times d_k}$ of matrix algebras of orders $d_1, \ldots, d_k$. These orders are the character degrees of G.
- If we compute the dimensions of both sides, we have $|G| = \sum_i d_i^2$.
- If G has an abelian subgroup A, then all the character degrees of G are less than or equal to the index $[G : A]$.

Group Method of Matrix Multiplication

Definition (right quotient set)

Let S be an arbitrary set, the *right quotient set of S*
$Q(S) = \{s_1 s_2^{-1} : s_1, s_2 \in S\}$.

Definition (double product property)

We say that subsets S_1, S_2 of a group G satisfy the *double product property if*
$q_1 q_2 = 1$ *implies* $q_1 = q_2 = 1$, *where* $q_i \in Q(S_i)$.

Definition (triple product property)

A group G realizes $\langle n_1, n_2, n_3 \rangle$ if there are subsets $S_1, S_2, S_3 \subseteq G$ such that $|S_i| = n_i$, and for $q_i \in Q(S_i)$, if $q_1 q_2 q_3 = 1$ then $q_1 = q_2 = q_3 = 1$.
We call this condition on S_1, S_2, S_3 the **triple product property**.

Group Method of Matrix Multiplication

Theorem (CU03)

Suppose G realizes $\langle n, m, p\rangle$ and the character degrees of G are $\{d_i\}$. Then $(nmp)^{\omega/3} \leq \sum_i {d_i}^{\omega}$.

Theorem (CU03)

Suppose G realizes $\langle n, m, p\rangle$ and has largest character degree d. Then $(nmp)^{\omega/3} \leq d^{\omega-2}|G|$.

Triple product property of Sylow subgroups

For a prime number p, a **Sylow p-subgroup** of a group G is a maximal p-subgroup of G

Theorem

Suppose group G has Sylow p-subgroup P, Sylow q-subgroup Q and Sylow r-subgroup R, p, q, r are pairwisely coprime. Then G realizes $\langle |P|, |Q|, |R| \rangle$ via P, Q, R.

Corollary

Suppose a group G has Sylow p-subgroup P and Sylow q-subgroup Q, p, q coprime. Then $P, Q \subset G$ satisfy double product property.

The simultaneous double product property

Definition (CKSU05)

We say that n pairs of subsets A_i, B_i(for $1 \leq i \leq n$) of a group G satisfy the *simultaneous double product property if*

- *for all i, the pair A_i, B_i satisfies the double product property, and*
- *for all i,j,k, $a_i(a'_j)^{-1}b_j(b'_k)^{-1} = 1$ implies $i = k$, where $a_i \in A_i, a'_j \in A_j, b_j \in B_j, b'_k \in B_k$.*

The simultaneous triple product property

Definition (CKSU05, Definition 5.1, simultaneous triple product property)

We say that n triples of subsets A_i, B_i, C_i(for $1 \leq i \leq n$) of a group G satisfy the *simultaneous triple product property if*

- *for each i, the three subsets A_i, B_i, C_i satisfies the triple product property, and*
- *for all i,j,k, $a_i(a'_j)^{-1}b_j(b'_k)^{-1}c_k(c'_i)^{-1} = 1$ implies $i = j = k$, for $a_i \in A_i, a'_j \in A_j, b_j \in B_j, b'_k \in B_k, c_k \in C_k$ and $c'_i \in C_i$.*

Theorem (CKSU05, Theorem7.1)

If n triples of subsets $A_i, B_i, C_i \subset H$ *satisfy the simultaneous triple product property, then the following subsets* H_1, H_2, H_3 *of* $G = Sym_n \ltimes H^n$ *satisfy the triple product property:*

$H_1 = \{h\pi : \pi \in Sym_n, h_i \in A_i \text{ for every } i\}$

$H_2 = \{h\pi : \pi \in Sym_n, h_i \in B_i \text{ for every } i\}$

$H_3 = \{h\pi : \pi \in Sym_n, h_i \in C_i \text{ for every } i\}$

An example giving a non-trivial bound for ω

Example

Let $H = Cyc_n^3$, H_1, H_2, H_3 are three factors of H, we define these sets:
$A_1 = H_1 \setminus \{0\}, B_1 = H_2 \setminus \{0\}, C_1 = H_3 \setminus \{0\}$
$A_2 = H_2 \setminus \{0\}, B_2 = H_3 \setminus \{0\}, C_2 = H_1 \setminus \{0\}$

Proposition (CKSU05, proposition 5.2)

The two triples defined above $A1, B1, C1$ and A_2, B_2, C_2 satisfy simultaneous triple product property.

An example giving a non-trivial bound for ω

Proof.

For $i \in \{1,2\}$ define $U_i = A_i - C_i$, $V_i = B_i - A_i$, and $W_i = C_i - B_i$. Now only need to show that if $u_i + v_j + w_k = 0$ with $u_i \in U_i, v_j \in V_j$ and $w_k \in W_k$, then $i = j = k$.
By observation we have:

$$U_1 = W_2 = \{(x,0,z) \in Cyc_n^3 : x \neq 0, z \neq 0\},$$

$$V_1 = U_2 = \{(x,y,0) \in Cyc_n^3 : x \neq 0, y \neq 0\},$$

$$W_1 = V_2 = \{(0,y,z) \in Cyc_n^3 : y \neq 0, z \neq 0\}.$$

If i,j,k are not all equal, then two of them must be equal but different from the third. In each case, in the repeated set one coordinate is zero but the other set is always nonzero in that coordinate. □

An example giving a non-trivial bound for ω

Example

Let $G = Sym_2 \ltimes H^2$, we set up H_i':
$H_1' = \{h\pi : \pi \in Sym_2, h_i \in A_i \text{ for every } i\}$
$H_2' = \{h\pi : \pi \in Sym_2, h_i \in B_i \text{ for every } i\}$
$H_3' = \{h\pi : \pi \in Sym_2, h_i \in C_i \text{ for every } i\}$
By [CKSU05, Theorem 7.1], we know that $H_1', H_2', H_3' \subset G$ satisfy TPP. Since $H^2 \subset G$ is abelian, $d_G \leq [G : H] = |Sym_2| = 2$.

An example giving a non-trivial bound for ω

Example

Then we have:

$$(|H_1'||H_2'||H_3'|)^{\frac{\omega}{3}} \leq \sum_i d_i^{\omega} \leq |G|d^{\omega-2} \leq |G|(2!)^{\omega-2}$$

$$(2!(n-1)^2)^{\omega} \leq 2^{\omega-2}2!n^6$$

$$2(n-1)^{2\omega} \leq n^6$$

$$\omega \leq \frac{6\lg n - \lg 2}{2\lg(n-1)}, n \geq 3$$

By calculation, we get a best bound for ω when $n = 41$: $\omega \leq 2.9261305$.

Contents

Definition (BCS1997 chap 14, def14.7)

Let k be a field and U, V, W finite dimensional k-vector space. Let $\eta : U \times V \to W$ be a k-bilinear map. For $i \in \{1, \ldots, r\}$ let $f_i \in U^*$, $g_i \in V^*$(dual spaces of U and V resp. over k) and $w_i \in W$ such that $\eta(u, v) = \sum_{i=1}^{r} f_i(u)g_i(v)w_i$ for all $u \in U$, $v \in V$. Then $\{f_1, g_1, w_1; \ldots; f_r, g_r, w_r\}$ is called a *k-bilinear algorithm of length r for η*, or simply a *bilinear algorithm* when k is fixed. The minimal length of all bilinear algorithms for η is called the *rank* $R(\eta)$ of η. Let A be a k-algebra. The *rank* $R(A)$ of A is defined as the rank of its bilinear multiplication map.

Rank

- Let G be a group, F is a field. The group algebra $F[G]$ is is the set of all linear combinations of finitely many elements of G with coefficients in F.
- For a group G, $R(G) := R(\mathbb{C}[G])$. We write $\bar{R}(G) := \sum_i R(d_i)$ for the best known upper bound and $\underline{R}(G)$ for the best known lower bound for $R(G)$.
- The rank for multiplication of an $n \times m$ matrix and an $m \times p$ matrix, denoted as $R(n, m, p)$, is defined as the exact number of required multiplications to compute the product.
- The rank for $n \times n$ matrices multiplication, denoted as $R(n)$, is defined analogously.

Relation between RANK and ω

Relation between rank for matrix multiplication and matrix multiplication exponent ω is well described in the following proposition.

Proposition (BSC1997)

For any field K, $\omega(K) = inf\{h \in \mathbb{R}^+ | R(n,n,n) = O(n^h), n \to \infty\}$

Small matrix multiplication—background

The famous result $O(n^{2.81})$ is based on an algorithm (Strassen's algorithm, 1969) that can compute the product of two 2×2 matrices with only 7 multiplications. In [DIStable, table 3], we have a list of Upper bounds for $R(n)$:

$n \times n$	upper bound for $R(n)$	algorithm
2×2	7	Strassen
3×3	23	Laderman
4×4	49	Strassen
5×5	100	Makarov
6×6	161	Strassen

Small matrix multiplication—background

- Winograd: cannot produce better results with 2×2 matrices.
- Hedtke and Murthy: the group-theoretic framework is not able to produce better bounds for 3×3 and 4×4 matrices.
- Sarah Hart, Ivo Hedtke, Matthias M$\ddot{u}$ller-Hannemann and Sandeep Murthy in 2013: the group-theoretic framework is not able to produce better bounds for 5×5 matrices.

We consider the case for 6×6 matrices multiplication to see whether this particular TPP approach can give us a better bound.

Small matrix multiplication—background

Theorem (CU03, Theorem 2.3)

Let F be any field. If group G realizes $\langle n, m, p\rangle$, then the number of field operations required to multiply $n \times m$ with $m \times p$ matrices over F is at most the number of operations required to multiply two elements of $F[G]$.

Hence we have $R(n, m, p) \leq R(\mathbb{C}[G]) =: R(G)$.

6×6 small matrix multiplication

Problem Statement: Is there a group with order less than 90 that can realize $\langle 6, 6, 6 \rangle$ TPP(triple product property) and have multiplication rank less than 161[DIStable]?

Since the search space is too large, my main thinking is to reduce the search space by lots of necessary conditions.

Necessary conditions for 6×6 small matrix multiplication

For a finite group G, let $T(G)$ be the number of irreducible complex characters of G and $b(G)$ the largest degree of an irreducible character of G.

Theorem (APlowerbounds, Theorem 6)

Let G be a group.
(1)If $b(G) = 1$, then $R(G) = |G|$.
(2)If $b(G) = 2$, then $R(G) = 2|G| - T(G)$.
(3)If $b(G) \geq 3$, then $R(G) \geq 2|G| + b(G) - T(G) - 1$.

Theorem

If G is an abelian group realizing $\langle 6, 6, 6 \rangle$, then $R(G) \geq 216$.

So we only need to consider non-abelian groups from now on.

Necessary conditions for 6×6 small matrix multiplication

Theorem (HHMM555, lemma3.3)

If G is non-abelian, then $T(G) \leq \frac{5}{8}|G|$. Equality implies that $|G : Z(G)| = 4$.

we have:
$R(G) \geq 2|G| - T(G) \geq (11/8)|G|$
Since we want $R(G) < 161$, then we have:
$(11/8)|G| < 161$
$|G| \leq 117$.

Necessary conditions for 6×6 small matrix multiplication

Definition ($\langle 6,6,6 \rangle$C1 candidate)

If a group G realizes $\langle 6,6,6 \rangle$ and has $\underline{R}[G] < 161$, we call this group a $\langle 6,6,6 \rangle$ *C1 candidate*.

Necessary conditions for 6×6 small matrix multiplication

Lemma (Neumannnote2011, Observation 3.1)

If (S, T, U) is a TPP triple, then $|S|(|T| + |U| - 1) \leq |G|$, $|T|(|S| + |U| - 1) \leq |G|$ and $|U|(|S| + |T| - 1) \leq |G|$.

Proposition

If group G is a $\langle 6, 6, 6 \rangle$ C1 candidate, then $66 \leq |G| \leq 117$.

Necessary conditions for 6×6 small matrix multiplication

Definition (HHMM555, definition3.4)

Let G be a group with a TPP triple (S, T, U), and suppose H is a subgroup of index 2 in G. We define $S_0 = S \cap H, T_0 = T \cap H, U_0 = U \cap H$, $S_1 = S \setminus H$, $T_1 = T \setminus H$ and $U_1 = U \setminus H$.

Necessary conditions for 6×6 small matrix multiplication

Lemma

Suppose G realizes $\langle 6, 6, 6 \rangle$. If G has a subgroup H of index 2, then H realizes $\langle 3, 3, 3 \rangle$.

Proof.

Suppose G realizes $\langle 6, 6, 6 \rangle$ via the TPP triple (S, T, U). If $|S_0| < |S_1|$, then for any $a \in S_1$, replace S by Sa^{-1}. This will have the effect of interchanging S_0 and S_1. Hence we may assume that $|S_0| \geq |S_1|$, $|T_0| \geq |T_1|$ and $|U_0| \geq |U_1|$. Now (S_0, T_0, U_0) is a TPP triple of H, and since each of them has at least 3 elements, clearly H realizes $\langle 3, 3, 3 \rangle$. □

Necessary conditions for 6×6 small matrix multiplication

Theorem (generalized)

If group G realizes $\langle n, n, n\rangle$. When n is odd, if G has a subgroup H of index 2, then H realizes $\langle \frac{n+1}{2}, \frac{n+1}{2}, \frac{n+1}{2}\rangle$; When n is even, if G has a subgroup H of index 2, then H realizes$\langle \frac{n}{2}, \frac{n}{2}, \frac{n}{2}\rangle$.

Theorem

If G realizes $\langle 6, 6, 6\rangle$ and $|G| < 90$, then G has no abelian subgroups of index 2.

6×6 small matrix multiplication—result

Remark

After all these necessary conditions and GAP calculations on the bound of $R(G)$ (rule out those groups G with $R(G) \geq 161$).

Among all the groups of order less than 90, possible C1 candidates are listed as below by their GAP ID (56 groups in total):
(68,3),(72,3),(72,15),(72,16),(72,19),(72,20),(72,21),(72,22), (72,23),(72,24),(72,25), (72,39),(72,40),(72,41),(72,42),(72,43), (72,44),(72,45),(72,46),(72,47),(75,2),(78,1), (78,2),(80,3), (80,15),(80,18),(80,28),(80,29),(80,30),(80,31),(80,32),(80,33), (80,34), (80,39),(80,40),(80,41),(80,42),(80,49),(80,50),(81,3), (81,4),(81,6),(81,7),(81,8), (81,9),(81,10),(81,12),(81,13), (81,14),(84,1),(84,2),(84,7),(84,8),(84,9),(84,10),(84,11).

What's next if we ever get a C1 candidate?

If we find a group G has $\langle 6, 6, 6 \rangle$ TPP property and $\underline{R}(G) < 161$, then we still don't know if this leads to a nontrivial matrix multiplication algorithm. It could require 161 scalar multiplications or more.

What's next if we ever get a C1 candidate?

To constract the algorithm induced by the given TPP triple we have several steps:

- First construct the embeddings $A \mapsto e_A$ and $B \mapsto e_B$ of matrices $A = [a_{s,t}]$ and $B = [b_{t,u}]$ in $\mathbb{C}[G]$: $a_{s,t} \mapsto a_{s,t}s^{-1}t,\ b_{t,u} \mapsto b_{t,u}t^{-1}u$ for all $s \in S, t \in T, u \in U$.
- the next step is to apply Wedderburn's structure theorem:

$$\mathbb{C}[G] \cong \mathbb{C}^{d_1 \times d_1} \times ... \times \mathbb{C}^{d_l \times d_l},$$

  where $d_1, ...d_l$ are the character degrees of G.
- Now the given matrices are represented by $l-$tuples of matrices $e_A \mapsto (A_1, ...A_l)$ and $e_B \mapsto (B_1, ...B_l)$.
- The last step is to find best algorithms for the small products A_iB_i. Then transform the result back.

What's next if we ever get a C1 candidate?

Example

Symmetric group of order 3 $G := S_3$ realizes $\langle 2, 2, 2\rangle$ via the TPP triple $S = \{1_G, (1, 2)\}, T = \{1_G, (1, 3)\}, U = \{1_G, (2, 3)\}$. First transform matrices $A = (a_{ij})$ and $B = (b_{ij})$ into $\mathbb{C}[G]$:

$$e_A = a_{11}1_G + a_{12}(1, 3) + a_{21}(1, 2) + a_{22}(1, 3, 2),$$

$$e_B = b_{11}1_G + b_{12}(2, 3) + b_{21}(1, 3) + b_{22}(1, 3, 2).$$

Afterwards, since the character degree structure of S_3 is $(1^2, 2^1)$, with $\mathbb{C}[G] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C}^{2\times 2}$, we construct the map $f : \mathbb{C}[G] \to \mathbb{C} \times \mathbb{C} \times \mathbb{C}^{2\times 2}$. Finally we get

What's next if we ever get a C1 candidate?

Example

$$f(e_A) = (a_{11} + a_{12} + a_{21} + a_{22}, a_{11} + a_{22} - a_{12} - a_{21},$$
$$\begin{bmatrix} a_{11} - a_{22} - a_{12} & a_{21} + a_{22} \\ a_{21} - a_{22} - a_{12} & a_{11} + a_{12} \end{bmatrix}),$$

$$f(e_B) = (b_{11} + b_{12} + b_{21} + b_{22}, b_{11} + b_{22} - b_{12} - b_{21},$$
$$\begin{bmatrix} b_{11} + b_{12} - b_{21} - b_{22} & b_{22} + b_{12} \\ -b_{21} - b_{22} & b_{11} - b_{12} + b_{21} \end{bmatrix}).$$

We need minimum 9 multiplications to calculate $f(e_A)f(e_B)$. Afterwards, we transform back to get the product of A and B.

Contents

Constructing TPP triples

Definition (IHupgrade2015, TPP capacity)

Denote the *TPP capacity* of group G as $\beta(G)$, $\beta(G) := max\{npm,$ where G realizes $\langle n, p, m\rangle\}$.

Lemma

A_4 realizes $\langle 3, 3, 2\rangle$, $\beta(A_4) = 18$.

TPP triples: $S : \{(1), (13)(24)\}$; $T : \{(1), (243), (234)\}$; $U : \{(1), (124), (142)\}$.

constructing TPP triples

Proposition

$G = C_6 \times A_4$ realizes $\langle 6, 6, 3\rangle$ via S, T, U, where

$S =$

$\{(1,1),(1,(13)(24)),(\bar{3}^{(1)},1),(\bar{3}^{(1)},(13)(24)),(\bar{3}^{(2)},1),(\bar{3}^{(2)},(13)(24))\}$,

$T =$

$\{(1,1),(1,(243)),(1,(234)),(\bar{2}^{(1)},1),(\bar{2}^{(1)},(243)),(\bar{2}^{(1)},(234))\}$,

$U = \{(1,1),(1,(124)),(1,(142))\}$.

Constructing TPP triples

Proposition

$G = C_3 \times A_4$ realizes $\langle 6, 4, 3 \rangle$ via S, T, U, where

$S =$
$\{(1,1), (1,(13)(24)), (\bar{3}^{(1)}, (13)(24)), (\bar{3}^{(2)}, (13)(24)), (\bar{3}^{(1)}, 1), (\bar{3}^{(2)}, 1)\}$,

$T = \{(1,1), (1,(14)(23)), (1,(143)), (1,(134))\}$,

$U = \{(1,1), (1,(123)), (1,(132))\}$.

Motivation

- From the examples above we can see that once I got a "TPP" triple of a subgoup, say A_4 , I would like to expand it in some way to get a "TPP" triple of a bigger group, say $C_6 \times A_4$ or $C_3 \times A_4$.
- It's easier sometimes to obtain a TPP triple of a smaller group, so I would like to find some theory behind, say relations between TPP of A_4 and TPP of $C_n \times A_4$. (C_n: cyclic group of order n)

Definition (IHupgrade2015, basic TPP triple)

According to Neumann we call a TPP triple (S, T, U) that fulfills $1 \in S \cap T \cap U$ a basic TPP triple.

It's enough to consider basic TPP triples.

constructing TPP triples—some principles

We take $\langle 6,6,6\rangle$ for S_2, T_2, U_2 for example:

S_2	T_2	U_2
$(1,1)$	$(1,1)$	$(1,1)$
$(1,s_1)$	$(1,t_1)$	$(1,u_1)$
$(1,s_2)$	$(1,t_2)$	$(2,z_1)$
$(2,x_1)$	$(2,y_1)$	$(2,z_2)$
$(2,x_2)$	$(2,y_2)$	$(2,z_3)$
$(2,x_3)$	$(2,y_3)$	$(2,z_4)$

Here,we have $S=\{1,s_1,s_2\}, T=\{1,t_1,t_2\}, U=\{1,u_1\}, X=\{x_1,x_2,x_3\}, Y=\{y_1,y_2,y_3\}, Z=\{z_1,z_2,z_3,z_4\}$. And $C_2=\{1,2\}$ is the cyclic group of order 2, 1 is the unit and 2 represents the 2-ordered element in it.

constructing TPP triples—some principles

Theorem

If $S_2, T_2, U_2 \subset C_2 \times B$ satisfy TPP and $S \cap X \neq \phi$, then $Y \cap T = \phi$ and $Z \cap U = \phi$ must hold.

Proof.

When $S_2, T_2, U_2 \subset D$ has TPP property, if $S \cap X \neq \phi$. Suppose $Y \cap T \neq \phi$, w.l.o.g., $y_1 = t_1$, assume $s_1 = x_1$, then we have $(1, s_1)(2, x_1)^{-1}(1, y_1)(2, t_1)^{-1}(1, u)(1, u)^{-1} = 1$, but obviously $(1, s_1) \neq (2, x_1)$, contradiction! With the same approach, we can obtain $Z \cap U \neq \phi$. □

constructing TPP triples—some principles

Theorem

If $S_3, T_3, U_3 \subset C_3 \times B$ satisfy TPP and $S \cap X \neq \phi$, then we have $Y \cap T = \phi$ and $Z \cap U = \phi$.

Proposition

If $S_2, T_2, U_2 \subset C_2 \times B$ satisfy TPP, then the subset triples (S, Y, U), (S, Y, Z), (S, T, Z), (X, T, U), (X, T, Z), (X, Y, U), (X, Y, Z) of B all satisfy TPP.

constructing TPP triples—some principles

Theorem

If $S_2, T_2, U_2 \subset C_2 \times B$ satisfy TPP, and $S_2|_B$ contains some repeated elements, then B realizes $\langle a, b, c\rangle$, where $a = r + 1$ (r is the number of elements that has more than one occurrence), $b = |T_2|$, $c = |U_2|$.

Constructing TPP triples—some principles

Theorem

If $S', T', U' \subset C_n \times B$ *satisfy TPP and the multiset* $S_i|_B$ *contains some repeated elements, then* B *realizes* $\langle a, b, c\rangle$*, where* $a = \max\{r+1, \max_i |S_i|\}$ *(*r *is the number of elements that has more than one occurrence),* $b = \max\{|T_i|\}$*,* $c = \max\{|U_i|\}$*.*

Contents

Main results

- An example leading to a non-trivial bound: $\omega \leq 2.9262$
- TPP and DPP property of Sylow subgroups of a given group.
- 6×6 small matrix multiplication: Reduces to 56 candidates for groups of order < 90.
- Relations between the TPP of an arbitrary group B and the group $C_n \times B$.

Reference

- (CKSU05) Cohn H, Kleinberg R, Szegedy B, e al. Group-theoretic algorithms for matrix multiplication[C]. Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on. IEEE, 2005: 379-388.
- (CU03) Cohn H, Umans C. A group-theoretic approach to fast matrix multiplication[C]. Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on. IEEE, 2003: 438-449.
- (HHMM555) Hart S, Hedtke I, Mller-Hannemann M, et al. A fast search algorithm for$\langle m, m, m \rangle$ Triple Product Property triples and an application for 5×5 matrix multiplication[J]. Groups Complexity Cryptology, 2015, 7(1): 31-46.

Reference

- (APlowerbounds) Pospelov A. Group-theoretic lower bounds for the complexity of matrix multiplication[C]. International Conference on Theory and Applications of Models of Computation. Springer Berlin Heidelberg, 2011: 2-13.
- (strassen1969) Strassen V. Gaussian elimination is not optimal[J]. Numerische mathematik, 1969, 13(4): 354-356.
- (CW90) Coppersmith D, Winograd S. Matrix multiplication via arithmetic progressions[J]. Journal of symbolic computation, 1990, 9(3): 251-280.

Reference

- (AS2010) Davie A M, Stothers A J. Improved bound for complexity of matrix multiplication[J]. Proceedings of the Royal Society of Edinburgh: Section A Mathematics, 2013, 143(02): 351-369.
- (VW2012) Williams V V. Multiplying matrices faster than Coppersmith-Winograd[C]. Proceedings of the forty-fourth annual ACM symposium on Theory of computing. ACM, 2012: 887-898.
- (LeGall2014) Le Gall F. Powers of tensors and fast matrix multiplication[C]. Proceedings of the 39th international symposium on symbolic and algebraic computation. ACM, 2014: 296-303.

Reference

- (AFL2015) Ambainis A, Filmus Y, Le Gall F. Fast matrix multiplication: limitations of the coppersmith-winograd method[C]. Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing. ACM, 2015: 585-593.
- (DIStable) DrevetC, Islam M N, Schost. Optimization techniques for small matrix multiplication[J]. Theoretical Computer Science, 2011, 412(22): 2219-2236.
- (IHupgrade2015) Hedtke I. Upgrading Subgroup Triple-Product-Property Triples[J]. Journal of Experimental Algorithmics (JEA), 2015, 20: 1.1.
- (Neumannnote2011) Peter M. Neumann. A note on the triple product property for subsets of finite groups. LMS J. Comput.Math., 14:232-237, 2011.

Reference

- (BCS1997) Brgisser P, Clausen M, Shokrollahi A. Algebraic Complexity Theory[M]. Springer Science&Business Media, 1996.

Thank You