Journal of Symbolic Computation 68 (2015) 230–258

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Relaxed Hensel lifting of triangular sets ☆

Romain Lebreton

University of Waterloo, Waterloo, ON, Canada

ARTICLE INFO

Article history:
Received 15 October 2013
Accepted 29 March 2014
Available online 19 September 2014

Keywords:
Polynomial system solving
Online algorithm
Relaxed algorithm
Triangular set
Univariate representation
p-Adic integer
Power series

ABSTRACT

In this paper, we present a new lifting algorithm for triangular sets over general p-adic rings. Our contribution is to give, for any p-adic triangular set, a shifted algorithm of which the triangular set is a fixed point. Then we can apply the relaxed recursive p-adic framework and deduce a relaxed lifting algorithm for this triangular set. We compare our algorithm to the existing technique and report on implementations inside the C++ library GEOMSOLVEX of MATHEMAGIX (van der Hoeven et al., 2002). Our new relaxed algorithm is competitive and compare favorably on some examples.

1. Introduction

The introduction is made of five subsections. We present the setting of triangular sets with p-adic coefficients in Section 1.1, together with the statement of our lifting problem. We present in Section 1.2 our model of computation for algorithms on p-adics. Section 1.3 introduces the framework in which online algorithms are used to lift triangular sets. Finally, our results and contributions are stated in Section 1.4, followed by an outline of the paper in Section 1.5.

1.1. Statement of the problem

Our goal in this paper is to extend a growing body of work on *relaxed algorithms* to the context of lifting techniques for *univariate representations* and *triangular sets*.

☆ This work has been partly supported by the ANR grant HPAC (ANR-11-BS02-013).
E-mail address: rlebreton@uwaterloo.ca.

http://dx.doi.org/10.1016/j.jsc.2014.09.012
0747-7171/

It is well-known that, under some regularity conditions, techniques such as Newton iteration can be used to compute a power series root of an equation such as $f(T, x(T)) = 0$, with f in $\Bbbk[T, X]$, or a p-adic integer root of an equation of the form $f(x) = 0$ with f in $\mathbb{Z}[X]$.

Relaxed methods, introduced by van der Hoeven (van der Hoeven, 2002), offer an alternative to Newton iteration. The case of computing one power series root, or one p-adic root, of a *system* of polynomial equations was worked out in van der Hoeven (2011), Berthomieu and Lebreton (2012); for this problem, the relaxed algorithm was seen to behave better than Newton iteration in some cases, for instance for multivariate systems with a large number of equations.

In this paper, we go beyond the case of lifting a single root of a multivariate system: we deal with all roots at once, introducing relaxed algorithms that deal with objects such as univariate and triangular representations. This paper is based on the Ph.D. thesis (Lebreton, 2012).

Example 1. We consider the polynomial system $\boldsymbol{f} = (f_1, f_2)$ in $\mathbb{Z}[X_1, X_2]$ with

$$f_1 := 33X_2^3 + 14699X_2^2 + 6761112X_2 + 276148X_1 - 11842820$$
$$f_2 := X_2^2 + 66X_1X_2 - 75X_2 - 94X_1 - 22.$$

Let $\boldsymbol{t}_0$ be the triangular set of $(\mathbb{Z}/7\mathbb{Z})[X_1, X_2]$, that is a lexicographical Gröbner basis for $X_1 < X_2$, given by

$$\boldsymbol{t}_0 := \left(X_1^2 + 5X_1, X_2^2 + 3X_1X_2 + 2X_2 + 4X_1 + 6\right).$$

We lift the triangular set $\boldsymbol{t}_0$ defined modulo 7 to triangular sets $\boldsymbol{t}$ defined modulo 7^2, 7^3 and so on. At the first step, we have

$$\boldsymbol{t}_1 = \big(X_1^2 + (5 + 5\cdot 7)X_1 + 7,$$
$$X_2^2 + (3 + 2\cdot 7)X_1X_2 + (2 + 3\cdot 7)X_2 + 4X_1 + (6 + 3\cdot 7)\big)$$

in $(\mathbb{Z}/7^2\mathbb{Z})[X_1, X_2]$. We iterate again and find

$$\boldsymbol{t}_2 = \big(X_1^2 + \left(5 + 5\cdot 7 + 6\cdot 7^2\right)X_1 + \left(7 + 7^2\right),$$
$$X_2^2 + \left(3 + 2\cdot 7 + 7^2\right)X_1X_2 + \left(2 + 3\cdot 7 + 5\cdot 7^2\right)X_2$$
$$+ \left(4 + 5\cdot 7^2\right)X_1 + \left(6 + 3\cdot 7 + 6\cdot 7^2\right)\big)$$

in $(\mathbb{Z}/7^3\mathbb{Z})[X_1, X_2]$. The precision is enough to recover the integer triangular set

$$\boldsymbol{t} := \left(X_1^2 - 9X_1 + 56, X_2^2 + 66X_1X_2 - 75X_2 - 94X_1 - 22\right) \in \mathbb{Z}[X_1, X_2].$$

Our techniques of p-adic lifting applies to general p-adic rings. Let R be a commutative domain with unit. We consider an element $p \in R - \{0\}$, and we write R_p for the completion of the ring R for the p-adic valuation. We will assume that $R/(p)$ is a field (equivalently, that p generates a maximal ideal). This is not compulsory but will be useful later on when we deal with linear algebra modulo (p). We also assume that $\bigcap_{i\in\mathbb{N}}(p^i) = \{0\}$, so that R can be seen as a subset of R_p. Note that the set of natural numbers $\mathbb{N}$ contains 0 in this paper.

Two classical examples of p-adic rings are the formal power series ring $\Bbbk[[T]]$, which is the completion of the ring of polynomials $\Bbbk[T]$ for the ideal (T), and the ring of p-adic integers $\mathbb{Z}_p$, which is the completion of the ring of integers $\mathbb{Z}$ for the ideal (p), with p a prime number.

Consider a system of polynomial equations $\boldsymbol{f} = (f_1, \ldots, f_s) \in R[X_1, \ldots, X_s]$. Denote by $\mathcal{I}$ the ideal generated by $(f_1, \ldots, f_s)$ in $Q[X_1, \ldots, X_s]$, where Q is the total field of fractions of R. In what follows, we make the following assumptions, denoted (H):

(1) the algebraic set $V = V(\mathcal{I}) \subset \overline{Q}^s$ has dimension zero in an algebraic closure $\overline{Q}$;
(2) the Jacobian determinant of $(f_1, \ldots, f_s)$ vanishes nowhere on V.