Research Article

Stavros Kousidis* and Andreas Wiemers

On the first fall degree of summation polynomials

https://doi.org/10.1515/jmc-2017-0022
Received April 26, 2017; revised March 22, 2019; accepted May 17, 2019

Abstract: We improve on the first fall degree bound of polynomial systems that arise from a Weil descent along Semaev's summation polynomials relevant to the solution of the Elliptic Curve Discrete Logarithm Problem via Gröbner basis algorithms.

Keywords: Polynomial systems, Gröbner bases, discrete logarithm problem, elliptic curve cryptosystem

MSC 2010: 13P15, 13P10, 14H52

Communicated by: María González Vasco

1 Introduction

Finding solutions to algebraic equations is a fundamental task. A common approach is a Gröbner basis computation via an algorithm such as Faugère's $F4$ and $F5$ (see [4, 5]). In recent applications, Gröbner basis techniques have become relevant to the solution of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Here one seeks solutions to polynomial equations arising from a Weil descent along Semaev's summation polynomials [13] which represents a crucial step in an index calculus method for the ECDLP; see, e.g., [12, 14]. The efficiency of Gröbner basis algorithms is governed by a so-called *degree of regularity*, that is, the highest degree occurring along the subsequent computation of algebraic relations. It is widely believed that this often intractable complexity parameter is closely approximated by the degree of the first non-trivial algebraic relation, the *first fall degree*. In particular, the algorithms for the ECDLP of Petit and Quisquater [12] are sub-exponential under the assumption that this approximation is in $o(1)$.

In the present paper, we will improve Petit's and Quisquater's [12] first fall degree bound $m^2 + 1$ for the system arising from the Weil descent along Semaev's $(m + 1)$-th summation polynomial. That is, we prove that a degree fall occurs at degree $m^2 - m + 1$ by exhibiting the highest degree homogeneous part of that polynomial system. In fact, this degree is $m^2 - m$, so that we expect the bound to be sharp except for the somewhat pathological case $m = 2$ that has been discussed by Kosters and Yeo [10]. This allows us to sharpen the asymptotic run time of the index calculus algorithm for the ECDLP as exhibited in the complexity analysis of Petit and Quisquater [12].

***Corresponding author: Stavros Kousidis,** Federal Office for Information Security, Godesberger Allee 185–189, 53175 Bonn, Germany, e-mail: st.kousidis@googlemail.com. https://orcid.org/0000-0002-6947-4963
Andreas Wiemers, Federal Office for Information Security, Godesberger Allee 185–189, 53175 Bonn, Germany, e-mail: alterego@web.de

2 The first fall degree

The notion of the first fall has been described by Faugère and Joux [6, Section 5.1], Granboulan, Joux and Stern [7, Section 3], Dubois and Gama [3, Section 2.2] and Ding and Hodges [2, Section 3]. Although the concept of the first fall degree has been called *minimal degree* [6] and *degree of regularity* [2, 3, 7], we actually adopt the terminology and definition of Hodges, Petit and Schlather [8]. For readability reasons we include a brief and tailored account of the first fall degree and refer the reader to [8, Section 2] for details and greater generality.

Our considerations take place over a degree n extension $\mathbb{F}_{2^n}$ of the binary field $\mathbb{F}_2$. Consider the decomposition of the graded ring

$$S = \mathbb{F}_{2^n}[X_0, \dots, X_{N-1}]/(X_0^2, \dots, X_{N-1}^2)$$

into its homogeneous components

$$S = S_0 \oplus S_1 \oplus \cdots \oplus S_N.$$

Each S_j is the $\mathbb{F}_{2^n}$-vector space generated by the monomials of degree j. Let I be an ideal in S generated by homogeneous polynomials $h_1, \dots, h_r \in S_d$ all of the same degree d. Then we have a surjective map

$$\phi : S^r \to I, \quad (g_1, \dots, g_r) \mapsto g_1 h_1 + \cdots + g_r h_r.$$

Without loss of generality we furthermore assume

$$0 < r = \dim_{\mathbb{F}_{2^n}} \sum_{j=1}^{r} \mathbb{F}_{2^n} h_j.$$

Let e_i denote the canonical i-th basis element of the free S-module S^r. The S-module U generated by the elements

$$h_j e_i + h_i e_j \quad \text{and} \quad h_k e_k, \quad \text{where } i, j, k = 1, \dots, r,$$

is a subset of $\ker(\phi)$. If we restrict ϕ to the $\mathbb{F}_{2^n}$-subvector space $S^r_{j-d} \subset S^r$, we obtain a surjective map

$$\phi_{j-d} : S^r_{j-d} \to I \cap S_j$$

whose kernel contains the $\mathbb{F}_{2^n}$-subvector space $U_{j-d} = U \cap S^r_{j-d}$ and hence factors through

$$\bar{\phi}_{j-d} : S^r_{j-d}/U_{j-d} \to I \cap S_j.$$

Definition 2.1 (cf. [8, Definition 2.1]). The first fall degree of a homogeneous system $h_1, \dots, h_r \in S_d$ and its linear span $\sum_{j=1}^r \mathbb{F}_{2^n} h_j$, respectively, is the smallest j such that the induced $\mathbb{F}_{2^n}$-linear map $\bar{\phi}_{j-d}$ is not injective, that is, the smallest j such that $\dim_{\mathbb{F}_{2^n}}(I \cap S_j) < \dim_{\mathbb{F}_{2^n}}(S^r_{j-d}/U_{j-d})$. It is denoted by $D_{ff}(\sum_{j=1}^r \mathbb{F}_{2^n} h_j)$.

Following [8], we now consider the ring of functions

$$A_{\mathbb{F}_{2^n}} = \mathbb{F}_{2^n}[X_0, \dots, X_{N-1}]/(X_0^2 - X_0, \dots, X_{N-1}^2 - X_{N-1})$$

as a finite-dimensional filtered algebra whose filtration components $[A_{\mathbb{F}_{2^n}}]_d$, $d \in \mathbb{N}$, are given by the polynomials up to degree d. The associated graded ring of $A_{\mathbb{F}_{2^n}}$ is

$$\mathrm{Gr}(A_{\mathbb{F}_{2^n}}) = \mathbb{F}_{2^n}[X_0, \dots, X_{N-1}]/(X_0^2, \dots, X_{N-1}^2),$$

whose graded components

$$[\mathrm{Gr}(A_{\mathbb{F}_{2^n}})]_d = [A_{\mathbb{F}_{2^n}}]_d / [A_{\mathbb{F}_{2^n}}]_{d-1} \quad \text{for } d \in \mathbb{N}$$

are given by the homogeneous polynomials of degree d. Any linear subspace $V \subset [A_{\mathbb{F}_{2^n}}]_d$ induces a homogeneous linear subspace $\bar{V} \subset [\mathrm{Gr}(A_{\mathbb{F}_{2^n}})]_d$ via the canonical projection $\pi_d : [A_{\mathbb{F}_{2^n}}]_d \to [\mathrm{Gr}(A_{\mathbb{F}_{2^n}})]_d$.

Definition 2.2 (cf. [8, Definition 2.2]). Consider a polynomial system $p_1, \dots, p_r \in [A_{\mathbb{F}_{2^n}}]_d$ and its linear span $V = \sum_{j=1}^r \mathbb{F}_{2^n} p_j \subset [A_{\mathbb{F}_{2^n}}]_d$, respectively. We assume without loss of generality that $\dim_{\mathbb{F}_{2^n}} V = r > 0$. The first

fall degree of V is

$$D_{ff}(V) = \begin{cases} d, & \dim_{\mathbb{F}_{2^n}} \bar{V} < \dim_{\mathbb{F}_{2^n}} V, \\ D_{ff}(\bar{V}) & \text{else}, \end{cases}$$

where $D_{ff}(\bar{V} = \sum_{j=1}^{r} \mathbb{F}_{2^n} \pi_d(p_j))$ is given in Definition 2.1.

3 Weil descent along summation polynomials

We prove that the first fall degree of the polynomial system that arises from a Weil descent along Semaev's summation polynomial S_{m+1} is bounded from above by $m^2 - m + 1$. This is an improvement over $m^2 + 1$ that results from [8, Theorem 5.2] and [12, Section 4]. Let us briefly introduce the summation polynomials and describe the Weil descent.

Semaev [13] introduced the m-th summation polynomial $S_m(x_1, \ldots, x_m) \in \mathbb{K}[x_1, \ldots, x_m]$ on an elliptic curve $E : y^2 = x^3 + a_4x + a_6$ over a finite field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) \neq 2, 3$ by the following defining property: for elements $x_1, \ldots, x_m$ in the algebraic closure $\bar{\mathbb{K}}$ one has $S_m(x_1, \ldots, x_m) = 0$ if and only if there exist $y_1, \ldots, y_m \in \bar{\mathbb{K}}$ such that $(x_1, y_1), \ldots, (x_m, y_m) \in E(\bar{K})$ and $(x_1, y_1) + \cdots + (x_m, y_m) = 0$ on E. Semaev gave a recursive formula based on resultants to compute those polynomials and described some properties [13, Theorem 1]. The summation polynomials can also be given in characteristic 2. We consider $\mathbb{K} = \mathbb{F}_{2^n}$, an ordinary, i.e. non-singular, elliptic curve $E : y^2 + xy = x^3 + a_2x^2 + a_6$, and the projection to the x-coordinate $x(P_i) = x(x_i, y_i) = x_i$ of $P_i \in E$. Then still

$$S_2(x_1, x_2) = x_1 - x_2,$$

and from Diem's general description [1, Lemma 3.4, Lemma 3.5] one can deduce

$$S_3(x_1, x_2, x_3) = (x_1^2 + x_2^2)x_3^2 + x_1x_2x_3 + x_1^2x_2^2 + a_6$$
$$S_{m+1}(x_1 \ldots, x_m, x_{m+1}) = \mathrm{Res}_X(S_m(x_1, \ldots, x_{m-1}, X), S_3(x_m, x_{m+1}, X))$$

and the degree of S_{m+1} in each variable x_i is 2^{m-1}. Note that these formulas have also been outlined by Petit and Quisquater [12, Section 5] who also refer to Diem [1].

To describe the Weil descent along those summation polynomials (see, e.g., [12, Section 4]) we fix a basis $1, z, \ldots, z^{n-1}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let W be a subvector space in $\mathbb{F}_{2^n}$ of dimension n' and basis $\nu_1, \ldots, \nu_{n'}$ over $\mathbb{F}_2$. We introduce mn' variables y_{ij} that model the linear constraints

$$x_i = \sum_{l=1}^{n'} y_{il}\nu_l,$$

set x_{m+1} to an arbitrary element $c \in \mathbb{F}_{2^n}$, and obtain the equation system

$$S_{m+1}(x_1, \ldots, x_m, c) = S_{m+1}\Big(\sum_{l=1}^{n'} y_{1l}\nu_l, \ldots, \sum_{l=1}^{n'} y_{ml}\nu_l, c\Big) = f_0(y_{ij}) + zf_1(y_{ij}) + \cdots + z^{n-1}f_{n-1}(y_{ij}).$$

The first fall degree of interest is that of the reduced polynomial system

$$s_k \equiv f_k \bmod (y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'}), \quad \text{where } k = 0, \ldots, n-1. \tag{3.1}$$

Note that $s_0, \ldots, s_{n-1} \in \mathbb{F}_2[y_{11}, \ldots, y_{mn'}]/(y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'})$.

By the definition of the first fall degree, we are interested in the highest degree homogeneous part of $s_0, \ldots, s_{n-1}$ whose degree can be determined as follows.

Lemma 3.1. *Let $m \geq 3$. The highest degree homogeneous part of the polynomial system*

$$s_0, \ldots, s_{n-1} \in \mathbb{F}_2[y_{11}, \ldots, y_{mn'}]/(y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'})$$

from equation (3.1) *is induced by the monomial*

$$(x_1 \cdots x_m)^{2^{m-1}-1} \cdot x_{m+1}$$

in the summation polynomial $S_{m+1}(x_1, \ldots, x_m, x_{m+1})$, and hence its degree is less than or equal to $m^2 - m$.

Proof. First, we show the existence of the monomial $(x_1 \cdots x_m)^{2^{m-1}-1} \cdot x_{m+1}$ in $S_{m+1}(x_1, \ldots, x_m, x_{m+1})$. We have

$$S_3(x_1, x_2, x_3) = (x_1^2 + x_2^2)x_3^2 + x_1x_2x_3 + x_1^2x_2^2 + a_6$$
$$S_{m+1}(x_1 \ldots, x_m, x_{m+1}) = \mathrm{Res}_X(S_m(x_1, \ldots, x_{m-1}, X), S_3(x_m, x_{m+1}, X))$$

and the degree of S_{m+1} in each variable x_i is 2^{m-1}. The resultant of $f, g \in \mathbb{F}_{2^n}[X]$ of degree k and l is the determinant of the Sylvester matrix

$$\mathrm{Res}_X(f, g) = \det(\mathrm{Syl}(f, g)) = \det \begin{pmatrix} f_k & \cdots & f_0 & & \\ & f_k & \cdots & f_0 & \\ & \ddots & & & \ddots \\ & & f_k & \cdots & f_0 \\ g_l & \cdots & g_0 & & \\ & g_l & \cdots & g_0 & \\ & \ddots & & & \ddots \\ & & g_l & \cdots & g_0 \end{pmatrix}.$$

That is, with

$$S_3(x_m, x_{m+1}, X) = (x_m^2 + x_{m+1}^2)X^2 + x_mx_{m+1}X + x_m^2x_{m+1}^2 + a_6$$
$$S_m(x_1, \ldots, x_{m-1}, X) = c_{2^{m-2},m}X^{2^{m-2}} + \cdots + c_{0,m},$$

where each $c_{i,m} \in \mathbb{F}_{2^n}[x_1, \ldots, x_{m-1}]$, we have

$$S_{m+1}(x_1 \ldots, x_m, x_{m+1}) = \det(\mathrm{Syl}(S_m, S_3)).$$

To be concrete, $\mathrm{Syl}(S_m, S_3)$ is the matrix

$$\begin{pmatrix} c_{2^{m-2},m} & c_{2^{m-2}-1,m} & \cdots & c_{0,m} & 0 \\ 0 & c_{2^{m-2},m} & \cdots & c_{1,m} & c_{0,m} \\ x_m^2 + x_{m+1}^2 & x_mx_{m+1} & x_m^2x_{m+1}^2 + t & & \\ & \ddots & & \ddots & \\ & & x_m^2 + x_{m+1}^2 & x_mx_{m+1} & x_m^2x_{m+1}^2 + t \end{pmatrix}$$

with a total of $2^{m-2} + 2$ rows and columns. In order to prove our claim we have to identify specific summands in the Leibniz formula of the determinant. That is, we consider

$$\det(\mathrm{Syl}(S_m, S_3)) = \sum_{\pi} \mathrm{sgn}(\pi) \prod_{i=1}^{2^{m-2}+2} \mathrm{Syl}(S_m, S_3)_{i,\pi_i} \tag{3.2}$$

and argue that for the relevant summands no cancellation over $\mathbb{F}_{2^n}$ occurs. Note that the sign of a permutation is $1 \in \mathbb{F}_{2^n}$.

Step 1: Prove by induction (start with $x_1^2x_2^2$ in S_3) that S_{m+1} contains the monomial $(x_1 \cdots x_m)^{2^{m-1}}$ in its term $c_{0,m+1}$. For that we consider the permutation

$$\sigma = (\sigma_1, \ldots, \sigma_{2^{m-2}+2}) = (2^{m-2} + 1, 2^{m-2} + 2, 1, 2, \ldots, 2^{m-2}) \tag{3.3}$$

and obtain

$$\begin{aligned} S_{m+1}(x_1 \ldots, x_m, x_{m+1}) &= \mathrm{sgn}(\sigma) \prod_{i=1}^{2^{m-2}+2} \mathrm{Syl}(S_m, S_3)_{i,\sigma_i} + \cdots \\ &= c_{0,m}c_{0,m} \prod_{i=1}^{2^{m-2}} (x_m^2 + x_{m+1}^2) + \cdots \\ &= \left((x_1 \cdots x_{m-1})^{2^{m-2}}\right)^2 \cdot x_m^{2^{m-1}} + \cdots \\ &= (x_1 \cdots x_{m-1}x_m)^{2^{m-1}} + \cdots. \end{aligned}$$

Note that specifying $\sigma_1 = 2^{m-2} + 1$ and $\sigma_2 = 2^{m-2} + 2$ determines σ since the remaining entries in $\mathrm{Syl}(S_m, S_3)$ form an upper triangular matrix with $x_m^2 + x_{m+1}^2$ on the diagonal.

Step 2: Prove by induction (start with $x_1x_2x_3$ in S_3) that S_{m+1} contains the monomial $(x_1 \cdots x_m)^{2^{m-1}-1} \cdot x_{m+1}$, i.e. $(x_1 \cdots x_m)^{2^{m-1}-1}$ in its term $c_{1,m+1}$. For that we consider the permutation

$$\tau = (\tau_1, \ldots, \tau_{2^{m-2}+2}) = (2^{m-2}, 2^{m-2} + 2, 1, \ldots, 2^{m-2} - 1, 2^{m-2} + 1) \tag{3.4}$$

and obtain

$$\begin{aligned} S_{m+1}(x_1 \ldots, x_m, x_{m+1}) &= \operatorname{sgn}(\tau) \prod_{i=1}^{2^{m-2}+2} \mathrm{Syl}(S_m, S_3)_{i,\tau_i} + \cdots \\ &= c_{1,m}c_{0,m} \cdot x_m x_{m+1} \prod_{i=1}^{2^{m-2}-1} (x_m^2 + x_{m+1}^2) + \cdots \\ &= (x_1 \cdots x_{m-1})^{2^{m-2}-1} \cdot (x_1 \cdots x_{m-1})^{2^{m-2}} \cdot x_m x_{m+1} (x_m^2)^{2^{m-2}-1} + \cdots \\ &= (x_1 \cdots x_{m-1}x_m)^{2^{m-1}-1} \cdot x_{m+1} + \cdots . \end{aligned}$$

Note that specifying $\tau_1 = 2^{m-2}$ and $\tau_2 = 2^{m-2} + 2$ determines τ since the remaining entries in $\mathrm{Syl}(S_m, S_3)$ form an upper triangular matrix with $x_m^2 + x_{m+1}^2, \ldots, x_m^2 + x_{m+1}^2, x_m x_{m+1}$ on the diagonal.

Second, in order to exclude potential cancellations we have to show that the permutations σ in (3.3) and τ in (3.4) are the only possible choices to produce the monomials $(x_1 \cdots x_m)^{2^{m-1}}$ and $(x_1 \cdots x_m)^{2^{m-1}-1} \cdot x_{m+1}$ in S_{m+1}, respectively. For that, we prove by induction (start with x_1x_2 in S_3) that the only multiples of $(x_1 \cdots x_m)^{2^{m-1}-1}$ in the coefficients of S_{m+1} are $(x_1 \cdots x_m)^{2^{m-1}}$ in $c_{0,m+1}$ and $(x_1 \cdots x_m)^{2^{m-1}-1}$ in $c_{1,m+1}$. Indeed, the factor $(x_1 \cdots x_{m-1})^{2^{m-1}-1}$ in the variables $x_1, \ldots, x_{m-1}$ can only be produced by products $c_{i,m} \cdot c_{j,m}$ of entries taken from the first two rows of the Sylvester matrix $\mathrm{Syl}(S_m, S_3)$. Since the degree of S_m in each variable $x_1, \ldots, x_{m-1}$ is 2^{m-2}, each of the entries $c_{0,m}, \ldots, c_{2^{m-2},m}$ is a sum of monomials in the variables $x_1, \ldots, x_{m-1}$ where each monomial is either

(i) no multiple of $(x_1 \cdots x_{m-1})^{2^{m-2}-1}$ or

(ii) a multiple $(x_1 \cdots x_{m-1})^{2^{m-2}-1} \cdot x_1^{\delta_1} \cdots x_{m-1}^{\delta_{m-1}}$, with $\delta_i \in \{0, 1\}$.

Therefore, the monomials in the products $c_{i,m} \cdot c_{j,m}$ that contribute to the determinant (3.2) occur in the following forms:

$$((x_1 \cdots x_{m-1})^{2^{m-2}-1})^2 \cdot x_1^{\delta_1+\delta_1'} \cdots x_{m-1}^{\delta_{m-1}+\delta_{m-1}'}, \tag{3.5}$$

$$(x_1 \cdots x_{m-1})^{2^{m-2}-1} \cdot x_1^{\delta_1} \cdots x_{m-1}^{\delta_{m-1}} \cdot \mu, \tag{3.6}$$

$$\mu \cdot \mu', \tag{3.7}$$

where μ and μ' denote elements that are no multiples of $(x_1 \cdots x_{m-1})^{2^{m-2}-1}$. Consequently, a monomial in the product $c_{i,m} \cdot c_{j,m}$ that is now a multiple of $(x_1 \cdots x_{m-1})^{2^{m-1}-1}$ can only arise in case (3.5) if for each $k = 1, \ldots, m-1$ the following condition holds:

$$2 \cdot (2^{m-2} - 1) + \delta_k + \delta_k' \geq 2^{m-1} - 1 \quad \Longleftrightarrow \quad \delta_k + \delta_k' \geq 1.$$

Due to the degree restriction of S_m, a product $c_{i,m} \cdot c_{j,m}$ where the monomials in $c_{i,m}$ and $c_{j,m}$ are all of the form (3.6) or (3.7) cannot produce a multiple of $(x_1 \cdots x_{m-1})^{2^{m-1}-1}$. Therefore, we are left with products of the terms $c_{0,m}$ and $c_{1,m}$ by the induction hypothesis. Since $c_{1,m} \cdot c_{1,m}$ only produces $(x_1 \cdots x_{m-1})^{2^{m-1}-2}$, the permutations $\pi = (\pi_1, \pi_2, \ldots, \pi_{2^{m-2}+2})$ in the Leibniz formula (3.2) that produce multiples of the monomial $(x_1 \cdots x_{m-1})^{2^{m-1}-1}$ must have either $(\pi_1, \pi_2) = (\sigma_1, \sigma_2)$ or $(\pi_1, \pi_2) = (\tau_1, \tau_2)$ as given in (3.3) and (3.4), respectively. This determines our permutations σ and τ completely.

To finish the proof, our degree claim in Lemma 3.1 is argued as follows. The variables y_{ij} of the s_k are over $\mathbb{F}_2$, where taking squares is a linear operation. Therefore, the degrees of the homogeneous parts of the system $s_0, \ldots, s_{n-1}$ depend only on the Hamming weight $\mathrm{wt}(x_1^{\alpha_1} \cdots x_m^{\alpha_m}) = \sum \mathrm{wt}(\alpha_i)$ of a monomial in S_{m+1}. Since the degree of S_{m+1} in each variable x_i is 2^{m-1}, the monomial $(x_1 \cdots x_m)^{2^{m-1}-1} \cdot x_{m+1}$, when x_{m+1} is set to

an element $c \in \mathbb{F}_{2^n}$, produces the highest Hamming weight $\sum_{i=1}^{m} \mathrm{wt}(2^{m-1}-1) = m(m-1)$. To be precise, we consider

$$x_i^{2^j} = \Big(\sum_{l=1}^{n'} y_{il} v_l\Big)^{2^j} = \sum_{l=1}^{n'} y_{il} v_l^{2^j}$$

and obtain

$$(x_1 \cdots x_m)^{2^{m-1}-1} \cdot c = c \prod_{i=1}^{m} \prod_{j=0}^{m-2} \sum_{l=1}^{n'} y_{il} v_l^{2^j}, \tag{3.8}$$

which is of degree less than or equal to $m(m-1)$ in the variables y_{ij}. □

We are ready to prove the main result.

Theorem 3.2. *Let $n' \geq m \geq 3$ and $c \in \mathbb{F}_{2^n} \setminus \{0\}$, and consider the polynomial system*

$$s_0, \ldots, s_{n-1} \in \mathbb{F}_2[y_{11}, \ldots, y_{mn'}]/(y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'})$$

from equation (3.1)*, that results from the Weil descent along the summation polynomial $S_{m+1}(x_1, \ldots, x_m, c)$. The first fall degree of $s_0, \ldots, s_{n-1}$ is less than or equal to $m^2 - m + 1$.*

Proof. Consider the finite-dimensional filtered algebra

$$A_{\mathbb{F}_2} = \mathbb{F}_2[y_{11}, \ldots, y_{mn'}]/(y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'}).$$

The linear span

$$\sum_{j=0}^{n-1} \mathbb{F}_2 s_j$$

is inside the degree $d = m^2 - m$ subspace of the filtered algebra $A_{\mathbb{F}_2}$ due to Lemma 3.1. By [8, Corollary 2.4], an extension of the base field, i.e.

$$A_{\mathbb{F}_{2^n}} = \mathbb{F}_{2^n}[y_{11}, \ldots, y_{mn'}]/(y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'}),$$

does not affect the first fall degree. That is,

$$Dff\Big(\sum_{j=0}^{n-1} \mathbb{F}_2 s_j\Big) = Dff\Big(\sum_{j=0}^{n-1} \mathbb{F}_{2^n} s_j\Big).$$

By [8, Definition 2.2], the first fall degree of the subspace $\sum_{j=0}^{n-1} \mathbb{F}_{2^n} s_j$ of $A_{\mathbb{F}_{2^n}}$ is

$$Dff\Big(\sum_{j=0}^{n-1} \mathbb{F}_{2^n} s_j\Big) = \begin{cases} d = m^2 - m, & \dim_{\mathbb{F}_{2^n}} \bar{V} < \dim_{\mathbb{F}_{2^n}} V \\ Dff(\bar{V}) & \text{else,} \end{cases}$$

where $\bar{V}$ denotes the induced homogeneous subspace of $\sum_{j=0}^{n-1} \mathbb{F}_{2^n} s_j$ in the associated graded ring

$$\mathrm{Gr}(A_{\mathbb{F}_{2^n}}) = \mathbb{F}_{2^n}[y_{11}, \ldots, y_{mn'}]/(y_{11}^2, \ldots, y_{mn'}^2).$$

If $\dim_{\mathbb{F}_{2^n}} \bar{V} < \dim_{\mathbb{F}_{2^n}} V$, our claim follows. Otherwise we consider the polynomial

$$P_0 = c \prod_{i=1}^{m} \prod_{j=0}^{m-2} \sum_{l=1}^{n'} y_{il} v_l^{2^j},$$

which is an element of the homogeneous subspace $\bar{V}$ by Lemma 3.1, and in particular equation (3.8). Now, for any

$$x_k = \sum_{l=1}^{n'} y_{kl} v_l$$

we have a non-trivial relation

$$x_k P_0 = c \sum_{l=1}^{n'} y_{kl}^2 v_l^2 \cdot \prod_{j=1}^{m-2} \sum_{l=1}^{n'} y_{kl} v_l^{2^j} \cdot \prod_{i=1, i\neq k}^{m} \prod_{j=0}^{m-2} \sum_{l=1}^{n'} y_{il} v_l^{2^j} = 0 \in \mathrm{Gr}(A_{\mathbb{F}_{2^n}})$$

of degree $d+1 = m^2 - m + 1$ unless $P_0 = 0 \in \mathrm{Gr}(A_{\mathbb{F}_{2^n}})$. Therefore, it remains to show that $P_0 \neq 0$. For that purpose, we recall that $c \in \mathbb{F}_{2^n} \setminus \{0\}$, $v_1, \ldots, v_{n'}$ are linearly independent, and $n' \geq m$. Consider the linear change of variables

$$Y_{ij} = x_i^{2^j} = \Big(\sum_{l=1}^{n'} y_{il} v_l \Big)^{2^j} = \sum_{l=1}^{n'} y_{il} v_l^{2^j}.$$

This is induced by the $m \times n'$ matrix

$$\begin{pmatrix} v_1 & \cdots & v_{n'} \\ v_1^2 & \cdots & v_{n'}^2 \\ \vdots & \ddots & \vdots \\ v_1^{2^{m-2}} & \cdots & v_{n'}^{2^{m-2}} \end{pmatrix}$$

that can be completed to an invertible linear transform by [11, Lemma 3.51] since we have assumed $v_1, \ldots, v_{n'}$ to be linearly independent and $n' \geq m$. By using such an invertible linear transform on any block of variables

$$y_{i1}, \ldots, y_{in'},$$

we get new variables

$$Y_{10}, \ldots, Y_{m,n'-1}.$$

Under this change of variables, P_0 is mapped to the non-zero element

$$c \prod_{i=1}^{m} \prod_{j=0}^{m-2} Y_{ij} \in \mathbb{F}_{2^n}[Y_{10}, \ldots, Y_{m,n'-1}]/(Y_{10}^2, \ldots, Y_{m,n'-1}^2). \qquad \square$$

Remark 3.3. Our Theorem 3.2 remains true also in the case $m = 2$ with first fall degree less than or equal to $2 \cdot 1 + 1 = 3$. This bound is not sharp though, in fact the first fall degree in the case $m = 2$ equals 2 [10, Corollary 4.11 and Remark 4.12].

4 Experiments and conclusion

In the light of the first fall degree bound given in Theorem 3.2, we computed a Gröbner basis for the ideal resulting from the Weil descent along the summation polynomial $S_{m+1}(x_1, \ldots, x_m, x_{m+1})$ for $m = 2, 3, 4$ on an AMD Opteron CPU with Magma's `GroebnerBasis()` function. Again, we set the verbose level to 1 and extracted the empirical first fall degree D_{ff} as the step degree of the first step where new lower degree (i.e. less than step degree) polynomials are added. The empirical degree of regularity D_{reg} is the highest step degree that appears during the Gröbner basis computation. In each experiment we chose a random non-singular elliptic curve over $\mathbb{F}_{2^n}$, a random subvector space of dimension $n' = \lceil n/m \rceil$ as the factor basis, and set x_{m+1} to the x-coordinate of a random point on the curve. The experimental results that extend the ones present in the literature by Petit and Quisquater [12] and Kosters and Yeo [10] are displayed in Table 1.

Like Kosters and Yeo [10, Section 5], we observed a raise in the regularity degree for $m = 2$ in our experiments and were able to verify their observation that with the low degree polynomials $W = \mathrm{span}\{1, z, \ldots, z^{n'}\}$ chosen as the factor basis (cf. [14, Section 4.5]) the raise in the regularity degree was produced for slightly greater $n = 45$. It would be very interesting to observe a raise in the degree of regularity for higher Semaev polynomials, but time and memory amounts become a serious issue for $m \geq 3$. However, such observations might neither falsify [12, Assumption 2] that $D_{\mathrm{reg}} = D_{ff} + o(1)$ nor lead to further evidence that the gap between the degree of regularity and the first fall degree depends on n as discussed in [9, Section 5.2].

However, we believe our first fall degree bound $m^2 - m + 1$ for Semaev polynomials to be sharp for $m \geq 3$, and rephrase [12, Assumption 2] as the following question:

$$D_{\mathrm{reg}} = m^2 - m + 1 + o(1)\,? \tag{4.1}$$

Note that our upper bound on the first fall degree of summation polynomials is a first step towards answering

m	n	n'	$m(m-1)+1$	D_{ff}	D_{reg}	s	GB
2	34	17	3	2	4	188	1.2
	35	18	3	2	4	1 237	16.1
	36	18	3	2	4	1 342	16.4
	37	19	3	2	5	2 542	29.2
	38	19	3	2	5	2 815	25.2
	39	20	3	2	5	4 785	45.6
	40	20	3	2	5	4 858	46.3
	41	21	3	2	5	7 930	65.3
	42	21	3	2	5	8 901	66.7
	43	22	3	2	5	16 816	95.5
	44	22	3	2	5	15 690	96.8
	45	23	3	2	5	38 352	140.0
	46	23	3	2	5	31 735	140.7
	47	24	3	2	5	103 200	207.7
	48	24	3	2	5	86 636	208.2
3	13	5	7	7	7	14	0.6
	14	5	7	7	7	14	0.7
	15	5	7	7	7	14	0.7
	16	6	7	7	7	597	13.5
	17	6	7	7	7	656	13.3
	18	6	7	7	7	729	34.1
	19	7	7	7	7	16 571	92.2
	20	7	7	7	7	17 684	101.2
	21	7	7	7	7	17 681	90.2
4	13	4	13	13	13	467	25.0
	14	4	13	13	13	487	25.8
	15	4	13	13	13	592	26.3
	16	4	13	13	13	755	27.6

Table 1: Empirical data for the Weil descent along the summation polynomial S_{m+1} over $\mathbb{F}_{2^n}$ with n'-dimensional factor basis. Displayed are the observed first fall degree D_{ff}, degree of regularity D_{reg}, the time in seconds s and space requirement in gigabyte GB. All values are averaged over 10 repetitions. For the case $m = 2$ see also Remark 3.3.

this question. The first fall degree generically bounds the degree of regularity from below. Hence, any further lower bound on the degree of regularity associated to the specific case of a Weil descent along summation polynomials can potentially answer (4.1).

Assuming an affirmative answer to (4.1), we can furthermore sharpen the asymptotic complexity of the index calculus algorithm for the ECDLP as presented by Petit and Quisquater [12, Section 5]. In the paragraph *A new complexity analysis* of [12, Section 5] it is argued that the complexity of the index calculus approach via summation polynomials is dominated by the Gröbner basis computation. Under the assumption that the degree of regularity is approximated closely by the first fall degree [12, Assumption 2], Petit and Quisquater derive [12, Proposition 4], i.e. that the discrete logarithm can asymptotically be solved in sub-exponential time

$$\mathcal{O}\left(2^{c\log(n)(n^{2/3}+1)}\right), \tag{4.2}$$

where $c = \frac{2\omega}{3}$, ω is the linear algebra constant ($\omega = \log(7)/\log(2)$ is used in the following estimates), and $n^{2/3}+1$ is an upper bound for the first fall degree of the m-th summation polynomial when $m = n^{1/3}$ [12, Proposition 1]. They state that, by following this analysis, the index calculus approach beats generic algorithms with run time $\mathcal{O}(2^{n/2})$ for any $n \geq N$ where N is an integer approximately equal to 2 000. Now, based on Theorem 3.2, we assume $D_{\text{reg}} \approx m^2 - m + 1 = n^{2/3} - n^{1/3} + 1$ and sharpen (4.2) to

$$\mathcal{O}\left(2^{c\log(n)(n^{2/3}-n^{1/3}+1)}\right).$$

Hence, the turning point to solve the ECDLP faster than a generic algorithm is an integer approximately equal to 1 250. Note that this is still far from cryptographically relevant sizes of n up to 521.

References

[1] C. Diem, On the discrete logarithm problem in elliptic curves, *Compos. Math.* **147** (2011), no. 1, 75–104.

[2] J. Ding and T. J. Hodges, Inverting HFE systems is quasi-polynomial for all fields, in: *Advances in Cryptology—CRYPTO 2011*, Springer, Berlin (2011), 724–742.

[3] V. Dubois and N. Gama, The degree of regularity of HFEsystems, in: *Advances in Cryptology—ASIACRYPT 2010*, Springer, Berlin (2010), 557–576.

[4] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), *J. Pure Appl. Algebra* **139** (1999), no. 1–3, 61–88.

[5] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation—ISSAC '02*, IEEE Press, Piscataway (2002), 75–83.

[6] J.-C. Faugère and A. Joux, Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases, in: *Advances in Cryptology—CRYPTO 2003*, Springer, Berlin (2003), 44–60.

[7] L. Granboulan, A. Joux and J. Stern, Inverting HFE is quasipolynomial, in: *Advances in Cryptology—CRYPTO*, Springer, Berlin (2006), 345–356.

[8] T. J. Hodges, C. Petit and J. Schlather, First fall degree and Weil descent, *Finite Fields Appl.* **30** (2014), 155–177.

[9] M.-D. Huang, M. Kosters and S. L. Yeo, Last fall degree, HFE, and Weil descent attacks on ECDLP, in: *Advances in Cryptology—CRYPTO 2015*, Springer, Berlin 2015, 581–600.

[10] M. Kosters and S. L. Yeo, Notes on summation polynomials, preprint (2015), http://arxiv.org/abs/1505.02532.

[11] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University, New York, 1986.

[12] C. Petit and J.-J. Quisquater, On polynomial systems arising from a Weil descent, in: *Advances in Cryptology – ASIACRYPT 2012*, Springer, Berlin (2012), 451–466.

[13] I. Semaev, Summation polynomials and the discrete logarithm problem on elliptic curves, IACR Cryptology ePrint Archive (2004), https://eprint.iacr.org/2004/031.pdf.

[14] I. Semaev, New algorithm for the discrete logarithm problem on elliptic curves, preprint (2015), http://arxiv.org/abs/1504.01175.