

A search for c-Wieferich primes

Alex Samuel Bamunoba*

*Department of Mathematics, Makerere University
P. O. Box 7062, Kampala, Uganda
bamunoba@cns.mak.ac.ug*

Jonas Bergström

*Department of Mathematics, Stockholm University
SE-106 91, Stockholm, Sweden
jonasb@math.su.se*

Received 31 December 2019

Revised 19 November 2020

Accepted 20 November 2020

Published 29 December 2020

Let q be a power of a prime number p , $\mathbb{F}_q$ be a finite field with q elements and $\mathcal{G}$ be a subgroup of $(\mathbb{F}_q, +)$ of order p . We give an existence criterion and an algorithm for computing maximally $\mathcal{G}$ -fixed c-Wieferich primes in $\mathbb{F}_q[T]$. Using the criterion, we study how c-Wieferich primes behave in $\mathbb{F}_q[T]$ extensions.

Keywords: c-Wieferich primes; $\mathcal{G}$ -fixed polynomials; Artin–Schreier polynomials; Carlitz module.

Mathematics Subject Classification 2020: 11A99, 12E05

1. Introduction

Let p be a prime number, $q = p^m$ for some $m \in \mathbb{Z}_{\geq 1}$, $\mathbb{F}_q$ be a finite field of q elements and T be an indeterminate. Let $\mathcal{A} := \mathbb{F}_q[T]$ be the ring of polynomials in T defined over $\mathbb{F}_q$ and $\mathcal{A}_+$ be the set of monic polynomials in $\mathcal{A}$. We shall use the symbols $\mathcal{P}$ and $\mathcal{Q}$ to denote monic irreducible (also called prime) polynomials in $\mathcal{A}$. The symbol $\mathcal{Q}_d$ will denote any prime polynomial in $\mathcal{A}$ of degree d . For each $i \in \mathbb{Z}_{\geq 1}$, we let $[i] := T^{q^i} - T$ and $L_i := [i][i-1] \cdots [1]$. The symbol $[i]$ represents the product of all prime polynomials in $\mathcal{A}$ of degree dividing i while L_i represents the least common multiple of monic polynomials in $\mathcal{A}$ of degree i . We shall adopt the convention that, “the value of an empty product is 1” and therefore, set $[0] := 1 =: L_0$.

*Corresponding author.

This is an Open Access article published by World Scientific Publishing Company. It is distributed under the terms of the Creative Commons Attribution 4.0 (CC BY) License which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Let $\mathbf{k} := \mathbb{F}_q(T)$ be the field of fractions of $\mathcal{A}$, $\mathcal{K}$ be a fixed algebraic closure of $\mathbf{k}$ and $\tau : \mathcal{K} \rightarrow \mathcal{K}, \alpha \mapsto \alpha^q$ be the Frobenius $\mathbb{F}_q$ -automorphism of $\mathcal{K}$. Let $\mathbf{k}\{\tau\}$ be the polynomial ring in τ over $\mathbf{k}$ with multiplication satisfying the commutation relation $\tau\theta = \theta^q\tau$ for any $\theta \in \mathbf{k}$. It is clear that $\mathbf{k}\{\tau\}$ is an $\mathbb{F}_q$ -algebra, (sometimes called, the twisted polynomial ring over $\mathbf{k}$). Let $\mathcal{A}(\mathbf{k})$ be the set of additive polynomials over $\mathbf{k}$. Recall that, a polynomial $g \in \mathbf{k}[X]$ is said to be additive over $\mathbf{k}$ if $g(X+Y) = g(X) + g(Y)$ as a polynomial in $\mathbf{k}[X, Y]$. With the usual addition of polynomials in $\mathcal{A}(\mathbf{k})$ and multiplication given by composition of polynomial mappings, $\mathcal{A}(\mathbf{k})$ becomes a ring, called the ring of additive polynomials over $\mathbf{k}$. To each $G \in \mathbf{k}\{\tau\}$, we associate an element $g \in \mathcal{A}(\mathbf{k})$ defined by letting G act on the indeterminate X via τ . For example, if $G = \tau + T\tau^0$, then $g = (\tau + T\tau^0)X = X^q + TX$. This gives a bijection between $\mathbf{k}\{\tau\}$ and $\mathcal{A}(\mathbf{k})$.

The ring homomorphism $\rho : \mathcal{A} \rightarrow \mathbf{k}\{\tau\}$ characterized by $T \mapsto \tau + T\tau^0$ is called the Carlitz $\mathcal{A}$ -module homomorphism. This ring homomorphism is in fact a homomorphism of $\mathbb{F}_q$ -algebras. The mapping ρ is an $\mathcal{A}$ -module homomorphism because it induces a “new $\mathcal{A}$ -action” on $\mathcal{K}$ as follows: consider the mapping $* : \mathcal{A} \times \mathcal{K} \rightarrow \mathcal{K}$ defined by $(N, \alpha) \mapsto \rho^N \alpha$, where ρ^N is the Carlitz N -endomorphism over $\mathcal{A}$. Since to each $\rho^N \in \mathbf{k}\{\tau\}$, there is a corresponding additive polynomial $\rho_N(X)$, called the Carlitz N -polynomial (actually ρ^N is defined over $\mathcal{A}$, since the image of $\mathcal{A}$ under ρ is a subring of $\mathbf{k}\{\tau\}$). The action $*$ is equivalently defined as: $N * \alpha = \rho^N \alpha = \rho_N(\alpha)$, evaluating the polynomial $\rho_N(X)$ at α . We call the pair $(\rho, \mathcal{K}) =: \mathcal{C}(\mathcal{K})$, the Carlitz $\mathcal{A}$ -module (or Carlitzification of $\mathcal{K}$). The Carlitz $\mathcal{A}$ -module homomorphism ρ is the simplest example of a sign normalized rank one Drinfeld $\mathcal{A}$ -module. Technically, ρ can also be thought of as the functor from the category of $\mathcal{A}$ -algebras to the category of $\mathcal{A}$ -modules which sends an $\mathcal{A}$ -algebra $\mathcal{K}$ to the unique $\mathcal{A}$ -module $\mathcal{C}(\mathcal{K})$ which has $\mathcal{K}$ as the underlying Abelian group, and such that the (left) multiplication by T of an $\alpha \in \mathcal{K}$ is $\rho_T(\alpha) = \alpha^q + T\alpha$. For an introduction to the general theory of Drinfeld $\mathcal{A}$ -modules, see [3, 9, 12].

With this background, we are in a position to define the notion of c -Wieferich (or Carlitz–Wieferich) primes.

Definition 1.1. Let $a \in \mathcal{A} - \{0\}$. A prime polynomial $\mathcal{P}$ in $\mathcal{A}$ is said to be a c -Wieferich prime to base a if

$$\rho_{\mathcal{P}}(a) \equiv a^{q^{\deg(\mathcal{P})}} \pmod{\mathcal{P}^2}. \quad (1.1)$$

This notion of c -Wieferich primes was introduced in 1994 by Thakur [11]. In [13], Thakur showed that, if a is a p th power, (i.e. the derivative of a is 0), then (1.1) is equivalent to $\rho_{\mathcal{P}}(a) \equiv a \pmod{\mathcal{P}^2}$. Since for any N in $\mathcal{A}$, the Carlitz N -polynomial $\rho_N(X)$ is $\mathbb{F}_q$ -linear, it follows that the congruence $\rho_{\mathcal{P}}(a) \equiv a \pmod{\mathcal{P}^2}$ for any $a \in \mathbb{F}_q^\times$ is equivalent to $\rho_{\mathcal{P}-1}(1) \equiv 0 \pmod{\mathcal{P}^2}$. Therefore, a prime polynomial $\mathcal{P}$ in $\mathcal{A}$ is a c -Wieferich prime to base $\alpha \in \mathbb{F}_q^\times$ (or base 1) if $\rho_{\mathcal{P}-1}(1) \equiv 0 \pmod{\mathcal{P}^2}$. In this paper, the term “ c -Wieferich prime” will refer to a c -Wieferich prime to base 1. For example, $T^6 + T^4 + T^3 + T^2 + 2T + 2$, $T^9 + T^6 + T^4 + T^2 + 2T + 2$, $T^{12} + 2T^{10} + T^9 +$

$2T^4 + 2T^3 + T^2 + 1$ and $T^{15} + T^{13} + T^{12} + T^{11} + 2T^{10} + 2T^7 + 2T^5 + 2T^4 + T^3 + T^2 + T + 1$ are all *c*-Wieferich primes in $\mathbb{F}_3[T]$. These are the only *c*-Wieferich primes in $\mathbb{F}_3[T]$ of degree at most 60. However, in the case of $q = 2$, there is an anomolous behavior where all the prime polynomials in $\mathbb{F}_2[T] - \{T, T + 1\}$ are *c*-Wieferich primes. This is because $\rho_{\mathcal{P}-1}(1) = 0$ for any prime $\mathcal{P} \in \mathbb{F}_2[T]$ of degree at least 2.

Examples of *c*-Wieferich primes in $\mathbb{F}_q[T]$ (for $q \geq 3$) are quite rare and it is computationally intensive to use Definition 1.1 to find them. For this reason, we search for other conditions that can be used in order to gain more insight and be able to compute these objects. To achieve this, we need some extra notation. For each $n \in \mathbb{Z}_{\geq 0}$, let F_n denote the numerator of $\sum_{j=0}^n (-1)^j (L_j)^{-1}$ written as a rational polynomial without common factors. It is an easy exercise to show that the polynomials F_n are monic in $\mathcal{A}$ and solutions to the recurrence relation $F_0 = 1$, $F_i = (-1)^i + [i]F_{i-1}$, for $i = 1, 2, \dots$. For the proof, see [1, Lemma 4.2].

Proposition 1.2 ([1, Proposition 4.3]). *$\mathcal{P}$ is a *c*-Wieferich prime in $\mathcal{A}$ if and only if $F_{\deg(\mathcal{P})-1} \equiv 0 \pmod{\mathcal{P}}$.*

Proposition 1.2 was independently discovered by Thakur in his work on *c*-Wieferich primes, see [13]. The last three examples of *c*-Wieferich primes in $\mathbb{F}_3[T]$ listed on p. 2 were obtained using Proposition 1.2.

There is a link between *c*-Wieferich primes and the Carlitz-Goss zeta value at 1. To see this, let

$$\zeta_{\mathcal{A}}(1) := \sum_{a \in \mathcal{A}_+} \frac{1}{a} \quad \text{and} \quad \zeta_{\mathcal{A}, \mathcal{P}}(1) := \sum_{\substack{a \in \mathcal{A}_+ \\ (a, \mathcal{P})=1}} \frac{1}{a},$$

where $\zeta_{\mathcal{A}, \mathcal{P}}(1)$ is the Carlitz-Goss $\mathcal{P}$ -adic zeta value at 1. For $q > 2$, D. Thakur showed that, a prime $\mathcal{P} \in \mathcal{A}$ is a *c*-Wieferich prime if and only if $\mathcal{P}$ divides $\zeta_{\mathcal{A}, \mathcal{P}}(1)$ if and only if $\mathcal{P}^2$ divides $\zeta_{\mathcal{A}}(1)$, see [13, Theorem 5]. For the link between *c*-Wieferich primes and Mersenne primes, refer to [7].

Proposition 1.2 leads us to a naive algorithm for computing *c*-Wieferich primes.

Algorithm 1. Computing *c*-Wieferich primes I.

Input: q - size of the base field of $\mathcal{A}$, and n - the degree of *c*-Wieferich primes required.

Output: Product of *c*-Wieferich primes of degree less than or equal to n , (in fact dividing n).

(1) $F \leftarrow 1$, B an empty list.

(2) for $i = 1$ to $n - 1$

$$F \leftarrow (-1)^i + [i]F, \text{ (where } [i] = T^{q^i} - T \text{)}$$

(3) $B \leftarrow \text{GCD}([n], F)$

Return: B

Table 1. Examples of c-Wieferich primes in some $\mathbb{F}_q[T]$ with q small.

$\mathbb{F}_q$	$f_{\min}^t(X)$	c-Wieferich primes in $\mathbb{F}_q[T]$ of least degrees
$\mathbb{F}_3$		$T^6 + T^4 + T^3 + T^2 + 2T + 2, T^9 + T^6 + T^4 + T^2 + 2T + 2$
$\mathbb{F}_{2^2}$	$X^2 + X + 1$	$T^2 + T + t, T^2 + T + t + 1$
$\mathbb{F}_5$		$T^5 + T + 1, T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$
$\mathbb{F}_7$		$T^7 + 6T + 3, T^{14} + 5T^8 + 5T^7 + T^2 + 2T + 3$
$\mathbb{F}_{2^3}$	$X^3 + X + 1$	$T^2 + T + 1, T^2 + T + t + 1, T^2 + T + t^2 + 1, T^2 + T + t^2 + t + 1,$ $T^4 + T + 1, T^4 + T + t + 1,$ $T^4 + T + t^2 + 1, T^4 + T + t^2 + t + 1$
$\mathbb{F}_{3^2}$	$X^2 + 2X + 2$	$T^3 + (t+1)T + 1, T^3 + (t+1)T + t,$ $T^3 + (t+1)T + 2t + 2, T^3 + (2t+2)T + 1,$ $T^3 + (2t+2)T + t + 1, T^3 + (2t+2)T + 2t + 1$
$\mathbb{F}_{2^4}$	$X^4 + X + 1$	$T^2 + T + t^3, \dots, T^2 + T + t^3 + t^2 + t + 1, T^3 + T + 1, T^3 + T^2 + 1, \dots$ $T^3 + (t^3 + t^2 + t + 1)T^2 + (t^3 + t + 1)T + t, \dots$
$\mathbb{F}_{3^3}$	$X^3 + 2X + 1$	—
$\mathbb{F}_{5^2}$	$X^2 + 4X + 2$	$T^5 + 4T + 3, T^5 + 4T + t, T^5 + 4T + 2t + 2, T^5 + 4T + 3t + 4$ and $T^5 + 4T + 4t + 1$
$\mathbb{F}_{7^2}$	$X^2 + 6X + 3$	$T^7 + 6T + t + 1, T^7 + 6T + 2t + 4, T^7 + 6T + 3t, T^7 + 6T + 4t + 3,$ $T^7 + 6T + 6t + 2, T^7 + 6T + 5, T^7 + 6T + 5t + 6$

In Algorithm 1, one recursively computes F_i for $i = 1$ to $n - 1$ and lastly, the greatest common divisor of F_{n-1} and $[n]$. This yields a product of c-Wieferich primes in $\mathcal{A}$ of degree dividing n . Another way to check for existence of c-Wieferich primes of degree say dividing n is to compute $\text{resultant}([n], F_{n-1})$, the resultant of $[n]$ and F_{n-1} . If $\text{resultant}([n], F_{n-1}) \neq 0$, then there are some c-Wieferich primes of degree dividing n . In Table 2, we give experimental evidence for the existence of c-Wieferich primes in $\mathcal{A}$, using Algorithm 1 implemented in SAGE Mathematics software. We used $\mathbb{F}_q := \mathbb{F}_p(t)$ with $f_{\min}^t(X)$, the minimum polynomial of t over $\mathbb{F}_p$.

The examples in Table 2 indicate the non-existence of c-Wieferich primes of degree 1. This is in accordance with [1, Corollary 4.5] which tells us that, there are no c-Wieferich primes of degree 1. Although Algorithm 1 works well for small degrees, its misgiving lies in the exponential growth of the degrees of the polynomials involved at the third step. This motivates us to search for more efficient algorithms.

Thakur [13] points out that, the naive guess that the degree of the c-Wieferich prime is a multiple of the characteristic of $\mathbb{F}_q$ fails in characteristic 2 by Mauduit's examples in [6]. We will give more counter-examples in the case when q is even. Despite this, we still believe that Thakur's naive guess is true in odd characteristic and it is one of the motivations for this paper. The remainder of the paper is organized as follows. In Sec. 2, we will give preliminary results from the theory of finite fields that will be used in proving the criterion for maximally $\mathcal{G}$ -fixed c-Wieferich primes. In Sec. 3, we establish two criteria for maximally $\mathcal{G}$ -fixed c-Wieferich primes in $\mathcal{A}$. In Sec. 4, we explain two algorithms (based on Theorems 3.3 and 3.4) and use them to demonstrate computations of $\mathcal{G}$ -fixed c-Wieferich primes. In Sec. 5, we give a mixed bag of results regarding the distribution of c-Wieferich primes in constant field extensions of $\mathbb{F}_q[T]$.

2. Some Results from Finite Field Theory

Theorem 2.1. *Let p be the characteristic of $\mathbb{F}_q$, $\beta \in \mathbb{F}_q^\times$ and $\gamma \in \mathbb{F}_{q^r}^\times$ for some $r \in \mathbb{Z}_{\geq 1}$. The trinomial $T^p - \beta T - \gamma$ is irreducible over $\mathbb{F}_{q^r}$ if and only if it has no root in $\mathbb{F}_{q^r}$.*

Proof. Modify the arguments in the proof of [5, Theorem 3.78]. $\square$

The prime polynomials of the form $T^p - \beta T - \gamma$ where $\beta \in \mathbb{F}_q^\times$ and $\gamma \in \mathbb{F}_{q^r}$, $r \in \mathbb{Z}_{\geq 1}$ will be called *almost Artin–Schreier primes* for $\mathbb{F}_{q^r}[T]$. If $q = p$, and $\beta = 1$, then these are the Artin–Schreier primes for $\mathbb{F}_p[T]$. The next result describes precisely the decomposition of polynomials of the form $T^q - T - \alpha \in \mathbb{F}_{q^r}[T]$.

Theorem 2.2. *Let $q \geq 3$, $\alpha \in \mathbb{F}_{q^r}$ for some $r \in \mathbb{Z}_{\geq 1}$. If $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) \neq 0$, then $T^q - T - \alpha$ factors as*

$$T^q - T - \alpha = (T^p - \beta T - \gamma_1) \cdots (T^p - \beta T - \gamma_{p-1q}), \quad (2.1)$$

where $\beta = (\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha))^{p-1}$ and $\gamma_1, \dots, \gamma_{p-1q} \in \mathbb{F}_{q^r}^\times$ are distinct. If $\text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = 0$, then $T^q - T - \alpha$ splits completely in $\mathbb{F}_{q^r}[T]$.

Proof. Modify the arguments in the proof of [5, Theorem 3.80]. $\square$

Example 2.3. Let $\mathbb{F}_{3^4} := \mathbb{F}_3(t)$ where $f_{\min}^t(X) = X^4 + 2X^3 + 2$ is the minimal polynomial of t over $\mathbb{F}_3$. Then $t \in \mathbb{F}_{3^4}$ is a primitive element and $\text{Tr}_{\mathbb{F}_{3^4}/\mathbb{F}_{3^2}}(t) = t^9 + t = t^3 + t^2 \neq 0$. By Theorem 2.2, there exists a unique $\beta \in \mathbb{F}_9^\times$ such that $T^9 - T - t$ factors in $\mathbb{F}_{3^4}[T]$ into almost Artin–Schreier primes. Using SAGE,

$$\begin{aligned} T^9 - T - t &= (T^3 + (2t^3 + 2t^2 + 2)T + 2t^2 + t)(T^3 + (2t^3 + 2t^2 + 2)T + t^3 + t) \\ &\quad \times (T^3 + (2t^3 + 2t^2 + 2)T + 2t^3 + t^2 + t). \end{aligned}$$

Taking another primitive element as $\alpha = t^3 + t + 1 \in \mathbb{F}_{3^4}$. We find that $\text{Tr}_{\mathbb{F}_{3^4}/\mathbb{F}_{3^2}}(t^3 + t + 1) = 0$. By Theorem 2.2, the polynomial $T^9 - T - (t^3 + t + 1)$ splits completely in $\mathbb{F}_{3^4}[T]$. Using SAGE, we find that

$$\begin{aligned} T^9 - T - (t^3 + t + 1) &= (T + t^2 + 2t + 1)(T + t^2 + 2t + 2)(T + t^3 + 2t^2 + 2t) \\ &\quad \times (T + t^3 + 2t^2 + 2t + 1)(T + t^3 + 2t^2 + 2t + 2)(T + 2t^3 + 2t) \\ &\quad \times (T + 2t^3 + 2t + 1)(T + 2t^3 + 2t + 2)(T + t^2 + 2t). \end{aligned}$$

There are a number of ways that $\mathbb{F}_q$ acts on $\mathbb{F}_q[T]$ as a subgroup of $\text{GL}_2(\mathbb{F}_q)$. Of all these, we prefer the translation action $\star$ because it preserves monicity of polynomials and fixes F_i 's, (hence the property of being a c -Wieferich prime). For each $\alpha \in \mathbb{F}_q$, we set $\alpha \star f = f(T + \alpha)$ and the stabiliser of f to be the set $\text{stab}(f) := \{\alpha \in \mathbb{F}_q : \alpha \star f = f\}$. Let $\mathcal{G}$ be a subgroup of $\mathbb{F}_q$ and $f \in \mathbb{F}_q[T]$; we say f is a $\mathcal{G}$ -fixed (or a $\mathcal{G}$ -translation invariant) polynomial if $\mathcal{G} \subseteq \text{stab}(f)$. Note that, every $f \in \mathbb{F}_q[T]$ is $\{0\}$ -fixed. We also say that, a polynomial f is a maximally $\mathcal{G}$ -fixed polynomial

if $\text{stab}(f) = \mathcal{G}$, i.e. amongst the subgroups of $\mathbb{F}_q$ that fix f , $\mathcal{G}$ is the “largest”. If a polynomial $f \in \mathbb{F}_q[T]$ is maximally $\{0\}$ -fixed, then (with abuse of language), we also call it a non-fixed polynomial in $\mathbb{F}_q[T]$. The set of non-fixed polynomials is non-empty, since T is always a member and the set of maximally $\mathbb{F}_q$ -fixed polynomials is also non-empty, since the constant polynomial 1 is always a member of this set. Moreover, one can easily prove that these sets are infinite.

For each subgroup $\mathcal{G}$ of $\mathbb{F}_q$, we define $[1]_{\mathcal{G}} := \prod_{\alpha \in \mathcal{G}} (T + \alpha) = \prod_{\alpha \in \mathcal{G}} (T - \alpha)$. It is clear that $[1]_{\mathcal{G}}$ divides $[1]$, where $[1] = T^q - T$. In addition, if $\#\mathcal{G} = p$, then there exists a $\chi \in \mathbb{F}_q^\times$ such that $\mathcal{G} = \chi\mathbb{F}_p$ and that $[1]_{\mathcal{G}} = T^p - \beta T$ where $\beta = \chi^{p-1}$. The almost Artin–Schreier prime polynomials in $\mathbb{F}_{q^r}[T]$ (i.e. primes of the form $T^p - \beta T - \gamma$ where $\beta \in \mathbb{F}_q^\times$ and $\gamma \in \mathbb{F}_{q^r}$) are by construction $\mathcal{G}$ -fixed with $\mathcal{G} = w\mathbb{F}_p$ where w is a solution to the equation $X^{p-1} - \beta = 0$. Therefore, any prime polynomial $\mathcal{P}$ in $\mathcal{A}$ that decomposes as a product of such primes with fixed $\beta = \chi^{p-1}$ is a $\mathcal{G}$ -fixed prime. This characterization will be used in Theorem 3.3.

The motivation for studying $\mathcal{G}$ -fixed primes in $\mathbb{F}_q[T]$ arose from the following example, (see [1, p. 356]): consider the field $\mathbb{F}_{3^2} := \mathbb{F}_3(t)$ where t is such that $t^2 + 2t + 2 = 0$. Using SAGE, we obtained $T^3 + (t+1)T + 1$ as one of the c-Wieferich primes in $\mathbb{F}_{3^2}[T]$. Let $\mathcal{G}_1 = \{0, 1, 2\}$ and $\mathcal{G}_2 = \{0, t+2, 2t+1\}$, (both additive subgroups of the additive group $\mathbb{F}_{3^2}$ each of order 3). It is easy to check that $T^3 + (t+1)T + 1$ is invariant under translation by elements of $\mathcal{G}_2$ but not $\mathcal{G}_1$. In this case, we say that $\mathcal{P}$ is a $\mathcal{G}_2$ -fixed c-Wieferich prime.

Proposition 2.4. *Let f be a monic polynomial in $\mathbb{F}_q[T]$ and $\mathcal{G}$ be a subgroup of $\mathbb{F}_q$. Then f is a $\mathcal{G}$ -fixed polynomial if and only if $f = g([1]_{\mathcal{G}})$ for some $g \in \mathbb{F}_q[T]$.*

Proof. ($\Leftarrow$) This follows immediately from the fact that $[1]_{\mathcal{G}}$ is $\mathcal{G}$ -fixed. ($\Rightarrow$) For the converse, assume that f is a monic $\mathcal{G}$ -fixed polynomial of degree n . This implies that $g_1 = f - f(0)$ is also a $\mathcal{G}$ -fixed monic polynomial. Moreover, T divides g_1 since $g_1(0) = 0$. Since g_1 is a $\mathcal{G}$ -fixed monic polynomial, g_1 is divisible by all the translates $T + \alpha$, $\alpha \in \mathcal{G}$ and so, $[1]_{\mathcal{G}}$ divides g_1 . Put $f_1 = [1]_{\mathcal{G}}^{-s} g_1$, where s is the number of times T divides g_1 , then repeat the procedure. Since f is a polynomial, this procedure terminates (after at most n steps). Looking at the sequence of operations in reverse reveals that f is a monic polynomial in $[1]_{\mathcal{G}}$. $\square$

From [8, Theorem 7], it follows that there are no primes $\mathcal{P}$ in $\mathcal{A}$ whose stabiliser has order $> p$, the characteristic of $\mathbb{F}_q$. So if f is a prime in $\mathcal{A}$, then f is fixed by a subgroup of $\mathbb{F}_q$ of order at most p . In the subsequent discussions, the phrase “ $\mathcal{G}$ -fixed prime polynomials” implies that $\mathcal{G}$ is a subgroup of $\mathbb{F}_q$ of order at most p .

Theorem 2.5. *Let $\mathcal{G}$ be a subgroup of the additive group of $\mathbb{F}_q$ of order p and f be a $\mathcal{G}$ -fixed prime polynomial in $\mathcal{A}$ of degree ps . Then f factors into a product of almost Artin–Schreier $\mathcal{G}$ -fixed primes in $\mathbb{F}_{q^s}[T]$.*

Proof. From [8, Theorem 2.7(b)], it follows that the degree of f is divisible by p , say equal to ps . Since f is irreducible over $\mathbb{F}_q$ with ζ as one of its roots, it follows that $\mathbb{F}_{q^{ps}} = \mathbb{F}_q(\zeta)$ is the splitting field of f over $\mathbb{F}_q$. Since f is a $\mathcal{G}$ -fixed polynomial in $\mathcal{A}$, for each root $\zeta \in \mathbb{F}_{q^{ps}}$ of f , the element $\zeta + a$ is also a root of f for any $a \in \mathcal{G}$. Define $g := \prod_{a \in \mathcal{G}} (T - (\zeta + a))$. Since $\mathcal{G}$ is a subgroup of $\mathbb{F}_q$ of order p , it follows that $\mathcal{G} = \chi \mathbb{F}_p$ for some $\chi \in \mathbb{F}_q^\times$. Since f is irreducible over $\mathbb{F}_q$, and $\zeta + \chi$ is one of its roots, it follows that there exists a $t \in \mathbb{Z}_{\geq 1}$ such that $\zeta^{q^t} = \zeta + \chi$ and so $\zeta^{q^{pt}} = (\zeta + \chi)^{q^{(p-1)t}} = \zeta^{q^{(p-1)t}} + \chi = \zeta^{q^{(p-2)t}} + 2\chi = \dots = \zeta$. Galois theory then tells us that $g \in \mathbb{F}_{q^s}[T]$ and that $g = \prod_{a \in \mathcal{G}} (T - (\zeta + a)) = (T - \zeta) \prod_{i \in \mathbb{F}_p^\times} (T - \zeta - i\chi) = T^p - \chi^{p-1}T - (\zeta^p - \chi^{p-1}\zeta)$, a $\mathcal{G}$ -fixed polynomial. Since g has no root in $\mathbb{F}_{q^s}$, Theorem 2.1 tells us that g is irreducible over $\mathbb{F}_{q^s}$ of almost Artin-Schreier type in $\mathbb{F}_{q^s}[T]$. So f decomposes into almost Artin-Schreier $\mathcal{G}$ -fixed primes in $\mathbb{F}_{q^s}[T]$. $\square$

3. Criterion for c -Wieferich Primes in $\mathbb{F}_q[T]$

In this section, we let $\mathcal{G}$ be an additive subgroup of $\mathbb{F}_q$ of order at-most p and derive two criteria used to compute $\mathcal{G}$ -fixed c -Wieferich primes in $\mathcal{A}$. Before, we do this, let us first state and prove Lemma 3.1 which will be useful at a few places in the deduction of the main results of this section, i.e. Theorems 3.3 and 3.4.

Lemma 3.1. *Let $s, \ell \in \mathbb{Z}_{\geq 0}$ and $\mathcal{Q}_d$ be a degree d prime in $\mathcal{A}$ and $0 \leq \ell < d$. If F_i is the polynomial defined recursively as $F_0 = 1$ and $F_i = (-1)^i + [i]F_{i-1}$, for $i \in \mathbb{Z}_{\geq 1}$, then $F_{sd+\ell} \equiv (-1)^{sd}F_\ell \pmod{\mathcal{Q}_d}$.*

Proof. We have that $[sd + \ell] = [sd]^{q^\ell} + [\ell] \equiv [\ell] \pmod{\mathcal{Q}_d}$, where $\mathcal{Q}_d$ is a degree d prime polynomial in $\mathcal{A}$. We proceed by induction on ℓ with the base case $F_{sd} = (-1)^{sd} + [sd]F_{sd-1} \equiv (-1)^{sd}F_0 \pmod{\mathcal{Q}_d}$. Then for $\ell > 0$, by induction $F_{sd+\ell} = (-1)^{sd+\ell} + [sd + \ell]F_{sd+\ell-1} \equiv (-1)^{sd+\ell} + [\ell](-1)^{sd}F_{\ell-1} = (-1)^{sd}F_\ell \pmod{\mathcal{Q}_d}$. $\square$

Definition 3.2. Let $\chi \in \mathbb{F}_q$, $s \in \mathbb{Z}_{\geq 1}$ and $B_{q,s,\chi}$ be the set of equivalence classes of α 's of degree s over $\mathbb{F}_q$, (θ_1 is related to θ_2 if $\theta_1^{q^i} = \theta_2$ for some $i \in \mathbb{Z}_{\geq 0}$) such that $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = \chi$ and $F_{ps-1} \equiv 0 \pmod{T^q - T - \alpha}$.

We will often write $\alpha \in B_{q,s,\chi}$ when referring to any representative of the equivalence class of α in $B_{q,s,\chi}$.

Theorem 3.3. *For $q \geq 3$, $s \geq 1$, and $\chi \in \mathbb{F}_q^\times$, let $\mathcal{G} = \chi \mathbb{F}_p$. Then the $\mathcal{G}$ -fixed c -Wieferich primes of degree ps are precisely the prime factors over $\mathbb{F}_q$ of $R_{q,s,\alpha} = \prod_{i=1}^s (T^q - T - \alpha^{q^i})$ for $\alpha \in B_{q,s,\chi}$. Moreover, these factors are distinct so the number of $\mathcal{G}$ -fixed c -Wieferich primes is $p^{-1}q|B_{q,s,\chi}|$.*

Proof. Let $\mathcal{G} = \chi \mathbb{F}_p$ and f be a $\mathcal{G}$ -fixed c -Wieferich prime in $\mathbb{F}_q[T]$ of degree ps . By Theorem 2.5, we have $f = \prod_{i=1}^s (T^p - \chi^{p-1}T - \gamma^{q^i})$ for some $\gamma \in \mathbb{F}_{q^s}$ of degree s over $\mathbb{F}_q$. Since f is a prime polynomial in $\mathbb{F}_q[T]$ of degree ps , it follows that

$g := T^p - \chi^{p-1}T - \gamma^{q^j}$ is irreducible over $\mathbb{F}_{q^s}$. Let ζ be a root of g (so ζ will have degree ps over $\mathbb{F}_q$) and $h = \prod_{\varepsilon \in \mathbb{F}_q} (T - (\zeta + \varepsilon))$. Then $h = T^q - T - \alpha$, where $\alpha = \prod_{\varepsilon \in \mathbb{F}_q} (\zeta + \varepsilon)$. If $\zeta^{q^k} = \zeta + \varepsilon$ for some $\varepsilon \in \mathbb{F}_q$, then it follows that $\zeta^{q^{kp}} = \zeta$ which implies that s divides k . It follows that α has degree s over $\mathbb{F}_q$, since whenever ζ^{q^k} is a root of h for some $k > 0$, then s divides k . Since $\alpha \in \mathbb{F}_{q^s}$, this implies that $\zeta^{q^s} = \zeta + w$, where $w = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$. We first show that $w\mathbb{F}_p = \mathcal{G}$. For any $i = 0, 1, \dots, p-1$, we have $\zeta^{q^{is}} = \zeta + iw$. Since g is the minimum polynomial of ζ over $\mathbb{F}_{q^s}$, we have $\gamma^{q^j} = \mathcal{N}_{\mathbb{F}_{q^{ps}}/\mathbb{F}_{q^s}}(\zeta) = \zeta\zeta^{q^s} \cdots \zeta^{q^{s(p-1)}} = \zeta(\zeta + w) \cdots (\zeta + (p-1)w) = \zeta^p - w^{p-1}\zeta$, i.e. $\zeta^p - w^{p-1}\zeta - \gamma^{q^j} = 0$. Since $\zeta^p - \chi^{p-1}\zeta = 0$, it follows that $w = a\chi$ for some $a \in \mathbb{F}_p^\times$ and hence $w\mathbb{F}_p = a\chi\mathbb{F}_p = \chi\mathbb{F}_p = \mathcal{G}$. Now, since $f(\zeta) = 0$, we have $F_{ps-1}(\zeta) = 0$. This together with the fact F_{ps-1} is $\mathbb{F}_q$ -fixed, we obtain $F_{ps-1}(\zeta + \varepsilon) = 0$ for any $\varepsilon \in \mathbb{F}_q$ and hence $F_{ps-1} \equiv 0 \pmod{h}$. With these two results, we can conclude that $\alpha \in B_{q,s,\chi}$ and that f divides $R_{q,s,\alpha}$. Say now that f is a prime factor in $\mathbb{F}_q[T]$ of $R_{q,s,\alpha}$ for some $\alpha \in B_{s,q,\chi}$. Since α has degree s over $\mathbb{F}_q$, it follows that f has degree ps and f will be a $\mathcal{G}$ -fixed polynomial by Theorem 2.2. By assumption, $F_{ps-1} \equiv 0 \pmod{R_{q,s,\alpha}}$ and so f is a $\mathcal{G}$ -fixed c-Wieferich prime of degree ps . This finishes the proof of the first statement. If $R_{q,s,\alpha}$ and $R_{q,s,\beta}$ are not coprime (share a root), then $R_{q,s,\alpha} = R_{q,s,\beta}$ because fixing any root ζ of $R_{q,s,\alpha}$ or $R_{q,s,\beta}$, we can get all the roots by taking $\zeta^{q^i} + \varepsilon$ with $\varepsilon \in \mathbb{F}_q$ and $i = 1, \dots, s$. Since $R_{q,s,\alpha} = R_{q,s,\beta}$ if and only if $\alpha = \beta^{q^i}$ for some $i = 1, \dots, s$, the last statement follows. $\square$

Observe that if $\mathcal{P}$ is a $\mathcal{G}$ -fixed prime over $\mathbb{F}_q$ of degree ps , then so is $\mathcal{Q} = \mathcal{P}(T + \zeta)$ for any $\zeta \in \mathbb{F}_q - \mathcal{G}$. This is because, for any $\chi \in \mathcal{G}$, we have $\mathcal{Q}(T + \chi) = \mathcal{P}(T + \zeta + \chi) = \mathcal{P}(S + \chi) = \mathcal{P}(S) = \mathcal{P}(T + \zeta) = \mathcal{Q}$, hence $\mathcal{Q}$ is another $\mathcal{G}$ -fixed prime. It is clear that $\mathcal{Q} \neq \mathcal{P}$, since $\mathcal{P}$ is a $\mathcal{G}$ -fixed prime, hence $\mathcal{P}$ and $\mathcal{Q}$ are in different orbits. Moreover, $\mathcal{Q}$ is unique up to translation by an element of $\mathcal{G}$. So there are $p^{-1}q = \#(\mathbb{F}_q/\mathcal{G})$ possible choices of such $\mathcal{G}$ -fixed primes. In other words, if $\mathcal{S}$ is the set of $\mathcal{G}$ -fixed c-Wieferich primes of degree ps over $\mathbb{F}_q$, then the other $\frac{q-1}{p-1} - 1$ subgroups of $\mathbb{F}_q$ each of order p permute these $\#\mathcal{S}$ distinct c-Wieferich primes.

We now state the second criterion that characterizes non-fixed c-Wieferich primes in $\mathbb{F}_q[T]$.

Theorem 3.4. *Let $q \geq 3$ and $s \geq 1$. The non-fixed c-Wieferich primes in $\mathbb{F}_q[T]$ of degree s are precisely the prime factors over $\mathbb{F}_q$ of $R_{q,s,\alpha} = \prod_{i=1}^s (T^q - T - \alpha^{q^i})$ for $\alpha \in B_{q,s,0}$.*

Proof. Let f be a non-fixed c-Wieferich prime in $\mathbb{F}_q[T]$ of degree s . Then $f = \prod_{i=1}^s (T - \gamma^{q^i})$ for some $\gamma \in \mathbb{F}_{q^s}$ of degree s over $\mathbb{F}_q$. Let $\zeta = \gamma^{q^i}$ for one of the i 's, $g = T - \zeta$ and define $h = \prod_{\varepsilon \in \mathbb{F}_q} (T - (\zeta + \varepsilon))$. Then $h = T^q - T - \alpha$, where $\alpha = \prod_{\varepsilon \in \mathbb{F}_q} (\zeta + \varepsilon)$. Since g has degree 1 over $\mathbb{F}_{q^s}$ and divides h , it follows by Theorem 2.2 that $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = 0$. It follows that α has degree s over $\mathbb{F}_q$. Since $F_{s-1}(\zeta) = 0$ and F_{s-1} is $\mathbb{F}_q$ -fixed, it follows that $F_{s-1}(\zeta + \varepsilon) = 0$ and hence

$F_{s-1} \equiv 0 \pmod{h}$. We conclude that $\alpha \in B_{q,s,0}$ and that f divides $R_{q,s,\alpha}$. Say now that f is a prime factor in $\mathbb{F}_q[T]$ of $R_{q,s,\alpha}$ for some $\alpha \in B_{s,q,0}$. Since α has degree s over $\mathbb{F}_q$, it follows that f has degree s and f will be a non-fixed polynomial. By hypothesis, $F_{s-1} \equiv 0 \pmod{T^q - T - \alpha}$ hence $F_{s-1} \equiv 0 \pmod{R_{q,s,\alpha}}$ and so f is a non-fixed *c*-Wieferich prime. $\square$

In Table 4, there is an instance of Theorem 3.4, the case where $q = 2^4$ and $s = 3$.

If there exists some $\mathcal{G}$ -fixed *c*-Wieferich prime $\mathcal{P} \in \mathbb{F}_q[T]$ of degree pn , then Theorem 3.3 guarantees existence of an $\alpha \in \mathbb{F}_{q^n}$ of degree n over $\mathbb{F}_q$ and $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$ such that $F_{pn-1} \equiv 0 \pmod{T^q - T - \alpha}$. Since $\alpha \in \mathbb{F}_{q^n}$, and $[\mathbb{F}_{q^{pn}} : \mathbb{F}_{q^n}] = p$, it follows that $\text{Tr}_{\mathbb{F}_{q^{pn}}/\mathbb{F}_q}(\alpha) = 0$. Eventhough α may no longer be of degree pn over $\mathbb{F}_q$, the congruence relation $F_{pn-1} \equiv 0 \pmod{T^q - T - \alpha}$ still holds in $\mathbb{F}_{q^{pn}}$. In particular, if the condition in Theorem 3.4 that α is of degree s over $\mathbb{F}_q$ is relaxed, then Theorem 3.4 can be used to yield both $\mathcal{G}$ -fixed and non-fixed *c*-Wieferich primes in $\mathcal{A}$. For example, Theorem 3.3 with $q = 3^2$ and $s = 1$ yields the same *c*-Wieferich primes as Theorem 3.4 with $q = 3^2$ and $s = 3$ (with the relaxed condition).

4. Computing $\mathcal{G}$ -Fixed *c*-Wieferich Primes in $\mathbb{F}_{q^r}[T]$

We use Theorem 3.3 to develop Algorithm 2 used to compute $\mathcal{G}$ -fixed *c*-Wieferich primes in $\mathbb{F}_q[T]$, where $\mathcal{G}$ is any subgroup of $(\mathbb{F}_q, +)$ of order p . For each $i \in \mathbb{Z}_{\geq 1}$, we have $[i] = [1]^{q^{i-1}} + \cdots + [1] \equiv \alpha^{q^{i-1}} + \cdots + \alpha \pmod{[1] - \alpha}$ over $\mathbb{F}_{q^s}$. In particular, if $q = p$, and $\alpha \in \mathbb{F}_q^\times$, then $[1] - \alpha$ is an Artin-Schreier prime in $\mathbb{F}_q[T]$. Moreover, $[n] \equiv n\alpha \pmod{[1] - \alpha}$ for each $n \in \mathbb{Z}_{\geq 1}$. This fits well with results in [1, Sec. 5].

A modification of Algorithm 2 using Theorem 3.4 yields non-fixed *c*-Wieferich primes. However, an algorithm based on Theorem 3.3 is much more efficient and faster in computing fixed *c*-Wieferich primes. In Table 2, we give *c*-Wieferich primes in $\mathbb{F}_{32}[T]$ with corresponding elements (used to compute them) of degree s over $\mathbb{F}_9$. We do the same for the rings $\mathbb{F}_5[T]$ and $\mathbb{F}_{16}[T]$ as indicated in Tables 3 and 4, respectively. Observe that, all *c*-Wieferich primes of degree 2 and 6 in $\mathbb{F}_{16}[T]$ are $\mathbb{F}_2$ -invariant. The examples highlighted in blue in Table 5 are $\{0, t\}$ -invariant *c*-Wieferich primes in $\mathbb{F}_{24}[T]$, while that in red was discovered by Mauduit.

We demonstrate how to compute the *c*-Wieferich primes of degree 3 over $\mathbb{F}_{24}$. To determine these non-fixed *c*-Wieferich primes of degree 3 in $\mathbb{F}_{24}[T]$ according to Theorem 3.4, we set the degree of the extension to be $s = 3$ and search all the

Table 2. Some elements in subfields of $\overline{\mathbb{F}_{32}}$ and the corresponding *c*-Wieferich primes.

s	α in $\mathbb{F}_{9s}$ of degree s over $\mathbb{F}_9$ with $\text{Tr}_{\mathbb{F}_{9s}/\mathbb{F}_9}(\alpha) \neq 0$	<i>c</i> -Wieferich primes
1	$\{t, 2t + 1\}$	$T^3 + (t + 1)T + 1, T^3 + (t + 1)T + t,$ $T^3 + (t + 1)T + 2t + 2, T^3 + (2t + 2)T + 1,$ $T^3 + (2t + 2)T + t + 1, T^3 + (2t + 2)T + 2t + 1.$
2, 3, 4, 5, 6, 7, 8	—	—

Algorithm 2 Computing translation invariant c-Wieferich primes in $\mathbb{F}_q[T]$

Input: p – characteristic of the prime field, ℓ – extension degree, $q = p^\ell$, $\mathcal{B}$ – a list of elements in $\mathbb{F}_{q^s}$ of degree s over $\mathbb{F}_q$.

Output: $\mathcal{F}$ – a list of translation invariant c-Wieferich primes in $\mathbb{F}_q[T]$ of degree ps .

(1) $\mathcal{F}$ and $\mathcal{W}$ are empty lists.

(2) for α in $\mathcal{B}$

$\beta \leftarrow \alpha$, $F \leftarrow -1 + \alpha$

for $i = 2$ to $ps - 2$

$\alpha \leftarrow \alpha^q$, $\beta \leftarrow \beta + \alpha$, $F \leftarrow (-1)^i + \beta F$

if $F = 0$

$\mathcal{W} \leftarrow \alpha$

(3) $w \leftarrow 1$

(4) for $i = 1$ to size of $\mathcal{W}$

$w \leftarrow (T^q - T - \mathcal{W}_i)w$, // $\mathcal{W}_i$ is the i th element in $\mathcal{W}$

(5) $\mathcal{F} \leftarrow$ prime factors of w as an element in $\mathbb{F}_q[T]$.

Return: $\mathcal{F}$

Table 3. Some elements in subfields of $\overline{\mathbb{F}_5}$ and the corresponding c-Wieferich primes.

s	α in $\mathbb{F}_{5^s}$ of degree s over $\mathbb{F}_5$ with $\text{Tr}_{\mathbb{F}_{5^s}/\mathbb{F}_5}(\alpha) \neq 0$	c-Wieferich primes
1	$\{4\}$	$T^5 + 4T + 1$
2	$\{2t + 2, 3t + 4\}$	$T^{10} + 3T^6 + 4T^5 + T^2 + T + 1$
4	$\{t^3 + t^2 + 4, t + 4, 3t^3 + 3t^2 + t + 4, t^3 + t^2 + 3t + 4, t^3 + t^2 + 3t + 4\}$	$T^{20} + T^{16} + 4T^{15} + T^{12} + 3T^{11} + T^8 + 2T^7 + T^5 + T^4 + T^3 + 4T + 1$
3, 5, 6, 7, 8, 10, 11,	—	—

elements $\alpha \in \mathbb{F}_{2^{12}}$ with $\text{Tr}_{\mathbb{F}_{2^{12}}/\mathbb{F}_{2^4}}(\alpha) = 0$ and $F_2 \equiv 0 \pmod{T^{2^4} - T - \alpha}$. For example, we used the cubic field extension $\mathbb{F}_{2^4}(z)$ with $f_{\min}^z(X) = X^3 + X + 1$. Using SAGE, we found $B_{2^4,3,0} = \{\alpha\} = \{\alpha_1 = z^{11} + z^9 + z^6 + z^5 + z^4 + z^2 + 1, \alpha_2 = z^{10} + z^9 + z^8 + z^7 + z^5 + z^4 + z, \alpha_3 = z^{11} + z^{10} + z^8 + z^7 + z^6 + z^2 + z + 1\}$. So $R_{2^4,3,0} = (T^{2^4} - T - \alpha_1)(T^{2^4} - T - \alpha_2)(T^{2^4} - T - \alpha_3) = T^{48} + T^{33} + T^{18} + T^{16} + T^3 + T + 1 \in \mathbb{F}_{2^4}[T]$. Upon factorisation of $R_{2^4,3,0} \in \mathbb{F}_{2^4}[T]$, we obtain the list of c-Wieferich primes of degree 3 indicated in the third column of Table 5, (with $f_{\min}^t(X) = X^4 + X + 1$). Since $T^3 + T + 1$ is a non-fixed c-Weiferich prime, there are 15 more non-fixed c-Weiferich primes obtained by applying a translation $\mathbb{F}_{2^4}$ -automorphism to $T^3 + T + 1$, for example, $\sigma_t(T^3 + T + 1) = (T + t)^3 + (T + t) + 1 = T^3 + tT^2 + (t^2 + 1)T + t^3 + t + 1$. We summarise these results in Table 5. Observe the similarity in the primes of Tables 4 and 5. We also observe that all the c-Wieferich primes of degree 2 and 6 in $\mathbb{F}_{2^4}[T]$ are $\mathbb{F}_2$ -invariant. The examples highlighted in blue are $\{0, t\}$ -invariant c-Wieferich primes in $\mathbb{F}_{2^4}[T]$, while that in red was discovered by Mauduit [6].

Table 4. Some elements in subfields of $\overline{\mathbb{F}_{16}}$ and the corresponding c -Wieferich primes.

s	α in $\mathbb{F}_{16^s}$ of degree s over $\mathbb{F}_{16}$ with $\text{Tr}_{\mathbb{F}_{16^s}/\mathbb{F}_{16}}(\alpha) \neq 0$	c -Wieferich primes
1	$\{1\}$	$T^2 + T + t^3, T^2 + T + t^3 + 1, T^2 + T + t^3 + t^2 + t,$ $T^2 + T + t^3 + t, T^2 + T + t^3 + t^2, T^2 + T + t^3 + t^2 + 1,$ $T^2 + T + t^3 + t + 1, T^2 + T + t^3 + t^2 + t + 1.$
2	—	—
3	$\{z^{11} + z^9 + z^6 + z^5 + z^4 + z^2,$ $z^{11} + z^{10} + z^8 + z^7 + z^6$ $+ z^2 + z, z^{10} + z^9 + z^8 + z^7$ $+ z^5 + z^4 + z + 1\}$	$T^6 + T^5 + t^3T^4 + T^3 + (t^2 + 1)T^2 + (t^3 + t^2)T$ $+ t^2 + t + 1,$ $T^6 + T^5 + (t^3 + 1)T^4 + T^3 + (t^2 + 1)T^2$ $+ (t^3 + t^2 + 1)T + t + 1,$ $T^6 + T^5 + (t^3 + t)T^4 + T^3 + (t + 1)T^2$ $+ t^3T + t^2 + t,$ $T^6 + T^5 + (t^3 + t + 1)T^4 + T^3 + (t + 1)T^2$ $+ (t^3 + 1)T + t^2,$ $T^6 + T^5 + (t^3 + t^2)T^4 + T^3 + tT^2$ $+ (t^3 + t^2 + t + 1)T + t^2 + t.$ $T^6 + T^5 + (t^3 + t^2 + 1)T^4 + T^3 + tT^2$ $+ (t^3 + t^2 + t)T + t^2 + 1,$ $T^6 + T^5 + (t^3 + t^2 + t)T^4 + T^3 + t^2T^2$ $+ (t^3 + t + 1)T + t.$ $T^6 + T^5 + (t^3 + t^2 + t + 1)T^4 + T^3 + t^2T^2$ $+ (t^3 + t)T + t^2 + t + 1.$

From literature, there are three c -Wieferich primes of degrees 5, 10 and 20 defined over $\mathbb{F}_5[T]$ obtained by brute force/other methods. Using Theorem 3.3, we searched for c -Wieferich primes of degree up to 55 and obtained a new c -Wieferich prime of degree 45. In particular, $T^{45} + T^{41} + 3T^{40} + T^{37} + T^{36} + 2T^{35} + T^{33} + 4T^{32} + T^{31} + T^{30} + T^{29} + 2T^{28} + 2T^{27} + 4T^{26} + 4T^{21} + 3T^{20} + 4T^{17} + T^{15} + 4T^{13} + 2T^{12} + 4T^9 + 4T^8 + 2T^7 + 4T^6 + T^5 + T^4 + 2T^3 + T^2 + 3T + 2 \in \mathbb{F}_5[T]$ represented by the triple $(5, 1, 9)$ highlighted in Table 6.

We now give some of the “highest” degree examples of c -Wieferich primes (summarized in Table 6) we obtained in different rings for $p < 20$. We found all of the possible c -Wieferich primes in the listed cases, but we only present a few of them. In $\mathbb{F}_{3^4}[T]$, we found $T^9 + T^6 + T^4 + T^3 + T^2 + T + 1, \dots, T^9 + T^6 + T^4 + (2t^3 + 2t^2 + 2t + 1)T^3 + T^2 + (t^3 + t^2 + t + 1)T + t^3 + 2t + 2$ where $t^4 + 2t^3 + 2 = 0$. In the ring $\mathbb{F}_{7^3}[T]$, we found $T^{14} + 5T^8 + 4T^7 + T^2 + 3T + 6, \dots, T^{14} + 5T^8 + (6t^2 + 6t)T^7 + T^2 + (t^2 + t)T + t^2 + 6t + 6$ where $t^3 + 6t^2 + 4 = 0$. In $\mathbb{F}_{11^2}[T]$, we obtained $T^{33} + (5t + 3)T^{23} + 10T^{22} + (3t + 1)T^{13} + (4t + 9)T^{12} + (8t + 4)T^{11} + (7t + 8)T^3 + (10t + 7)T^2 + (2t + 3)T + 3t + 9, \dots, T^{33} + (6t + 1)T^{23} + (10t + 2)T^{22} + (8t + 2)T^{13} + (6t + 2)T^{12} + (3t + 7)T^{11} + (4t + 3)T^3 + (5t + 3)T^2 + (6t + 5)T + 4t + 1$ where $t^2 + 7t + 2 = 0$. Lastly, in $\mathbb{F}_{19^2}[T]$, we obtained $T^{38} + (8t + 10)T^{20} + 18T^{19} + (18t + 12)T^2 + (15t + 14)T + 16t + 1, \dots, T^{38} + (11t + 18)T^{20} + (18t + 11)T^{19} + (t + 11)T^2 + (8t + 15)T + 12t + 18 \in \mathbb{F}_{19^2}[T]$ where $t^2 + 18t + 2 = 0$.

There are some more examples not summarized in Table 6, these include $T^{129} + 40T^{87} + 7T^{86} + 3T^{45} + 29T^{44} + 17T^{43} + 42T^3 + 7T^2 + 26T + 10, T^{129} + 40T^{87} +$

Table 5. Some elements in subfields of $\overline{\mathbb{F}_{2^4}}$ and the corresponding c-Wieferich primes.

s	α in $\mathbb{F}_{16^s}$ of degree s over $\mathbb{F}_{16}$ with $\text{Tr}_{\mathbb{F}_{16^s}/\mathbb{F}_{16}}(\alpha) = 0$	c-Wieferich primes of degree s in $\mathcal{A}$
1	—	—
2	$\{1\}$	$T^2 + T + t^3 + t^2, T^2 + T + t^3 + 1,$ $T^2 + T + t^3 + t, T^2 + T + t^3 + t^2 + 1,$ $T^2 + T + t^3, T^2 + T + t^3 + t^2 + t,$ $T^2 + T + t^3 + t^2 + t + 1, T^2 + T + t^3 + t + 1,$ $T^3 + T + 1, T^3 + tT^2 + (t^2 + 1)T + t^3 + t + 1,$ $T^3 + T^2 + 1, T^3 + t^2T^2 + tT + t^3 + 1,$ $T^3 + (t^2 + 1)T^2 + (t + 1)T + t^3 + t^2 + t,$ $T^3 + (t^2 + t + 1)T^2 + (t^2 + t + 1)T + t^2 + t + 1,$ $T^3 + (t^3 + 1)T^2 + (t^3 + t^2)T + t^2 + t + 1,$ $T^3 + (t^3 + t + 1)T^2 + t^3T + t^2 + t,$ $T^3 + (t^3 + t)T^2 + (t^3 + 1)T + t^2,$ $T^3 + (t^3 + t^2)T^2 + (t^3 + t^2 + t)T + t^2 + 1,$ $T^3 + (t^3 + t^2 + 1)T^2 + (t^3 + t^2 + t + 1)T + t^2 + t,$ $T^3 + (t^3 + t^2 + t)T^2 + (t^3 + t)T + t^2 + t + 1,$ $T^3 + (t^2 + t)T^2 + (t^2 + t)T + t^2 + t,$ $T^3 + t^3T^2 + (t^3 + t^2 + 1)T + t + 1,$ $T^3 + (t + 1)T^2 + t^2T + t^3 + t^2 + 1,$ $T^3 + (t^3 + t^2 + t + 1)T^2 + (t^3 + t + 1)T + t$
5	—	—
6	$\{z^{20} + z^{19} + z^{18} + z^{16} + z^{15} + z^{13}$ $+ z^{11} + z^{10} + z^6 + z^2 + 1, z^{23} + z^{21}$ $+ z^{19} + z^{15} + z^{14} + z^{13} + z^{11} + z^{10}$ $+ z^9 + z^7 + z^4 + z^3 + 1, z^{23} + z^{21}$ $+ z^{20} + z^{18} + z^{16} + z^{14} + z^9 + z^7$ $+ z^6 + z^4 + z^3 + z^2 + 1\}$	product of c-Wieferich primes of degree 6 is $T^{48} + T^{33} + T^{32} + T^{18} + T^3 + T^2 + 1$ see Table 2

$22T^{86} + 3T^{45} + 42T^{44} + 28T^{43} + 42T^3 + 22T^2 + 15T + 23$ in $\mathbb{F}_{43}[T]$. In $\mathbb{F}_{61}[T]$, we found $T^{183} + 58T^{123} + 52T^{122} + 3T^{63} + 18T^{62} + 35T^{61} + 60T^3 + 52T^2 + 26T + 35$. In $\mathbb{F}_{131}[T]$, we found $T^{393} + 128T^{263} + 129T^{262} + 3T^{133} + 4T^{132} + 50T^{131} + 130T^3 + 129T^2 + 81T + 33$. In $\mathbb{F}_{463}[T]$, we found $T^{926} + 461T^{464} + 193T^{463} + T^2 + 270T + 277$ and $T^{926} + 461T^{464} + 188T^{463} + T^2 + 275T + 182$.

5. c-Wieferich Primes Under Constant Field Extensions

In characteristic 2, the polynomial $f = T^3 + T^2 + 1$ is always irreducible over $\mathbb{F}_{2^{3m \pm 1}}$ for any $m \in \mathbb{Z}_{\geq 1}$. This is because f is a prime polynomial in $\mathbb{F}_2[T]$ and its degree over $\mathbb{F}_2$ is always coprime to $3m \pm 1$ for any $m \in \mathbb{Z}_{\geq 1}$. In [6], Mauduit showed that $T^3 + T^2 + 1$ is a non-fixed c-Wieferich prime in $\mathbb{F}_{2^4}[T]$. In addition, Mauduit proved that the polynomial $T^3 + T^2 + 1 \in \mathbb{F}_2[T]$ is a non-fixed c-Wieferich prime for all rings of the form $\mathbb{F}_{2^{3m+1}}[T]$, $m \in \mathbb{Z}_{\geq 0}$. However, in her list, Mauduit left out a number of possible candidates, see Table 5 for more examples. We now generalise Mauduit’s horizontal existence result as follows.

Theorem 5.1. *Let $\mathcal{P}$ be a prime polynomial in $\mathbb{F}_q[T]$ of degree m . For any $n \in \mathbb{Z}_{\geq 1}$, we have that $\mathcal{P}$ is a c -Wieferich prime in $\mathbb{F}_q[T]$, if and only if $\mathcal{P}$ is a c -Wieferich prime in $\mathbb{F}_{q^{mn+1}}[T]$.*

Before we state the proof Theorem 5.1, we shall need the following extra notation. For each $i, j \in \mathbb{Z}_{\geq 1}$, we define the symbols $[i]_{q^j}$ and $F_{q^j, i}$ as follows: $[i]_{q^j} = T^{q^{ji}} - T$, and $F_{q^j, i} = (-1)^i + [i]_{q^j} F_{q^j, i-1}$ with $F_{q^j, 0} = 1$.

Proof. Let $r = mn + 1$ where $n \in \mathbb{Z}_{\geq 0}$ and $\mathcal{Q}_m$ be any prime polynomial in $\mathbb{F}_q[T]$ of degree m . Since m is coprime to r , we have $\mathcal{Q}_m$ is a prime polynomial in $\mathbb{F}_{q^r}[T]$, hence $[m]_q = T^{q^m} - T \equiv 0 \pmod{\mathcal{Q}_m}$. It follows that, for any $i \in \mathbb{Z}_{\geq 1}$, we have $[i]_{q^r} = T^{q^{ri}} - T = T^{q^{(mn+1)i}} - T \equiv T^{q^m \cdots q^m \cdot q^i} - T \equiv T^{q^i} - T = [i]_q \pmod{\mathcal{Q}_m}$. Therefore, $F_{q^r, m-1} \equiv F_{q, m-1} \pmod{\mathcal{Q}_m}$ and the claim follows from this result. $\square$

We know that $f = T^3 + T^2 + 1$ and $f(T + 1) = T^3 + T + 1$ are non-fixed c -Wieferich primes in $\mathbb{F}_2[T]$. By Theorem 5.1, it follows that they are c -Wieferich primes in $\mathbb{F}_{2^{3n+1}}[T]$, (see Table 5). Another example is the polynomial $\mathcal{P} = T^6 + T^4 + T^3 + T^2 + 2T + 2$ which is a fixed c -Wieferich prime for $\mathbb{F}_3[T]$. By Theorem 5.1, $\mathcal{P}$ is a c -Wieferich prime for $\mathbb{F}_q[T]$ where $q = 3^{6m+1}$ and $m \in \mathbb{Z}_{\geq 1}$. On the other hand, the fixed polynomial $\mathcal{P}_1 = T^6 + T^4 + 2T^3 + T^2 + T + 2 = 2^{-\deg(\mathcal{P})}\mathcal{P}(2T)$ is not a c -Wieferich prime polynomial in $\mathbb{F}_3[T]$ but in $\mathbb{F}_{3^5}[T]$. By Theorem 5.1, the polynomial $\mathcal{P}_1$ is also a c -Wieferich prime in the rings of the form $\mathbb{F}_{3^{5(6n+1)}}[T]$ for any $n \in \mathbb{Z}_{\geq 0}$. Furthermore, since the Diophantine equation $6n + 1 = 30k + 5$ has no integer solutions, it follows that there is no ring extension $\mathbb{F}_{3^r}[T]$ in which both $\mathcal{P}$ and $\mathcal{P}_1$ occur as c -Wieferich primes.

To understand the behaviour above, consider the triple (p, m, s) , where p is a prime number and $s, m \in \mathbb{Z}_{\geq 1}$. We say $\mathcal{P}$ is a c -Wieferich prime for the triple (p, m, s) if there exists a subgroup $\mathcal{G}$ of $(\mathbb{F}_{p^m}, +)$ such that $\mathcal{P}$ is a $\mathcal{G}$ -fixed c -Wieferich prime in $\mathbb{F}_{p^m}[T]$ of degree ps . For example, $\mathcal{P} = T^6 + T^4 + T^3 + T^2 + 2T + 2$ is a c -Wieferich prime for the triples $(3, 1, 2)$, $(3, 7, 2)$, $(3, 13, 2)$, $\dots$ since $\mathcal{P}$ is an $\mathbb{F}_3$ -fixed c -Wieferich prime of degree 6 in $\mathbb{F}_3[T]$, $\mathbb{F}_{3^7}[T]$ and $\mathbb{F}_{3^{13}}[T]$.

For each q and $s \in \mathbb{Z}_{\geq 1}$, we let $B_{q, s} = \bigcup_{\chi \in \mathbb{F}_q^\times} B_{q, s, \chi}$. Each element of $B_{q, s}$ has $p^{-1}q$ distinct c -Wieferich primes associated to it. We now summarize some of the data we have computed regarding counts of c -Wieferich primes associated to the triples (p, m, s) in Table 6. The values in the table are (p, m, s) and $|B_{p^m, s}|$, and they give at least some indication about how these numbers vary.

For example, for the triple $(3, 2, 1)$, we have $B_{3^2, 1} = \{t, 2t + 1 : t^2 + 2t + 2 = 0\}$ and hence $3^{-1} \cdot 3^2 \cdot 2 = 6$ different fixed c -Wieferich primes of degree 3, namely $\mathcal{L} = \{T^3 + (t + 1)T + 1, T^3 + (t + 1)T + t, T^3 + (t + 1)T + 2t + 2, T^3 + (2t + 2)T + 1, T^3 + (2t + 2)T + t + 1, T^3 + (2t + 2)T + 2t + 1\}$, (also see Table 1 or Table 2). By Theorem 5.1, these same primes correspond to the triples $(3, 2(3n + 1), 1)$ where

Table 6. Counts of fixed c-Wieferich primes.

(p, m, s)	#	(p, m, s)	#	(p, m, s)	#	(p, m, s)	#	(p, m, s)	#	(p, m, s)	#
(3,1,1)	0	(3,1,2)	1	(3,1,3)	1	(3,1,4)	1	(3,1,5)	1	(3,1,6)	0
(3,1,7)	0	(3,1,8)	0	(3,1,9)	0	(3,1,10)	0	(3,1,11)	0	(3,1,12)	0
(3,1,13)	0	(3,1,14)	0	(3,1,15)	0	(3,1,16)	0	(3,1,17)	0	(3,2,1)	2
(3,2,2)	0	(3,2,3)	0	(3,2,4)	0	(3,2,5)	0	(3,2,6)	0	(3,2,7)	0
(3,2,8)	0	(3,3,1)	0	(3,3,2)	1	(3,3,3)	0	(3,3,4)	0	(3,3,5)	0
(3,4,1)	2	(3,4,2)	0	(3,4,3)	1	(3,4,4)	0	(3,5,1)	0	(3,5,2)	1
(3,5,3)	0	(3,6,1)	2	(3,6,2)	0	(3,7,1)	0	(3,7,2)	1	(3,8,1)	2
(3,8,2)	0	(3,9,1)	0	(3,10,1)	2	(3,11,1)	0	(3,12,1)	2	(3,13,1)	0
(3,14,1)	2	(3,15,1)	0	(3,16,1)	2	(3,17,1)	0	(5,1,1)	1	(5,1,2)	1
(5,1,3)	0	(5,1,4)	1	(5,1,5)	0	(5,1,6)	0	(5,1,7)	0	(5,1,8)	0
(5,1,9)	1	(5,1,10)	0	(5,1,11)	0	(5,2,1)	1	(5,2,2)	0	(5,2,3)	0
(5,2,4)	0	(5,2,5)	0	(5,3,1)	4	(5,3,2)	1	(5,3,3)	0	(5,4,1)	1
(5,4,2)	0	(5,5,1)	1	(5,5,2)	1	(5,6,1)	4	(5,7,1)	1	(5,8,1)	1
(5,9,1)	4	(5,10,1)	1	(5,11,1)	1	(7,1,1)	1	(7,1,2)	1	(7,1,3)	0
(7,1,4)	0	(7,1,5)	0	(7,1,6)	0	(7,1,7)	0	(7,1,8)	0	(7,1,9)	0
(7,2,1)	3	(7,2,2)	0	(7,2,3)	1	(7,2,4)	0	(7,3,1)	4	(7,3,2)	1
(7,3,3)	3	(7,4,1)	3	(7,4,2)	0	(7,5,1)	1	(7,6,1)	6	(7,7,1)	1
(7,8,1)	3	(7,9,1)	4	(11,1,1)	1	(11,1,2)	0	(11,1,3)	1	(11,1,4)	0
(11,1,5)	0	(11,1,6)	0	(11,1,7)	0	(11,2,1)	1	(11,2,2)	2	(11,2,3)	2
(11,3,1)	1	(11,3,2)	0	(11,4,1)	5	(11,5,1)	6	(11,6,1)	1	(11,7,1)	1

$n \in \mathbb{Z}_{\geq 0}$. We demonstrate this below:

- (1) In $\mathbb{F}_{3^4}[T]$, we have $B_{3^4,1} = \{2w^3 + 2w^2 + 1, w^3 + w^2 : w^4 + 2w^3 + 2 = 0\}$. This is the image of $B_{3^2,1}$ under the embedding $\iota : \mathbb{F}_{3^2} \rightarrow \mathbb{F}_{3^4}$ defined by $t \mapsto w^3 + w^2$. So the primes in $\mathcal{L}$ again appear among c-Wieferich primes in $\mathbb{F}_{3^4}[T]$, (in this case there are $3^{-1} \cdot 3^4 \cdot 2$ distinct c-Wieferich primes in $\mathbb{F}_{3^4}[T]$ of degree 3). For example, $T^3 + (t+1)T + 1$ is identified with $T^3 + (w^3 + w^2 + 1)T + 1$ in $\mathbb{F}_{3^4}[T]$.
- (2) In $\mathbb{F}_{3^8}[T]$, we have $B_{3^8,1} = \{2w^7 + 2w^6 + 2w^5 + w + 2, w^7 + w^6 + w^5 + 2w + 2 : w^8 + 2w^5 + w^4 + 2w^2 + 2w + 2 = 0\}$. This is the image of $B_{3^2,1}$ under $\iota : \mathbb{F}_{3^2} \rightarrow \mathbb{F}_{3^8}$ defined by $t \mapsto w^7 + w^6 + w^5 + 2w + 2$.

Attached to the triple $(3, 5, 2)$ is a c-Wieferich prime $\mathcal{Q} = T^6 + T^4 + 2T^3 + T^2 + T + 2$. One can easily show that $\mathcal{Q}$ is one of the two fixed primes in $\mathbb{F}_3[T]$ of degree 6, (the other being $\mathcal{P} = T^6 + T^4 + T^3 + T^2 + 2T + 2$). Furthermore, we have already seen that $\mathcal{P}$ is a c-Wieferich prime in $\mathbb{F}_3[T]$ while $\mathcal{Q}$ is a c-Wieferich prime in $\mathbb{F}_{3^5}[T]$. With this limited data, a natural question arises: given a q , do all fixed primes in $\mathbb{F}_q[T]$ become c-Wieferich primes in some $\mathbb{F}_{q^r}[T]$? We provide a partial answer in Lemma 5.2 and Theorem 5.3.

Lemma 5.2. Fix $s \in \mathbb{Z}_{\geq 1}$ and an element $\alpha \in \mathbb{F}_{q^s}$ of degree s over $\mathbb{F}_q$. Fix $k \in \mathbb{Z}_{\geq 1}$ and put $r = 1 + sk$. Then for any $n \in \mathbb{Z}_{\geq 1}$, we have that $F_{q^n} \equiv 0 \pmod{T^q - T - \alpha}$ if and only if $F_{q^r, n} \equiv 0 \pmod{T^{q^r} - T - \alpha}$. In particular, for a fixed $\chi \in \mathbb{F}_q^\times$, we have $\alpha \in B_{q^r, s, \chi}$ if and only if $\alpha \in B_{q, s, \chi}$.

Proof. Put $f_{q,0} = 1$ and define $f_{q,i} \in \mathbb{F}_q[x]$ recursively as follows $f_{q,i}(x) = (-1)^i + (\sum_{j=0}^i x^{q^j})f_{q,i-1}(x)$. Since $\alpha \in \mathbb{F}_{q^s}$, we have $\alpha^{q^r} = (\alpha^{q^{sk}})^q = \alpha^q$ and so $f_{q,n}(\alpha) = f_{q^r,n}(\alpha)$. Since $F_{q,n} \equiv f_{q,n}(\alpha)(\text{mod } T^q - T - \alpha)$ and $F_{q^r,n} \equiv f_{q^r,n}(\alpha)(\text{mod } T^{q^r} - T - \alpha)$, the first equivalence then follows. For the second equivalence, it remains only to note that α also has degree s over $\mathbb{F}_{q^r}$ and $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_{q^r}}(\alpha) = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$. $\square$

Theorem 5.3. Let $s \in \mathbb{Z}_{\geq 1}$ be fixed, $E_{q,s} = \{k \in \mathbb{Z}_{\geq 0} : p \nmid 1 + sk\}$ and $\mathcal{G}$ be a subgroup of $(\mathbb{F}_q, +)$ of order p , (i.e. $\mathcal{G} = \chi\mathbb{F}_p$ for some $\chi \in \mathbb{F}_q^\times$). If there is

- (1) a $\mathcal{G}$ -fixed c -Wieferich prime $\mathcal{P}$ over $\mathbb{F}_q$ of degree ps , then this prime polynomial is a factor of $R_{q,s,\alpha}$ for some $\alpha \in \mathbb{F}_{q^s}$ of degree s over $\mathbb{F}_q$ and $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) \neq 0$. For each $k \in E_{q,s}$, there exists a $\mathcal{G}$ -fixed prime over $\mathbb{F}_q$ that is a prime factor of $R_{q,s,\beta}$, where $\beta = \alpha - \frac{k}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$. Moreover, this prime factor is a c -Wieferich prime polynomial in $\mathbb{F}_{q^{1+sk}}[T]$.
- (2) no $\mathcal{G}$ -fixed c -Wieferich prime over $\mathbb{F}_q$ of degree ps , then none of the $\mathcal{G}$ -fixed primes over $\mathbb{F}_q$ is a c -Wieferich prime in $\mathbb{F}_{q^r}[T]$ for any $r \in \mathbb{Z}_{\geq 1}$.

Proof. Let $\mathcal{G} = \chi\mathbb{F}_p$ for some $\chi \in \mathbb{F}_q^\times$ and $\mathcal{P}$ be a $\mathcal{G}$ -fixed c -Wieferich prime in $\mathbb{F}_q[T]$ of degree ps . By Theorem 3.3, $\mathcal{P}$ is a factor of $R_{q,s,\alpha}$ for some α of degree s over $\mathbb{F}_q$ and that $\chi = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) \neq 0$. In particular, $F_{q,ps-1} \equiv 0 \pmod{T^q - T - \alpha}$. Take any $k \in E_{q,s}$ and put $r = 1 + sk$. By Lemma 5.2, $F_{q^r,ps-1} \equiv 0 \pmod{T^{q^r} - T - \alpha}$. Since r is coprime to s , we have α , (as an element of $\mathbb{F}_{q^{rs}}$) has degree s over $\mathbb{F}_{q^r}$. So $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_{q^r}}(\alpha) = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$.

Let $\beta = \alpha - \frac{k}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$. Clearly $\beta \in \mathbb{F}_{q^s}$. We now show that β gives rise to c -Wieferich primes over $\mathbb{F}_{q^r}$ of degree ps . First, we show that β has degree s over $\mathbb{F}_q$ and $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\beta) \neq 0$. Assume that β has degree less than s , i.e. $\beta^{q^{ri}} = \beta^{q^{rj}}$ for some $1 \leq i < j < s$. Then $\alpha^{q^{ri}} - \frac{k}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = \alpha^{q^{rj}} - \frac{k}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$ which implies that $\alpha^{q^{ri}} = \alpha^{q^{rj}}$, a contradiction to the fact α has degree s over $\mathbb{F}_{q^r}$. Furthermore, $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\beta) = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) - \frac{ks}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) \neq 0$.

If $w \in \mathbb{F}_{q^s}$, then the trinomial $T^q - T - w$ divides $T^{q^r} - T - \alpha$ if and only if $\alpha = w + k\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(w)$. This implies that $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(w) = \frac{1}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$, hence $w = \alpha - \frac{k}{1+sk}\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = \beta$. As such, it follows that the polynomial $R_{q,s,\beta}$ divides $R_{q^r,s,\alpha}$. By Theorem 2.1, the trinomial $T^q - T - \beta$ decomposes into $\mathcal{G}$ -fixed primes over $\mathbb{F}_{q^s}$. As such, the prime factors of $R_{q,s,\beta}$ over $\mathbb{F}_q$ are $\mathcal{G}$ -fixed primes of degree ps . In addition, these are also c -Wieferich primes in $\mathbb{F}_{q^r}[T]$, since they divide $F_{q^r,ps-1}$. Note that if p divides $1 + sk$, then $T^q - T - w$ does not divide $T^{q^r} - T - \alpha$ for any $w \in \mathbb{F}_{q^s}$ since $\text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) \neq 0$.

For the second part, let $\mathcal{P} \in \mathbb{F}_q[T]$ be a $\mathcal{G}$ -fixed prime of degree ps . Assume that $\mathcal{P}$ is a c -Wieferich prime in $\mathbb{F}_{q^r}[T]$ for some $r = 1 + sk$ with $k \in E_{q,s} - \{0\}$ and that there are no fixed c -Wieferich primes in $\mathbb{F}_q[T]$ of degree ps . By Theorem 3.3, there exists an $\alpha \in \mathbb{F}_{q^{rs}}^\times$ of degree s over $\mathbb{F}_{q^r}$ with $\text{Tr}_{\mathbb{F}_{q^{rs}}/\mathbb{F}_{q^r}}(\alpha) \neq 0$ such that $F_{q^r,ps-1} \equiv 0 \pmod{T^{q^r} - T - \alpha}$, i.e. $\mathcal{P}$ divides $\mathcal{R}_{q^r,s,\alpha}$. Since $\mathcal{P}$ is a $\mathcal{G}$ -fixed prime of degree ps , it follows from Theorem 2.5 that it factors into almost Artin-Schreier

primes in $\mathbb{F}_{q^s}[T]$. Say that one is $\mathcal{Q} = T^p - \beta T - \lambda$, with $\beta = \chi^{p-1}$ for some $\chi \in \mathbb{F}_q^\times$. We have $\mathcal{Q}$ divides $T^{q^r} - T - \alpha$ and then we see that $\prod_{a \in \mathbb{F}_p} \mathcal{Q}(T + a\chi) = T^q - T - w$ divides $T^{q^r} - T - \alpha$ where $w \in \mathbb{F}_{q^s}$. The polynomial $T^q - T - w$ divides $T^{q^r} - T - \alpha$ if and only if $w = \alpha - \frac{k}{1+sk} \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha)$, hence $\alpha \in \mathbb{F}_{q^s}$. Lemma 5.2 then tells us that there exists a $\mathcal{G}$ -fixed c-Wieferich prime of degree ps in $\mathbb{F}_q[T]$ which is a contradiction. $\square$

Given a $\mathcal{G}$ -fixed c-Wieferich prime $\mathcal{P}$ in $\mathbb{F}_q[T]$ of degree ps and $k \in E_{q,s}$, how do we find the $\mathcal{G}$ -fixed primes $\mathcal{Q}$ in $\mathbb{F}_q[T]$ that are c-Wieferich primes in $\mathbb{F}_{q^{1+sk}}[T]$? Suppose that the prime $\mathcal{P}$ comes from $\alpha \in B_{q,s,\chi}$ and that $\mathcal{P}$ divides $R_{q,s,\alpha} = \prod_{i=1}^s (T^q - T - \alpha^{q^i})$. From the proof of Theorem 5.3, $\mathcal{Q}$ is a prime factor of $R_{q,s,\beta}$. Now,

$$\begin{aligned} R_{q,s,\beta} &= \prod_{i=1}^s (T^q - T - \beta^{q^i}) = \prod_{i=1}^s \left(T^q - T - \alpha^{q^i} + \frac{k}{(1+sk)} \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) \right) \\ &= \prod_{i=1}^s ((T+x)^q - (T+x) - \alpha^{q^i}), \end{aligned}$$

where x is any root of $X^q - X - \frac{k}{(1+sk)} \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = 0$. By Theorem 2.2, $x \in \mathbb{F}_{q^p}$, (and the set of solutions of $X^q - X - \frac{k}{(1+sk)} \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = 0$ is $x + \mathbb{F}_q$). Comparing the factorisation of $R_{q,s,\beta}$ to that of $R_{q,s,\alpha}$, we see that $R_{q,s,\beta}$ has $p^{-1}q$ distinct prime factors of the form $\mathcal{P}(T+x)$, and $\mathcal{Q}$ is one of them. Observe that, if p is coprime to s , then the set map $f_s : E_{q,s} \rightarrow \mathbb{F}_p - \{s^{-1}\}$ defined by $k \mapsto \frac{k}{1+sk}$ is surjective, and if p divides s , then the set map $f_s : E_{q,s} \rightarrow \mathbb{F}_p - \{0\}$ defined by $k \mapsto \frac{k}{1+sk}$ is surjective. So we only need $p-1$ distinct values of k in $E_{q,s}$ to determine all the possible roots to $X^q - X - \frac{k}{(1+sk)} \text{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(\alpha) = 0$, for a fixed α . For this matter, we need only $D_{q,s} = \{k \in \mathbb{Z}_{\geq 0} : p \nmid (1+sk), k \leq p-1\}$ instead of the full set $E_{q,s}$.

The polynomials $\mathcal{P} = T^6 + T^4 + T^3 + T^2 + 2T + 2$ and $\mathcal{Q} = T^6 + T^4 + 2T^3 + T^2 + T + 2$ are both fixed polynomials in $\mathbb{F}_3[T]$, in fact the only fixed prime polynomials of degree 6. We have already seen that $\mathcal{P}$ is a c-Wieferich prime in $\mathbb{F}_3[T]$ while $\mathcal{Q}$ is not. Furthermore, $\mathcal{Q}$ is a c-Wieferich prime in $\mathbb{F}_{3^5}[T]$ while $\mathcal{P}$ is not. In fact, there exists no ring $\mathbb{F}_{3^m}[T]$ in which both $\mathcal{P}$ and $\mathcal{Q}$ are c-Wieferich primes simultaneously. In any case, here we have $E_{3,2} = \{0, 2\}$. For $r = 5$, solving $X^3 - X - 2 \cdot 5^{-1} \text{Tr}_{\mathbb{F}_{3^2}/\mathbb{F}_3}(\alpha) = 0$ yields $X = z$, where $z^3 + 2z + 1 = 0$ as a solution. So $\mathcal{P}(T+z) = T^6 + 2z^3T^3 + z^6 + T^4 + T^3z + Tz^3 + z^4 + T^3 + z^3 + T^2 + 2zT + z^2 + 2T + 2z + 2 = T^6 + T^4 + (2z^3 + z + 1)T^3 + T^2 + (z^3 + 2z + 2)T + z^6 + z^4 + z^3 + z^2 + 2z + 2 = T^6 + T^4 + 2T^3 + T^2 + T + 2$.

Also when we consider the fixed prime polynomials $\mathcal{R} = T^9 + T^6 + T^4 + T^2 + 2T + 2$ and $\mathcal{S} = T^9 + T^6 + T^4 + T^3 + T^2 + T + 1$ in $\mathbb{F}_3[T]$. We have already seen that $\mathcal{R}$ is a c-Wieferich prime in $\mathbb{F}_3[T]$, but not $\mathcal{S}$. In this case, we have $E_{3,3} = \{0, 1, 2\}$. Since $s \equiv 0 \pmod{3}$, we obtain c-Wieferich primes in $\mathbb{F}_{3^{1+3k}}[T]$ by first solving $X^3 - X - k \text{Tr}_{\mathbb{F}_{3^3}/\mathbb{F}_3}(\alpha) = 0$. For $r = 4$, solving $X^3 - X - \text{Tr}_{\mathbb{F}_{3^3}/\mathbb{F}_3}(\alpha) = 0$ over $\mathbb{F}_{3^3}$ yields $X = z \in \mathbb{F}_{3^3}$ where $z^3 + 2z + 1 = 0$. So $\mathcal{R}(T+z) = T^9 + T^6 + T^4 + T^3 + T^2 + T + 1 = \mathcal{S}$, which

is a c -Wieferich prime in $\mathbb{F}_{3^4}[T]$, that is defined over $\mathbb{F}_3$. Furthermore, for $r = 7$, solving $X^3 - X - 2\text{Tr}_{\mathbb{F}_{3^3}/\mathbb{F}_3}(\alpha) = 0$ over $\mathbb{F}_{3^3}$ yields $x = 2z \in \mathbb{F}_{3^3}$, where $z^3 + 2z + 1 = 0$. We obtain the prime $\mathcal{T} = \mathcal{R}(T + 2z) = T^9 + T^6 + T^4 + 2T^3 + T^2 + 2$ which is another fixed prime in $\mathbb{F}_3[T]$ that is a c -Wieferich prime in $\mathbb{F}_{3^7}[T]$. The other fixed primes in $\mathbb{F}_3[T]$ of degree 9 are $T^9 + 2T^6 + 2T^4 + 2T^2 + 2T + 1$, $T^9 + 2T^6 + 2T^4 + T^3 + 2T^2 + T + 2$, and $T^9 + 2T^6 + 2T^4 + 2T^3 + 2T^2 + 1$. These are not c -Wieferich primes in any $\mathbb{F}_{3^k}[T]$. In fact, in $\mathbb{F}_{3^{10}}[T]$, the prime $\mathcal{R}$ resurfaces as a c -Wieferich prime, then $\mathcal{S}$ in $\mathbb{F}_{3^{13}}[T]$ and $\mathcal{T}$ in $\mathbb{F}_{3^{16}}[T]$ and the process/cycle is repeated.

Corollary 5.4. *Let $\mathcal{G}$ be a fixed subgroup of $\mathbb{F}_q$ of order p . If there exists a $\mathcal{G}$ -fixed c -Wieferich prime in $\mathbb{F}_q[T]$ of degree p , then each $\mathcal{G}$ -fixed prime in $\mathbb{F}_q[T]$ of degree p is a c -Wieferich prime in at-least one of the constant field extensions $\mathbb{F}_{q^r}[T]$ of $\mathbb{F}_q[T]$ where $r \in \{1, \dots, p-1\}$.*

Proof. Theorem 5.3 shows that if there exists a $\mathcal{G}$ -fixed c -Wieferich prime in $\mathbb{F}_q[T]$ of degree p , then we will find $p^{-1}q$ $\mathcal{G}$ -fixed c -Wieferich primes in $\mathbb{F}_{q^r}[T]$ for $r = 1 + sk$ with $0 \leq k < p-1$. All these primes are distinct giving a total $p^{-1}q(p-1)$ primes. Let $\mathcal{G} = \chi\mathbb{F}_p$ for some $\chi \in \mathbb{F}_q^\times$. The map $\theta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ defined by $\theta(x) = x^p - \chi x$ is $\mathbb{F}_p$ -linear whose image has size $p^{-1}q$. By Theorem 2.1, the number of almost Artin-Schreier primes in $\mathbb{F}_q[T]$ of degree p is $q - p^{-1}q = p^{-1}q(p-1)$. By Theorem 2.5, a $\mathcal{G}$ -fixed prime of degree p is an almost Artin-Schreier prime, hence the result. $\square$

Remark 5.5. Corollary 5.4 does not contradict the existence of more than one almost Artin-Schreier c -Wieferich primes in $\mathbb{F}_q[T]$. It asserts that when any such prime is considered, we can use Theorem 5.3. to find extensions where all the rest of the $\mathcal{G}$ -fixed primes in $\mathbb{F}_q[T]$ will be c -Wieferich primes. For example, for $q = 13$, there exists two distinct c -Wieferich primes $T^{13} + 12T + 1$ and $T^{13} + 12 + 8$ of Artin-Schreier type. These stem from different α s, in particular $\alpha \in B_{13,1} = \{5, 12\}$. But they will yield the same Artin-Schreier/ c -Wieferich primes $\{T^{13} + 12T + 1, T^{13} + 12T + 2, \dots, T^{13} + 12T + 12\}$ although in different extension rings. For example, if $q = 13$ and $r = 2$, then the “line” of c -Wieferich primes $\mathcal{P}_1 = T^{13} + 12T + 1$ yields $T^{13} + 12T + 7$ while that of $\mathcal{P}_2 = T^{13} + 12T + 8$ yields $T^{13} + 12T + 4$.

From our extensive computations, we were unable to find any non-fixed c -Wieferich prime in $\mathbb{F}_q[T]$ for odd characteristic. However, for characteristic two fields, we found more examples of non-fixed c -Wieferich primes. These results generalize those of [1, Sec. 5] on computing c -Wieferich primes.

Acknowledgment

We thank A. Keet, F. Breuer and D. Thakur for their patience and their helpful comments after reading the many drafts of this paper. The first author also thanks the second for hosting him as postdoc at Stockholm University. This research was (in part) carried out at the Department of Mathematics, Makerere University and at

the Institute with Department of Stockholm University with financial support from the Makerere-Sida Bilateral Programme Phase IV, Project 316 “Capacity building in Mathematics and its applications”.

References

- [1] A. Bamunoba, A note on Carlitz Wieferich primes, *J. of Number Theory* **174** (2017) 343–357.
- [2] L. Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935) 137–168.
- [3] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Vol. 35 (Springer, 1998).
- [4] T. Garefalakis, On the action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, *J. Pure Appl. Algebra* **215** (2011) 1835–1843.
- [5] R. Lidl and H. Niederreiter, *Finite Fields (The Encyclopedia of Mathematics and its Applications)* (Cambridge University Press, 1997).
- [6] V. Mauduit, Carmichael-Carlitz polynomials and Carlitz-Fermat quotients, Finite fields and applications (Glasgow, 1995), London Mathematical Society Lecture Note Series, Vol. 233 (Cambridge Univ. Press, 1996), pp. 229–242.
- [7] D. Quan Nguyen Ngoc, Carlitz module analogues of Mersenne primes, Wieferich primes, and certain prime elements in cyclotomic function fields, *J. Number Theory* **125** (2014) 181–193.
- [8] L. Reis, The action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited, *J. Pure Appl. Algebra* **222**(5) (2018) 1087–1094.
- [9] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics (Springer-Verlag, Berlin, New York, 2002).
- [10] W. Stein *et al.*, *Sage Mathematics Software (Version 8.6)*, The Sage Development Team, <http://www.sagemath.org/>.
- [11] D. Thakur, Iwasawa theory and cyclotomic function fields, in *Proceedings of the Conference on Arithmetic Geometry (Tempe, AZ 1993)*, eds. J. Jones and N. Childress, Contemporary Mathematics, Vol. 174 (American Mathematical Society, 1994), pp. 157–165.
- [12] D. Thakur, *Function Field Arithmetic* (World Scientific Publishing Co, Inc., 2004).
- [13] D. Thakur, Fermat vs Wilson congruences, arithmetic derivatives and zeta values, *Finite Fields Appl.* **32** (2015) 192–206.