Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the last fall degree of zero-dimensional Weil descent systems

Ming-Deh A. Huang [a], Michiel Kosters [b], Yun Yang [c], Sze Ling Yeo [d]

[a] USC, United States
[b] UCI, United States
[c] NTU, Singapore
[d] I2R, Singapore

ARTICLE INFO

Article history:
Received 7 September 2016
Accepted 24 June 2017
Available online xxxx

MSC:
13P10
13P15

Keywords:
Polynomial system
Gröbner basis
Last fall degree
Zero-dimensional
First fall degree
Weil descent
HFE
ECDLP

ABSTRACT

In this article we will discuss a mostly theoretical framework for solving zero-dimensional polynomial systems. Complexity bounds are obtained for solving such systems using a new parameter, called the *last fall degree*, which does not depend on the choice of a monomial order. The method is similar to certain MutantXL algorithms, but our abstract formulation has advantages. For example, we can *prove* that the cryptographic systems multi-HFE and HFE are insecure.

More generally, let k be a finite field of cardinality q^n and let k' be the subfield of cardinality q. Let $\mathcal{F} \subset k[X_0, \ldots, X_{m-1}]$ be a finite subset generating a zero-dimensional ideal. We give an upper bound of the last fall degree of the Weil descent system of $\mathcal{F}$ from k to k', which depends on q, m, the last fall degree of $\mathcal{F}$, the degree of $\mathcal{F}$ and the number of solutions of $\mathcal{F}$, but not on n. This shows that such Weil descent systems can be solved efficiently if n grows and the other parameters are fixed. In particular, one can apply these results to show a weakness in the cryptographic protocols HFE and multi-HFE.

E-mail addresses: mdhuang@usc.edu (M.-D.A. Huang), kosters@gmail.com (M. Kosters), YANG0379@e.ntu.edu.sg (Y. Yang), slyeo@i2r.a-star.edu.sg (S.L. Yeo).

http://dx.doi.org/10.1016/j.jsc.2017.08.002
0747-7171/

Please cite this article in press as: Huang, M.-D.A., et al. On the last fall degree of zero-dimensional Weil descent systems. J. Symb. Comput. (2017), http://dx.doi.org/10.1016/j.jsc.2017.08.002

1. Introduction

Let k be a field and let $\mathcal{F} \subset R = k[X_0, \ldots, X_{m-1}]$ be a finite subset which generates a zero-dimensional ideal I. By this we mean that $\dim_k(R/I) = e < \infty$. Let $R_{\leq i}$ be the set of polynomials in R of degree at most i. Suppose that we want to find the finitely many solutions of $\mathcal{F}$ in k^m (or in $\overline{k}^m$). We denote an algebraic closure of k by $\overline{k}$.

One of the most common methods is the following. First fix a monomial order on R, such as the degree reverse lexicographic order, and then compute a Gröbner basis of the ideal generated by $\mathcal{F}$ using for example F_4 or F_5 (Faugère, 1999, 2002). Then one computes a Gröbner basis for the lexicographic order using FGLM (Faugère et al., 1993), and one uses this to find all the solutions. It is often very hard to estimate the complexity of such algorithms. The largest degree which one sees in such a computation of a Gröbner basis for the degree reverse lexicographic order is called the *degree of regularity*, and this degree essentially determines the complexity of such algorithms. One approach to obtain heuristic complexity bounds on the degree of regularity is the use of the so-called *first fall degree assumption*. For $i \in \mathbf{Z}_{\geq 0}$, we let $V_{\mathcal{F},i}$ be the smallest k-vector space of $R_{\leq i}$ such that

i. $\{f \in \mathcal{F} : \deg(f) \leq i\} \subseteq V_{\mathcal{F},i}$;
ii. if $g \in V_{\mathcal{F},i}$ and if $h \in R$ with $\deg(hg) \leq i$, then $hg \in V_{\mathcal{F},i}$.

The first fall degree is defined to be the first d such that $V_{\mathcal{F},d} \cap R_{\leq d-1} \neq V_{\mathcal{F},d-1}$ (and if it does not exist, it is defined to be 0; note that this definition of the first fall degree differs slightly from most definitions as in Petit and Quisquater, 2012, but behaves a lot better). The heuristic claim is that the first fall degree is close to the degree of regularity for many systems (see for example Petit and Quisquater, 2012). A quote from Ding and Hodges (2011) is "Our conclusions rely on no heuristic assumptions beyond the standard assumption that the Gröbner basis algorithms terminate at or shortly after the degree of regularity" (note that in Ding and Hodges, 2011 the definition of degree of regularity coincides with the first fall degree definition of Petit and Quisquater, 2012). It is quite often easy to give an upper bound on the first fall degree, just by counting arguments (see Ding and Hodges, 2011 for example). However, in Kosters and Yeo (2015), the second and third author of this article raise doubt to the first fall degree heuristic.

In the first part of this article, section 2, we will try to rectify the situation. We will define the notion of *last fall degree*, which is the largest d such that $V_{\mathcal{F},d} \cap R_{\leq d-1} \neq V_{\mathcal{F},d-1}$. We denote the last fall degree of $\mathcal{F}$ by $d_{\mathcal{F}}$. We show how one can solve the system by computing $V_{\mathcal{F},\max\{d_{\mathcal{F}},e\}}$ and multivariate factoring algorithms (Proposition 2.11). We will also prove different properties of the last fall degree, for example, that the degree of regularity is bounded below by the last fall degree and above by the maximum of e and the last fall degree. Furthermore, the last fall degree behaves well with respect to certain operations (such as linear change of variables and linear change of equations). It must be said that we do not know how to compute the last fall degree without having an upper bound, say coming from the degree of regularity. We will compare our approach with other approaches for solving systems, most notably with MutantXL and standard Gröbner basis algorithms (Subsection 2.5).

In the second part of this article, Section 3 and Section 4, we will give an application of our new framework around the last fall degree. Assume that k is a finite field of cardinality q^n with subfield k' of cardinality q. Let $\mathcal{F}'$ be the Weil descent system of $\mathcal{F}$ to k'. This is the system one obtains when one expresses all equations with the help of a basis of k/k'. This is a system in nm variables and hence seems to be much harder to solve than the original system. We give upper bounds on $d_{\mathcal{F}'}$ in terms of q, m, $d_{\mathcal{F}}$, the degree of $\mathcal{F}$ and the number of solutions of $\mathcal{F}$, but not on n. This generalizes practical and mathematical results, if $m = 1$ (Bettale et al., 2013; Ding and Hodges, 2011; Faugère and Joux, 2003; Petit, 2013). This shows that some versions of multi-HFE (HFE stands for hidden field equations) are much easier to tackle than one would expect. Let us now give a precise formulation of the main theorem.

We denote by $Z(\mathcal{F})$ the set of zeros of $\mathcal{F}$ over $\overline{k}$. For $r \in \mathbf{R}_{\geq 0}$ and $c, t \in \mathbf{R}_{\geq 1}$ we set

$$\tau(r, c, t) = \lfloor 2t(c-1)\left(\log_c\left(\frac{r}{2t} + 1\right) + 1\right)\rfloor.$$

Note that this function increases when r increases.

Please cite this article in press as: Huang, M.-D.A., et al. On the last fall degree of zero-dimensional Weil descent systems. J. Symb. Comput. (2017), http://dx.doi.org/10.1016/j.jsc.2017.08.002