Simple Multivariate Polynomial Multiplication

Victor Pan

TR-93-003

August 1993

Simple Multivariate Polynomial Multiplication

Victor Pan*
Mathematics & Computer Science Dept.
Lehman College, CUNY, Bronx, NY 10468

Summary: We observe that polynomial evaluation and interpolation can be performed fast over a multidimensional grid (lattice), and we apply this observation in order to obtain the bounds

$$M(c,m) \le c^m\big(1+m+1.5m+2\log_2 c\big)$$

over the fields of constants supporting FFT on c points, c being a power of 2, and

$$M(c,m) = O[N \log N \log\log c)\ ,$$

over any field, where $N = c^m$, and $M(c,m)$ denotes the number of arithmetic operations required in order to multiply (over any field F) a pair of m-variate polynomials whose product has degree at most $c-1$ in each variable, so that $M(c,m) = O(N \log N)$ if $c = O(1)$, $m \to \infty$ (over any field F), versus the known bound of $O(N \log N \log\log N)$.

* This work was supported by NSF Grants CCR-8805782, CCR-9020690 and by PSC-CUNY Awards #661340, #662478, #668541 and #669290.

1. Introduction. A common approach to multiplication over any fixed field F of a pair of m-variate polynomials $u = u(x_1, \ldots, x_m)$ and $v = v(x_1, \ldots, x_m)$ of degrees at most $d(i)$ in x_i, $i = 1, \ldots, m$, is to map them first into univariate polynomials in x, according to Kronecker's map

$$x_{k+1} = x^{D(1)\ldots D(k)} , \qquad k = 0, \ldots, m-1 , \tag{1}$$

then to multiply these two polynomials by using the known algorithms, and finally, to recover the coefficients of the polynomial $p = uv$,

$$p = p(x_1, \ldots, x_m) = \sum_{i_1, \ldots, i_m} p_{i_1, \ldots, i_m} x_1^{i_1} \ldots x_m^{i_m} , \tag{2}$$

by applying the map (1) again. It suffices to set

$$D(i) = 2d(i) + 1 , \qquad i = 1, \ldots, m ,$$

to ensure the correct answers, since the degree of p in x_i is at most $2d(i)$.

Hereafter, we set

$$d = \max_i d(i) + 1 > 1 , \quad c \geq 2d - 1 = \max_i \big(2d(i) + 1\big) , \quad N = c^m ,$$

and let $M(c, m) = M_F(c, m)$ denote the minimum number of arithmetic operations required in order to multiply u and v over a field F.

The univariate image of the multivariate polynomial $p = uv$ has degree at most N, so that we may apply the known algorithms for multiplication of univariate polynomials ([BM], [CK], [N], [S]) and deduce that

$$M_F(c, m) = O(N \log N) \tag{3}$$

if F supports FFT on 2^n points, for $n = \lceil \log_2 N \rceil$, and

$$M_F(c, m) = O(N \log N \log\log N) \tag{4}$$

over any field (or even ring or algebra) F.

Decreasing the bound (4) to the level of (3) over any field (ring or algebra) F is a well known challenge, both for the computational complexity theory and for the computational practice. [The known lower bound is $\Omega(N)$ over any field.]

In this short paper we achieve the above goal of reaching the bound (3), in the multivariate case where $c = O(1)$ and $m \to \infty$ [see (13)]. Our approach does not give any good results in the univariate case (see Remark 2), being a rare (if not the only) example of techniques whose power is lost in the transition from multivariate to univariate polynomial computations.

To understsand the reason for this, observe that the algorithms of [N], [CK] and all other known fastest algorithms for univariate polynomial multiplication over any field (or ring or algebra) perform several arithmetic operations in order to reduce the problem to multiplication of multivariate polynomials of lower degrees, which exactly reverses whatever Kronecker's mapping (1) does. Our idea is to avoid such a back-and-forth transition, thus saving the arithmetic operations involved. This gives us the desired bound (13).

Remark 1. For completeness, we shall cite an alternative algorithm of [CKL], which reaches the bound $O(M(N,1)\log N)$ for multiplication of polynomials over the fields of constants having characteristic 0, provided that N bounds the overall number of monomials of the dense polynomial product. This makes the algorithm of [CKL] superior to ours (over the fields of characteristic 0) for multiplication of the m-variate polynomials whose terms have total degree in all the variables bounded by a single fixed value d.

2. The Improved Computation. We will rely on the following very simple identity:

$$u(x_1,\dots,x_m) = u_{x_1}(x_2,\dots,x_m) \tag{5}$$

where

$$u_{x_1}(x_2,\dots,x_m) = \sum_{i_2,\dots,i_m} u_{i_2\dots i_m}(x_1)x_2^{i_2}\dots x_m^{i_m}\ ,\ u_{i_2\dots i_m}(x_1) = \sum_{i_1} u_{i_1 i_2\dots i_m}x_1^{i_1}\ ,$$

and on the similar identities for $v(x_1, \ldots, x_m)$ and $p(x_1, \ldots, x_m)$.

Let $G = G(c(1), \ldots, c(m))$ denote an m-dimensional grid (or lattice) G where the variable x_j takes $c(j)$ distinct values in F or in its algebraic extension K modulo an irreducible polynomial of degree a over F such that

$$|K| = |F|^{a+1}, a + 1 = \lceil \log c(j) / \log |F| \rceil \ . \tag{6}$$

To simplify the subsequent estimates, assume that $c(j) = c$ for all j and let $E(c, m)$ denote the number of arithmetic operations required in order to evaluate on the grid G an m-variate polynomial [such as $u(x_1, \ldots, x_m)$ or $v(x_1, \ldots, x_m)$] whose degree in each variable is less than d. The identity (5) reduces the latter problem for $u(x_1, \ldots, x_m)$ to the evaluation of d^{m-1} univariate polynomials $u_{i_2 \ldots i_m}(x_1)$ at c points x_1 and of c polynomials $u_{x_1}(x_2, \ldots, x_m)$ in $m - 1$ variables $x_2, \ldots, x_m$ at c^{m-1} points of an $(m-1)$-dimensional grid, so that

$$\begin{aligned} E(c, m) &\le d^{m-1} E(c, 1) + cE(c, m-1) \le (d + c) d^{m-2} E(c, 1) + c^2 E(c, m-2) \\ &\le \ldots \le \sum_{i=0}^{m-1} d^i c^{m-1-i} E(c, 1) = c^m \frac{1 - (d/c)^m}{d - 1} E(c, 1) \le 2c^m E(c, 1) \ . \end{aligned}$$

The same bounds apply to the evaluation of $v(x_1, \ldots, x_m)$ on G, and similarly, we deduce the bound $I(c, m) \le mc^{m-1} I(c, 1)$ where $I(c, m)$ denotes the number of arithmetic operations required in order to solve the interpolation problem of computing the coefficients of an m-variate polynomial of degree less than c in every variable, provided we are given its values on the grid G.

Given two multivariate polynomials, we may apply the evaluation-and-interpolation technique of [T] and compute the coefficients of their product. Since $d(j)$ bounds the degrees of the input polynomials in x_j, their product has degree at most $c - 1$ in x_j for all j, so that

$$M(c, m) - c^m \le 2E(c, m) + I(c, m) \le c^{m-1}(4E(c, 1) + mI(c, 1)) \tag{7}$$

arithmetic operations in F suffice if $|F| \ge c$.

Over the fields of constants that contain a principal c-th root of 1, and thus support FFT on c points (assuming that c is a power of 2), we choose the grid G so as to perform the evaluation and interpolation on a set of the c-th roots of 1 by means of FFT [so that $E(c,1)$ and $I(c,1)-c$ are replaced by $2c\log_2 c$ in this case ([BM, pp. 84-85])] and arrive at the bound

$$M(c,m) \le c^m(1+m+2(m+4)\log_2 c)\ .$$

Over any field F, such that $|F| \ge c$, we substitute into (7) the known bound

$$\max\{E(c,1), I(c,1)\} \le \gamma\, M(c,1)\log_2 c, \tag{8}$$

for some fixed constant γ, and obtain that

$$M(c,m) \le \gamma c^{m-1}(\log_2 c)M(c,1)(m+4) = O(N(\log N)M(c,1)/c), \tag{9}$$

where $N = c^m$. We may substitute the known upper bound

$$M(s,1) = O(s\log s\log\log s) \tag{10}$$

([CK], [N], [S]) and obtain from (9) that

$$M(c,m) = O(N\log N\log c\log\log c)\ , \tag{11}$$

if $N = c^m$, $|F| \ge c$. If $|F| < c$, we may shift to an algebraic extension K of F with the increase of the complexity bound (11) by the factor of $M(\log c/\log|F|,1)$ [see (6)], which turns into $O(1)$ if $c = O(1)$.

Instead of increasing the bound (11), however, we may decrease it by removing the factor of $\log c$ if we recursively generate roots of 1, as in [CK], [N], and choose the points of the grid G having their coordinates equal to such roots. This way, we may replace $4E(c,1)+mI(c,1)$ in (7) by $O(mc\log c\log\log c)$ and obtain that

$$M(c,m) = O(c^m m\log c\log\log c) = O(N\log N\log\log c)\ . \tag{12}$$

Note that both of the bounds (11) and (12) lead to the bound

$$M(c,m) = O(N \log N) \quad \text{if} \quad c = O(1) \quad \text{and} \quad m \to \infty \,, \tag{13}$$

over any field F, versus $O(N \log N \log\log N)$ of the approach based on (1).

Remark 2, *applications to the Univariate Polynomial Multiplication over any Field of Constants.* We may substitute into (7) the classical bound $\max\{E(s,1), I(s,1)\} = O(s^2)$ (over any field F), rather than (10); then we may apply the homomorphism from the class of univariate polynomials $p(x)$ of degrees at most $c^m - 1$ to the class of polynomials $p(x_1, \ldots, x_m)$ of (2) given by the substitution of variables $x_1 = x$, $x_2 = x^c$, $x_3 = x^{c^2}, \ldots, x_m = x^{c^{m-1}}$ [compare (1)]. The resulting upper bound on $M(s,1)$, however, is inferior to (10).

Acknowledgement. I thank Erich Kaltofen for his helpful comments.

References

[BM] A. Borodin and I. Munro, *The Computational Complexity of Algebraic and Numeric Problems*, American Elsevier, New York, 1976.

[CKL] J. F. Canny, E. Kaltofen and Y. Lakshman, "Solving Systems of Nonlinear Polynomial Equations Faster," *Proc. ACM-SIGSAM Int. Symp. on Symb. and Alg. Comp.* (1989) 121–128.

[CK] D. G. Cantor and E. Kaltofen, On Fast Multiplication of Polynomials over Arbitrary Algebras, *Acta Inf.* 2 (1991) 693–701.

[N] H. J. Nusbaumer, Fast Polynomial Transform Algorithms on Digital Computers, *IEEE Trans. on ASSP* 28 (1980) 205–215.

[S] A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Characteristik 2, *Acta Inf.* 7 (1977) 395–398.

[T] A. T. Toom, "The Complexity of a Scheme of Functional Elements Realizing the Multiplication of Integers," *Soviet Math. Doklady* 3 (1963) 714–716.