ON THE FIRST FALL DEGREE OF ALGEBRAIC EQUATIONS

STAVROS KOUSIDIS AND ANDREAS WIEMERS

Abstract. We give an alternative approach and improvements on bounds developed by Hodges, Petit and Schlather [5], and Petit and Quisquater [9] concerning the first fall degree of algebraic equations. In particular, we improve on the first fall degree bound of polynomial systems that arise from a Weil descent along Semaev's summation polynomials [10].

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 $m(m - 1) + 1$. Our derivation takes as an input a result proved by Hodges, Petit and Schlather [5] on the first fall degree of systems induced by a multivariate polynomial. For the latter we develop an alternative approach based on a dimension argument via a Hilbert series, that allows us to slightly improve their result in many cases and explain the discrepancies presented in their experiments.

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

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

Date: November 19, 2015.

2. The first fall degree

Let K be a finite field of size q, and consider the decomposition of the graded ring $S = K[X_0, \dots, X_{n-1}]/(X_0^q, \dots, X_{n-1}^q)$ into its homogeneous components

$$S = S_0 \oplus S_1 \oplus \cdots \oplus S_{(q-1)n}.$$

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

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

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

$$f_j e_i - f_i e_j \text{ and } f_k^{q-1} e_k$$

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

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

whose kernel contains the K-subvector space $U_j = U \cap S^r_{j-d}$ and hence factors through

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

Definition 2.1. The first fall degree of a homogeneous system $f_1, \dots, f_r \in S_d$ is the smallest j such that the induced K-linear map $\bar{\phi}_{j-d}$ is not injective, that is the smallest j such that $\dim_K(I \cap S_j) < \dim_K(S^r_{j-d}/U_j)$. For a general system of equations we define its first fall degree as the first fall degree of its highest degree homogeneous part.

This definition is essentially equal to [5, Definition 2.2].

3. Some transformations of algebraic equations

Let $E[X]$ be a univariate polynomial ring with coefficients in a degree n finite field extension E of K with $\#K = q = p^m$, and let $\tau : E \to E$ where $\tau(\alpha) = \alpha^p$ denote the Frobenius automorphism with m-fold composition $\tau^m(\alpha) = \alpha^q$. Fix a basis of E over K by $1, z, \dots, z^{n-1}$ and let

$$X = X_0 + zX_1 + \cdots + z^{n-1}X_{n-1} \in E[X_0, \dots, X_{n-1}].$$

The K-linear polynomials $Y_j = X^{q^j}$ can be written as a linear transform of $(X_0, \dots, X_{n-1})$ via the Vandermonde matrix (Cf. [4, §4.2] for the case $q = 2$)

$$\begin{aligned} V &= V(z, \tau^m(z), \dots, \tau^{m(n-1)}(z)) \qquad (3.1) \\ &= \begin{pmatrix} 1 & z & z^2 & \cdots & z^{n-1} \\ 1 & \tau^m(z) & \tau^m(z^2) & \cdots & \tau^m(z^{n-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \tau^{m(n-1)}(z) & \tau^{m(n-1)}(z^2) & \cdots & \tau^{m(n-1)}(z^{n-1}) \end{pmatrix}. \end{aligned}$$

That is

$$(Y_0, Y_1, \dots, Y_{n-1}) = (X, X^q, \dots, X^{q^{n-1}}) = (X_0, X_1, \dots, X_{n-1}) \cdot V^t, \tag{3.2}$$

and in particular

$$\begin{aligned} Y_j = X^{q^j} &= X_0 + \tau^{mj}(z)X_1 + \cdots + \tau^{mj}(z^{n-1})X_{n-1} \\ &= X_0 + z^{q^j}X_1 + \cdots + (z^{q^j})^{n-1}X_{n-1}. \end{aligned} \tag{3.3}$$

Each X^i can be written as a polynomial in the K-linear variables Y_j by a q-ary expansion of i. Recall that as an endomorphism of E we have $X^{q^n} - X = 0$ and hence without loss of generality $i < q^n$, that is

$$X^i = X^{a_0}(X^q)^{a_1} \cdots (X^{q^{n-1}})^{a_{n-1}} = Y_0^{a_0} Y_1^{a_1} \cdots Y_{n-1}^{a_{n-1}} \tag{3.4}$$

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

$$f(X) = F((X_0, \dots, X_{n-1}) \cdot V^t) = \sum_{i=0}^{n-1} z^i F_i(X_0, \dots, X_{n-1}), \tag{3.5}$$

where we have arranged the terms on the left-hand side as equations $F_0, \dots, F_{n-1} \in E[X_0, \dots, X_{n-1}]$ (in fact the coefficients of the F_j lie in K) 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 $F, F^{\tau^m}, \dots, F^{\tau^{m(n-1)}} \in E[Y_0, \dots, Y_{n-1}]$ via

$$V \cdot \begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ F_{n-1} \end{pmatrix} (X_0, \dots, X_{n-1}) = \begin{pmatrix} F \\ F^{\tau^m} \\ \vdots \\ F^{\tau^{m(n-1)}} \end{pmatrix} ((X_0, \dots, X_{n-1}) \cdot V^t). \tag{3.6}$$

In particular, each entry is given by

$$F^{\tau^{mj}}((X_0, \dots, X_{n-1}) \cdot V^t) = \sum_{i=0}^{n-1} \tau^{mj}(z^i) F_i(X_0, \dots, X_{n-1}). \tag{3.7}$$

The system in $F_0, \dots, F_{n-1}$ regarded in $E[X_0, \dots, X_{n-1}]$ can be augmented by the field equations $X_0^q - X_0, \dots, X_{n-1}^q - X_{n-1}$ to produce solutions in the base field K. Likewise a linear transform of the field equations forces K-valued solutions of $F, F^{\tau^m}, \dots, F^{\tau^{m(n-1)}}$ as follows. Recall from (3.2) and (3.3) that

$$Y_j^q = \sum_{i=0}^{n-1} (z^{q^{j+1}})^i X_i^q \quad \text{and} \quad Y_{j+1} = \sum_{i=0}^{n-1} (z^{q^{j+1}})^i X_i \tag{3.8}$$

That is, we have the following linear transform

$$CV \cdot \begin{pmatrix} X_0^q - X_0 \\ \vdots \\ X_{n-2}^q - X_{n-2} \\ X_{n-1}^q - X_{n-1} \end{pmatrix} = \begin{pmatrix} Y_0^q - Y_1 \\ \vdots \\ Y_{n-2}^q - Y_{n-1} \\ Y_{n-1}^q - Y_0 \end{pmatrix} \tag{3.9}$$

where C denotes the circulant matrix

$$C = \begin{pmatrix} \mathbf{0} & \mathrm{Id}_{n-1} \\ 1 & \mathbf{0} \end{pmatrix}. \tag{3.10}$$

Therefore, the extension of the linear transformation in (3.6) such that the systems $F_\bullet = (F_0, \ldots, F_{n-1})^t$ and $F^{\tau^{m\bullet}} = (F, F^{\tau^m}, \ldots, F^{\tau^{m(n-1)}})^t$ viewed in $E[X_0, \ldots, X_{n-1}]$ equally produce solutions in K is given by

$$\begin{aligned} \begin{pmatrix} V & \mathbf{0} \\ \mathbf{0} & CV \end{pmatrix} \cdot \begin{pmatrix} F_\bullet \\ X_\bullet^q - X_\bullet \end{pmatrix} (X_0, \ldots, X_{n-1}) \\ = \begin{pmatrix} F^{\tau^{m\bullet}} \\ Y_\bullet^q - Y_{\bullet+1} \end{pmatrix} ((X_0, \ldots, X_{n-1}) \cdot V^t). \end{aligned} \tag{3.11}$$

Note that the application of τ^m naturally performs as a cyclic shift on the variables $Y_i = X^{q^j}$. Therefore, each $F^{\tau^{mj}}$ can be computed from F by the application of τ^{mj} 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 (3.6) and (3.11) seem to be common knowledge, see e.g. [4, 4.2], [9, 4.4].

4. A dimension argument for the first fall degree

Consider the polynomial $f \in E[X]$ its expansion $F \in E[Y_0, \ldots, Y_{n-1}]$ and rearrangement $F_1, \ldots, F_{n-1} \in E[X_0, \ldots, X_{n-1}]$ from (3.5). We add the field equations

$$p_i \equiv F_i \bmod (X_0^q - X_0, \ldots, X_{n-1}^q - X_{n-1}). \tag{4.1}$$

Recall that the first fall degree of $p_0, \ldots, p_{n-1}$ is defined to be the first fall degree of its highest degree homogeneous part in Definition 2.1.

Proposition 4.1. *The first fall degree of* $(p_0, \ldots, p_{n-1})$ *is equal to the first fall degree induced by the highest degree homogeneous component of* $F(Y_0, \ldots, Y_{n-1}) \in E[Y_0, \ldots, Y_{n-1}]/(Y_0^q, \ldots, Y_{n-1}^q)$.

Proof. Let d_0 be the highest degree that appears in the $p_0, \ldots, p_{n-1}$. Each homogeneous part of $F(Y_0, \ldots, Y_{n-1}) \in E[Y_0, \ldots, Y_{n-1}]$ of degree d is of the form

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

Let $A^{(d_1)}$ be the highest degree homogeneous part of F. Since the variable transform (3.2) is linear, it is clear that the maximal degree of each

$F_i \in E[X_0, \dots, X_{n-1}]$ from (3.5) is $\leq a_0 + \cdots + a_{n-1} \leq d_1$ and so $d_0 \leq d_1$. We consider the following commutative diagram where ϕ, ψ are linear isomorphisms induced by the Vandermonde matrix V^t from (3.2) and π_X, π_Y are the natural projections.

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

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

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

where $c \in E$ and μ is a monomial of degree d_1 such that each X_i appears with degree $< q$. Therefore μ remains unchanged when lifted along π_X and reduced by the field equations $(X_0^q - X_0, \dots, X_{n-1}^q - X_{n-1})$, and consequently $d_0 = d_1$. □

We have translated the analysis of the first fall degree to the quotient ring $E[Y_0, \dots, Y_{n-1}]/(Y_0^q, \dots, Y_{n-1}^q)$. Since the ideal consists of the pairwise coprime monomials $Y_0^q, \dots, Y_{n-1}^q$ its Hilbert series is well-known as

$$HS_{E[Y_0,\dots,Y_{n-1}]/(Y_0^q,\dots,Y_{n-1}^q)}(t) = \frac{(1-t^q)^n}{(1-t)^n} = (1 + t + t^2 + \cdots + t^{q-1})^n.$$

This enables us to deduce a bound on the first fall degree by a simple dimension argument.

From now on let $f(X) \in E[X]$ have $\deg_E f \leq q^M - 1$ and $\deg_K f = d$, and assume $M \leq n$. Then $f(X) = F(Y_0, \dots, Y_{n-1})$ is a polynomial in the variables $Y_0, \dots, Y_{M-1}$. We want to bound the first fall degree with respect to the truncated ring $R = E[Y_0, \dots, Y_{M-1}]/(Y_0^q, \dots, Y_{M-1}^q)$. By Proposition 4.1 we can assume without loss of generality that F is an element of the degree d homogeneous component R_d. Consequently, we have an E-linear mapping

$$\begin{array}{ccc} R_{j-d} & \longrightarrow & R_j \\ \mu & \mapsto & \mu F \end{array}$$

that has a non-trivial kernel if

$$\dim_E R_{j-d} > \dim_E R_j.$$

The dimensions of the components R_δ of the graded ring R are encoded in the Hilbert series

$$HS_R(t) = \frac{(1-t^q)^M}{(1-t)^M} = (1 + t + t^2 + \cdots + t^{q-1})^M = \sum_{\delta=0}^{(q-1)M} h_\delta t^\delta$$

where

$$h_\delta = \sum_{\substack{k_0+\cdots+k_{q-1}=M \\ k_1+2k_2+\cdots+(q-1)k_{q-1}=\delta}} \binom{M}{k_0, k_1, \ldots, k_{q-1}}. \tag{4.2}$$

Note 4.2. The summands from (4.2) can be interpreted as follows. The multinomial $\binom{M}{k_0,k_1,\ldots,k_{q-1}} = \frac{M!}{k_0!k_1!\cdots k_{q-1}!}$ counts the number of monomials in $M = k_0 + \cdots + k_{q-1}$ variables where, due to the restriction via the weighted sum $k_1 + 2k_2 + \cdots + (q-1)k_{q-1} = \delta$, we have k_i many variables that appear with degree i, and the total degree of the monomial is δ.

Proposition 4.3. *The polynomial $HS_R(t)$ has the following properties*

1. *$HS_R(t)$ is reciprocal of degree $(q-1)M$, that is $t^{(q-1)M}HS_R(\frac{1}{t})$ and hence $h_i = h_{(q-1)M-i}$,*
2. *$HS_R(t)$ is strongly unimodular for $M > 1$, that is $h_0 < h_1 < \cdots < h_{\lfloor\frac{1}{2}(q-1)M\rfloor} = h_{\lceil\frac{1}{2}(q-1)M\rceil} > \cdots > h_{(q-1)M-1} > h_{(q-1)M}$,*
3. *$h_0 = h_{(q-1)M} = 1$.*

Since we did not find a proper reference for those claims we include a sketchy representation theoretic explanation. Alternatively they can be proven by induction on M starting with $(1+t+t^2+\cdots+t^{q-1})^2(1+t+t^2+\cdots+t^{q-1})^{M-2}$.

Proof. Interpret the polynomial $(1+t+t^2+\cdots+t^{q-1})^M$ as the character of the $\mathfrak{sl}(2,\mathbf{C})$ tensor product representation $V_{q-1}^{\otimes M}$ where V_{q-1} is the irreducible representation of highest weight $(q-1)\omega_1$. The reciprocity follows from the reflection symmetry via the Weyl group acting on $V_{q-1}^{\otimes M}$. The strong unimodality follows from Steinberg's formula [3, Proposition 25.29], which says that the difference $h_{\delta+1} - h_\delta$ for $\delta = 0, \ldots, \lfloor\frac{1}{2}(q-1)M\rfloor$ is identical to the multiplicity m_{i+1} (here $m_0 = c_0 - c_{-1} = 1 - 0 = 1$) in the decomposition of the tensor product into irreducible sub-representations

$$V_{q-1}^{\otimes M} = \bigoplus_{i=0}^{\lfloor\frac{1}{2}(q-1)M\rfloor} V_{(q-1)M-2i}^{\oplus m_i}.$$

On the other hand, an iterated application of the Clebsch-Gordan decomposition [3]

$$V_k \otimes V_l = V_{k+l} \oplus V_{k+l-2} \oplus \cdots \oplus V_{|k-l|}$$

shows $m_i > 0$. □

From the properties listed in Proposition 4.3 one can easily deduce

Lemma 4.4. *The inequality* $\dim_E R_{j-d} > \dim_E R_j$ *holds iff*

$$j \geq \frac{(q-1)M+d}{2} + 1.$$

Proof. Since $j-d > (q-1)M-j$ we have $h_{j-d} > h_{(q-1)M-j} = h_j$ by strong unimodality and reciprocity, and vice versa. □

Corollary 4.5. *The first fall degree of F is $\leq \frac{(q-1)M+d}{2}+1$.*

Note 4.6. The Corollary 4.5 has been stated in [5, Theorem 4.9] with their rank s being our M. There the proof goes via complexes and alternating sums. Our deduction is purely positive via a dimension argument on a graded ring with a well understood Hilbert series.

Note 4.7. In the case $q=2$ the above Hilbert series reduces to binomials $HS_R(t) = \sum \binom{n}{\delta} t^\delta$ and the above argument specializes to

$$\dim_E R_{j-d} = \binom{M}{j-d} > \binom{M}{j} = \binom{M}{M-j} = \dim_E R_j$$

iff

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

This gives the first fall degree $\leq \frac{M+d}{2}+1$.

5. Improving the first fall degree bound

We improve our bound when $q=2$ first, i.e. for now E is an extension of degree n over $\mathbf{F}_2$. For a subset $J \subset \Omega = \{0,\ldots,M-1\}$ we denote by μ_J the monomial $\prod_{i\in J} Y_i$ and write a homogeneous polynomial $F \in E[Y_0,\ldots,Y_{M-1}]/(Y_0^2,\ldots,Y_{M-1}^2)$ of degree d as $F = \sum_{|J|=d} c_J \mu_J$.

Observation 5.1 ($E \cong \mathbf{F}_2^n$). *Assume $M-j = j-d$ and let $\binom{M}{j-d}$ be odd. Denote by $I_{j-d} \subset \Omega = \{0,\ldots,M-1\}$ a subset of cardinality $j-d$. Then, the linear transform*

$$(c_{I_{j-d},I'_{j-d}}) \in E^{\binom{M}{j-d}\times\binom{M}{j-d}}$$

given by

$$\mu_{I_{j-d}} F = \sum_{I_{j-d}\cap I'_{j-d}=\emptyset} c_{I_{j-d},I'_{j-d}} \mu_\Omega / \mu_{I'_{j-d}}$$

has a non-trivial kernel. We will explain this behaviour in detail. 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 of degree j since it is considered as an element in the quotient ring $E[Y_0,\ldots,Y_{M-1}]/(Y_0^2,\ldots,Y_{M-1}^2)$. Since $M-j=j-d$ we can further write

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

Because of the symmetry of I_{j-d} and I'_{j-d} the coefficients $c_{I_{j-d},I'_{j-d}} = c_{\Omega\setminus(I'_{j-d}\cup I_{j-d})}$ 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.*

When $\binom{M}{j-d}$ is even one cannot expect the determinant of the transform $(c_{I_{j-d},I'_{j-d}})$ from Observation 5.1 to vanish. Instead the following approach yields a first fall.

Observation 5.2 ($E \cong \mathbf{F}_2^n$)**.** *When* $M - j = j - d$ *and* $\binom{M}{j-d}$ *is even we consider the two polynomials* $F \in E[Y_0, \ldots, Y_{M-1}]$ *and* $F^\tau \in E[Y_1, \ldots, Y_M]$ *from* (3.6) *where* $\tau : E \to E$ *is the Frobenius automorphism* $\tau(\alpha) = \alpha^2$*. We assume* $M \leq n - 1$ *such that* τ *acts as a simple shift on the variables* Y_i *without turning round, and denote by* $I_i \subset \Omega = \{0, \ldots, M - 1\}$ *and* $I'_i \subset \{1, \ldots, M\}$ *subsets of cardinality* i*, respectively. Consider the linear subspace spanned by the* $2\binom{M}{j-d} = 2\binom{M}{j}$ *many products*

$$\mu_{I_{j-d}} F = \sum_{I_j \supset I_{j-d}} c^F_{I_j \setminus I_{j-d}} \mu_{I_j}$$

$$\mu_{I'_{j-d}} F^\tau = \sum_{I'_j \supset I'_{j-d}} c^{F^\tau}_{I'_j \setminus I'_{j-d}} \mu_{I'_j}.$$

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* $\{1, \ldots, M - 1\}$*. That is, the defect of that linear transform is at least* $\binom{M-1}{j} > 0$*, hence we have a first fall.*

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

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

in $E[Y_0, \ldots, Y_{n-1}]$ generated by the system in (3.11). 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 $p = 2$ and discrepancy $B > D_{ff}$ from [5, Table 1] (their t being our M). We were able to reproduce their experimental data on D_{ff} and D_{reg}. The white cells document our first fall degree bound I_{ff} that solves this discrepancy when $\frac{M+d}{2} \in \mathbf{N}$ according to Observation 5.1 when $\binom{M}{j-d}$ is odd and Observation 5.2 when $\binom{M}{j-d}$ is even. The defect $\binom{M-1}{j}$ is listed as appropriate, and two further experiments with $p = 2, M = 8, d = 4, 6$ are conducted. In the case

Table 1. Empirical and theoretical first fall degree for degree d homogeneous $F(Y_0, \dots, Y_{M-1})$ with coefficients in $E \cong \mathbf{F}_2^n$. The empirical data is based on 10 repetitions.

p	$t(=M)$	d	n	B	D_{ff}	D_{reg}	$\frac{M+d}{2}$	I_{ff}	$\binom{M}{j-d}$	$\binom{M-1}{j}$
2	6	2	11	5	4.0	4.0	4	4	15	–
2	6	2	13	5	4.0	4.0	4	4	15	–
2	6	2	17	5	4.0	4.0	4	4	15	–
2	6	4	11	6	5.0	5.0	5	5	6	1
2	6	4	13	6	5.0	5.0	5	5	6	1
2	6	4	17	6	5.0	5.1	5	5	6	1
2	7	2	11	5	4.0	4.0	4.5	5	–	–
2	7	2	13	5	4.0	4.0	4.5	5	–	–
2	7	2	17	5	4.0	4.0	4.5	5	–	–
2	7	3	11	6	5.0	5.0	5	5	21	–
2	7	3	13	6	5.0	5.0	5	5	21	–
2	7	3	17	6	5.0	5.0	5	5	21	–
2	7	5	11	7	6.0	6.0	6	6	7	–
2	7	5	13	7	6.0	6.0	6	6	7	–
2	7	5	17	7	6.0	6.1	6	6	7	–
2	8	4	15	7	6.0	6.0	6	6	28	7
2	8	6	15	8	7.0	7.0	7	7	8	1

$p = 2, t = M = 7, d = 2$ we have $\frac{M+d}{2} \notin \mathbf{N}$ and hence $I_{ff} \leq 5.5$, i.e. $I_{ff} = 5$, by Corollary 4.5.

The argument about the singularity of an odd dimensional symmetric matrix in Observation 5.1 does not generalize beyond characteristic 2. But there is a multinomial version of Observation 5.2 in the general case $\#K = q = p^m$.

Let $\mu_{j-d}(Y_0, \dots, Y_{M-1})$ and $\mu'_{j-d}(Y_1, \dots, Y_M)$ be monomials of degree $j - d$ from $E[Y_0, \dots, Y_{n-1}]/(Y_0^q, \dots, Y_{n-1}^q)$. Denote the following dimensions of the i-th homogeneous components

$$\begin{aligned} h_i^M &= \dim_E(E[Y_0, \dots, Y_{M-1}]/(Y_0^q, \dots, Y_{M-1}^q))_i \\ &= \dim_E(E[Y_1, \dots, Y_M]/(Y_1^q, \dots, Y_M^q))_i \end{aligned}$$

and

$$h_i^{M-1} = \dim_E(E[Y_1, \dots, Y_{M-1}]/(Y_1^q, \dots, Y_{M-1}^q))_i.$$

Observation 5.3 ($E \cong \mathbf{F}_q^n$)**.** *Let $(q-1)M - j = j - d$. Consider the two polynomials $F \in E[Y_0, \dots, Y_{M-1}]$ and $F^{\tau^m} \in E[Y_1, \dots, Y_M]$ from (3.6) where $\tau : E \to E$ is the Frobenius automorphism $\tau(\alpha) = \alpha^q$. We assume $M \leq n - 1$ such that τ acts as a simple shift on the variables Y_i without*

Table 2. Empirical and theoretical first fall degree for degree d homogeneous $F(Y_0, \ldots, Y_{M-1})$ with coefficients in $E \cong \mathbf{F}_3^n$.

p	$t(=M)$	d	n	B	D_{ff}	D_{reg}	$M + \frac{d}{2}$	I_{ff}	h_j^{M-1}
3	3	2	13	5	4.0	4.5	4	4	1
3	4	2	13	6	5.0	5.9	5	5	3
3	4	3	13	7	6.0	6.4	5.5	6	–
3	5	2	13	7	6.0	6.6	6	6	10
3	5	3	13	8	7.0	7.7	6.5	7	–
3	5	4	13	8	7.0	7.7	7	7	4

turning round. Consider the linear subspace spanned by

$$\mu_{j-d}F = \sum_{\mu_j} c^F_{\mu_{j-d},\mu_j} \mu_j,$$

$$\mu'_{j-d}F^{\tau^m} = \sum_{\mu'_j} c^{F^{\tau^m}}_{\mu'_{j-d},\mu'_j} \mu'_j.$$

As we have $h^M_{j-d} = h^M_{(q-1)M-j} = h^M_j$ by assumption and reciprocity (likewise for h^{M-1}_{j-d}), the coefficients $c^F_{\mu_{j-d},\mu_j}, c^{F^{\tau^m}}_{\mu'_{j-d},\mu'_j}$ form a matrix with $2h^M_j$ rows and $h^M_j + (h^M_j - h^{M-1}_j)$ columns since the above representations overlap exactly in the h^{M-1}_j many monomials μ_j from $E[Y_1, \ldots, Y_{M-1}]/(Y_1^q, \ldots, Y_{M-1}^q)$. Therefore we have a first fall, and the defect is at least

$$h_j^{M-1} = \sum_{\substack{k_0 + \cdots + k_{q-1} = M-1 \\ k_1 + 2k_2 + \cdots + (q-1)k_{q-1} = j}} \binom{M-1}{k_0, k_1, \ldots, k_{q-1}} > 0.$$

Our dimension arguments allow us to improve on all instances from [5, Table 1] when $p = 3$ (for brevity we restrict ourselves to $n = 13$). Again we compute a Groebner basis for the ideal $I = (F, F^{\tau^m}, \ldots, F^{\tau^{m(n-1))}}, Y_0^q - Y_1, \ldots, Y_{n-2}^q - Y_{n-1}, Y_{n-1}^q - Y_0)$ in $E[Y_0, \ldots, Y_{n-1}]$ from (3.11) with first fall degree bound denoted by I_{ff}. When $j' = M + \frac{d}{2} \in \mathbf{N}$ we apply Observation 5.3 to obtain $I_{ff} = j'$. When $M = 4, d = 3$ and $M = 5, d = 3$ our Lemma 4.4 applies. One can of course, for example when $M = 4, d = 3$, directly consider the E-linear map $R_3 \to R_6, \mu \mapsto \mu F$ and the corresponding Hilbert series $(1+t+t^2)^4 = 1 + 4t + 10t^2 + 16t^3 + 19t^4 + 16t^5 + 10t^6 + 4t^7 + t^8$ to deduce a non-trivial kernel and hence the first fall degree $I_{ff} = 6$.

We conclude with some further experiments listed in Table 3.

6. Weil descent along summation polynomials

Let $E = \mathbf{F}_2^n$ and fix a basis $1, z, \ldots, z^{n-1}$ of E over $\mathbf{F}_2$. We will derive the bound $\leq m(m-1) + 1$ on the first fall degree of the polynomial system that arises from a Weil descent along Semaev's summation polynomial

Table 3. Empirical and theoretical first fall degree for degree d homogeneous $F(Y_0, \dots, Y_{M-1})$ with coefficients in $E \cong \mathbf{F}_q^n, q = 2^2, 5, 7, 2^3$. The empirical data is based on 10 repetitions.

q	$t(= M)$	d	n	B	D_{ff}	D_{reg}	$\frac{(q-1)M+d}{2}$	I_{ff}	h_j^{M-1}
4	3	2	15	7	6.0	6.0	5.5	6	–
4	3	3	15	8	6.0	6.0	6	6	1
4	4	2	15	9	6.0	6.0	7	7	6
4	4	3	15	9	8.0	8.0	7.5	8	–
5	3	2	13	9	7.0	7.0	7	7	2
5	3	3	13	10	8.0	8.0	7.5	8	–
7	3	2	13	13	9.0	9.0	10	10	3
8	3	2	13	15	10.0	10.0	11.5	12	–

$S_{m+1}(x_1, \dots, x_{m+1})$ [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. Let V be a subvector space in $E/\mathbf{F}_2$ of dimension n' with basis $\nu_1, \dots, \nu_{n'}$ over $\mathbf{F}_2$. 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 $e \in E$, and obtain the equation system

$$\begin{aligned} S_{m+1}(x_1, \dots, x_m, x_{m+1}) &= S_{m+1}\left(\sum_{l=1}^{n'} y_{1l}\nu_l, \dots, \sum_{l=1}^{n'} y_{ml}\nu_l, e\right) \\ &= f_0(y_{ij}) + zf_1(y_{ij}) + \cdots + z^{n-1}f_{n-1}(y_{ij}) \end{aligned}$$

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

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

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

Proposition 6.1. *Let $m \geq 3$. The highest degree homogeneous part of the polynomial system $s_0, \dots, s_{n-1}$ 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 $S_{m+1}(x_1, \dots, x_m, x_{m+1})$.*

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

$$\begin{aligned} S_3(x_1, x_2, x_3) &= (x_1^2 + x_2^2)X^2 + x_1x_2x_3 + x_1^2x_2^2 + t \\ S_{m+1}(x_1 \dots, x_m, x_{m+1}) &= \mathrm{Res}_X(S_m(x_1, \dots, x_{m-1}, X), S_3(x_m, x_{m+1}, X)) \end{aligned}$$

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

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

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

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

Step 2: Prove by induction (start with $x_1 x_2 x_3$ 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

$$S_{m+1}(x_1 \ldots, x_m, x_{m+1})$$

$$\begin{aligned}
&= c_1c_0x_mx_{m+1}\prod_{i=1}^{2^{m-2}-1}(x_m^2+x_{m+1}^2)+\dots\\
&= (x_1^{2^{m-2}-1}\cdots x_{m-1}^{2^{m-2}-1})(x_1^{2^{m-2}}\cdots x_{m-1}^{2^{m-2}})x_mx_{m+1}(x_m^2)^{2^{m-2}-1}+\dots\\
&= x_1^{2^{m-1}-1}\cdots x_{m-1}^{2^{m-1}-1}x_m^{2^{m-1}-1}x_{m+1}+\dots
\end{aligned}$$

The degree claim is argued as follows. The variables y_{ij} of the s_k are over $\mathbf{F}_2$ 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 $e\in E$, 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

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

where $\gamma_k\in E$ and the l_j for $j=0,\dots,m-2$ are pairwise distinct. □

We are ready to prove

Theorem 6.2. *The first fall degree of the polynomial system $s_0,\dots,s_{n-1}$ 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) [8, Lemma 3.51]. Therefore the first fall degree of the polynomial $F_e \in E[Y_{ij}], e \in E$, given by

$$F_e(Y_{10}, \ldots, Y_{1(m-2)}, \ldots, Y_{m0}, \ldots, Y_{m(m-2)}) = S_{m+1}(x_1, \ldots, x_m, e)$$

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

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

with some $c \in E$. This is of degree $d = m(m-1)$ in $M = m(m-1)$ many variables Y_{ij} over $\mathbf{F}_2$. Corollary 4.5 now gives that the first fall degree of F_e 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 $2^m - 1$. In fact, Proposition 6.1 demonstrates that for a specific polynomial system one can improve the bound on the first fall degree by a closer analysis of the resulting highest degree homogeneous part.

Remark 6.4. When $q > 2$ a close analysis analogous to Theorem 6.2 is possible. One needs the digit sums of the exponents of the monomials of S_{m+1} in their q-adic representation. That would allow to describe the highest degree homogeneous component in F_e via the variable change $Y_{ij} = x_i^{q^j}$. We leave it as an open problem to find such a description since we consider the case $q = 2$ to be the most important one.

Remark 6.5. 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 6.6. When the vector space $V \subset E/\mathbf{F}_2$ 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 (3.6) and (3.11), respectively, since by the subfield condition there is some k such that $F = F^{\tau^{mk}}$ 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 $S_{m+1}(x_1, \ldots, x_m, x_{m+1})$ 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. < 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 $\mathbf{F}_2^n$, 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 $V = \operatorname{span}\{1, z, \dots, z^{n'}\}$ 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 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 4. Empirical data for the Weil descent along the summation polynomial S_{m+1} over $\mathbf{F}_2^n$ 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 6.5	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