Exhaustive search of optimal formulae for bilinear maps

S. Covanov[1]

[1] *Université de Lorraine, France, {svyatoslav.covanov}@inria.fr*

Finding optimal formulae for computing bilinear maps is a problem of algebraic complexity theory [3, 2, 16, 8], initiated by the discoveries of Strassen [16] and Karatsuba [9]. It consists to determine almost optimal algorithms for important problems of complexity theory, among which the well studied complexity of matrix multiplication [16, 5, 10] and the complexity of polynomial multiplication [9, 17, 15, 6].

In the field of complexity of polynomial multiplication, the first improvement over the schoolbook method came from Karatsuba [9] in 1962, who proposed a decomposition of the bilinear map corresponding to the product of two polynomials of degree 2

$$P = p_0 + p_1 X \text{ and } Q = q_0 + q_1 X. \tag{1}$$

The product $P \cdot Q$ requires, to be computed, 4 multiplications using the schoolbook algorithm: p_0q_0, p_1q_0, p_0q_1, p_1q_1. With the Karatsuba algorithm, the coefficients of the product $P \cdot Q$ can be retrieved from the computation of the 3 following multiplications: p_0q_0, $(p_0+p_1)(q_0+q_1)$, p_1q_1. In particular, Karatsuba's algorithm can be used to improve the binary complexity of the multiplication of two n-bit integers: instead of $O(n^2)$ with the naive schoolbook algorithm, we obtain $O(n^{\log_2 3})$. Then, given a degree $d > 1$, computing the minimal amount of multiplications required for the product of polynomials of degree d leads to even better complexities and produces optimal formulae for a particular product.

The main obstacle to finding optimal formulae is the fact that the decomposition of bilinear maps is known to be NP-hard [7]. Montgomery proposed in [11] an algorithm to compute such a decomposition for the particular case of polynomials of small degree over a finite field. The author takes advantage of the fact that the number of all optimal formulae is limited on a finite field. He gets new formulae for the multiplication of polynomials of degree 5, 6 and 7 over $\mathbb{F}_2$. In [12], Oseledets proposes a heuristic approach and uses the formalism of vector spaces to solve the bilinear rank problem for the polynomial product over $\mathbb{F}_2$. Later, Barbulescu et al. proposed in [1] a unified framework, developping the idea proposed by Oseledets using the vector

spaces formalism, permitting the authors to compute the bilinear rank of different applications, such as the short product or the middle product over a finite field. Their algorithm allows one to generate all the possible rank decomposition of any bilinear map over a finite field. This work is the main inspiration of the current presentation.

Our work is an improvement to the algorithm introduced in [1], allowing one to increase the family of bilinear maps over a finite field for which we are able to compute all the optimal formulae. Our algorithm relies on the automorphism group stabilizing a bilinear map, seen as a vector space, and on a topological invariant of such a vector space. It can be used for proving lower bounds on the rank of a bilinear map and it has applications for improving upper bounds on the Chudnovsky-Chudnovsky algorithms [4, 14, 13]. Especially, we compute all the decompositions for the short product of polynomials P and Q modulo X^5 and the product of 3×2 by 2×3 matrices. The latter problem was out of reach with the method used in [1]: we prove, in particular, that the set of possible decompositions for this matrix product is essentially unique, up to the automorphism group.

References

[1] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. *Arithmetic of finite fields: 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings*, chapter Finding Optimal Formulae for Bilinear Maps, pages 168–186. Springer, 2012. doi:10.1007/978-3-642-31662-3_12.

[2] R. W. Brockett and D. Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and its Applications*, 19(3):207 – 235, 1978. doi:10.1016/0024-3795(78)90012-5.

[3] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1st edition, 2010.

[4] D. Chudnovsky and G. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285 – 316, 1988. doi:10.1016/0885-064X(88)90012-X.

[5] D. Coppersmith and S. Winograd. Computational algebraic complexity editorial matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251 – 280, 1990. doi:10.1016/S0747-7171(08)80013-2.

[6] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, ArXiv, 2014. arXiv:1407.3360.

[7] J. Håstad. Tensor rank is np-complete. *Journal of Algorithms*, 11(4):644 – 654, 1990. doi:10.1016/0196-6774(90)90014-6.

[8] J. JáJá. Optimal evaluation of pairs of bilinear forms. *SIAM Journal on Computing*, 8(3):443–462, 1979. doi:10.1137/0208037.

[9] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics-Doklady*, 7:595–596, 1963. (English translation).

[10] F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 296–303. ACM, 2014. doi:10.1145/2608628.2608664.

[11] P. Montgomery. Five, six, and seven-term Karatsuba-like formulae. *Computers, IEEE Transactions on*, 54(3):362–369, 2005. doi:10.1109/TC.2005.49.

[12] I. Oseledets. Optimal Karatsuba-like formulae for certain bilinear forms in gf(2). *Linear Algebra and its Applications*, 429(8-9):2052 – 2066, 2008. doi:10.1016/j.laa.2008.06.004.

[13] M. Rambaud. *Arithmetic of Finite Fields: 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers*, chapter Finding optimal Chudnovsky-Chudnovsky multiplication algorithms, pages 45–60. Springer, 2015. doi:10.1007/978-3-319-16277-5_3.

[14] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489 – 517, 2012. doi:10.1016/j.jco.2012.02.005.

[15] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3-4):281–292, 1971. doi:10.1007/BF02242355.

[16] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356. doi:10.1007/BF02165411.

[17] A. L. Toom. The complexity of a scheme of functional elements realizing the multiplication of integers. *Soviet Mathematics Doklady*, 3:714–716, 1963. (English translation).