Information Processing Letters 139 (2018) 30–34

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A probabilistic algorithm for verifying polynomial middle product in linear time

Pascal Giorgi

LIRMM, University of Montpellier, CNRS, Montpellier, France

ARTICLE INFO

Article history:
Received 4 July 2017
Received in revised form 19 June 2018
Accepted 19 June 2018
Available online 5 July 2018
Communicated by Or Meir

Keywords:
Probabilistic algorithm
Design of algorithm
Computation on polynomials
Polynomial multiplication

ABSTRACT

Polynomial multiplication and its variants are a key ingredient in effective computer algebra. While verifying a polynomial product is a well known task, it was not yet clear how to do a similar approach for its middle product variant. In this short note, we present a new algorithm that provides such a verification with the same complexity and probability that for the classical polynomial multiplication. Furthermore, we extend our algorithm to verify any operations that compute only a certain chunk of the product, which is the case for instance of the well known short product operation.

1. Introduction

Polynomial multiplication is a fundamental tool in computer algebra as it often plays a central role in most efficient algorithms. In some cases, one may not need to compute the whole result of the product and this can be taken into account to speed up the computation. For instance, when dealing with truncated power series one need to only compute the lowest part of the polynomial multiplication. The latter operation is also referenced as short product in [1]. Another situation occurs within polynomial division or inversion where only the middle terms of a specific product are needed [2–4]. This specific operation is called the middle product in [2].

Let $F, G \in \mathbb{K}[X]$ be two polynomials defined over a field $\mathbb{K}$ such that $\deg F = s-1, \deg G = 2s-2$. The middle product of FG denoted by $\mathsf{MP}_s(F,G)$ corresponds to the coefficients of degree $s-1$ to $2s-2$ from the product FG. Let $FG = \sum_{i=0}^{3s-3} h_i X^i$ then $\mathsf{MP}_s(F,G) = h_{s-1} + h_s X + h_{s+1}X^2 + \cdots + h_{2s-2}X^{s-1}$. Let $M(n)$ denote the complexity function for the multiplication of two polynomials of $\mathbb{K}[X]$ of degree at most n. Computing $\mathsf{MP}_s(F,G)$ through a full product requires $2M(s) + O(s)$ operations in $\mathbb{K}$. As shown in [2], dedicated algorithms can compute $\mathsf{MP}_s(F,G)$ twice faster. One remarkable property of middle product is to be the transposed problem of polynomial multiplication using the Tellegen principle [5]. This strong result tells us that every polynomial multiplication algorithm can be turned into an algorithm for middle product with the same asymptotic complexity, i.e. $M(s) + O(s)$. Since the seminal work of Karatsuba [6], many fast polynomial multiplication algorithms have been designed in order to reach a quasi-linear time complexity [7, Chapter 8]. As of today, the best result over finite fields is $O(d \log d\, 8^{\log^* d} \log p)$ operations[1] for the product of degree d polynomials [8]. A common feature of all these algorithms is to be much more complex than the naive product, meaning their implementation could be complicated and errors prone. Using Tellegen principle to derive a middle product algorithm introduces another level of difficulty that might further complicate its implementations.

E-mail address: pascal.giorgi@lirmm.fr.

[1] $\log^*$ is the iterated logarithm function.

https://doi.org/10.1016/j.ipl.2018.06.014
0020-0190/© 2018 Elsevier B.V. All rights reserved.

A classic way to check computations is to use *a posteriori* verification. The idea is to provide an algorithm that can check the result with an asymptotically better complexity than the operation itself. The simplicity of the algorithm must ensure its implementation's robustness. Such a verification is of great interest when one wants to check a computation from an untrusted cloud server. In order to check a polynomial product FG one can pick a random point α and check that $F(\alpha)G(\alpha) = (FG)(\alpha)$. If not, it is clear that the product is wrong. If the results agree, it is well known through Zippel–Schwartz–Lipton–DeMillo lemma [9–11] that the product FG is correct with a probability greater than $1 - \frac{d}{N}$ where N corresponds to the number of sampling points for α and $\deg FG < d$. Assuming $N > d$, one can decrease the probability to $1 - \frac{d^k}{N^k}$ by picking k different points. One advantage of this verification is that polynomial evaluation has a linear time complexity and can be implemented easily through Horner's rules.

To the best of our knowledge, the verification of the middle product has not been investigated yet and we provide a similar linear time algorithm for it. One motivation of this work came from our experiment to compute the kernel of a large sparse matrix arising in discrete logarithm computation. In particular, one part of the computation was relying on polynomial middle product with matrix coefficients [12]. Unfortunately, our code failed to produce correct results when polynomial degrees were above 500 000. Since quadratic time verification was not feasible, we decided to develop a fast approach. Note that our algorithm might also be of interest for the recent Middle-Product Learning With Error problem [13].

We start the next section by giving a matrix interpretation to the verification of polynomial product. Using this interpretation, we will define in the following sections our probabilistic verification for the middle product. Finally, in the last section we show how our method easily extends to the short product and any other operations that compute any partial chunk of a polynomial product.

2. Certifying polynomial multiplication

Let $F, G \in \mathbb{K}[X]$ where $F = f_0 + f_1X + \cdots + f_{m-1}X^{m-1}$ and $G = g_0 + g_1X + \cdots + g_{n-1}X^{n-1}$. Assuming F is fixed, the product $H = FG = \sum_{i=0}^{m+n-2} h_iX^i$ can be described through a linear application from $\mathbb{K}^n$ to $\mathbb{K}^{m+n}$. The matrix for this application corresponds to a Toeplitz matrix built from the coefficients of F. Let us denote $\mathcal{A}_F$ such a matrix, the product of F by G correspond to the following matrix-vector product:

$$\underbrace{\begin{pmatrix} f_0 & & \\ f_1 & \ddots & \\ \vdots & \ddots & f_0 \\ f_{m-1} & & f_1 \\ & \ddots & \vdots \\ & & f_{m-1} \end{pmatrix}}_{\mathcal{A}_F} \times \underbrace{\begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix}}_{v_G} = \underbrace{\begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{m+n-2} \end{pmatrix}}_{v_H} \qquad (1)$$

where $\mathcal{A}_F \in \mathbb{K}^{(m+n-1)\times n}$, $v_G \in \mathbb{K}^n$ and $v_H \in \mathbb{K}^{m+n-1}$.

A classic way to certify the product $H = FG$ is to choose a random α from a finite subset $S \subset \mathbb{K}$ and to check $H(\alpha) = F(\alpha)G(\alpha)$. Of course, some values of α may lead to a positive answer while $H \neq FG$. However, the number of such α is at most $\deg H$ as they correspond to the roots of the polynomial $(H - FG) \neq 0$ over the field $\mathbb{K}$. The probability of success is then greater than $1 - \frac{\deg H}{|S|}$, which corresponds exactly to the Zippel–Schwartz–Lipton–DeMillo lemma [9–11] on univariate polynomials. This approach reduces the verification to three polynomial evaluations and one product and thus has a linear time complexity of $O(\deg F + \deg G + \deg H)$.

Using the matrix version for polynomial product depicted in Equation (1), this latter approach corresponds exactly to multiplying both parts of the equation on the left by the row vector $\vec{\alpha} = [1, \alpha, \alpha^2, \ldots, \alpha^{m+n-2}]$. By definition of v_H, we clearly have $\vec{\alpha} \cdot v_H = H(\alpha)$. Using the Toeplitz structure of the matrix $\mathcal{A}_F$ we have $\vec{\alpha}\mathcal{A}_F = F(\alpha)[1, \alpha, \ldots, \alpha^{n-1}]$, which gives $(\vec{\alpha}\mathcal{A}_F) \cdot v_G = F(\alpha)G(\alpha)$. The probability result can be retrieved with the specific Freivalds certificate for matrix multiplication given in [14].

3. Certifying middle product

In order to illustrate our strategy we start this section with an example. Let A, B be two polynomials of $\mathbb{K}[X]$ of degree respectively 3 and 6, with $A = a_0 + a_1X + a_2X^2 + a_3X^3$ and $B = b_0 + b_1X + b_2X^2 + b_3x^3 + b_4X^4 + b_5X^5 + b_6X^6$. We want to compute $C_M = c_3 + c_4X + c_5X^2 + c_6X^3$ where $C = AB = \sum_{i=0}^{9} c_iX^i$. Using Equation (1) one can easily remark that the middle product operation corresponds to using only certain rows of the linear application for the full multiplication by A. Equation (2) illustrates this remark on our example. The grey area highlights the rows used by the middle product operation. One may note that this is an important observation in Tellegen transposition principle for the middle product [5].

$$\begin{pmatrix} a_0 & & & & & & \\ a_1 & a_0 & & & & & \\ a_2 & a_1 & a_0 & & & & \\ a_3 & a_2 & a_1 & a_0 & & & \\ & a_3 & a_2 & a_1 & a_0 & & \\ & & a_3 & a_2 & a_1 & a_0 & \\ & & & a_3 & a_2 & a_1 & a_0 \\ & & & & a_3 & a_2 & a_1 \\ & & & & & a_3 & a_2 \\ & & & & & & a_3 \end{pmatrix} \times \underbrace{\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \end{pmatrix}}_{v_B} = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \end{pmatrix} \qquad (2)$$

In order to certify the coefficients of the middle product $\mathsf{MP}_4(A, B) = c_3 + c_4X + c_5X^2 + c_6X^3$, one can multiply the grey part of equation (2) with the vector $[1, \alpha, \alpha^2, \alpha^3]$ with $\alpha \in \mathbb{K}$. In particular, this corresponds to certifying that $[1, \alpha, \alpha^2, \alpha^3] \cdot [c_3, c_4, c_5, c_6]^T = c_M(\alpha)$ is equal to

$$\gamma = \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{pmatrix}^T \times \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & & & \\ & a_3 & a_2 & a_1 & a_0 & & \\ & & a_3 & a_2 & a_1 & a_0 & \\ & & & a_3 & a_2 & a_1 & a_0 \end{pmatrix} v_B. \qquad (3)$$

More generally, let $F, G, H \in \mathbb{K}[X]$ such that $\deg F = \deg H = s - 1$, $\deg G = 2s - 2$ and $H = \mathsf{MP}_s(F, G)$. As for