Journal of Symbolic Computation 72 (2016) 182–195

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Common composites of triangular polynomial systems and hash functions ☆

Domingo Gómez-Pérez [a], Jaime Gutierrez [b], Alina Ostafe [c]

[a] Department of Mathematics, University of Cantabria, E-39071 Santander, Spain
[b] Department of Applied Mathematics and Computer Science, University of Cantabria, E-39071 Santander, Spain
[c] Department of Applied Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

ARTICLE INFO

Article history:
Received 29 January 2014
Accepted 29 January 2014
Available online 2 March 2015

Keywords:
Polynomial systems
Composition
Collision

ABSTRACT

We study common composites of triangular polynomial and rational function systems with favorable effects under composition: polynomial degree growth. We construct classes of such systems that do not have common composites. This property makes them suitable for the construction of a recently proposed hash function. We give estimates for the number of collisions of this hash function using these systems. We also mention as future work the study of common composites of systems with sparse representation and pose an open problem related to their usability as hash functions.

1. Introduction

The goal of this paper is to study common composites in certain classes of polynomial and rational function systems. We aim to construct concrete classes of systems that are *J-composite unique*, that is, the composition of any J systems in these classes is unique. We note that in the multivariate case

☆ A.O. would like to thank University of Cantabria for its hospitality and support by the Spanish Ministry Economia y Competitividad MTM2011-24678 during her visits in 2011 and 2012, when this work was initiated. During the preparation of this paper, D.G.-P. was partially supported by the Spanish Government Projects MTM2011-24678 and TIN2011-27479-C04-04, J.G., by the Spanish Ministry Economia y Competitividad MTM2011-24678 and A.O., by the Swiss National Science Foundation Grant PA00P2-139679 and the University of New South Wales Vice Chancellor's Fellowship.

E-mail addresses: domingo.gomez@unican.es (D. Gómez-Pérez), jaime.gutierrez@unican.es (J. Gutierrez), alina.ostafe@unsw.edu.au (A. Ostafe).

http://dx.doi.org/10.1016/j.jsc.2015.02.005
0747-7171/

these are the first results of this type and we hope that such constructions can be of independent interest.

A theorem due to Ritt (1922) states that if a univariate polynomial, whose degree is coprime to the characteristic of the field of coefficients, can be written in two different forms, as composition of J indecomposable polynomials and J' indecomposable polynomials, respectively, then $J = J'$ and there exists a finite chain of transformations that convert one into the other. It is known that Ritt's Theorem does not hold if the hypothesis on the degree and the characteristic of the field of coefficients is omitted. In Gutierrez and Sevilla (2006), the authors construct counterexamples for any field of positive characteristic p, and in von zur Gathen et al. (2010) the authors study the case of lineralized polynomials of degree p^2. The degree of compositions of univariate polynomials grows exponentially on the number of composites. This implies that, in order to obtain systems with slow degree growth under composition, we need to work in the multivariate case.

For multivariate polynomials and rational functions, it is not even clear what the most interesting notions of decompositions are, see Faugère and Perret (2009a, 2009b), Faugère et al. (2010), von zur Gathen et al. (2003), Gutierrez et al. (2002) for different approaches, as well as connections to intermediate subfield problems, which are extensions of the univariate case, and applications to cryptography.

Our motivation for studying classes of systems that are J-composite unique comes from studying hash functions defined by triangular polynomial systems that are masked by compositions with polynomial functions. Hash functions are deterministic procedures that take a block of data of arbitrary length and digest it into a string of fixed size. They are of special importance because they are commonly used in digital signatures and due to the NIST hash function competition, hash functions have attracted considerable attention.

In Ostafe and Shparlinski (2010c), the authors proposed a new construction of hash functions based on compositions of triangular polynomial systems. This construction was motivated by that of Charles et al. (2009) and in some sense it may be considered as its extension.

Studying collisions of this hash function reduces to studying common composites in certain classes of triangular systems that define these functions. Moreover, having a slow degree growth under composition allows us to obtain an estimate for the number of collisions of the hash function.

The paper is structured as follows. In Sections 2.2 and 2.3 we study collisions in compositions of triangular rational function systems with slow degree growth that were introduced in Ostafe and Shparlinski (2010a, 2010b, 2010c). We also give explicit constructions of classes of systems with slow degree growth under composition that are J-composite unique.

In Section 3.1 we study the hash function defined in Ostafe and Shparlinski (2010c) with the systems constructed in Sections 2.2 and 2.3. Moreover, in Section 3.2 we give estimates for the number of collisions of hash values with polynomial systems with slow degree growth. We end this paper by studying common composites of polynomial systems with sparse representation and proposing as an open problem finding bounds on the number of collisions of the hash function with such systems.

We recall that the notation $U = O(V)$ is equivalent to the statement that the inequality $|U| \le c\,V$ holds with some constant $c > 0$ (that may depend on the degrees and the number of variables of the polynomials involved).

2. Common composites of rational function systems

2.1. Composite unique rational function systems

In this section, we introduce some notation and a central concept in this article in its full generality, so we present our results for any general field $\mathbb{K}$ with characteristic $\mathrm{char}(\mathbb{K})$. To refer to the set of nonzero elements of $\mathbb{K}$, we will write $\mathbb{K}^*$. Also, $\mathbb{K}[X_1, \ldots, X_m]$ and $\mathbb{K}(X_1, \ldots, X_m)$ are the ring of polynomials and the rational function field, respectively, in the variables $X_1, \ldots, X_m$ with coefficients in $\mathbb{K}$, $m \ge 2$, and in some cases we need that $m \ge 3$. When this restriction is clear from the context, we do not mention it explicitly.

For a polynomial F in $\mathbb{K}[X_1, \ldots, X_m]$, we denote by $\deg F$ and by $\deg_{X_i} F$ the total degree and the degree with respect to X_i of F, respectively. For a rational function in its lowest terms, that is,