A NOTE ON THE GROUP-THEORETIC APPROACH TO
FAST MATRIX MULTIPLICATION

IVO HEDTKE

Abstract. In 2003 Cohn and Umans introduced a group-theoretic approach to fast
matrix multiplication. This involves finding large subsets \( S, T \) and \( U \) of a group \( G \)
satisfying the Triple Product Property (TPP) as a means to bound the exponent \( \omega \) of
the matrix multiplication. We show that \( S, T \) and \( U \) may be be assumed to contain
the identity and be otherwise disjoint. We also give a much shorter proof of the upper
bound \(|S| + |T| + |U| \leq |G| + 2\).

1. Introduction

The naive algorithm for matrix multiplication is an \( \mathcal{O}(n^3) \) algorithm. From Volker
Strassen ([5]) we know that there is an \( \mathcal{O}(n^{2.81}) \) algorithm for this problem. Winograd
optimized Strassen’s algorithm. While the Strassen-Winograd algorithm
is the variant that is always implemented (for example in the famous GEMMW pack-
age), there are faster ones (in theory) that are impractical to implement. The fastest
known algorithm runs in \( \mathcal{O}(n^{2.376}) \) time (see [3] from Don Coppersmith and Shmuel
Winograd). Most researchers believe that an optimal algorithm with \( \mathcal{O}(n^2) \) runtime
exists, but since 1987 no further progress was made in finding one.

Because modern architectures have complex memory hierarchies and increasing par-
allelism, performance has become a complex tradeoff, not just a simple matter of
counting flops. Algorithms which make use of this technology were described in [1]
by D’Alberto and Nicolau. An also well known method is Tiling: The normal
algorithm can be speeded up by a factor of two by using a six loop implementation that
blocks submatrices so that the data passes through the L1 Cache only once.

In 2003 COHN and UMANs introduced in [2] a group-theoretic approach to fast matrix
multiplication. The main idea is to embed the matrix multiplication over a ring $R$ into
the group ring $RG$, where $G$ is a (finite) group. A group $G$ admits such an embedding,
if there are subsets $S$, $T$ and $U$ which fulfill the so called *Triple Product Property*.

**Definition** (Right Quotient). Let $G$ be a group and $\emptyset \neq X \subseteq G$ be a nonempty subset
of $G$. The *right quotient* $Q(X)$ of $X$ is defined by $Q(X) := \{ xy^{-1} : x, y \in X \}$.

**Definition** (TPP). We say that the nonempty subsets $S$, $T$, and $U$ of a group $G$ fulfill
the *Triple Product Property* (TPP) if for $s \in Q(S)$, $t \in Q(T)$ and $u \in Q(U)$, $stu = 1$
holds iff $s = t = u = 1$.

COHN and UMANs found a way to bound the exponent $\omega$ of the matrix multiplication
with their framework. Therefore, for a fixed group $G$ we search for TPP triples $S$, $T$ and
$U$ which maximize $|S| \cdot |T| \cdot |U|$, for example with a brute force computer search. Here
one can use MURTHY’s upper bound (s. Corollary[6]) and our intersection condition (s.
Theorem[1]).

2. Results

We show that $S$, $T$ and $U$ may be be assumed to contain the identity and be otherwise
disjoint.

**Theorem 1.** If $S'$, $T'$ and $U'$ fulfill the TPP, then there exists a triple $S$, $T$ and $U$
with

$$|S| = |S'|, \quad |T| = |T'|, \quad |U| = |U'| \quad \text{and} \quad S \cap T = T \cap U = S \cap U = 1$$

which also fulfills the TPP.
For the proof of our main result we need some auxiliary results.

**Lemma 2.** Let $\emptyset \neq X \subseteq G$ be a nonempty subset of a group $G$ and $g \in G$. Then

1. $1 \in Q(X)$,
2. $g \in Q(X) \iff g^{-1} \in Q(X)$ and
3. $|X| \leq |Q(X)|$.

**Proof.** (1) Because $X \neq \emptyset$ there exists an $x \in X$ and so $1 = xx^{-1} \in Q(X)$ follows.

(2) If $g \in Q(X)$ then there are $x, y \in X$ with $g = xy^{-1}$. This implies, that $g^{-1} = (xy^{-1})^{-1} = yx^{-1} \in Q(X)$.

(3) For a fixed $x \in X$ the map $X \to Q(X)$, $y \mapsto yx^{-1}$ is injective and therefore $|X| \leq |Q(X)|$ holds. \hfill \Box

**Lemma 3.** If $S, T$ and $U$ fulfill the TPP then

$$Q(X) \cap Q(Y) = 1$$

holds for all $X \neq Y \in \{S, T, U\}$.

**Proof.** We know $1 \in Q(X) \cap Q(Y)$ from Lemma 2(1). Now assume that $|Q(X) \cap Q(Y)| \geq 2$. In this case there is an $1 \neq x \in Q(X) \cap Q(Y)$. From Lemma 2(2) we know, that $x^{-1} \in Q(X) \cap Q(Y)$, too. Moreover 1 is an element of every right quotient and therefore the factors $x, x^{-1}$ and 1 occur in $\{stu : s \in Q(S), t \in Q(T), u \in Q(U)\}$ and the TPP is not fulfilled. So we have $|Q(X) \cap Q(Y)| = 1$ which completes the proof. \hfill \Box

Theorem 4 and Corollary 6 below are originally due to Murthy (2009). Our proofs are somewhat shorter.

**Theorem 4** (Murthy’s minimal disjointness property). If $S, T$ and $U$ fulfill the TPP then

$$|X \cap Y| \leq 1$$

holds for all $X \neq Y \in \{S, T, U\}$. 
Proof. Assume that $|X \cap Y| \geq 2$. Then there are $x \neq y \in X \cap Y$. Therefore we have $1 \neq xy^{-1} \in Q(X) \cap Q(Y)$. This is a contradiction to Lemma 3.

Now we can prove our main result.

Proof of Theorem 4. We fix $s_0 \in S'$, $t_0 \in T'$ and $u_0 \in U'$. Now we define $S := \{ss_0^{-1} : s \in S'\}$ and $T$ and $U$ in the same way. Obviously $|S| = |S'|$, $|T| = |T'|$ and $|U| = |U'|$ holds. Because of

$$Q(S) = \{ss^{-1} : s, \tilde{s} \in S\} = \{ss_0^{-1}(\tilde{s}s_0^{-1})^{-1} : s, \tilde{s} \in S'\} = \{ss^{-1} : s, \tilde{s} \in S'\} = Q(S'),$$

$$Q(T) = Q(T')$$
and $Q(U) = Q(U')$ the triple $S$, $T$ and $U$ fulfill the TPP, too. It is also clear, that $1 \in S$, $1 \in T$ and $1 \in U$. The result now follows from Theorem 4.

Finally we can prove the upper bound of $|G| + 2$ for the additive size of a TPP triple.

**Theorem 5.** If $S$, $T$ and $U$ fulfill the TPP then $|Q(S)| + |Q(T)| + |Q(U)| \leq |G| + 2$.

**Proof.** Note that $Q(S) \cup Q(T) \cup Q(U) \subset G$ and

$$|Q(S) \cup Q(T) \cup Q(U)|$$

$$= |Q(S)| + |Q(T)| + |Q(U)| - |Q(S) \cap Q(T)| - |Q(T) \cap Q(U)| - |Q(S) \cap Q(U)|$$

$$+ |Q(S) \cap Q(T) \cap Q(U)|.$$

Because of Lemma 3 all intersections have size 1 and the statement follows.

**Corollary 6** (Murthy). If $S$, $T$ and $U$ fulfill the TPP then $|S| + |T| + |U| \leq |G| + 2$.

**Proof.** The statement follows from Lemma 3 and Theorem 5.

Note that Theorem 5 is more effective than Corollary 6 when searching for TPP triples.
Acknowledgements

I would like to thank David J. Green for our inspiring discussions.

References

[1] D’Alberto, P., Nicolau, A., 2009. Adaptive Winograd’s Matrix Multiplications. ACM Trans. Math. Softw. 36, 1, Article 3.

[2] Cohn, H., Umans, C., 2003. 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, pp. 438-449.

[3] Coppersmith, D., Winograd, S., 1987. Matrix Multiplication via Arithmetic Progressions. STOC ’87: Proc. of the nineteenth annual ACM symposium on Theory of Computing.

[4] Murthy, S., 2009. A Short Note on Disjointness Conditions for Triples of Group Subsets Satisfying the Triple Product Property. arXiv: 0908.3671

[5] Strassen, V., 1969. Gaussian Elimination is not Optimal. Numer. Math. 13:354–356.

Mathematical Institute, University of Jena, D-07737 Jena, Germany

E-mail address: Ivo.Hedtke@uni-jena.de