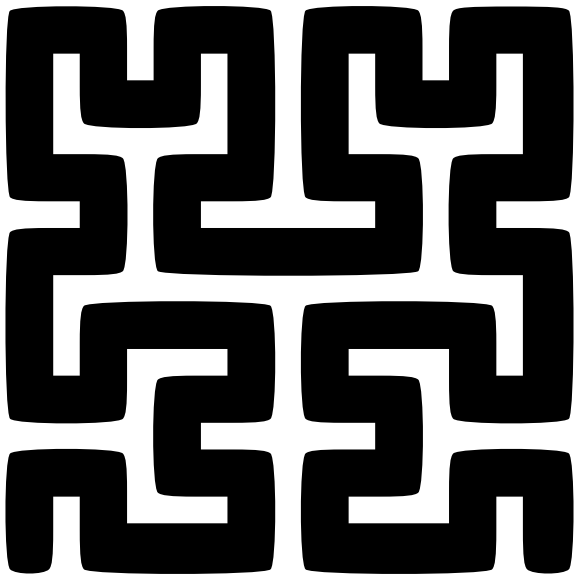

Polynesian Journal of Mathematics

Volume 2, Issue 2

Using Tschirnhaus transformations to find roots in quintic polynomials over $\mathbb{F}_{2^m}$

Peter Beelen Emil Astrup Wrisberg

Received 14 Dec 2024
Accepted 27 Mar 2025
Published 11 Apr 2025
Communicated by Gaetan Bisson

DOI: 10.69763/polyjmath.2.2

Polynesian Journal of Mathematics
Volume 2, Issue 2 (Apr. 2025)

Using Tschirnhaus transformations to find roots in quintic polynomials over $\mathbb{F}_{2^m}$

Peter Beelen Emil Astrup Wrisberg

Department of Applied Mathematics and Computer Science
Technical University of Denmark
DK-2800, Kongens Lyngby, Denmark

Abstract

In this article we present an algorithm to find the roots of a quintic polynomial with coefficients in $\mathbb{F}_{2^m}$, the finite field with 2^m elements, provided that the polynomial has five distinct roots in this field. The algorithm uses algebraic transformations, called Tschirnhaus transformations, to convert a given quintic polynomial into a normal form, namely $x^5 + x + f$ or $x^5 + f$. A table lookup is then applied to read off the roots of a polynomial in normal form, after which the roots are transformed back. The size of the lookup table is roughly $2^m/60$, implying that for practical values of m (such as $m = 8, 10, 12$) the lookup table size is very modest (namely 7, 17, 71). We also describe a polynomial $P_m(T)$ whose roots correspond to the values of $f \in \mathbb{F}_{q^m}$ such that the polynomial $x^{q+1} - x - f$ has $q + 1$ distinct roots in $\mathbb{F}_{q^m}$, generalizing a result of Berlekamp, Rumsey, and Solomon from 1966.

Keywords: Root finding, quintic polynomials over a finite field, Tschirnhaus transformation.

1 Introduction

Having efficient algorithms to find the roots of low degree polynomials is very useful when decoding generalized Reed–Solomon (GRS) codes defined over a finite field $\mathbb{F}_q$. Several of the standard algorithms for decoding these codes, find a polynomial $p(x)$ whose roots indicate the position of the errors in the received word. More specifically, a code word in a q-ary GRS code of length n and dimension k is of the form $c = (u_1 f(\alpha_1), \ldots, u_n f(\alpha_n))$, where $f(x) \in \mathbb{F}_q[x]$ is a polynomial of degree at most $k - 1$, $\alpha_1, \ldots, \alpha_n$ are distinct elements of $\mathbb{F}_q$ and $u_1, \ldots, u_n$ are nonzero (not necessarily distinct) elements of $\mathbb{F}_q$. If $r = (r_1, \ldots, r_n) = c + e$ is the received word and $e = (e_1, \ldots, e_n)$ is the error vector, fast decoders exist that recover c from r if we assume that at most $t := w_H(e) \leqslant \lfloor (n-k)/2 \rfloor$ errors have occurred. A very common procedure is to find the error-locator polynomial, that is to say a polynomial $p(x) \in \mathbb{F}_q[x]$ of degree $t = w_H(e)$ such that $p(\alpha_i) = 0$ if and only if $e_i \neq 0$. As a part of the decoding algorithm, the roots of

this polynomial $p(x)$ need to be found. Note that if the number of errors does not exceed $\lfloor (n-k)/2 \rfloor$, then the roots of $p(x)$ are distinct (no multiple roots) and all lie in the finite field $\mathbb{F}_q$. Also note that this decoder is used for binary subfield subcodes of GRS codes, including BCH codes. We are especially interested in the finite fields $\mathbb{F}_{2^m}$, because these are the most important in practical applications. If $\lfloor (n-k)/2 \rfloor \leqslant 4$, finding the roots of $p(x)$ is done using explicit formulas for its roots. Indeed, for polynomials $p(x) \in \mathbb{F}[x]$ of degree up to 4 and coefficients in a field $\mathbb{F}$, it is well known that there exist explicit solution formulas for the roots of $p(x)$ in terms of nested radicals of degree 2 and 3 in the coefficients of $p(x)$. Here a radical of an element u of prime degree p is defined to be a solution to the equation $x^p = u$ (resp. a solution to the equation $x^p - x = u$) if the characteristic of $\mathbb{F}$ is not p (resp. is equal to p). Such solution formulas have been the mathematical basis of fast algorithms to compute the roots of polynomials $p(x) \in \mathbb{F}_q[x]$ of degree up to 4, where $\mathbb{F}_q$ is the finite field with q elements. Algorithms using algebraic solution formulas to find the roots of polynomials of degree up till 4 are for example given in [2], [3], [6], [9], [11]. If the degree of the polynomial exceeds 4, no solution formula for the roots of $p(x)$ in terms of radicals exists in general and other methods are used. In [2, 3] solution methods for polynomials of higher degree are proposed by extending polynomials to affine polynomials, for which the roots can be found by solving a linear system of equations. For polynomials of degree 5 this already requires an extension to a polynomial of degree 16, where it may be inefficient to find the 5 correct roots. Other techniques in the literature involve searching through the elements of $\mathbb{F}_q$ in various ways, [8], [12].

In this article we aim to give an efficient method to find the roots of a quintic polynomial with five distinct roots in $\mathbb{F}_{2^m}$ using a lookup table of size roughly $2^m/60$. This lookup table can be precomputed and indeed we assume this has been done. Our approach presupposes that m is even, since it turns out that if m is odd, the size of the lookup table is significantly larger. The main results of this article are the following. First of all, we give a criterion that can be used to theoretically determine whether or not a polynomial in $\mathbb{F}_q[x]$ of degree d has d distinct roots in $\mathbb{F}_q$. We will use this to describe for which values of $f \in \mathbb{F}_{q^m}$ the polynomial $x^{q+1} - x - f \in \mathbb{F}_{q^m}[x]$ has $q+1$ distinct roots in $\mathbb{F}_{q^m}$. This extends results in [4] where the number of such polynomials was found. Secondly, we show, 1) given a quintic polynomial $p(x) \in \mathbb{F}_{2^m}[x]$ with m even, how to decide whether or not $p(x)$ has 5 distinct roots in $\mathbb{F}_{2^m}$ and 2) in the affirmative case, find these 5 distinct roots. The amount of computations needed for part 1) is $O(m)$ operations in $\mathbb{F}_{2^m}$. The table lookup in part 2) can be done in complexity $O(m)$ using a binary search tree.

In the first part of the algorithm, a given quintic polynomial $p(x)$ is transformed into a polynomial of the form $x^5 + x + F$, of the form $x^5 + F$, or the problem is reduced to solving a quartic equation for which efficient algorithms already exist (see above). The used transformations are called Tschirnhaus transformations in the literature. In the second part of the algorithm, the roots of a quintic polynomial in normal form are found using a lookup table and then transformed back to give the roots of the original quintic polynomial $p(x)$. If the transformed polynomial $x^5 + x + F$ does not occur in the lookup table, the algorithm concludes that $p(x)$ does not have all its roots in $\mathbb{F}_{2^m}$

or that it has multiple roots. We will show that this table has size at most $\lfloor 2^m/60 \rfloor + 3$. For several practical values of m, the size of the lookup table size is very modest. For example for $m = 2, 4, 6, 8, 10, 12, 14$, the table sizes are $0, 3, 1, 7, 17, 71, 273$. This article is an extended version of parts of a bachelor project carried out by the second author. More precisely, several of the results in Section 3 of this article can be found in [14].

2 The Frobenius map and completely splitting polynomials

Definition 2.1. *Let $\mathbb{F}_q$ be a finite field with q elements and $p(x) \in \mathbb{F}_q[x]$ a polynomial of degree $d > 0$. We say that $p(x)$ splits completely over $\mathbb{F}_q$, if $p(x)$ has d distinct roots in $\mathbb{F}_q$.*

As mentioned before, our interest in completely splitting polynomials comes from the decoding of GRS and BCH codes.

Definition 2.2. *Let q be a fixed prime power and $p(x) \in \mathbb{F}_q[x]$ be a non-zero polynomial and write $\langle p(x) \rangle$ for the ideal in $\mathbb{F}_q[x]$ generated by $p(x)$. We denote by $F_n : \mathbb{F}_q[x]/\langle p(x) \rangle \to \mathbb{F}_q[x]/\langle p(x) \rangle$ the Frobenius map on the quotient ring $\mathbb{F}_q[x]/\langle p(x) \rangle$ defined by $F_n(a(x) + \langle p(x) \rangle) = a(x)^{q^n} + \langle p(x) \rangle$.*

It is easy to verify that the Frobenius map is a ring homomorphism as well as a linear map of $\mathbb{F}_q$-vector spaces (hence it is a homomorphism of $\mathbb{F}_q$-algebras). Berlekamp's factorization algorithm of polynomials with coefficients in $\mathbb{F}_q$ is based on properties of the Frobenius map. We will use it to study completely splitting polynomials.

Theorem 2.3. *Let $\mathbb{F}_q$ be the finite field with q elements and $p(x) \in \mathbb{F}_q[x]$ a polynomial of degree $d > 0$. Then $p(x)$ splits completely over $\mathbb{F}_q$ if and only if the Frobenius map $F_1 : \mathbb{F}_q[x]/\langle p(x) \rangle \to \mathbb{F}_q[x]/\langle p(x) \rangle$ is the identity map.*

Proof. The polynomial $p(x)$ splits completely over $\mathbb{F}_q$ if and only if $p(x)$ divides $x^q - x$. This implies that $p(x)$ splits completely over $\mathbb{F}_q$ if and only if $F_1(x + \langle p(x) \rangle) = x + \langle p(x) \rangle$. Since the Frobenius operator F_1 is completely determined by the image of $x + \langle p(X) \rangle$, this implies the theorem. □

This theorem is very useful to classify polynomials of a specific form that split completely.

Example 2.4. Let $p(x) = x^q - x - f$, with $f \in \mathbb{F}_{q^m}$. Then $F_m(x + \langle p(x) \rangle) = x + f + \cdots + f^{q^{m-1}} + \langle p(x) \rangle$. Hence Theorem 2.3 implies the well known result that the polynomial $x^q - x - f$ has q distinct roots in $\mathbb{F}_{q^m}$ if and only if $\mathrm{Tr}_m(f) = 0$, where Tr_m denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

In the remainder of this section we study the splitting over $\mathbb{F}_{q^m}$ of polynomials of the form $x^{q+1} - x - f$. For $q = 4$, these are quintic polynomials that we will use later. We start by stating a theorem which is a direct consequence of Lemma 4.4 from [4].

Theorem 2.5. *Let q be a prime power and m a positive integer. Then there are exactly $\left\lfloor \frac{q^{m-1}}{q^2-1} \right\rfloor$ values of $f \in \mathbb{F}_{q^m} \setminus \{0\}$ for which $x^{q+1} - x - f$ splits completely over $\mathbb{F}_{q^m}$.*

Proof. Lemma 4.4 in [4] deals with polynomials of the form $p(x) = x^{q+1} - bx + b$ over a field $F = \mathbb{F}_{Q^m}$ such that $F \cap \mathbb{F}_q = \mathbb{F}_Q$ for some Q and $b \in F\backslash\{0\}$. The lemma then states that if N_{Q+1} denotes the number of $b \in F\backslash\{0\}$ such that $p(x)$ has exactly $Q+1$ roots in F, then

$$N_{Q+1} = \begin{cases} \frac{Q^{m-1}-1}{Q^2-1} & \text{if } m \text{ is odd,} \\ \frac{Q^{m-1}-Q}{Q^2-1} & \text{if } m \text{ is even.} \end{cases}$$

First of all, we choose $F = \mathbb{F}_{q^m}$ so that $q = Q$. Second of all, note that introducing the variables $f = -b^{-1/q}$ and $y = -xf$, then $x^{q+1} - bx + b = 0$ if and only if $y^{q+1} - y - f = 0$. Hence the theorem follows. □

This theorem has the following consequence.

Corollary 2.6. *Suppose that m is even. There exist exactly $\left\lfloor \frac{2^m}{60} \right\rfloor$ nonzero values of $f \in \mathbb{F}_{2^m}$ such that the polynomial $x^5 + x + f$ splits completely over $\mathbb{F}_{2^m}$.*

Proof. Choosing $q = 4$ and $\ell = m/2$, the theorem implies that there exist exactly $\left\lfloor \frac{q^{\ell-1}}{q^2-1} \right\rfloor = \left\lfloor \frac{2^m}{60} \right\rfloor$ nonzero values of $f \in \mathbb{F}_{4^\ell} = \mathbb{F}_{2^m}$ such that the polynomial $x^5 + x + f$ splits completely over $\mathbb{F}_{2^m}$. □

Using Theorem 2.3, it is possible to describe the $\left\lfloor \frac{q^{m-1}}{q^2-1} \right\rfloor$ values of f from Theorem 2.5 as roots of a polynomial. We do this in the following theorem.

Theorem 2.7. *Let q be a prime power and m a positive integer. Let $P_m(T) \in \mathbb{F}_q[T]$ be the polynomial recursively defined by*

$$P_1(T) := 1, \quad P_2(T) := 1, \quad \text{and} \quad P_n(T) := P_{n-1}(T) + T^{q^{n-3}} P_{n-2}(T) \quad \text{for } n \geqslant 3.$$

Then $\deg P_m(T) = \left\lfloor \frac{q^{m-1}}{q^2-1} \right\rfloor$ and the polynomial $x^{q+1} - x - f \in \mathbb{F}_{q^m}[x]$ splits completely over $\mathbb{F}_{q^m}$ if and only if $P_m(f) = 0$.

Proof. The statement about the degree of $P_m(T)$ follows directly using induction on m. It is then clear that $P_m(T)$ has at most $\left\lfloor \frac{q^{m-1}}{q^2-1} \right\rfloor$ roots in $\mathbb{F}_{q^m}$. Therefore, if we can prove that $x^{q+1} - x - f \in \mathbb{F}_{q^m}[x]$ splits completely over $\mathbb{F}_{q^m}$ implies $P_m(f) = 0$, then we deduce that the roots of $P_m(T)$ exactly characterize the $\left\lfloor \frac{q^{m-1}}{q^2-1} \right\rfloor$ values of f from Theorem 2.5.

Now assume that the polynomial $p(x) = x^{q+1} - x - f \in \mathbb{F}_{q^m}[x]$ splits completely over $\mathbb{F}_{q^m}$. In particular, $f \neq 0$, since otherwise $p(x)$ has only two roots 0 and 1. By Theorem 2.3, we know that the Frobenius map $F_m : \mathbb{F}_{q^m}[x]/\langle p(x)\rangle \to \mathbb{F}_{q^m}[x]/\langle p(x)\rangle$ is the identity map. In the quotient ring $\mathbb{F}_{q^m}[x]/\langle p(x)\rangle$ the element $x + \langle p(x)\rangle$ is a unit (since $f \neq 0$) and we can write $x^q + \langle p(x)\rangle = \frac{x+f+\langle p(x)\rangle}{x+\langle p(x)\rangle}$. Now let us write $t := x + \langle p(x)\rangle$, then we have $t^q = \frac{t+f}{t}$. Hence the q^{th} power map on t can be described as $\mu(t)$, where μ is the linear fractional transformation corresponding to the matrix $A := \begin{pmatrix} 1 & f \\ 1 & 0 \end{pmatrix}$. For $i \geqslant 0$, we denote by $A^{(i)}$, the matrix obtained from A by raising all of its coefficients

to the q^i-th power. In particular $A^{(0)} = A$. Clearly $F_m(t) = t^{q^m} = (\mu \circ \cdots \circ \mu)(t)$, where $\mu \circ \cdots \circ \mu$ denotes the m-fold composite of μ with itself. This implies that $F_m(t)$ can be described as the linear fractional transformation corresponding to the matrix $A^{(m-1)} \cdots A^{(0)}$. For $n \geqslant 1$, write $B_n := A^{(n-1)} \cdots A^{(0)}$ as well as $B_n = \begin{pmatrix} a_n & c_n \\ b_n & d_n \end{pmatrix}$. By definition of B_n, we have

$$\begin{pmatrix} a_1 & c_1 \\ b_1 & d_1 \end{pmatrix} = A = \begin{pmatrix} 1 & f \\ 1 & 0 \end{pmatrix}$$

and, for $n \geqslant 2$,

$$\begin{aligned} \begin{pmatrix} a_n & c_n \\ b_n & d_n \end{pmatrix} &= A^{(n-1)} \cdot B_{n-1} = \begin{pmatrix} 1 & f^{q^{n-1}} \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{n-1} & c_{n-1} \\ b_{n-1} & d_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} a_{n-1} + f^{q^{n-1}} b_{n-1} & c_{n-1} + f^{q^{n-1}} d_{n-1} \\ a_{n-1} & c_{n-1} \end{pmatrix}. \end{aligned}$$

This immediately implies that the coefficients b_n satisfy the recursion

$$b_1 := 1, \quad b_2 := 1, \quad \text{and} \quad b_n := b_{n-1} + f^{q^{n-2}} b_{n-2} \quad \text{for } n \geqslant 3.$$

Using induction on n, it is easy to see that each b_n is a q^{th} power when viewed as polynomial in f. Moreover, by definition of the polynomials $P_n(T)$, we have for all $n \geqslant 1$, $P_n(f)^q = b_n$. If the polynomial $p(x) = x^{q+1} - x - f \in \mathbb{F}_{q^m}[x]$ splits completely over $\mathbb{F}_{q^m}$, then $F_m(t) = t$, implying that B_m is a multiple of the identity matrix. In particular, we must have $b_m = 0$. This implies that also $P_m(f) = b_m^{1/q} = 0$, as desired. □

This theorem generalizes Theorem 4 in [2], where a similar result was obtained for $q = 2$. The polynomials $P_m(T)$ are very simple to compute. The first few are given in the following table.

m	$P_m(T)$
1	1
2	1
3	$1 + T$
4	$1 + T + T^q$
5	$1 + T + T^q + T^{q^2} + T^{q^2+1}$
6	$1 + T + T^q + T^{q^2} + T^{q^2+1} + T^{q^3} + T^{q^3+1} + T^{q^3+q}$
7	$1 + T + T^q + T^{q^2} + T^{q^2+1} + T^{q^3} + T^{q^3+1} + T^{q^3+q} + T^{q^4} + T^{q^4+1} + T^{q^4+q} + T^{q^4+q^2} + T^{q^4+q^2+1}$

It is not hard to see with induction that for general m, the polynomial $P_m(T)$ is the sum of all terms of the form $T^{q^{i_1}+\cdots+q^{i_\ell}}$, where $\ell \geqslant 0$, $0 \leqslant i_1 < \cdots < i_\ell \leqslant m-3$, and

where the tuple $(i_1, \ldots, i_\ell)$ does not contain any consecutive integers. This generalizes a similar description mentioned in [2] for $q = 2$. The polynomials $P_m(T)$ are somewhat sparse: using induction one obtains that the number of terms occurring in $P_m(T)$ is equal to the m^{th} Fibonacci number which is roughly equal to $\left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right)^m / \sqrt{5}$. Finally note that as a consequence of Theorems 2.3 and 2.5, we deduce that $P_m(T)$ has simple roots only, all of which lie in $\mathbb{F}_{q^m}$.

In the next section, we will study quintic polynomials with coefficients in $\mathbb{F}_{2^m}$, with m a positive integer. In particular, we will encounter quintic polynomials of the form $x^5 + x + f$ with $f \in \mathbb{F}_{2^m}$. If m is even, we now know that there exactly $\lfloor 2^m/60 \rfloor$ values of $f \in \mathbb{F}_{2^m}$ such that $x^5 + x + f$ splits completely over $\mathbb{F}_{2^m}$. We finish this section by investigating what happens if m is odd.

Proposition 2.8. *Let m be an odd, positive integer and $f \in \mathbb{F}_{2^m}$. Then the polynomial $x^5 + x + f$ does not split completely over $\mathbb{F}_{2^m}$.*

Proof. Let us write $m = 2n + 1$. We use the same approach as in the proof of Theorem 2.7. In particular, write $p(x) := x^5 + x + f$ and $t := x + \langle p(x) \rangle \in \mathbb{F}_{2^m}[x]/\langle p(x) \rangle$. First of all, note that for $f = 0$, the polynomial $p(x)$ does not split completely, so we may assume $f \neq 0$. Similarly as in the proof of Theorem 2.7, we obtain that

$$t^{2^{2n}} = t^{4^n} = \frac{a_n t + c_n}{b_n t + d_n}, \quad \text{with} \quad \begin{pmatrix} a_n & c_n \\ b_n & d_n \end{pmatrix} = B_n = \begin{pmatrix} 1 & f^{q^{n-1}} \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & f \\ 1 & 0 \end{pmatrix}.$$

Hence

$$t^{2^m} = \left(\frac{a_n t + c_n}{b_n t + d_n}\right)^2 = \frac{a_n^2 t^2 + c_n^2}{b_n^2 t^2 + d_n^2}.$$

By Theorem 2.3, $p(x)$ splits over $\mathbb{F}_{2^m}$ if and only if $t^{2^m} = t$. This would imply $a_n^2 t^2 + c_n^2 = b_n^2 t^3 + d_n^2 t$ or equivalently $a_n^2 x^2 + c_n^2 + b_n^2 x^3 + d_n^2 x \in \langle p(x) \rangle$. Since $\deg p(x) = 5 > 3$, this implies $a_n = b_n = c_n = d_n = 0$, which is impossible since $a_n d_n - b_n c_n = \det B_n = f^{q^{n-1}+\cdots+1} \neq 0$. □

3 Simplifying Tschirnhaus transformations

In this section we explain an algorithm finding the five roots of a quintic polynomial $p(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + f \in \mathbb{F}_{2^m}[x]$, assuming that m is even and that $p(x)$ splits completely over $\mathbb{F}_{2^m}$. The algorithm will use a lookup table of size $\lfloor 2^m/60 \rfloor$. If the input polynomial is a quintic polynomial that does not split over $\mathbb{F}_{2^m}$, the procedure will detect this, but not return any of its roots. Note that we may assume that $m \geqslant 3$, since otherwise the field size is so small that no quintic polynomial can have five distinct roots in it.

The first step of the algorithm puts the input polynomial in a preliminary normal form, implying that we may assume that either $b = c = 0$ or that we already know a root of $p(x)$.

Lemma 3.1. *Let $p(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + f \in \mathbb{F}_{2^m}[x]$. If $c = 0$, let $y = x + b$. Then $p(x) = 0$ if and only if*

$$y^5 + dy^2 + (e + b^4)y + (b^2d + be + f) = 0.$$

If $c \neq 0$ and $p(d/c) \neq 0$ let $y = \frac{1}{x+d/c} + \frac{p'(d/c)}{p(d/c)}$. Then $p(x) = 0$ if and only if

$$y^5 + \frac{c}{p(d/c)}y^2 + \left(\frac{p'(d/c)^4}{p(d/c)^4 + \frac{b+d/c}{p(d/c)}}\right)y + \left(\frac{cp'(d/c)^3}{p(d/c)^3} + \frac{(b + d/c)p'(d/c)}{p(d/c)^2} + 1\right) = 0.$$

Proof. Follows by direct computation. □

If $p(x) = x^5 + f$, then $y = x$ in Lemma 3.1 and the resulting equation in y is just $y^5 + f$. To deal with this type of equation, one could use one of the already known algorithms for computing fifth roots (e.g. [1],[7]). For some situations this might be preferable, but we will show how to deal with these polynomials without having to resort to these algorithms, increasing the size of the lookup table with at most three entries. Note that if 5 divides $2^m - 1$, which happens if and only if m is a multiple of 4, many splitting polynomials of the form $x^5 + f$ exist, namely $(2^m - 1)/5$, while we are aiming for a lookup table of size $\lfloor 2^m/60 \rfloor$. We use a simple trick to deal with polynomials of this form.

Lemma 3.2. *Let $p(x) = x^5 + f$ and suppose that $f \neq 1$. If $y = x/(x + 1) + f/(f + 1)$, then $p(x) = 0$ if and only if*

$$y^5 + \frac{f(f^2 + f + 1)}{(f + 1)^4}y + \frac{f^2}{(f + 1)^2} = 0.$$

Proof. This follows from direct computation. □

If $f^3 \neq 1$, the resulting polynomial is of the form $X^5 + EX + F$ with $E \neq 0$. Lemma 3.1 does not cover the case where $c \neq 0$ and $p(d/c) = 0$, but of course in this case, $p(x)$ has the root d/c. After factoring out the term $x + d/c$, one is left with a quartic polynomial, for which fast root finding techniques are available already in the literature (see the references given in the introduction). In the remaining cases Lemma 3.1 implies that $p(x)$ can be transformed in a polynomial of the form $y^5 + Dy^2 + Ey + F$. If $D = 0$, then we either assume that $p(x) = x^5 + \alpha$, with $\alpha^3 = 1$, or that $E \neq 0$. The complexity of computing the transformed polynomial is is a constant number of operations and in particular does not depend on m.

Lemma 3.3. *Let $p(x) = x^5 + dx^2 + ex + f \in \mathbb{F}_{2^m}[x]$. If $e \neq 0$, let $y = e^{-1/4}x$. Then $p(x) = 0$ if and only if*

$$y^5 + de^{-3/4}y^2 + y + e^{-5/4}f = 0.$$

Proof. Follows by direct computation. □

If $e \neq 0$, a fourth root of e needs to be computed. Since we are working in $\mathbb{F}_{2^m}$, such a root is uniquely determined and given by $e^{1/4} = e^{2^{m-2}}$. Computing $e^{1/4}$ can therefore be done in at most $m-2$ operations using repeated squaring. Faster is to use a normal basis to represent the elements of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. In this case computing $e^{1/4}$ has a constant cost. However, for simplicity we will not use this observation. Yet another possibility is to use fast modular composition of functions of the form $h(t) = z^{2^t}$. Since $h(h(t)) = z^{2^{2t}}$, this approach gives rise to an algorithm capable of computing $e^{1/4}$ in complexity $O(\log(m))$.

Combining the above lemmas, we obtain the following.

Proposition 3.4. *Let $p(x) = x^5 + bx^4 + cx^3 + dx^2 + ex + f \in \mathbb{F}_{2^m}[x]$ and assume that $p(x)$ splits completely over $\mathbb{F}_{2^m}$. We can reduce the problem of finding all 5 roots of $p(x)$ using $O(m)$ operations in $\mathbb{F}_{2^m}$ to the problem of finding all roots of a polynomial $q(x) \in \mathbb{F}_{2^m}[x]$ that splits completely over $\mathbb{F}_{2^m}$ and additionally satisfies one of the following conditions:*

(i) $\deg q(x) = 4$, *or*

(ii) $q(x) = x^5 + \alpha$, *with* $\alpha^3 = 1$, *or*

(iii) $q(x) = x^5 + Dx^2 + x + F$ *for certain* $D, F \in \mathbb{F}_{2^m}$, *or*

(iv) $q(x) = x^5 + Dx^2 + F$ *for certain* $D, F \in \mathbb{F}_{2^m}$, $D \neq 0$.

In case (i) an algorithm to find the roots of a quartic polynomial will need to be used as for example given in [2] or [6]. These algorithms use at most $O(m)$ operations in $\mathbb{F}_{2^m}$.

In case (ii), the polynomial $q(x)$ splits completely over $\mathbb{F}_{2^m}$ if and only if m is a multiple of 4. Indeed if $q(x)$ splits, $\mathbb{F}_{2^m}$ contains all fifth roots of unity, that is 5 divides $2^m - 1$. This implies that m is a multiple of 4. Conversely, if m is a multiple of 4, then 15 divides $2^m - 1$. Hence any α satisfying $\alpha^3 = 1$ is a fifth power in $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^m}$ contains all fifth roots of unity. This implies that the polynomials $p(x)$ split completely over $\mathbb{F}_{2^m}$. Hence case (ii) only occurs if m is a multiple of 4.

In case (iii), the case that $D = F$ cannot occur, since otherwise $q(x)$ has 1 as multiple root. The case that $F = 0$ can also easily be dealt with, since in that case $q(x)$ has root 0 and the remaining roots are the roots of the quartic polynomial $x^4 + Dx + 1$. Therefore we may assume from now on that in case (iii) $F \neq 0$ and $D \neq F$.

Similarly, in case (iv), $F \neq 0$, since otherwise 0 is a multiple root. Therefore we assume from now on that in case (iv) $DF \neq 0$.

The polynomials in cases (iii) and (iv) above, still contain two parameters D and F, but it turns out that if m is even, algebraic transformations called Tschirnhaus transformations, can be used to eliminate a further parameter. Such transformations were introduced in 1683 [13] by E.W. von Tschirnhaus (see [10] for a translation into English). We give a brief overview of this method applied to quintic polynomials. If $p(x) \in \mathbb{F}_{2^m}[x]$ is a monic, quintic polynomial with roots $x_1, \ldots, x_5$, then the coefficients of $p(x)$ are the elementary symmetric polynomials in $x_1, \ldots, x_5$. A Tschirnhaus transformation of $p(x)$ is obtained by finding the monic, quintic polynomial $q(y) \in \mathbb{F}_{2^m}[y]$ whose roots are the five quantities $y_1, \ldots, y_5$, where $y_i := x_i^4 + g_3 x_i^3 + g_2 x_i^2 + g_1 x_i + g_0$ and $g_0, \ldots, g_4$ are chosen elements from $\mathbb{F}_{2^m}$. The idea is to try to choose $g_0, \ldots, g_4$ in such a way that the polynomial $q(y)$ has less nonzero coefficients than $p(x)$. The coefficients

of $q(y)$ are the elementary symmetric polynomials in $y_1, \dots, y_5$ and hence symmetric polynomials in $x_1, \dots, x_5$. This means that the coefficients of $q(y)$ can be expressed in the coefficients of $p(x)$, which can be done easily for example using a computer. We say that $q(y)$ is the Tschirnhaus transform of $p(x)$ with respect to the transformation $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$. If the roots of $q(y)$ are known, the roots of $p(x)$ can be computed. One straightforward, but somewhat naive, approach is to use the relation $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$ and to solve a quartic equation for each root of $q(y)$, but usually it is possible to use the equations $p(x) = 0$ and $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$ to express x as a linear combination of powers of y. In these cases, we can find the inverse Tschirnhaus transformation. Then the roots of $p(x)$ can directly be computed from those of $q(y)$.

We now indicate how to choose $g_0, \dots, g_3$ for the families of quintic polynomials from Proposition 3.4 in such a way that the resulting Tschirnhaus transform is of the form $y^5 + y + F$ or $y^5 + F$.

Proposition 3.5. *Let $p(x) = x^5 + dx^2 + x + f \in \mathbb{F}_{2^m}$ and assume $df(d+f) \neq 0$. Suppose that $g_0, \dots, g_3$ are chosen such that*

$$g_2 = \frac{f}{d}, \quad g_3^2 + \frac{(d+f)^2}{d^3}g_3 + \frac{f}{d} = 0, \quad g_0 = dg_3, \quad g_1 = d + g_3\frac{f}{d},$$

then the Tschirnhaus transform of $p(x)$ with respect to $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$ is given by $q(y) = y^5 + Ey + F$, with

$$E = \frac{(d+f)^8}{d^{13}}\left((d^3f + d^2 + f^2)g_3 + d^2(d^3 + f)\right)$$

and

$$F = \frac{(d+f)^{10}}{d^{17}}\left((d^5f + d^4 + f^4)g_3 + (d+f)^2d^2f\right).$$

Moreover, the inverse Tschirnhaus transformation is given by

$$x = \frac{d^6(d+f)^2g_3 + d^3(d^5f + d^4 + f^4)}{f^2(d+f)^6}y^3 + \frac{d^4g_3 + d(d^3f + d^2 + f^2)}{f^2(d+f)^2}y.$$

Proof. Let us denote by $q(y) = y^5 + \beta y^4 + \gamma y^3 + \delta y^2 + \varepsilon y + \zeta$ the Tschirnhaus transform of $p(x)$ with respect to the transformation $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$. A direct, but lengthy, computation shows that

$$\beta = g_3d + g_0 \quad \text{and} \quad \gamma = d^2g_3^2 + (d + fg_2)g_3 + d^2g_2 + (dg_2 + f)g_1.$$

Choosing g_2, g_3, g_0 such that $g_2 = f/d$, $d^2g_3^2 + (d + fg_2)g_3 + d^2g_2 = 0$ and $g_0 = dg_3$, we make sure that $\beta = \gamma = 0$. Moreover, with these choices, we obtain that:

$$\delta = (dg_1 + d^2 + fg_3)(g_1^2 + g_3^2 + (d^5 + d^2f + f^3)/d^3).$$

Hence the first part of the lemma follows. The expressions for E, F and the inverse Tschirnhaus transformation, can easily be verified using a computer. Indeed consider

the ideal $\langle x^5 + dx^2 + x + f, y + x^4 + g_3x^3 + g_2x^2 + g_1x + g_0\rangle \subset \mathbb{F}_{2^m}(d, f, g_3)[x, y]$, where d and f are considered independent transcendental elements over $\mathbb{F}_{2^m}$ and g_3 satisfies the quadratic equation given in the proposition. Computing a Gröbner basis of this ideal with respect to the lexicographic order $\prec$ such that $y \prec x$, one obtains precisely the polynomial $y^5 + Ey + F$ and the inverse Tschirnhaus transformation. □

Similarly one obtains the following.

Proposition 3.6. *Let $p(x) = x^5 + dx^2 + f \in \mathbb{F}_{2^m}$ and assume $df \neq 0$. Suppose that $g_0, \ldots, g_3$ are chosen such that*

$$g_2 = \frac{f}{d}, \quad g_3^2 + \frac{f^2}{d^3}g_3 + \frac{f}{d} = 0, \quad g_0 = dg_3, \quad g_1 = d + g_3\frac{f}{d},$$

then the Tschirnhaus transform of $p(x)$ with respect to $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$ is given by $q(y) = y^5 + Ey + F$, with

$$E = \frac{f^8}{d^{10}}\left(fg_3 + d^2\right)$$

and

$$F = \frac{f^{11}}{d^{17}}\left((d^5 + f^3)g_3 + d^2f^2\right).$$

Moreover, the inverse Tschirnhaus transformation is given by

$$x = \frac{d^6fg_3 + d^3(d^5 + f^3)}{f^7}y^3 + \frac{d^4}{f^3}y.$$

Proof. The proof is very similar to that of Proposition 3.5. Let $q(y) = y^5 + \beta y^4 + \gamma y^3 + \delta y^2 + \varepsilon y + \zeta$ the Tschirnhaus transform of $p(x)$ with respect to the transformation $y = x^4 + g_3x^3 + g_2x^2 + g_1x + g_0$. Then

$$\beta = g_3d + g_0 \quad \text{and} \quad \gamma = d^2g_3^2 + fg_2g_3 + d^2g_2 + (dg_2 + f)g_1.$$

Choosing g_2, g_3, g_0 such that $g_2 = f/d$, $d^2g_3^2 + fg_2g_3 + d^2g_2 = 0$ and $g_0 = dg_3$, we make sure that $\beta = \gamma = 0$. Moreover, we obtain that:

$$\delta = (dg_1 + d^2 + fg_3)(g_1^2 + (d^5 + f^3)/d^3).$$

Hence the first part of the lemma follows. The expressions for E, F and the inverse Tschirnhaus transformation, can easily be obtained performing a Gröbner basis computation. □

The choice of especially g_2 in Propositions 3.5 and 3.6 is a clever trick used in the classical study of quintic polynomials over the complex numbers, e.g. [5]. The point is that because of this choice, the expression for γ in the proof of the propositions, reduces to a polynomial in the variable g_3 only, giving the key to the choice of the other variables in the Tschirnhaus transformation. However, we cannot be sure that the two possible values of g_3 lie in $\mathbb{F}_{2^m}$. Fortunately, this turns out to be the case if we assume both that m is even and that the polynomial $p(x)$ splits completely over $\mathbb{F}_{2^m}$.

Lemma 3.7. *Let $d, f \in \mathbb{F}_{2^m} \setminus \{0\}$ and suppose that m is even. If the polynomial $x^5 + dx^2 + x + f$ splits completely in $\mathbb{F}_{2^m}$, then the equation $g_3^2 + \frac{(d+f)^2}{d^3} g_3 + \frac{f}{d} = 0$ has two solutions in $\mathbb{F}_{2^m}$. If the polynomial $x^5 + dx^2 + f$ splits completely in $\mathbb{F}_{2^m}$, then the equation $g_3^2 + \frac{f^2}{d^3} g_3 + \frac{f}{d} = 0$ has two distinct solutions in $\mathbb{F}_{2^m}$.*

We postpone the proof of this lemma to the appendix. Now that we know that the two possibilities for g_3 are in $\mathbb{F}_{2^m}$, we have a choice of which g_3 to pick. In Proposition 3.5, the sum of the two possibilities for g_3 equals $(d + f)^2/d^3$, in Proposition 3.6 f^2/d^3. It is then easy to see that in either proposition, we can always choose g_3 such that in the resulting transformed equation $y^5 + Ey + F$, the coefficient E is not zero. Using a similar scaling trick as in Lemma 3.3, we then obtain the following.

Theorem 3.8. *Let $p(x) = x^5 + dx^2 + x + f$ or $p(x) = x^5 + dx^2 + f$ be a polynomial that splits completely in $\mathbb{F}_{2^m}$ and assume that $df \neq 0$ and m is even. Then there exists an invertible Tschirnhaus transformation such that the transformed polynomial is of the form $y^5 + y + F$ for some $F \in \mathbb{F}_{2^m}$.*

Once the transformed polynomial of the form $y^5 + y + F$ is obtained, a simple table lookup in the table of all completely splitting polynomials of the form $x^5 + x + f$ allows one to determine whether or not $x^5 + x + F$ occurs in the table. If yes, the roots of the transformed polynomial $x^5 + x + F$ can be read off and using the inverse transformations, the roots of $p(x)$ can be computed. If $x^5 + x + F$ does not occur in the table, the original polynomial $p(x)$ did not split completely. Using a binary search tree, the table lookup can be done in complexity $O(m)$, since we have seen in Corollary 2.6 that the table size is $\lfloor 2^m/60 \rfloor$, since there are precisely that many completely splitting polynomials of the form $x^5 + x + f$ over $\mathbb{F}_{2^m}$.

Remark 3.9. The assumption the m is even in the above theorem is essential. Indeed, assume that m is odd, $p(x)$ splits completely, and g_3 could be chosen from $\mathbb{F}_{2^m}$. Then Theorem 3.8 would imply that there exists a polynomial of the form $x^5 + x + F \in \mathbb{F}_{2^m}[x]$ that splits completely over $\mathbb{F}_{2^m}$. This is a contradiction with Proposition 2.8. If m is odd, it is clear that g_3 can be chosen from the field $\mathbb{F}_{2^{2m}}$, yielding $x^5 + x + F \in \mathbb{F}_{2^{2m}}[x]$. However, there are $\lfloor 2^{2m}/60 \rfloor$ completely splitting polynomials of this form. Experiments for small m (see [14]) suggest that roughly half of these are obtained by transforming totally splitting polynomials $p(x)$ over $\mathbb{F}_{2^m}$. Therefore for odd m, the above approach still works to some extent, but one is forced to work over the larger field $\mathbb{F}_{2^{2m}}$ when transforming the polynomial and the roots, and the size of the lookup table seems to become roughly $2^{2m}/120$, which is much larger than what is needed for even m.

Example 3.10. To illustrate the algorithm described above, we give a small example for the field $\mathbb{F}_{2^8}$. We write the nonzero elements of $\mathbb{F}_{2^8}$ as a power of a primitive element a satisfying $a^8 = a^4 + a^3 + a^2 + 1$. In this case the lookup table contains seven polynomials. Three of them are of the form $x^5 + f$ with $f^3 = 1$, while the remaining four are of the form $x^5 + x + f$ with $f^4 + f + 1 = 0$ (see Theorem 2.7).

POLYNOMIAL	ROOTS
$x^5 + 1$	$1, a^{51}, a^{102}, a^{153}, a^{204}$
$x^5 + a^{85}$	$a^{17}, a^{68}, a^{119}, a^{170}, a^{221}$
$x^5 + a^{170}$	$a^{34}, a^{85}, a^{136}, a^{187}, a^{238}$
$x^5 + x + a^{17}$	$a^{43}, a^{136}, a^{175}, a^{178}, a^{250}$
$x^5 + x + a^{34}$	$a^{17}, a^{86}, a^{95}, a^{101}, a^{245}$
$x^5 + x + a^{68}$	$a^{34}, a^{172}, a^{190}, a^{202}, a^{235}$
$x^5 + x + a^{136}$	$a^{68}, a^{89}, a^{125}, a^{149}, a^{215}$

Now as an example, consider the polynomial

$$p(x) := x^5 + a^{14}x^4 + a^{91}x^3 + a^{202}x^2 + a^5x + a^{89}.$$

Lemma 3.1 applies with the case that $c \neq 0$ and $p(d/c) \neq 0$. Therefore we first use the substitution $y = \frac{1}{x+a^{111}} + a^{130}$ (with inverse substitution $x = \frac{1}{y+a^{130}} + a^{111}$.) Then $p(x) = 0$ if and only if

$$p_1(y) := y^5 + a^{145}y^2 + a^{115}y + a^{107} = 0.$$

Therefore we now continue the algorithm with the polynomial $p_1(x)$. Applying the transformation $y = a^{35}x$ from Lemma 3.3 to $p_1(x)$, we obtain the transformed polynomial

$$p_2(y) := y^5 + a^{250}y^2 + y + a^{27}.$$

We continue the algorithm with $p_2(x)$.

At this point the Tschirnhaus transformation begins to play a role. Applying Proposition 3.5 to $p_2(x)$, we obtain that $g_2 = a^{32}$ and that g_3 needs to satisfy $g_3^2 + a^{75}g_3 + a^{32} = 0$. As predicted by Lemma 3.7, this equation has two solutions in $\mathbb{F}_{2^8}$ which turn out to be a^{47} and a^{240}. We choose $g_3 = a^{47}$. Then we obtain $g_0 = a^{42}$ and $g_1 = a^{35}$. Hence the Tschirnhaus transformation that we need to use is $y = x^4 + a^{47}x^3 + a^{32}x^2 + a^{35}x + a^{42}$. The inverse Tschirnhaus transformation is $x = a^{201}y^3 + a^{126}y$ and the transformed polynomial is

$$p_3(y) := y^5 + a^{135}y + a^{241}.$$

Finally applying Lemma 3.3 again to $p_3(x)$ with the transformation $y = a^{30}x$, we obtain

$$p_4(y) := y^5 + y + a^{136},$$

which is the seventh polynomial on the lookup table.

Now we simply calculate the roots of $p(x)$ starting with those of $p_4(x)$ from the lookup table and then working our way backwards using the inverse transformations:

POLYNOMIAL	TRANSFORMATION	ROOTS
$p_4(x) = x^5 + x + a^{136}$		$a^{68}, a^{89}, a^{125}, a^{149}, a^{215}$
$p_3(x) = x^5 + a^{135}x + a^{241}$	$x \to a^{225}x$	$a^{38}, a^{59}, a^{95}, a^{119}, a^{185}$
$p_2(x) = x^5 + a^{250}x^2 + x + a^{27}$	$x \to a^{201}x^3 + a^{126}x$	$a^{87}, a^{213}, a^{242}, a^{97}, a^{153}$
$p_1(x) = x^5 + a^{145}x^2 + a^{115}x + a^{107}$	$x \to a^{220}x$	$a^{52}, a^{178}, a^{207}, a^{62}, a^{118}$
$p(x) = x^5 + a^{14}x^4 + a^{91}x^3 + a^{202}x^2 + a^5x + a^{89}$	$x \to \frac{1}{x+a^{130}} + a^{111}$	$1, a, a^{13}, a^{18}, a^{57}$

Hence we conclude that $p(x)$ splits completely and has roots $1, a, a^{13}, a^{18}, a^{57}$.

Remark 3.11. It is possible to reduce the size of the lookup table somewhat more using the Frobenius map. More precisely, if $x^5 + x + f$ is a polynomial in the lookup table and $f \notin \mathbb{F}_2$, then $x^5 + x + f^2$ is also in the table and the roots can easily be obtained by taking the squares of the roots of the first polynomial. A similar remark applies to polynomials in the table of the form $x^5 + f$. Hence the table can be compressed somewhat by only choosing representatives of orbits arising under the action of the Frobenius map. In the previous example, one can in this way reduce the size of the lookup table from seven to three. Indeed, the polynomials $x^5 + a^{85}, x^5 + a^{170}$ form one orbit as do the polynomials $x^5 + x + a^{17}, x^5 + x + a^{34}, x^5 + x + a^{68}, x^5 + x + a^{136}$. In general on may expect a reduction by a factor roughly m of the size of the lookup table.

4 Acknowledgements

We would like to thank Søren Forchhammer and Knud J. Larsen from DTU Photonics for bringing the problem of finding the roots of a degree five error-locator polynomial to our attention. This lead to the bachelor thesis of the second author on which this article is based [14]. The authors would also like to thank the referees of this paper for valuable suggestions and comments. Finally, we would like to acknowledge the support from The Danish Council of Scientific Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B.

5 Appendix: proof of Lemma 3.7

Now we give the proof of Lemma 3.7.

Proof. Write $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. We will show that the roots of the polynomial $t^2 + \frac{(d+f)^2}{d^3}t + \frac{f}{d}$ can be expressed in terms of α and the roots of the polynomial $x^5 + dx^2 + x + f$. This will immediately imply that $g_3 \in \mathbb{F}_{2^m}$ if m is even and $p(x)$ splits completely over $\mathbb{F}_{2^m}$. What we will do is to treat d and f as algebraically independent transcendental variables, consider $p(x)$ as polynomial with coefficients in $\mathbb{F}_4(d, f)$ and then to study the splitting field of $p(x)$. We will show that an element ρ_3 in this splitting field exists such that $\rho_3^2 + \frac{(d+f)^2}{d^3}\rho_3 + \frac{f}{d} = 0$. We start with the field $\mathbb{F}_4(d, f)$. Let $x_1, \ldots, x_5$ denote

the five roots of $x^5 + dx^2 + x + f$ in an algebraic closure of $\mathbb{F}_4(d, f)$. Note that $p(x)$ has 5 distinct roots viewed as a polynomial in $\mathbb{F}_4(d, f)[x]$, since its derivative is $x^4 + 1$ and 1 is not a root of $p(x)$. Since the polynomial $p(x)$ is irreducible as element of $\mathbb{F}_4(d, f)[x]$, the extension $\mathbb{F}_4(d, f, x_1)/\mathbb{F}_4(d, f)$ has degree five. However, there is no need yet to deal with extensions, since the equation $f = x_1^5 + dx_1^2 + x_1$ implies that $\mathbb{F}_4(d, f, x_1) = \mathbb{F}_4(d, x_1)$. Seen as element of $\mathbb{F}_4(d, x_1)[x]$, the polynomial $p(x)$ factors into irreducibles as follows

$$p(x) = (x - x_1)(x^4 + x_1x^3 + x_1^2x^2 + (x_1^3 + d)x + x_1^4 + dx_1 + 1).$$

This means that the extension $\mathbb{F}_4(d, x_1, x_2)/\mathbb{F}_4(d, x_1)$ has degree 4, but since $x_2^4 + x_1x_2^3 + x_1^2x_2^2 + (x_1^3 + d)x_2 + x_1^4 + dx_1 + 1 = 0$, d can be expressed in x_1 and x_2. Therefore we have $\mathbb{F}_4(d, x_1, x_2) = \mathbb{F}_4(x_1, x_2)$, which is a more convenient description for doing calculations. The polynomial $p(x)$ seen as element of $\mathbb{F}_4(x_1, x_2)[x]$ factors into irreducibles in the following way:

$$p(x) = (x - x_1)(x - x_2) \left(x^3 + (x_2 + x_1)x^2 + (x_2^2 + x_1x_2 + x_1^2)x + \frac{x_1x_2^3 + x_1^2x_2^2 + x_1^3x_2 + 1}{x_2 + x_1}\right).$$

We obtain that $\mathbb{F}_4(x_1, x_2, x_3)/\mathbb{F}_4(x_1, x_2)$ is an algebraic extension of degree 3. The final step comes from the factorization of $p(x)$ as element in $\mathbb{F}_4(x_1, x_2, x_3)[x]$

$$p(x) = (x - x_1)(x - x_2)(x - x_3) \left(x^2 + (x_3 + x_2 + x_1)x + x_3^2 + x_2x_3 + x_1x_3 + x_2^2 + x_1x_2 + x_1^2\right).$$

We have now described the splitting field of $p(x)$ as algebraic extension of degree six of $\mathbb{F}_4(x_1, x_2)$, where x_1 and x_2 can be viewed as independent transcendental variables. Using this description, it is computationally very simple to factor the polynomial $s(t) := t^2 + \frac{(d+f)^2}{d^3}t + \frac{f}{d}$ viewed as polynomial in the variable t and coefficients in $\mathbb{F}_4(x_1, x_2, x_3, x_4)$. Using the Magma computer algebra package, one finds that the polynomial $s(t)$ has two roots in $\mathbb{F}_4(x_1, x_2, x_3, x_4)$. One of these roots ρ_3 satisfies

$$\begin{aligned} d^3\rho_3 = &\frac{(x_1 + 1)^4(x_2 + 1)^4}{x_2 + x_1}\left(x_3^2 + x_2^2 + x_2x_1 + x_1^2\right)x_4 + (x_1 + 1)^4(x_2 + 1)^4x_3^2 \\ &+ \frac{(x_1^5 + x_1)(x_2^5 + x_2)}{x_2 + x_1}x_3 \\ &+ \frac{x_1x_2^{12} + x_1^2x_2^{11} + \alpha^2(x_1^4 + 1)x_2^9 + \alpha(x_1^5 + x_1)x_2^8 + \alpha(x_1^6 + x_1^2)x_2^7}{(x_2 + x_1)^3} \\ &+ \frac{\alpha^2(x_1^7 + x_1^3)x_2^6 + (\alpha^2x_1^8 + \alpha x_1^4 + 1)x_2^5 + (\alpha x_1^9 + \alpha^2x_1^5)x_2^4 + (\alpha x_1^6 + \alpha^2x_1^2)x_2^3}{(x_2 + x_1)^3} \\ &+ \frac{(x_1^{11} + \alpha^2x_1^7 + \alpha x_1^3)x_2^2 + (x_1^{12} + \alpha^2x_1^8 + \alpha)x_2 + (\alpha x_1^9 + x_1^5 + \alpha^2x_1)}{(x_2 + x_1)^3}. \end{aligned}$$

For a specific choice of $d, f \in \mathbb{F}_{2^m}$ such that $d \neq 0$ and $p(x)$ (now again seen as polynomial in $\mathbb{F}_{2^m}[x]$) splits completely over $\mathbb{F}_{2^m}$, then the found expression for ρ_3

can be evaluated for those d, f and resulting $x_1, \ldots, x_5$. Even though we do not know $x_1, \ldots, x_5$ explicitly, we do know from the assumption that $p(x)$ splits completely for our choice of d and f, that all of its roots $x_1, \ldots, x_5$ are in $\mathbb{F}_{2^m}$ and that $x_1 + x_2 \neq 0$. Therefore the evaluation of ρ_3 yields a value g_3 in $\mathbb{F}_{2^m}$. Moreover, since ρ_3 was a root of $s(t)$, the obtained value g_3 is a root of $t^2 + \frac{(d+f)^2}{d^3}t + \frac{f}{d}$. This is exactly what we wanted to show. Exactly the same approach works for the case $x^5 + dx^2 + f$, but we leave the details to the reader. □

References

[1] P.S.L.M. Barreto and J.F. Voloch. Efficient computation of roots in finite fields. *Designs, Codes and Cryptography* 39(2), pp. 275–280, 2006.

[2] E. Berlekamp, H. Rumsey, and G. Solomon. Solutions of algebraic equations over fields of characteristic 2. *JPL Space Programs Summary* No. 37-39, Vol. IV, pp. 219–226, 1966.

[3] E. Berlekamp, H. Rumsey, and G. Solomon. Solutions of algebraic equations over finite fields. *Information and Control* 10, pp. 553–564, 1967.

[4] A.W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields and Their Applications* 10, pp. 285–305, 2004.

[5] E.S. Bring. *Meletemata quaedam mathematematica circa transformationem æquationum algebraicarum.* Lund University, Promotionschrift, 1786.

[6] C.-L. Chen. Formulas for the solutions of quadratic equations over GF(2^m). *IEEE Transactions on Information Theory* 28(5), pp. 792–794, 1982.

[7] J. Doliskani and É. Schost. Taking roots over high extensions of finite fields. *Mathematics of Computation* 83(285), pp. 435–446, 2014.

[8] S.V. Fedorenko and P.V. Trifonov. Finding roots of polynomials over finite fields. *IEEE Transactions on Communications* 50(11), pp. 1709–1711, 2002.

[9] S. Gravano. Decoding the triple-error-correcting (15,5) binary BCH code by the analytic solution of the cubic error-locator polynomial over GF(2^4). *International Journal of Electronics Theoretical and Experimental*, 68(2), pp. 175–180, 1990.

[10] R.F. Green. A method for removing all intermediate terms from a given equation. (Translation of: E.W. von Tschirnhaus. Methodus auferendi omnes terminos intermedios ex data æquatione. *Acta Eruditorum*, pp. 204–207, 1683.) *ACM SIGSAM Bulletin* 37(1), pp. 1–3, 2003.

[11] H. Okano and H. Imai. A construction method of high-speed decoders using ROMs for Bose–Chaudhuri–Hocquenghem and Reed–Solomon codes. *IEEE Transactions on Computers* 36(10), pp. 1165–1171, 1987.

[12] T.-K. Truong, J.-H. Jeng, and I.S. Reed. Fast algorithm for computing the roots of error locator polynomials up to degree 11 in Reed–Solomon decoders. *IEEE Transactions on Communications* 49(5), pp. 779–783, 2001.

[13] E.W. von Tschirnhaus. Methodus auferendi omnes terminos intermedios ex data æquatione. *Acta Eruditorum*, pp. 204–207, 1683.

[14] E.A. Wrisberg. *Algebraic structure of low degree polynomials*. Bachelor thesis, Technical University of Denmark (DTU), 2017.