ACTA ARITHMETICA
Online First version

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

(Acta Arith. 194 (2020), 315–318)

by

Kaloyan Slavov

Abstract. We correct a gap in the paper of the title. Let $f(T)$ be a monic polynomial of degree d with coefficients in a finite field $\mathbb{F}_q$. 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 $f(T)+sT+b$ has a given factorization type λ over $\mathbb{F}_q$, as $b \in \mathbb{F}_q$ is chosen uniformly at random, is $p_\lambda + O_d(q^{-1/2})$, where p_λ is the probability that a permutation in S_d has cycle shape λ. The assumptions allow $(q, 2d) > 1$.

The statements of Theorem 1.3 and Corollary 1.4(a) in [1] are incorrect without an additional hypothesis. The polynomial $f(T) = T^7$ in characteristic 2 provides a counterexample. Before stating the corrected results, we recall the necessary notation.

Fix a positive integer $d > 1$. For a partition λ of d, let p_λ denote the probability that a permutation in S_d has cycle shape λ. Let $\mathbb{F}_q$ be a finite field. Let $f \in \mathbb{F}_q[T]$ be a monic polynomial of degree d. For $m \in \{0, 1, 2\}$, define

$$I(f, m) = \{f(T) + a_m T^m + \cdots + a_1 T + a_0 \mid a_0, \ldots, a_m \in \mathbb{F}_q\}.$$

Consider the statement

(∗) For any partition λ of d, the probability for an element of $I(f, m)$ to have factorization type λ is $p_\lambda + O_d(q^{-1/2})$ as $q \to \infty$.

Let $D^2 f$ denote the second Hasse derivative of f. For a polynomial $f(T) \in \mathbb{F}_q[T]$, let $\widetilde{f}(x, y)$ denote the polynomial in $\mathbb{F}_q[x, y]$ defined by

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

2020 *Mathematics Subject Classification*: Primary 14G15; Secondary 12F10.
Key words and phrases: monodromy group, Chebotarev density theorem, generically étale morphism, factorization type, finite field.
Received 4 December 2025; revised 16 May 2025.
Published online 9 June 2026.

DOI: 10.4064/aa251204-28-5

We now state the corrected main results. Compared to Theorem 1.3 in [1], we now add assumption (iii).

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

COROLLARY 2. *Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as in Theorem 1. Then f satisfies $(*)$ with $m=1$.*

Corollary 1.4(b) in [1] still holds as stated in [1], by Lemma 4 below.

EXAMPLE 3. Theorem 1 and Corollary 2 apply to $f(T) = T^{12} + T^3 \in \mathbb{F}_q[T]$ with q a power of 2; the gcd of $\widetilde{f}(x,y) - f'(x)$ and $\widetilde{(f')}(x,y)$ is $x-y$.

The mistake in the proof of Theorem 1.3 in [1] is in defining the bad locus $B = B_1 \cup B_2 \cup B_3$ in a circular way, with B_2 depending on s (which is supposed to be excluded from the bad locus in the end). We now fix this by redefining the curves X_1 and X_2, and hence the set B_2, in a way that depends only on f.

Proof of Theorem 1. Follow the proof of Theorem 1.3 in [1], but replace the first two sentences of the fourth paragraph by the following.

Consider

$$X_1 := V(\widetilde{f}(x,y) - f'(x)) \subset \mathbb{A}^2 \quad \text{and} \quad X_2 := V(\widetilde{(f')}(x,y)) \subset \mathbb{A}^2.$$

The gcd assumption ([1]) (iii) and Bézout's theorem imply that there are at most $(d-1)(d-2)$ pairs $(\alpha,\beta) \in (X_1 \cap X_2)(\overline{\mathbb{F}_q})$ with $\alpha \neq \beta$. ∎

LEMMA 4. *Let $f(T) \in \mathbb{F}_q[T]$ be a monic polynomial of degree d. If q is even, assume $\deg f'(T) \geq 1$. Then for all but at most $d-1$ values of $a \in \mathbb{F}_q$, the polynomial $f_a(T) := f(T) + aT^2$ satisfies condition* (iii) *in Theorem 1.*

Proof. The polynomials appearing in (iii) are

$$A_a(x,y) = \widetilde{f_a}(x,y) - f_a'(x) = \widetilde{f}(x,y) - f'(x) + a(y-x),$$
$$B_a(x,y) = \widetilde{(f_a')}(x,y) = \widetilde{(f')}(x,y) + 2a.$$

CASE 1: *q is even.* The assumption $\deg f'(T) \geq 1$ implies $\widetilde{(f')} \neq 0$. Thus $B_a(x,y)$ is a nonzero polynomial, independent of a. It has at most $d-2$ irreducible factors. For each irreducible factor h of $B_a(x,y)$ with h not associate to $x-y$, there is at most one value of $a \in \mathbb{F}_q$ such that $h \mid A_a(x,y)$.

([1]) The reason we can allow powers of $x-y$ as common factors in (iii) is that we only need to control the locus where $\alpha \neq \beta$.

This gives at most $d-2$ values of a such that $\gcd(A_a, B_a)$ is not a power of $x-y$.

Case 2: *q is odd, $d \geq 3$.* The polynomial

$$P(x,y) := 2A_a(x,y) - (y-x)B_a(x,y) = 2\widetilde{f}(x,y) - f'(x) - f'(y)$$

is nonzero, since it contains the mixed term $x^{d-2}y$.

If $a \in \mathbb{F}_q$ is such that an irreducible h divides both A_a and B_a, then $h \mid P$. Since $\deg P \leq d-1$, there are at most $d-1$ possibilities for h. But for a given h, there is at most one value of $a \in \mathbb{F}_q$ such that $h \mid B_a$.

Case 3: *q is odd, $d = 2$.* In this case, $A_a(x,y) = (a+1)(y-x)$ and $B_a(x,y) = 2(a+1)$. So $\gcd(A_a, B_a) = 1$ for $a \neq -1$. ∎

To apply Theorem 1 to a specific polynomial, one has to compute the gcd of the two polynomials that appear in the statement; this task is computationally easy. Numerical evidence suggests that when q is odd, (ii) implies (iii) in Theorem 1. We propose the following

Conjecture 5. Let k be a field with $\mathrm{char}(k) \neq 2$ and let $f \in k[T]$. Suppose $D^2 f \neq 0$. Then the polynomials $\widetilde{f}(x,y) - f'(x)$ and $\widetilde{(f')}(x,y)$ in $k[x,y]$ have no common factors.

References

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

Kaloyan Slavov
Department of Pharmacy
Medical University Sofia
1000 Sofia, Bulgaria
E-mail: k.slavov@pharmfac.mu-sofia.bg
and
Department of Mathematics
ETH Zürich
8092 Zürich, Switzerland
E-mail: kaloyan.slavov@math.ethz.ch