LOWER BOUNDS FOR THE MULTIPlicative COMPLEXITY OF MATRIX MULTIPLICATION

MARKUS BLÄSER

Abstract. We prove a lower bound of \( km + mn + k - m + n - 3 \) for the multiplicative complexity of the multiplication of \( k \times m \)-matrices with \( m \times n \)-matrices using the substitution method.

Key words. Matrix multiplication, multiplicative complexity, lower bound, substitution method

Subject classifications. 68Q20, 68Q25.

1. Introduction

In this work we prove a lower bound for the multiplicative complexity of the multiplication of \( k \times m \)-matrices with \( m \times n \)-matrices. Roughly speaking, our problem is the following: Given two matrices

\[
X = \begin{pmatrix}
x_{1,1} & x_{1,2} & \cdots & x_{1,m} \\
x_{2,1} & x_{2,2} & \cdots & x_{2,m} \\
\vdots & \vdots & & \vdots \\
x_{k,1} & x_{k,2} & \cdots & x_{k,m}
\end{pmatrix}, \quad Y = \begin{pmatrix}
y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\
y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\
\vdots & \vdots & & \vdots \\
y_{m,1} & y_{m,2} & \cdots & y_{m,n}
\end{pmatrix}
\]

with indeterminates \( x = \{x_{1,1}, \ldots, x_{k,m}\} \) and \( y = \{y_{1,1}, \ldots, y_{m,n}\} \) over a given field \( F \), how many multiplications are necessary to compute the product \( XY \), i.e., the bilinear forms

\[
f_{k,\nu} = \sum_{\mu=1}^{m} x_{\kappa,\mu} y_{\mu,\nu}, \quad 1 \leq \kappa \leq k, \ 1 \leq \nu \leq n.
\]

More precisely, we want to know how many products

\[
p_{\lambda} = u_{\lambda}(x, y)v_{\lambda}(x, y), \quad 1 \leq \lambda \leq l,
\]
of linear forms \( u_\lambda, v_\lambda \in F[x, y] \) are necessary such that every \( f_{\kappa,\nu} \) can be written as

\[
f_{\kappa,\nu} = \sum_{\lambda=1}^{l} \omega_{\kappa,\nu,\lambda} p_\lambda \quad \text{with scalars } \omega_{\kappa,\nu,\lambda} \in F.
\]

The best lower bound so far is due to Lafon & Winograd (1978). They show that \( km + mn - m + n - 1 \) multiplications of the above form are necessary to compute the product of a \( k \times m \)-matrix with an \( m \times n \)-matrix, if \( k \geq 2 \).

Their main tool for proving this bound is the so-called substitution method introduced by Pan (1966). As a second tool they use the so-called sandwiching to normalize the products \( p_\lambda \) in a certain way.

Using a result from algebraic geometry, we conclude that the products \( p_\lambda \) can be further normalized and prove that \( km + mn + k - m + n - 3 \) multiplications are necessary to compute the product of a \( k \times m \)-matrix with an \( m \times n \)-matrix, if \( n \geq k \geq 2 \).

2. Matrix multiplication and complexity

To fix the model of computation, let \( F \) be a field and let \( \mathbf{x} = \{x_1, \ldots, x_k\} \) be a set of indeterminates over \( F \). If \( G = \{g_1, \ldots, g_n\} \subseteq F(\mathbf{x}) \), then the multiplicative complexity of \( G \) is the minimal number of non-scalar multiplications and divisions to compute all rational functions in \( G \). If we only consider sets of quadratic forms and restrict ourselves to infinite fields, then, according to Strassen (1973), we may use a restricted definition of multiplicative complexity:

**Definition 2.1.** Let \( F \) be an infinite field, \( \mathbf{x} = \{x_1, \ldots, x_k\} \) a set of indeterminates over \( F \), and \( Q = \{q_1, \ldots, q_n\} \subseteq F[\mathbf{x}] \), a set of quadratic forms in \( \mathbf{x} \).

1. A sequence \( \beta = (u_1, v_1, \ldots; u_l, v_l) \), such that the \( u_\lambda, v_\lambda \in F[\mathbf{x}] \) are linear forms in \( \mathbf{x} \), is called a quadratic computation of length \( \ell(\beta) := l \) for \( Q \) over \( F \), if there are scalars \( \omega_{\nu,\lambda} \in F \) such that

\[
q_\nu(\mathbf{x}) = \sum_{\lambda=1}^{l} \omega_{\nu,\lambda} u_\lambda(\mathbf{x}) v_\lambda(\mathbf{x}) \quad \text{for all } 1 \leq \nu \leq n.
\]

2. The length of a shortest quadratic computation for \( Q \) over \( F \) is called the multiplicative complexity of \( Q \) over \( F \) and is denoted by \( C_F(Q) \).