Designs, Codes and Cryptography (2019) 87:1657–1671
https://doi.org/10.1007/s10623-018-0568-0

Factorization of a class of composed polynomials

Lucas Reis[1,2]

Received: 11 March 2018 / Revised: 20 September 2018 / Accepted: 26 September 2018 /
Published online: 9 October 2018

Abstract
In this paper, we provide the degree distribution of irreducible factors of the composed polynomial $f(L(x))$ over $\mathbb{F}_q$, where $f(x) \in \mathbb{F}_q[x]$ is irreducible and $L(x) \in \mathbb{F}_q[x]$ is a linearized polynomial. We further provide some applications of our main result, including lower bounds for the number of irreducible factors of $f(L(x))$, constructions of high degree irreducible polynomials and the explicit factorization of $f(x^q - x)$ under certain conditions on $f(x)$.

Keywords Factorization · Finite fields · Linearized polynomials · $\mathbb{F}_q$-order

Mathematics Subject Classification 12E20 · 11T30

1 Introduction

The factorization of polynomials as well as constructions of irreducible polynomials over finite fields play important roles in modern communications. Applications include algebraic coding theory [1], cryptography [8] and computational number theory. Many methods on the construction of irreducible polynomials [7] and the factorization of reducible polynomials [2] consider compositions of the form $f(g(x))$, where f is an irreducible polynomial. For a generic polynomial $g \in \mathbb{F}_q[x]$, there is no efficient method to determine the factorization of the composition $f(g(x))$ or even just obtain the degrees of its irreducible factors. In general [5], the factorization of $f(g(x))$ is strongly related to the factorization of $g(x) - \alpha \in \mathbb{F}_{q^n}[x]$, where $\alpha \in \mathbb{F}_{q^n}$ is any root of $f(x)$. If $g(x)$ has some additional field structure, the factorization of $g(x) - \alpha \in \mathbb{F}_{q^n}[x]$ and therefore $f(g(x)) \in \mathbb{F}_q[x]$ may be treatable. For instance, if $g = x^d$ is a monomial, g has a multiplicative structure: if $\gcd(d, q) = 1$ and α_0 is a root of $x^d - \alpha$, the roots of $x^d - \alpha$ are $\gamma\alpha_0$, where γ varies through the roots of $x^d - 1$. Butler [3] obtained the following result:

Communicated by G. Kyureghyan.

✉ Lucas Reis
lucasreismat@gmail.com

[1] Departamento de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, Brazil

[2] Present Address: School of Mathematics and Statistics, Carleton University, Ottawa, Canada

Theorem 1 *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n such that any of its roots has multiplicative order e. Let m be a positive integer such that $\gcd(m, q) = 1$ and $m = m_1 m_2$, where $\gcd(m_1, e) = 1$ and each prime factor of m_2 divides e. Then*

(i) *each root of $f(x^m)$ has multiplicative order of the form Mm_2e, where $M|m_1$;*
(ii) *if $M|m_1$, then $f(x^m)$ has exactly $\frac{nm_2\varphi(M)}{\mathrm{ord}_{Mm_2e}q}$ irreducible factors of degree $\mathrm{ord}_{Mm_2e}q$ with roots of multiplicative order Mm_2e, where φ is the Euler Phi Function and $\mathrm{ord}_b a$ is the order of a modulo b.*

Recently [2], the authors propose an efficient method to obtain the factorization of $f(x^m)$ under some special conditions on m and $f(x)$. Another interesting class of polynomials is the *linearized* polynomials $L = \sum_{i=0}^{m} a_i x^{q^i} \in \mathbb{F}_q[x]$. These polynomials induce $\mathbb{F}_q$-linear maps in any finite extension of $\mathbb{F}_q$. Using the additive structure of linearized polynomials, Long and Vaughan [10] obtain an implicit description of the degree distribution of irreducible factors of $f(L(x))$ in the case that L is linearized. However, the degrees of the irreducible factors are not explicitly given and the number of irreducible factors of each degree depends on the kernels of linear maps in extensions of $\mathbb{F}_q$; perhaps, this is due to the methods in Linear Algebra employed. The aim of this paper is to provide a far more explicit version of such result, in the sense that all the quantities depend only on elementary functions. Our approach relies on the $\mathbb{F}_q$-order of elements in finite fields, that corresponds to an additive analogue of the multiplicative order. In this correspondence, polynomial analogues of many number theoretic functions arise. In particular, our description yields a linearized analogue of Theorem 1. A more detailed account in our main result provides a lower bound for the number N of irreducible factors of $f(L(x))$ over $\mathbb{F}_q$ and, in particular, we obtain a characterization of the irreducible polynomials of the form $f(L(x))$: the irreducible polynomials arise exactly when $N = 1$. We explore special cases when $N = 2$ and, in particular, we obtain a method to produce high degree irreducible polynomials from primitive polynomials. We further present an efficient method to obtain the explicit factorization of $f(L(x)) \in \mathbb{F}_q[x]$ in the case that $L = x^q - x$ and f is an irreducible polynomial of degree n and trace zero, where n is relatively prime with q.

2 Preliminaries

In this section, we provide a background material that is used along the way. Throughout this paper, we fix $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime p. We start with some basic notations: $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$ and $\mathrm{ord}(\alpha) := \min\{d > 0 \mid \alpha^d = 1\}$ is the multiplicative order of $\alpha \in \overline{\mathbb{F}}_q^*$. For $\alpha \in \overline{\mathbb{F}}_q$, $m_\alpha(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of α over $\mathbb{F}_q$ and $\deg(\alpha) := \deg(m_\alpha)$ is the degree of α over $\mathbb{F}_q$. It is known that, if $d = \deg(\alpha)$, then $\mathbb{F}_{q^d}$ is the smallest extension of $\mathbb{F}_q$ that contains α and $m_\alpha(x) = \prod_{i=0}^{d-1}(x - \alpha^{q^i})$: the elements α^{q^i} are the *conjugates* of α. In the following theorem, we summarize some basic facts on the multiplicative order of elements in finite fields.

Theorem 2 *Let $\alpha \in \overline{\mathbb{F}}_q^*$ be an element of multiplicative order $\mathrm{ord}(\alpha) = e$. The following hold:*

(i) $\deg(\alpha) = \mathrm{ord}_e q$;
(ii) *if $\beta = \alpha^s$, then $\mathrm{ord}(\beta) = \frac{e}{\gcd(e,s)}$.*

In addition, for any positive integer E relatively prime with q, there exist $\varphi(E)$ elements $\alpha \in \overline{\mathbb{F}}_q^*$ such that $\mathrm{ord}(\alpha) = E$.

The previous theorem can be proved using the definition of cyclotomic polynomials over finite fields and Theorem 2.47 of [9].

2.1 Linearized polynomials and the $\mathbb{F}_q$-order

For a polynomial $g \in \mathbb{F}_q[x]$ with $g(x) = \sum_{i=0}^{m-1} a_i x^i$, the polynomial

$$L_g(x) := \sum_{i=0}^{m-1} a_i x^{q^i},$$

is the *q-associate* of g. Of course, L_g is always a linearized polynomial; conversely, any linearized polynomial $L \in \mathbb{F}_q[x]$ is the q-associate of some polynomial in $\mathbb{F}_q[x]$. In the following lemma, we show that the q-associates have interesting arithmetic properties.

Lemma 1 *Let $g, h \in \mathbb{F}_q[x]$. The following hold:*

(i) $L_g(x) + L_h(x) = L_{g+h}(x)$;
(ii) $L_g(L_h(x)) = L_{gh}(x)$.

Proof For the proof of this result, see Section 3.4 of [9]. □

For an element $\alpha \in \overline{\mathbb{F}}_q$, we set $I_\alpha = \{g \in \mathbb{F}_q[x] \mid L_g(\alpha) = 0\}$. From Lemma 1, I_α is an ideal of $\mathbb{F}_q[x]$ and, if $\alpha \in \mathbb{F}_{q^d}$, $L_{x^d-1}(\alpha) = \alpha^{q^d} - \alpha = 0$, hence $x^d - 1 \in I_\alpha$. In particular, I_α is a nontrivial ideal of $\mathbb{F}_q[x]$ and so I_α is generated by a polynomial $m_{\alpha,q}(x)$, which we can suppose to be monic. Therefore, for any $\alpha \in \overline{\mathbb{F}}_q$ and any $g \in \mathbb{F}_q[x]$, we have that $L_g(\alpha) = 0$ if and only if g is divisible by $m_{\alpha,q}(x)$.

Definition 1 For an element $\alpha \in \overline{\mathbb{F}}_q$, the polynomial $m_{\alpha,q}(x)$ is the $\mathbb{F}_q$-*order* of α over $\mathbb{F}_q$.

For instance, the element 0 has $\mathbb{F}_q$-order $m_{0,q}(x) = 1$ and any element $c \in \mathbb{F}_q^*$ has $\mathbb{F}_q$-order $m_{c,q}(x) = x - 1$. In general, for $\alpha \in \mathbb{F}_{q^d}$, $m_{\alpha,q}(x)$ divides $x^d - 1$; in particular, $\gcd(m_{\alpha,q}(x), x) = 1$. It is straightforward to check that the $\mathbb{F}_q$-order of an element α coincides with the $\mathbb{F}_q$-order of any of its conjugates α^{q^i}. The $\mathbb{F}_q$-order of an element is the *additive* analogue of the multiplicative order in finite fields: in this analogy, Theorem 2 can be translated to $\mathbb{F}_q$-order with a suitable change of some arithmetic functions.

Definition 2 Let $f, g \in \mathbb{F}_q[x]$.

(i) The *norm* of f is $N(f) = q^d$, where $d = \deg(f)$.
(ii) The *Euler Phi function* for polynomials over $\mathbb{F}_q$ is

$$\Phi_q(f) = \left| \left(\frac{\mathbb{F}_q[x]}{\langle f \rangle} \right)^* \right|,$$

where $\langle f \rangle$ is the ideal generated by f in $\mathbb{F}_q[x]$.
(iii) if $\gcd(f, g) = 1$, $\mathcal{O}(f, g) := \min\{k > 0 \mid f^k \equiv 1 \pmod{g}\}$ is the order of f modulo g.

The function Φ_q is multiplicative (Chinese Remainder Theorem) and

$$\Phi_q(g^s) = q^{(s-1)d}(q^d - 1) = N(g)^{s-1}(N(g) - 1),$$

if g is an irreducible polynomial of degree d and s is a positive integer: compare $\Phi_q(g^s)$ with $\varphi(r^s) = r^{s-1}(r-1)$ if r is a prime number. For more details on the function Φ_q, see Section 3.4 of [9]. It is straightforward to check that $\mathcal{O}(f, g)$ divides $\Phi_q(g)$. In duality to the multiplicative order in finite fields, we have the following additive version of Theorem 2.

Theorem 3 *Let $\alpha \in \overline{\mathbb{F}}_q$ be an element of $\mathbb{F}_q$-order $m_{\alpha,q}(x) = h$. The following hold:*

(i) $\deg(\alpha) = \mathcal{O}(x, h)$;
(ii) *if $\beta = L_g(\alpha)$, then β has $\mathbb{F}_q$-order $m_{\beta,q}(x) = \frac{h}{\gcd(h,g)}$.*

In addition, for any polynomial H relatively prime with x, there exist $\Phi_q(H)$ elements $\alpha \in \overline{\mathbb{F}}_q$ such that $m_{\alpha,q}(x) = H$.

Proof (i) Observe that $\deg(\alpha)$ is the least positive integer k such that $\alpha \in \mathbb{F}_{q^k}$. Also, for any positive integer d, we have that $\alpha \in \mathbb{F}_{q^d}$ if and only if

$$L_{x^d-1}(\alpha) = \alpha^{q^d} - \alpha = 0,$$

that is, $m_{\alpha,q}(x) = h$ divides $x^d - 1$. Now, the result follows from definition of $\mathcal{O}(x, h)$.
(ii) This item follows by direct calculations.
For the proof of the last statement, see Theorem 11 of [11]. □

It is well known that, for any positive integer n, $\sum_{d|n} \varphi(d) = n$. As follows, we also have the polynomial version of this result.

Lemma 2 *For any polynomial $g \in \mathbb{F}_q[x]$ of degree d, the following holds:*

$$\sum_{h|g} \Phi_q(h) = q^d = N(g), \tag{1}$$

where h is monic and polynomial division is over $\mathbb{F}_q$.

Proof We observe that if $g = x^s g_0$ with $s \geq 1$ and $\gcd(g_0, x) = 1$, then

$$\begin{aligned}\sum_{h|g} \Phi_q(h) &= \sum_{i=0}^{s} \sum_{h|g_0} \Phi_q(hx^i) \\ &= \sum_{h|g_0} \Phi_q(h) \left(1 + \sum_{i=1}^{s} q^{i-1}(q-1)\right) = q^s \sum_{h|g_0} \Phi_q(h),\end{aligned}$$

where $q^s = N(x^s)$. In particular, it is sufficient to prove Eq. (1) for the case $\gcd(g, x) = 1$: in this case, the formal derivative of $L_g(x)$ is a nonzero constant and so the equation $L_g(x) = 0$ has exactly $\deg(L_g) = q^d$ distinct solutions in $\overline{\mathbb{F}}_q$. It is straightforward to see that, for $\alpha \in \overline{\mathbb{F}}_q$, $L_g(\alpha) = 0$ if and only if $m_{\alpha,q}(x)$ divides g and the result follows from Theorem 3. □

3 The additive analogue of Theorem 1

So far we have provided a duality between the multiplicative order and the $\mathbb{F}_q$-order in finite fields. At this point, it is clear what are the objects in this additive-multiplicative correspondence. We summarize them as follows.

$\mathbb{Z} \leftrightarrow$	$\mathbb{F}_q[x]$
$q \leftrightarrow$	x
$\lvert n\rvert = n \leftrightarrow$	$N(f) = q^{\deg(f)}$
$\mathrm{ord}(\alpha) \leftrightarrow$	$m_{\alpha,q}(x)$
$\varphi(n) \leftrightarrow$	$\Phi_q(f)$
$\mathrm{ord}_b a \leftrightarrow$	$\mathcal{O}(f, g)$
primes $\leftrightarrow$	monic irreducible polynomials
monomials $\leftrightarrow$	linearized polynomials

Motivated by this correspondence, we present the linearized version of Theorem 1.

Theorem 4 *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n such that any of its roots has $\mathbb{F}_q$-order h. Let $g \in \mathbb{F}_q[x]$ be a monic polynomial such that $\gcd(g(x), x) = 1$ and write $g = g_1 g_2$, where $\gcd(g_1, h) = 1$ and each irreducible factor of g_2 divides h. If L_g denotes the q-associate of g and $\deg(g_2) = m$, then*

(i) *each root of $f(L_g(x))$ has $\mathbb{F}_q$-order of the form Gg_2h, where G divides g_1;*
(ii) *if G divides g_1, $f(L_g(x))$ has exactly*

$$\frac{nN(g_2)\Phi_q(G)}{\mathcal{O}(x, Gg_2h)} = \frac{nq^m\Phi_q(G)}{\mathcal{O}(x, Gg_2h)},$$

irreducible factors of degree $\mathcal{O}(x, Gg_2h)$ with roots of $\mathbb{F}_q$-order Gg_2h.

Remark 1 The condition $\gcd(g, x) = 1$ in Theorem 4 is not restrictive: if $g = x^s g_0$ with $\gcd(x, g_0) = 1$, then

$$f(L_g(x)) = f(L_{g_0}(x))^{q^s},$$

and Theorem 4 can be applied for the composition $f(L_{g_0}(x))$.

Remark 2 It is worth mentioning that some particular cases of Theorem 4 were previously considered, where it is obtained an explicit description on the degree distributions. For instance, see Theorem 3.63 of [9] and Theorem 3.2 of [4].

Example 1 We consider $q = 2$, $f = x^2+x+1$ and $g = x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$. In this case, the roots of f have $\mathbb{F}_q$-order equals $h = x^2 + 1$ and then, in the notation of Theorem 4, $g = g_1g_2$, where $g_1 = x^3 + x^2 + 1$ and $g_2 = x + 1$. In addition, $n = \deg(f) = 2$ and $m = \deg(g_2) = 1$, $\mathcal{O}(x, g_2h) = \mathcal{O}(x, (x + 1)^3) = 4$ and $\mathcal{O}(x, g_1g_2h) = \mathcal{O}(x, (x^3 + x^2 + 1)(x + 1)^3) = 28$. Also, $\Phi_q(1) = 1$, and $\Phi_q(g_1) = 7$. According to Theorem 4, the polynomial

$$f(L_g(x)) = f(x^{16} + x^4 + x^2 + x) = x^{32} + x^{16} + x^8 + x + 1,$$

has exactly $\frac{2\cdot 2^1}{4} = 1$ irreducible factor of degree 4 (with roots of $\mathbb{F}_q$-order $(x + 1)^3$) and $\frac{2\cdot 2^1\cdot 7}{28} = 1$ irreducible factor of degree 28 (with roots of $\mathbb{F}_q$-order $(x^3 + x^2 + 1)(x + 1)^3$). If we compute the factorization of $f(L_g(x))$ over $\mathbb{F}_2$ we obtain

$$x^{32} + x^{16} + x^8 + x + 1 = F_1(x) \times F_2(x),$$

where $F_1(x) = x^4 + x + 1$ and $F_2(x) = x^{28} + x^{25} + x^{24} + x^{22} + x^{20} + x^{19} + x^{18} + x^{17} + x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + 1$.

Before we proceed in the proof of Theorem 4, we need some technical lemmas.

Lemma 3 *For any $\alpha, \beta \in \overline{\mathbb{F}}_q$ with $\alpha \neq \beta$ and any polynomial $h \in \mathbb{F}_q[x]$ not divisible by x, the following hold:*

(i) *the polynomials $L_h(x) - \alpha$ and $L_h(x) - \beta$ are relatively prime;*
(ii) *the polynomial $L_h(x) - \alpha$ has only simple roots in $\overline{\mathbb{F}}_q$.*

Proof (i) This item is straightforward.
(ii) Since h is not divisible by x, the formal derivative of the polynomial $L_h(x) - \alpha$ is a nonzero constant and so $L_h(x) - \alpha$ cannot have repeated roots. □

Lemma 4 *Let $\alpha \in \overline{\mathbb{F}}_q$ be an element with $\mathbb{F}_q$-order $h(x) = m_{\alpha,q}(x)$ and let $g \in \mathbb{F}_q[x]$ be any polynomial not divisible by x. If there exists a polynomial H not divisible by x and an element $\beta \in \overline{\mathbb{F}}_q$ such that β has $\mathbb{F}_q$-order $H = m_{\beta,q}$ and $L_g(\beta) = \alpha$, then h divides H and the number of such elements β is at most $\frac{\Phi_q(H)}{\Phi_q(h)}$.*

Proof From Theorem 3, if $L_g(\beta) = \alpha$, then $h = m_{\alpha,q} = \frac{m_{\beta,q}}{\gcd(g, m_{\beta,q})}$ and so h divides $m_{\beta,q} = H$. Therefore, we have the natural group inclusion $\mathbb{G}_1 \subseteq \mathbb{G}_2$, where $\mathbb{G}_1 = \left(\frac{\mathbb{F}_q[x]}{\langle h \rangle}\right)^*$ and $\mathbb{G}_2 = \left(\frac{\mathbb{F}_q[x]}{\langle H \rangle}\right)^*$. In particular, if $M = \Phi_q(h) = |\mathbb{G}_1|$ and $A_1, \ldots, A_M \in \mathbb{F}_q[x]$ are the polynomials such that $\gcd(A_i, h) = 1$ and $\deg(A_i) < \deg(h)$, then there exist polynomials $B_1, \ldots, B_M \in \mathbb{F}_q[x]$ such that $B_i \equiv A_i \pmod{h}$, $\gcd(B_i, H) = 1$ and $\deg(B_i) < \deg(H)$.

Let $S_h \subset \overline{\mathbb{F}}_q$ be the set of elements with $\mathbb{F}_q$-order h. In particular, $\alpha \in S_h$; we claim that $S_h = C$, where $C = \{L_{A_i}(\alpha) \,|\, 1 \leq i \leq M\}$. For this, we observe that, since $\deg(A_i) < \deg(h)$, the differences $A_i - A_j$ with $i \neq j$ are not divisible by h and so $0 \neq L_{A_i - A_j}(\alpha) = L_{A_i}(\alpha) - L_{A_j}(\alpha)$. In particular, C has $|M| = \Phi_q(h) = |S_h|$ distinct elements. Since $\gcd(A_i, h) = 1$, it follows from Theorem 3 that the $\mathbb{F}_q$-order of any $L_{A_i}(\alpha)$ equals h, hence $C \subseteq S_h$ and so $C = S_h$. In addition, if $\gamma \in \overline{\mathbb{F}}_q$ is any element of $\mathbb{F}_q$-order $H = m_{\gamma,q}$ and $L_g(\gamma) = \alpha$, from Theorem 3, $\gamma_i := L_{B_i}(\gamma)$ has $\mathbb{F}_q$-order $\frac{H}{\gcd(B_i, H)} = H$ and satisfies

$$L_g(\gamma_i) = L_g(L_{B_i}(\gamma)) = L_{B_i}(\alpha) = L_{A_i}(\alpha).$$

In particular, for any $\theta \in S_h$, the number of elements $\beta \in \overline{\mathbb{F}}_q$ with $\mathbb{F}_q$-order equals H that satisfies $L_g(\beta) = \theta$ is the same. From Theorem 3, there exist $\Phi_q(H)$ elements with $\mathbb{F}_q$-order equals H and, since S_h has $\Phi_q(h)$ elements, the result follows. □

3.1 Proof of Theorem 4

Proof Following the notation of Theorem 4, let $\alpha \in \mathbb{F}_{q^n}$ be any root of f, hence

$$f(x) = \prod_{i=0}^{n-1} \left(x - \alpha^{q^i}\right).$$

Let β be any root of $f(L_g(x))$. In particular, $L_g(\beta)$ is a root of f and, without loss of generality, suppose that $L_g(\beta) = \alpha$.

(i) Set $H = m_{\beta,q}$, the $\mathbb{F}_q$-order of β. From Lemma 4, $m_{\alpha,q}(x) = h$ divides H. Additionally, since $L_{gh}(\beta) = L_h(L_g(\beta)) = L_h(\alpha) = 0$, H divides gh. In particular, there exist

divisors h_1 of g_1 and h_2 of g_2 such that $H = hh_1h_2$. Because $L_g(\beta) = \alpha$, from Theorem 3, it follows that

$$h = \frac{H}{\gcd(H, g)} = \frac{hh_1h_2}{\gcd(hh_1h_2, g)},$$

and so $h_1h_2 = \gcd(hh_1h_2, g)$. Since h_1h_2 divides $g_1g_2 = g$, we have that

$$\gcd(hh_1h_2, g) = h_1h_2 \cdot \gcd\left(h, \frac{g}{h_1h_2}\right).$$

Therefore, $\gcd(h, \frac{g}{h_1h_2}) = 1$, i.e., $\gcd(h, \frac{g_1}{h_1} \cdot \frac{g_2}{h_2}) = 1$. Recall that g_1 and h are relatively prime and every irreducible divisor of g_2 divides h: from the previous equality, we conclude that $\frac{g_2}{h_2} = 1$, i.e., $h_2 = g_2$. In particular, $H = Gg_2h$, where $G = h_1$ is a divisor of g_1.

(ii) For each divisor G of g_1, let $n(G, f)$ be the number of elements $\gamma \in \overline{\mathbb{F}}_q$ such that γ has $\mathbb{F}_q$-order Gg_2h and is a root of $f(L_g(x))$. Since

$$f(L_g(x)) = \prod_{i=0}^{n-1} \left(L_g(x) - \alpha^{q^i}\right),$$

from Lemma 3, $f(L_g(x))$ has only simple roots. In particular, from the previous item, it follows that

$$\sum_{G|g_1} n(G, f) = \deg(f(L_g(x))) = nq^{\deg(g)}.$$

In addition, we observe that any root γ of $f(L_g(x))$ satisfies $L_g(\gamma) = \alpha^{q^i}$ for some $0 \leq i \leq n-1$ and the $\mathbb{F}_q$-order of α^{q^i} equals $m_{\alpha,q} = h$. Therefore, from Lemma 4, it follows that $n(G, f) \leq n \cdot \frac{\Phi_q(Gg_2h)}{\Phi_q(h)}$; since every prime divisor of g_2 divides h and $\gcd(G, h) = 1$, we have that

$$\Phi_q(Gg_2h) = \Phi_q(G)\Phi_q(g_2h) = \Phi_q(G)N(g_2)\Phi_q(h),$$

hence $n(G, f) \leq n \cdot N(g_2)\Phi_q(G)$. From Eq. (1), we have that $\sum_{G|g_1} \Phi_q(G)$ equals $N(g_1)$ and then

$$\begin{aligned} nq^{\deg(g)} &= \sum_{G|g_1} n(G, f) \leq \sum_{G|g_1} n \cdot N(g_2)\Phi_q(G) = n \cdot N(g_2) \sum_{G|g_1} \Phi_q(G) \\ &= n \cdot N(g_2)N(g_1) = n \cdot N(g) = nq^{\deg(g)}. \end{aligned}$$

Therefore, we necessarily have equality $n(G, f) = n \cdot N(g_2)\Phi_q(G)$. In particular, we have shown that, for each divisor G of g_1, there exist $n \cdot N(g_2)\Phi_q(G)$ roots of $f(L_g(x))$ with $\mathbb{F}_q$-order equals Gg_2h. In addition, from the previous item, this describes all the roots of $f(L_g(x))$. From item (i) of Theorem 3, an element $\beta \in \overline{\mathbb{F}}_q$ with $\mathbb{F}_q$-order Gg_2h has degree $\deg(\beta) = \mathcal{O}(x, Gg_2h)$: in this case, the $n \cdot N(g_2)\Phi_q(G)$ roots of $f(L_g(x))$ with $\mathbb{F}_q$-order Gg_2h are divided in

$$\frac{n \cdot N(g_2)\Phi_q(G)}{\mathcal{O}(x, Gg_2h)} = \frac{nq^{\deg(g_2)}\Phi_q(G)}{\mathcal{O}(x, Gg_2h)} = \frac{nq^m\Phi_q(G)}{\mathcal{O}(x, Gg_2h)}$$

sets, according to their minimal polynomial over $\mathbb{F}_q$. In conclusion, for each divisor G of g_1, $f(L_g(x))$ has $\frac{nq^m\Phi_q(G)}{\mathcal{O}(x,Gg_2h)}$ irreducible factors of degree $\mathcal{O}(x, Gg_2h)$ and this describes the factorization of $f(L_g(x))$ over $\mathbb{F}_q$. □

4 Applications of Theorem 4

In this section, we provide some consequences of Theorem 4. We observe that, under the conditions of Theorem 4, the number $NI(f, g)$ of irreducible factors of $f(L_g(x))$ satisfies

$$NI(f, g) = \sum_{G|g_1} \frac{nq^m \Phi_q(G)}{\mathcal{O}(x, Gg_2h)}. \tag{2}$$

In particular, it is interesting to find estimates for the numbers $\mathcal{O}(x, F)$, where F is a polynomial not divisible by x. We start with the following definition.

Definition 3 For a polynomial $F \in \mathbb{F}_q[x]$, $\nu(F)$ is the greatest nonnegative integer d with the property that there exists an irreducible polynomial $h \in \mathbb{F}_q[x]$ such that h^d divides F. Also, $\mathrm{rad}(F)$ denotes the *squarefree* part of F, i.e., $\mathrm{rad}(F)$ equals the product of the distinct irreducible divisors of F.

Since finite fields are *perfect fields*, $\nu(F)$ is the maximal multiplicity of a root of F over $\overline{\mathbb{F}}_q$. Moreover, it is clear that F divides $\mathrm{rad}(F)^{\nu(F)}$. The following lemma provides some basic facts on the numbers $\mathcal{O}(x, F)$.

Lemma 5 *Let $F, G \in \mathbb{F}_q[x]$ be polynomials not divisible by x. The following hold:*

(i) *if* $\gcd(F, G) = 1$, *then*

$$\mathcal{O}(x, FG) = \mathrm{lcm}(\mathcal{O}(x, F), \mathcal{O}(x, G)) \leq \mathcal{O}(x, F) \cdot \mathcal{O}(x, G).$$

In particular, if F is squarefree, $\mathcal{O}(x, F)$ is not divisible by p.

(ii) $\mathcal{O}(x, F) = \mathcal{O}(x, \mathrm{rad}(F)) \cdot p^r$, *where* $r = \lceil \log_p \nu(F) \rceil$.

(iii) *If* $\mathrm{rad}(F)$ *divides* G, *then*

$$\mathcal{O}(x, FG) = \mathcal{O}(x, G) \cdot p^u, \tag{3}$$

where $u = \lceil \log_p(\nu(FG)) \rceil - \lceil \log_p(\nu(G)) \rceil$ *satisfies*

$$u \leq \lceil \log_p(\nu(F)/\nu(G) + 1) \rceil \leq \left\lceil \frac{\nu(F)}{\nu(G)} \right\rceil, \ \nu(G) \geq 1.$$

Proof (i) The equality $\mathcal{O}(x, FG) = \mathrm{lcm}(\mathcal{O}(x, F), \mathcal{O}(x, G))$ follows by direct calculations. If F is squarefree and factors as $F = F_1 \cdots F_j$, where each F_i is irreducible and of degree d_i, $\mathcal{O}(x, F)$ is the least common multiple of the numbers $\mathcal{O}(x, F_i)$, for $1 \leq i \leq j$. Recall that $\mathcal{O}(x, F_i)$ divides $\Phi_q(F_i) = q^{d_i} - 1$, which is not divisible by p. In particular, $\mathcal{O}(x, F)$ is not divisible by p.

(ii) Let $s = \mathcal{O}(x, \mathrm{rad}(F))$ and $S = \mathcal{O}(x, F)$. In particular, $\mathrm{rad}(F)$ divides $x^s - 1$ and, since $\mathrm{rad}(F)$ is squarefree, from the previous item, it follows that s is not divisible by p. For $r = \lceil \log_p \nu(F) \rceil$, we have $p^r \geq \nu(F)$, hence $(x^s - 1)^{p^r} = x^{sp^r} - 1$ is divisible by $\mathrm{rad}(F)^{\nu(F)}$. Recall that F divides $\mathrm{rad}(F)^{\nu(F)}$, hence F divides $x^{sp^r} - 1$ and so S divides sp^r. Clearly, S is divisible by s and then $S = sp^e$ for some nonnegative integer $e \leq r$. Since s is not divisible by p, the polynomial $x^s - 1$ has no repeated irreducible factors and so $\nu(x^{sp^e} - 1) = p^e$. However, F divides $x^{sp^e} - 1$, and then $p^e = \nu(x^{sp^e} - 1) \geq \nu(F)$. Therefore, $e \geq \lceil \log_p \nu(F) \rceil = r$ and, since $e \leq r$, we necessarily have $e = r$.

(iii) Since $\mathrm{rad}(F)$ divides G, $\mathrm{rad}(G) = \mathrm{rad}(FG)$ and so Eq. (3) follows from the previous item. We observe that $\nu(FG) \leq \nu(F) + \nu(G)$ for any polynomials F and G. In addition, $\lceil y_0 - y \rceil \geq \lceil y_0 \rceil - \lceil y \rceil$ for any real numbers $y_0 > y > 0$, and then for $\nu(G) \geq 1$,

$$u = \lceil \log_p(\nu(FG)) \rceil - \lceil \log_p(\nu(G)) \rceil \leq \lceil \log_p(\nu(F)/\nu(G) + 1) \rceil.$$

To finish the proof, we observe that $\log_a(y+1) \leq y$ for any real numbers $y \geq 1$ and $a \geq 2$.

□

As follows, we obtain a lower bound on the number $NI(f,g)$ of irreducible factors of $f(L_g(x))$ over $\mathbb{F}_q$: in particular, a characterization of the irreducible polynomials of the form $f(L_g(x))$ is given.

Theorem 5 *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n such that any of its roots has $\mathbb{F}_q$-order h. Let $g \in \mathbb{F}_q[x]$ be a (non constant) monic polynomial such that $\gcd(g,x) = 1$ and write $g = g_1 g_2$, where $\gcd(g_1, h) = 1$ and each irreducible factor of g_2 divides h. If L_g denotes the q-associate of g and $\deg(g_2) = m$, the number $NI(f,g)$ of irreducible factors of $f(L_g(x))$ over $\mathbb{F}_q$ satisfies the following:*

$$NI(f,g) \geq \frac{q^m W(g_1)}{p^u} \geq W(g_1)\left(\frac{q}{p}\right)^m, \tag{4}$$

where $u = \lceil \log_p(v(g_2 h)) \rceil - \lceil \log_p(v(h)) \rceil$ and $W(g_1)$ is the number of distinct monic divisors of g_1 over $\mathbb{F}_q$. In particular, $f(L_g(x))$ is irreducible over $\mathbb{F}_q$ if only if $q = p$ and the triple (p,h,g) satisfies one of the following conditions:

1. *p is any prime and $g = H$ is a polynomial of degree one that divides h but does not divide $\frac{x^n-1}{h}$;*
2. *$p = 2$, $g(x) = x^2 + 1$, h is squarefree and is divisible by $x+1$.*

Proof Let α be any root of f, hence $\deg(\alpha) = n$ and $h = m_{\alpha,q}(x)$. From item (i) of Theorem 3, $n = \mathcal{O}(x,h)$. From item (i) of Lemma 5, for each divisor G of g_1, we have $\mathcal{O}(x, Gg_2h) \leq \mathcal{O}(x,G) \cdot \mathcal{O}(x, g_2h)$. We have the trivial bound $\mathcal{O}(x,G) \leq \Phi_q(G)$. Since $\mathrm{rad}(g_2)$ divides h, from item (iii) of Lemma 5, we have that

$$\mathcal{O}(x, g_2h) = \mathcal{O}(x,h) \cdot p^u = np^u.$$

Taking these estimates into Eq. (2), we obtain the following inequality:

$$NI(f,g) = \sum_{G|g_1} \frac{nq^m \Phi_q(G)}{\mathcal{O}(x, Gg_2h)} \geq \sum_{G|g_1} \frac{nq^m \Phi_q(G)}{np^u \Phi_q(G)} = \frac{q^m}{p^u} \sum_{G|g_1} 1 = \frac{q^m W(g_1)}{p^u}.$$

In addition, item (iii) of Lemma 5 shows that $u \leq \lceil \frac{v(g_2)}{v(h)} \rceil \leq v(g_2) \leq \deg(g_2) = m$ and so $p^u \leq p^m$. This proves Inequality (4).

If $f(L_g(x))$ is irreducible, then $NI(f,g) = 1$: since $NI(f,g)$ is at least $W(g_1)(q/p)^m$ (which is a positive integer), if $f(L_g(x))$ is irreducible, then $W(g_1)(q/p)^m = 1$ and so $q = p$ and $W(g_1) = 1$, i.e., $g_1 = 1$ and $g_2 = g$. In particular, h is a non constant polynomial and so $v(h) \geq 1$. We have another restrictive condition: $q^m = p^u$. Since $q = p$, it follows that $u = m$. Since $v(h) \geq 1$, from item (iii) of Lemma 5 we have that $u \leq \lceil \log_p(v(g_2)/v(h) + 1) \rceil < \log_p(v(g_2)/v(h) + 1) + 1$, hence

$$m - 1 = u - 1 < \log_p(v(g_2)/v(h) + 1) \leq \log_p(m+1). \tag{5}$$

It follows by induction on a and b that $a^{b-1} \geq b+1$ if $a, b \geq 2$ are positive integers such that $a \geq 3$ or $b \geq 3$. In particular, Inequality (5) is false unless $m = 1$ and p is any prime number or $m = 2$ and $p = 2$. We divide into cases.

1. If $m = 1$ and p is any prime number, since $g_2 = g$, it follows that g equals a polynomial H of degree one that divides h: taking account in Eq. (2) we have $NI(f, g) = \frac{np}{\mathcal{O}(x,hH)}$. In particular, $f(L_g(x))$ is irreducible if and only if $\mathcal{O}(x, hH) = np$. Of course, $\mathcal{O}(x, hH)$ is divisible by $\mathcal{O}(x, h) = n$ and so $\mathcal{O}(x, hH) = np$ if and only if $\mathcal{O}(x, hH) \neq n$: since, h divides $x^n - 1$ and H is irreducible, we have that $\mathcal{O}(x, hH) \neq n$ if and only if H does not divide $\frac{x^n-1}{h}$.
2. If $m = 2$ and $p = 2$, Inequality (5) yields

$$1 < \log_2(\nu(g)/\nu(h) + 1) \leq \log_2 3,$$

hence $1 < \nu(g)/\nu(h) \leq 2$. Since $\nu(g) \leq \deg(g) = \deg(g_2) = 2$ and $\nu(h) \geq 1$, it follows that $\nu(g) = 2 = \deg(g)$ and $\nu(h) = 1$ and so g is the square of an irreducible polynomial of degree one and h is squarefree. Since $\gcd(g, x) = 1$ and $x, x + 1$ are the only degree one irreducible polynomials over $\mathbb{F}_q = \mathbb{F}_2$, it follows that $g = (x+1)^2 = x^2+1$: taking account in Eq. (2) we obtain

$$NI(f, g) = \frac{4n}{\mathcal{O}(x, h(x + 1)^2)}.$$

In particular, $f(L_g(x))$ is irreducible if and only if $\mathcal{O}(x, h(x + 1)^2) = 4n$. Let i be the greatest power of $x+1$ that divides h; since h is squarefree, $i \leq 1$ and $\nu(h(x+1)^2) = 2+i$. If $h_0 = \text{lcm}(x + 1, h)$, then $\text{rad}(h(x + 1)^2) = h_0$ and $\mathcal{O}(x, h_0) = n$. From item (ii) of Lemma 5, it follows that $\mathcal{O}(x, h(x+1)^2) = \mathcal{O}(x, h_0)\cdot 2^r = n2^r$, where $r = \lceil \log_p(2+i) \rceil$. Therefore, $f(L_g(x))$ is irreducible if and only if $n2^r = \mathcal{O}(x, h(x+1)^2) = 4n$, i.e., $r = 2$. The latter is equivalent to $i = 1$, i.e., h is divisible by $x + 1$. □

Remark 3 If we take $q = p$ a prime and $g(x) = x - 1$, condition 1 in Theorem 5 can be translated as follows: if $f \in \mathbb{F}_p[x]$ is a monic irreducible polynomial of degree n such that any of its roots has $\mathbb{F}_p$-order h, then $f(x^p - x) \in \mathbb{F}_p[x]$ is irreducible if and only if $x - 1$ divides h but does not divide $\frac{x^n-1}{h}$. Since $x - 1$ divides $x^n - 1$, the latter occurs if and only if h does not divide $H = \frac{x^n-1}{x-1}$. If α is any root of f, the $\mathbb{F}_q$-order of α is h and so h does not divide $H = \frac{x^n-1}{x-1}$ if and only if $L_H(\alpha) \neq 0$: we see that $L_H(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i} = a_{n-1}$, where a_{n-1} is the coefficient of x^{n-1} in $f(x)$, commonly called the *trace* of $f(x)$.

Based on the previous remark, the following corollary is straightforward.

Corollary 1 *If $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial, then $f(x^p - x)$ is irreducible if and only if the coefficient a_{n-1} of x^{n-1} in $f(x)$ is not zero.*

Remark 4 If we take $q = p = 2$ and $g(x) = x^2 + 1$, following the ideas in Remark 3, condition 2 in Theorem 5 can be translated as follows: if $f(x) \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree n such that any of its roots has $\mathbb{F}_2$-order h, then $f(x^4 + x) \in \mathbb{F}_2[x]$ is irreducible if and only if h is squarefree and the coefficient a_{n-1} of x^{n-1} in $f(x)$ is not zero. From items (i) and (ii) of Lemma 5, h is squarefree if and only if $\mathcal{O}(x, h) = n$ is not divisible by $p = 2$, i.e., n is odd.

Based on the previous remark, we obtain the following corollary.

Corollary 2 *If $f(x) \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree n, then $f(x^4+x) \in \mathbb{F}_2[x]$ is irreducible if and only if the coefficient a_{n-1} of x^{n-1} in $f(x)$ is not zero and n is odd.*

Remark 5 It is worth mentioning that the irreducible polynomials $f(L(x)) \in \mathbb{F}_q[x]$ with L a p-linearized polynomial (i.e., $L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$) were previously characterized in Theorem 6 of [6]. In particular, this result covers Corollaries 1 and 2.

We observe that the irreducible polynomials of the form $f(L_g(x))$ arising from Theorem 5 are such that every irreducible factor of g divides the $\mathbb{F}_q$-order h of the roots of f. In the following theorem, we consider the opposite situation.

Theorem 6 *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n such that any of its roots has $\mathbb{F}_q$-order h. Let $g \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree $d \geq 1$ such that $\gcd(g, x) = \gcd(g, h) = 1$ and write $e = \mathcal{O}(x, g)$. Then $f(L_g(x))$ factors as one irreducible polynomial of degree n and $\frac{n(q^d-1)}{\operatorname{lcm}(n,e)}$ irreducible polynomials of degree $\operatorname{lcm}(n, e)$. In particular, $f(L_g(x))$ factors into irreducible polynomials of the same degree if and only if g divides $x^n - 1$ and, in this case, the degree of each irreducible factor is n.*

Proof From item (i) of Theorem 3, $\mathcal{O}(x, h) = n$. We observe that $\Phi_q(g) = q^d - 1$ and, since $\gcd(g, h) = 1$, item (i) of Lemma 5 yields

$$\mathcal{O}(x, gh) = \operatorname{lcm}(\mathcal{O}(x, g), \mathcal{O}(x, h)) = \operatorname{lcm}(n, e).$$

Now, the degree distribution of irreducible factors of $f(L_g(x))$ follows from Theorem 4. Since the degrees of the irreducible factors of $f(L_g(x))$ are n and $\operatorname{lcm}(n, e)$, the polynomial $f(L_g(x))$ factors into irreducible polynomials of the same degree k if and only if $k = n$ and $\operatorname{lcm}(n, e) = n$, i.e., e divides n. The latter is equivalent to g divides $x^n - 1$. □

Remark 6 When a polynomial F is known to factor as irreducible polynomials of the same degree over a finite field, we have an efficient probabilistic method that provides the complete factorization of F: in the algorithm proposed in [14], if F has degree M, the expected number of operations in $\mathbb{F}_q$ to obtain the factorization of F over $\mathbb{F}_q$ is $O(M^{1.688} + M^{1+o(1)} \log q)$.

Corollary 3 *If $f(x) = \sum_{i=0}^{n} a_x^i \in \mathbb{F}_q[x]$ is an irreducible polynomial of degree n such that $a_{n-1} = 0$ and n is not divisible by the characteristic p of $\mathbb{F}_q$, then $f(x^q - x)$ factors as q irreducible polynomials of degree n.*

Proof Let α be any root of f and let h be the $\mathbb{F}_q$-order of α, hence $f(x) = \prod_{i=0}^{n-1}(x - \alpha^{q^i})$ and so $L_H(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} = a_{n-1} = 0$. In particular, H is divisible by h. Since n is not divisible by p, $x^n - 1 = H(x) \cdot (x - 1)$ has only simple roots, hence $\gcd(H, x - 1) = 1$ and then $\gcd(h, x - 1) = 1$. Now, the result follows from Theorem 6 with $g = x - 1$. □

If $g(x) \neq x$ is an irreducible polynomial of degree d and $\alpha \in \mathbb{F}_{q^d}$ is any root of g, we observe that $\mathcal{O}(x, g) = \operatorname{ord}(\alpha)$: in fact, the polynomial g divides $x^s - 1$ if and only if $\alpha^s = 1$. We have the bound $\mathcal{O}(x, g) \leq \Phi_q(g) = q^d - 1$ and equality holds if and only if $\operatorname{ord}(\alpha) = q^d - 1$, i.e., α is a generator of $\mathbb{F}_{q^d}^*$. In this case, α is a *primitive* element of $\mathbb{F}_{q^d}$ and g is commonly called a *primitive polynomial*. From Theorem 6, we have the following corollary.

Corollary 4 *Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n and let $g(x) \neq x, x - 1$ be an irreducible polynomial of degree d such that any of its roots has order $e = \mathcal{O}(x, g)$ and $\gcd(n, e) = 1$. The following hold:*

(i) *the polynomial $f(L_g(x))$ factors as one irreducible polynomial of degree n and $\frac{(q^d-1)}{e}$ irreducible factors of degree ne;*

(ii) *if g is a primitive polynomial, then $f(L_g(x))$ factors as one irreducible polynomial of degree n and one irreducible polynomial of degree $n(q^d-1)$.*

Proof Since $g(x) \neq x-1$ and $\gcd(n,e)=1$, one can see that g does not divide h. In particular, we are in the conditions of Theorem 6 and, since $\operatorname{lcm}(n,e)=ne$, item (i) follows from Theorem 6. Item (ii) follows directly from item (i) with $e=q^d-1$. □

4.1 Construction of high degree irreducible polynomials

Observe that item (ii) of Corollary 4 suggests the construction of irreducible polynomials of high degree from primitive polynomials: for instance, if f is an irreducible polynomial of degree n and g is a primitive polynomial of degree d such that $\gcd(n, q^d-1)=1$ with $q^d-1>1$, then $g(x)\neq x-1$. In particular, $f(L_g(x))$ factors as one irreducible polynomial G_1 of degree n and one irreducible polynomial G_2 of degree $n(q^d-1)>n$. We have $G_1=\gcd(f(L_g(x)), x^{q^n}-x)$ and so $G_2=\frac{f(L_g(x))}{G_1}$ is an irreducible polynomial of degree $n(q^d-1)$.

Remark 7 Similar ideas in the construction of irreducible polynomials of degree $n(q^d-1)$ were previously employed in [7], but with a different approach.

In the case $q=2$, the following proposition shows that we can iterate this construction.

Proposition 1 *Let $f\in\mathbb{F}_2[x]$ be an irreducible polynomial of degree n, let $\{d_1,\ldots,d_k\}$ be a set of pairwise relatively prime positive integers such that $d_i\geq 2$ and $\gcd(n,2^{d_i}-1)=1$ for any i. In addition, let $g_1,\ldots,g_k$ be primitive polynomials such that $\deg(g_i)=d_i$. Set $f_1=f$, $n_1=n$ and for $1\leq j\leq k$, let*

$$n_{j+1}=n(2^{d_1}-1)\cdots(2^{d_j}-1) \text{ and } f_{j+1}(x)=\frac{f_j(L_{g_j}(x))}{\gcd(f_j(L_{g_j}(x)), x^{2^{n_j}}+x)}.$$

For each $1\leq j\leq k+1$, $f_j(x)$ is an irreducible polynomial of degree n_j.

Proof We observe that, from hypothesis, the numbers d_i are pairwise relatively prime and so $\gcd(2^{d_i}-1, 2^{d_j}-1)=2^{\gcd(d_i,d_j)}-1=1$ for any $1\leq i<j\leq k$, i.e., the numbers $2^{d_i}-1$ are pairwise relatively prime. The fact that f_j is irreducible follows after applying the argument previously given for the pair $(f,g)=(f_j,g_j)$. □

We can apply Proposition 1 to a wide variety of sets $\{d_1,\ldots,d_k\}$. For instance, one may pick $\{d_1,\ldots,d_k\}$ as a set of distinct primes and n a power of two.

Example 2 Consider $f_1(x)=x^4+x+1\in\mathbb{F}_2[x]$ an irreducible polynomial of degree $n=4$ and let $g_1(x)=x^2+x+1$ and $g_2(x)=x^3+x+1$ be primitive polynomials. We obtain $f_2(x)=x^{12}+x^9+x^8+x^6+x^3+x^2+1$ and $f_3(x)=x^{84}+x^{81}+x^{80}+x^{76}+x^{73}+x^{72}+x^{70}+x^{69}+x^{67}+x^{65}+x^{60}+x^{57}+x^{56}+x^{54}+x^{51}+x^{50}+x^{45}+x^{44}+x^{42}+x^{39}+x^{38}+x^{36}+x^{30}+x^{27}+x^{26}+x^{16}+x^{15}+x^{14}+x^{13}+x^{10}+x^8+x^7+x^6+x^5+1$.

5 The explicit factorization of $f(x^q-x)$

From Corollary 3, we known that if f is an irreducible polynomial of degree n and trace zero, where n is not divisible by the characteristic p of $\mathbb{F}_q$, then $f(x^q-x)$ factors as q irreducible

polynomials of degree n. In this section, we provide an efficient method to obtain the explicit factorization of $f(x^q - x)$ under these conditions. We first observe that if $g(x)$ is an n degree irreducible factor of $f(x^q - x)$, then for any $a \in \mathbb{F}_q$, $g(x + a)$ is an irreducible polynomial of degree n and divides $f((x + a)^q - (x + a)) = f(x^q - x)$. One may wonder if $g(x + a)$ is distinct from $g(x)$. From Theorem 2.5 of [12], the following lemma is straightforward.

Lemma 6 *Let $g \in \mathbb{F}_q[x]$ be a polynomial of degree at least n and suppose that $a \in \mathbb{F}_q^*$ is such that $g(x + a) = g(x)$. Then n is divisible by p.*

From the previous lemma, we obtain the following result.

Corollary 5 *Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree n such that n is not divisible by p and suppose that $f(x^q - x)$ factors as q monic irreducible polynomials of degree n over $\mathbb{F}_q$. If $g(x)$ is one of these irreducible factors, then $f(x^q - x)$ factors as $\prod_{a\in\mathbb{F}_q} g(x + a)$.*

Proof From the previous observations, for any $a \in \mathbb{F}_q$, $g(x + a)$ is a monic irreducible polynomial of degree n that divides $f(x^q - x)$. Since there are exactly q polynomials $g(x+a)$ with $a \in \mathbb{F}_q$ and they are all monic, it is sufficient to prove that they are all different. For this, if $g(x + a) = g(x + b)$ with $a \neq b$ elements of $\mathbb{F}_q$, then $g_0(x + a_0) = g_0(x)$, where $g_0(x) = g(x + b)$ is a polynomial of degree n and $a_0 = a - b \neq 0$. From Lemma 6, n is divisible by p, contradicting our hypothesis. □

In particular, we have shown that the knowledge of just one irreducible factor $g(x)$ of $f(x^q - x)$ is sufficient to obtain the complete factorization of such a polynomial: the irreducible factors are $g(x + a)$ with $a \in \mathbb{F}_q$. In the following theorem, we show how to obtain one of these irreducible factors and hence obtain the explicit factorization of $f(x^q - x)$.

Theorem 7 *Let $f(x) = x^n + \sum_{i=}^{n-1} a_i x^i \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n such that $a_{n-1} = 0$ and n is not divisible by the characteristic p of $\mathbb{F}_q$. Let α be any root of f. For*

$$\beta = -\frac{1}{n}\sum_{i=1}^{n-1} i\alpha^{q^{n-1-i}} = -\frac{1}{n}(\alpha^{q^{n-2}} + 2\alpha^{q^{n-3}} + \cdots + (n-2)\alpha^q + (n-1)\alpha),$$

the following hold:

(i) *β is a root of $f(x^q - x)$ and, in particular, the minimal polynomial $g(x)$ of β has degree n and satisfies $g(x) = \prod_{i=0}^{n-1}(x - \beta^{q^i})$;*

(ii) *$g(x)$ is an irreducible factor of $f(x^q - x)$ and*

$$f(x^q - x) = \prod_{a\in\mathbb{F}_q} g(x + a),$$

is the complete factorization of $f(x^q - x)$ over $\mathbb{F}_q$.

Proof Under our hypothesis, Corollary 3 ensures that $f(x^q - x)$ factors as q irreducible polynomials of degree n. In particular, we are under the conditions of Corollary 5 and so it suffices to prove that β is a root of $f(x^q - x)$. We observe that

$$\beta^q - \beta = -\frac{1}{n}\sum_{i=1}^{n-1}\left(i\alpha^{q^{n-i}} - i\alpha^{q^{n-1-i}}\right) = -\frac{1}{n}\left(\alpha^{q^{n-1}} + \ldots + \alpha^q - (n-1)\alpha\right)$$
$$= -\frac{1}{n}\left(\alpha^{q^{n-1}} + \cdots + \alpha^q + \alpha\right) + \alpha = a_{n-1} + \alpha = \alpha,$$

since $0 = a_{n-1} = \sum_{i=0}^{n-1} \alpha^{q^i}$. In particular, $\beta^q - \beta$ is a root of $f(x)$ and so β is a root of $f(x^q - x)$. □

Remark 8 Using an algorithm of Shoup (see [13], Theorem 3.4), the minimal polynomial of β can be obtained with $O(n^{1.688})$ operations in $\mathbb{F}_q$. Since $f(x^q - x)$ has degree qn and factors as polynomials of the same degree, one may compare our method with the probabilistic approach of von zur Gathen and Shoup [14], which gives the same factorization with $O((qn)^{1.688} + (qn)^{1+o(1)} \log q)$ operations in $\mathbb{F}_q$ (see Remark 6). In this comparison, our method is fairly better when q is small, and is far more efficient if q is large.

Example 3 Let $f(x) = x^4 + x - 1 \in \mathbb{F}_5[x]$ be an irreducible polynomial. In the notation of Theorem 7, $n = 4$ and $p = 5$: we obtain $g(x) = x^4 - x^2 - x - 2$ and so

$$f(x^5 - x) = (x^5 - x)^4 + (x^5 - x) - 1 = \prod_{i=0}^{4} [(x+i)^4 - (x+i)^2 - (x+i) - 2],$$

or

$$\begin{aligned} x^{20} + x^{16} + x^{12} + x^8 + x^5 + x^4 - x - 1 = {} & (x^4 - x^2 - x - 2) \times (x^4 + x^3 + 2x - 1) \\ & \times (x^4 + 2x^3 - 2x^2 + x + 2) \\ & \times (x^4 - 2x^3 - 2x^2 + 2x - 2) \\ & \times (x^4 - x^3 + x + 2). \end{aligned}$$

In the case that f has degree 2 or has degree 3 and q is even, the minimal polynomial of β in Theorem 7 can be explicitly computed from the coefficients of f and, in particular, we obtain the factorization of special classes of polynomials over finite fields.

Corollary 6 *Let q be a power of a prime p. The following hold.*

(i) *if $p \neq 2$ and $a \in \mathbb{F}_q^*$ is a nonsquare, $f(x) = x^2 - a$ is irreducible and*

$$f(x^q - x) = x^{2q} - 2x^{q+1} + x^2 - a = \prod_{c \in \mathbb{F}_q} \left(x^2 + 2cx + c^2 - \frac{a}{4}\right).$$

(ii) *if $p = 2$ and $f(x) = x^3 + ax + b$ is irreducible over $\mathbb{F}_q$, then*

$$\begin{aligned} f(x^q - x) = f(x^q + x) &= x^{3q} + x^{2q+1} + x^{q+2} + ax^q + x^3 + ax + b \\ &= \prod_{c \in \mathbb{F}_q} f(x + c) \\ &= \prod_{c \in \mathbb{F}_q} (x^3 + cx^2 + (c^2 + a)x + c^3 + ac + b). \end{aligned}$$

Proof We observe that, from the hypothesis in items (i) and (ii), we are under the conditions of Theorem 7 and so only the computation of the polynomial $g(x)$ is needed.

(i) In this case, we have p odd and $n = 2$. Let α be a root of $f(x) = x^2 - a$, hence $\alpha^2 = a$. From Theorem 7, we obtain $\beta = -\alpha/2$, $g(x) = x^2 - a/4$ and the result follows.

(ii) In this case, $n = 3$ is such that n is not divisible by p. Let α be a root of $f(x) = x^3 + ax + b$. From Theorem 7, we obtain $\beta = \alpha^q + 2\alpha = \alpha^q$, $g(x) = f(x)$ and the result follows.

□

Acknowledgements This work was conducted during a visit to Carleton University, supported by the program CAPES-PDSE (process - 88881.134747/2016-01).

References

1. Berlekamp E.R.: Algebraic Coding Theory. McGraw-Hill, New York (1968).
2. Brochero Martínez F.E., Reis L.: Factoring polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$. Finite Fields Appl. **49**, 166–179 (2018).
3. Butler M.C.R.: The irreducible factors of $f(x^m)$ over a finite field. J. Lond. Math. Soc. **30**, 480–482 (1955).
4. Cao X., Hu L.: On the reducibility of some composite polynomials over finite fields. Des. Codes Cryptogr. **64**, 229–239 (2012).
5. Cohen S.D.: On irreducible polynomials of certain types in finite fields. Math. Proc. Camb. **66**, 335–344 (1969).
6. Cohen S.D.: The irreducibility of compositions of linear polynomials over a finite field. Comput. Math. **47**(2), 149–152 (1982).
7. Kyuregyan M.K., Kyureghyan G.M.: Irreducible compositions of polynomials over finite fields. Des. Codes Cryptogr. **61**, 301–314 (2011).
8. Lenstra Jr. H.W.: On the Chor–Rivest knapsack cryptosystem. J. Cryptol. **3**, 149–155 (1991).
9. Lidl R., Niederreiter H.: Introduction to Finite Fields and Their Applications. Cambridge University Press, New York (1986).
10. Long A.F., Vaughan T.P.: Factorization of $Q(h(T)(x))$ over a finite field where $Q(x)$ is irreducible and $h(T)(x)$ is linear I. Linear Algebra Appl. **11**, 53–72 (1975).
11. Ore O.: Contributions to the theory of finite fields. Trans. Am. Math. Soc. **36**, 243–274 (1934).
12. Reis L.: The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited. J. Pure Appl. Algebra **222**, 1087–1094 (2018).
13. Shoup V.: Fast construction of irreducible polynomials over finite fields. J. Symb. Comput. **17**, 371–391 (1994).
14. von zur Gathen J., Shoup V.: Computing Frobenius maps and factoring polynomials. Comput. Complex **2**, 1547–570 (1992).