Journal of Complexity 31 (2015) 590–616

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

Polynomial-time algorithms for quadratic isomorphism of polynomials: The regular case

Jérémy Berthomieu [a,b,c,*], Jean-Charles Faugère [c,a,b], Ludovic Perret [a,b,c]

[a] *Sorbonne Universités*, UPMC *Univ Paris 06, Équipe* PolSys, LIP6, *F-75005, Paris, France*

[b] CNRS, UMR *7606*, LIP6, *F-75005, Paris, France*

[c] INRIA, *Équipe* PolSys, *Centre Paris – Rocquencourt, F-75005, Paris, France*

ARTICLE INFO

Article history:
Received 1 April 2014
Accepted 19 March 2015
Available online 12 April 2015

Keywords:
Quadratic forms
Computer algebra
Polynomial isomorphism
Multivariate cryptography
Module isomorphism

ABSTRACT

Let $\mathbf{f} = (f_1, \ldots, f_m)$ and $\mathbf{g} = (g_1, \ldots, g_m)$ be two sets of $m \geq 1$ nonlinear polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ ($\mathbb{K}$ being a field). We consider the computational problem of finding – if any – an invertible transformation on the variables mapping $\mathbf{f}$ to $\mathbf{g}$. The corresponding equivalence problem is known as *Isomorphism of Polynomials with one Secret* (IP1S) and is a fundamental problem in multivariate cryptography. Amongst its applications, we can cite Graph Isomorphism (GI) which reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables, according to Agrawal and Saxena. The main result is a randomized polynomial-time algorithm for solving IP1S for quadratic instances – a particular case of importance in cryptography.

To this end, we show that IP1S for quadratic polynomials can be reduced to a variant of the classical module isomorphism problem in representation theory. We show that we can essentially *linearize* the problem by reducing quadratic-IP1S to test the orthogonal simultaneous similarity of symmetric matrices; this latter problem was shown by Chistov, Ivanyos and Karpinski (ISSAC 1997) to be equivalent to finding an invertible matrix in the linear space $\mathbb{K}^{n\times n}$ of $n \times n$ matrices over $\mathbb{K}$ and to compute the square root in a certain representation in a matrix algebra. While computing square roots of matrices can be done efficiently

[*] Correspondence to: Laboratoire d'Informatique de Paris 6, Université Pierre-et-Marie-Curie, Boîte Courrier 169, 4 place Jussieu, F-75252 Paris Cedex 05, France.

E-mail addresses: jeremy.berthomieu@lip6.fr (J. Berthomieu), jean-charles.faugere@inria.fr (J.-C. Faugère), ludovic.perret@lip6.fr (L. Perret).

http://dx.doi.org/10.1016/j.jco.2015.04.001

using numerical methods, it seems difficult to control the bit complexity of such methods. However, we present exact and polynomial-time algorithms for computing a representation of the square root of a matrix in $\mathbb{K}^{n\times n}$, for various fields (including finite fields), as a product of two matrices. Each coefficient of these matrices lies in an extension field of $\mathbb{K}$ of polynomial degree. We then consider #IP1S, the counting version of IP1S for quadratic instances. In particular, we provide a (complete) characterization of the automorphism group of homogeneous quadratic polynomials. Finally, we also consider the more general *Isomorphism of Polynomials* (IP) problem where we allow an invertible linear transformation on the variables *and* on the set of polynomials. A randomized polynomial-time algorithm for solving IP when $\mathbf{f} = (x_1^d, \ldots, x_n^d)$ is presented. From an algorithmic point of view, the problem boils down to factoring the determinant of a linear matrix (*i.e.* a matrix whose components are linear polynomials). This extends to IP a result of Kayal obtained for PolyProj.

1. Introduction

A fundamental question in computer science is to provide algorithms allowing to test if two given objects are *equivalent* with respect to some transformation. In this paper, we consider equivalence of nonlinear polynomials in several variables. Equivalence of polynomials has profound connections with a rich variety of fundamental problems in computer science, ranging – among others topics – from cryptography (*e.g.* Patarin [42], Tang and Xu [52,53], Yang et al. [58]), arithmetic complexity (*via* Geometric Complexity Theory (GCT) for instance, see [11,32,39,40]), testing low degree affine-invariant properties ([6,27,28], . . .). As we will see, the notion of equivalence can come with different flavours that impact the intrinsic hardness of the problem considered.

In [1,47], the authors show that Graph Isomorphism reduces to equivalence of cubic polynomials with respect to an invertible linear change of variables (a similar reduction holds between $\mathbb{F}$-algebra Isomorphism and cubic equivalence of polynomials). This strongly suggests that solving equivalence problems efficiently is a very challenging algorithmic task.

In cryptography, the hardness of deciding equivalence between two sets of m polynomials with respect to an invertible linear change of variables is the security core of several cryptographic schemes: the seminal zero-knowledge ID scheme of Patarin [42], and more recently group/proxy signature schemes [52,53,58]. Note that there is a subtle difference between the equivalence problem considered in [1,31,47] and the one considered in cryptographic applications.

Whilst Agrawal and Saxena [1]; Kayal [31]; Saxena [47] restrict their attention to $m = 1$, arbitrary $m \geq 1$ is usually considered in cryptographic applications. In the former case, the problem is called *Polynomial Equivalence* (PolyEquiv), whereas it is called *Isomorphism of Polynomials with One Secret* (IP1S) problem in the latter case. We emphasize that the hardness of equivalence can drastically vary in function of m. An interesting example is the case of quadratic forms. The problem is completely solved when $m = 1$, but no polynomial-time algorithm exists for deciding simultaneous equivalence of quadratic forms. In this paper, we make a step ahead to close this gap by presenting a randomized polynomial-time algorithm for solving simultaneous equivalence of quadratic forms over various fields.

Equivalence of multivariate polynomials is also a fundamental problem in Multivariate Public-Key Cryptography (MPKC). This is a family of asymmetric (encryption and signature) schemes whose public-key is given by a set of m multivariate equations [37,42]. To minimize the public-key storage, the multivariate polynomials considered are usually quadratic. The basic idea of MPKC is to construct a public-key which is equivalent to a set of quadratic multivariate polynomials with a specific structure