Journal of Symbolic Computation 72 (2016) 231–251

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

A simple and fast online power series multiplication and its analysis [☆]

Romain Lebreton [a], Éric Schost [b]

[a] LIRMM, UMR 5506 CNRS, Université Montpellier II, Montpellier, France
[b] Computer Science Department, Western University, London, Ontario, Canada

ARTICLE INFO

Article history:
Received 24 November 2014
Accepted 17 February 2015
Available online 5 March 2015

Keywords:
Online algorithm
Relaxed algorithm
Multiplication of power series
Arithmetic complexity

ABSTRACT

This paper focuses on *online* (or *relaxed*) algorithms for the multiplication of power series over a field and their complexity analysis. We propose a new online algorithm for the multiplication using middle and short products of polynomials as building blocks, and we give the first precise analysis of the arithmetic complexity of various online multiplications. Our algorithm is faster than Fischer and Stockmeyer's by a constant factor; this is confirmed by experimental results.

1. Introduction

Let $\mathbb{A}$ be a commutative ring with unity, and let x be an indeterminate over $\mathbb{A}$ (the commutativity hypothesis may not be required but greatly simplifies the setting of this paper). Given two power series $a = \sum_{i \geqslant 0} a_i x^i$ and $b = \sum_{i \geqslant 0} b_i x^i$ in $\mathbb{A}[[x]]$, we are interested in computing the coefficients c_i of the product $c = ab$ under the following constraint: we cannot use the coefficients a_i or b_i before we have computed $c_0, \ldots, c_{i-1}$. This condition is useful to model situations where the inputs a, b and the output c are related by a feedback loop, *i.e.* where $c_0, \ldots, c_{i-1}$ are needed in order to determine a_i and b_i (see the discussion below).

Previous work Algorithms that satisfy such a constraint were introduced by Fischer and Stockmeyer (1974); following that reference, we will call them *online* (the notion of an online algorithm extends beyond this question of power series multiplication, see for instance Hennie, 1966). Still following

[☆] This work has been partly supported by the ANR grant HPAC (ANR-11-BS02-013), NSERC and the CRC program.
E-mail addresses: lebreton@lirmm.fr (R. Lebreton), eschost@uwo.ca (É. Schost).

http://dx.doi.org/10.1016/j.jsc.2015.03.001
0747-7171/© 2015 Elsevier Ltd. All rights reserved.

Fischer and Stockmeyer, we will also consider *half-line* multiplication, where one of the arguments, say b, is assumed to be known in advance at arbitrary precision; in other words, the only constraint for such algorithms is that we cannot use the coefficient a_i before we have computed $c_0, \ldots, c_{i-1}$.

It seems that few applications of online power series multiplication were given at the time (Fischer and Stockmeyer, 1974) was written. Recently, van der Hoeven rediscovered Fischer and Stockmeyer's half-line and online multiplication algorithms, which he respectively called *semi-relaxed* and *relaxed* (van der Hoeven, 1997, 2002). In addition, as alluded to above, he showed that online multiplication is the key to computing power series solutions of large families of differential equations or of more general functional equations; this result was extended in Berthomieu and Lebreton (2012) to further families of linear and polynomial equations, showing the fundamental importance of online multiplication.

We complete this brief review of online multiplication by mentioning its adaptation to real numbers in Schröder (1997) and its extension to the multiplication of p-adic integers in Berthomieu et al. (2011).

The results of the papers Fischer and Stockmeyer (1974), Schröder (1997), van der Hoeven (1997), van der Hoeven (2002), Berthomieu et al. (2011) can be summarized by saying that online multiplication is slower than "classical" multiplication by at most a logarithmic factor. More precisely, let us denote by $\mathsf{M}(n)$ a function such that polynomials of degree at most $n-1$ in $\mathbb{A}[x]$ can be multiplied in $\mathsf{M}(n)$ ring operations in $\mathbb{A}$. For instance, using the naive algorithm gives $\mathsf{M}(n) = \mathcal{O}(n^2)$, Karatsuba's algorithm gives $\mathsf{M}(n) = \mathcal{O}(n^{\log_2(3)})$ and Fast Fourier Transform (FFT) techniques allow us to take $\mathsf{M}(n)$ quasi-linear: in the presence of roots of unity in $\mathbb{A}$ of orders 2^ℓ for any $\ell \geqslant 0$, FFT gives $\mathsf{M}(n) = 9 \cdot 2^\ell \ell + \mathcal{O}(2^\ell)$ with $\ell = \lceil \log_2(n) \rceil$ (hence the behavior of a "staircase" function, see von zur Gathen and Gerhard, 2003, Chapter 8.2).

Then, the results in Fischer and Stockmeyer (1974) and van der Hoeven (1997, 2002) show that half-line multiplication to precision n, *i.e.* with input and output modulo x^n, can be done in time

$$\mathsf{H}(n) = \mathcal{O}\left(\sum_{k=0}^{\lfloor \log_2(n) \rfloor} \frac{n}{2^k} \mathsf{M}(2^k) \right)$$

and that online multiplication to precision n can be done in time $\mathsf{O}(n) = \mathcal{O}(\mathsf{H}(n))$. In all cases, if $\mathsf{M}(n)/n$ is increasing, $\mathsf{H}(n)$ is $\mathcal{O}(\mathsf{M}(n)\log(n))$, since all terms in the sum are bounded from above by $\mathsf{M}(n)$; for naive or Karatsuba's multiplication, $\mathsf{H}(n)$ is actually $\mathcal{O}(\mathsf{M}(n))$. The algorithm introduced by van der Hoeven (2003) for half-line multiplication improves on the one reported above by a constant factor.

Recent progress has been made on online multiplication (van der Hoeven, 2007, 2014): these papers give an online algorithm that multiplies power series on a wide range of rings in time $\mathsf{M}(n)\log(n)^{o(1)}$, which improves on the costs given here. However, this algorithm is significantly more complex; we believe that there is still an interest in developing simpler and reasonably fast algorithms, such as the one given here.

Our contribution In this paper, we introduce a simple and fast algorithm for online multiplication, based on the ideas from van der Hoeven (2003). We compare it to previous algorithms by giving the first precise analysis of the arithmetic complexity of the various online and half-line multiplication algorithms mentioned up to now. For this complexity measure, our algorithm is faster than Fischer and Stockmeyer's by a constant factor; this is confirmed by experimental results. This paper is based on the PhD thesis (Lebreton, 2012). To the best of our knowledge, the complexity estimates of Tables 1 and 2 are published for the first time.

Polynomial multiplication algorithms For the rest of this paper, we will consider the *arithmetic cost* of our algorithms, that is the number of additions and multiplications in $\mathbb{A}$ they perform. The algorithms in this paper rely on two variants of polynomial multiplication, called middle and short products. In order to describe them, we introduce the following notation, used in all that follows: if $a = \sum_i a_i x^i$ is