Is there a group with order less than 90 that can realize 6×6 matrix multiplication better than Strassen's algorithm?

Jiayue Qi

January 16, 2017

1 Problem statement

Problem Restatement: The problem is equal to "Is there a group with order less than 90 that can realize $< 6, 6, 6 >$ TPP property and have multiplication rank less than 161?[1]".

2 Method to solve it

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

2.1 necessary conditions and how they reduce the search space

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 2.1 ([2]. *,Theorem 6 and Remark 2] 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* $R(G) \geq 2|G| + b(G) - T(G) - 1$.

Definition 1 (Triple Product Property)**.** *We say that the nonempty subsets* S, T *and* U *of a group* G *satisfy the* Triple Product Property*(TPP) if for* $s \in Q(S)$, $t \in Q(T)$ *and* $u \in Q(U)$, *stu=1 holds if and only if s=t=u=1. If this holds,we say the the group G realizes* $< |S|, |T|, |U| >$ *via* S, T, U.

Definition 2. *Let* $\beta(G)$ *be the maximum of n*m*p, where G realizes* $< n, m, p >$.

Theorem 2.2. *For an abelian group,* $\omega = 3$.

Proof. If G is abelian and non-trivial($|G| \neq 1$), then b(G)=1 and from Theorem 1 we have: $R(G) = |G|$. And from page 3 of [3],we know that $R(n, m, p) \leq R(G)$. So $\beta(G) \leq R(G) = |G|$. From Theorem 1.7. in [3], we have $\omega \leq 3$. □

Remark 2.1. *Then Since we are looking for non-trivial solutions for* ω*, now we only need to consider non-abelian groups.*

Lemma 2.1. *(abelian judgements)*
(1)If $|G|$ is a prime then G is abelian.
(2)If $|G| = pq$, where p and q are primes,p¡q, if $q \not\equiv 1 mod p$, then G is abelian.
(3)If $|G| = pq^2$, p and q are two distinct primes and p doesn't divide —Aut(G)—, then G is abelian.
(4)If $|G| = pqr$, p, q and r are three distinct primes and q¡r, $r \not\equiv 1(mod q)$, qr ¡p, $p \not\equiv 1(mod r)$, $p \not\equiv 1(mod q)$, then G is abelian.

Theorem 2.3. *([3]) If G is non-abelian, then $T(G) \leq (5/8)|G|$.Equality implies that $|G : Z(G)| = 4$.*

Remark 2.2. *Then if we combine Theorem 2 and Theorem 3, we have:*
$R(G) \geq 2|G| - T(G) \geq (11/8)|G|$.
Since we want $R(G) \leq 161$, then we have:
$(11/8)|G| < 161$
$|G| \leq 117$.

Definition 3. *(C1 candidates,similar but not quite the same to [3],Definition 3.2) A group G that realizes $< 6, 6, 6 >$ and satisfies $\underline{R}[G] < 161$ will be called* C1 candidate.

Theorem 2.4. *([4],Observation 3.1) Let (s,t,u) be the parameters of a TPP triple in G. Then $s(t + u - 1) \leq |G|$, $t(s + u - 1) \leq |G|$ and $u(s + t - 1) \leq |G|$.*

Proposition 1. *If G is a C1 candidate, then $66 \leq |G| \leq 117$.*

Proof. From the theorem above, we have $|G| \geq 6 * (6 * 6 - 1) = 66$. Consider Theorem 1 and Theorem 4 above, we have $R(G) \geq 2|G| - T(G) \geq (11/8)|G|$. And $\underline{R}[G] < 161$, then we have $|G| \leq 117$. □

Remark 2.3 (GAP experiment). *After the "abelian judgement (1),(2) and (4)" stated above, if G is a C1 candidate, then $|G| \in \{66, 68, 70, 72, 74, 75, 76, 78, 80, 81, 82, 84, 86, 88, 90, 92, 93, 94, 96, 98, 99, 100, 102, 104, 105, 106, 108, 110, 111, 112, 114, 116, 117\}$.*

Definition 4. *([5],Definition 3.4) 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 $U_1 = U \setminus H$.*

Lemma 2.2. *Suppose G realizes $< 6, 6, 6 >$. If G has a subgroup H of index 2, then H realizes $< 3, 3, 3 >$.*

Proof. Suppose G realizes $< 6, 6, 6 >$ with 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 S_0,T_0 and U_0 has at least 3 elements, then H realizes $< 3, 3, 3 >$. □

Lemma 2.3. *([3],Lemma 3.6) Suppose G has a TPP triple (S,T,U). Let H be an abelian subgroup of index 2 in G. Then the following hold.*
a)$|S_0^{-1}T_0U_0| = |S_0||T_0||U_0|$;
b)$|S_1^{-1}T_1U_0| \geq |S_1||T_1|$;

c)$|S_1^{-1}U_1| = |S_1||U_1|$;
d)$S_0^{-1}T_0U_0 \cap S_1^{-1}T_1U_0 = \emptyset$;
e)$S_0^{-1}T_0U_0 \cap S_1^{-1}U_1T_0 = \emptyset$;
f)$S_1^{-1}T_1U_0 \cap S_1^{-1}U_1T_0 = \emptyset$.

Lemma 2.4. *If G realizes* $< 6,6,6 >$ *and* $|G| < 90$*,then G has no abelian subgroups of index 2.*

Proof. Suppose G has an abelian subgroup H of index 2 and realizes $< 6,6,6 >$ via the TPP triple (S,T,U). Define $S_0, T_0, U_0, S_1, T_1, U_1$ as before. Then, as proved above, we may assume $|S_0| \geq 3$, $|T_0| \geq 3$ and $|U_0| \geq 3$. Without loss of generality we may assume that $|S_0| \geq |T_0|$ and $|S_0| \geq |U_0|$.Now since $|G| \leq 95$, then $|H| \leq 47$. From the last lemma, we have
$47 \geq |H| \geq |S_0^{-1}T_0U_0 \cup S_1^{-1}U_1T_0 \cup S_1^{-1}T_1U_0|$

$= |S_0||T_0||U_0| + |S_1^{-1}U_1T_0| + |S_1^{-1}T_1U_0| \qquad (3)$
$\geq |S_0||T_0||U_0| + |S_1||U_1| + |S_1||T_1|. \qquad (4)$
If $|U_0| \geq 4$, then $|H| \geq 64$,contradiction.So $|U_0| = 3$:
(a)$|U_0| = 3 = |T_0| = |S_0|$,then from (4)we have: $|H| \geq 45$,contradiction.

(b)$|U_0| = 3 = |T_0|$,$|S_0| = 4$,then from (4) we have:$|H| \geq 48$,contradiction.

(c)$|U_0| = 3$,$|T_0| = |S_0| = 4$,then from (4) we have $|H| \geq 58$,contradiction.

(d)$|U_0| = 3 = |T_0|$,$|S_0| = 5$,then from (4) we have $|H| \geq 51$,contradiction.

(e)$|U_0| = 3$,$|T_0| = 4$,$|S_0| = 5$,then from (4) we have $|H| \geq 65$,contradiction.

(f)$|U_0| = 3$,$|T_0| = |S_0| = 5$, then from (4) we have $|H| \geq 79$,contradiction.

(g)$|U_0| = 3 = |T_0|$,$|S_0| = 6$,then from (4) we have $|H| \geq 54$,contradiction.

(h)$|U_0| = 3, |T_0| = 4, |S_0| = 6$,then from (4) we have $|H| \geq 72$, contradiction.

(i)$|U_0| = 3, |T_0| = 5, |S_0| = 6$,then from (4) we have $|H| \geq 90$,contradiction.

(j)$|U_0| = 3, |T_0| = |S_0| = 6$,then from (4) we have $|H| \geq 108$,contradiction. □

Remark 2.4. *Up to now,among groups of order* ≤ 89*, we have these 56 left for C1 candidates:*
(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).

Theorem 2.5. *([5],Theorem 1.8) Suppose G realizes* $< n,m,p >$ *and the character degrees of G are* $\{d_i\}$*. Then*
$(nmp)^{\omega/3} \leq \sum d_i^{\omega}$.

Proposition 2. *The above theorem yields a nontrivial bound on ω if and only if $(nmp)^{\omega/3} \geq \sum d_i^{\omega}$.*

Remark 2.5. *Since we are using the inequality stated in the proposition, in order to make ω nontrivial, we need to search for groups has $\sum d_i^{\omega} < 216$.*

Remark 2.6. *(GAP experiment) So up to now,with the help of GAP experiment,we have these 18 groups(listed in their GAP ID)*
left as C1 candidates when its order < 90:(72,3),(72,16),(72,20),(72,21),(72,22),(72,23),(72,24),(72,25),(72,42),(72,46),(72,47),(81,3),(81,4),(81,6),(81,12),(81,13),(81,14),(84,10).

References

[1] Charles- Eric Drevet, Md. Nazrul Islam, and ‘ Eric Schost. Optimization techniques for small matrix multiplication.Theoretical Computer Science 412(22):219C2236, 2011

[2] Alexey Pospelov. Group-Theoretic Lower Bounds for the Complexity of Matrix Multiplication. In Theory and Applications of Models of Computation, volume 6648 of Lecture Notes in Comput. Sci., pages 2C13. Springer,Heidelberg, 2011.

[3] Sarah Hart, Ivo Hedtke, Matthias Meuller-Hannemann and Sandeep Murthy. A Fast Search Algorithm for $< m, m, m >$ Triple Product Property Triples and An Application for 5 5 Matrix Multiplication. arXiv:1305.0448v1 [math.GR] 1 May 2013.

[4] Peter M. Neumann. A note on the triple product property for subsets of finite groups. LMS J. Comput. Math., 14:232C237, 2011.

[5] Henry Cohn, Robert Kleinberg, Balazs Szegedy, and Christopher Umans. Group-theoretic Algorithms for Matrix Multiplication. pages 379C388, Los Alamitos, CA, USA, 2005. IEEE Computer Society.