Factorization patterns on nonlinear families of univariate polynomials over a finite field

Guillermo Matera

Universidad de Buenos Aires and CONICET

Joint work with Mariana Pérez and Melina Privitelli

Universidad Nacional de General Sarmiento and CONICET

Carleton Finite Fields eSeminar
July 22, 2020

Notations

$\mathbb{F}_q$	finite field of q elements and characteristic p,
$\overline{\mathbb{F}}_q$	algebraic closure of $\mathbb{F}_q$,
$M(r)$	the set of monic polynomials of $\mathbb{F}_q[T]$ of degree r.

Let $\boldsymbol{\lambda} := 1^{\lambda_1} \dots r^{\lambda_r}$ be such that $r = \lambda_1 + 2\lambda_2 + \cdots + r\lambda_r$.

$f \in M(r)$ has factorization pattern $\boldsymbol{\lambda}$ if it has λ_i irreducible factors of degree i in $\mathbb{F}_q[T]$ for $1 \leq i \leq r$.

For $A \subset M(r)$, we denote

$$\mathcal{T}_{\boldsymbol{\lambda}}(A) := |\{f \in A : f \text{ has factorization pattern } \boldsymbol{\lambda}\}|.$$

Factorization patterns on linear families

[Cohen, Acta Arith. 17, 1970] For fixed r,

$$\mathcal{T}_{\boldsymbol{\lambda}}(M(r)) = \mathcal{T}(\boldsymbol{\lambda})\, q^r + \mathcal{O}(q^{r-\frac{1}{2}}),$$

where $\mathcal{T}(\boldsymbol{\lambda})$ is the proportion of elements in the rth symmetric group with cycle pattern $\boldsymbol{\lambda}$.

Examples

- If $\boldsymbol{\lambda} := (0, \ldots, 0, 1)$ (irreducible polynomials), then

$$\mathcal{T}(\boldsymbol{\lambda}) = \frac{1}{r} \ \text{ and } \ \mathcal{T}_{\boldsymbol{\lambda}}(M(r)) \approx \frac{q^r}{r} \ \text{(Gauss)}.$$

- For $\boldsymbol{\lambda} := (r, 0, \ldots, 0)$ (linear factors),

$$\mathcal{T}(\boldsymbol{\lambda}) = \frac{1}{r!} \ \text{ and } \ \mathcal{T}_{\boldsymbol{\lambda}}(M(r)) \approx \frac{q^r}{r!}.$$

Factorization patterns on linear families

We call $A \subset M(r)$ uniformly distributed if

$$\mathcal{T}_{\boldsymbol{\lambda}}(A) \sim \mathcal{T}(\boldsymbol{\lambda})|A|.$$

[Cohen, J. London Math. Soc. 6, 1972] Let $p > r$. Then the following linear families $A \subset M(r)$ are uniformly distributed:

- The elements of $M(r)$ with s coefficients preassigned (assuming $A \not\subset \mathbb{F}_q[T^l]$ for any $l > 1$);
- $C_r(f,g) := \{h \in M(r) : h \equiv f \mod g\}$, where $f, g \in \mathbb{F}_q[T]$ are relatively prime with $\deg f < r$.

Factorization patterns on linear families

[Bank et al, Duke J Math 164, 2015] For any characteristic p, the following linear families $A \subset M(r)$ are uniformly distributed:

- The elements of $M(r)$ with the first $r - s \geq 3$ consecutive coefficients preassigned;
- $C_r(f, g) := \{h \in M(r) : h \equiv f \mod g\}$, where $f, g \in \mathbb{F}_q[T]$ are relatively prime with $\deg f \leq r - 4$.

[Cesaratto, M, Pérez, Combinatorica 37, 2017] For characteristic $p > 2$, let $A_s \subset M(r)$ be set of $f \in M(r)$ with the first $r - s \geq 3$ consecutive coefficients preassigned. Then

$$|\mathcal{T}_{\boldsymbol{\lambda}}(A_s) - \mathcal{T}(\boldsymbol{\lambda}) q^s| \leq q^{s-1}\left(2\mathcal{T}(\boldsymbol{\lambda}) rs \frac{(r-1)!}{(r-s)!} q^{\frac{1}{2}} + 20\mathcal{T}(\boldsymbol{\lambda}) r^2 s^2 \frac{(r-1)!^2}{(r-s)!^2}\right).$$

Factorization patterns on nonlinear families

Problem 2.2 of [Gao, Howell, Panario, Proc. Fq4, 1999] asks for estimates on the number of polynomials of a given degree with a given factorization pattern lying in nonlinear families:

for $m < r$, indeterminates $\boldsymbol{A} := (A_{r-1}, \ldots, A_0)$ over $\overline{\mathbb{F}}_q$, and $G_1, \ldots, G_m \in \mathbb{F}_q[\boldsymbol{A}]$, consider the algebraic variety

$$W = \{\boldsymbol{a} \in \overline{\mathbb{F}}_q^r : G_1(\boldsymbol{a}) = 0, \ldots, G_m(\boldsymbol{a}) = 0\},$$

and the family

$$\mathcal{A} := \{T^r + a_{r-1}T^{r-1} + \cdots + a_0 \in M(r) : (a_{r-1}, \ldots, a_0) \in W\}.$$

[Chatzidakis et al., J. Reine Angew. Math. 427, 1992]
[Fried et al., Israel J. Math. 85, 1994] Let $n := \dim W$. There is a constant $d \geq 0$ such that, for large q,

$$|\mathcal{T}_{\boldsymbol{\lambda}}(\mathcal{A})| = d\mathcal{T}(\boldsymbol{\lambda})q^n + \mathcal{O}(q^{n-\frac{1}{2}}).$$

Factorization patterns on nonlinear families

Aims:

- provide a general criterion for a nonlinear family $\mathcal{A} \subset M(r)$ to be uniformly distributed (in the sense of Cohen);
- find explicit estimates on $|\mathcal{A}_{\boldsymbol{\lambda}}|$ for any factorization pattern $\boldsymbol{\lambda}$.

For a fixed k, let $\mathbb{F}_q[\boldsymbol{A}_k] := \mathbb{F}_q[A_{r-1}, \dots, A_{k+1}, A_{k-1}, \dots, A_0]$, let $G_1, \dots, G_m \in \mathbb{F}_q[\boldsymbol{A}_k]$ and $W := \{G_1 = 0, \dots, G_m = 0\}$. Let

$$\mathcal{A} := \{T^r + a_{r-1}T^{r-1} + \cdots + a_0 \in M(r) : G_i(\boldsymbol{a}_k) = 0 \ (1 \le i \le m)\}.$$

For the weight $\mathrm{wt} : \mathbb{F}_q[\boldsymbol{A}_k] \to \mathbb{N}_0$, $\mathrm{wt}(A_j) := r - j$ $(0 \le j \le r-1)$, denote by $G_1^{\mathrm{wt}}, \dots, G_m^{\mathrm{wt}}$ the components of highest weight of $G_1, \dots, G_m$. Let $(\partial \boldsymbol{G} / \partial \boldsymbol{A}_k)$ be the Jacobian matrix of $G_1, \dots, G_m$ with respect to $\boldsymbol{A}_k$. Assume that $G_1, \dots, G_m$ satisfy the conditions:

(H_1) $G_1, \dots, G_m$ form a regular sequence of $\mathbb{F}_q[\boldsymbol{A}_k]$.

(H_2) $(\partial \boldsymbol{G} / \partial \boldsymbol{A}_k)$ has full rank on every point of W.

(H_3) $G_1^{\mathrm{wt}}, \dots, G_m^{\mathrm{wt}}$ satisfy (H_1) and (H_2).

Let $\overline{\mathbb{F}}_q[T]_r$ be the set of monic polynomials of $\overline{\mathbb{F}}_q[T]$ of degree r.
For $\mathcal{B} \subset \overline{\mathbb{F}}_q[T]_r$, the discriminant locus $\mathcal{D}(\mathcal{B})$ of $\mathcal{B}$ is

$$\begin{aligned}\mathcal{D}(\mathcal{B}) &:= \{f \in \mathcal{B} \colon \ f \text{ not square–free}\} \\ &:= \{f \in \mathcal{B} : \mathrm{Disc}(f) := \mathrm{Res}(f, f') = 0\}.\end{aligned}$$

(see [Fried, Smith, Acta Arith 44, 1984] and [M, Pérez, Privitelli, Acta Arith 165, 2014] for the study of discriminant loci).

Our next conditions require that the discriminant intersects well W, and the same happens on the highest weight:

(H_4) $\mathcal{D}(W)$ has codimension ≥ 1 in W.

(H_5) $\mathcal{D}(V(G_1^{\mathrm{wt}}, \ldots, G_m^{\mathrm{wt}}))$ has codim ≥ 1 in $V(G_1^{\mathrm{wt}}, \ldots, G_m^{\mathrm{wt}})$.

We also need the first subdiscriminant locus $\mathcal{S}_1(\mathcal{B})$ of $\mathcal{B} \subset \overline{\mathbb{F}}_q[T]_r$:

$$\begin{aligned}\mathcal{S}_1(\mathcal{B}) &:= \{f \in \mathcal{D}(\mathcal{B}) : \deg \gcd(f, f') > 1\} \\ &:= \{f \in \mathcal{D}(\mathcal{B}) : \mathrm{Subdisc}(f) := \mathrm{Subres}(f, f') = 0\}.\end{aligned}$$

We require that $\mathcal{D}(W)$ and $\mathcal{S}_1(W)$ intersect well W:

(H_6) $(A_0 \cdot \mathcal{S}_1)(W) := \{\boldsymbol{a}_0 \in W : a_0 = 0\} \cup \mathcal{S}_1(W)$ has codimension at least one in $\mathcal{D}(W)$.

Suppose that $\mathrm{char}(\mathbb{F}_q) > 3$. Let $r, m \in \mathbb{Z}_{\geq 0}$ be such that $3 \leq r - m$ and $L_1, \ldots, L_m \in \mathbb{F}_q[A_{r-1}, \ldots, A_3]$ linear polynomials which are linearly independent. In [Cesaratto, M, Pérez, Combinatorica 37, 2017] the following linear family is considered:

$$\mathcal{A} := \left\{ T^r + a_{r-1} T^{r-1} + \cdots + a_0 \in M(r) : L_j(a_{r-1}, \ldots, a_3) = 0 \ \forall j \right\}.$$

We have:

Lemma: $L_1, \ldots, L_m$ satisfy hypotheses (H_1)–(H_6).

Examples of linear and nonlinear families

In [Gao, Howell, Panario, Proc. Fq4, 1999] there are experimental results on the number of irreducible polynomials on certain families over $\mathbb{F}_q$. In particular, the following family is considered.

Suppose that $\mathrm{char}(\mathbb{F}_q) > 3$. For $s, r \in \mathbb{Z}_{\geq 0}$ with $3 \leq s \leq r - 2$, let

$$\mathcal{A} := \{T^r + g(T)T + 1 : \ g \in \mathbb{F}_q[T] \text{ and } \deg g \leq s - 1\}.$$

Observe that $\mathcal{A}$ is isomorphic to the set of $\mathbb{F}_q$–rational points of the affine $\mathbb{F}_q$–subvariety of $\mathbb{A}^r$ defined by

$$G_1 := A_0 - 1, \ G_2 := A_{s+1}, \dots, G_{r-s} := A_{r-1}.$$

Lemma: $\mathcal{A}$ satisfies hypotheses (H_1)–(H_6) are fulfilled.

Examples of linear and nonlinear families

Let $r, t_1, \ldots, t_r \in \mathbb{Z}_{\geq 0}$ with r even. Suppose that $\mathrm{char}(\mathbb{F}_q) > 3$ does not divide $(r-1)(r+1)\big((r-1)^{r-1} + r^r\big)$. Consider the polynomial $G \in \mathbb{F}_q[A_1, \ldots, A_r]$ defined in the following way:

$$G := \det \begin{pmatrix} A_r & 1 & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ A_1 & \ldots & \ldots & A_r & 1 \end{pmatrix}$$

$$:= \sum_{t_1 + 2t_2 + \ldots + rt_r = r} (-1)^{\Delta(t_1, \ldots, t_r)} \frac{(t_1 + \cdots + t_r)!}{t_1! \ldots t_r!} A_r^{t_1} \cdots A_1^{t_r},$$

where $\Delta(t_1, t_2, \ldots, t_r) := r - \sum_{i=1}^{r} t_i$ (this is the well–known Trudi formula). $H_r := G(\Pi_r, \ldots, \Pi_1)$ is critical in the study of deep holes of the standard Reed–Solomon codes (see Cafure, M, Privitelli, Adv. Math. Commun. 6, 2012).

Examples of linear and nonlinear families

We consider the following family of polynomials:

$$\mathcal{A}_{\mathcal{N}} := \{\, T^{r+1} + a_r T^r + \cdots + a_0 \in M(r+1) : G(a_r, \ldots, a_1) = 0\}.$$

Observe that $\mathcal{A}_{\mathcal{N}}$ may be seen as the set of $\mathbb{F}_q$–rational points of the $\mathbb{F}_q$–variety $W := V(G) \subset \mathbb{A}^{r+1}$.

Lemma: $\mathcal{A}_{\mathcal{N}}$ satisfies hypotheses (H_1)–(H_6).

A simple example: consider $\boldsymbol{\lambda} := (r, 0, \ldots, 0)$ and the family

$$A_s := \left\{ T^r + a_{r-1} T^{r-1} + \cdots + a_0 : a_{r-s-1}, \ldots, a_0 \in \mathbb{F}_q \right\}.$$

Let $X_1, \ldots, X_r$ be indeterminates, $\boldsymbol{X} := (X_1, \ldots, X_r)$ and

$$G(\boldsymbol{X}, T) := (T + X_1) \cdots (T + X_r) = T^r + \Pi_1 T^{r-1} + \cdots + \Pi_r,$$

where $\Pi_1, \ldots, \Pi_r \in \mathbb{F}_q[\boldsymbol{X}]$ are the elementary symmetric polynomials.

- $f \in M(r)$ has pattern $\boldsymbol{\lambda} \Leftrightarrow \exists\, \boldsymbol{x} \in \mathbb{F}_q^r$ with $f = G(\boldsymbol{x}, T)$.
- $G(\boldsymbol{x}, T) \in A_s \Leftrightarrow \Pi_j(\boldsymbol{x}) = a_{r-j}$ for $1 \leq j \leq s$.

We conclude that

$$\mathcal{T}_{\boldsymbol{\lambda}}(A_s) \sim \frac{1}{r!} \cdot \left| \{\Pi_1 = a_{r-1}, \ldots, \Pi_s = a_{r-s}\} \cap \mathbb{F}_q^r \right|.$$

Factorization patterns on nonlinear families

Fix $a_{r-1}, \ldots, a_{r-s} \in \mathbb{F}_q$ and consider the $\mathbb{F}_q$–variety

$$V := \{\boldsymbol{x} \in \overline{\mathbb{F}}_q^r : \Pi_1(\boldsymbol{x}) = a_{r-1}, \ldots, \Pi_s(\boldsymbol{x}) = a_{r-s}\}.$$

Fact: V is a complete intersection. In particular,

- all the irreducible components of V have dimension $r - s$;
- the degree of V is $\leq \deg \Pi_1 \cdots \deg \Pi_s = s!$.

To estimate $|V(\mathbb{F}_q)|$, we need to prove that V is absolutely irreducible (=irreducible as an $\overline{\mathbb{F}}_q$–variety). For this purpose, we study its singular locus.

In Cesaratto, M, Pérez, Privitelli [J. Combin. Theory A 124, 2014], M, Pérez, Privitelli [Acta Arith. 165, 2014], Cesaratto, M, Pérez [Combinatorica 37, 2017] we study the singular locus of complete intersections defined by symmetric polynomials.

Theorem: Singular points $\boldsymbol{x} := (x_1, \ldots, x_r) \in V$ correspond to polynomials $f \in A_s$ which are not square-free.

This leads us to consider the discriminant locus of A_s. Let $\boldsymbol{a} := (a_{r-s-1}, \ldots, a_0) \in \overline{\mathbb{F}}_q^{r-s}$ and let

$$f_{\boldsymbol{a}} := T^r + a_{r-1}T^{r-1} + \cdots + a_{r-s}T^{r-s} + a_{r-s-1}T^{r-s-1} + \cdots + a_0 \in A_s.$$

Then the discriminant locus of A_s is

$$\mathcal{D}(A_s) := \{\boldsymbol{a} \in \overline{\mathbb{F}}_q^{r-s} : f_{\boldsymbol{a}} \text{ is not square-free}\}.$$

Factorization patterns on nonlinear families

Theorem (Fried, Smith [Acta Arith. 44, 1984]): Let $A(i_1,\ldots,i_s)\subset M(r)$ be the family of monic polynomials with fixed coefficients $a_{i_1},\ldots,a_{i_s}$. There exists $n(i_1,\ldots,i_s)\in\mathbb{N}$ such that $\mathcal{D}(A(i_1,\ldots,i_s))$ is absolutely irreducible if $\gcd\big(n(i_1,\ldots,i_s),p\big)=1$.

In M, Pérez, Privitelli [Acta Arith. 165, 2014] we prove:

Theorem: For $p>2$ and $r-s\geq 3$, the discriminant locus $\mathcal{D}(A_s)$ is absolutely irreducible.

Corollary: $\mathrm{Sing}(V)$ has dimension $\leq \dim(V)-2$.

Combining this result with explicit estimates for singular projective complete intersections we obtain:

Theorem: For $p>2$ y $r-s\geq 3$, we have

$$\left|\mathcal{T}_{\boldsymbol{\lambda}}(A_s)-\frac{q^{r-s}}{r!}\right|\leq\frac{(r+2)!}{r!}q^{r-s-\frac{1}{2}}+6\frac{((s+2)!)^2}{r!}q^{r-s-1}.$$

(precise for $s\lesssim r/2$)

Factorization patterns on nonlinear families

Our main result shows that:

- any family $\mathcal{A}$ satisfying (H_1)–(H_6) is uniformly distributed (in the sense of Cohen),
- provides explicit estimates on $|\mathcal{A}_{\boldsymbol{\lambda}}|$.

More precisely, we have the following result:

Theorem: For $m < r$ and a factorization pattern $\boldsymbol{\lambda}$, we have

$$\big||\mathcal{A}_{\boldsymbol{\lambda}}| - \mathcal{T}(\boldsymbol{\lambda})\, q^{r-m}\big| \leq q^{r-m-1}\big(\mathcal{T}(\boldsymbol{\lambda})(D\delta\, q^{\frac{1}{2}} + 14D^2\delta^2 + r^2\delta) + r^2\delta\big),$$

where $\delta := \prod_{i=1}^{m} \mathrm{wt}(G_i)$ and $D := \sum_{i=1}^{m}(\mathrm{wt}(G_i) - 1)$.

Average-case analysis of factorization

As an application of our theorem, we determine the average-case analysis of the classical factorization algorithm applied to any family $\mathcal{A}$ satisfying (H_1)–(H_6).

Problem: given $f \in M(r)$, find the factorization of f as $f = f_1^{e_1} \cdots f_r^{e_r}$, where the $f_i \in \mathbb{F}_q[T]$ are irreducible, monic, pairwise distinct and $e_i > 0$.

The classical factorization algorithm roughly proceeds by the following steps:

1. Elimination of repeated factors (ERF).
2. Distinct-degree factorization (DDF).
3. Equal-degree factorization (EDF).

Average-case analysis of factorization

Let $\mathcal{M}(r) := r \log r \log\log r$, $\mathcal{U}(r) := \mathcal{M}(r) \log r$.

There exist $\tau_1, \tau_2 > 0$ such that:

- multiplication of $f, g \in M(r)$: $\tau_1 \mathcal{M}(r)$ operations in $\mathbb{F}_q$,
- division with remainder of $f, g \in M(r)$: $\tau_1 \mathcal{M}(r)$ ops in $\mathbb{F}_q$,
- gcd of $f, g \in M(r)$: $\tau_2 \mathcal{U}(r)$ operations in $\mathbb{F}_q$.

Von zur Gathen, Gerhard [Modern computer algebra, CUP, 1999]: On input $f \in M(r)$, in worst-case, the classical factorization algorithm performs $\mathcal{O}(r\mathcal{M}(r)\log(rq))$ operations in $\mathbb{F}_q$:

ERF: $\mathcal{O}(\mathcal{U}(r) + r\log(\frac{q}{p}))$ operations in $\mathbb{F}_q$.

DDF: $\mathcal{O}(s\mathcal{M}(r)\log(rq))$ operations in $\mathbb{F}_q$,
where $s =$ highest degree of the irreducible factors of f.

EDF: $\mathcal{O}((k\log q + \log r)\mathcal{M}(r)\log s)$ operations in $\mathbb{F}_q$,
where $s =$ number of irreducible factors of degree k of f.

Average-case analysis of factorization

Flajolet, Gourdon, Panario [J. Algorithms 40, 2001]: average-case analysis (based on the distribution of factorization patterns in $M(r)$). Assuming that classical polynomial multiplication is used:

- ERF: $\mathcal{O}(r^2)$ operations in $\mathbb{F}_q$.
- DDF: $\mathcal{O}(r^3 \log q)$ operations in $\mathbb{F}_q$.
- EDF: $\mathcal{O}(r^2 \log q)$ operations in $\mathbb{F}_q$.

We consider the uniform probability on $\mathcal{A}$ and the random variable $\mathcal{X} : \mathcal{A} \to \mathbb{Z}_{\geq 0}$, $\mathcal{X}(f) =$ number of operations in $\mathbb{F}_q$ performed by the classical factorization algorithm on input f.

Aim: To obtain an upper bound on

$$E[\mathcal{X}] := \frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{X}(f).$$

Average-case analysis of factorization

Recall that $\mathrm{ERF}(f_1^{e_1} \cdots f_r^{e_r}) = f_1 \cdots f_r$. Let $\mathcal{X}_1 : \mathcal{A} \to \mathbb{Z}_{\geq 0}$, $\mathcal{X}_1(f) =$ number of operations in $\mathbb{F}_q$ of $\mathrm{ERF}(f)$, and let

$$E[\mathcal{X}_1] := \frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{X}_1(f).$$

Let $\mathcal{A}^{sq} = \{f \in \mathcal{A} : f \text{ is square-free}\}$ and $\mathcal{A}^{nsq} := \mathcal{A} \setminus \mathcal{A}^{sq}$.

- $f \in \mathcal{A}^{nsq} \Leftrightarrow \mathrm{Disc}(f) = 0 \Rightarrow |\mathcal{A}^{nsq}| = \mathcal{O}(q^{r-m-1})$.
- For $q \gg 0$, $|\mathcal{A}| \geq \frac{1}{2} q^{r-m} \Rightarrow \mathrm{Prob}[\mathcal{A}^{sq}] > 1/2$.

Theorem: For $q > 15\delta_G^{13/3}$, $\delta_G = \deg(G_1) \cdots \deg(G_m)$,

$$E[\mathcal{X}_1] \leq c_2 \,\mathcal{U}(r) + c_3 \log\left(\frac{q}{p}\right) \delta_G \frac{r^3}{q},$$

where c_2, c_3 are constants independent of r and q.

Next we consider DDF: $\mathrm{DDF}(\mathrm{ERF}(f)) := (b(1), \ldots, b(s))$, where

$b(k) =$ product of all irreducible factors of degree k of $\mathrm{ERF}(f)$.

Let $\mathcal{X}_2 : \mathcal{A} \to \mathbb{Z}_{\geq 0}$, $\mathcal{X}_2(f) =$ number of operations in $\mathbb{F}_q$ of $\mathrm{DDF}(\mathrm{ERF}(f))$, and

$$E[\mathcal{X}_2] := \frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{X}_2(f).$$

Theorem: For $q > 15\delta_{\mathsf{G}}^{13/3}$,

$$E[\mathcal{X}_2] \leq \xi \left(2\,\tau_1\,\lambda(q) + \tau_1 + \tau_2 \log r\right)\mathcal{M}(r)\,(r+1)\big(1 + o(1)\big),$$

where $\xi \sim 0.62432945\ldots$ is the Golomb constant.

Theorem: The probability that DDF outputs the complete factorization of a random $f \in \mathcal{A}$ is

$\left(e^{-\gamma} + \frac{e^{-\gamma}}{r} + \mathcal{O}\left(\frac{\log r}{r^2}\right)\right)\big(1+o(1)\big)$, $e^{-\gamma} \sim 0.5614\ldots$, γ Euler's constant.

Average-case analysis of factorization

Finally we consider EDF: if $\mathrm{DDF}(f) = (b(1), \ldots, b(s))$, then $\mathrm{EDF}(f)$ factorizes each $b(k)$. Let $\mathcal{X}_3 : \mathcal{A} \to \mathbb{Z}_{\geq 0}$, $\mathcal{X}_3(f) =$ number of operations in $\mathbb{F}_q$ of $\mathrm{EDF}(\mathrm{DDF}(\mathrm{ERF}(f)))$, and

$$E[\mathcal{X}_3] := \frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{X}_3(f) = \sum_{k=1}^{\lceil r/2 \rceil} \underbrace{\frac{1}{|\mathcal{A}|} \sum_{f \in \mathcal{A}} \mathcal{X}_{3,k}(f)}_{E[\mathcal{X}_{3,k}]},$$

$$\mathcal{X}_{3,k}(f) := \mathrm{Cost}(\mathrm{EDF}(b(k))).$$

Theorem: For $q > 15\delta_{\mathsf{G}}^{13/3}$,

$$E[\mathcal{X}_3] = \tau\, \mathcal{M}(r) \log q\, (1 + o(1)),$$

where τ is a constant independent of q and r.

Thanks!!!