ACM Communications in Computer Algebra, Vol.xx, No.xx, Issue xxx, month 201x

A family of schemes for multiplying 3×3 matrices with 23 coefficient multiplications

Marijn Heule*, Manuel Kauers† and Martina Seidl‡

Department of Computer Science · The University of Texas · Austin TX, USA
Institute for Algebra · Johannes Kepler University · Linz, Austria
Institute for Formal Methods and Verification · Johannes Kepler University · Linz, Austria

marijn@cs.utexas.edu · manuel.kauers@jku.at · martina.seidl@jku.at

Abstract

We present a 17-dimensional family of multiplication schemes for 3×3 matrices with 23 multiplications applicable to arbitrary coefficient rings.

In 1976, Laderman [6] presented the first scheme for computing the product of two 3×3 matrices using only 23 multiplications in the coefficient ring. His record still stands. Laderman's short paper does not make a lot of words. Essentially he just states his result and makes some brief comments about it. In view of the applicable page limit, we do the same here. The rest of the story can be found in [3] and [4].

Let R be a ring and S be a subring of the centralizer of R. Let $x_1, \dots, x_{17} \in S$ be arbitrary, define $x_{i,j} = x_i x_j + 1$ for $i, j = 1, \dots, 17$ and set

$$p_1 = x_{2,3} + x_3 \qquad p_2 = x_7 x_{5,6} + x_5$$
$$p_3 = x_4 x_{2,3} + x_2 \qquad p_4 = x_{14} x_{12,13} + x_{12}$$
$$p_5 = x_{16} x_{10,15} + x_{10} \qquad p_6 = x_4 x_{2,3} + x_{3,4} + x_2$$
$$p_7 = x_8 x_{11} x_{5,6} + x_8 x_9 x_{5,6} - x_6 x_{11}$$
$$p_8 = x_7 x_8 x_9 x_{5,6} + x_7 x_8 x_{11} x_{5,6} - x_{11} x_{6,7} + x_5 x_8 x_9 + x_5 x_8 x_{11}.$$

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in R^{3\times3}, \quad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \in R^{3\times3}, \quad \text{and} \quad C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = AB.$$

Then the entries of C can be computed from the entries of A and B as follows:

$$m_1 = (a_{11} + x_1 a_{12} + a_{13}) \times (b_{33})$$

---

*Supported by NSF under grant CCF-1526760 and by AFRL Award FA8750-15-2-0096

†Supported by the Austrian FWF grants P31571-N32, F5004

‡Supported by the Austrian FWF grant NFN S11408-N23

$$
\begin{aligned}
m_2 &= (a_{11} + a_{21} - a_{22})\\
&\times (b_{21} - b_{23})\\
m_3 &= (a_{11} + a_{21} + a_{31} + a_{33})\\
&\times (b_{11} + b_{12} - b_{13})\\
m_4 &= (a_{11} + a_{21} + a_{32})\\
&\times (b_{12} - b_{21} + b_{23})\\
m_5 &= (a_{11} + a_{21})\\
&\times (b_{11} - b_{13} + b_{21} - b_{23})\\
m_6 &= (a_{11} - a_{23})\\
&\times (b_{11} - b_{33})\\
m_7 &= (a_{11} - a_{31} + a_{32})\\
&\times (- b_{12})\\
m_8 &= (a_{11} + a_{33})\\
&\times (b_{12} - b_{13} + b_{33})\\
m_9 &= (a_{11})\\
&\times (b_{13} - b_{33})\\
m_{10} &= (a_{12} + a_{13} + a_{22} + a_{23} + a_{32})\\
&\times (b_{21} + b_{22} - b_{23})\\
m_{11} &= (a_{12} + a_{13} + a_{23})\\
&\times (b_{21} + b_{22} - b_{23} - b_{32})\\
m_{12} &= (a_{12} + a_{13} - a_{33})\\
&\times (b_{32})\\
m_{13} &= (a_{12})\\
&\times (x_{3,4}\, b_{22} - p_6\, b_{23} - x_{3,4}\, b_{32} + p_6 x_1\, b_{33})\\
m_{14} &= (a_{12})\\
&\times (x_3\, b_{22} - p_1\, b_{23} - x_3\, b_{32} + p_1 x_1\, b_{33})\\
m_{15} &= (a_{13} + a_{23})\\
&\times (- b_{21} - b_{22} + b_{23} + b_{31} + b_{32} - b_{33})\\
m_{16} &= (- p_2\, a_{21} + p_2 x_9\, a_{22} - p_2\, a_{23} - x_{6,7}\, a_{31} + p_8\, a_{32} - x_{6,7}\, a_{33})\\
&\times (b_{11})\\
m_{17} &= (x_{5,6}\, a_{21} - x_9 x_{5,6}\, a_{22} + x_{5,6}\, a_{23} + x_6\, a_{31} - p_7\, a_{32} + x_6\, a_{33})\\
&\times (b_{11})\\
m_{18} &= (a_{22} + x_8\, a_{32})\\
&\times (x_9\, b_{11} + b_{21})\\
m_{19} &= (x_{15,16}\, a_{23} + p_5\, a_{33})\\
&\times (b_{11} - b_{31})\\
m_{20} &= (a_{32})\\
&\times (x_{11} x_{13,14}\, b_{11} + p_4\, b_{12} - x_{13,14}\, b_{21} + p_4\, b_{22})\\
m_{21} &= (- a_{32})
\end{aligned}
$$

$$
\begin{aligned}
&\times (\; x_{11}x_{13}\, b_{11} + x_{12,13}\, b_{12} - x_{13}\, b_{21} + x_{12,13}\, b_{22} \;)\\
m_{22} &= (\; x_{15}\, a_{23} + x_{10,15}\, a_{33})\\
&\times (\; - b_{11} + b_{31} \;)\\
m_{23} &= (\; a_{33})\\
&\times (\; x_{17}\, b_{11} - b_{12} + b_{13} - x_{17}\, b_{31} + b_{32} - b_{33})
\end{aligned}
$$

$$
\begin{aligned}
c_{11} &= m_1 + m_6 + m_{11} - x_{2,3}m_{13} + p_3m_{14} + m_{15} + x_{10,15}m_{19} + p_5m_{22}\\
c_{12} &= m_8 + m_9 + m_{12} + p_1m_{13} - p_6m_{14} + x_{15}x_{17}m_{19} + x_{17}x_{15,16}m_{22} + m_{23}\\
c_{13} &= m_1 + m_9 + x_3m_{13} - x_{3,4}m_{14}\\
c_{21} &= x_6m_{16} + x_{6,7}m_{17} + m_{18} - x_{10,15}m_{19} + x_8x_{12,13}m_{20} + p_4x_8m_{21} - p_5m_{22}\\
c_{22} &= m_2 + m_4 - m_8 - m_9 + m_{10} - m_{11} - m_{12} - x_{15}x_{17}m_{19} + x_{13}m_{20} + x_{13,14}m_{21} - x_{17}x_{15,16}m_{22} - m_{23}\\
c_{23} &= m_2 - m_5 + m_6 - m_9 + x_6m_{16} + x_{6,7}m_{17} + m_{18} + x_8x_{12,13}m_{20} + p_4x_8m_{21}\\
c_{31} &= -x_{5,6}m_{16} - p_2m_{17} + x_{15}m_{19} - x_{12,13}m_{20} - p_4m_{21} + x_{15,16}m_{22}\\
c_{32} &= m_7 + m_8 + m_9 + x_{15}x_{17}m_{19} - x_{13}m_{20} - x_{13,14}m_{21} + x_{17}x_{15,16}m_{22} + m_{23}\\
c_{33} &= -m_3 + m_4 + m_5 + m_7 + m_8 + m_9 - x_{5,6}m_{16} - p_2m_{17} - x_{12,13}m_{20} - p_4m_{21}
\end{aligned}
$$

Remarks:

- It is straight-forward (but tedious) to confirm the correctness of the above scheme by expanding all definitions and observing that we have $c_{i,j} = \sum_k a_{i,k}b_{k,j}$ for all i, j.
- The scheme performs only 23 multiplications of two elements of R, one for each m_k (plus a number of additions and a number of multiplications of an element of S with an element of R).
- Since we can take $R = T^{n\times n}$ and $S = \{cI_n : c \in T\}$ for any $n \in \mathbb{N}$ and any ring T, the scheme can be used recursively to multiply any two elements of $T^{n\times n}$ with $\mathrm{O}(n^{\log_3 23})$ operations in T.
- Since $\log_2 7 < \log_3 23$, we cannot beat Strassen's algorithm [9] in this way. It is still not known whether there are schemes for 3×3 matrices with fewer than 23 multiplications.
- We can show that, unfortunately, there is no way to instantiate the parameters $x_1, \ldots, x_{17}$ in such a way that the scheme can be simplified to a scheme with only 22 multiplications in R.
- The polynomials in $x_1, \ldots, x_{17}$ appearing in the scheme describe variety of dimension 17. In this sense, there is no redundancy among the parameters.
- In contrast to the families discovered by Johnson and McLoughlin [5], our scheme not only has more parameters, but it also has the feature that no assumption on the ring R is needed.
- Our parametrized family is unrelated to the family of [5] and to other known schemes [6, 1, 7, 8] for multiplying 3×3 matrices with 23 coefficient multiplications.
- Our scheme was found by a combination of SAT solving, described in more detail in [3], and computer algebra methods, described in more detail in [4].
- We have a few other schemes with 17 parameters, dozens with fewer parameters, and altogether thousands of new isolated solutions. They are available electronically at [2].

References

[1] Nicolas Courtois, Gregory V. Bard, and Daniel Hulme. A new general-purpose method to multiply 3×3 matrices using only 23 multiplications. *CoRR*, abs/1108.2830, 2011.

[2] Marijn J.H. Heule, Manuel Kauers, and Martina Seidl. Matrix multiplication repository. `http://www.algebra.uni-linz.ac.at/research/matrix-multiplication/`. Accessed: 2019-04-26.

[3] Marijn J.H. Heule, Manuel Kauers, and Martina Seidl. Local search for fast matrix multiplication. In *Proceedings of SAT'19*, 2019. to appear.

[4] Marijn J.H. Heule, Manuel Kauers, and Martina Seidl. New ways to multiply 3×3 matrices. Technical Report 1905.10192, ArXiv, 2019.

[5] Rodney W. Johnson and Aileen M. McLoughlin. Noncommutative bilinear algorithms for 3×3 matrix multiplication. *SIAM J. Comput.*, 15(2):595–603, 1986.

[6] Julian D. Laderman. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications. *Bulletin of the American Mathematical Society*, 82(1):126–128, 1976.

[7] Jinsoo Oh, Jin Kim, and Byung-Ro Moon. On the inequivalence of bilinear algorithms for 3×3 matrix multiplication. *Information Processing Letters*, 113(17):640–645, 2013.

[8] A. V. Smirnov. The bilinear complexity and practical algorithms for matrix multiplication. *Computational Mathematics and Mathematical Physics*, 53(12):1781–1795, 2013.

[9] Volker Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.