Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# On the arithmetic complexity of Strassen-like matrix multiplications

Murat Cenk [a], M. Anwar Hasan [b]

[a] *Institute of Applied Mathematics, Middle East Technical University, 06800, Ankara, Turkey*
[b] *Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada*

ARTICLE INFO

*Article history:*
Received 9 May 2013
Accepted 3 June 2016
Available online xxxx

*Keywords:*
Fast matrix multiplication
Strassen-like matrix multiplication
Computational complexity
Cryptographic computations
Computer algebra

ABSTRACT

The Strassen algorithm for multiplying $2 \times 2$ matrices requires seven multiplications and 18 additions. The recursive use of this algorithm for matrices of dimension $n$ yields a total arithmetic complexity of $(7n^{2.81} - 6n^2)$ for $n = 2^k$. Winograd showed that using seven multiplications for this kind of matrix multiplication is optimal. Therefore, any algorithm for multiplying $2 \times 2$ matrices with seven multiplications is called a Strassen-like algorithm. Winograd also discovered an additively optimal Strassen-like algorithm with 15 additions. This algorithm is called the Winograd's variant, whose arithmetic complexity is $(6n^{2.81} - 5n^2)$ for $n = 2^k$ and $(3.73n^{2.81} - 5n^2)$ for $n = 8 \cdot 2^k$, which is the best-known bound for Strassen-like multiplications. This paper proposes a method that reduces the complexity of Winograd's variant to $(5n^{2.81} + 0.5n^{2.59} + 2n^{2.32} - 6.5n^2)$ for $n = 2^k$. It is also shown that the total arithmetic complexity can be improved to $(3.55n^{2.81} + 0.148n^{2.59} + 1.02n^{2.32} - 6.5n^2)$ for $n = 8 \cdot 2^k$, which, to the best of our knowledge, improves the best-known bound for a Strassen-like matrix multiplication algorithm.



*E-mail addresses:* mcenk@metu.edu.tr (M. Cenk), ahasan@uwaterloo.ca (M.A. Hasan).

http://dx.doi.org/10.1016/j.jsc.2016.07.004
0747-7171/

## 1. Introduction

Let $O(n^{\omega})$ be the complexity of multiplying two $n \times n$ matrices. An ordinary matrix multiplication algorithm requires $n^3$ multiplications and $(n^3 - n^2)$ additions, which means that, $\omega \leq 3$ for the ordinary method. Strassen (1969) showed that two $2 \times 2$ matrices can be multiplied with seven multiplications rather than eight. The recursive use of this algorithm yields $\omega \leq 2.81$. Pan (1978, 1980, 1984) used his trilinear aggregating techniques to obtain $\omega \leq 2.795$ and $\omega \leq 2.781$, respectively. In other work, Bini et al. (1979) presented approximation algorithms and produced one with $\omega \leq 2.7799$. Schönhage (1981) introduced the concept of disjoint matrix multiplication in 1981 and was able to obtain $\omega \leq 2.5479$. Strassen (1986) obtained $\omega \leq 2.4785$ by introducing a new method called the laser method, which was used by Coppersmith and Winograd (1990) in order to determine the well known bound $\omega \leq 2.376$. This upper bound has recently been reduced to $w \leq 2.374$ by Stothers (2010) and to $w \leq 2.373$ by Williams (2012) through the use of constructions similar to those of Coppersmith and Winograd. On the other hand, Cohn and Umans (2003) approached this problem by introducing a new group-theoretic approach. Cohn et al. (2005) also proposed several multiplication algorithms using this approach, but the bounds were no better than the Coppersmith–Winograd's results.

One of the algorithms most widely employed for practical applications is the algorithm that uses seven multiplications for multiplying $2 \times 2$ matrices, as proposed by Strassen (1969). Winograd (1971) proved the number of multiplications to be optimal. Thus, the algorithms using seven multiplications for $2 \times 2$ matrix multiplications are called Strassen-like algorithms. In Probert (1976), it was shown that the optimal number of additions in a Strassen-like algorithm is 15, and Winograd proposed such an algorithm that uses seven multiplications and 15 additions. This algorithm is called Winograd's variant. Strassen-like algorithms provide greater efficiency for sizes in practical use than other algorithms that have better matrix exponent because of the hidden factor in big-O notation. It should be noted that Pan's trilinear aggregation techniques (Pan, 1978, 1980) also yield practical algorithms. For example, Kaporin (2004) worked on Pan's techniques and compared their complexities with that of the Winograd's variant. He reported that Pan's techniques yield an arithmetic complexity of $(4.894n^{2.7760} - 16.16n^2)$ for $n = 18 \cdot 48^k$ and that this complexity provides a computational time comparable to that produced by Strassen-like algorithms for matrices of medium-large size, $2000 \leq n \leq 10000$.

There are various works on the practical aspects of Strassen-like algorithms. In Huss-Lederman et al. (1996), an efficient and portable Strassen's matrix multiplication algorithm was studied. It was reported that Strassen's algorithm outperforms the standard algorithm for practically used sizes. The use of Strassen's algorithm in practical applications was also discussed in Cohen and Roth (1976), Bailey (1988) and Douglas et al. (1994). Counting the number of arithmetic operations and memory allocations were studied in Boyer et al. (2009) in which several new schedules for Strassen–Winograd's algorithm were proposed and it was shown how the extra memory allocation requirement could be reduced. In addition, matrix computations over finite fields can be found in Albrecht et al. (2010), Dumas et al. (2002, 2008, 2004), and a Strassen-like algorithm for chain products and matrix squaring with better complexity was proposed in Bodrato (2010).

The work presented in this paper deals with the arithmetic complexity of widely used Strassen-like algorithms such as ones found in cryptographic computations (Joux, 2009; Bard, 2009), in which the matrices are generally over finite fields and no stability problems exist. For this study, the-best known Strassen-like arithmetic complexities have been decreased from $(6n^{2.81} - 5n^2)$ to $(5n^{2.81} + 0.5n^{2.59} + 2n^{2.32} - 6.5n^2)$ for $n = 2^k$ and from $(3.73n^{2.81} - 5n^2)$ to $(3.55n^{2.81} + 0.148n^{2.59} + 1.02n^{2.32} - 6.5n^2)$ for $n = 8 \cdot 2^k$, i.e., when the algorithm is stopped at the point when the size of matrices becomes eight and then the ordinary method is applied. To the best of our knowledge, this is the first time a technique which improves the best known arithmetic complexity for the Strassen-like matrix multiplication has been proposed.

**Notation and model of computation:** The matrices that appear throughout the paper are over an arbitrary ring $\mathcal{R}$. The dimension of matrices is shown by $n$ and $n = 2^k$ is assumed for a positive integer $k$. $M_{\otimes}(n)$ and $M_{\oplus}(n)$ denote the number of multiplications and additions/subtractions in $\mathcal{R}$ needed for multiplying $n \times n$ matrices over $\mathcal{R}$, respectively. The total arithmetic cost, i.e. the sum

Please cite this article in press as: Cenk, M., Hasan, M.A. On the arithmetic complexity of Strassen-like matrix multiplications. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.07.004