TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 6, June 1995

DISTINCT DEGREE FACTORIZATIONS FOR POLYNOMIALS OVER A FINITE FIELD

ARNOLD KNOPFMACHER AND RICHARD WARLIMONT

ABSTRACT. Let $\widetilde{\mathbb{F}}_q[X]$ denote the multiplicative semigroup of monic polynomials in one indeterminate X, over a finite field $\mathbb{F}_q$. We determine for each fixed q and fixed n the probability that a polynomial of degree n in $\mathbb{F}_q[X]$ has irreducible factors of distinct degrees only. These results are of relevance to various polynomial factorization algorithms.

1. INTRODUCTION

Let $\widetilde{\mathbb{F}}_q[X]$ denote the multiplicative semigroup of monic polynomials in one indeterminate X over a finite field with q elements. Many deterministic as well as probabilistic factorization algorithms for polynomials in $\widetilde{\mathbb{F}}_q[X]$ require that a distinct degree factorization of the polynomial be performed as the initial step. See, e.g., Knuth [6, pp. 429–431] and more recently [1, 2, 3, 8]. Further references can be found in Shparlinski [9, Chapter 1]. In particular, the further application of all such algorithms becomes unnecessary in the case that the polynomial has only irreducible factors of distinct degrees. The probability that this occurs, as determined below, is therefore of particular interest when applying any such methods. Previously, Greene and Knuth [4, p. 48] also considered this question but only in the limiting case $q \to \infty$, for which they showed that an asymptotic probability $e^{-\gamma}$ is obtained, where γ is Euler's constant. In practice, however, such factorization algorithms are most frequently applied over small finite fields, in particular when $q = 2$. Our result allows us to compute an accurate probability in this case as well as for a finite field of any fixed size.

These results indicate that a distinct degree factorization of a polynomial has a significantly lower probability of occurrence than the limiting value $e^{-\gamma}$ when the size of the field is small.

We determine in addition the related probability that a polynomial has all its *distinct* irreducible factors of different degrees. In this case we show that these probabilities are higher than the limiting value of $e^{-\gamma}$ for small finite fields. Since the square-free part of a polynomial is easily determined [7, Chapter 6], this larger class of polynomials also admits a rapid method of factorization.

Received by the editors May 7, 1992 and, in revised form, April 7, 1994; originally communicated to the *Proceedings of the AMS* by William W. Adams.

1991 *Mathematics Subject Classification.* Primary 11T06, 11T55.

As is well known there are q^n monic polynomials of degree n in $\mathbb{F}_q[X]$ and

$$\pi(n, q) = \frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$$

monic irreducible polynomials of degree n, where $\mu(\cdot)$ denotes the Möbius function.

Let $\partial f(X)$ denote the degree of $f(X) \in \widetilde{\mathbb{F}}_q[X]$.

Let $\gamma_0(n, q)$ denote the number of polynomials $f(X) \in \widetilde{\mathbb{F}}_q[X]$ of degree n with canonical factorization

$$f(X) = p_1(X) \cdots p_k(X), \quad \text{where } \partial(p_i(X)) \neq \partial(p_j(X)) \text{ for } i \neq j.$$

Let $\gamma_1(n, q)$ denote the number of polynomials $f(X) \in \widetilde{\mathbb{F}}_q[X]$ of degree n with canonical factorization

$$f(X) = p_1(X)^{\alpha_1} \cdots p_k(X)^{\alpha_k} \qquad (\alpha_j \in \mathbb{N}),$$

where $\partial(p_i(X)) \neq \partial(p_j(X))$ for $i \neq j$. Put

$$(1) \qquad L_j(q) := \prod_{m=1}^{\infty} \left(1 + \frac{\pi(m, q)}{q^m - j}\right) \exp(-1/m) \qquad (j = 0, 1).$$

We formulate our results.

Theorem 1. *There is some absolute constant* $c > 0$ *such that*

$$(2) \qquad |\gamma_j(n, q)q^{-n} - L_j(q)| \leq c/n \quad \textit{for all } n \geq 1 \ (j = 0, 1).$$

Corollary.

$$(3) \qquad \lim_{n\to\infty} \gamma_j(n, q) q^{-n} = L_j(q) \qquad (j = 0, 1).$$

For comparative purposes, we note that $\gamma_2(n, q)/q^n = \frac{q-1}{q}$, where $\gamma_2(n, q)$ denotes the number of *squarefree* polynomials of degree n, $n \geq 2$, in $\widetilde{\mathbb{F}}_q[x]$. (See, e.g., [7, Chapter 6].)

Using the above formulas and a computer leads to the following estimates of these probabilities for small q.

q	$L_0(q)$	$L_1(q)$	$\frac{\gamma_2(n,q)}{q^n}$
2	0.39673	0.66559	0.5
3	0.46934	0.61230	0.666
4	0.49834	0.59477	0.75
5	0.51370	0.58615	0.8
7	0.52951	0.57769	0.857
8	0.53408	0.57530	0.875
9	0.53752	0.57353	0.888
∞	$e^{-\gamma} = 0.5614\cdots$	$e^{-\gamma}$	1

The numerical results suggest that as $q \to \infty$, $L_0(q)$ increases monotonically to $e^{-\gamma}$ while $L_1(q)$ decreases monotonically to $e^{-\gamma}$. These observations are made precise in the next theorem.

Theorem 2. *Let q be a real variable with $q \geq 2$. Then*

$$e^{-\gamma}\left(1-\frac{3}{2q}\right) \leq L_0(q) \leq e^{-\gamma}\left(1-\frac{1}{3q}\right). \tag{4}$$

$$L_0(q) \text{ is a strictly increasing function of } q. \tag{5}$$

$$e^{-\gamma}\left(1+\frac{1}{16(q-1)}\right) \leq L_1(q) \leq e^{-\gamma}\left(1+\frac{7}{18(q-1)}\right). \tag{6}$$

$$L_1(q) \text{ is a strictly decreasing function of } q. \tag{7}$$

Remark. The multiplicative semigroup $\widetilde{\mathbb{F}}_q[X]$ constitutes the simplest example of an additive arithmetical semigroup (G, ∂) satisfying axiom $A^{\#}$, as introduced by J. Knopfmacher [5]. Distinct degree factorization can be studied in this more general context. We shall deal with these questions elsewhere.

2. PROOF OF RESULTS

Lemma. *Let the complex sequences (a_n), (b_m) be formally related by*

$$1+\sum_{n=1}^{\infty} a_n w^n = \exp\left(\sum_{m=1}^{\infty} b_m w^m\right).$$

Assume there is some constant $K > 0$ such that $|b_m| \leq Km^{-2}$ for all m. Then

$$|a_n| \leq e^{16K} n^{-2} \quad \textit{for all } n.$$

Proof. One has

$$a_n = \sum_{k=1}^{n} \frac{1}{k!} B_k(n),$$

where

$$B_k(n) := \sum_{m_1+\cdots+m_k=n} b_{m_1}\cdots b_{m_k}.$$

From this we see that

$$|a_n| \leq \sum_{k=1}^{n} \frac{K^k}{k!} S_k(n)$$

where

$$S_k(n) := \sum_{m_1+\cdots+m_k=n} (m_1\cdots m_k)^{-2}.$$

We prove by induction on k that

$$S_k(n) \leq 16^k n^{-2}$$

and this will yield our results. Firstly

$$S_1(n) = n^{-2}.$$

Now let $k > 1$ and assume

$$S_{k-1}(n) \leq 16^{k-1} n^{-2}.$$

One has

$$\begin{aligned} S_k(n) &= \sum_{m=1}^{n-1} m^{-2} S_{k-1}(n-m) \\ &\leq 16^{k-1} \sum_{m=1}^{n-1} m^{-2}(n-m)^{-2} \\ &\leq 16^{k-1} \left(\sum_{n \leq \frac{m}{2}} m^{-2} \left(\frac{n}{2}\right)^{-2} \sum_{\frac{n}{2}<m<n} \left(\frac{n}{2}\right)^{-2} (n-m)^{-2} \right) \\ &\leq 16^{k-1} \cdot 2 \cdot 4 \cdot \left(\sum_{h=1}^{\infty} h^{-2} \right) n^{-2} \leq 16^k n^{-2}. \quad \square \end{aligned}$$

We now derive generating functions for $\gamma_j(n, q)$, $j = 0, 1$.

Put $P_m := \{p \text{ irreducible} \mid \partial(p) = m\}$. Then

$$\begin{aligned} \sum_{n=0}^{\infty} \gamma_1(n, q) z^n &= \prod_{m=1}^{\infty} \left(1 + \sum_{p \in P_m} \sum_{\alpha=1} z^{\alpha \partial(p)} \right) \\ &= \prod_{m=1}^{\infty} \left(1 + \pi(m, q) \frac{z^m}{1 - z^m} \right). \end{aligned}$$

Similarly,

$$\sum_{n=0}^{\infty} \gamma_0(n, q) z^n = \prod_{m=1}^{\infty} \left(1 + \sum_{p \in P_m} z^{\partial(p)} \right) = \prod_{m=1}^{\infty} (1 + \pi(m, q) z^m).$$

Proof of Theorem 1. We start by combining the above generating functions to obtain

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \gamma_j(n, q) z^n &= \prod_{m=1}^{\infty} \left(1 + \pi(m, q) \frac{z^m}{1 - jz^m} \right) \\ &= \prod_{m=1}^{\infty} (1 + (\pi(m, q) - j) z^m) \frac{1}{1 - jz^m} \qquad (|z| < q^{-1}). \end{aligned}$$

Put

$$\delta_j(n, q) := \gamma_j(n, q) q^{-n}, \qquad \varepsilon_j(m, q) := (\pi(m, q) - j) q^{-m},$$

and substitute $z = wq^{-1}$ ($|w| < 1$). Then

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \delta_j(n, q) w^n &= \prod_{m=1}^{\infty} (1 + \varepsilon_j(m, q) w^m) \frac{1}{1 - jq^{-m} w^m} \\ &= \frac{1}{1 - w} F_j(w) G_j(w) \end{aligned}$$

where

$$F_j(w) := \frac{1 + (1 - jq^{-1}) w}{1 - jq^{-1} w} \exp(-w)$$

and

$$G_j(w) := \prod_{m=2}^{\infty}(1+\varepsilon_j(m,q)w^m)\frac{\exp(-\frac{w^m}{m})}{1-jq^{-m}w^m}.$$

Let us write

$$G_j(w) = \exp(S_j(w,q)).$$

We shall show that $S_j(w,q)$ can be expanded into a power series

$$S_j(w,q) = \sum_{m=1}^{\infty} b_j(m,q)w^m$$

and that there is some absolute constant $c > 0$ such that

$$(8) \qquad |b_j(m,q)| \le cm^{-2} \quad \text{for all } m.$$

One has

$$S_j(w,q) = \sum_{m=2}^{\infty}\sigma_j(w;m,q)$$

where

$$\begin{aligned}\sigma_j(w;m,q) &:= \log(1+\varepsilon_j(m,q)w^m) - \frac{w^m}{m} + \log\frac{1}{1-jq^{-m}w^m}\\ &= \left(\varepsilon_j(m,q)-\frac{1}{m}\right)w^m + \sum_{k=2}^{\infty}\frac{(-1)^{k+1}}{k}\varepsilon_j(m,q)^k w^{mk}\\ &\quad + \sum_{k=1}^{\infty}\frac{1}{k}(jq^{-m})^k w^{mk}.\end{aligned}$$

From this we see that

$$b_j(m,q) = r_j(m,q) + s_j(m,q) + t_j(m,q)$$

where

$$\begin{aligned}r_j(m,q) &:= \varepsilon_j(m,q) - 1/m,\\ s_j(m,q) &:= \sum_{\substack{kl=m\\ k,l\ge 2}}\frac{(-1)^{k+1}}{k}\varepsilon_j(l,q)^k,\\ t_j(m,q) &:= q^{-m}\sum_{\substack{k|m\\ k<m}}\frac{j^k}{k}.\end{aligned}$$

One finds (see §3, (13) and (15))

$$\frac{1}{l} - \frac{2}{l}q^{-l/2} - jq^{-l} \le \varepsilon_j(l,q) \le \frac{1}{l} - jq^{-l}$$

and

$$|\varepsilon_j(l,q)| \le 1/l \quad \text{for } l \ge 2.$$

Therefore

$$|r_j(m,q)| \le \frac{2}{m}q^{-m/2} + q^{-m} \le 2^{-m/2+1}.$$

Further

$$|s_j(m, q)| \le \sum_{\substack{kl=m \\ k, l \ge 2}} \frac{1}{k}\left(\frac{1}{l}\right)^k = \frac{1}{m}\sum_{\substack{kl=m \\ k, l \ge 2}} \left(\frac{1}{l}\right)^{k-1} \le \frac{1}{m}\sum_{2 \le k \le \frac{m}{2}} \left(\frac{k}{m}\right)^{k-1}$$

$$= \frac{1}{m^2}\sum_{2 \le k \le \frac{m}{2}} k\left(\frac{k}{m}\right)^{k-2} \le \frac{1}{m^2}\sum_{k=2}^{\infty} k2^{2-k}.$$

Finally

$$|t_j(m, q)| \le 2^{-m}\tau(m).$$

Together these yield (8). Now let

$$F_j(w) = \sum_{n=0}^{\infty} c_j(n, q)w^{-n} \quad \text{and} \quad G_j(w) = \sum_{n=0}^{\infty} a_j(n, q)w^{-n}.$$

Then

$$F_j(w)G_j(w) = \sum_{n=0}^{\infty} d_j(n, q)w^{-n},$$

where

$$d_j(n, q) := \sum_{kl=n} c_j(k, q)a_j(l, q).$$

Now we have

$$\delta_j(n, q) = \sum_{h=0}^{n} d_j(h, q) = L_j(q) - \sum_{h>n} d_j(h, q),$$

using the result

$$\sum_{h=0}^{\infty} d_j(h, q) = F_j(1)G_j(1) = L_j(q).$$

Therefore

$$|\delta_j(n, q) - L_j(q)| \le \sum_{h>n} |d_j(h, q)| \le \sum_{kl>n} |c_j(k, q)|\,|a_j(l, q)|$$

$$= \left(\sum_{k>n} |c_j(k, q)|\right)\left(\sum_{l=0}^{\infty} |a_j(l, q)|\right) + \sum_{k \le n} |c_j(k, q)| \sum_{l > \frac{n}{k}} |a_j(l, q)|.$$

There is an absolute constant $c_1 > 0$ such that $|c_j(k, q)| \le c_1 2^{-k}$ for all k. From (8) and our lemma we infer that there is some absolute constant $c_2 > 0$ such that $|a_j(l, q)| \le c_2 l^{-2}$ for all l. Therefore

$$|\delta_j(n, q) - L_j(q)| \ll 2^{-n} + \sum_{k \le n} 2^{-k}\frac{k}{n} \ll n^{-1}. \quad \square$$

Remark. If we write

$$\sigma_j(w; m, q) = \left(\varepsilon_j(m, q) - \frac{1}{m}\right)w^m - \frac{1}{2}\varepsilon_j(m, q)^2 w^{2m} + \sum_{k=3}^{\infty} \cdots + \sum_{k=1}^{\infty} \cdots,$$

we obtain

$$b_j(m, q) = b(m) + b_j^*(m, q),$$

where

$$b(m) := -\frac{1+(-1)^m}{m^2}$$

and $|b_j^*(m, q)| \leq cm^{-3}$ with $c > 0$ absolute.

This refinement in the evaluation of $b_j(m, q)$ will possibly entail a corresponding improvement of Theorem 1:

$$\gamma_j(n, q)q^{-n} = L_j(q) + L_j^*(q)n^{-1} + O(n^{-2})$$

with an absolute O-constant. We do not pursue this matter further.

3. The proof of Theorem 2

The number q comes from $\mathbb{F}_q[X]$ and thus is a power of a prime. In particular, q is a real number ≥ 2. We put

$$\sigma(q, m) := m\pi(m, q) = \sum_{d|m} \mu(d)q^{m/d}$$

and shall study the expressions

$$L_j(q) := \prod_{m=1}^{\infty} \left(1 + \frac{1}{m}\frac{\sigma(q, m)}{q^m - j}\right) \exp(-1/m) \qquad (j = 0, 1),$$

as functions of the real variable $q \geq 2$. We first collect some well-known facts which are needed in the sequel:

$$\sum_{j=1}^{k} q^j < 2q^k, \tag{9}$$

$$\sigma(q, 1) = q, \tag{10}$$

$$\sigma(q, m) = q^m - q^{m/p} \quad \text{if } m = p^\alpha, \tag{11}$$

and, in particular,

$$\sigma(q, p) = q^p - q, \tag{12}$$

$$\sigma(q, m) > q^m - 2q^{m/2}, \tag{13}$$

$$\sigma(q, m) > 0, \tag{14}$$

$$\sigma(q, m) \leq q^m - q \quad \text{for } m > 1, \tag{15}$$

$$\log\frac{1}{1-y} \leq \frac{1}{2}y\left(1 + \frac{1}{1-y}\right) \quad \text{for } 0 \leq y < 1, \tag{16}$$

$$\prod_{m=1}^{\infty}\left(1 + \frac{1}{m}\right)\exp\left(-\frac{1}{m}\right) = e^{-\gamma}. \tag{17}$$

We prove the results for the case $j = 0$. The proofs for $j = 1$ are similar although somewhat more technical.

Proof of (4). We have

$$L_0(q) = \prod_{m=1}^{\infty}\left(1 + \frac{\sigma(q, m)}{mq^m}\right)\exp\left(-\frac{1}{m}\right) = e^{-\gamma}A(q),$$

where

$$A(q) := \prod_{m=1}^{\infty}\left(1+\frac{1}{m+1}(\sigma(q\,,\,m)q^{-m}-1)\right).$$

Now

$$A(q)=\prod_{m=1}^{\infty}\left(1+\frac{\sigma(q\,,\,m)-q^m}{(m+1)q^m}\right)=\left(1-\frac{1}{3q}\right)B(q),$$

where

$$B(q) := \prod_{m=3}^{\infty}\left(1+\frac{\sigma(q\,,\,m)-q^m}{(m+1)q^m}\right).$$

From (15) we get $B(q)<1$. This yields the upper part of (4). Next,

$$B(q)=\left(1-\frac{1}{4q^2}\right)\left(1-\frac{1}{5q^2}\right)\left(1-\frac{1}{6q^4}\right)C(q),$$

where

$$C(q) := \prod_{m=6}^{\infty}\left(1+\frac{\sigma(q\,,\,m)-q^m}{(m+1)q^m}\right).$$

Put $y_m(q) := \frac{2}{m+1}q^{-m/2}$. From (13) and (16) we get

$$\begin{aligned}C(q) &\geq \prod_{m=6}^{\infty}(1-y_m(q)) = \exp\left(-\sum_{m=6}^{\infty}\log\frac{1}{1-y_m(q)}\right)\\ &\geq \exp\left(-\sum_{m=6}^{\infty}\frac{1}{2}y_m(q)\left(1+\frac{1}{1-y_m(q)}\right)\right)\\ &\geq \exp\left(-\frac{1}{7}\left(1+\frac{1}{1-y_6(2)}\right)\frac{1}{1-\frac{1}{\sqrt{2}}}q^{-3}\right)\\ &\geq \exp\left(-\frac{55}{54}q^{-3}\right)\geq 1-\frac{55}{54}q^{-3}.\end{aligned}$$

Now we have

$$\begin{aligned}A(q) &\geq \left(1-\frac{1}{3q}\right)\left(1-\frac{1}{4q^2}\right)\left(1-\frac{1}{5q^2}\right)\left(1-\frac{1}{6q^4}\right)\left(1-\frac{55}{54}\frac{1}{q^3}\right)\\ &\geq 1-\left(\frac{1}{3q}+\frac{1}{4q^2}+\frac{1}{5q^2}+\frac{1}{6q^4}+\frac{55}{54}\frac{1}{q^3}\right)\\ &\geq 1-\left(\frac{1}{3}+\frac{1}{8}+\frac{1}{10}+\frac{1}{48}+\frac{55}{216}\right)\frac{1}{q}\geq 1-\frac{3}{2q},\end{aligned}$$

which yields the lower part of (4).

Proof of (5). We show that $f_m(q) := \sigma(q\,,\,m)q^{-m}$ is a strictly increasing function of $q \geq 2$ for $m>1$ fixed, from which the result follows.

If m is a power of a prime p then (11) yields $f_m(q)=1-q^{m/p-m}$, which is strictly increasing. Otherwise let $p_1<p_2$ be the two smallest prime factors of m. Then

$$f_m(q)=\sum_{d|m}\mu(d)q^{m/d-m}$$

and

$$f'_m(q) = mq^{-m-1}\tau(q\,,\,m)\,,$$

where

$$\begin{aligned}\tau(q\,,\,m) &:= \sum_{d|m}\mu(d)\left(\frac{1}{d}-1\right)q^{m/d}\\ &> \left(1-\frac{1}{p_1}\right)q^{m/p_1} - \sum_{j=1}^{m/p_1p_2} q^j\\ &> \frac{1}{2}q^{m/p_1} - 2q^{m/p_1p_2} \quad \text{(by (9))}\\ &= \frac{1}{2}q^{m/p_1p_2}(q^{m(p_2-1)/p_1p_2} - 4)\\ &\ge \frac{q}{2}(q^2-4) \ge 0\,,\end{aligned}$$

as required. □

References

1. E. Bach and V. Shoup, *Factoring polynomials using fewer random bits*, J. Symbolic Comput. **9** (1990), 229–239.
2. M. Ben-Or, *Probabilistic algorithms in finite fields*, Proc. 22nd Annual Sympos. Foundations of Computer Science, 1981, pp. 394–398.
3. D. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), 587–592.
4. D. H. Greene and D. E. Knuth, *Mathematics for the analysis of algorithms*, 3rd ed., Birkhäuser, Basel, 1990.
5. J. Knopfmacher, *Analytic arithmetic of algebraic function fields*, Marcel Dekker, New York, 1979.
6. D. E. Knuth, *The art of computer programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, MA, 1981.
7. M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, Berlin, 1992.
8. V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), 261–267.
9. I. E. Shparlinski, *Computational and algorithmic problems in finite fields*, Kluwer, Dordrecht, 1992.

Department of Computational and Applied Mathematics, University of Witwatersrand, P.O. Wits, 2050 South Africa

NWF-Mathematik, Universität Regensburg, 93053 Regensburg, Germany
E-mail address: arnoldk@gauss.cam.wits.ac.za