IRREDUCIBLE POLYNOMIALS OF GIVEN FORMS

SHUHONG GAO, JASON HOWELL, AND DANIEL PANARIO

ABSTRACT. We survey under a unified approach on the number of irreducible polynomials of given forms: $x^n + g(x)$ where the coefficient vector of g comes from an affine algebraic variety over $\mathbb{F}_q$. For instance, all but $2 \log n$ coefficients of $g(x)$ are prefixed. The known results are mostly for large q and little is know when q is small or fixed. We present computer experiments on several classes of polynomials over $\mathbb{F}_2$ and compare our data with the results that hold for large q. We also mention some related applications and problems of (irreducible) polynomials with special forms.

1. The general problem and known results

Let $\mathbb{F}_q$ denote a finite field with q elements and V an affine algebraic variety over $\mathbb{F}_q$, say defined by r polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \cdots, x_n]$. Let V_q be the $\mathbb{F}_q$-rational points in V, i.e.

$$V_q = \{(t_1, \cdots, t_n) \in \mathbb{F}_q^n : f_i(t_1, \cdots, t_n) = 0, 1 \le i \le r\}. \tag{1}$$

We define $I_n(V_q)$ to be the number of points $(t_1, \cdots, t_n) \in V_q$ such that

$$F(x) = x^n + t_1 x^{n-1} + \cdots + t_{n-1} x + t_n \tag{2}$$

is irreducible in $\mathbb{F}_q[x]$. We also denote by $P(V_q)$ the set of all polynomials in (2) with $(t_1, \cdots, t_n) \in V_q$. For example, when the polynomials $f_1, \ldots, f_r$ are linear in $x_1, \ldots, x_n$, V is a coset of a linear subspace. If the linear subspace has dimension m then V is called a linear variety of dimension m. For a linear variety V of dimension m, $P(V_q)$ can be rewritten as

$$P(V_q) = \{x^n + g_0(x) + a_1 g_1(x) + \cdots + a_m g_m(x) : (a_1, \ldots, a_m) \in \mathbb{F}_q^m\}, \tag{3}$$

where $g_i \in \mathbb{F}_q[x]$ has degree at most $n-1$ for $0 \le i \le m$, and $g_1, \ldots, g_m$ are linearly independent over $\mathbb{F}_q$.

Problem 1.1. *Let V be an affine variety over $\mathbb{F}_q$. Determine $I_n(V_q)$.*

When V is a linear variety, we require that not all the constants in $g_0(x)$, $g_1(x), \ldots, g_m(x)$ are zero and that the polynomials $x^n + g_0(x), g_1(x), \ldots, g_m(x)$ are relatively prime; otherwise $I_n(V_q) = 0$ trivially.

When $V_q = \mathbb{F}_q^n$, $I_n(V_q)$ is just the number of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ and there is a well–known formula for it. Generally one would not expect to find an explicit formula for $I_n(V_q)$. In practice, it often suffices to have a good lower bound or an asymptotic formula for it. We are most interested in the asymptotic behaviour of $I_n(V_q)$. We note that counting the number of points in V_q

Date: June 16, 1998 (revised).

1991 *Mathematics Subject Classification.* Primary 11T55; Secondary 12Y05.

Key words and phrases. Finite fields, irreducible polynomials, affine algebraic varieties, smooth polynomials.

itself is already a difficult problem; the reader is referred to Wan's paper [39] for more information.

When V is a linear affine variety, $I_n(V_q)$ has been studied by several people. Suppose that $a(x) \in \mathbb{F}_q[x]$ has degree $r < n-1$ and $b(x) \in \mathbb{F}_q[x]$ has degree $\leq n-1$. Artin [1] studies $I_n(V_q)$ for $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$ for $1 \leq i \leq n-r$; here $I_n(V_q)$ is the number of monic irreducible polynomials $F(x)$ in $\mathbb{F}_q[x]$ of degree n that are congruent to $b(x)$ modulo $a(x)$. Hayes [23] generalizes Artin's result to the case where $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$, $1 \leq i \leq n-r-s$, where s is fixed with $0 \leq s \leq n-r-1$ (that is, the first s coefficients $t_1, \ldots, t_s$ of $F(x)$ are fixed).

Theorem 1.2 ([1, 23])**.** *Let $s \geq 0$ and $r \geq 0$ be integers with $m = n-r-s \geq 1$. Let $a(x) \in \mathbb{F}_q[x]$ have degree $r \leq n-1$ and $b(x) \in \mathbb{F}_q[x]$ degree $\leq n-1$. Suppose in (3) $g_0 = b(x)$ and $g_i(x) = a(x)x^{i-1}$, $1 \leq i \leq m$. Then, for large q,*

$$I_n(V_q) = \frac{1}{\kappa(a)} \frac{q^m}{n} + O\left(\frac{q^{nv}}{n}\right) \tag{4}$$

for some $1/2 \leq v < 1$ where $\kappa(a) = \varphi(a)/q^r$ and $\varphi(a)$ is the number of units in $\mathbb{F}_q[x]/(a(x))$.

The estimate (4) is nontrivial only if $m > n/2$. Lower bounds for $\kappa(a)$ are known. By Theorem 2.1 and its proof in [18],

$$1 \geq \kappa(a) \geq \begin{cases} \left(1 - \frac{1}{q}\right)^r & \text{if } r \leq q, \\ \left(1 - \frac{1}{q}\right) \frac{1}{e^{0.83}(1+\log_q r)} & \text{if } r > q, \end{cases}$$

where r is the degree of $a(x)$. Hence

$$1 \leq \frac{1}{\kappa(a)} \leq \begin{cases} \left(1 + \frac{1}{q-1}\right)^r & \text{if } r \leq q, \\ \left(1 + \frac{1}{q-1}\right) e^{0.83}(1 + \log_q r) & \text{if } r > q. \end{cases}$$

Note that for fixed r, $1/\kappa(a)$ goes to 1 when $q \mapsto \infty$. But for fixed q, $1/\kappa(a)$ can be arbitrarily big when $r \mapsto \infty$. In fact, Theorem 3.4 in [18] shows that there is an infinite sequence of r such that

$$e^{\epsilon}\sqrt{1 + \log_q r} \leq \frac{1}{\kappa(x^r - 1)} \leq e^{0.83}(1 + \log_q r)$$

for some constant ϵ depending only on q.

Theorem 1.2 improves previous work of Uchiyama [42] for $b(x) = x^r$ and Carlitz [8] for $b(x) = x^r$ and $s = r = 1$. By using Theorem 1.2, Hsu [25] proves that there is always an irreducible polynomial of degree n in $\mathbb{F}_q[x]$ with the lower or higher half of the coefficients fixed at any values.

The special polynomial $x^n + x + a$ (i.e. $m = 1$, $g_0 = x$ and $g_1 = 1$ in (3)), has attracted much attention. Chowla [9] conjectures that the number of such irreducibles is asymptotically q/n. Later, Cohen [11] and Ree [32] prove independently that indeed the number is $q/n + O(q^{1/2})$. They both use a function field analog of the Čebotarev density theorem, or Weil's theorem on the Riemann hypothesis for function fields over a finite field [41], and the fact that the Galois group of the polynomial $x^n + x + t$ over the function field $\mathbb{F}_q(t)$ is the symmetric group S_n of order n. The latter fact was previously determined by Birch and Swinnerton-Dyer [3] and a simple proof of it is given by Hayes [24]. In fact, Cohen considers the more general polynomials (3) for $m = 1$ in [11] and for an arbitrary m in [12]. In

other words, Cohen determines $I_n(V_q)$ for a linear affine variety V under certain restrictions.

Theorem 1.3 ([12],Theorem 3)**.** *Let V be a linear affine variety of dimension m over $\mathbb{F}_q$. Under certain conditions on V and for large q,*

$$I_n(V_q) = \frac{q^m}{n} + O(q^{m-\frac{1}{2}}), \tag{5}$$

where the implied constant depends only on n.

The estimate (5) works for all m when q is large, but the error term is worse than (4) when $m > n/2$. We omit the description of the exact conditions on V because they seem complicated and not easy to verify. Also, we believe that some of the conditions can be removed or simplified. Cohen gives simple conditions for two special cases of V:

(a) $g_i = x^{k_i}$, $1 \le i \le m$, with $n > k_1 > k_2 > \cdots > k_m \ge 0$;
(b) $g_0 = b(x)$ and $g_i = a(x)x^{i-1}$ for $1 \le i \le m$ where $m \ge 1$, $a(x) \in \mathbb{F}_q[x]$ has degree $n-m$ and $b(x) \in \mathbb{F}_q[x]$ has degree at most $n-1$.

Let p be the characteristic of $\mathbb{F}_q$. For these two special cases, Cohen's conditions are: (a) $p > n$, $P(V_q)$ is not a subset of $\mathbb{F}_q[x^\ell]$ for any $\ell > 1$, and $g_0(0) \neq 0$ if $k_m > 0$; (b) $p > n$, and $x^n + b(x)$ and $a(x)$ are relatively prime. These two cases correspond to Theorems 1 and 2 in [12]. Cohen also considers the more general problem of determining the number of polynomials in $P(V_q)$ with a given factorization pattern; the general result is described in the next section.

In case (a) above, Stepanov [37] independently proves a formula for $I_n(V_q)$ by using the deep Deligne-Weil theorem [14]. For an arbitary variety, the problem has been studied by Chatzidakis, van den Dries and Macintyre [10], Wan [38], and Fried, Haran and Jarden [15] in a more general setting.

Theorem 1.4 ([10, 15, 38])**.** *Let V be an affine variety of dimension m over $\mathbb{F}_q$. Then, for large q, there is a constant $d \ge 0$ such that*

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}). \tag{6}$$

In the above formula for $I_n(V_q)$, d depends on the variety. Also, if we replace q by q^k then the constant d may vary with k but is periodic. An interesting question is to determine d for special classes of varieties. As Theorem 1.3 indicates, d could be 1. At the end of our paper, we will give an example where $d = n$.

The above accounts essentially all we know about $I_n(V_q)$. These results are proved exclusively for large q. Little is known about $I_n(V_q)$ when q is small (or fixed). In Section 3, we present computer experiments on $I_n(V_q)$ for several special cases of linear varieties V over $\mathbb{F}_q$ for $q = 2$. We compare our data with the asymptotic formulas above that are valid for large q. It turns out these formulas hold very well for small q and the error terms are small as well.

For completeness, we comment in Section 2 on some related results and applications of polynomials of special forms, and describe two interesting related problems that arise in algorithm designs.

2. Related results, applications and problems

Sparse irreducible polynomials (i.e., when most coefficients are fixed at 0) over finite fields have several applications in computer algebra, coding theory and cryptography. In practice, $\mathbb{F}_{2^n}$ are among the most useful fields. Suppose that there is an irreducible polynomial $x^n + g(x) \in \mathbb{F}_2[x]$ with $g(x)$ having a small degree, say $\deg(g) \leq \log n + O(1)$. In [34], Shoup shows that exponentiation in $\mathbb{F}_{2^n}$ can be sped up using this type of polynomial, which is desirable in implementing pseudorandom number generators and several public-key cryptosystems. By exploring the low degree of $g(x)$, Coppersmith [13] designs one of the fastest algorithms for computing discrete logarithms in $\mathbb{F}_{2^n}$. Recently, Gao [16] constructs elements of provable high orders in finite fields by using irreducible factors of $x^n + g(x)$ with $\deg g(x)$ small. Irreducible polynomials with a few nonzero terms are also important in efficient hardware implementation of feedback shift registers and finite field arithmetic ([2, 21, 40]).

When the degree n is a power of 2, there is always an irreducible binomial or trinomial over $\mathbb{F}_q$. For example, when $q \equiv 1 \bmod 4$, if $a \in \mathbb{F}_q$ is a quadratic nonresidue then $x^{2^k} - a$ is irreducible over $\mathbb{F}_q$ for all $k \geq 0$. When $q \equiv 3 \bmod 4$, there is no irreducible binomial of degree 2^k for $k \geq 2$. In this case, we have from [6] the following construction of irreducible trinomials. Suppose that $q = p^m$ where m is odd and $p \equiv 3 \bmod 4$ is a prime. Let $2^v | (p+1)$, $2^{v+1} \nmid (p+1)$. Then $v \geq 2$. Compute $u \in \mathbb{F}_p$ iteratively as follows:

$$\begin{aligned} u_1 &= 0, \\ u_i &= \pm \left(\frac{u_{i-1} + 1}{2} \right)^{\frac{p+1}{4}} \pmod p, \quad \text{for } 1 < i < v, \\ u_v &= \pm \left(\frac{u_{v-1} - 1}{2} \right)^{\frac{p+1}{4}} \pmod p, \end{aligned}$$

where one can take at each step any of the signs arbitrarily. Let $u = u_v$. Then

$$x^{2^k} - 2u x^{2^{k-1}} - 1$$

is irreducible over $\mathbb{F}_p$, and over $\mathbb{F}_q$ as well, for all $k \geq 1$. Other constructions of more general sparse irreducible polynomials appear in [35, Theorem 1], and [19, Theorem 5.1]. Irreducible trinomials have been extensively studied and tabulated (see [27, Chapter 3], [4, 5, 22, 43, 44]).

The factorization "behaviour" of polynomials of special forms are important in algorithm designs. This is particularly true for index-calculus methods for computing discrete logarithms in $\mathbb{F}_{q^n}$ for small q. Coppersmith's algorithm for computing discrete logarithms in $\mathbb{F}_{2^n}$ has a good running time if polynomials of the form

$$u_1(x)h(x) + u_2(x) \tag{7}$$

behave like random polynomials of the same degree where $h(x) \in \mathbb{F}_2[x]$ is fixed and $u_1(x), u_2(x) \in \mathbb{F}_2[x]$ are chosen at random of certain degrees. Recently Semaev [33] designs another fast algorithm for computing discrete logarithms in $\mathbb{F}_{q^n}$ when q and n satisfy one of the two conditions:

(a) if $r = 2n + 1$ is a prime and $\mathbb{Z}_r^\times =< q, -1 >$;
(b) if $q^n - 1$ has a small primitive prime divisor r, i.e., $r | (q^n - 1)$ but $r \nmid (q^k - 1)$ for $1 \leq k < n$.

The condition (a) is equivalent to the existence of an optimal normal basis in $\mathbb{F}_{q^n}$; see [29, 20]. In case (a), the running time analysis of Semaev's algorithm relies on the assumption that polynomials of the following forms behave like random polynomials:

$$\sum_{k=d-m}^{d} c_k D_k(x), \quad \sum_{k=d-m}^{d} c_k \phi_{i_k}(x) \tag{8}$$

where $c_k \in \mathbb{F}_q$ vary, but $m < d < n$ and $i_k \leq d$ are fixed, D_k are the well–known Dickson polynomials defined by

$$D_0 = 2, \quad D_1 = x, \quad D_k = xD_{k-1} - D_{k-2}, \ k \geq 2,$$

and ϕ_k are defined by

$$\phi_0 = 1, \quad \phi_k = D_k - D_{k-1} + \cdots + (-1)^{k-1} D_1 + (-1)^k, k \geq 1.$$

In case (b), Semaev assumes that polynomials of the following forms behave like random polynomials:

$$\sum_{k=1}^{m} c_k x^{i_k}, \quad \sum_{k=1}^{m} c_k x^{j_k} \tag{9}$$

where $c_k \in \mathbb{F}_q$ vary, and i_k, j_k are related but fixed.

The polynomials in (7), (8) and (9) are special cases of $P(V_q)$ for a linear variety V as in (3). For index-calculus methods, it is important to know how polynomials in $P(V_q)$ are distributed. Particularly, how many polynomials in $P(V_q)$ are smooth? Here "smooth" means that the polynomials have only irreducible factors of degrees up to a given bound. The phrase "behave like random polynomials" above means that the proportion of smooth polynomials among the polynomials of the form (7), (8), or (9) is approximately the same as that among all polynomials in $\mathbb{F}_q[x]$ of the same degree. This raises the question of finding a good lower bound or asymptotic formula for the number of smooth polynomials in $P(V_q)$. Let $V_q \subseteq \mathbb{F}_q^n$ and $r \leq n$. Define $S_r(V_q)$ to be the number of polynomials in $P(V_q)$ that have no irreducible factors of degrees $> r$.

Problem 2.1. *Let V be an affine variety over $\mathbb{F}_q$ and $r \leq n$. Determine $S_r(V_q)$.*

When $V_q = \mathbb{F}_q^n$, $S_r(V_q)$ is well studied. Let $N_q(n, r) = S_r(\mathbb{F}_q^n)$, the number of r-smooth polynomials of degree n over $\mathbb{F}_q$. Odlyzko [30] gives estimates when $q = 2$ that easily generalize to any q (see [26]). Using the saddle point method when $n \to \infty$ and $n^{1/100} \leq r \leq n^{99/100}$, one has

$$N_q(n, r) = q^n \left(\frac{r}{n}\right)^{(1+o(1))\frac{n}{r}}.$$

Car [7] shows that for large values of r, say $r > cn \log\log n / \log n$, the smooth polynomials behave like the well–known number theoretic Dickman function. Later, Soundararajan [36] obtained estimates for the full range of q, r and n. Recently, Panario, Gourdon and Flajolet [31] used an analytic approach to show that the smooth polynomials also behave like the Dickman function for $r > (\log n)^{1/k}$ for k a positive integer constant. Nothing is known about $S_r(V_q)$ when $V_q \neq \mathbb{F}_q^n$.

More precise information on the distribution of polynomials in $P(V_q)$ can be obtained by studying the number of polynomials that have a given factorization pattern. A polynomial of degree n is said to have a factorization pattern $\lambda =$

$1^{a_1}2^{a_2}\dots n^{a_n}$ if it has exactly a_i irreducible factors of degree i for $1 \le i \le n$. The number of polynomials in $P(V_q)$ with factorization pattern λ is denoted by $I_\lambda(V_q)$. This agrees with our previous notation $I_n(V_q)$ when $\lambda = n$.

Problem 2.2. *Let V be an affine variety over $\mathbb{F}_q$ and λ any factorization pattern. Determine $I_\lambda(V_q)$.*

When V is a linear variety, $I_\lambda(V_q)$ has been studied by Cohen. To state his result, for any factorization pattern $\lambda = 1^{a_1}2^{a_2}\dots n^{a_n}$ we define

$$T(\lambda) = \frac{1}{a_1!a_2!\cdots a_n!1^{a_1}2^{a_2}\cdots n^{a_n}}$$

which represents the proportion of permutations with cycle pattern λ in the symmetric group S_n. When q is large, $T(\lambda)$ is also asymptotically the proportion of polynomials with factorization pattern λ among all monic polynomials of degree n in $\mathbb{F}_q[x]$.

Theorem 2.3 ([12],Theorem 3)**.** *Let V be a linear affine variety of dimension m over $\mathbb{F}_q$. Under certain conditions on V and for large q,*

$$I_\lambda(V_q) = \frac{1}{T(\lambda)} \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}), \tag{10}$$

where the implied constant depends only on n.

The exact conditions are not stated here for the same reasons as in Theorem 1.3. Also, the two special cases (a) and (b) for Theorem 1.3 apply to Theorem 2.3 as well. More work need to be done to simplify Cohen's conditions. In the case (a), Stepanov [37] also proves a similar result.

For an arbitary variety V, Problem 2.2 is studied by Chatzidakis, van den Dries and Macintyre [10], and Fried, Haran and Jarden [15] in a more general setting.

Theorem 2.4 ([10, 15])**.** *Let V be an affine variety of dimension m over $\mathbb{F}_q$ and λ any facterization pattern of a polynomial of degree n. Then there is a constant $d \ge 0$ such that, for large q,*

$$I_\lambda(V_q) = d \cdot \frac{q^m}{n} + O(q^{m-\frac{1}{2}}). \tag{11}$$

It is interesting to determine the constant d for special varieties V. Cohen's result above indicates that for certain linear variety, $d = T(\lambda)$.

When q is small or fixed, little is known about Problem 2.2. It is not even clear what can be proved for fixed q when m and n are large. Probably new methods are needed to attack it. A resolution of Problem 2.2 will shed light on Problem 2.1.

3. Experimental results

In this section we present experimental results on $I_n(V_q)$ when q is small. The following is a list of types of polynomials we consider. All polynomials are over $\mathbb{F}_2$. However, similar experiments can be conducted over any finite field. We seek for the number of irreducible polynomials of the given forms. Let m be a positive integer (in most of our computation we let $m = 2\lceil \log n \rceil$).

(A) $f(x) = x^n + xg(x) + 1$, $\deg g(x) \le m-1$.
(B) $f(x) = x^n + x^k g(x) + 1$ where $\deg g(x) \le m-1$ and $1 \le k \le n-m-1$.
(C) $f(x) = g_0(x) + x^k g(x) + 1$, $g_0(x)$ has degree n and is randomly chosen, where $\deg g(x) \le m-1$ and $1 \le k \le n-m-1$.

(D) $f(x) = g_0(x) + a_1 g_1(x) + \cdots + a_m g_m(x)$, where $g_0, g_1, \ldots, g_m \in \mathbb{F}_2[x]$ are randomly chosen and are linearly independent over $\mathbb{F}_2$ with $\deg g_0(x) = n$ and $\deg g_i(x) < n$ for $1 \le i \le m$.

(D.1) $g_0(x) = D_n(x)/x$, $g_i(x) = D_{k-i}(x)/x$, $1 \le i \le m$, where $D_n(x)$ is a Dickson polynomial of order n and $m \le k < n$.

(D.2) $g_0(x) = x^n + 1$, $g_i(x) = x^{k_i}$, $1 \le i \le m$, where $k_1, \ldots, k_m$ are randomly chosen satisfying $n > k_1 > \cdots > k_m > 0$.

(D.1) and (D.2) are polynomials from (8) and (9). In all the cases, V is an affine variety of dimension m over $\mathbb{F}_2$. For a linear variety of dimension m over $\mathbb{F}_q$, Theorem 1.2 indicates that $I_n(V_q) \sim dq^m/n$ for some constant $d \ge 1$ and d can be arbitrarily large. Theorem 1.3 suggests that this constant d is equal to 1 for many linear varieties, and the error term is $O(q^{m-1/2})$ when q is large. For linear varieties, we expect a smaller error term. So we hypothesize that

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O\left(\frac{q^{m/2}}{n}\right)$$

where d is a constant depending on the variety V. It turns out that $d = 1$ or 2 for most of the above types of polynomials. We will also give examples with $d > 2$. To see the size of the constant in $O(\cdot)$, we compute $c > 0$ such that

$$\left| I_n(V_q) - d \cdot \frac{q^m}{n} \right| \le c \cdot \frac{q^{m/2}}{n},$$

i.e.,

$$\left| I_n(V_q) \cdot \frac{n}{q^{m/2}} - d \cdot q^{m/2} \right| \le c.$$

In our tables,

$$\begin{aligned} \textit{density} &= \frac{I_n(V_q) n}{q^m}, \\ c &= \left| I_n(V_q) \cdot \frac{n}{q^{m/2}} - d \cdot q^{m/2} \right| \end{aligned}$$

up to certain accuracy. We computed Case A for n up to 500 and $m = 2\lceil \log n \rceil$. Table 1 contains the values of d, *density* and c for some selected values of n.

In other tables, S stands for *smallest*, L for *largest*, and A for *average*. In Table 2, 3, 5 and 6, for each $1 \le k \le n-m-1$, we compute $I_n(V_q)$ and the corresponding *density* and c, then we find the smallest, largest, and average of them for each of *density* and c. In Table 4, we make 10 random choices for $\{g_0, g_1, \ldots, g_m\}$ for each pair of n and m, and for each choice we compute *density* and c, then find the smallest, largest, and average of them.

In Table 7, compute some classes of polynomials with larger d, using polynomials in Theorem 1.2 with $\kappa(a)$ small. For example when $a = x^2 - x$, $x^4 - x$, $x^8 - x$, or $x^{16} - x$, the corresponding d is expected to be $\frac{1}{\kappa(a)} = 4$, 5.33, 5.22, and 6.47, respectively. This is indeed verified by our computation. These polynomials provide examples for Problem 27 in [28].

We also did an experiment on the existence of irreducible polynomials of the form $x^n + g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) = \log n + O(1)$. For $q = 2$ and $n \le 2000$, it turns out that such irreducibles always exist with $\deg g(x) \le \log n + 3$.

The computation of these tables is time consuming especially when m is large, since one needs to test irreducibility of 2^m polynomials to get a single value of

n	m	d	*density*	c
25	10	2	2.02637	0.84375
50	12	2	2.22168	14.1875
50	13	2	2.12402	11.2253
50	14	2	2.08435	10.7969
50	15	2	2.04620	8.36375
50	16	2	2.04239	10.8516
50	17	2	2.01797	6.50759
50	18	2	1.98898	5.64062
75	14	2	1.88141	15.1797
100	14	2	2.00195	0.2500
125	14	2	1.77002	29.4375
150	16	2	2.03934	10.0703
175	16	2	1.99203	2.03906
200	16	2	2.00195	0.50000
225	16	2	2.00157	0.40234
250	16	2	2.03323	8.50781
275	18	2	1.94387	28.7363
300	18	2	2.02789	14.2812
325	18	2	1.85595	73.7559
350	18	2	1.97067	15.0156
375	18	2	1.96552	17.6523
400	18	2	2.00042	0.21875
425	18	2	2.03466	17.7480
450	18	2	1.99470	2.71093
475	18	2	2.02579	13.2070
500	18	2	2.08473	43.3828

TABLE 1. Case A

			density			c		
n	m	d	S	L	A	S	L	A
25	10	2	1.83105	2.09961	1.9987	0.719	5.407	2.409
50	12	2	1.95312	2.24609	2.0874	0.125	15.750	6.515
75	14	2	1.81274	2.12402	1.9689	0.055	23.969	10.144
100	14	2	1.86157	2.39258	2.1517	0.251	50.250	20.267
125	14	2	1.75476	2.30408	1.9857	0.141	38.922	11.135

TABLE 2. Case B

$I_n(V_q)$. The data in our tables are based on several thousand values of $I_n(V_q)$ for m up to 18.

The data in our tables indicate that $c < n$, i.e. the error term is $O(q^{m/2})$. For a linear variety V of dimension m over $\mathbb{F}_q$, it seems that

$$I_n(V_q) = d \cdot \frac{q^m}{n} + O(q^{m/2})$$

where $d \geq 1$ is a constant depending only on the variety V and the implied constant in $O(\cdot)$ is independent of m, n and q.

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	2	1.31836	2.41699	1.9092	1.500	21.813	7.163
50	12	2	1.75781	2.63672	2.0459	0.125	40.750	12.838
75	14	2	1.73035	2.22015	1.99468	0.0546875	34.5156	8.26629

TABLE 3. Case C

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	1	0.732422	1.36719	1.074220	0.750	11.750	5.325
50	12	1	0.732422	1.22070	0.969238	1.625	17.125	7.969
75	14	1	0.924683	1.14441	1.031800	0.265	18.485	9.205
100	14	1	0.903320	1.09863	0.988770	0.125	12.625	6.851
125	14	1	0.823975	1.23596	0.997925	2.859	30.204	12.710
150	16	1	0.888062	1.16272	1.001590	5.218	41.657	17.451

TABLE 4. Case D

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	1	0.732422	1.17188	1.00911	0.032	8.5625	3.492
50	12	1	0.805664	1.19629	1.03053	0.063	12.5625	4.594
75	14	1	0.833131	1.16731	0.99538	0.266	21.4141	7.036
100	14	1	0.830078	1.17798	1.01333	0.126	22.7812	7.334
125	14	1	0.793457	1.14441	0.98901	0.071	26.4375	8.403

TABLE 5. Case D.1: Dickson polynomials

			density			*c*		
n	m	d	S	L	A	S	L	A
25	10	2	1.31836	2.41699	1.9092	1.501	21.813	7.163
50	12	2	1.75781	2.63672	2.0459	0.125	40.751	12.838

TABLE 6. Case D.2

Our experiments do not cover the arbitrary variety case. In general, $I_n(V_q)$ is much more difficult to determine. When q is small, it is even not clear what to expect on the size of $I_n(V_q)$. When q is large, we have some control on the major term of $I_n(V_q)$, but the constant d is yet to be determined. We hope that our experimental results will stimulate more interests in this problem.

Finally, we remark that when $F(x)$ is a multivariate polynomial, Theorem 1.4 also holds [10, 15, 38]. Here we would like to provide an example with $d/n = 1$. Let $\mathbb{F}$ be any field over which x and y are algebraically independent. Define a polynomial

$$F(x, y) = x^m + y^n + x^u y^v + \sum c_{ij} x^i y^j$$

				density			*c*		
n	m	$a(x)$	d	S	L	A	S	L	A
25	10	$x^2 - x$	4	3.61328	4.49219	4.01106	0.125	15.75	5.24129
25	10	$x^4 - x$	5.33	4.66309	5.85938	5.33936	0.2475	21.3413	5.72504
25	10	$x^8 - x$	5.22	4.6875	5.7373	5.23529	0.1475	17.04	6.20377
50	12	$x^2 - x$	4	3.50342	4.62646	4.00031	0.25	40.0938	9.91799
50	12	$x^4 - x$	5.33	4.74854	5.98145	5.36126	0.28625	41.6925	10.7219
50	12	$x^8 - x$	5.22	4.63867	5.99365	5.24532	0.295	49.5138	11.6792
50	12	$x^{16} - x$	6.47	5.94482	7.10449	6.44112	0.0175	40.6075	11.3236
75	14	$x^2 - x$	4	3.63922	4.30298	3.98748	0.109375	46.1797	12.1067
75	14	$x^4 - x$	5.33	4.953	5.86395	5.34038	0.20875	68.3459	14.4665
75	14	$x^8 - x$	5.22	4.83398	5.61676	5.21434	0.19125	50.7853	12.7299

TABLE 7. Theorem 1.2

where $c_{ij} \in \mathbb{F}$ and the sum is over all pairs (i, j) such that in the real Euclidean plane the point (i, j) is inside the triangle determined by the points $(m, 0)$, $(0, n)$ and (u, v) (so $un + vm \neq mn$). In [17], it is proved that if $\gcd(m, n, u, v) = 1$ then $F(x, y)$ is absolutely irreducible over $\mathbb{F}$. In particular, let $\mathbb{F} = \mathbb{F}_q$ and

$$F(x, y, z_1, \ldots, z_k) = x^m + y^n + x^u y^v + \sum x^i y^j c_{ij}(z_1, \ldots, z_k)$$

where $c_{ij}(z_1, \ldots, z_k)$ are polynomials in $\mathbb{F}_q[z_1, \ldots, z_k]$ and the sum is same as above. Then for any point $(a_1, \ldots, a_k) \in \mathbb{F}_q^k$, the bivariate polynomial $F(x, y, a_1, \ldots, a_k)$ is (absolutely) irreducible over $\mathbb{F}_q$. Let $V_q = \mathbb{F}_q^k$, a variety of dimension k. Then the number of points a in V_q such that $F(x, y, a)$ is irreducible is exactly q^k. So in Theorem 1.4 for multivariate polynomials $F(x)$, the constant d/n is 1 and the error term is zero.

Acknowledgement. We thank Daqing Wan for his useful comments on the first draft of the paper. We used Victor Shoup's NTL package in our computations.

REFERENCES

[1] E. ARTIN, Quadratische Körper im Gebiete der höheren Kongruenzen. II. *Math. Z.*, **19** (1924), 207–246.

[2] E.R. BERLEKAMP, Bit-serial Reed-Solomon encoders. *IEEE Trans. Info. Th.*, **28** (1982), 869-874.

[3] J. BIRCH AND H. SWINNERTON-DYER, Note on a problem of Chowla. *Acta Arith. 5* (1959), 417–423.

[4] I.F. BLAKE, S. GAO AND R. LAMBERT, Constructive problems for irreducible polynomials over finite fields. *Information Theory and Applications*, eds., A. GULLIVER AND N. SECORD, LNCS 793, Springer-Verlag, 1994, 1-23.

[5] I.F. BLAKE, S. GAO AND R. LAMBERT, Construction and distribution problems for irreducible trinomials over finite fields. *Applications of Finite Fields*, ed., D. GOLLMANN, Oxford, Clarendon Press, 1996, 19–32.

[6] I.F. BLAKE, S. GAO AND R.C MULLIN, Explicit factorization of $x^{2^k} + 1$ over F_p with prime $p \equiv 3 (\mathrm{mod}\ 4)$. *App. Alg. in Eng., Comm. and Comp.*, **4** (1993), 89–94.

[7] M. CAR, Théorèmes de densité dans $\mathbb{F}_q[X]$. *Acta Arith.* **48** (1987), 145–165.

[8] L. CARLITZ, Theorem of Dickson on irreducible polynomials. *Proc. Amer. Math. Soc.* **3** (1952), 693–700.

[9] S. CHOWLA, A note on the construction of finite galois fields GF(p^n). *J. Math. Anal. Appl. 15* (1966), 53–54.

[10] Z. Chatzidakis, L. van den Dries and A. Macintyre, Definable sets over finite fields. *J. Reine Angew. Math.* **427** (1992), 107–135.
[11] S.D. Cohen, The distribution of polynomials over finite fields. *Acta Arith.* **17** (1970), 255–271.
[12] S.D. Cohen, Uniform distribution of polynomials over finite fields. *J. London Math. Soc.* **6** (1972), 93–102.
[13] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two. *IEEE Trans. Info. Theory* **30** (1984), 587–594.
[14] P. Deligne, La conjecture de Weil I. In *Publ. Math. IHES*, **43** (1974), 273–307.
[15] M. Fried, D. Haran and M. Jarden, Effective counting of the points of definable sets over finite fields. *Israel J. Math.*, **85** (1994), no. 1-3, 103-133.
[16] S. Gao, Elements of provable high orders in finite fields. Preprint (9 pages) 1997. To appear in *Proc. American Math. Soc.*.
[17] S. Gao, Absolute irreducibility of polynomials via Newton polytopes. In preparation.
[18] S. Gao and D. Panario, Density of normal elements. *Finite Fields and Their Applications* **3** (1997), 141–150.
[19] S. Gao and D. Panario, Tests and constructions of irreducible polynomials over finite fields. In *Foundations of Computational Mathematics*, ed. F. Cucker and M. Shub, 346–361. Springer Verlag, 1997.
[20] S. Gao and H.W. Lenstra, Jr., Optimal normal bases. *Designs, Codes and Cryptography* **2** (1992), 315-323.
[21] S.W. Golomb, *Shift register sequences*. Aegean Park Press, Laguna Hills, California, 1982.
[22] T. Hansen and G.L. Mullen, Primitive polynomials over finite fields. *Math. Comp.*, **59** (1992), 639–643.
[23] D.R. Hayes, The distribution of irreducibles in $\mathbb{F}_q[x]$. *Trans. American Math. Soc.* **117** (1965), 101–127.
[24] D.R. Hayes, The Galois group of $x^n + x - t$. *Duke Math. J.* **40** (1973), 459–461.
[25] C.-H. Hsu, The distribution of irreducibles in $\mathbb{F}_q[t]$. *J. Number Theory* **61** (1996), 85–96.
[26] R. Lovorn Bender and C. Pomerance, Rigorous discrete logarithm computations in finite fields via smooth polynomials. *Computational perspectives on number theory* (Chicago, IL, 1995), 221–232, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.
[27] A.J. Menezes, I.F. Blake, X. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*. Kluwer Academic Publishers, Boston, Dordrecht, Lancaster, 1993.
[28] G.L. Mullen and I.E. Shparlinski, Open problems and conjectures in finite fields. In *Finite Fields and Applications* (S.D. Cohen and H. Niederreiter Eds.), Cambridge University Press, Lecture Note Series of London Math. Society, Vol. 233 (1996), 243-268.
[29] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, Optimal normal bases in $GF(p^n)$. *Discrete Applied Math.* **22** (1988/1989), 149-161.
[30] A. Odlyzko, Discrete logarithms and their cryptographic significance. In *Advances in Cryptology, Proceedings of Eurocrypt 1984*, *Lecture Notes in Computer Science*, Vol. 209, Springer-Verlag, 1985, 224–314.
[31] D. Panario, X. Gourdon and P. Flajolet *An analytic approach to smooth polynomials over finite fields*. In Algorithmic Number Theory Symposium (Proceedings of ANTS III, Ed. J. P. Buhler), Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, 1998, 226-236.
[32] R. Ree, Proof of a conjecture of S. Chowla. *J. Number Theory 3* (1971), 210–212.
[33] I. A. Semaev, An algorithm for evaluation of discrete logarithms in some nonprime finite fields. Preprint 1994. To appear in *Math. Comp.*.
[34] V. Shoup, 1994. Private communication.
[35] I.E. Shparlinski, Finding irreducible and primitive polynomials. *Appl. Alg. Eng. Comm. Comp.* **4** (1993), 263–268.
[36] K. Soundararajan, Asymptotic formulae for the counting function of smooth polynomials. To appear in *J. London Math. Soc.*.
[37] S.A. Stepanov, The number of irreducible polynomials of a given form over a finite field. *Math. Notes* **41** (1987), 165–169.
[38] D. Wan, Hilbert sets and zeta functions over finite fields. *J. Reine Angew. Math.* **427** (1992), 193-207.

[39] D. Wan, Computing Zeta functions over finite fields. These proceedings, to appear.
[40] M. Wang and I.F. Blake, Bit-serial multiplication in finite fields. *IEEE Trans. Comput.*, **38** (1989), 1457-1460.
[41] S. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent. *Actualités Sei. et Ind.* **1041**, Paris 1948.
[42] S. Uchiyama, Sur les polynomes irréductibles dans un corps fini. II. *Proc. Japan Acad.* **31** (1955), 267–269.
[43] M. Živković, A table of primitive binary polynomials. *Math. Comp.*, **62** (1994), 385–386.
[44] M. Živković, Table of primitive binary polynomials. *Math. Comp.*, **63** (1994), 301–306.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-1907, USA *E-mail address*: sgao,howell@math.clemson.edu

Department of Computer Science, University of Toronto, Toronto, Ontario M5S 3G4, Canada *E-mail address*: daniel@cs.toronto.edu