# ON THE FIRST FALL DEGREE OF SUMMATION POLYNOMIALS

STAVROS KOUSIDIS AND ANDREAS WIEMERS

Abstract. We improve on the first fall degree bound of polynomial systems that arise from a Weil descent along Semaev's summation polynomials.

## 1. Introduction

Finding solutions to algebraic equations is a fundamental task. A common approach is a Groebner basis computation via an algorithm such as Faugère's $F4$ and $F5$ [1, 2]. In recent applications Groebner 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 [10] which represents a crucial step in an index calculus method for the ECDLP, see e.g. [9, 11]. The efficiency of Groebner 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 [9] 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 [9] first fall degree bound $m^2+1$ for the system arising from Semaev's $(m+1)$-th summation polynomial. That is, we prove that a first fall occurs at degree $m(m-1)+1$. Along our argumentation we can improve on special instances of a general bound proved by Hodges, Petit and Schlather [5] on the first fall degree of systems induced by a multivariate polynomial. This allows us to explain some discrepancies presented in their experiments.

## 2. Notation

Our considerations take place over a degree $n$ extension $\mathbb{F}_{2^n}$ of the binary field $\mathbb{F}_2$. The notions in §3 and §4 generalise easily to $\mathbb{F}_{q^n}$ with $q$ being an

Federal Office for Information Security, Godesberger Allee 185–189, 53175 Bonn, Germany

*E-mail address*: st.kousidis@googlemail.com.

*Date*: November 27, 2015.

arbitrary prime power. We will comment on some specific generalisations to $\mathbb{F}_{q^n}$ throughout the text.

## 3. The first fall degree

Consider the decomposition of the graded ring

$$S = \mathbb{F}_2[X_0, \ldots, X_{n-1}]/(X_0^2, \ldots, X_{n-1}^2)$$

into its homogeneous components

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

Each $S_j$ is a $\mathbb{F}_2$-vector space generated by the monomials of degree $j$. Let $I$ be an ideal in $S$ generated by homogeneous polynomials $f_1, \ldots, f_r \in S_d$ all of the same degree $d$. Then we have a surjective map

$$\begin{array}{cccl} \phi: & S^r & \longrightarrow & I \\ & (g_1, \ldots, g_r) & \mapsto & g_1 f_1 + \cdots + g_r f_r. \end{array}$$

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

$$f_j e_i + f_i e_j \text{ and } f_k e_k \tag{3.1}$$

is a subset of $\ker(\phi)$. If we restrict $\phi$ to the $\mathbb{F}_2$-subvector space $S_{j-d}^r \subset S^r$ we obtain a surjective map

$$\phi_{j-d}: \quad S_{j-d}^r \quad \longrightarrow \quad I \cap S_j$$

whose kernel contains the $\mathbb{F}_2$-subvector space $U_{j-d} = U \cap S_{j-d}^r$ and hence factors through

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

**Definition 3.1** (Cf. [5, Definition 2.2])**.** The first fall degree of a homogeneous system $f_1, \ldots, f_r \in S_d$ is the smallest $j$ such that the induced $\mathbb{F}_2$-linear map $\bar{\phi}_{j-d}$ is not injective, that is the smallest $j$ such that $\dim_{\mathbb{F}_2}(I \cap S_j) < \dim_{\mathbb{F}_2}(S_{j-d}^r / U_{j-d})$. For a general system of equations we define its first fall degree as the first fall degree of its highest degree homogeneous part.

**Note 3.2.** If $j < 2d$ then $U_{j-d} = 0$ and the first fall degree depends on the non-injectivity of $\phi_{j-d} : S_{j-d}^r \to I \cap S_j$, it equals the smallest $j$ such that $\dim_{\mathbb{F}_2}(I \cap S_j) < \dim_{\mathbb{F}_2}(S_{j-d}^r)$.

## 4. Some transformations of algebraic equations

Let $\mathbb{F}_{2^n}[X]$ be a univariate polynomial ring, and let $\tau : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \tau(\alpha) = \alpha^2$ denote the Frobenius automorphism. Fix a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ by $1, z, \ldots, z^{n-1}$ and let

$$X = X_0 + zX_1 + \cdots + z^{n-1} X_{n-1} \in \mathbb{F}_{2^n}[X_0, \ldots, X_{n-1}].$$

The $\mathbb{F}_2$-linear polynomials $Y_j = X^{2^j}$ can be written as a linear transform of $(X_0, \ldots, X_{n-1})$ via the Vandermonde matrix

$$V = V(z, \tau(z), \ldots, \tau^{n-1}(z)) \tag{4.1}$$

$$= \begin{pmatrix} 1 & z & z^2 & \cdots & z^{n-1} \\ 1 & \tau(z) & \tau(z^2) & \cdots & \tau(z^{n-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \tau^{n-1}(z) & \tau^{n-1}(z^2) & \cdots & \tau^{n-1}(z^{n-1}) \end{pmatrix}.$$

That is

$$(Y_0, Y_1, \dots, Y_{n-1}) = (X, X^2, \dots, X^{2^{n-1}}) = (X_0, X_1, \dots, X_{n-1}) \cdot V^t, \tag{4.2}$$

and in particular

$$Y_j = X^{2^j} = X_0 + \tau^j(z)X_1 + \cdots + \tau^j(z^{n-1})X_{n-1}. \tag{4.3}$$

Each $X^i$ can be written as a polynomial in the $\mathbb{F}_2$-linear variables $Y_j$ by a binary expansion of $i$. Recall that as an endomorphism of $\mathbb{F}_{2^n}$ we have $X^{2^n} - X = 0$ and hence without loss of generality $i < 2^n$, that is

$$X^i = X^{a_0}(X^2)^{a_1} \cdots (X^{2^{n-1}})^{a_{n-1}} = Y_0^{a_0} Y_1^{a_1} \cdots Y_{n-1}^{a_{n-1}} \tag{4.4}$$

in $\mathbb{F}_{2^n}[Y_0, \dots, Y_{n-1}]$ of degree $\leq a_0 + \cdots + a_{n-1}$ where $a_i \in \{0, 1\}$. To summarize, any polynomial $f \in \mathbb{F}_{2^n}[X]$ can be written as a polynomial $F \in \mathbb{F}_{2^n}[Y_0, \dots, Y_{n-1}]$ in the $\mathbb{F}_2$-linear variables $Y_j$ such that the degree in each variable is $< 2$, and each variable $Y_i$ arises from a linear change of the variables $X_0, \dots, X_{n-1}$. To be precise,

$$f(X) = F((X_0, \dots, X_{n-1}) \cdot V^t) = \sum_{i=0}^{n-1} z^i F_i(X_0, \dots, X_{n-1}), \tag{4.5}$$

where we have arranged the terms on the left-hand side as equations $F_0, \dots, F_{n-1} \in \mathbb{F}_{2^n}[X_0, \dots, X_{n-1}]$ (in fact the coefficients of the $F_j$ lie in $\mathbb{F}_2$) according to the basis $1, z, \dots, z^{n-1}$. We apply the Vandermonde matrix $V$ to the vector of equations $F_0, \dots, F_{n-1}$ to obtain an equivalent system of algebraic equations $F, F^\tau, \dots, F^{\tau^{n-1}} \in \mathbb{F}_{2^n}[Y_0, \dots, Y_{n-1}]$ via

$$V \cdot \begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ F_{n-1} \end{pmatrix} (X_0, \dots, X_{n-1}) = \begin{pmatrix} F \\ F^\tau \\ \vdots \\ F^{\tau^{n-1}} \end{pmatrix} ((X_0, \dots, X_{n-1}) \cdot V^t). \tag{4.6}$$

In particular, each entry is given by

$$F^{\tau^j}((X_0, \dots, X_{n-1}) \cdot V^t) = \sum_{i=0}^{n-1} \tau^j(z^i) F_i(X_0, \dots, X_{n-1}). \tag{4.7}$$

The system in $F_0, \dots, F_{n-1}$ regarded in $\mathbb{F}_{2^n}[X_0, \dots, X_{n-1}]$ can be augmented by the field equations $X_0^2 - X_0, \dots, X_{n-1}^2 - X_{n-1}$ to produce solutions in the base field $\mathbb{F}_2$. Likewise a linear transform of the field equations forces

$K$-valued solutions of $F, F^\tau, \ldots, F^{\tau^{n-1}}$ as follows. Recall from (4.3) that

$$Y_j^2 = \sum_{i=0}^{n-1} (z^{2^{j+1}})^i X_i^2 \quad \text{and} \quad Y_{j+1} = \sum_{i=0}^{n-1} (z^{2^{j+1}})^i X_i \tag{4.8}$$

That is, we have the following linear transform

$$CV \cdot \begin{pmatrix} X_0^2 - X_0 \\ \vdots \\ X_{n-2}^2 - X_{n-2} \\ X_{n-1}^2 - X_{n-1} \end{pmatrix} = \begin{pmatrix} Y_0^2 - Y_1 \\ \vdots \\ Y_{n-2}^2 - Y_{n-1} \\ Y_{n-1}^2 - Y_0 \end{pmatrix} \tag{4.9}$$

where $C$ denotes the circulant matrix

$$C = \begin{pmatrix} \mathbf{0} & \mathrm{Id}_{n-1} \\ 1 & \mathbf{0} \end{pmatrix}. \tag{4.10}$$

Therefore, the extension of the linear transformation in (4.6) such that the systems $F_\bullet = (F_0, \ldots, F_{n-1})^t$ and $F^{\tau^\bullet} = (F, F^\tau, \ldots, F^{\tau^{n-1}})^t$ viewed in $\mathbb{F}_{2^n}[X_0, \ldots, X_{n-1}]$ equally produce solutions in $\mathbb{F}_2$ is given by

$$\begin{aligned} &\begin{pmatrix} V & \mathbf{0} \\ \mathbf{0} & CV \end{pmatrix} \cdot \begin{pmatrix} F_\bullet \\ X_\bullet^q - X_\bullet \end{pmatrix} (X_0, \ldots, X_{n-1}) \\ &\qquad = \begin{pmatrix} F^{\tau^\bullet} \\ Y_\bullet^q - Y_{\bullet+1} \end{pmatrix} ((X_0, \ldots, X_{n-1}) \cdot V^t). \end{aligned} \tag{4.11}$$

Note that the application of $\tau$ naturally performs as a cyclic shift on the variables $Y_i = X^{2^j}$. Therefore, each $F^{\tau^j}$ can be computed from $F$ by the application of $\tau^j$ to the coefficients of $F$ and its evaluation at $(Y_j, \ldots, Y_{n-1}, Y_0, \ldots, Y_{j-1})$. The linear isomorphisms in (4.6) and (4.11) seem to be common knowledge, see e.g. [4, 4.2], [9, 4.4].

When we reduce the system $F_0, \ldots, F_{n-1}$ by the field equations $X_0^2 - X_0, \ldots, X_{n-1}^2 - X_{n-1}$ it is important to note that the degree of the resulting highest degree homogeneous component cannot drop below the degree of its counterpart in $F, F^\tau, \ldots, F^{\tau^{n-1}}$. In other words we have the following invariance.

**Proposition 4.1.** *The first fall degree of $p_0, \ldots, p_{n-1}$ given by*

$$p_i \equiv F_i \bmod (X_0^2 - X_0, \ldots, X_{n-1}^2 - X_{n-1}).$$

*is equal to the first fall degree of $F, F^\tau, \ldots, F^{\tau^{n-1}}$.*

*Proof.* Due to the linearity of the transforms (4.6) and (4.11) we only have to compare the degrees of the highest degree homogeneous parts. Let $d_0$ be the highest degree that appears in the $p_0, \ldots, p_{n-1}$. As explained previously $\tau$ performs as a cyclic shift on the variables $Y_i$, so it is sufficient to consider the homogeneous parts of $F$ which are of the form

$$A^{(d)} = \sum_{\substack{a_0 + \cdots + a_{n-1} = d \\ a_0, \ldots, a_{n-1} \in \{0,1\}}} c_{a_0, \ldots, a_{n-1}} Y_0^{a_0} Y_1^{a_1} \cdots Y_{n-1}^{a_{n-1}}.$$

Let $A^{(d_1)}$ be the highest degree homogeneous part of $F$. Since the transform (4.6) is linear, it is clear that the maximal degree of each $F_i$ is $\le a_0 + \cdots + a_{n-1} \le d_1$ and so $d_0 \le d_1$. We consider the following commutative diagram where $\phi, \psi$ are linear isomorphisms induced by the Vandermonde matrix $V^t$ from (4.2) and $\pi_X, \pi_Y$ are the natural projections.

$$\begin{tikzcd}
\mathbb{F}_{2^n}[X_0,\ldots,X_{n-1}] \arrow[r, "\phi"] \arrow[d, "\pi_X"'] & \mathbb{F}_{2^n}[Y_0,\ldots,Y_{n-1}] \arrow[d, "\pi_Y"] \\
\mathbb{F}_{2^n}[X_0,\ldots,X_{n-1}]/(X_0^q,\ldots,X_{n-1}^q) \arrow[r, "\psi"] & \mathbb{F}_{2^n}[Y_0,\ldots,Y_{n-1}]/(Y_0^q,\ldots,Y_{n-1}^q)
\end{tikzcd}$$

We have $\pi_Y(A^{(d_1)}) \neq 0$ since the variables $Y_i$ appear with powers $a_i \in \{0,1\}$. Since $\psi$ is a linear isomorphism we obtain

$$0 \neq \psi^{-1}(\pi_Y(A^{(d_1)})) = c\mu + \cdots$$

where $c \in \mathbb{F}_{2^n}$ and $\mu$ is a monomial of degree $d_1$ such that each $X_i$ appears with degree $< 2$. Therefore $\mu$ remains unchanged when lifted along $\pi_X$ and reduced by the field equations $(X_0^2 - X_0, \ldots, X_{n-1}^2 - X_{n-1})$, and consequently $d_0 = d_1$. $\square$

## 5. A first fall degree bound

From now on let $f(X) \in \mathbb{F}_{2^n}[X]$ have $\deg_{\mathbb{F}_{2^n}} f \le 2^M - 1$ and $\deg_{\mathbb{F}_2} f = d$, and assume $M \le n$. Then $f(X) = F(Y_0, \ldots, Y_{n-1})$ is an element of the truncated graded ring

$$\begin{aligned} R^{0,M-1} &= \mathbb{F}_{2^n}[Y_0,\ldots,Y_{M-1}]/(Y_0^2,\ldots,Y_{M-1}^2) \\ &= R_0^{0,M-1} \oplus R_1^{0,M-1} \oplus \cdots \oplus R_M^{0,M-1}. \end{aligned}$$

For studying its first fall degree we can assume without loss of generality that $F$ is an element of the degree $d$ homogeneous component $R_d^{0,M-1}$.

**Proposition 5.1.** *The $\mathbb{F}_{2^n}$-linear mapping*

$$\begin{array}{ccc} R_{j-d}^{0,M-1} & \longrightarrow & R_j^{0,M-1} \\ \mu & \mapsto & \mu F \end{array}$$

*has a non-trivial kernel if*

$$j \ge \frac{M+d}{2} + 1.$$

*Proof.* The dimensions of the components $R_\delta$ of the graded ring $R$ are encoded in the Hilbert series

$$HS_{R^{0,M-1}}(t) = \frac{(1-t^2)^M}{(1-t)^M} = (1+t)^M = \sum_{\delta=0}^{M} \binom{M}{\delta} t^\delta.$$

A non-trivial kernel occurs if

$$\dim_{\mathbb{F}_{2^n}} R_{j-d}^{0,M-1} = \binom{M}{j-d} > \binom{M}{j} = \binom{M}{M-j} = \dim_{\mathbb{F}_{2^n}} R_j^{0,M-1},$$

i.e. if

$$j - d > M - j \Leftrightarrow j \geq \frac{M+d}{2} + 1.$$

□

According to Note 3.2 the non-injectivity of $\mu \mapsto \mu F$ yields a first fall degree bound when trivial relations cannot occur.

**Corollary 5.2.** *If $j < 2d$ the first fall degree of $F$ is $\leq \frac{1}{2}(M+d)+1$.*

This bound can be generalized to $\leq \frac{1}{2}((q-1)M+d)+1$ for polynomials $F$ that have coefficients in $\mathbb{F}_{q^n}$, when still $j < 2d$. Hodges, Petit and Schlather [5, Theorem 4.9] prove that general bound without the restriction on $j$. However, in our restricted setting we can improve Corollary 5.2 by one due to the following observations.

**Proposition 5.3.** [1] *Assume $M - j = j - d$, such that $M + d$ and $M - d$ are even and $\dim_{\mathbb{F}_{2^n}} R^{0,M-1}_{(M-d)/2} = \dim_{\mathbb{F}_{2^n}} R^{0,M-1}_{(M+d)/2} = \binom{M}{j-d}$. Then, the linear transform*

$$\begin{array}{ccc} R^{0,M-1}_{(M-d)/2} & \longrightarrow & R^{0,M-1}_{(M+d)/2} \\ \mu & \mapsto & \mu F \end{array}$$

*has a non-trivial kernel if $\binom{M}{j-d}$ is odd. If furthermore $M < 3d$, the first fall degree of $F$ is $\leq \frac{1}{2}(M+d)$.*

*Proof.* For a subset $J \subset \Omega = \{0, \ldots, M-1\}$ we denote the monomial $\mu_J = \prod_{i \in J} Y_i$ and write the homogeneous polynomial $F = \sum_{|J|=d} c_J \mu_J$. Denote by $I_{j-d} \subset \Omega = \{0, \ldots, M-1\}$ a subset of cardinality $j - d$ and consider

$$\mu_{I_{j-d}} F = \sum_{J \cap I_{j-d} = \emptyset} c_J \mu_{J \cup I_{j-d}}.$$

Each $\mu_{J \cup I_{j-d}}$ is an element of $R^{0,M-1}_{(M+d)/2}$. Since $M - j = j - d$ we can further write

$$\mu_{I_{j-d}} F = \sum_{I'_{j-d} \cap I_{j-d} = \emptyset} c_{\Omega \setminus (I'_{j-d} \cup I_{j-d})} \mu_\Omega / \mu_{I'_{j-d}}. \tag{5.1}$$

Because of the symmetry of $I_{j-d}$ and $I'_{j-d}$ the coefficients on the right-hand side of (5.1) form a square symmetric matrix of odd dimension $\binom{M}{j-d}$. Since any symmetric matrix in characteristic 2 is also anti-symmetric its determinant vanishes. If $M < 3d$, then $j < 2d$ and there are no trivial relations according to Note 3.2. Hence we have a first fall. □

When $\binom{M}{j-d}$ is even one cannot expect the determinant of the linear transform from Proposition 5.3 to vanish. Instead the following approach yields a first fall.

[1] Timothy J. Hodges informed us that he and Sergio Molina observed the same behavior and anti-symmetry argument in ongoing unpublished work.

**Proposition 5.4.** *Assume $M-j=j-d$, such that $M+d$ and $M-d$ are even, and recall the polynomials $F \in R_d^{0,M-1}$ and $F^\tau \in R_d^{1,M}$ from (4.6). We assume $M \leq n-1$ such that $\tau$ acts as a simple shift on the variables $Y_i$ without turning round. Then, the defect of the linear transform*

$$\begin{array}{ccc} R^{0,M-1}_{(M-d)/2} \oplus R^{1,M}_{(M-d)/2} & \longrightarrow & R^{0,M}_{(M+d)/2} \\ (\mu,\mu') & \mapsto & \mu F + \mu' F^\tau \end{array}$$

*is at least $\binom{M-1}{j} > 0$. If furthermore $M < 3d$, the first fall degree of $F, F^\tau$ is $\leq \frac{1}{2}(M+d)$.*

*Proof.* We denote by $I_i \subset \Omega = \{0,\dots,M-1\}$ and $I'_i \subset \{1,\dots,M\}$ subsets of cardinality $i$, respectively. Consider the linear subspace in $R^{0,M}_{(M+d)/2}$ spanned by the $2\binom{M}{j-d} = 2\binom{M}{j}$ many products

$$\begin{aligned} \mu_{I_{j-d}} F &= \sum_{I_j \supset I_{j-d}} c^F_{I_j \setminus I_{j-d}} \mu_{I_j}, \\ \mu_{I'_{j-d}} F^\tau &= \sum_{I'_j \supset I'_{j-d}} c^{F^\tau}_{I'_j \setminus I'_{j-d}} \mu_{I'_j}. \end{aligned}$$

Then, the coefficients $c^F_{I_j \setminus I_{j-d}}, c^{F^\tau}_{I'_j \setminus I'_{j-d}}$ form a matrix with $2\binom{M}{j}$ rows and $\binom{M}{j} + (\binom{M}{j} - \binom{M-1}{j})$ columns, since the above representations overlap exactly in the $\binom{M-1}{j}$ many subsets $I_j$ from $\{1,\dots,M-1\}$. That is, the defect of that linear transform is at least $\binom{M-1}{j} > 0$ as claimed. If $M < 3d$, then $j < 2d$ and there are no trivial relations according to Note 3.2. Hence we have a first fall. □

Let us compile a list of experiments. We choose uniformly at random a homogeneous polynomial $F(Y_0,\dots,Y_{M-1})$ of degree $d$ in $\mathbb{F}_{2^n}[Y_0,\dots,Y_{n-1}]$ such that the degree in each variable $Y_i$ is $\leq q-1$. and compute a Groebner basis of the ideal

$$I = (F, F^{\tau^m}, \dots, F^{\tau^{m(n-1))}}, Y_0^2 - Y_1, \dots, Y_{n-2}^2 - Y_{n-1}, Y_{n-1}^2 - Y_0)$$

in $\mathbb{F}_{2^n}[Y_0,\dots,Y_{n-1}]$ generated by the system in (4.11). The computation is done with Magma's `GroebnerBasis()` function tuned to verbosity level 1. The empirical first fall degree $D_{ff}$ is read off as the step degree of the first step where new lower degree (i.e. < step degree) polynomials are added. The empirical degree of regularity $D_{reg}$ is read off as the highest step degree of all steps where new polynomials are added.

The gray colored part of Table 1 is a copy of the lines with $p=2$, discrepancy $B > D_{ff}$ from [5, Table 1] (their $t$ being our $M$), and $t > 3d$. We were able to reproduce their experimental data on $D_{ff}$ and $D_{reg}$. The white cells document our first fall degree bound $(M+d)/2$ that solves the discrepancy $B > D_{ff}$ according to Proposition 5.3 when $\binom{M}{j-d}$ is odd and Proposition 5.4 when $\binom{M}{j-d}$ is even. The defect $\binom{M-1}{j}$ is listed as appropriate.

TABLE 1. Empirical and theoretical first fall degree for degree $d$ homogeneous $F(Y_0, \ldots, Y_{M-1})$ with coefficients in $\mathbb{F}_{2^n}$. The empirical data is based on 10 repetitions.

| $p$ | $t(=M)$ | $d$ | $n$ | $B$ | $D_{ff}$ | $D_{reg}$ | $\frac{M+d}{2}$ | $\binom{M}{j-d}$ | $\binom{M-1}{j}$ |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 6 | 4 | 11 | 6 | 5.0 | 5.0 | 5 | 6 | 1 |
| 2 | 6 | 4 | 13 | 6 | 5.0 | 5.0 | 5 | 6 | 1 |
| 2 | 6 | 4 | 17 | 6 | 5.0 | 5.1 | 5 | 6 | 1 |
| 2 | 7 | 3 | 11 | 6 | 5.0 | 5.0 | 5 | 21 | – |
| 2 | 7 | 3 | 13 | 6 | 5.0 | 5.0 | 5 | 21 | – |
| 2 | 7 | 3 | 17 | 6 | 5.0 | 5.0 | 5 | 21 | – |
| 2 | 7 | 5 | 11 | 7 | 6.0 | 6.0 | 6 | 7 | – |
| 2 | 7 | 5 | 13 | 7 | 6.0 | 6.0 | 6 | 7 | – |
| 2 | 7 | 5 | 17 | 7 | 6.0 | 6.1 | 6 | 7 | – |

**Remark 5.5.** There is a multinomial version of Proposition 5.4 for polynomials with coefficients in $\mathbb{F}_{q^n}$ assuming $(q-1)M - j = j - d$. The defect of the analogous linear transform is the coefficient of $t^j$ in $(1+t+\cdots+t^{q-1})^{M-1}$. That way one can improve the bound of Hodge, Petit and Schlather [5, Theorem 4.9] to $\leq ((q-1)M + d)/2$ when $(q-1)M < 3d$. The latter restriction does not scale well with $q$ but excludes trivial relations such as $f_i e_j - f_j e_i$ from (3.1), and of course $f_k^{q-1} e_k$. However, this explains the discrepancy in [5, Table 1] in the case $p = 3, t = 5, d = 4$.

## 6. Weil descent along summation polynomials

We will derive the first fall degree bound $\leq m(m-1)+1$ for the polynomial system that arises from a Weil descent along Semaev's summation polynomial $S_{m+1}(x_1, \ldots, x_{m+1})$ [10]. This is an improvement over $m^2+1$ that results from [5, Theorem 5.2] and [9, §4]. We briefly describe the polynomial system arising from the Weil descent and refer the reader to e.g. [9] for more details. Fix a basis $1, z, \ldots, z^{n-1}$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and let $V$ be a random 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

$$\begin{aligned} S_{m+1}(x_1, \ldots, x_m, x_{m+1}) &= S_{m+1}\left(\sum_{l=1}^{n'} y_{1l}\nu_l, \ldots, \sum_{l=1}^{n'} y_{ml}\nu_l, c\right) \\ &= f_0(y_{ij}) + z f_1(y_{ij}) + \cdots + z^{n-1} f_{n-1}(y_{ij}) \end{aligned}$$

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

$$s_k \equiv f_k \bmod (y_{11}^2 - y_{11}, \ldots, y_{mn'}^2 - y_{mn'}).$$

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.

**Proposition 6.1.** *Let $m \geq 3$. The highest degree homogeneous part of the polynomial system $s_0, \ldots, s_{n-1}$ is of degree $m(m-1)$ and is induced by the monomial $x_1^{2^{m-1}-1} \cdots x_m^{2^{m-1}-1} x_{m+1}$ in the summation polynomial $S_{m+1}(x_1, \ldots, x_m, x_{m+1})$.*

*Proof.* First we show the existence of this monomial in $S_{m+1}$. Due to Semaev [10] we have

$$\begin{aligned} S_3(x_1, x_2, x_3) &= (x_1^2 + x_2^2)X^2 + x_1 x_2 x_3 + x_1^2 x_2^2 + t \\ S_{m+1}(x_1 \ldots, x_m, x_{m+1}) &= \mathrm{Res}_X(S_m(x_1, \ldots, x_{m-1}, X), S_3(x_m, x_{m+1}, X)) \end{aligned}$$

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 $k$ und $l$ is the determinant of the Sylvester matrix

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

That is, with

$$\begin{aligned} S_3(x_m, x_{m+1}, X) &= (x_m^2 + x_{m+1}^2)X^2 + x_m x_{m+1} X + x_m^2 x_{m+1}^2 + t \\ S_m(x_1, \ldots, x_{m-1}, X) &= c_{2^{m-1}} X^{2^{m-1}} + \cdots + c_0 \end{aligned}$$

we have

$$\begin{aligned} &S_{m+1}(x_1 \ldots, x_m, x_{m+1}) \\ &= \det \begin{pmatrix} c_{2^{m-1}} & c_{2^{m-1}-1} & \cdots & c_0 & 0 \\ 0 & c_{2^{m-1}} & \cdots & c_1 & c_0 \\ x_m^2 + x_{m+1}^2 & x_m x_{m+1} & x_m^2 x_{m+1}^2 + t & & \\ & \ddots & & \ddots & \\ & & x_m^2 + x_{m+1}^2 & x_m x_{m+1} & x_m^2 x_{m+1}^2 + t \end{pmatrix} \end{aligned}$$

with a total of $2 + 2^{m-2}$ rows and columns. In order to prove our claim we have to find proper Laplace expansions for the determinant of the Sylvester matrix.

Step 1: Prove by induction (start with $x_1^2 x_2^2$ in $S_3$) that $S_{m+1}$ contains the monomial $x_1^{2^{m-1}} \cdots x_m^{2^{m-1}}$. For that we expand along the term $c_0$ in the first two rows. The resulting minor is an upper triangular matrix in the last $2^{m-2}$ rows and hence

$$\begin{aligned} S_{m+1}(x_1 \dots, x_m, x_{m+1}) &= c_0 c_0 \prod_{i=1}^{2^{m-2}} (x_m^2 + x_{m+1}^2) + \dots \\ &= (x_1^{2^{m-2}} \cdots x_{m-1}^{2^{m-2}})^2 x_m^{2^{m-1}} + \dots \\ &= x_1^{2^{m-1}} \cdots x_{m-1}^{2^{m-1}} x_m^{2^{m-1}} + \dots \end{aligned}$$

Step 2: Prove by induction (start with $x_1x_2x_3$ in $S_3$) that $S_{m+1}$ contains the monomial $x_1^{2^{m-1}-1} \cdots x_m^{2^{m-1}-1} x_{m+1}$. For that we expand along $c_1$ in the first and along $c_0$ in the second row. The resulting minor is again an upper triangular matrix in the last $2^{m-2}$ rows and we have

$$\begin{aligned} &S_{m+1}(x_1 \dots, x_m, x_{m+1}) \\ &= c_1 c_0 x_m x_{m+1} \prod_{i=1}^{2^{m-2}-1} (x_m^2 + x_{m+1}^2) + \dots \\ &= (x_1^{2^{m-2}-1} \cdots x_{m-1}^{2^{m-2}-1})(x_1^{2^{m-2}} \cdots x_{m-1}^{2^{m-2}}) x_m x_{m+1} (x_m^2)^{2^{m-2}-1} + \dots \\ &= x_1^{2^{m-1}-1} \cdots x_{m-1}^{2^{m-1}-1} x_m^{2^{m-1}-1} x_{m+1} + \dots \end{aligned}$$

The degree claim 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 $s_0, \dots, s_{n-1}$ 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 $x_1^{2^{m-1}-1} \cdots x_{m-1}^{2^{m-1}-1} x_m^{2^{m-1}-1} x_{m+1}$, 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 the linear change

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

and obtain

$$\begin{aligned} x_1^{2^{m-1}-1} \cdots x_m^{2^{m-1}-1} c &= c \prod_{i=1}^{m} \prod_{j=0}^{m-2} Y_{ij} \\ &= c \prod_{i=1}^{m} \prod_{j=0}^{m-2} \sum_{l=1}^{n'} y_{il} \nu_l^{2^j} \\ &= \sum_k \gamma_k \prod_{i=1}^{m} \prod_{j=0}^{m-2} y_{il_j} + \text{ terms of degree } < m(m-1) \end{aligned}$$

where $\gamma_k \in \mathbb{F}_{2^n}$ and the $l_j$ for $j = 0, \dots, m-2$ are pairwise distinct. $\square$

We are ready to prove

**Theorem 6.2.** *The first fall degree of the polynomial system $s_0, \ldots, s_{n-1}$ resulting from the Weil descent along the summation polynomial $S_{m+1}, m \geq 3$ is $\leq m(m-1)+1$.*

*Proof.* We consider again the linear change of variables

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

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

$$\begin{pmatrix} \nu_1 & \cdots & \nu_{n'} \\ \nu_1^2 & \cdots & \nu_{n'}^2 \\ \vdots & \ddots & \vdots \\ \nu_1^{2^{m-1}} & \cdots & \nu_{n'}^{2^{m-1}} \end{pmatrix}$$

that can be completed to an invertible linear transform assuming $m \leq n'$ (which holds in any practical instance) by [8, Lemma 3.51]. Therefore the first fall degree of the polynomial $F_c \in \mathbb{F}_{2^n}[Y_{ij}], c \in E$, that is

$$F_c(Y_{10}, \ldots, Y_{1(m-1)}, \ldots, Y_{m0}, \ldots, Y_{m(m-1)}) = S_{m+1}(x_1, \ldots, x_m, c),$$

is equal to the first fall degree of the polynomial system $s_0, \ldots, s_{n-1}$. As explained earlier the monomial $x_1^{2^{m-1}-1} \cdots x_m^{2^{m-1}-1} c$ induces the highest degree homogeneous part of $F_c$, that is

$$A^{(m(m-1))} = c' \prod_{i=1}^{m} \prod_{j=0}^{m-2} Y_{ij}$$

with some $c' \in \mathbb{F}_{2^n}$. This is of degree $d = m(m-1)$ in $M = m(m-1)$ many variables $Y_{ij}$ over $\mathbb{F}_2$. Since $\frac{1}{2}(M+d)+1 = m(m-1)+1 < 2d$ our Corollary 5.2 now gives that the first fall degree of $F_c$ and hence of $s_0, \ldots, s_{n-1}$ is $\leq m(m-1)+1$. □

**Remark 6.3.** From [5, Theorem 5.2] and [9, §4] one deduces a first fall degree $\leq m^2+1$ for the summation polynomial $S_{m+1}$. The argumentation in our proof is completely analogous except that we do not generically bound the degree of $S_{m+1}$ in each variable (which is $2^{m-1}$) by $2^m - 1$.

**Remark 6.4.** Our Theorem 6.2 remains true also in the case $m = 2$ with first fall degree $\leq 2 \cdot 1 + 1 = 3$. This bound is not sharp though, in fact the first fall degree in the case $m = 2$ equals 2 [7, Corollary 4.11 and Remark 4.12].

**Remark 6.5.** When the vector space $V \subset \mathbb{F}_{2^n}/\mathbb{F}_2$ is a subfield the first fall degree equals the highest degree, that is $m(m-1)$, of the induced homogeneous part of $s_0, \ldots, s_{n-1}$. This is easy to see from the equation system (4.6) and (4.11), respectively, since by the subfield condition there is some $k$ such that $F = F^{\tau^k}$ which is a trivial relation that induces a first fall. Those symmetries explain certain observations in [12, §6].

In the light of the first fall degree bound given in Theorem 6.2 we computed a Groebner basis for the ideal resulting from the Weil descent along the summation polynomial $S_{m+1}(x_1, \dots, x_m, x_{m+1})$ 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. < step degree) polynomials are added. The empirical degree of regularity $D_{reg}$ is the highest step degree of all steps where new polynomials appear. 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.

Like Kosters and Yeo [7, §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 $V = \mathrm{span}\{1, z, \dots, z^{n'}\}$ chosen as the factor basis (Cf. [11, 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 [9, Assumption 2] that $D_{reg} = D_{ff} + \mathrm{o}(1)$ nor lead to further evidence that the gap between the degree of regularity and the first fall degree depends on $n$ as discussed in [6, §5.2].

However, we believe our first fall degree bound $m(m-1)+1$ to be sharp in generic cases, and rephrase [9, Assumption 2] as the following question:

$$D_{reg} = m^2 - m + 1 + \mathrm{o}(1) \ ? \tag{6.1}$$

## References


1. Jean Faugère, *A new efficient algorithm for computing Groebner bases (F4)*, Journal of Pure and Applied Algebra **139** (1999), no. 13, 61 – 88.
2. Jean Faugère, *A new efficient algorithm for computing Groebner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ISSAC '02, 2002, pp. 75–83.
3. William Fulton and Joe Harris, *Representation theory - a first course*, Springer, 2004.
4. Louis Granboulan, Antoine Joux, and Jacques Stern, *Inverting HFE is quasipolynomial*, CRYPTO, 2006, pp. 345–356.
5. Timothy J. Hodges, Christophe Petit, and Jacob Schlather, *First fall degree and Weil descent*, Finite Fields and Their Applications **30** (2014), 155–177.
6. Ming-Deh Huang, Michiel Kosters, and Sze Ling Yeo, *Last fall degree, HFE, and Weil descent attacks on ECDLP*, CRYPTO, 2015, pp. 581–600.
7. Michiel Kosters and Sze Ling Yeo, *Notes on summation polynomials*, Preprint **http://arxiv.org/abs/1505.02532** (2015).
8. Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, New York, NY, USA, 1986.
9. Christophe Petit and Jean-Jacques Quisquater, *On polynomial systems arising from a Weil descent*, ASIACRYPT, 2012, pp. 451–466.
10. Igor Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, IACR Cryptology ePrint Archive **2004** (2004), 31.

11. ______, *New algorithm for the discrete logarithm problem on elliptic curves*, Preprint **http://arxiv.org/abs/1504.01175** (2015).
12. Michael Shantz and Edlyn Teske, *Solving the Elliptic Curve Discrete Logarithm Problem using Semaev polynomials, Weil descent and Gröbner basis methods - An experimental study*, Number Theory and Cryptography, 2013, pp. 94–107.

TABLE 2. Empirical data for the Weil descent along the summation polynomial $S_{m+1}$ over $\mathbb{F}_{2^n}$ with $n'$-dimensional factor basis. The observed first fall degree $D_{ff}$, degree of regularity $D_{reg}$, the time in seconds $s$ and space requirement in gigabyte GB is based on 10 repetitions.

| $m$ | $n$ | $n'$ | $m(m-1)+1$ | $D_{ff}$ | $D_{reg}$ | $s$ | GB |
|---|---|---|---|---|---|---|---|
| 2 | 34 | 17 | see Remark 6.4 | 2 | 4 | 188 | 1.2 |
| 2 | 35 | 18 | | 2 | 4 | 1237 | 16.1 |
| 2 | 36 | 18 | | 2 | 4 | 1342 | 16.4 |
| 2 | 37 | 19 | | 2 | 5 | 2542 | 29.2 |
| 2 | 38 | 19 | | 2 | 5 | 2815 | 25.2 |
| 2 | 39 | 20 | | 2 | 5 | 4785 | 45.6 |
| 2 | 40 | 20 | | 2 | 5 | 4858 | 46.3 |
| 2 | 41 | 21 | | 2 | 5 | 7930 | 65.3 |
| 2 | 42 | 21 | | 2 | 5 | 8901 | 66.7 |
| 2 | 43 | 22 | | 2 | 5 | 16816 | 95.5 |
| 2 | 44 | 22 | | 2 | 5 | 15690 | 96.8 |
| 2 | 45 | 23 | | 2 | 5 | 38352 | 140.0 |
| 2 | 46 | 23 | | 2 | 5 | 31735 | 140.7 |
| 2 | 47 | 24 | | 2 | 5 | 103200 | 207.7 |
| 2 | 48 | 24 | | 2 | 5 | 86636 | 208.2 |
| 3 | 13 | 5 | 7 | 7 | 7 | 14 | 0.6 |
| 3 | 14 | 5 | 7 | 7 | 7 | 14 | 0.7 |
| 3 | 15 | 5 | 7 | 7 | 7 | 14 | 0.7 |
| 3 | 16 | 6 | 7 | 7 | 7 | 597 | 13.5 |
| 3 | 17 | 6 | 7 | 7 | 7 | 656 | 13.3 |
| 3 | 18 | 6 | 7 | 7 | 7 | 729 | 34.1 |
| 3 | 19 | 7 | 7 | 7 | 7 | 16571 | 92.2 |
| 3 | 20 | 7 | 7 | 7 | 7 | 17684 | 101.2 |
| 3 | 21 | 7 | 7 | 7 | 7 | 17681 | 90.2 |
| 4 | 13 | 4 | 13 | 13 | 13 | 467 | 25.0 |
| 4 | 14 | 4 | 13 | 13 | 13 | 487 | 25.8 |
| 4 | 15 | 4 | 13 | 13 | 13 | 592 | 26.3 |
| 4 | 16 | 4 | 13 | 13 | 13 | 755 | 27.6 |