Factorization type probabilities of polynomials with prescribed coefficients over a finite field

Kaloyan Slavov

January 17, 2022

Abstract

Let $f(T)$ be a monic polynomial of degree $d$ with coefficients in a finite field $\mathbb{F}_q$. Extending earlier results in the literature, but now allowing $(q, 2d) > 1$, we give a criterion for $f$ to satisfy the following property: for all but $d^2 - d - 1$ values of $s$ in $\mathbb{F}_q$, the probability that $f(T) + sT + b$ is irreducible over $\mathbb{F}_q$ (as $b \in \mathbb{F}_q$ is chosen uniformly at random) is $1/d + O(q^{-1/2})$.

1 Introduction

Fix a positive integer $d$. Gauss proved that the probability for a monic polynomial of degree $d$ with coefficients in a finite field $\mathbb{F}_q$ to be irreducible is $1/d + O(d(q^{-1/2}))$. In fact, for any partition $\lambda = (\lambda_i)_{i=1}^k$ of $d$, the probability for a random monic $\mathbb{F}_q$-polynomial of degree $d$ to have exactly $k$ irreducible factors over $\mathbb{F}_q$ of degrees $\lambda_1, ..., \lambda_k$ (i.e., to have factorization type $\lambda$) is $p_\lambda + O_d(q^{-1/2})$, where $p_\lambda$ is the probability that a permutation in $S_d$ has cycle structure $\lambda$.

The setting in which some coefficients of the polynomial are fixed and the remaining ones vary in $\mathbb{F}_q$ has been studied extensively. For a monic polynomial $f(T) \in \mathbb{F}_q[T]$ of degree $d$ and an integer $m$ with $0 \leq m < d$, it is conventional to define the $m$-th “short interval” in $\mathbb{F}_q[T]$ around $f$ to be

$I(f, m) = \{ f(T) + a_mT^m + \cdots + a_1T + a_0 \mid a_0, ..., a_m \in \mathbb{F}_q \}$.

We are particularly interested in the small cases $m = 0, 1$. One naturally asks for assumptions on $f$ under which the following expected statement holds true:

2010 Mathematics subject classification. Primary 14G15; Secondary 12F10.

Key words and phrases. Monodromy group, Chebotarev density theorem, generically étale morphism, factorization type, finite field.

This research was supported by NCCR SwissMAP of the SNSF.
For any partition $\lambda$ of $d$, the probability for an element of $I(f, m)$ to have factorization type $\lambda$ is $p_\lambda + O_d(q^{-1/2})$.

While a “sufficiently general” polynomial $f \in \mathbb{F}_q[T]$ will satisfy (*) with $m = 1$ or even with $m = 0$, one is interested in an explicit criterion that can be used to check that a specific $f$ satisfies (*). Along these lines, Bank, Bary-Soroker, and Rosenzweig (2) prove the following

**Theorem 1.** Let $f(T) \in \mathbb{F}_q[T]$ be a monic polynomial of degree $d$. Suppose $(q, d(d-1)) = 1$. Then $f$ satisfies (*) with $m = 1$.

A monic polynomial $f(T) \in \mathbb{F}_q[T]$ of degree $d$ is called a Morse polynomial if the equation $f'(T) = 0$ has exactly $d-1$ distinct roots over $\overline{\mathbb{F}}_q$, and the values of $f$ at them are all distinct. For a Morse polynomial $f(T)$, (*) holds with $m = 0$ (see [4] or [5]). For $j \geq 0$, the $j$-th Hasse derivative of a polynomial $f = \sum a_i T^i$ is defined as

$$D^j f = \sum \binom{i}{j} a_i T^{i-j},$$

so $f$ has a zero of order at least $k$ at $\alpha$ precisely when $D^j f(\alpha) = 0$ for all $j = 0, \ldots, k-1$.

The proposition below weakens the assumption $(q, d(d-1)) = 1$; it is stated as Proposition 7 in [5] and attributed to Jarden and Razon (Proposition 4.3 in [4]).

**Proposition 2.** Let $f(T) \in \mathbb{F}_q[T]$ be a monic polynomial of degree $d$. Suppose $f'' \neq 0$ and $(q, 2d) = 1$. Then for all but $O_d(1)$ values of $s \in \mathbb{F}_q$, the polynomial $f(T) + sT$ is a Morse polynomial, and hence satisfies (*) with $m = 0$. In particular, $f$ satisfies (*) with $m = 1$.

**Remark 3.** The assumption $(q, 2d) = 1$ is essential in Proposition [2]. Indeed, if char $\mathbb{F}_q \mid d$, a polynomial of degree $d$ is never a Morse polynomial. Also, even if the condition $f'' \neq 0$ is replaced by the weaker $D^2 f \neq 0$ (see the paragraph preceding Proposition 7 in [5]), Proposition [2] still does not hold in characteristic 2. For example, $T^7 + sT$ is never a Morse polynomial when $q$ is a power of 2, and in fact $f(T) = T^7$ fails to satisfy (*) with $m = 1$.

The goal of this note is to give a criterion for a polynomial to satisfy (*), but allowing $(q, 2d) > 1$.

For a field $k$ and a polynomial $f(T) \in k[T]$, let $\tilde{f}(x, y)$ denote the polynomial in $k[x, y]$ defined by

$$f(x) - f(y) = (x - y) \tilde{f}(x, y).$$

We now state our main result.

**Theorem 4.** Let $f(T) \in \mathbb{F}_q[T]$ be a monic polynomial of degree $d$. Suppose $D^2 f \neq 0$, $\deg f' \geq 1$, and the polynomials $\tilde{f}(x, y) - f'(x)$ and $\tilde{f}'(x, y)$ have no common factors besides possibly a power of $x - y$. Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$, the polynomial $f(T) + sT$ satisfies (*) with $m = 0$. 
Corollary 5. Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as in Theorem 4. Then $f$ satisfies (\*) with $m = 1$.

When $q$ is odd, Corollary 5 also follows from Corollary 1.4 in [3].

Example 6. Theorem 4 and Corollary 5 apply to $f(T) = T^{12} + T^3 \in \mathbb{F}_q[T]$ with $q$ a power of 2; the gcd of $\tilde{f}(x, y) - f'(x)$ and $\tilde{f}'(x, y)$ is $x - y$.

Remark 7. The statements of Theorem 4 and Corollary 5 would be false if one drops the gcd assumption. A counterexample is $f(T) = T^7$ in characteristic 2. Thus Theorem 4 here corrects the false Theorem 1.3 in our previous version [8] of this paper.

To apply Theorem 4 to a specific polynomial, one has to compute the greatest common divisor of the two polynomials that appear in the statement; this task is computationally easy. In fact, based on modest numerical evidence, we state the following

Conjecture 8. Let $k$ be a field and let $f \in k[T]$. Suppose $f'' \neq 0$. Then the polynomials $\tilde{f}(x, y) - f'(x)$ and $\tilde{f}'(x, y)$ in $k[x, y]$ have no common factors.

In other words, we conjecture that the assumptions in Theorem 4 not only cover further examples when $q$ is a power of 2 or char $\mathbb{F}_q | d$ but are actually strictly weaker than the assumptions in Proposition 2.

The proof of Theorem 4 is based on the technique employed by Entin in a variety of problems solved in [3], with an extra ingredient (Lemma 9 below) developed by the author in an earlier work, concerning the irreducibility of the perturbations of a certain curve. Namely, for $s \in \mathbb{F}_q$, we set up a generically étale map $\varphi_s : \mathbb{A}^1 \to \mathbb{A}^1$ of degree $d$ such that for any $b \in \mathbb{A}^1(\mathbb{F}_q)$ with $d$ preimages over $\mathbb{F}_q$, the conjugacy class in $S_d$ that the action of the Frobenius $\text{Fr}_q$ on $\varphi_s^{-1}(b)$ gives rise to has cycle structure corresponding to the factorization type of the polynomial $f(T) + sT + b$ in $\mathbb{F}_q[T]$. The statement will then follow by the Chebotarev density theorem for function fields, once we show that the monodromy group of $\varphi_s$ is the full symmetric group $S_d$. To this end, we check the criterion proven in [1].

2 The proof

We say that a polynomial $f(T) \in \overline{\mathbb{F}}_q[T]$ is “affine linearized” if it has the form $f(T) = \sum a_i T^{p^i} + f(0)$, where $p = \text{char} \mathbb{F}_q$.

Lemma 9. Let $f(T) \in \overline{\mathbb{F}}_q[T]$ be a polynomial of degree $d$, which is not affine linearized. For all but at most $d - 1$ values of $s \in \overline{\mathbb{F}}_q$, the polynomial $\tilde{f}(x, y) + s$ is geometrically irreducible.

Proof. The author has proven this as Lemma 19 in [7]. We sketch the proof here as well. First, an elementary undetermined coefficients argument shows that if $f$ is not affine linearized, the polynomial $\tilde{f}(x, y)$ cannot be written as $Q(h(x, y))$ for a polynomial $Q$ with deg $Q > 1$. Then we apply the main result of [6].
Lemma 10. Let \( f \in \mathbb{F}_q[T] \) be a polynomial that satisfies the hypotheses of Theorem 4. Then for all but \( d^2 - 2d \) values of \( s \in \mathbb{F}_q \), there exists a \( b \in \overline{\mathbb{F}}_q \) such that the polynomial \( f(T) + sT + b \) has a unique root of multiplicity 2 and \( d - 2 \) simple roots over \( \overline{\mathbb{F}}_q \).

Proof. Let \( B_1 = \{-f'(\alpha) \mid D^2f(\alpha) = 0\} \); then \( |B_1| \leq d - 2 \) and for any \( s \not\in B_1 \) and \( b \in \overline{\mathbb{F}}_q \), the polynomial \( f(T) + sT + b \) has no roots over \( \overline{\mathbb{F}}_q \) of multiplicity 3 or more.

Define
\[
X_1 := V(\tilde{f}(x, y) - f'(x)) \subset \mathbb{A}^2 \quad \text{and} \quad X_2 := V(\tilde{f}(x, y)) \subset \mathbb{A}^2.
\]
By Bézout’s theorem, there are at most \((d - 1)(d - 2)\) pairs \((\alpha, \beta) \in (X_1 \cap X_2)(\overline{\mathbb{F}}_q)\) with \( \alpha \neq \beta \). Let
\[
B_2 = \{-f'(\alpha) \mid (\alpha, \beta) \in (X_1 \cap X_2)(\overline{\mathbb{F}}_q) \text{ for some } \beta \in \overline{\mathbb{F}}_q, \beta \neq \alpha\};
\]
then \( |B_2| \leq (d - 1)(d - 2) \). Suppose \( \alpha \neq \beta \) in \( \overline{\mathbb{F}}_q \) are both roots of multiplicity at least 2 of some polynomial \( f(T) + sT + b \) with \( s, b \in \overline{\mathbb{F}}_q \). Explicitly, \( f(\alpha) + s\alpha + b = f(\beta) + s\beta + b = 0 \) and \( f'(\alpha) + s = f'(\beta) + s = 0 \). These imply \((\alpha, \beta) \in (X_1 \cap X_2)(\overline{\mathbb{F}}_q)\), hence \( s \in B_2 \).

The set \( B := B_1 \cup B_2 \) satisfies \(|B| \leq d^2 - 2d\). Let \( s \not\in B \). Choose \( \alpha \in \overline{\mathbb{F}}_q \) such that \( f'(\alpha) + s = 0 \) and set \( b := -f(\alpha) - s\alpha \). The polynomial \( f(T) + sT + b \) satisfies the requirement. \( \square \)

Proof of Theorem 4. For any \( s \in \mathbb{F}_q \), define
\[
\Omega_s := \{(t, b) \in \mathbb{A}_q^2 \mid f(t) + st + b = 0\}.
\]
The projection \( \Omega_s \to \mathbb{A}_q^1 \), \((t, b) \mapsto t\) is an isomorphism and the map \( \varphi_s : \Omega_s \to \mathbb{A}_q^1 \), \((t, b) \mapsto b\) is a generically étale morphism of degree \( d \) between geometrically irreducible \( \mathbb{F}_q \)-varieties.

The polynomial \( f(T) \) is not affine linearized, since \( \deg f' \geq 1 \). Combining Lemma 9 and Lemma 10, there exists a set \( B \subset \mathbb{F}_q \) of cardinality at most \( d^2 - d - 1 \) such that for any \( s \in \mathbb{F}_q \setminus B \), the following hold:

(i) the polynomial \( \tilde{f}(x, y) + s \) is geometrically irreducible, and

(ii) there exists a \( b \in \overline{\mathbb{F}}_q \) such that the polynomial \( f(T) + sT + b \) has a unique root of multiplicity 2 and \( d - 2 \) simple roots over \( \overline{\mathbb{F}}_q \).

Let \( s \in \mathbb{F}_q \setminus B \). By (ii), the fiber of \( \varphi_s \) over some \( b \in \overline{\mathbb{F}}_q \) consists of \( d - 1 \) points over \( \overline{\mathbb{F}}_q \), with \( \varphi_s \) being étale at \( d - 2 \) of them. Thus the assumption of Proposition 3 in [1] is satisfied. Moreover, the complement of the diagonal in \( \Omega_s \times_{\mathbb{A}_q^1, \varphi_s} \Omega_s \) is isomorphic to
\[
\Delta^c := \{(x, y) \in \mathbb{A}_q^2 \mid \tilde{f}(x, y) + s = 0, x \neq y\}.
\]
It is nonempty because we can pick a \( \beta \in \overline{\mathbb{F}}_q \) such that \( f'(\beta) + s \neq 0 \), set \( b := -f(\beta) - s\beta \) (so \( \beta \) is a simple root of \( f(T) + sT + b \)), let \( \gamma \) be any other root of \( f(T) + sT + b \) (note:
deg $f \geq 2$, since $\deg f' \geq 1$) and observe that $(\beta, \gamma) \in \Delta^c$. Thus $\Delta^c$ is a nonempty open subset of $V(\bar{f}(x, y) + s)$ and by (i) is geometrically irreducible. Therefore the assumption of Proposition 2 in [1] is satisfied as well. We conclude that the geometric monodromy group of the map $\varphi_s$ is the full $S_d$.

Let $U$ be a dense open subset of $\mathbb{A}^1_b$ such that $\varphi_s|_{\varphi^{-1}_s(U)}: \varphi^{-1}_s(U) \to U$ is finite and étale. The statement now follows from Theorem 3 in [3], which is a version of the Chebotarev density theorem for function fields. \hfill \Box

**Remark 11.** We can also deduce Corollary 4 directly from the criterion in [1], without going through Theorem 4. Namely, consider

$$
\Omega := \{(t, s, b) \in \mathbb{A}^3 \mid f(t) + st + b = 0\}
$$

and $\varphi: \Omega \to \mathbb{A}^2_{s,b}$. If $\Delta$ and $\Delta'$ denote the diagonals of $\Omega \times_{\mathbb{A}^2_{s,b}} \Omega$ and $\mathbb{A}^1_t \times \mathbb{A}^1_t$ respectively, then the map $\Omega \times_{\mathbb{A}^2_{s,b}} \Omega - \Delta \to \mathbb{A}^1_t \times \mathbb{A}^1_t - \Delta'$ is an isomorphism, so the source is geometrically irreducible. The existence of $(s, b) \in \mathbb{A}^2(\mathbb{F}_q)$ such that $f(T) + sT + b$ has a unique root of multiplicity 2 and $d - 2$ simple roots over $\mathbb{F}_q$ follows from Lemma 10.

**Acknowledgments**

I thank Bjorn Poonen and Alexei Entin for comments.

**References**

[1] E. Ballico, A. Hefez, *On the Galois group associated to a generically étale morphism*, Communications in Algebra, 14 (5), 899-909, 1986.

[2] E. Bank, L. Bary-Soroker, and L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*, Duke Math. J., 164 (2):277-295, 2015.

[3] A. Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, International Mathematics Research Notices, rnz120, https://doi.org/10.1093/imrn/rnz120, arXiv:1805.05454v2.

[4] M. Jarden and A. Razon. Skolem density problems over large Galois extensions of global fields. In Hilberts Tenth Problem: Relations with Arithmetic and Algebraic Geometry: Workshop on Hilberts Tenth Problem: Relations with Arithmetic and Algebraic Geometry, November 2-5, 1999, Ghent University, Belgium, volume 270, page 213. American Mathematical Soc., 2000.

[5] P. Kurlberg, L. Rosenzweig, *Prime and M"{o}bius correlations for very short intervals in $\mathbb{F}_q[x]$*, arXiv:1802.01215.

[6] D. Lorenzini, *Reducibility of polynomials in two variables*, J. of Algebra, 156 (1993), 65-75.
[7] K. Slavov, *An algebraic geometry version of the Kakeya problem*, Finite Fields and Their Applications, *37* (2016), 158-178.

[8] K. Slavov, *Factorization type probabilities of polynomials with prescribed coefficients over a finite field*, Acta Arithmetica *194* (2020), 315-318.