A NOTE ON THE TRIPLE PRODUCT PROPERTY SUBGROUP CAPACITY OF FINITE GROUPS

IVO HEDTKE

Abstract. In the context of group-theoretic fast matrix multiplication the TPP capacity is used to bound the exponent ω of matrix multiplication. We prove a new and sharper upper bound for the TPP subgroup capacity of a finite group.

1. Introduction

In the context of group-theoretic fast matrix multiplication (see [1] for an introduction) the *TPP subgroup capacity* is used to bound the exponent ω of matrix multiplication. New upper bounds for the TPP subgroup capacity can be used to identify groups that do not lead to a nontrivial upper bound for ω via subgroup *TPP triples*. Our new bound (2) also gives a hint why Cohn and Umans state that "nonabelian simple groups appear to be a fruitful source of groups" with a large TPP capacity: The TPP capacity of abelian groups is trivial and the normal core of simple groups is equal to 1. Some researchers believe that triples of subgroups will never lead to a new nontrivial upper bound for ω in the context of the (TPP). Maybe this new bound will help to prove or disprove this conjecture.

With $Q(X) := \{xy^{-1} : x, y \in X\}$ we denote the *right quotient* of X. A triple (S, T, U) of subsets $S, T, U \subseteq G$ of a group G fulfills the so-called *Triple Product Property* (TPP) if for $s \in Q(S)$, $t \in Q(T)$ and $u \in Q(U)$, $stu = 1$ holds iff $s = t = u = 1$. In this case we call (S, T, U) a *TPP triple* of G. The *TPP capacity* $\beta(G) := \max\{|S| \cdot |T| \cdot |U| : (S, T, U) \text{ is a TPP triple of } G\}$ is the biggest size of a TPP triple of G. We can use

$$\beta(G)^{\omega/3} \leq D_\omega(G) \tag{1}$$

to find new nontrivial upper bound for the exponent $\omega := \inf\{r \in \mathbb{R} : M(n) = \mathcal{O}(n^r)\}$ of matrix multiplication, where $D_\omega(G) := \sum d_i^\omega$ and $\{d_i\}$ are the character degrees of G. Here $M(n)$ denotes the number of field operations in characteristic 0 required to multiply two $(n \times n)$ matrices. The *TPP subgroup capacity* β_g is defined like β, but we restrict S, T and U to be subgroups of G. Note that $\beta_\mathrm{g} \leq \beta$ holds. Therefore, β_g can be used in the same way like β to bound ω, but the result is not as strong as with the TPP capacity β. On the other hand it is easier to deal with subgroups instead of subsets, especially in (brute-force) search algorithms (see [2] for details). Note that $\beta_\mathrm{g}(G) \geq |G|$, because $(G, 1, 1)$ is a TPP triple for every group G.

Fact 1. [1, Lem. 2.1] *Without loss of generality we can assume that* $|S| \geq |T| \geq |U|$.

Fact 2. [3] *If* (S, T, U) *is a TPP triple with* $|S| \geq |T| \geq |U|$, *then* $|S|(|T| + |U| - 1) \leq |G|$.

Fact 3. [2, Thm. 3.5] *If* (S, T, U) *is a TPP triple of subgroups of* G *and one of* S, T *or* U *is normal in* G, *then* $|S| \cdot |T| \cdot |U| \leq |G|$.

2. New Upper Bound for the TPP subgroup capacity

Theorem. *Let* G *be a finite group. Let* $\{S_i\}_{i=1}^k$ *be the list of all subgroups of* G, *sorted by their order such that* $|S_i| \leq |S_{i+1}|$. *Let* $N := \max\{i : |S_i| \leq |G|/(|S_3| + |S_2| - 1)\}$. *We define*

$$\Delta(S_i) := \max\left\{|S_j| \cdot |S_k| \ : \ 1 < k < j < i,\ |S_i|(|S_j| + |S_k| - 1) \leq |G|\right\},$$

and

$$b(G) := \max_{4 \leq i \leq N} \min\left\{\frac{|G| \cdot |S_i|}{|\mathrm{Core}_G(S_i)|}\ ,\ |S_i| \cdot \Delta(S_i)\right\}.$$

Then

$$\beta_\mathrm{g}(G) \leq \max\{b(G), |G|\} =: h(G). \tag{2}$$

Proof. According to Fact 1 we are only interested in triples of type (S_i, S_j, S_k) where $i \geq j \geq k$. We assume that $|S_k| > 1$, because a TPP triple (S_i, S_j, S_k) represents a $(|S_i| \times |S_j|) \times (|S_j| \times |S_k|)$ matrix multiplication and we only focus on true matrix-matrix products. Furthermore $i \neq j \neq k$ holds, because in every other case the triple (S_i, S_j, S_k) can not fulfill the TPP. Therefore it follows that $i \geq 4$. Now assume that (S_i, S_j, S_k) is a TPP triple in G. From Fact 2 we know that $|S_i|(|S_j| + |S_k| - 1) \leq |G|$ must hold. In the case where S_j and S_k are the smallest nontrivial distinct subgroups of G, what means that $j = 3$ and $k = 2$, this gives us the upper bound

$$|S_i| \leq \frac{|G|}{|S_3| + |S_2| - 1}$$

for S_i. It follows that we can restrict the search space for S_i to $\{S_i : i \leq N\}$. Combined we get $4 \leq i \leq N$. From NEUMANN (Fact 2) we know the upper bound

$$t(G) := \max\left\{|S_i| \cdot |S_j| \cdot |S_k| \quad : \quad S_i, S_j, S_k < G,\ |S_i| \geq |S_j| \geq |S_k| > 1,\ |S_i|(|S_j| + |S_k| - 1) \leq |G|\right\}$$

for β_{g}. Note that this equals to $\max_i |S_i| \cdot \Delta(S_i)$, the right-hand-side of $b(G)$. Assume that (S_i, S_j, S_k) is a TPP triple of subgroups of G. For every subset $A \subseteq S_i$ of S_i, (A, S_j, S_k) is a TPP triple, too. If S_i contains a normal subgroup $N \lhd G$ of G, then (N, S_j, S_k) is a TPP triple of G which fulfills the Fact 3. It follows that $|S_j| \cdot |S_k| \leq |G|/|N|$. Obviously, this holds for the biggest normal subgroup in S_i, too:

$$|S_i| \cdot |S_j| \cdot |S_k| \leq |S_i| \cdot \frac{|G|}{|\mathrm{Core}_G(S_i)|}.$$

Note that this is the left-hand-side of $b(G)$. We omitted the case $(G, 1, 1)$, so it could be possible that $b(G) < |G|$. We correct this via Eq. (2). □

3. Applications

Our new bound h is a combination of NEUMANNS's bound t (which is the formerly best known bound) and the observation about normal subgroups from HEDTKE and MURTHY. Obviously $\beta_g \leq h \leq t$ holds. Note, that Eq. (1) leads to a nontrivial upper bound iff $\beta(G) > D_3(G)$. Therefore we conclude that a group G with $\beta_{\mathrm{g}}(G) \leq D_3(G)$ will never realize a nontrivial ω via a TPP triple of subgroups. Tbl. 1 shows the effect of h and t at excluding such G's.

$\lvert G\rvert$	$\#G$'s	$\lvert\{G : t \leq D_3\}\rvert$	$\lvert\{G : h \leq D_3\}\rvert$	$\lvert G\rvert$	$\#G$'s	$\lvert\{G : t \leq D_3\}\rvert$	$\lvert\{G : h \leq D_3\}\rvert$
24	12	4	6	64	256	129	136
32	44	7	11	72	44	8	12
36	10	4	6	80	47	18	22
40	11	3	11	84	13	5	8
48	47	18	22	88	9	0	2
50	3	1	2	96	224	28	93
56	10	2	4	98	3	1	2
60	11	5	8	100	12	6	8

TABLE 1. Examples of the impact of the new bound for *nonabelian* groups.

References

[1] H. Cohn and C. Umans, *A Group-theoretic Approach to Fast Matrix Multiplication*, Proceedings of the 44th Annual Symposium on Foundations of Computer Science, 11-14 October 2003, Cambridge, MA, IEEE Computer Society (2003), 438–449.

[2] I. Hedtke and S. Murthy, *Search and test algorithms for Triple Product Property triples*, arXiv eprint 1104.5097, 2011.

[3] P. M. Neumann, *A note on the triple product property for subsets of finite groups*, to appear in Journal of Computation and Mathematics, London Mathematical Society, 2011.

INSTITUTE OF COMPUTER SCIENCE, UNIVERSITY OF HALLE-WITTENBERG, D-06099 HALLE, GERMANY
E-mail address: hedtke@informatik.uni-halle.de