Designs, Codes and Cryptography (2024) 92:695–708
https://doi.org/10.1007/s10623-023-01271-z

Constructing irreducible polynomials recursively with a reverse composition method

Anna-Maurin Graner[1] · Gohar M. Kyureghyan[1]

Received: 15 August 2022 / Revised: 27 February 2023 / Accepted: 28 June 2023 /
Published online: 4 August 2023

Abstract

We suggest a construction of the minimal polynomial m_{β^k} of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ from the minimal polynomial $f = m_\beta$ for all positive integers k whose prime factors divide $q-1$. The computations of our construction are carried out in $\mathbb{F}_q$. The key observation leading to our construction is that for $k \mid q-1$ holds

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

where $t = \max\{m \in \mathbb{N} : m \mid \gcd(n,k), f(X) = g(X^m), g \in \mathbb{F}_q[X]\}$ and ζ_k is a primitive k-th root of unity in $\mathbb{F}_q$. The construction allows to construct a large number of irreducible polynomials over $\mathbb{F}_q$ of the same degree. Since different applications require different properties, this large number allows the selection of the candidates with the desired properties.

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

Mathematics Subject Classification 11T06

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

This is one of several papers published in *Designs, Codes and Cryptography* comprising the “Special Issue: Coding and Cryptography 2022”.

✉ Anna-Maurin Graner
anna-maurin.graner@uni-rostock.de

Gohar M. Kyureghyan
gohar.kyureghyan@uni-rostock.de

[1] Institute of Mathematics, University of Rostock, Rostock, Germany

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 $\beta \in \mathbb{F}_{q^m}$. For an irreducible polynomial $f \in \mathbb{F}_q[X]$ the smallest positive integer e such that $f \mid X^e - 1$ or, equivalently, the multiplicative order of all of its roots, is called the *order* of f and is denoted by $e = \mathrm{ord}(f)$. If f has degree n and the order of f equals $q^n - 1$, we call f a *primitive* polynomial. 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 $|U_k| = k$ and throughout this paper we will use the notation ζ_k for a generating element of U_k. For a prime p and an integer m we denote by $\nu_p(m)$ the *p-adic valuation of m*, that is, $\nu_p(m) = v$ if $m = p^v \cdot r$ with $\gcd(p, r) = 1$.

The composition method is widely used to construct irreducible polynomials over finite fields, see for example [3, 8, 9, 11–14, 16]. Originally based on a theorem by Cohen [2], with this method one composes an irreducible polynomial with polynomials or rational functions such that the resulting composition is irreducible itself. The 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. Here, an irreducible polynomial f is extracted from the composition $f(X^2)$, which is obtained from 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 the composition $f(X^k)$ was studied by Albert [1] and Daykin [4]. We will use the ideas from [1] and [4] to generalize the results and extend the construction from [10].

Next we present results from [4] and [10]. We use a unified notation and 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 $C(X^2) = f(X) \cdot (-1)^n f(-X)$. More precisely, $C(X) = (-1)^n \sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^u c_u c_{2j-u} X^j$, where $c_0, \dots, c_n$ 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 $\mathrm{ord}(C) = \frac{e}{\gcd(e,2)}$.

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

Theorem 1 can be proved by elementary means and leads to the following construction, Construction KK, which is the key step of constructions [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 such that there does not exist a polynomial $D \in \mathbb{F}_q[X]$ with $f(X) = D(X^2)$. To construct the monic irreducible polynomial $C \in \mathbb{F}_q[X]$ of degree n over $\mathbb{F}_q$, do the following steps:*

Step 1. Compute the product $(-1)^n \cdot f(X) \cdot f(-X) = C(X^2)$.

Step 2. Extract C from the composition $C(X^2)$.

A similar transformation with X^3 has been studied in [1] for primitive polynomials over $\mathbb{F}_q$. The results from [1] have been generalized in [4]. The next theorem shows that the polynomial C from Theorem 1 and Construction KK is in fact the characteristic polynomial of $\beta^2 \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This observation will allow us to develop the generalizations of the results in [10].

Theorem 2 ([4]) *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*

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

Remark 1 The polynomials $f(\zeta_{k'}^j X)$ 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 $\chi_{\beta^k}(X^k)$ into irreducible factors over $\mathbb{F}_q$.

Theorem 3 ([4]) *Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and order e and let $\beta \in \mathbb{F}_{q^n}$ be 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 $q^m - 1$.*

Note that Theorem 1 (i) and (ii) follow directly from Theorems 2 and 3 by selecting $k = 2$. More precisely, Theorem 2 yields that the polynomial C in Theorem 1 not only exists, but is in fact the characteristic polynomial χ_{β^2}. If χ_{β^2} is irreducible, then it is the minimal polynomial m_{β^2} and it has order $\frac{e}{\gcd(e,2)}$.

Theorems 2 and 3 suggest the following construction of m_{β^k} from m_β.

Construction AD *Let $f \in \mathbb{F}_q[X]$ be a monic irreducible polynomial of degree n and order e and let $\beta \in \mathbb{F}_{q^n}$ be a root of f. Given a positive integer $k \leq e$ define $k' = \frac{k}{\gcd(q,k)}$. To construct the minimal polynomial m_{β^k} of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$, do the following steps:*

Step 1. Compute the product

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

Step 2. Extract χ_{β^k} from the composition $\chi_{\beta^k}(X^k)$.
Step 3. Determine m, the least positive integer for which $\frac{e}{\gcd(e,k)}$ divides $q^m - 1$.
Step 4. Find the factor m_{β^k} in the product $\chi_{\beta^k} = \left(m_{\beta^k}\right)^{\frac{n}{m}}$.

Remark 2 (a) Note that $\zeta_{k'}$ is an element of $\mathbb{F}_q$ if and only if $k' \mid q - 1$. Therefore, the computations of Step 1 in Construction AD are carried out in a pure extension field of $\mathbb{F}_q$ if $k' \nmid q - 1$.

(b) Construction AD can also be applied without the knowledge of the order e of the polynomial f. In that case we replace Steps 3 and 4 with factorizing χ_{β^k}, which will be an unknown power of the minimal polynomial m_{β^k} of β^k over $\mathbb{F}_q$.

(c) On the other hand, if the order e of f is known, it is possible to avoid the computation intensive Step 4 by selecting k such that $n = m$. Then the characteristic and the minimal polynomial of β^k over $\mathbb{F}_q$ are equal.
(d) Construction KK does not depend on the knowledge of the order of the intial polynomial f. If used iteratively, it can even give information on the order as we will discuss later.

In this paper we suggest a construction of the minimal polynomial m_{β^k} of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ from the minimal polynomial $f = m_\beta$ for all positive integers k whose prime factors divide $q-1$ which avoids the computation intensive Step 4 of Construction AD. Additionally, in this construction computations are carried out in $\mathbb{F}_q$ and it does not depend on the knowledge of the order of the initial polynomial f. While Construction KK only works for finite fields of odd size, our construction can also be used in finite fields of characteristic 2 which is attractive for applications in computer science. The key observation leading to our construction is that for $k \mid q-1$ holds

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

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

2 Theoretical background for the new construction

In Theorem 3 the order of the monic irreducible polynomial $f = m_\beta$ is used to determine the degree of the minimal polynomial m_{β^k} or, equivalently, the power to which the minimal polynomial of β^k is taken in the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this section we describe how to determine this exponent without the knowledge of the order of f.

Remark 3 If $\gcd(q,k) > 1$, the coefficients of m_{β^k} can easily be derived from the coefficients of $m_{\beta^{k'}}$ where $k' = \frac{k}{\gcd(q,k)}$. Indeed, 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 $\deg(m_{\beta^{k'}}) = \deg(m_{\beta^k}) = m$. Suppose that $m_{\beta^{k'}} = \sum_{i=0}^m a_i X^i$ and set $g = \sum_{i=0}^m a_i^{\gcd(q,k)} X^i \in \mathbb{F}_q[X]$. Then

$$\begin{aligned} g(\beta^k) &= \sum_{i=0}^m a_i^{\gcd(q,k)} \left(\beta^k\right)^i = \sum_{i=0}^m a_i^{\gcd(q,k)} \left(\beta^{k'}\right)^{i\cdot\gcd(q,k)} \\ &= \left(m_{\beta^{k'}}(\beta^{k'})\right)^{\gcd(q,k)} = 0. \end{aligned}$$

Thus, β^k is a root of g and since $\deg(g) = m = \deg(m_{\beta^k})$ the polynomial g is the minimal polynomial of β^k over $\mathbb{F}_q$. That is, $m_{\beta^k} = \sum_{i=0}^m a_i^{\gcd(q,k)} X^i$.

Using Remark 3, 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 $\mathbb{F}_q$.

Note that the main statement of the following theorem is the fact that the roots of the two polynomials $\chi_{\beta^k}(X)$ and $\chi_{\beta^k}(X^k)$ have the same multiplicity.

Theorem 4 *Let $k \in \mathbb{N}$ with $\gcd(q, k) = 1$. 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 $\chi_{\beta^k}(X^k)$ has multiplicity t. That is, the roots of $\chi_{\beta^k}(X)$ and the roots of $\chi_{\beta^k}(X^k)$ have the same multiplicity t.

Proof Since χ_{β^k} is the characteristic polynomial of β^k over $\mathbb{F}_q$, there exists a positive integer $t \geq 1$ such that $\chi_{\beta^k}(X^k) = \left(m_{\beta^k}(X^k)\right)^t$. Furthermore, $m_{\beta^k}(X^k) = \prod_{i=0}^{\frac{n}{t}-1}\left(X^k - \beta^{k \cdot q^i}\right)$ 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, $\chi_{\beta^k}(X^k) = \prod_{i=0}^{\frac{n}{t}-1}\prod_{j=1}^{k}\left(X - \zeta_k^j \beta^{q^i}\right)^t$. Note that the roots $\zeta_k^j \beta^{q^i}$ of $\chi_{\beta^k}(X^k)$ for $1 \leq j \leq k$ and $0 \leq i \leq \frac{n}{t} - 1$ 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 $j_1 = j_2$. To complete the proof recall that the roots of irreducible polynomials over finite fields are simple. □

The roots of the polynomial $\chi_{\beta^k}(X^k)$ 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.

Corollary 5 *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 $\chi_{\beta^k}(X^k)$ 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. By Theorem 2, we have

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

If $k \mid q - 1$, then U_k lies in $\mathbb{F}_q$ and for $1 \leq j \leq k$ the polynomials $\zeta_k^{-jn} f(\zeta_k^j X)$ are monic polynomials of degree n over $\mathbb{F}_q$. The element $\zeta_k^{-j}\beta$ is a root of $\zeta_k^{-jn} f(\zeta_k^j X)$ 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 $\zeta_k^{-jn} f(\zeta_k^j X)$ is the minimal polynomial of $\zeta_k^{-j}\beta$ over $\mathbb{F}_q$ and (1) yields the factorization of $\chi_{\beta^k}(X^k)$ into monic irreducible factors over $\mathbb{F}_q$. With Corollary 5 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 $\zeta_k^{-jn} f(\zeta_k^j X)$ 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 $\zeta_k^{-jn} f(\zeta_k^j X)$ are equal. For this we need the following easy proposition.

Proposition 6 *Let $k, m \in \mathbb{N}$ such that $\gcd(q, k) = 1 = \gcd(q, m)$ and $f \in \mathbb{F}_q[X]$. Then the following statements hold:*

(a) There exists $g \in \mathbb{F}_q[X]$ such that $f(X) = g(X^k)$ if and only if $f(X) = f(\zeta_k X)$.

(b) If there exist polynomials $g, h \in \mathbb{F}_q[X]$ such that $f = g(X^k) = h(X^m)$, then there exists a polynomial $u \in \mathbb{F}_q[X]$ such that $f(X) = u(X^{\mathrm{lcm}(k,m)})$.

Proof (a) If $f(X) = g(X^k)$, then $f(\zeta_k X) = g(\zeta_k^k X^k) = g(X^k) = f(X)$. 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 $0 \leq i \leq n$ such that $a_i \neq 0$. Consequently, $k = \operatorname{ord}(\zeta_k) \mid i$ for all $0 \leq i \leq n$ such that $a_i \neq 0$.

(b) We know that $k \mid i$ and $m \mid i$ for every $0 \leq i \leq n$ such that $a_i \neq 0$. Then also $\operatorname{lcm}(k, m) \mid i$ for every such i.

□

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

Theorem 7 *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 $f(0) \neq 0$. Set $t = \max\{m \in \mathbb{N} : m \mid \gcd(n, k), f(X) = g(X^m)$ for a polynomial $g \in \mathbb{F}_q[X]\}$. Then for $0 \leq j, j' \leq k-1$ the two polynomials $\zeta_k^{-jn} f(\zeta_k^j X)$ and $\zeta_k^{-j'n} f(\zeta_k^{j'} X)$ are equal if and only if $j \equiv j' \mod \frac{k}{t}$.*

Proof "⇐": Note that since $t \mid k$ 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

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

From the definition of t and Proposition 6 follows that $f(X) = f(\zeta_t X)$ and therefore also $f(X) = f(\zeta_t^v X)$. Thus, $\zeta_k^{-j'n} f(\zeta_t^v \zeta_k^{j'} X) = \zeta_k^{-j'n} f(\zeta_k^{j'} X)$.

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

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

Let $f = \sum_{i=0}^n a_i X^i \in \mathbb{F}_q[X]$. Then we have $\zeta_k^{-(j-j')n} f(\zeta_k^{j-j'} X) = \sum_{i=0}^n a_i \zeta_k^{-(j-j')(n-i)} X^i$. 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

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

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 Proposition 6 we obtain that $M := \{m \in \mathbb{N} : m \mid d, f(X) = g(X^m), g \in \mathbb{F}_q[X]\}$ is equal to the set $\{m \in \mathbb{N} : m \mid d, f(X) = f(\zeta_m X)\}$ 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 $f(X) = f(\zeta_t X)$, also $f(X) = f(\zeta_t^i X)$ 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, $j \equiv j' \mod \frac{k}{t}$. □

As a consequence for $k \mid q - 1$ we have the following result.

Corollary 8 *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 $\mathbb{F}_q$. Set $t = \max\{m \in \mathbb{N} : m \mid \gcd(n, k),\ f(X) = g(X^m)$ for a polynomial $g \in \mathbb{F}_q[X]\}$. Then*

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

Proof Using Theorem 7 we can rewrite equation (1) and obtain that the characteristic polynomial of $\beta^k \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ satisfies

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

and that the polynomials $\zeta_k^{-jn} f(\zeta_k^j X)$ for $1 \leq j \leq \frac{k}{t}$ are distinct. Then Corollary 5 completes the proof. □

Recall that Construction AD constructs the polynomial $\chi_{\beta^k}(X^k)$ 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 8, in our construction we directly compute the polynomial $m_{\beta^k}(X^k)$ from which the minimal polynomial m_{β^k} can then easily be extracted.

Remark 4 Note that if $k \mid q - 1$ and k is prime, then $t > 1$ if and only if $t = k$. Thus, if $f(X) = g(X^k)$ 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 $m_{\beta^k}(X^k) = \prod_{j=1}^{k} \zeta_k^{-jn} f(\zeta_k^j X) = (-1)^{n(k+1)} \prod_{j=1}^{k} f(\zeta_k^j X)$.

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 $m_{\beta^k}(X^{k_2}) = m_{\left(\beta^{k_1}\right)^{k_2}}(X^{k_2})$. Thus, instead of using the direct computation of m_{β^k} from m_β, we can apply Corollary 8 recursively. Meaning that we first compute the minimal polynomial of β^{k_1} and then with this polynomial compute $m_{\left(\beta^{k_1}\right)^{k_2}}(X^{k_2})$ 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 4 to suggest 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 $1 \leq i \leq m$ compute the monic irreducible polynomial f_i in the following way:*

If there exists a polynomial $g \in \mathbb{F}_q[X]$ such that $f_{i-1}(X) = g(X^{k_i})$, then $f_i = g$. Otherwise, compute

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

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 5 (a) All 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 $\gcd(n,k)$.

(b) If there exists a polynomial $g \in \mathbb{F}_q[X]$ such that $f = g(X^t)$ for a prime divisor t of k, then the minimal polynomial of β^k will be of lower degree. Observe that 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^m for any positive integer $m > 1$ and could be used instead of f. This fact was proved in [10] for $t = 2$. For the convenience of the reader, we include the generalized proof here.

Proof If $f(X) = \sum_{i=0}^n b_i X^i = g(X^t)$ for $t > 1$, then $b_{n-1} = 0$ and since f is monic, we have $b_n = 1$. Furthermore,

$$\begin{aligned} f(X+a) &= (X+a)^n + \underbrace{\sum_{i=0}^{n-2} b_i \ (X+a)^i}_{\deg(\ldots)<n-1} \\ &= \sum_{j=0}^{n} \binom{n}{j} a^j X^{n-j} + \sum_{i=0}^{n-2} b_i (X+a)^i \\ &= X^n + naX^{n-1} + \sum_{j=2}^{n} \binom{n}{j} a^j X^{n-j} + \sum_{i=0}^{n-2} b_i (X+a)^i. \end{aligned}$$

Since $\gcd(n,q) = 1$, char$(\mathbb{F}_q)$ does not divide n from which follows that $na \neq 0$ and there cannot exist any positive integer $m > 1$ such that $f(X+a) = h(X^m)$ for a polynomial $h \in \mathbb{F}_q[X]$. □

In [1] Albert defines a “cubing transformation", which is an iterated application of Construction AD for $k = 3$. He notices that if the order e of the initial polynomial and 3 are coprime, its behaviour is “periodic”. That is, after a certain amount of iterations it will yield the initial polynomial again. In [10] a similar construction for $k = 2$, the repeated application of Construction KK, is presented, which does not need the knowledge of the order e of the initial polynomial but can even be used to gain information on e. Our results allow to generalize the construction from [10] for primes k satisfying $k \mid q-1$ by applying Construction 1 iteratively.

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 $w = \nu_k(q^n-1)$ 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 $f_{i-1}(X) = g(X^k)$, then $f_i = g$. Otherwise, compute

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

and extract f_i from the composition. If $f_i = f_l$ for an integer l such that $0 \leq l \leq w$ and $l < i$, then stop.

With the notation from Construction 2, suppose that the construction terminates for the polynomial f_{l+s} which is equal to f_l, for integers $s \geq 1$ and $0 \leq l \leq \nu_k(q^n-1)$. Then we call the sequence

$$(f_0, f_1, \ldots, f_{l-1})$$

the *tail* of the construction and the sequence

$$(f_l, \ldots, f_{l+s-1})$$

the *orbit*. Note that the construction would yield the polynomials of the orbit repeatedly if we continued to iterate through the integers $i \geq l+s$. Observe that the length of the tail is l and the length of the orbit s.

Corollary 9 *With the notation from Construction 2, we suppose that Construction 2 terminated after a tail of length l and an orbit of length s.*

Then $\operatorname{ord}(f) = k^l \cdot r$ and r must satisfy

(I) $\gcd(k, r) = 1$,
(II) $s = \frac{\operatorname{ord}_r(k)}{d}$ *for a divisor d of* $\deg(f_l)$,
(III) Furthermore, for an integer $0 \leq j \leq \deg(f_l) - 1$, d must satisfy $\operatorname{ord}_r(q^j) = d$ and $k^s \equiv q^j \mod r$.

Proof Let $\beta \in \mathbb{F}_{q^n}$ be a root of f, that is, $f = m_\beta$ is the minimal polynomial of β over $\mathbb{F}_q$. Then with Construction 1 we know that $f_i = m_{\beta^{k^i}}$ for every $i \geq 0$. Further, let $\operatorname{ord}(f) = e$ and $e = k^v \cdot r$ with $\gcd(k, r) = 1$. Then with Theorem 3 the minimal polynomial of β^{k^i}, that is, the polynomial f_i, has order

$$\operatorname{ord}(f_i) = \begin{cases} \frac{e}{k^i} = k^{v-i} \cdot r & \text{for } 0 \leq i \leq v, \\ r & \text{for } i \geq v. \end{cases} \tag{4}$$

Since the order of the polynomials $(f_0, f_1, \ldots, f_{v-1})$ strictly decreases, these polynomials cannot appear twice in the sequence $(f_i)_{i\geq 0}$. Note that $v \leq w = \nu_k(q^n-1)$. Thus, the polynomial f_v, which is the first polynomial of order r of the sequence $(f_i)_{i\geq 0}$, is an element of the sequence $(f_0, f_1, \ldots, f_w)$.

We need to examine $\mathbb{Z}_r^*$, the multiplicative group modulo r, to see that f_v is the first polynomial to appear twice in the sequence $(f_i)_{i\geq 0}$ and therefore $v = l$. The subgroup $\langle k\rangle$ of $\mathbb{Z}_r^*$ generated by k has order $\mathrm{ord}_r(k)$, which is the multiplicative order of k modulo r. This implies that $\beta^{k^{v+\mathrm{ord}_r(k)}} = \beta^{k^v}$ and obviously the minimal polynomials of β^{k^v} and $\beta^{k^{v+\mathrm{ord}_r(k)}}$ over $\mathbb{F}_q$ are equal. Thus, $f_v = f_{v+\mathrm{ord}_r(k)}$ and we have shown that f_v does appear again in the sequence.

However, the length s of the orbit is not always equal to $\mathrm{ord}_r(k)$. The polynomials f_{i_1} and f_{i_2} are equal if and only if $\beta^{k^{i_1}}$ and $\beta^{k^{i_2}}$ are $\mathbb{F}_q$-conjugates. Thus, it is possible that there exists a positive integer u smaller than $\mathrm{ord}_r(k)$ such that $\beta^{k^{v+u}}$ is an $\mathbb{F}_q$-conjugate of β^{k^v} and the minimal polynomial $f_{v+u} = m_{\beta^{k^{v+u}}}$ also is equal to $f_v = m_{\beta^{k^v}}$. To account for this, we choose $u \in \mathbb{N}$ to be the smallest positive integer that satisfies

$$\langle k\rangle \cap \langle q\rangle = \langle k^u\rangle = \langle q^j\rangle \leq \mathbb{Z}_r^* \quad \text{for an integer } 0 \leq j \leq \deg(f_v) - 1. \tag{5}$$

Note that since $\langle k^{\mathrm{ord}_r(k)}\rangle = \langle q^0\rangle$ such an integer u exists and satisfies $u \leq \mathrm{ord}_r(k)$. Then $\beta^{k^{v+u}} = \left(\beta^{k^v}\right)^{q^j}$ and $f_{v+u} = f_v$. Moreover, the minimal polynomials of $\beta^{k^{v+i}}$ for $0 \leq i \leq u-1$ are distinct because we selected u to be the smallest positive integer to satisfy (5). Consequently, $v = l$, which shows that (I) holds, and the length s of the orbit equals u.

Set $d := |\langle q^j\rangle| = |\langle k^s\rangle|$ which is a divisor of $\deg(f_l)$, since $\langle q^j\rangle \leq \langle q\rangle$ and $|\langle q\rangle| = \deg(f_l)$. Then because of $\langle k^s\rangle$ being a subgroup of $\langle k\rangle$, we have $s = \frac{|\langle k\rangle|}{|\langle k^s\rangle|} = \frac{\mathrm{ord}_r(k)}{d}$ which shows that (II) holds. (III) follows directly from equation (4) and our definition of d. □

Note that with equation (4) in the proof of Corollary 9 the polynomials f_i for $0 \leq i \leq l-1$ of the tail of Construction 2 have order $k^{l-i} \cdot r$ and all polynomials of the orbit have order r.

If $p_1, \ldots, p_m$ are the distinct prime factors of $q-1$, and $\mathrm{ord}(f) = e = p_1^{v_1} \cdots p_m^{v_m} \cdot r$ with $\gcd(q, r) = 1$ and $v_1 \geq 0, \ldots, v_m \geq 0$. Then Construction 2 allows us to determine the p_i-adic valuations $v_1, \ldots, v_m$ of the order of f. Additionally, Corollary 9 (II) and (III) give further conditions on the factor r. In most of our computations the conditions on the factor r were so restrictive that Construction 2 yielded the exact order e of f.

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 Corollary 9, 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.

4 Implementation of the construction

In this section we discuss which polynomials can be obtained from a given initial polynomial f with Construction 1 and how to select the integers k for which we apply the construction. All discussions in this section are about this fixed polynomial f. Suppose that f is of degree n, has order e and $\beta \in \mathbb{F}_{q^n}$ is a root of f. Then β has multiplicative order e and the subgroup $\langle\beta\rangle = \{\beta^k : 0 \leq k \leq e-1\}$ of $\mathbb{F}_{q^n}^*$ contains all elements of $\mathbb{F}_{q^n}$ with multiplicative order dividing e. Consequently, the set of all polynomials of the form m_{β^k} for $k \geq 0$ is in fact $\{m_{\beta^k} : 0 \leq k \leq e-1\}$ and contains all monic irreducible polynomials over $\mathbb{F}_q$ whose order divides e.

Let $p_1, \ldots, p_m$ be the distinct prime factors of $q-1$. Then we can apply Construction 1 for any integer k that is an element of the set

$$\mathcal{A} := \{p_1^{i_1} \cdots p_m^{i_m} : i_1, \ldots, i_m \geq 0\}.$$

Since the element β has multiplicative order e, Construction 1 yields the minimal polynomial of $\beta^{k \pmod{e}}$ over $\mathbb{F}_q$. Thus, the set of polynomials that we can construct with the integers in $\mathcal{A}$ is

$$\mathcal{M} := \{m_{\beta^{k \pmod{e}}} : k = p_1^{i_1} \ldots p_m^{i_m}, i_1, \ldots, i_m \geq 0\}.$$

However, we would like to emphasize that the construction should not be restricted to the elements of $\mathcal{A}$ which are smaller than e, here denoted by $\mathcal{A}_{<e}$. An integer $k \in \mathcal{A}$, $k \geq e$, can yield a polynomial that cannot be constructed by choosing all elements of $\mathcal{A}_{<e}$. This is the case if its representative $k \pmod{e}$ in $\mathbb{Z}_e$ is not an element of $\mathcal{A}$ as can be seen from the following example:

Example 1 Let $\mathbb{F}_8 = \mathbb{F}(a)$ where a is a root of the monic irreducible polynomial $X^3+X+1 \in \mathbb{F}_2[X]$. We consider the primitive monic irreducible polynomial $f = X^5 + aX^4 + X^3 + aX^2 + (a^2+a)X + a^2 \in \mathbb{F}_8[X]$ of order $e = 32\,767 = 7 \cdot 31 \cdot 151$. Since $8-1=7$, we can apply Construction 1 for all elements of $\mathcal{A} = \{7^i : i \geq 0\}$. Note that we can use the notation of Construction 2 and say that the construction yields a tail of length 1 and an orbit of length 150. By this we mean that the polynomials m_{β^7} and $m_{\beta^{7^{151}}}$ are equal, where β is a root of f.

The smallest positive integer i such that 7^i is greater than or equal to e is 6. In fact, $7^6 \pmod{e} = 117\,649 \pmod{e} = 19\,348 = 2^2 \cdot 7 \cdot 691 \notin \mathcal{A}$. Thus, if we had restricted ourselves to $\mathcal{A}_{<e}$, we would only have found 5 of the 151 possible polynomials.

The number of polynomials that we can construct with Construction 1, which is the size of $\mathcal{M}$, obviously depends on the size of $\mathcal{A}$ considered in $\mathbb{Z}_e$:

$$\mathcal{A}_{\bmod e} = \{p_1^{i_1} \cdots p_m^{i_m} \pmod{e} : i_1, \ldots, i_m \geq 0\}.$$

Note that in general $|\mathcal{M}|$ is smaller than the size of $\mathcal{A}_{\bmod e}$, because in $\mathcal{A}_{\bmod e}$ exponents can belong to $\mathbb{F}_q$-conjugates which then yield the same polynomial multiple times.

We believe that it is not possible to give a closed formula for $|\mathcal{M}|$ in general since computing $|\mathcal{A}_{\bmod e}|$ is difficult. Indeed, it is related to determining the order of some prime numbers in $\mathbb{Z}_r^*$. In order to see this, suppose that $e = p_1^{v_1} \ldots p_m^{v_m} \cdot r$ with $\gcd(q-1, r) = 1$ and $v_1, \ldots, v_m \geq 0$. Then by the Chinese Remainder Theorem the ring $\mathbb{Z}_e$ is isomorphic to $\mathbb{Z}_{p_1^{v_1}} \times \ldots \times \mathbb{Z}_{p_m^{v_m}} \times \mathbb{Z}_r$. To determine $|\mathcal{A}_{\bmod e}|$, in particular, we need to calculate the size of the multiplicative subgroup $\langle p_1, \ldots, p_m \rangle$ in $\mathbb{Z}_r^*$.

The behaviour of Construction 2 allows us to discuss the selection of the integers $k = p_1^{i_1} \cdots p_m^{i_m}$, $i_1 \geq 0, \ldots, i_m \geq 0$, for Construction 1 so that the number of multiple constructions of the same polynomial is reduced. First, we can obtain a naive upper bound on the exponents $i_1, \ldots, i_m$ by computing Construction 2 separately for every prime integer p_j, $1 \leq j \leq m$. Suppose then that the tail has a length of v_j and the orbit a length of s_j, which is a divisor of the multiplicative order $\operatorname{ord}_{e/p_j^{v_j}}(p_j)$. We set $i_j \leq v_j + s_j$. We would like to note that if the order e of the initial polynomial $f = m_\beta$ is known, the values v_j and s_j can be determined directly with Corollary 9.

In order to eliminate the remaining duplicates, we suggest the following procedure: We select an integer $k = p_1^{i_1} \cdots p_{m-1}^{i_{m-1}}$ with $i_j \leq v_j + s_j$ for every $1 \leq j \leq m-1$ and compute m_{β^k}. Then we construct the polynomials $m_{\beta^{k \cdot p_m^i}}$ by applying Construction 1 for p_m repeatedly.

With this we obtain a tail $(m_{\beta^k}, \dots, m_{\beta^{k\cdot p_m^{v_m-1}}})$ and an orbit $(m_{\beta^{k\cdot p_m^{v_m}}}, \dots, m_{\beta^{k\cdot p_m^{v_m+(s-1)}}})$. Note that the length s of the orbit depends on k.

Two integers k_1 and k_2 have either the same or a distinct tail. This will happen if and only if $k_1 \equiv k_2 \cdot q^j \mod e$ for an integer $0 \leq j \leq n-1$. Clearly if the tail is the same, the orbits coincide too. Thus, if the first tail polynomial is equal, the computation can be stopped. The polynomials of the orbits of two different integers are also either distinct or equal. Equal orbits can also occur for integers with distinct tails. In this case the orbit polynomials appear in a shifted order. It is easy to see that any other integer of the form $k_1 \cdot \left(\frac{k_2}{k_1}\right)^l$ with $l \geq 0$ will yield the same orbit. For such integers we compute only the tail.

Example 2 As we have seen before, the number of constructed polynomials only depends on the order of the initial polynomial. As an example for our computations we consider the polynomials

$$\begin{aligned} f_1 &= X^8 + X^5 + X^3 + X^2 + a, \\ f_2 &= X^9 + (a^2+a)X^8 + (a^3+a^2)X^7 + aX^6 + X^5 + (a^3+a^2+a)X^4 \\ &\quad + (a^2+a+1)X^3 + a^2X^2 + a^3X + a^3 + a^2 + a \end{aligned}$$

over $\mathbb{F}_{16} = \mathbb{F}(a)$, where a is a root of the monic irreducible polynomial $X^4 + X + 1$ over $\mathbb{F}_2$.

The polynomial f_1 is primitive and has order $4\,294\,967\,295 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65\,537$. Construction 1 with f_1 as initial polynomial yields 1 114 113 monic irreducible polynomials of degree 8. Computing m_{β^k} for values of k of the form 3^j, $j \geq 0$, and then applying the construction repeatedly for 5, there are 33 orbits of 32 768 polynomials each. The orbit for $k = 1$ contains 32 768 of the 67 108 864 monic irreducible polynomials of order $3 \cdot 17 \cdot 257 \cdot 65537$ over $\mathbb{F}_{16}$ and the other 32 orbits for $k = 3^j$, $1 \leq j \leq 32$, yield 1 048 576 of the 33 554 432 monic irreducible polynomials of order $17 \cdot 257 \cdot 65\,537$ over $\mathbb{F}_{16}$. f_1 has 5 non-zero coefficients and yields a weight distribution of $4^6 5^{384} 6^{7225} 7^{65997} 8^{331084} 9^{709417}$, which means that there exist 6 polynomials with smaller weight and 384 polynomials with the same weight. Hence, from these we could try to choose polynomials with other required properties that our initial polynomial might lack.

The polynomial f_2 has order $68\,719\,476\,735 = 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$ and yields 4 644 monic irreducible polynomials over $\mathbb{F}_{16}$ of degree 9 with the weight distribution $6^2 7^{47} 8^{373} 9^{1401} 10^{2821}$. Even though the number of constructed polynomials is not very large, we could find polynomials of weight 6, 7 and 8. Considering the orbits for repeated application of Construction 1 for 5 with starting polynomials m_{β^k} with $k = 3^j$, $j \geq 0$, there are 21 orbits of 216 polynomials each and the construction yields 3 888 of the 40 310 784 polynomials of order $509\,033\,161 = 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$.

An interesting class of polynomials are the so-called *normal polynomials* or *N-polynomials* (see [5, 6, 11, 13, 15]). A monic irreducible polynomial of degree n with a root α is called *normal* if its roots $\alpha, \alpha^q \dots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$ or, equivalently, if the degree of the greatest common divisor of the polynomials $g_\alpha = \alpha X^{n-1} + \alpha^q X^{n-2} + \dots + \alpha^{q^{n-2}} X + \alpha^{q^{n-1}}$ and $X^n - 1$ over $\mathbb{F}_{q^n}$ is 0. This concept has been extended in [7] to *k-normal* polynomials which satisfy that the greatest common divisor of the two polynomials g_α and $X^n - 1$ has degree k. Tables 1and 2show that Construction 1 also yields a large number of k-normal polynomials for small values of k which could be used for respective applications. Since the number of k-polynomials decreases with k increasing, this distribution of k-normality is to be expected (see [7]).

Table 1 Weight and k-normality distribution for f_1

Weight	Total	0-normal	1-normal	2-normal	3-normal
4	6	1	5	0	0
5	384	139	240	5	0
6	7 225	4 160	2 927	136	2
7	65 997	47 088	17 746	1 119	44
8	331 084	283 554	44 713	2 625	192
9	709 417	709 417	0	0	0

Table 2 Weight and k-normality distribution for f_2

Weight	Total	0-normal	1-normal	2-normal	3-normal	4-normal
6	2	1	1	0	0	0
7	47	28	15	4	0	0
8	373	256	102	14	1	0
9	1 401	1 091	290	18	0	2
10	2 821	2 475	339	5	2	0

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Albert A.A.: Fundamental concepts of higher algebra. University of Chicago Press, Chicago (1956).
2. Cohen S.: On irreducible polynomials of certain types in finite fields. Math. Proc. Camb. Philos. Soc. **66**(2), 335–344 (1969).
3. Cohen S.: The explicit construction of irreducible polynomials over finite fields. Des. Codes Cryptogr. **2**(2), 169–174 (1992).
4. Daykin D.E.: Generation of irreducible polynomials over a finite field. Am. Math. Mon. **72**(6), 646–648 (1965).
5. Gathen J.V.Z., Giesbrecht M.: Constructing normal bases in finite fields. J. Symb. Comput. **10**(6), 547–570 (1990).
6. Gao, S.: Normal bases over finite fields. PhD Thesis (1993).
7. Huczynska S., Mullen G., Panario D., Thomson D.: Existence and properties of k-normal elements over finite fields. Finite Fields Appl. **24**, 170–183 (2013).
8. Kyuregyan, M.K.: Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics. Finite Fields Appl. **12**(3), 357–378 (2006).
9. Kyuregyan, M.K., Kyureghyan, G.M.: Irreducible compositions of polynomials over finite fields. Des. Codes Cryptogr. **61**(3), 301–314 (2011).
10. Kyureghyan, G.M., Kyuregyan, M.K.: A recurrent construction of irreducible polynomials of fixed degree over finite fields. Appl. Algebra Eng. Commun. Comput. **33**, 163–171 (2022).

11. Kyuregyan, M.K.: Iterated constructions of irreducible polynomials over finite fields with linearly independent roots. Finite Fields Appl. **10**(3), 323–341 (2004).
12. McNay, G.: Topics in finite fields. Ph.D. Thesis at the University of Glasgow (1995).
13. Meyn H.: Explicit N-polynomials of 2-power degree over finite fields. Des. Codes Cryptogr. **6**(2), 107–116 (1995).
14. Panario D., Reis L., Wang Q.: Construction of irreducible polynomials through rational transformations. J. Pure Appl. Algebra **224**(5), 106241 (2020).
15. Semaev I.: Construction of polynomials irreducible over a finite field with linearly independent roots. Math. USSR-Sbornik **63**(2), 507 (1989).
16. Ugolini S.: Sequences of binary irreducible polynomials. Discret. Math. **313**(22), 2656–2662 (2013).