Constructing irreducible polynomials recursively with a reverse composition method

Anna-Maurin Graner and Gohar Kyureghyan

University of Rostock, Germany
{anna-maurin.graner,gohar.kyureghyan}@uni-rostock.de

Abstract. In this paper we explain the connections between two recursive constructions of irreducible polynomials in $\mathbb{F}_q[X]$ given in [2, 5] and [10]. We use ideas from [2, 5] to suggest a construction which generalizes and extends the one from [10]. This construction allows to gain information on the order of a monic irreducible polynomial solely from its non-zero coefficients.

Keywords: Recursive construction · Irreducible polynomial · Composition method · Multiplicative order · k-th power · Characteristic polynomial.

1 Introduction

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. For $\beta \in \mathbb{F}_{q^n}$, we denote by $m_\beta \in \mathbb{F}_q[X]$ the minimal polynomial and by $\chi_\beta \in \mathbb{F}_q[X]$ the characteristic polynomial of β over $\mathbb{F}_q$. We call β a *proper* element of $\mathbb{F}_{q^n}$ if $\beta \in \mathbb{F}_{q^n}$ and there does not exist a proper subfield $\mathbb{F}_{q^m} < \mathbb{F}_{q^n}$ such that $\beta \in \mathbb{F}_{q^m}$. Furthermore, for $k \in \mathbb{N}$ we denote by U_k the group of the k-th roots of unity over $\mathbb{F}_q$, that is, the roots of the polynomial $X^k - 1 \in \mathbb{F}_q[X]$. Note that U_k need not be a subset of $\mathbb{F}_q$, but $U_k \subseteq \mathbb{E}$ for an extension field $\mathbb{E} \geq \mathbb{F}_q$. If $\gcd(q, k) = 1$, then there exists a primitive k-th root of unity ζ_k in $\mathbb{E}$ such that $U_k = \langle \zeta_k \rangle$.

The so-called composition method is widely used to construct irreducible polynomials, see for example [1, 4, 6–9, 11–14]. Originally based on a theorem by Cohen [3], with this method one composes an irreducible polynomial with polynomials or rational functions such that this composition then is irreducible itself. This composition usually is of higher degree than the initial polynomial. In order to find polynomials with good cryptographic or arithmetic properties, it is of interest to construct a large number of irreducible polynomials of the same degree from which good candidates can be selected. In [10] Kyureghyan and Kyuregyan introduce a recursive construction of irreducible polynomials which reverses the composition method, as the authors extract an irreducible polynomial f from the composition $f\left(X^2\right)$, which they were able to construct with the knowledge of its factorization. This construction yields a large number of polynomials of the same degree as the initial polynomial.

During our search for possible generalizations of the recursive construction from [10] (in this paper Construction KK), we noticed that there exist related constructions for the composition $f\left(X^k\right)$ by Albert and Daykin in [2] and [5], whose ideas we present jointly in Construction AD. The crucial difference between these two constructions is that Construction AD depends on the knowledge of the order of the initial polynomial, whereas Construction KK works without this knowledge due to Theorem 1 (iii). Furthermore, the computations in Construction KK are done in $\mathbb{F}_q$ whereas some computations in Construction AD are in a pure extension field of $\mathbb{F}_q$, which is not desirable for implementations. In this paper we first explain the connections between Construction KK and Construction AD. Then we develop a new construction based on ideas from these constructions, generalizing Construction KK. The methods used to develop the theoretical background for this construction are different from those in [10] and use ideas from [2] and [5].

In the following we present results from [10] and [5]. We use a unified notation und terminology so that the similarities of the approaches become visible. The following result [10, Corollary 3] details all the information needed to formulate Construction KK.

Theorem 1 [10]. *Let q be odd and $f \in \mathbb{F}_q[X]$, $f \neq X$, be a monic irreducible polynomial of degree n and order e. Let $\beta \in \mathbb{F}_{q^n}$ be a root of f. Then the following statements hold:*

(i) There exists a polynomial $C \in \mathbb{F}_q[X]$ such that $C\left(X^2\right) = f(X)\cdot(-1)^n f(-X)$. More precisely, $C(X) = (-1)^n \sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^u c_u c_{2j-u} X^j$, where $c_0, \ldots, c_n$ are the coefficients of f and $c_u = 0$ for $u > n$.

(ii) If C is irreducible, it is the minimal polynomial of β^2 over $\mathbb{F}_q$ and $\operatorname{ord}(C) = \frac{e}{\gcd(e,2)}$.

(iii) The polynomial C is irreducible if and only if there does not exist a polynomial $D \in \mathbb{F}_q[X]$ such that $f(X) = D\left(X^2\right)$.

Theorem 1 can be proved by elementary means and leads to the following construction, Construction KK, which combines the ideas from [10, Construction 1] and [10, Construction 2]. Note that Theorem 1 (iii) allows to determine whether the polynomial C is irreducible by a simple examination of the coefficients of the polynomial f.

Construction KK [10]. *Let q be odd and $f \in \mathbb{F}_q[X]$, $f \neq X$, a monic irreducible polynomial of degree n. Further, let $q^n - 1 = 2^u w$ with $w \in \mathbb{N}$ odd and $u \in \mathbb{N}$.*
Set $C_0 = f$. For $i \geq 0$, if there does not exist a polynomial $D \in \mathbb{F}_q[X]$ such that $C_i(X) = D\left(X^2\right)$ and additionally, if $i > u$ holds $C_i \neq C_j$ for all $0 \leq j \leq u$, then construct the monic irreducible polynomial $C_{i+1} \in \mathbb{F}_q[X]$ of degree n as follows:

$$C_{i+1}\left(X^2\right) := (-1)^n C_i(X)\, C_i(-X).$$

Otherwise stop.

In the proof of Theorem 1 the authors mention that if C is reducible, it is the square of another polynomial. We observe here that the polynomial C is in fact the characteristic polynomial of $\beta^2 \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This will follow from the next theorem. Thus, Construction KK is a computation of the characteristic polynomial of $\beta^{2^i} \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $\beta \in \mathbb{F}_{q^n}$ is a root of f. This leads us to Construction AD, which is the computation of the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ for $k \in \mathbb{N}$. The key results leading to Construction AD are the following. Note that Theorem 1 (i) and (ii) follow directly from these.

Theorem 2 [5]. *Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and $\beta \in \mathbb{F}_{q^n}$ a root of f. Let $k \in \mathbb{N}$ and $k' = \frac{k}{\gcd(q,k)}$. Then the characteristic polynomial $\chi_{\beta^k} \in \mathbb{F}_q[X]$ of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfies*

$$\chi_{\beta^k}\left(X^k\right) = (-1)^{n(k+1)} \prod_{j=1}^{k} f\left(\zeta_{k'}^j X\right).$$

Remark 1. The polynomials $f\left(\zeta_{k'}^j X\right)$ for $1 \leq j \leq k$ are not necessarily polynomials over $\mathbb{F}_q$ and need not be irreducible. Thus in general, Theorem 2 does not describe the factorization of $\chi_{\beta^k}\left(X^k\right)$ into irreducible factors over $\mathbb{F}_q$.

Theorem 3 [5]. *Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and order e and let $\beta \in \mathbb{F}_{q^n}$ a root of f. Then for $k \in \mathbb{N}$ the characteristic polynomial $\chi_{\beta^k} \in \mathbb{F}_q[X]$ of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfies $\chi_{\beta^k} = \left(m_{\beta^k}\right)^{\frac{n}{m}}$, where the minimal polynomial m_{β^k} of β^k over $\mathbb{F}_q$ has order $\frac{e}{\gcd(e,k)}$ and degree m, which is the least positive integer for which $\frac{e}{\gcd(e,k)}$ divides $q^m - 1$.*

Recall that a polynomial $f \in \mathbb{F}_q[X]$ of degree n is called primitive, if all roots of f have multiplicative order $q^n - 1$ or, equivalently, the smallest positive integer e, such that f divides $X^e - 1$, is $e = q^n - 1$. Theorems 2 and 3 already appear for primitive polynomials in [2]. Based on these two theorems Albert defines the so-called "cubing transformation" which is the computation of $m_{\beta^{3^i}} \in \mathbb{F}_q[X]$ for $i \geq 0$. As the reader will notice, this is very close to the construction from [10], where $k = 2$ is used instead of $k = 3$. However, note that in Theorem 3 the order of the initial polynomial $f = m_\beta$ is used to determine the exponent of the minimal polynomial of β^k in the characteristic polynomial of β^k over $\mathbb{F}_q$. This exponent is needed in order to extract m_{β^k} from χ_{β^k}. Construction KK does not depend on the knowledge of the order of f, see Theorem 1 (iii). It can even be used to gain information on the order of f, as we will later discuss for the general construction in $\mathbb{F}_q$. Note that Construction KK yields only polynomials of fixed degree while Albert also constructs polynomials of lower degree.

Daykin uses Theorems 2 and 3 to define a sequence of minimal polynomials m_{β^k}, in which every monic irreducible polynomial, whose order divides the order e of the initial polynomial f, appears exactly once. See [5, Theorem 4] for a proof of this fact. The sequence as defined by Daykin is described in the following construction.

Construction AD [5, Theorem 4]. *Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and order e. Further, let $\beta \in \mathbb{F}_{q^n}$ be a root of f. Set $k_1 = 1$ and add $f = m_\beta$ to the empty sequence.*
For $i \geq 2$ choose k_i to be the least positive integer such that $k_i \leq e$ and $k_i \not\equiv k_l q^j \mod e$ for all $1 \leq l < i$ and $0 \leq j < \deg\left(m_{\beta^{k_i}}\right)$. Then add $m_{\beta^{k_i}}$ to the sequence.

In Theorem 2 the group of the k'-th roots of unity $U_{k'}$ is a subgroup of $\mathbb{F}_q^*$ if and only if $k' \mid q-1$. Therefore, the computations for Construction AD are carried out in a pure extension field of $\mathbb{F}_q$ if $k_i \nmid q-1$, which is not attractive for implementations since computations in extension fields are complicated and expensive. Furthermore, note that in order to compute the sequence defined by Construction AD, one has to compute the polynomial $\chi_{\beta^k}\left(X^k\right)$ with the formula from Theorem 2 and then extract the irreducible factor of the polynomial χ_{β^k} over $\mathbb{F}_q$ in order to obtain the minimal polynomial m_{β^k}, which is not a simple computation. With our new construction we will be able to directly compute the polynomial $m_{\beta^k}\left(X^k\right)$ from which m_{β^k} can easily be extracted, see Corollary 2.

2 Theoretical background for the new construction

The aim of this paper is to suggest a construction for $k \geq 2$, which can be computed in $\mathbb{F}_q$ and does not depend on the knowledge of the order of the initial polynomial f. Our construction works not only for integers k dividing $q-1$ but also for some k such that U_k is not a subgroup of $\mathbb{F}_q$. Recall that in Construction AD the order of f is used to determine the degree of the minimal polynomial m_{β^k} or, equivalently, the power to which the minimal polynomial is taken in the characteristic polynomial. This information allows to extract the minimal polynomial from the characteristic polynomial. In this section we describe how to determine this power without the knowledge of the order of f.

Remark 2. If $\gcd(q,k) > 1$, the coefficients of m_{β^k} can easily be derived from the coefficients of $m_{\beta^{k'}}$ where $k' = \frac{k}{\gcd(q,k)}$, as Albert mentions in [2]. Indeed, suppose that $\deg(m_{\beta^k}) = m$. Then

$$m_{\beta^k}\left(X^k\right) = \prod_{i=0}^{m-1}\left(X^k - \beta^{k\cdot q^i}\right) = \left(\prod_{i=0}^{m-1}\left(X^{k'} - \beta^{k'\cdot q^i}\right)\right)^{\gcd(q,k)}.$$

Theorem 3 implies that $\operatorname{ord}(m_{\beta^k}) = \frac{e}{\gcd(e,k)} = \frac{e}{\gcd(e,k')} = \operatorname{ord}(m_{\beta^{k'}})$ and therefore $\deg(m_{\beta^{k'}}) = \deg(m_{\beta^k}) = m$. Thus, $m_{\beta^k}\left(X^k\right) = \left(m_{\beta^{k'}}\left(X^{k'}\right)\right)^{\gcd(q,k)}$ or, equivalently, $m_{\beta^k}\left(X^{\gcd(q,k)}\right) = \left(m_{\beta^{k'}}(X)\right)^{\gcd(q,k)} = \sum_{i=0}^{m} a_i^{\gcd(q,k)} X^{i\cdot\gcd(q,k)}$ where $m_{\beta^{k'}} = \sum_{i=0}^{m} a_i X^i$. Consequently, $m_{\beta^k} = \sum_{i=0}^{m} a_i^{\gcd(q,k)} X^i$.

Using Remark 2, we can restrict our discussion to the case that $\gcd(q,k) = 1$. Nontheless, note that all results hold also for integers k such that $\gcd(q,k) > 1$.

The main advantage of considering only the case $\gcd(q,k) = 1$ is that there always exist exactly k distinct k-th roots of unity in an extension field $\mathbb{E} \geq \mathbb{F}_q$ of $\mathbb{F}_q$.

Theorem 4. *Let $k \in \mathbb{N}$ such that $\gcd(q,k) = 1$. Further, let $\beta \in \mathbb{F}_{q^n}$ be a proper element of $\mathbb{F}_{q^n}$ and χ_{β^k} be the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $\chi_{\beta^k} = \left(m_{\beta^k}\right)^t$ for a positive integer $t \in \mathbb{N}$ if and only if every root of the polynomial $\chi_{\beta^k}\left(X^k\right)$ appears with multiplicity t.*

Proof. Since χ_{β^k} is the characteristic polynomial of β^k over $\mathbb{F}_q$, there exists a positive integer $t \in \mathbb{N}$ such that $\chi_{\beta^k}\left(X^k\right) = \left(m_{\beta^k}\left(X^k\right)\right)^t$. Furthermore, $m_{\beta^k}\left(X^k\right) = \prod_{i=0}^{\frac{n}{t}-1}\left(X^k - \beta^{k\cdot q^i}\right)$ and for every i the polynomial $X^k - \left(\beta^{q^i}\right)^k$ has k distinct roots of the form $\zeta_k^j\beta^{q^i}$ in an extension field of $\mathbb{F}_q$, where $1 \leq j \leq k$. Thus, $\chi_{\beta^k}\left(X^k\right) = \prod_{i=0}^{\frac{n}{t}-1}\prod_{j=1}^{k}\left(X - \zeta_k^j\beta^{q^i}\right)^t$. Note that the roots $\zeta_k^j\beta^{q^i}$ of $\chi_{\beta^k}\left(X^k\right)$ are distinct. Indeed, if for $1 \leq j_1, j_2 \leq k$ and $0 \leq i_1, i_2 \leq \frac{n}{t}-1$ the two roots $\zeta_k^{j_1}\beta^{q^{i_1}}$ and $\zeta_k^{j_2}\beta^{q^{i_2}}$ were equal, we would have $\left(\beta^k\right)^{q^{i_1}} = \left(\zeta_k^{j_1}\beta^{q^{i_1}}\right)^k = \left(\zeta_k^{j_2}\beta^{q^{i_2}}\right)^k = \left(\beta^k\right)^{q^{i_2}}$ and since the elements $\left(\beta^k\right)^{q^i}$ of $\mathbb{F}_{q^{\frac{n}{t}}}$ are distinct, we have $i_1 = i_2$ and consequently also $j_1 = j_2$. □

The roots of the polynomial $\chi_{\beta^k}\left(X^k\right)$ lie in an extension field of $\mathbb{F}_q$. Since we later want to work in $\mathbb{F}_q$, we state the following immediate consequence of Theorem 4, which follows directly from the fact that the roots of every irreducible factor are distinct.

Corollary 1. *Let $k \in \mathbb{N}$ such that $\gcd(q,k) = 1$. Further, let $\beta \in \mathbb{F}_{q^n}$ be a proper element of $\mathbb{F}_{q^n}$ and χ_{β^k} be the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*
Then $\chi_{\beta^k} = \left(m_{\beta^k}\right)^t$ for a positive integer t if and only if every irreducible factor of $\chi_{\beta^k}\left(X^k\right)$ over $\mathbb{F}_q$ appears with multiplicity t.

Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and $\beta \in \mathbb{F}_{q^n}$ be a root of f. Recall that with Theorem 2, we have

$$\chi_{\beta^k}\left(X^k\right) = (-1)^{(k+1)n}\prod_{j=1}^{k} f\left(\zeta_k^j X\right) = \prod_{j=1}^{k}\zeta_k^{-jn} f\left(\zeta_k^j X\right). \tag{1}$$

If $k \mid q-1$, then U_k lies in $\mathbb{F}_q$ and for $1 \leq j \leq k$ the polynomials $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ are monic polynomials of degree n over $\mathbb{F}_q$. The element $\zeta_k^{-j}\beta$ is a root of $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ and since β is a proper element of $\mathbb{F}_{q^n}$, the element $\zeta_k^{-j}\beta$ also is a proper element of $\mathbb{F}_{q^n}$. Consequently, the polynomial $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ is the minimal polynomial of $\zeta_k^{-j}\beta$ over $\mathbb{F}_q$ and (1) yields the factorization of $\chi_{\beta^k}\left(X^k\right)$

into monic irreducible factors over $\mathbb{F}_q$. With Corollary 1 we obtain that the exponent of the minimal polynomial of β^k over $\mathbb{F}_q$ in the characteristic polynomial χ_{β^k} is equal to the multiplicity of every polynomial $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ in the factorization (1). Thus, in the case that $k \mid q-1$, we need to determine under which conditions the polynomials of the form $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ are equal. For this we need the following fact.

Fact 1. *Let $k \in \mathbb{N}$ such that $\gcd(k,q)=1$ and $f \in \mathbb{F}_q[X]$. Then there exists $g \in \mathbb{F}_q[X]$ such that $f(X)=g(X^k)$ if and only if $f(X)=f(\zeta_k X)$.*

Proof. If $f(X)=g(X^k)$, then $f(\zeta_k X)=g\left(\zeta_k^k X^k\right)=g\left(X^k\right)=f(X)$. Vice versa, suppose that $f(X)=f(\zeta_k X)$. Then if $f(X)=\sum_{i=0}^n a_i X^i$, we have $f(\zeta_k X)=\sum_{i=0}^n a_i \zeta_k^i X^i$. Thus, $\zeta_k^i=1$ for all $0 \le i \le n$ such that $a_i \neq 0$. Consequently, $k=\operatorname{ord}(\zeta_k) \mid i$ for all $0 \le i \le n$ such that $a_i \neq 0$. □

The following theorem states that it can be seen directly from the non-zero coefficients of the polynomial f, which polynomials of the form $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ are equal.

Theorem 5. *Let $k \in \mathbb{N}$ such that $\gcd(k,q)=1$ and let $f \in \mathbb{F}_q[X]$ be a polynomial of degree n such that $f(0) \neq 0$. Then for $0 \le j, j' \le k-1$ the two polynomials $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ and $\zeta_k^{-j'n} f\left(\zeta_k^{j'} X\right)$ are equal if and only if $j \equiv j' \mod \frac{k}{t}$ where $t=\max\{m \mid \gcd(n,k) : f(X)=g(X^m)$ for a polynomial $g \in \mathbb{F}_q[X]\}$.*

Proof. "⇐": Note that since $t=\gcd(k,t)$, the element $\zeta_k^{\frac{k}{t}}=\zeta_t$ generates the subgroup U_t of the t-th roots of unity of $\mathbb{F}_q^*$. If $j \equiv j' \mod \frac{k}{t}$, then $j-j'=v \cdot \frac{k}{t}$ for an integer v and we have

$$\begin{aligned}\zeta_k^{-jn} f\left(\zeta_k^j X\right) &= \zeta_k^{-(j-j')n} \zeta_k^{-j'n} f\left(\zeta_k^{(j-j')} \zeta_k^{j'} X\right) &&= \zeta_k^{-\frac{k}{t} \cdot v \cdot n} \zeta_k^{-j'n} f\left(\zeta_k^{\frac{k}{t} \cdot v} \zeta_k^{j'} X\right) \\ &= \zeta_k^{-k \cdot v \cdot \frac{n}{t}} \zeta_k^{-j'n} f\left(\zeta_t^v \zeta_k^{j'} X\right) &&= \zeta_k^{-j'n} f\left(\zeta_t^v \zeta_k^{j'} X\right).\end{aligned}$$

From the definition of t and Fact 1 follows that $f(X)=f(\zeta_t X)$ and therefore also $f(X)=f(\zeta_t^v X)$. Thus, $\zeta_k^{-j'n} f\left(\zeta_t^v \zeta_k^{j'} X\right)=\zeta_k^{-j'n} f\left(\zeta_k^{j'} X\right)$.

"⇒": Suppose that $\zeta_k^{-jn} f\left(\zeta_k^j X\right)=\zeta_k^{-j'n} f\left(\zeta_k^{j'} X\right)$. Then also

$$\begin{aligned}\zeta_k{}^{-(j-j')n} f\left(\zeta_k^{j-j'} X\right) &= \zeta_k^{j'n} \cdot \zeta_k^{-jn} f\left(\zeta_k^j \left(\zeta_k^{-j'} X\right)\right) \\ &= \zeta_k^{j'n} \cdot \zeta_k^{-j'n} f\left(\zeta_k^{j'} \left(\zeta_k^{-j'} X\right)\right) = f(X)\end{aligned} \tag{2}$$

Let $f=\sum_{i=0}^n a_i X^i \in \mathbb{F}_q[X]$. Then we have $\zeta_k^{-(j-j')n} f\left(\zeta_k^{j-j'} X\right)=$ $\sum_{i=0}^n a_i \zeta_k^{-(j-j')(n-i)} X^i$. For this polynomial to be equal to $f(X)$, we need $k \mid (j-j')(n-i)$ for all $a_i \neq 0$. Note that $a_0=f(0) \neq 0$. Consequently, $k \mid (j-j') \cdot n$.

Let $d := \gcd(n,k)$, then $\frac{k}{d} \mid (j-j')$ and there exists $v \in \mathbb{N}$ such that $j-j' = v \cdot \frac{k}{d}$. Furthermore, the element $\zeta_k^{\frac{k}{d}} = \zeta_d$ generates the subgroup U_d of the d-th roots of unity of $\mathbb{F}_q$ and we obtain

$$\zeta_k^{-(j-j')n} f\left(\zeta_k^{(j-j')} X\right) = \zeta_k^{-v \cdot \frac{k}{d} \cdot d \cdot \frac{n}{d}} f\left(\zeta_k^{v \cdot \frac{k}{d}} X\right) = f\left(\zeta_d^v X\right). \tag{3}$$

If $l = \frac{d}{\gcd(d,v)}$, the element $\zeta_d^v = \zeta_l$ generates the set U_l of the l-th roots of unity over $\mathbb{F}_q$. Equations (2) and (3) yield that $f(X) = f(\zeta_l X)$. Note that $\gcd(d,q) = 1$ and with Fact 1 we obtain that $M := \{m \mid d : f(X) = g(X^m), g \in \mathbb{F}_q[X]\}$ is equal to the set $\{m \mid d : f(X) = f(\zeta_m X)\}$ and consequently, $l \in M$. Let $t := \max M$. We will prove that M is in fact the set of all divisors of t. Note that if $f(X) = f\left(\zeta_t X\right)$, also $f(X) = f\left(\zeta_t^i X\right)$ for all $1 \leq i \leq t$ and any divisor m of t satisfies that $\zeta_m = \zeta_t^{\frac{t}{m}}$. Thus, all divisors of t are elements of M. Suppose that there exists an element $m \in M$ such that m does not divide t. Then for all $0 \leq i \leq n$ such that $a_i \neq 0$, we have $m \mid i$ and $t \mid i$. Consequently, $\operatorname{lcm}(m,t) = t \cdot \frac{m}{\gcd(m.t)} \mid i$ and since both m and t divide d, we obtain $\operatorname{lcm}(t,m) \in M$. But $\operatorname{lcm}(t,m) > t$, because $m \nmid t$. This is a contradiction to the choice of t and M is in fact the set of all divisors of t. Consequently, the fact $l \in M$ is equivalent to $l \mid t$. Recall that $l = \frac{d}{\gcd(d,v)}$ and therefore $\frac{d}{\gcd(d,v)} \mid t$ which is equivalent to $\frac{d}{t} \mid \gcd(d,v)$ and this again is equivalent to $\frac{d}{t} \mid v$. Thus, there exists an integer w such that $v = \frac{d}{t} \cdot w$. Recall that $v = \frac{j-j'}{\frac{k}{d}}$ and we have $j - j' = \frac{k}{t} \cdot w$. Consequently, $j \equiv j' \mod \frac{k}{t}$. □

If $k \mid q-1$, then obviously $\gcd(k,q) = 1$ and we can use Theorem 5 to rewrite equation (1) for a monic irreducible polynomial $f \in \mathbb{F}_q[X]$, $f \neq X$, of degree n with $\beta \in \mathbb{F}_{q^n}$ a root of f and we obtain that the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfies:

$$\chi_{\beta^k}\left(X^k\right) = \prod_{j=1}^{k} \zeta_k^{-jn} f\left(\zeta_k^j X\right) = \left(\prod_{j=1}^{\frac{k}{t}} \zeta_k^{-jn} f\left(\zeta_{k^j} X\right)\right)^t,$$

where $t = \max\{m \mid \gcd(n,k) : f(X) = g(X^m) \text{ for a polynomial } g \in \mathbb{F}_q[X]\}$ and the polynomials $\zeta_k^{-jn} f\left(\zeta_k^j X\right)$ for $1 \leq j \leq \frac{k}{t}$ are distinct. These observations and Corollary 1 yield the following method to compute the polynomial $m_{\beta^k}\left(X^k\right)$.

Corollary 2. *Let $k \in \mathbb{N}$ such that $k \mid q-1$ and let $f \in \mathbb{F}_q[X]$, $f \neq X$, be a monic irreducible polynomial of degree n. Further, let $\beta \in \mathbb{F}_{q^n}$ be a root of f and $m_{\beta^k} \in \mathbb{F}_q[X]$ be the minimal polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then*

$$m_{\beta^k}\left(X^k\right) = \prod_{j=1}^{\frac{k}{t}} \zeta_k^{-jn} f\left(\zeta_k^j X\right),$$

where $t = \max\{m \mid \gcd(n,k) : f(X) = g(X^m)$ for a polynomial $g \in \mathbb{F}_q[X]\}$.

Recall that Construction AD constructs the polynomial $\chi_{\beta^k}\left(X^k\right)$ with the formula from Theorem 2 and then extracts the irreducible factor of the polynomial χ_{β^k} over $\mathbb{F}_q$ in order to obtain the minimal polynomial m_{β^k} of β^k. Using Corollary 2, in our construction we directly compute the polynomial $m_{\beta^k}\left(X^k\right)$ from which the minimal polynomial m_{β^k} can then easily be extracted.

Remark 3. Note that if $k \mid q-1$ and k is prime, then $t > 1$ if and only if $t = k$. Thus, if $f(X) = g\left(X^k\right)$ for a polynomial $g \in \mathbb{F}_q[X]$, then the minimal polynomial of β^k over $\mathbb{F}_q$ satisfies $m_{\beta^k}(X) = g(X)$. Otherwise, we obtain m_{β^k} by extracting it from the composition $m_{\beta^k}\left(X^k\right) = \prod_{j=1}^{k} \zeta_k^{-jn} f\left(\zeta_k^j X\right) = (-1)^{n(k+1)} \prod_{j=1}^{k} f\left(\zeta_k^j X\right)$.

3 The new recursive construction of m_{β^k} from m_β

Observe that for $k, k_1, k_2 \in \mathbb{N}$ such that $k = k_1 \cdot k_2$ and a proper element β of $\mathbb{F}_{q^n}$, we have $\beta^k = \left(\beta^{k_1}\right)^{k_2}$ and consequently $m_{\beta^k}\left(X^{k_2}\right) = m_{\left(\beta^{k_1}\right)^{k_2}}\left(X^{k_2}\right)$. Thus, instead of using the direct computation of m_{β^k}, we can apply the construction recursively. Meaning that we first compute the minimal polynomial of β^{k_1} and then with this polynomial compute $m_{\left(\beta^{k_1}\right)^{k_2}}\left(X^{k_2}\right)$ from which $m_{\beta^k} = m_{\left(\beta^{k_1}\right)^{k_2}}$ can easily be extracted. Using the unique prime factorization of an integer k, we can apply Remark 3 to define a construction for all $k \in \mathbb{N}$ whose prime factors divide $q-1$.

Construction 1. *Let $k \in \mathbb{N}$ such that $k = k_1 \cdots k_m$ where $k_1, \ldots, k_m$ are prime factors of $q-1$ (which are not necessarily distinct). Further, let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n. Set $f_0 := f$. For $1 \le i \le m$ compute the monic irreducible polynomial f_i in the following way:*
If there exists a polynomial $g \in \mathbb{F}_q[X]$ such that $f_{i-1}(X) = g\left(X^{k_i}\right)$, then $f_i = g$. Otherwise, compute

$$(-1)^{\deg(f_{i-1})\cdot(k_i+1)} \prod_{j=1}^{k_i} f_{i-1}\left(\zeta_{k_i}^j X\right) = f_i\left(X^{k_i}\right)$$

and extract f_i from the composition. Then f_m is the minimal polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $\beta \in \mathbb{F}_{q^n}$ is a root of f.

The main differences between Construction 1 and Construction AD are that all computations of Construction 1 are carried out in $\mathbb{F}_q$ and the construction relies solely on the examination of the non-zero coefficients of the polynomials f_i and not on the order of the initial polynomial f. Furthermore, while in Construction AD the minimal polynomial m_{β^k} needs to be extracted from the characteristic polynomial, it is computed directly in Construction 1.

Remark 4. The polynomials obtained with Construction 1 are of the same degree n as the initial polynomial f, if we select integers k such that $\gcd(n,k)=1$ or such that the order $\frac{e}{\gcd(e,k)}$ of the minimal polynomial of β^k does not divide $q^{\frac{n}{t}}-1$ for any divisor t of n, whose prime factors divide $\gcd(n,k)$. Furthermore, if there exists a polynomial $g \in \mathbb{F}_q[X]$ such that $f\left(X^l\right)$ for a prime divisor l of k, then the minimal polynomial of β^k will be of lower degree. In this case the polynomial $f(X+a)$ for any element $a \in \mathbb{F}_q \backslash \{0\}$ will not be a composition with X^l and could be used instead of f. This fact was proved in [10] for $l=2$.

The minimal polynomials of β^k and $\beta^{k'}$ for different integers k and k' are equal if β^k is an $\mathbb{F}_q$-conjugate of $\beta^{k'}$ or the element $\beta^{k'}$ itself. Then Construction 1 yields the same polynomial for k as for k'. This happens if and only if there exists an integer $0 \leq i \leq \deg\left(m_{\beta^{k'}}\right)-1$ such that $k \equiv k' \cdot q^i \mod e$, where e is the order of the minimal polynomial m_β of β over $\mathbb{F}_q$. In [2] Albert notices this and calls his cubing transformation "periodic" if it yields the initial polynomial repeatedly. This observation allows us to gain information on the prime factorization of the order of the minimal polynomial m_β with a second construction, Construction 2, which is an application of Construction 1. More precisely, we apply Construction 1 repeatedly for a fixed prime factor k of $q-1$ to compute the minimal polynomials of β^{k^l} for $l \in \mathbb{N}$ until two of these polynomials are equal. Then the number of steps before this polynomial appears for the first time will be the k-adic valuation $\nu_k(e)$ of $e=\operatorname{ord}(m_\beta)$. Let us examine why this is the case.

Let $v=\nu_k(e)$, that is $e=k^v \cdot r$ such that $\gcd(k,r)=1$. Theorem 3 yields that the minimal polynomial of β^{k^l} over $\mathbb{F}_q$ has order $\frac{e}{k^l}>r$ for all $1 \leq l \leq v-1$ and for all $l \geq v$ the order is equal to r. Thus, if we identify $m_{\beta^{k^v}}$ in the sequence of constructed polynomials, the number of steps needed to obtain this polynomial is $v=\nu_k(e)$. We need to examine $\mathbb{Z}_r^*$, the multiplicative group modulo r, to see that $m_{\beta^{k^v}}$ is the first polynomial which appears twice in the sequence and can therefore easily be identified. The subgroup $\langle k \rangle$ of $\mathbb{Z}_r^*$ generated by k has order $\operatorname{ord}_r(k)$, which is the multiplicative order of k modulo r. This implies that $\beta^{k^{v+\operatorname{ord}_r(k)}}=\beta^{k^v}$ and obviously the minimal polynomials of β^{k^v} and $\beta^{k^{v+\operatorname{ord}_r(k)}}$ are equal. However, it is possible that there exists a positive integer s smaller than $\operatorname{ord}_r(k)$ such that $\beta^{k^{v+s}}$ is an $\mathbb{F}_q$-conjugate of β^{k^v} and the minimal polynomial $m_{\beta^{k^{v+s}}}$ also is equal to $m_{\beta^{k^v}}$. To account for this, we choose $s \in \mathbb{N}$ to be the smallest positive integer such that for an integer $0 \leq i \leq \deg\left(m_{\beta^{k^v}}\right)-1$ holds the following:

$$\langle k \rangle \cap \langle q \rangle = \langle k^s \rangle = \langle q^i \rangle \leq \mathbb{Z}_r^*.$$

Note that since $\langle k^{\operatorname{ord}_r(k)} \rangle = \langle q^0 \rangle$ such an integer s exists and satisfies $s \leq \operatorname{ord}_r(k)$. Then $\beta^{k^{v+s}}$ and β^{k^v} are conjugates over $\mathbb{F}_q$ and their minimal polynomials are equal. Moreover, the minimal polynomials of $\beta^{k^{v+l}}$ for $0 \leq l \leq s-1$ are distinct and $m_{\beta^{k^v}}$ is in fact the first polynomial to appear twice in the sequence.

Remark 5. In order to find s, it is not necessary to check for every $0 \leq s \leq \operatorname{ord}_r(k)$ if the equation $k^s \equiv q^i \mod r$ holds for an integer $0 \leq i \leq \deg\left(m_{\beta^{k^v}}\right) =:$

m. We can simplify the search by using the fact that the order $\mathrm{ord}_r\left(k^s\right) = \mathrm{ord}_r\left(q^i\right) =: d$ is a divisor of m and since $|\langle k\rangle| = \mathrm{ord}_r(k)$, we have $s = \frac{\mathrm{ord}_r(k)}{d}$. Thus, we can define s as the integer $\frac{\mathrm{ord}_r(k)}{d}$, where d is the largest divisor of m such that there exists an integer $0 \leq i \leq m-1$ which satisfies the two conditions $\mathrm{ord}_r\left(q^i\right) = d$ and $k^{\frac{\mathrm{ord}_r(k)}{d}} \equiv q^i \mod r$.

Remark 6. In the original version of [10], the number of distinct polynomials produced by [10, Construction 1] is given as $\mathrm{ord}_r(2)$ where $\mathrm{ord}(f) = 2^v r$ with $v \geq 0$ and $r \geq 1$ odd. As we can see from Remark 5, this number is false, since the authors did not take into consideration that the construction could also yield the minimal polynomials of $\mathbb{F}_q$-conjugates over $\mathbb{F}_q$. Similarly, in [10, Remark 1] the information about the order of the initial polynomial $C_0(X)$ obtained by the construction should be changed to: $2^l t$ where t is an odd divisor of $q^n - 1$ and $k - l = \frac{\mathrm{ord}_t(2)}{d}$ for a divisor d of n.

Our observations suggest the following method to determine the k-adic valuation $\nu_k(\mathrm{ord}(f))$ of the order of an irreducible polynomial $f \in \mathbb{F}_q[X]$ for a prime factor k of $q-1$.

Construction 2. *Let k be a prime factor of $q-1$ and $f \in \mathbb{F}_q[X]$ a monic irreducible polynomial of degree n. Further let $w = \nu_k\left(q^n - 1\right)$ be the k-adic valuation of $q^n - 1$. Set $f_0 := f$. For $i \geq 1$ compute the monic irreducible polynomial f_i in the following way:*
If there exists a polynomial $g \in \mathbb{F}_q[X]$ such that $f_{i-1}(X) = g\left(X^k\right)$, then $f_i = g$. Otherwise, compute

$$(-1)^{\deg(f_{i-1})\cdot(k+1)} \prod_{j=1}^{k} f_{i-1}\left(\zeta_k^j X\right) = f_i\left(X^k\right)$$

and extract f_i from the composition. If $f_i = f_l$ for an integer $0 \leq l \leq w$ such that $l < i$, then stop. Then $\mathrm{ord}(f) = k^l \cdot r$ such that $\gcd(k, r) = 1$ and $i - l = \frac{\mathrm{ord}_r(k)}{d}$ for a divisor d of $\deg(f_i)$ such that $\mathrm{ord}_r\left(q^j\right) = d$ for an integer $0 \leq j \leq \deg(f_i) - 1$ and $k^{i-l} \equiv q^j \mod r$.

Note that if $p_1, \ldots, p_m$ are the distinct prime factors of $q-1$, and $\mathrm{ord}(f) = e = p_1^{v_1} \cdots p_m^{v_m} \cdot r$ such that $\gcd(q, r) = 1$ for integers $v_i \geq 0$, $1 \leq i \leq m$. Then Construction 2 allows us to determine the p_i-adic valuations $v_1, \ldots, v_m$ of the order of f and additionally gives information on the factor r of $\mathrm{ord}(f)$ which is coprime with $q-1$.

References

1. Abrahamyan, S., Alizadeh, M., Kyureghyan, M.: Recursive constructions of irreducible polynomials over finite fields. Finite Fields and Their Applications **18**(4), 738–745 (2012)
2. Albert, A.A.: Fundamental Concepts of Higher Algebra. University of Chicago Press, Chicago (1956)
3. Cohen, S.: On irreducible polynomials of certain types in finite fields. Mathematical Proceedings of the Cambridge Philosophical Society **66**(2), 335–344 (1969)
4. Cohen, S.: The explicit construction of irreducible polynomials over finite fields. Designs, Codes and Cryptography **2**(2), 169–174 (1992)
5. Daykin, D.E.: Generation of irreducible polynomials over a finite field. The American Mathematical Monthly **72**(6), 646–648 (1965)
6. Kyuregyan, M.: Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics. Finite Fields and Their Applications **9**(1), 39–58 (2003)
7. Kyuregyan, M.: Iterated constructions of irreducible polynomials over finite fields with linearly independent roots. Finite fields and Their Applications **10**(3), 323–341 (2004)
8. Kyuregyan, M.: Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics. Finite Fields and Their Applications **12**(3), 357–378 (2006)
9. Kyureghyan, G., Kyuregyan, M.: Irreducible compositions of polynomials over finite fields. arXiv preprint arXiv:1008.1863 (2010)
10. Kyureghyan, G., Kyuregyan, M.: A recurrent construction of irreducible polynomials of fixed degree over finite fields. Applicable Algebra in Engineering, Communication and Computing (2020)
11. McNay, G.: Topics in finite fields. Ph.D. Thesis at the University of Glasgow (1995)
12. Meyn, H.: Explicit N-polynomials of 2-power degree over finite fields. Designs, Codes and Cryptography **6**(2), 107–116 (1995)
13. Panario, D., Reis, L., Wang, Q.: Construction of irreducible polynomials through rational transformations. Journal of Pure and Applied Algebra **224**(5), 106241 (2020)
14. Ugolini, S.: Sequences of binary irreducible polynomials. Discrete Mathematics **313** (22), 2656–2662 (2013).