

A note on the triple product property for subsets of finite groups

Peter M. Neumann

ABSTRACT

The triple product property (TPP) for subsets of a finite group was introduced by Henry Cohn and Christopher Umans in 2003 as a tool for the study of the complexity of matrix multiplication. This note records some consequences of the simple observation that if (S_1, S_2, S_3) is a TPP triple in a finite group G , then so is (dS_1a, dS_2b, dS_3c) for any $a, b, c, d \in G$.

Let $s_i := |S_i|$ for $1 \leq i \leq 3$. First we prove the inequality $s_1(s_2 + s_3 - 1) \leq |G|$ and show some of its uses. Then we show (something a little more general than) that if G has an abelian subgroup of index v , then $s_1s_2s_3 \leq v^2|G|$.

1. Introduction

Throughout this note, G will denote a non-trivial finite group, n will be its order $|G|$, and S_1, S_2, S_3 will be subsets of sizes s_1, s_2, s_3 , respectively. Our interest is in the triple product property (TPP) defined by Cohn and Umans in their lovely paper [1]. For any subset $S \subseteq G$, let $Q(S)$ denote the (right) quotient set of S :

$$Q(S) := \{x_1x_2^{-1} \mid x_1, x_2 \in S\}.$$

Then (S_1, S_2, S_3) is said to be a TPP triple (or to have the triple product property) if

$$q_1 \in Q(S_1), q_2 \in Q(S_2), q_3 \in Q(S_3) \text{ and } q_1q_2q_3 = 1 \implies q_1 = q_2 = q_3 = 1.$$

I shall speak of the group G realising the parameter triple (or, simply, abusing language a little, the parameters) (s_1, s_2, s_3) . In this language (which is slightly different from that of Cohn and Umans) the first two lemmas of [1] are:

if the group G realises the triple (s_1, s_2, s_3) , then it realises any permutation of this triple;

if groups A and B realise triples (s_1, s_2, s_3) and (t_1, t_2, t_3) , respectively, then any extension of A by B realises the triple (s_1t_1, s_2t_2, s_3t_3) .

At the end of their Lemma 3.1, Cohn and Umans also pointed out that:

if the group G is abelian and (S_1, S_2, S_3) is a TPP triple, then the multiplication map $S_1 \times S_2 \times S_3 \rightarrow G$ must be injective and therefore $s_1s_2s_3 \leq n$.

We define $\beta(G)$ to be the maximum of $s_1s_2s_3$ over parameters (s_1, s_2, s_3) of TPP triples in G (in the context of the applications described by Cohn and Umans, such triples do better than others). We will call this the TPP *capacity* of G . The triple $(G, \{1\}, \{1\})$ guarantees that $\beta(G) \geq n$ (with equality if G is abelian); it is not hard to see that $\beta(G) < n^{3/2}$ (see [1, Lemma 3.1]). Related to the TPP capacity is the ratio $\beta(G)/n$, which I will denote $\rho(G)$ and call the TPP *ratio* of G . The pseudo-exponent $\alpha(G)$ of [1, Definition 3.1] is related to the TPP capacity by the equation $\alpha(G) = 3 \log n / \log \beta(G)$ (and this makes sense, since we have assumed that $n > 1$).

Briefly, the relevance of TPP triples in G and the pseudo-exponent $\alpha(G)$ to the computational complexity of matrix multiplication is this (see [1, Theorem 2.3]). Let A and B be $m \times p$ and

Received 17 June 2010; revised 13 December 2010.

2000 *Mathematics Subject Classification* 20D60 (primary), 68R05 (secondary).

$p \times q$ matrices respectively over a field F , and let $C := AB$, so that C is an $m \times q$ matrix over F . Suppose that G has a TPP triple (S_1, S_2, S_3) of subsets as above, where $s_1 = m, s_2 = p, s_3 = q$. The rows and columns of A may be indexed by S_1 and S_2 respectively, those of B by S_2 and S_3 , and those of C by S_1 and S_3 . Thus $A = (a_{st})_{s \in S_1, t \in S_2}, B = (b_{tu})_{t \in S_2, u \in S_3}$, and $C = (c_{su})_{s \in S_1, u \in S_3}$, where $c_{su} = \sum_{t \in S_2} a_{st}b_{tu}$. In the group algebra FG let

$$\bar{A} := \sum_{s \in S_1, t \in S_2} a_{st}s^{-1}t, \quad \bar{B} := \sum_{t \in S_2, u \in S_3} b_{tu}t^{-1}u.$$

As is easily checked, the TPP property of (S_1, S_2, S_3) implies that $\bar{A}\bar{B} = \sum_{g \in G} \lambda(g)g \in FG$, where $\lambda(s^{-1}u) = c_{su}$ for $s \in S_1, u \in S_3$. Therefore (see [1, Theorem 2.3]), one can read off the matrix product from the group algebra product by looking at the coefficients of $s^{-1}u$ with $s \in S_1, u \in S_3$. Now suppose that F is algebraically closed and of characteristic 0. Let d_1, d_2, \dots, d_k be the degrees of the irreducible matrix representations of G over F . By standard theorems of Maschke and Wedderburn (building on ingredients supplied by Molien, Frobenius, Burnside, Schur and others — see [3]), there is an isomorphism

$$\Phi : FG \rightarrow \bigoplus_{i=1}^k M_{d_i}(F),$$

where $M_d(F)$ is the algebra of $d \times d$ matrices over F . If

$$\Phi(\bar{A}) = \sum_{i=1}^k \bar{A}_i, \quad \Phi(\bar{B}) = \sum_{i=1}^k \bar{B}_i, \quad \Phi(\bar{A}\bar{B}) = \sum_{i=1}^k \bar{C}_i$$

(where $\bar{A}_i, \bar{B}_i, \bar{C}_i \in M_{d_i}(F)$), then $\bar{A}_i\bar{B}_i = \bar{C}_i$ for $1 \leq i \leq k$. Thus, if $R(m, p, q)$ denotes the minimum number of numerical multiplications required to effect the matrix multiplication $A \times B$ (so that certainly $R(m, p, q) \leq mpq$), and $R(d) := R(d, d, d)$, then, using Φ^{-1} and picking out coefficients of elements $s^{-1}u$ as above, we see that

$$R(m, p, q) \leq \sum_{i=1}^k R(d_i).$$

In particular, since $R(d_i) \leq d_i^3$, if $\sum d_i^3 < mpq$, then, once an isomorphism Φ has been pre-calculated, it would be possible to multiply $m \times p$ and $p \times q$ matrices with fewer than mpq numerical multiplications.

Thus (in considerably simplified form), the Cohn–Umans strategy is to find (if possible — and that this is possible is proved in [2]) groups for which the TPP capacity satisfies $\beta(G) \ll \delta'(G)$, where $\delta'(G) := \sum R(d_i)$ or, perhaps more simply but less usefully, $\beta(G) \ll \delta(G)$, where $\delta(G) := \sum d_i^3$. More precisely, for non-abelian G define $\gamma(G)$ by the equation $n = d_{\max}(G)^{\gamma(G)}$, where $d_{\max}(G) := \max\{d_i \mid 1 \leq i \leq k\}$. Then certainly $\gamma(G) > 2$. If $\alpha(G) < \gamma(G)$, then for the exponent ω of matrix multiplication one has $\omega \leq \alpha(G)(\gamma(G) - 2)/(\gamma(G) - \alpha(G))$ (see [1, Corollary 4.2]). What is wanted therefore is groups G for which the right side of this inequality is as small as possible. The ideal would be to get it close to 2. This would require $\alpha(G)$ to be only slightly larger than 2 and $(\gamma(G) - 2)/(\gamma(G) - \alpha(G))$ to be only slightly larger than 1. Thus it requires a balancing act: we need groups G where $\beta(G) = n^{\frac{3}{2} - \varepsilon_1}$ and $d_{\max}(G) = n^{\frac{1}{2} - \varepsilon_2}$ with $\varepsilon_1, \varepsilon_2$ small and positive; the condition that $\alpha(G) < \gamma(G)$ requires that $\varepsilon_1 < 3\varepsilon_2$; moreover, the bound for ω can be cast in the form $(1 - \varepsilon_1/3\varepsilon_2)\omega \leq 2$, and therefore we want $\varepsilon_1/\varepsilon_2$ to be small.

In this note we leave the representation theory and the applications to the complexity of matrix multiplication to one side (though both are implicit in one form or another). Our aim is merely to record the following very simple observation and some more-or-less immediate consequences of it. The first consequence has as a corollary a bound for $\beta(G)$ that slightly

improves the bound $\beta(G) < n^{3/2}$ due to Cohn and Umans. The second has as a consequence the fact that if G has an abelian subgroup of index v then $\beta(G) \leq v^2n$, which may be compared with the simple fact that if G has an abelian subgroup of index v then $d_{\max}(G) \leq v$.

2. An elementary observation

OBSERVATION 2.1. *Let (S_1, S_2, S_3) be a TPP triple in the group G . If $a, b, c, d \in G$, then (dS_1a, dS_2b, dS_3c) is a TPP triple in G .*

That (S_1a, S_2b, S_3c) is a TPP triple is immediate since $Q(Sg) = Q(S)$ for any $S \subseteq G$ and any $g \in G$. Also, $(S_1^\alpha, S_2^\alpha, S_3^\alpha)$ is a TPP triple for any $\alpha \in \text{Aut } G$, and so $(dS_1d^{-1}, dS_2d^{-1}, dS_3d^{-1})$ is a TPP triple, and therefore so is (dS_1, dS_2, dS_3) .

We will call the TPP triple (S_1, S_2, S_3) *basic* if $1 \in S_1 \cap S_2 \cap S_3$. It is an immediate corollary of the above proposition that any TPP triple is translation-equivalent to a basic one. Note that if (S_1, S_2, S_3) is a basic TPP triple, then so is any one of the triples obtained by permutation of its entries. Note also that if (S_1, S_2, S_3) is a basic TPP triple and $i \neq j$, then $S_i \cap S_j = \{1\}$.

3. Inequalities

Our first application of Observation 2.1 is to the proof of some simple inequalities.

OBSERVATION 3.1. *Let (s_1, s_2, s_3) be the parameters of a TPP triple in G . Then*

$$s_1(s_2 + s_3 - 1) \leq n, \quad s_2(s_1 + s_3 - 1) \leq n \quad \text{and} \quad s_3(s_1 + s_2 - 1) \leq n.$$

Proof. By Observation 2.1, any TPP triple with parameters (s_1, s_2, s_3) is translation-equivalent to a basic TPP triple (S_1, S_2, S_3) with the same parameters. I claim that the map $S_1 \times (S_2 \cup S_3) \rightarrow G$ given by $(s, x) \mapsto s^{-1}x$ is injective. Suppose that $s_1, s_2 \in S_1$, $x_1, x_2 \in S_2 \cup S_3$, and $s_1^{-1}x_1 = s_2^{-1}x_2$, that is, $s_2s_1^{-1}x_1x_2^{-1} = 1$. If x_1, x_2 both lie in S_2 , then we choose $z \in S_3$ and write this equation as $s_2s_1^{-1}x_1x_2^{-1}zz^{-1} = 1$; if x_1, x_2 both lie in S_3 , then we choose $y \in S_2$ and write the equation as $s_2s_1^{-1}yy^{-1}x_1x_2^{-1} = 1$; if (without loss of generality) $x_1 \in S_2$ and $x_2 \in S_3$, then we define $y := 1 \in S_2$ and $z := 1 \in S_3$ (possible since the triple is assumed to be basic) and write the equation as $s_2s_1^{-1}x_1y^{-1}zx_2^{-1} = 1$. In all cases, it follows that $s_2 = s_1$ and $x_2 = x_1$, and so the map described above is injective, as was claimed.

Then $|S_1(S_2 \cup S_3)| = s_1(s_2 + s_3 - 1)$, and so $s_1(s_2 + s_3 - 1) \leq |G| = n$. The other two inequalities follow by cyclic permutation of the members of the TPP triple.

EXAMPLES. It is easy to see from these inequalities that if $n = 60$, then $\beta(G) \leq 180$. There is a TPP triple with parameters $(5, 5, 5)$ in the alternating group $\text{Alt}(5)$, namely

$$S_1 := \langle (1\ 2\ 3\ 4\ 5) \rangle, \quad S_2 := \langle (1\ 3\ 4\ 5\ 2) \rangle, \quad S_3 := \langle (1\ 2\ 4) \cup \langle (3\ 4\ 5) \rangle \rangle,$$

and therefore $\beta(\text{Alt}(5)) \geq 125$. It would be interesting to know if there are triples with parameters $(6, 6, 4)$, $(6, 5, 5)$, or $(6, 6, 5)$ in $\text{Alt}(5)$ — or, indeed, in any other group of order 60. Mr Sandeep Murthy has attempted to compute the answers, but he has found his search space too large. For example, even for the ‘smallest’ case $(6, 6, 4)$, where one may assume using Observation 2.1 that (S_1, S_2, S_3) is basic, and moreover that $|S_1 \cap \text{Alt}(4)| \geq 2$ and $|S_2 \cap \text{Alt}(4)| \geq 2$, the search space has size several times larger than the set of all disjoint triples of subsets of sizes 4, 4, 3 in a set of size 48, and even a very crude back-of-an envelope estimate shows this to be larger than 10^{14} .

The inequalities of Observation 3.1 tell us that if G is a group that realises the parameter triple $(5, 5, 5)$, then $n \geq 45$. Groups of orders 45, 47, 49, 51, 53, and 59 are abelian, so cannot realise $(5, 5, 5)$. Groups of orders 46 and 50 have an abelian subgroup of index 2 and in

these cases it is easy to see that there can be no TPP triple with parameters (5, 5, 5). Thus, the smallest n such that there is a group of order n realising the triple (5, 5, 5) is one of 48, 52, 54, 55, 56, 57, 58, and 60. It could be quite interesting to pin it down precisely.

COROLLARY 3.2. *For any finite group G (of order n , recall) the TPP capacity satisfies*

$$\beta(G) \leq \left(\frac{1 + \sqrt{1 + 8n}}{4} \right)^3.$$

Proof. Let (m, p, q) be the parameters of a TPP triple of subsets of G such that $\beta(G) = mpq$. From the proposition, we know that

$$m(p + q - 1) \leq n, \quad p(m + q - 1) \leq n, \quad q(m + p - 1) \leq n.$$

Consider the following optimisation problem:

for a given real number $d > 3$, find real numbers a, b, c maximising the product abc subject to the six constraints $a \geq 1, b \geq 1, c \geq 1$, and

$$a(b + c - 1) \leq d, \quad b(a + c - 1) \leq d, \quad c(a + b - 1) \leq d.$$

I claim that its solution is $a = b = c = x$, where $x(2x - 1) = d$.

Without loss of generality, we may suppose that $a \geq b \geq c \geq 1$. Suppose for the moment that $b > c$. Let $h := \frac{1}{2}(b - c)$ and consider the triple $(a, b - h, c + h)$, that is $(a, \frac{1}{2}(b + c), \frac{1}{2}(b + c))$. It is clear that this satisfies the first four of the constraint inequalities. Furthermore,

$$\frac{1}{2}(b + c)(a + \frac{1}{2}b + \frac{1}{2}c - 1) - b(a + c - 1) = \frac{1}{4}(b - c)(b - c - 2a + 2) < 0,$$

since $b + 2 < 2a + c$. Therefore, $\frac{1}{2}(b + c)(a + \frac{1}{2}b + \frac{1}{2}c - 1) < b(a + c - 1) \leq d$ and so it satisfies also the fifth and sixth inequalities. But $\frac{1}{4}a(b + c)^2 > abc$ by the AM-GM Inequality. What this shows is that if $b > c$, then the product abc is not maximised. Thus, to maximise, we require that $b = c$ (given the assumption that $a \geq b \geq c$). Now a very similar proof shows that to maximise abc , we require that $a = b = c$. And then, if $x := a = b = c$, we maximise abc provided that we maximise x subject to the condition that $x(2x - 1) \leq d$. This of course requires that $x(2x - 1) = d$.

We have now shown that if x is the positive root of the equation $x(2x - 1) = n$, then $\beta(G) \leq x^3$. Thus,

$$\beta(G) \leq \left(\frac{1 + \sqrt{1 + 8n}}{4} \right)^3,$$

as the lemma states.

Crudely, the corollary tells us that $\beta(G) \leq (\frac{1}{2}n)^{3/2} + O(n)$, which is a small improvement on the observation by Cohn and Umans that $\beta(G) < n^{3/2}$ (see [1, Proof of Lemma 3.1]).

The equality $s_1(s_2 + s_3 - 1) = n$ can certainly hold. The above analysis shows, however, that if (S_1, S_2, S_3) is *proper* in the sense that $\min\{s_1, s_2, s_3\} \geq 2$, then it would require that $s_1 = \max\{s_1, s_2, s_3\}$. We assume in what follows that our TPP triple is proper.

EXAMPLES. The dihedral group of order $6k$ has a TPP triple with parameters $(2k, 2, 2)$ (see [1, Proposition 7.6]) for which equality holds.

The three subgroups $\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 2)(3\ 4)\rangle$ in $\text{Alt}(4)$ form a TPP triple with parameters $(3, 3, 2)$ for which equality holds.

Let $G := \text{Sym}(\Omega)$, where $\Omega := [1..m]$, choose $k \in \Omega$ such that $2 \leq k \leq m - 1$, let $S := \text{Stab}(k)$, the stabiliser of k , let $T := \langle(1\ 2 \dots k)\rangle$, and let $U := \langle(k\ k + 1 \dots m)\rangle$. Then (S, T, U) is a TPP triple in G . To see this, note that since S, T, U are subgroups the TPP condition is simply that if $stu = 1$ with $s \in S, t \in T, u \in U$, then $s = t = u = 1$. (Although 1 is being used both as a member of $[1..m]$ and as the identity in the group G , the context should make

clear which meaning is relevant at each point.) Then $ks = k$ and so $kst = kt = r$ for some $r \in \Omega$ in the range $1 \leq r \leq k$. If $r < k$ then $ru = r$ and so $k = kstu = r$, which is false. Thus $r = k$. This entails that $kt = k$ and so $t = 1$. Then $su = 1$, so $k = ksu = ku$, whence $u = 1$, so also $s = 1$. Therefore, (S, T, U) is a TPP triple, as claimed. Its parameters are $((m - 1)!, k, m - k + 1)$ and so for this triple we have the equality $s_1(s_2 + s_3 - 1) = m! = n$.

This last example is essentially due to Mr Sandeep Murthy, who showed me the case $m = 5$. It is rather disturbing. I had hoped that there might exist some number m such that if $\min\{s_1, s_2, s_3\} \geq m$ then it would be the case that $s_1(s_2 + s_3) \leq n$. The example shows this conjecture to be false. I suspect however that stronger inequalities than those of Observation 3.1 should be true when $\min\{s_1, s_2, s_3\}$ and $\max\{s_1, s_2, s_3\}$ are not too far apart. Or, perhaps, if $s_1s_2s_3 > n \log n$. For example, it seems quite possible that under some such condition the inequalities

$$s_1(s_2 + s_3) \leq n, \quad s_2(s_1 + s_3) \leq n \quad \text{and} \quad s_3(s_1 + s_2) \leq n$$

should hold. Although only a very small improvement on Observation 3.1, this would probably be worth having (if it is true), since its proof should involve insights leading to more significant advances. It would immediately lead to the bound $\beta(G) \leq (\frac{1}{2}n)^{3/2}$ for sufficiently large n ($n > 30$ would almost certainly suffice), which, though not a great improvement on the bound given above, is at least a little more agreeable.

4. Subgroups of small index

Observation 2.1 may also be used to derive a relationship between the TPP capacity of the group G and that of a subgroup H .

OBSERVATION 4.1. *Let H be a subgroup of the finite group G and let $v := |G : H|$. Then $\beta(G) \leq v^3\beta(H)$. Consequently, for the TPP ratios we have $\rho(G) \leq v^2\rho(H)$.*

Proof. Let (S, T, U) be a TPP triple in G with parameters (m, p, q) such that $\beta(G) = mpq$. Let the distinct right cosets of H in G be H, Hx_2, \dots, Hx_v . By Observation 2.1 we may independently right-translate each of S, T, U as necessary and assume that

$$|S \cap H| \geq |S \cap Hx_i|, \quad |T \cap H| \geq |T \cap Hx_i|, \quad |U \cap H| \geq |U \cap Hx_i|$$

for $1 \leq i \leq v$. Let $S_1 := S \cap H$, $T_1 := T \cap H$, $U_1 := U \cap H$, and let $m_1 := |S_1|, p_1 := |T_1|, q_1 := |U_1|$. Then (S_1, T_1, U_1) is a TPP triple of subsets of H with parameters (m_1, p_1, q_1) . Now

$$m = |S| = \sum_{i=1}^v |S \cap Hx_i| \leq v|S \cap H|,$$

that is, $m \leq vm_1$. Similarly, $p \leq vp_1$ and $q \leq vq_1$. Therefore,

$$\beta(G) = mpq \leq v^3m_1p_1q_1 \leq v^3\beta(H),$$

as required.

Translating this into a statement about the TPP ratio of the groups in question, we see that

$$\rho(G) = \frac{\beta(G)}{|G|} \leq \frac{v^3\beta(H)}{v|H|} = v^2\rho(H),$$

as claimed.

COROLLARY 4.2. *If there is an abelian subgroup H of index v in the finite group G (whose order, recall, is n), then $\beta(G) \leq v^2n$ and $\rho(G) \leq v^2$.*

For, by the observation at the end of the proof of Lemma 3.1 in [1], since H is abelian $\beta(H) = |H|$ and $\rho(H) = 1$.

In [2, Section 2] Cohn, Kleinberg, Szegedy and Umans exhibited a TPP triple with parameters $(2m(m - 1), 2m(m - 1), 2m(m - 1))$ in a wreath product $G := A \text{ wr } C_2$, where A is an abelian group of order m^3 . Here G has an abelian subgroup $A \times A$ of order m^6 and index $v = 2$ and their triple shows that

$$\rho(G) \geq \frac{(2m(m - 1))^3}{2m^6} = 4 \left(1 - \frac{1}{m}\right)^3,$$

which is very close to v^2 for large values of m . Taking direct products of these groups, we can create examples with arbitrarily large index v and $\rho(G)$ arbitrarily close to v^2 .

In practice, for the purposes that Cohn and Umans had in mind, Corollary 4.2 is unlikely to be of much help. For, in the notation of page 233, to get a bound for ω (the exponent of matrix multiplication) of the form $\omega < 2 + \varepsilon$ with ε small, we would want $d_{\max}(G) = n^{\frac{1}{2} - \varepsilon_2}$, where ε_2 is small. If G has an abelian subgroup of index v then $d_{\max}(G) \leq v$, so $v \geq n^{\frac{1}{2} - \varepsilon_2}$, and then $v^2 n \geq n^{2(1 - \varepsilon_2)}$, so that (since we know already that $\beta(G) < n^{3/2}$) the bound $\beta(G) \leq v^2 n$ would tell us nothing.

Acknowledgements. I am very grateful to Mr Sandeep Murthy who first drew my attention to the papers [1, 2], who pointed out some errors in an earlier draft of this paper, and who inspired the example at the end of Section 3. I am grateful also to an anonymous referee for two helpful suggestions.

References

1. HENRY COHN and CHRISTOPHER UMANS, ‘A group-theoretic approach to fast matrix multiplication’, *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS’03)* (IEEE, 2003) 438–449.
2. HENRY COHN, ROBERT KLEINBERG, BALÁZS SZEGEDY and CHRISTOPHER UMANS, ‘Group-theoretic algorithms for matrix multiplication’, *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS’05)* (IEEE, 2005) 379–388.
3. CHARLES W. CURTIS, *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*, AMS–LMS Series on History of Mathematics 15 (American Mathematical Society, 1999).

Peter M. Neumann
 The Queen’s College
 Oxford OX1 4AW
 United Kingdom

peter.neumann@queens.ox.ac.uk