

# Research Proposal: Algebraic Methods for Fast Matrix Multiplication

Hendrik Orem

Faculty Advisor: Professor Michael Orrison

## 1 Introduction

An improvement upon the naive  $O(n^3)$  algorithm for matrix multiplication was first presented by Strassen, obtaining the result in only  $O(n^{2.81})$  field operations [5]. This raises the question of what the best possible exponent  $k$  such that matrix multiplication can be carried out in at most  $O(n^k)$  time is. Clearly  $k \geq 2$ , since  $n^2$  is the size of the output. It is believed that the optimal  $k$  is exactly equal to 2, but this has yet to be proven [3]. Presently, the fastest known algorithm computes the product of two matrices in at most  $O(n^{2.38})$  operations.

Recent work by Cohn and Umans indicates a possible path to proving that the obvious lower bound of 2 is tight, namely an approach using techniques from group theory and representation theory [3]. Their proposed algorithm is analogous to the way that the *Discrete Fourier Transform* (DFT) computes the product of two polynomials by embedding them in a cyclic group algebra over the complex numbers, then computing the pointwise product of vectors in the appropriate complex vector space. Since abelian groups cannot yield the properties necessary to achieve  $k = 2$ , it is instead necessary to embed the matrices in a nonabelian group algebra. This complicates multiplication in the Fourier domain; rather than being simply pointwise vector multiplication, it becomes multiplication of block-diagonal matrices with block sizes determined by the irreducible representations of the group.

## 2 Proposed Research

A condition which is sufficient to show that  $k = 2$  is presented in a recent paper by Cohn, Kleinberg, Szegedy and Umans [2]. In particular, the paper states,

For arbitrarily large  $n$ , there exists an abelian group  $H$  with  $n$  pairs of subsets  $A_i, B_i$  satisfying the simultaneous double product property such that  $|H| = n^{2+o(1)}$  and  $|A_i||B_i| \geq n^{2-o(1)}$ .

The simultaneous double product property is a statement about the relationship between the quotient sets of the pairs  $A_i$  and  $B_i$ . This conjecture results from a question raised in the original paper by Cohn and Umas [3], namely whether there exists a group with subsets of sizes  $m, n, p$  satisfying what is called the triple product property and with character degrees  $d_i$  such that

$$mnp > \sum_i d_i^3.$$

Their later paper answered this question in the affirmative and gave some constructions which yielded bounds on  $k$  as low as 2.41.

The 2005 paper cited above provides both a combinatorial and an algebraic perspective on the problem of constructing such subsets of nonabelian groups. I would like to investigate constructions of such groups, using techniques from representation theory to work on a possible improvement on the bound on  $k$ . My coursework in representation theory and algorithms, combined with my coding experience, puts me in a position to contribute to the study of algebraic techniques in fast matrix multiplication.

### 3 Prior Research

The algebraic approach to fast matrix multiplication algorithms was first proposed in a 2003 paper by Cohn and Umas [3]. This paper poses a representation-theoretic question, which was answered in 2005 [2], that allowed for algorithms of comparable speed to the current record of  $O(n^{2.38})$ . Their best bound results from finding three subsets of a wreath product group, where the subsets are described by a *Uniquely Solvable Puzzle* (USP).

An understanding of FFTs on noncommutative groups could be helpful in exploring the algebraic formulation of fast matrix multiplication, although the computation of the transform is not the bottleneck in matrix multiplication. Summaries of the subject can be found in [1], [4] and [6].

## References

- [1] M. Clausen and U. Baum. *Fast Fourier transforms*. Wissenschaftsverlag, 1993.
- [2] H. Cohn, R. Kleinberg, B. Szegedy, and C. Umans. Group-theoretic algorithms for matrix multiplication. *Foundations of Computer Science. 46th Annual IEEE Symposium on*, pages 23–25, 2005.
- [3] H. Cohn and C. Umans. A group-theoretic approach to fast matrix multiplication. *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 438–449, 2003.
- [4] E Malm. *Decimation-in-frequency Fast Fourier Transforms for the Symmetric Group*. Harvey Mudd College Mathematics Department, 2005.
- [5] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.
- [6] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, 1999.