A function field approach toward good polynomials for further results on optimal LRC codes

Ruikai Chen, Sihem Mesnager

Version of Record: https://www.sciencedirect.com/science/article/pii/S1071579722000375
Manuscript_deb4f1535db298bb1fae00b325005dc8

A Function Field Approach Toward Good Polynomials for Further Results on Optimal LRC Codes

Ruikai Chen[1] and Sihem Mesnager[1,2]

[1] Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis, Laboratory Geometry, Analysis and Applications, LAGA, University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France,
chen_rk@outlook.com
[2] Telecom Paris, Polytechnic Institute of Paris, 91120 Palaiseau, France.
smesnager@univ-paris8.fr

Abstract. Because of the recent applications to distributed storage systems, researchers have introduced a new class of block codes, i.e., locally recoverable (LRC) codes. LRC codes can recover information from erasure(s) by accessing a small number of erasure-free code symbols and increasing the efficiency of repair processes in large-scale distributed storage systems. In this context, Tamo and Barg first gave a breakthrough by cleverly introducing a good polynomial notion. Constructing good polynomials for locally recoverable codes achieving Singleton-type bound (called optimal codes) is challenging and has attracted significant attention in recent years. This article aims to increase our knowledge of good polynomials for optimal LRC codes. Using tools from algebraic function fields and Galois theory, we continue investigating those polynomials and studying them by developing the Galois theoretical approach initiated by Micheli in 2019. Specifically, we push further the study of a crucial parameter $\mathcal{G}(f)$ (of a given polynomial f), which measures how much a polynomial is "good" in the sense of LRC codes. We provide some characterizations of polynomials with minimal Galois groups and prove some properties of finite fields where polynomials exist with a specific size of Galois groups. We also present some explicit shapes of polynomials with small Galois groups. For some particular polynomials f, we give the exact formula of $\mathcal{G}(f)$.

Keywords: Finite fields · Algebraic function fields · Galois groups · Good polynomials · LRC (Locally Recoverable) codes · Coding theory · Dickson polynomials.
Mathematics Subject Classification: 12E05, 11C08, 94B05.

1 Introduction

Locally recoverable (LRC) codes can recover information from erasure(s) by accessing a small number of erasure-free code symbols and increasing the efficiency of repair processes in large-scale distributed storage systems. LRC codes

and their variants have been extensively studied in recent years. In 2014, Tamo and Barg proposed in a very remarkable paper [**?**] a family of locally recoverable codes via so-called *good polynomials*. For an LRC code of locality r, a polynomial f over the finite field $\mathbb{F}_q$ of q elements (where q is a prime power) is called a good polynomial, if

1. the degree of f is $r+1$;
2. there exists a partition $\{A_1, \ldots, A_{\frac{N}{r+1}}\}$ of a set $A \subseteq \mathbb{F}_q$ of size N into sets of size $r+1$ such that f as a polynomial function is constant on each set A_i in the partition.

A good polynomial is a key ingredient for constructing optimal linear LRC codes. Tamo and Barg also constructed some polynomials with some restrictions. If there is an additive or multiplicative subgroup of order n of $\mathbb{F}_q$ (i.e., $q \equiv 0, 1 \pmod{n}$), then the annihilator polynomial of the subgroup is constant on each of its cosets. Based on their work, Liu, Mesnager, and Chen ([**?**]) presented more general construction approaches using function composition. Also, Liu, Mesnager, and Tang ([**?**]) have proved that the well-known Dickson polynomials and their composition with some functions are good candidates for good polynomials. Very recently in [**?**], good polynomials of low degree over finite fields have been characterized completely, leading to optimal LRC with new flexible localities.

In the sense of coding theory, if there exists m number of such subsets of $\mathbb{F}_q$ on which f is constant, then one can construct a locally recoverable code of length mn. Obviously, those polynomials with m large are preferred. Therefore, it is natural to introduce a parameter indicating how "good" a polynomial is. For a polynomial f of degree n over $\mathbb{F}_q$, define

$$\mathcal{G}(f) = |\{c \in \mathbb{F}_q \mid f(T) - c \text{ has } n \text{ distinct roots in } \mathbb{F}_q\}|$$

(where $|E|$ denotes the cardinality of a finite set E). By a simple investigation we have $\mathcal{G}(f) \leq \lfloor q/n \rfloor$. Micheli ([**?**]) discussed this problem in the context of algebraic function fields and Galois theory, pointing out that $\mathcal{G}(f)$ can be estimated by the order of its corresponding Galois group. In short, given an extension of rational function fields $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ defined by $f(x) = t$ with Galois closure M, if some condition is satisfied, then $\mathcal{G}(f)$ is close to $q/[M : \mathbb{F}_q(t)]$, with an error term $O(\sqrt{q})$. Note that up to the error term, the quantity $\mathcal{G}(f)$ must be q/m for some divisor m of $n!$. We can then characterize the Galois closure M, working on the function fields defined by the polynomial f, instead of studying the algebraic structure of $\mathbb{F}_q$.

The remainder of the paper is organized as follows. In Section **??**, we provide some background on algebraic function fields and notation used through this study. In Section **??**, we characterize those polynomials with minimal Galois groups and prove some properties of finite fields where polynomials exist with a specific size of Galois groups. By showing that, we know that expected good polynomials do not exist under several circumstances. In Section **??**, we present some explicit forms of polynomials with small Galois groups by considering the Dickson polynomials of the first kind and powers of linearized polynomials. For some particular polynomials f, the exact formula of $\mathcal{G}(f)$ is given.

2 Preliminaries

Let us first recall some basic concepts on algebraic function fields (see [**?**] for details). For an algebraic function field F/K (F is a finite extension of $K(t)$ for some t transcendental over K), the full constant field consists of all algebraic elements over K in F. For a place of F/K, let $\mathcal{O}_P$ be its valuation ring and v_P its discrete valuation. There is a one-to-one correspondence between the places and the discrete valuations of F/K. The triangle inequality for a discrete valuation is

$$v_P(a+b) \geq \min\{v_P(a), v_P(b)\},$$

for all $a, b \in F$, where the equality holds if $v_P(a) \neq v_P(b)$. The place P is called a zero of $a \in F$ if $v_P(a) > 0$, and a pole if $v_P(a) < 0$. Note that P is the unique maximal ideal of $\mathcal{O}_P$ and $K \subseteq \mathcal{O}_P$, so K can be embedded into $\mathcal{O}_P/P$. The degree of P is defined as $\deg(P) = [\mathcal{O}_P/P : K]$, and a place of degree one is called a rational place.

Assume that K is the full constant field of F/K and let F'/K', with full constant field K', be a finite separable extension of F/K. We say a place P' of F'/K' lies above P (or P lies below P') if $P \subseteq P'$. In this case, there exists a positive integer $e = e(P' \mid P)$ such that $v_{P'}(a) = e \cdot v_P(a)$ for all $a \in F$, called the ramification index of P' over P. With $\mathcal{O}_{P'}/P'$ regarded as an extension of $\mathcal{O}_P/P$, the relative degree of P' over P is $f(P' \mid P) = [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$. These two numbers satisfy

$$\sum_{P'} e(P' \mid P) f(P' \mid P) = [F' : F], \tag{1}$$

where the sum is extended over all places P' of F'/K' lying above P. If $e(P' \mid P) > 1$, then P' is said to be ramified in F'/F, and if there exists a ramified place of F'/K' lying above P, then P is said to be ramified in F'/F. Furthermore, a place P of F is said to split completely in F' if $e(P' \mid P) = f(P' \mid P) = 1$ for any place P' of F'/K' lying above P. If there is a place of F'/K' lying above a rational place of F/K with relative degree one, then $K' = K$. Particularly, if F'/F is Galois, then the Galois group $\mathrm{Gal}(F'/F)$ acts transitively on the set of places of F'/K' lying above P, where each place has the same ramification index and relative degree over P. As a consequence, (**??**) becomes

$$r \cdot e(P' \mid P) f(P' \mid P) = [F' : F], \tag{2}$$

for the number r of places of F'/K' lying above P.

If $F = K(t)$ for some t transcendental over K, then $F/K = K(t)/K$ is called a rational function field. A place of $K(t)/K$ is either the infinite place (the pole of t), or the place corresponding to the localization of $K[t]$ at an irreducible polynomial $p(t)$. The latter is simply denoted by $(p(t))$ if there is no ambiguity. We have special interest in a class of extensions of rational function fields. For two relatively prime polynomials f_0, f_1 over K, let x be an element in some extension of $K(t)$ satisfying $f_0(x)/f_1(x) = t$. Then $K(x)$, as an extension of

$K(t)$, is also a rational function field. The minimal polynomial of x over $K(t)$ is $f_0(T) - tf_1(T) \in K(t)[T]$, so that $[K(x) : K(t)] = \max\{\deg(f_0), \deg(f_1)\}$. If $f_1(x) = 1$ and $K(x)/K(t)$ is separable, then a place of $K(x)$ is ramified in $K(x)/K(t)$ if and only if it is the infinite place or a zero of $f_0'(x)$, where f_0' denotes the formal derivative of f_0. In general, for $c \in K$, if $f_0(T) - c$ is factored into irreducible polynomials in $K[T]$ as $\prod_{i=1}^{r} \varphi_i(T)^{e_i}$, then exactly the r places $(\varphi_1(x)), \ldots, (\varphi_r(x))$ of $K(x)$ lie above the place $(t - c)$ of $K(t)$, with $e((\varphi_i(x)) \mid (t - c)) = e_i$ and $f((\varphi_i(x)) \mid (t - c)) = \deg(\varphi_i)$.

For our purpose, the two lemmas are also necessary.

Lemma 1 ([?, Lemma 3.9.5]). *Let F'/F be a finite separable extension of function fields and let L be the Galois closure of F'/F. If a place P of F splits completely in F'/F, then P also splits completely in L/F.*

Lemma 2 ([?, Lemma 6.8]). *Let K be an arbitrary field and $t = f(x) \in K[x] \setminus K$ for a polynomial f over K, such that $K(x)$ and $K(t)$ are rational function fields. Then every intermediate field of $K(x)/K(t)$ is of the form $K(h(x))$ for some polynomials g, h over K such that $f = g \circ h$.*

Throughout this paper, we use the notation as follows. Given a finite field $\mathbb{F}_q$ with characteristic p, let f be a polynomial of degree $n < q$ over $\mathbb{F}_q$. Consider the rational function field $\mathbb{F}_q(t)$ with t transcendental over $\mathbb{F}_q$, and its finite extension $\mathbb{F}_q(x)$ defined by $f(x) = t$. Note that if $f(T) \in \mathbb{F}_q[T^p]$, then $f(T) - c$ will never have n distinct roots in $\mathbb{F}_q$ for any $c \in \mathbb{F}_q$. Therefore, suppose $f(T) \notin \mathbb{F}_q[T^p]$, so that $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is a finite separable extension. Then the splitting field of $f(T) - t$ over $\mathbb{F}_q(t)$ is exactly the Galois closure of $\mathbb{F}_q(x)/\mathbb{F}_q(t)$, denoted by M. In this sense, the Galois group of f is defined to be $\mathrm{Gal}(M/\mathbb{F}_q(t))$. We also assume that f is monic and $f(0) = 0$, since $\mathbb{F}_q(t) = \mathbb{F}_q(at + b)$ for any $a, b \in \mathbb{F}_q$ with $a \neq 0$.

The properties of f as a mapping on $\mathbb{F}_q$ are often associated with the structure of its Galois group. Specifically speaking, for $c \in \mathbb{F}_q$, if $f(T) - c$ splits into n distinct linear factors in $\mathbb{F}_q[T]$, then the rational place $(t - c)$ of $\mathbb{F}_q(t)$ splits completely in $\mathbb{F}_q(x)$. In 1970, Cohen showed the distribution of $f(T) - c$ with prescribed factorization as c varies over $\mathbb{F}_q$ ([**?**]), and recently Micheli gave a more specific description in [**?**]. The main result we need is presented in the following lemma.

Lemma 3 ([?]). *If the full constant field of $M/\mathbb{F}_q$ is $\mathbb{F}_q$, then*

$$\mathcal{G}(f) = \frac{q}{[M : \mathbb{F}_q(t)]} + O(\sqrt{q}).$$

More precisely,

$$\frac{q + 1 - 2g\sqrt{q}}{[M : \mathbb{F}_q(t)]} - \frac{R}{2} \leq \mathcal{G}(f) \leq \frac{q + 1 + 2g\sqrt{q}}{[M : \mathbb{F}_q(t)]},$$

where R is the number of ramified places of $M/\mathbb{F}_q(t)$ of degree one, and g is the genus of $M/\mathbb{F}_q$, both bounded by a constant independent of q.

The error term $O(\sqrt{q})$ is neglectable when q is sufficiently large. Therefore, in what follows, we study the splitting field M of $f(T)-t$ over $\mathbb{F}_q(t)$, as well as the corresponding Galois group. To construct a good polynomial, we can turn to find a polynomial f with $[M:\mathbb{F}_q(t)]$ as small as possible, such that $\mathbb{F}_q$ is the full constant field of $M/\mathbb{F}_q$. Meanwhile, by showing these polynomials' properties, it is clear that good polynomials do not exist in some cases.

3 Properties of Polynomials with Certain Size of Galois Groups

By Lemma **??**, the number $\mathcal{G}(f)$, which we are interested in, is approximately $q/[M:\mathbb{F}_q(t)]$. For the Galois group G of f, we have $n! \geq |G| = [M:\mathbb{F}_q(t)] = n[M:\mathbb{F}_q(x)] \geq n$. In most cases, $|G|$ is close to $n!$, so it is significant to discover the properties of f with $|G|$ small enough. Then we can assert that the desired polynomials do not exist with some given conditions. To begin with, we study the extreme case $|G| = n$, or equivalently $M = \mathbb{F}_q(x)$.

Proposition 4. *The splitting field of $f(T)-t$ over $\mathbb{F}_q(t)$ is $\mathbb{F}_q(x)$, if and only if*

$$f(T) = (h(T)+c)^k - c^k,$$

where $n = kp^l$ for $k, l \in \mathbb{N}$ with $q \equiv p^l \equiv 1 \pmod{k}$, $h(T) = \sum_{b\in B}(T-b)$ for an additive subgroup B of order p^l in $\mathbb{F}_q$ such that $\omega B = B$, ω a primitive k-th root of unity in $\mathbb{F}_q$, and $c = h(\alpha)$ for some $\alpha \in \mathbb{F}_q$.

Proof. Suppose $n > 2$. Since x is one root of $f(T)-t$, and all other roots, denoted by $g_1(x), \ldots, g_{n-1}(x)$, lie in $\mathbb{F}_q(x)$, one has

$$(-1)^n x g_1(x) \cdots g_{n-1}(x) = -t = -f(x). \tag{3}$$

For $i = 1, \ldots, n-1$, it follows from the equation $f(g_i(x)) - f(x) = 0$ that $g_i(x)$ is integral over $\mathbb{F}_q[x]$. The fact that $\mathbb{F}_q[x]$ is integrally closed then implies $g_i(x) \in \mathbb{F}_q[x]$, and then $\deg(g_i) = [\mathbb{F}_q(x) : \mathbb{F}_q(g_i(x))] = 1$. Now $g_i(x) = a_i x + b_i$ for some $a_i, b_i \in \mathbb{F}_q$ with $a_i \neq 0$. Note that the Galois group $G = \{\sigma_0, \ldots, \sigma_{n-1}\}$ of $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ is given by $\sigma_0(x) = x$ and $\sigma_i(x) = g_i(x)$, with $\sigma_i^n = \sigma_0$. By induction it is easily seen that

$$x = \sigma_i^n(x) = a_i^n x + (a_i^{n-1} + \cdots + a_i + 1)b_i,$$

so $a_i^n = 1$.

Suppose $\gcd(n, q-1) = 1$, which means $a_i = 1$ for each i. For $j = 0, \ldots, n-1$, we have $\sigma_j(g_i(x)) = g_i(g_j(x)) = x + b_i + b_j$ is also a root of $f(T) - t$. Since G acts transitively on $\{x, g_1(x), \ldots, g_{n-1}(x)\}$, for each i we have $b_i + b_j = 0$ for some j. It follows that the distinct n elements, $0, b_1, \ldots, b_{n-1}$, form an additive subgroup of $\mathbb{F}_q$. This happens only if n divides q. From (**??**) it follows that

$$f(x) = x(x-b_1)\cdots(x-b_{n-1}).$$

Now let $\gcd(n, q-1) \neq 1$. By the same argument, the n (not necessarily distinct) elements $1, a_1, \ldots, a_{n-1}$, where each occurs the same time, form a multiplicative subgroup of $\mathbb{F}_q$. While they are all n-th roots of unity, the subgroup is generated by ω, a primitive k-th root of unity for some integer k dividing n. If $n = k$, then G is cyclic and the n roots of $f(T) - t$ are given by $g_i(x) = \omega^i x + \frac{\omega^i - 1}{\omega - 1} b_1$, and according to (**??**),

$$f(x) = (-1)^{n-1} \prod_{i=0}^{n-1} \left(\omega^i x + \frac{\omega^i - 1}{\omega - 1} b_1 \right),$$

and then

$$\begin{aligned} f\left(x - \frac{b_1}{\omega - 1}\right) =& (-1)^{n-1} \prod_{i=0}^{n-1} \left(\omega^i x - \frac{b_1}{\omega - 1} \right) \\ =& (-1)^{n-1} \omega^{1+\cdots+n-1} \prod_{i=0}^{n-1} \left(x - \frac{\omega^{-i} b_1}{\omega - 1} \right) \\ =& x^n - \left(\frac{b_1}{\omega - 1} \right)^n. \end{aligned}$$

If $n > k$, then there are exactly n/k roots of $f(T) - t$ in the form: $x, x + \beta_1, \ldots, x + \beta_{n/k-1}$, with $\beta_1, \ldots, \beta_{n/k-1} \in \mathbb{F}_q^*$. Apparently $0, \beta_1, \ldots, \beta_{n/k-1}$ form an additive subgroup B of order n/k, so $n = kp^l$ for some $l \in \mathbb{N}$. The corresponding automorphisms of $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ also form a subgroup H of G. More precisely, it is a normal subgroup. If $\sigma \in G \setminus H$, i.e., $\sigma(x) = \omega^i x + \beta$ for some $\beta \in \mathbb{F}_q$ and $\omega^i \neq 1$, then $(\sigma^k)(x) = \omega^{ik} x + \frac{\omega^{ik} - 1}{\omega^i - 1} \beta = x$. The order of σ then divides k, while $\gcd(k, p^l) = 1$, so there is no other conjugate of H. Since H is normal, we have $\sigma^{-1} H \sigma = H$. Provided $\sigma' \in H$ with $\sigma'(x) = x + \beta_j$ $(0 < j < p^l)$, and $\sigma(x) = \omega^{-1} x + \beta$, it follows that $\sigma^{-1}(x) = \omega(x - \beta)$ and $(\sigma^{-1}\sigma'\sigma)(x) = \omega(\omega^{-1} x + \beta_j) = x + \omega\beta_j$. Then $\omega B = B$, which happens if and only if B is a vector space over $\mathbb{F}_p(\omega)$. Thus p^l is a power of the order of $\mathbb{F}_p(\omega)$, and $p^l \equiv 1 \pmod{k}$. Subsequently we determine the specific form of f.

By Lemma **??** and the fundamental theorem of Galois theory, there exists an intermediate field $\mathbb{F}_q(u)$ of $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ such that $t = g(u) \in \mathbb{F}_q[u]$ and $u = h(x) \in \mathbb{F}_q[x]$. Moreover, $H = \mathrm{Gal}(\mathbb{F}_q(x)/\mathbb{F}_q(u))$ and $\mathbb{F}_q(u)/\mathbb{F}_q(t)$ is a Galois extension of degree $k = \deg(g)$. Without loss of generality, let g and h be monic. As discussed before, $h(x) - h(0) = \sum_{b \in B} (x - b)$, and $g(u) - g(0) = (u + c)^k - c^k$ for some $c \in \mathbb{F}_q$. Hence

$$f(x) = \left(\sum_{b \in B} (x - b) + h(0) + c \right)^k - c^k + g(0).$$

It then suffices to set $g(0) = h(0) = 0$ for convenience. If one root of $f(T) - t$ is $\omega x + \beta$ for some $\beta \in \mathbb{F}_q$, then

$$(h(x) + c)^k - c^k = (h(\omega x + \beta) + c)^k - c^k,$$

which means

$$(h(x)+c)^k = (h(\omega x)+h(\beta)+c)^k = (\omega h(x)+h(\beta)+c)^k.$$

It follows that

$$\omega^i(h(x)+c) = \omega h(x)+h(\beta)+c$$

for some integer i. Since x is transcendental over $\mathbb{F}_q$, one has $\omega^i = \omega$ and $c = (\omega-1)^{-1}h(\beta) = h\left((\omega-1)^{-1}\beta\right)$.

With the above discussion, the converse is obvious. □

Now we have characterized those polynomials with minimal Galois groups. It turns out that they coincide with those constructed in [**?**]. The following result is already known, but it can be immediately derived as a consequence of the above proposition (cf. Proposition 3.2 and Theorem 3.3 in [**?**]). The converse is also true when q is sufficiently large with n fixed.

Corollary 5. *For the polynomial f of degree n over $\mathbb{F}_q$, $\mathcal{G}(f) = \left\lfloor \frac{q}{n} \right\rfloor$ if the condition in Proposition* **??** *is satisfied.*

Example 6. Let $q = 64$ and $n = 12 = 3 \times 2^2$. Note that $64 \equiv 2^2 \equiv 1 \pmod 3$, and $\omega^3 = 1$ implies $\omega^4 - \omega = 0$. Set $f(T) = (T^4 - T)^3$, so that $M = \mathbb{F}_q(x)$ and $\mathcal{G}(f) = 5$.

Observe that all those polynomials in Proposition **??** split completely over $\mathbb{F}_q$. In fact, we can prove more.

Theorem 7. *For some $c \in \mathbb{F}_q$, if $f(T)-c$ has an irreducible factor of multiplicity 1 in $\mathbb{F}_q[T]$, then the multiplicity of every irreducible factor of $f(T)-c$ divides $[M : \mathbb{F}_q(x)]$; if $f(T)-c$ has a root in $\mathbb{F}_q$, then the degree of every irreducible factor of $f(T)-c$ divides $[M : \mathbb{F}_q(x)]$.*

Proof. Let $\varphi_1(T)$ be an irreducible factor of multiplicity 1 of $f(T)-c$ in $\mathbb{F}_q[T]$ and assume that there is another irreducible factor $\varphi_2(T)$ of $f(T)-c$. Then $(\varphi_1(x))$ and $(\varphi_2(x))$ are places of $\mathbb{F}_q(x)/\mathbb{F}_q$ lying above the rational place $(t-c)$ of $\mathbb{F}_q(t)/\mathbb{F}_q$, with $e((\varphi_1(x)) \mid (t-c)) = 1$. Let P_1 and P_2 be places of M lying above $(\varphi_1(x))$ and $(\varphi_2(x))$ respectively. Since $M/\mathbb{F}_q(x)$ and $M/\mathbb{F}_q(t)$ are Galois, it follows from (**??**) that $e(P_1 \mid (\varphi_1(x)))$ divides $[M : \mathbb{F}_q(x)]$, and

$$\begin{aligned}
& e(P_2 \mid (\varphi_2(x)))e((\varphi_2(x)) \mid (t-c)) \\
=& e(P_2 \mid (t-c)) \\
=& e(P_1 \mid (t-c)) \\
=& e(P_1 \mid (\varphi_1(x)))e((\varphi_1(x)) \mid (t-c)) \\
=& e(P_1 \mid (\varphi_1(x))).
\end{aligned}$$

Hence, the multiplicity of $\varphi_2(T)$, equal to $e(\varphi_2(x) \mid (t-c))$, divides $[M : \mathbb{F}_q(x)]$. Consider the relative degree, and then the second assertion follows immediately. □

This theorem gives an easy way to determine a lower bound of $[M : \mathbb{F}_q(x)]$ for some polynomial f. Note that $f(0) = 0$, and we may suppose that $f(T)/T$ has irreducible factors of degree $d_1, \ldots, d_k$. Then $[M : \mathbb{F}_q(x)]$ is a multiple of $\mathrm{lcm}(d_1, \ldots, d_k)$. For instance, if $q = 19$ and $f(T) = T(T^2 + 1)(T^3 + 2T + 1)$, where $T^2 + 1$ and $T^3 + 2T + 1$ are irreducible in $\mathbb{F}_{19}[T]$, then $[M : \mathbb{F}_q(x)]$ is divisible by 6. On the other hand, we also learn that it is more likely to obtain a good polynomial for LRC codes, if choosing a polynomial splitting completely over $\mathbb{F}_q$.

It has been shown that only a few polynomials satisfy the condition for $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ being Galois. Now we investigate those for which $[M : \mathbb{F}_q(x)] > 1$. If this is the case, then there must exist another root y of $f(T) - t$ lying outside $\mathbb{F}_q(x)$, such that $\mathbb{F}_q(x)$ is isomorphic to $\mathbb{F}_q(y)$. We will start with the minimal polynomial of y over $\mathbb{F}_q(x)$.

Lemma 8. *Let $y \in M \setminus \mathbb{F}_q(x)$ be a root of $f(T) - t$ with minimal polynomial $T^m + a_{m-1}(x)T^{m-1} + \cdots + a_0(x)$ over $\mathbb{F}_q(x)$. Then $a_i(x) \in \mathbb{F}_q[x]$, $\deg(a_i) \le m - i$ for $0 \le i < m$ and $\deg(a_0) = m$.*

Proof. Note that $a_i(x)$ can be written as $a_i(x) = u_i(x)/v_i(x)$ for relatively prime polynomials u_i and v_i over $\mathbb{F}_q$. Then $y^m + a_{m-1}(x)y^{m-1} + \cdots + a_0(x) = 0$ is equivalent to

$$v(x)y^m + \frac{u_{m-1}(x)v(x)}{v_{m-1}(x)}y^{m-1} + \cdots + \frac{u_0(x)v(x)}{v_0(x)} = 0,$$

where $v(x) = v_0(x) \cdots v_{m-1}(x)$. Let $d = \gcd(v, \frac{u_{m-1}v}{v_{m-1}}, \ldots, \frac{u_0 v}{v_0})$, so that

$$F(T) = \frac{1}{d(T)}\left(v(T)y^m + \frac{u_{m-1}(T)v(T)}{v_{m-1}(T)}y^{m-1} + \cdots + \frac{u_0(T)v(T)}{v_0(T)}\right)$$

is a polynomial in $\mathbb{F}_q[y][T]$. Assume that $F(T)$ is reducible over $\mathbb{F}_q(y)$. By Gauss's Lemma, it is also reducible over $\mathbb{F}_q[y]$; that is, $F(T) = F_1(T)F_2(T)$ for some $F_1(T), F_2(T) \in \mathbb{F}_q[y][T] \setminus \mathbb{F}_q[y]$, with $F_1(x) = 0$ or $F_2(x) = 0$. If $F_1(T), F_2(T) \notin \mathbb{F}_q[T]$, then y is a root of a polynomial of lower degree over $\mathbb{F}_q(x)$. Hence, we may suppose $F_1(T) \in \mathbb{F}_q[T]$. According to the definition of $d(T)$, this happens only if $F_1(T) \in \mathbb{F}_q$. The contradiction shows that $F(T)$ is irreducible over $\mathbb{F}_q(y)$, with a root x. The degree of $F(T)$ is

$$[\mathbb{F}_q(x, y) : \mathbb{F}_q(y)] = \frac{[\mathbb{F}_q(x, y) : \mathbb{F}_q(t)]}{[\mathbb{F}_q(x) : \mathbb{F}_q(t)]} = \frac{[\mathbb{F}_q(x, y) : \mathbb{F}_q(t)]}{[\mathbb{F}_q(y) : \mathbb{F}_q(t)]} = [\mathbb{F}_q(x, y) : \mathbb{F}_q(x)],$$

so $\deg(u_0) - \deg(v_0) + \deg(v) - \deg(d) \le m$.

Let P be a place of $\mathbb{F}_q(x, y)$ lying above the infinite place P_∞ of $\mathbb{F}_q(x)$ with v_P the corresponding discrete valuation of P, and let e be the ramification index of P over P_∞. Note that $f(x) = f(y)$, i.e.,

$$x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = y^n + \alpha_{n-1}y^{n-1} + \cdots + \alpha_0,$$

for some $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{F}_q$. If $v_P(y) \geq 0$, then $v_P(f(y)) \geq 0$, but $v_P(f(x)) = -n \cdot e < 0$. As a result, $v_P(f(x)) = v_P(f(y)) = n \cdot v_P(y)$, by the triangle inequality, and then $v_P(y) = -e$. The same argument applies to the conjugates $y_1, \ldots, y_m$ of y with respect to $\mathbb{F}_q(x)$. It follows that

$$v_P(a_0(x)) = v_P(y_1) + \cdots + v_P(y_m) = -me,$$

and

$$v_P(a_i(x)) \geq v_P(y_1) + \cdots + v_P(y_{m-i}) = -(m-i)e,$$

for $i = 1, \ldots, m-1$, using the formula of the elementary symmetric polynomials. This indicates $\deg(u_0) - \deg(v_0) = m$ and $\deg(u_i) - \deg(v_i) \leq m - i$. Recalling that $\deg(u_0) - \deg(v_0) + \deg(v) - \deg(d) \leq m$ and d divides v, we have $\deg(v) = \deg(d)$. Then v divides $\frac{u_0 v}{v_0}, \ldots, \frac{u_{m-1} v}{v_{m-1}}$, and clearly $a_0(x), \ldots, a_{m-1}(x) \in \mathbb{F}_q[x]$. This completes the proof. □

Remark 9. The inequality $0 \leq \deg(a_i) \leq m-i$ for $0 \leq i < m$ is sharp in general. For example, let $f(T) = (T^3 + 1)^2$ over $\mathbb{F}_q$, where $\gcd(2, q) = \gcd(3, q) = 1$. Then there are elements x and y such that $f(x) = f(y) = t$ and $x^3 + y^3 + 2 = 0$. The minimal polynomial of y over $\mathbb{F}_q(x)$ is $T^3 + x^3 + 2$. On the other hand, let $f(T) = T^3 + T$ over $\mathbb{F}_q$, where $q \equiv 1 \pmod 3$. It is easy to verify that if $f(y) = f(x) = t$ and $y \neq x$, then the minimal polynomial of y over $\mathbb{F}_q(x)$ is $T^2 + xT + x^2 + 1$.

Let $\tau : \mathbb{F}_q(t) \to \mathbb{F}_q(u)$ be an isomorphism fixing $\mathbb{F}_q$ with $\tau(t) = u$ for some u transcendental over $\mathbb{F}_q$, and M' be the splitting field of $f(T) - u$. Then τ can be extended to an isomorphism from M to M'. If $f(x) = f(y) = t$, then $f(\tau(x)) = f(\tau(y)) = u$, and the minimal polynomial of $\tau(y)$ over $\mathbb{F}_q(\tau(x))$ is obtained by applying τ to each coefficients of that of y over $\mathbb{F}_q(x)$. Thus it suffices to study the function field defined by $f(x) = t^n$. To this end, we introduce the field of formal Laurent series over $\overline{\mathbb{F}_q}$.

Lemma 10 ([?, Theorem 6.12]). *Let $\overline{\mathbb{F}_q}((t))$ be the field of formal Laurent series $\sum_{j \geq j_0} c_j / t^j$ with $c_j \in \overline{\mathbb{F}_q}$. If $\gcd(n, q) = 1$, then there exists $\delta(t) = t + \sum_{j \geq 0} c_j / t^j \in \overline{\mathbb{F}_q}((t))$ such that $f(\delta(t)) = f(\delta(\omega t)) = t^n$, where $\omega \in \overline{\mathbb{F}_q}$ is a primitive n-th root of unity.*

Theorem 11. *If $[M : \mathbb{F}_q(x)] = m$ and $\gcd(n, q) = 1$, then $q^m \equiv 1 \pmod n$.*

Proof. With the notation in the above lemma, it suffices to consider the splitting field of $f(T) - t^n$ over $\mathbb{F}_q(t^n)$. Now that $\delta(\omega t)$ and $\delta(t)$ are different roots of $f(T) - t^n$, it follows from Lemma **??** that

$$\delta(\omega t)^m + a_{m-1}(\delta(t))\delta(\omega t)^{m-1} + \cdots + a_0(\delta(t)) = 0,$$

for some polynomials $a_0, \ldots, a_{m-1}$ over $\mathbb{F}_q$ with $\deg(a_i) \leq m-i$ for $i = 0, \ldots, m-1$. Let $r_i \in \mathbb{F}_q$ be the $(m-i)$-th coefficient of a_i. Then the coefficient of t^m in the above equation is

$$\omega^m + r_{m-1}\omega^{m-1} + \cdots + r_0 = 0,$$

which means $\omega \in \mathbb{F}_{q^m}$. Since ω is a primitive n-th root of unity, n must divide $q^m - 1$. □

If $\gcd(n, q) = 1$ and $q^2 \equiv 1 \pmod{n}$, such polynomial f with $[M : \mathbb{F}_q(x)] = 2$ does exist, and has a unique form. We will leave it in the next section.

Example 12. Consider polynomials of degree $n = 5$. Note that $\phi(5) = 4$ and $q^4 \equiv 1 \pmod{5}$. If $q \equiv \pm 1 \pmod{5}$, then it is easy to find polynomials such that $[M : \mathbb{F}_q(x)] = 2$, as will be seen. If $q \equiv \pm 2 \pmod{5}$, then $[M : \mathbb{F}_q(x)] \geq 4$, since in this case neither $q^2 \equiv 1 \pmod{5}$ nor $q^3 \equiv 1 \pmod{5}$.

One may ask what happens if $\gcd(n, q) \neq 1$. In fact, under some conditions, we can obtain similar results.

Proposition 13. *Let $[M : \mathbb{F}_q(x)] = m$ and $n = kp^l$ for some integer m, k, l with $\gcd(k, q) = \gcd(m, q) = 1$. If the Galois group $G = \mathrm{Gal}(M/\mathbb{F}_q(t))$ has a normal Sylow p-subgroup, then $q^m \equiv 1 \pmod{k}$.*

Proof. Let P be the Sylow p-subgroup of G with fixed field E, and $H = P \cdot \mathrm{Gal}(M/\mathbb{F}_q(x))$. Then H is a subgroup of order mp^l, as $P \cap \mathrm{Gal}(M/\mathbb{F}_q(x))$ is trivial. The fixed field F of H is $E \cap \mathbb{F}_q(x)$, and $[F : \mathbb{F}_q(t)] = |G|/|H| = k$. By Lemma **??**, there exists some polynomials g of degree k over $\mathbb{F}_q$ such that $F = \mathbb{F}_q(u)$ with $g(u) = t$. Now $E/\mathbb{F}_q(t)$ is Galois by the assumption that P is normal, so the Galois closure of $\mathbb{F}_q(u)/\mathbb{F}_q(t)$ is contained in E, and its degree over $\mathbb{F}_q(u)$ divides $[E : \mathbb{F}_q(u)] = m$. It follows from the above theorems that $q^m \equiv 1 \pmod{k}$. □

4 Instances of Polynomials with Small Galois Groups

4.1 Dickson Polynomials

Let $D_n(T, a)$ be the Dickson polynomial (of the first kind) of degree n for some parameter $a \in \mathbb{F}_q$, defined as

$$D_n(T, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i T^{n-2i}.$$

When $a = 0$, it is a monomial. A basic property of this polynomial is that

$$D_n(u + \frac{a}{u}, a) = u^n + \frac{a^n}{u^n}$$

for an indeterminate u. Moreover, if $n = kp^l$ for some integers k, l with $\gcd(k, q) = 1$, then $D_n(T, a) = D_k(T, a)^{p^l}$. For this reason we may assume $\gcd(n, q) = 1$. Let $\omega \in \mathbb{F}_{q^2}$ be a primitive n-th root of unity. Then

$$D_n(T, a) = T \prod_{i=1}^{(n-1)/2} \left(T^2 + a(\omega^i - \omega^{-i})^2\right),$$

if n is odd, and

$$D_n(T,a) - D_n(0,a) = T^2 \prod_{i=1}^{n/2-1} \left(T^2 + a(\omega^i - \omega^{-i})^2\right),$$

if n is even.

There are many other essential properties of the Dickson polynomials. In the context of this paper, it turns out that they can be characterized in another way. First, we shall discuss further the conclusion of Lemma **??**, and then extend Theorem **??** in the quadratic case, with the explicit form of the polynomial f (still we always assume that f is monic and $f(0) = 0$).

Using the notation in Lemma **??**, we claim that if, in addition, $n > 2$ and the term of degree $n-1$ of f vanishes, then $c_0 = 0$ and $c_1 \in \mathbb{F}_q$ for the root $\delta(t) = t + \sum_{j\geq 0} c_j/t^j \in \overline{\mathbb{F}_q}((t))$ of $f(T) - t^n$. Denote $f(T) = T^n + \gamma T^{n-2} + \cdots$ for $\gamma \in \mathbb{F}_q$. It can be checked that

$$\delta(t)^n = t^n + nc_0t^{n-1} + \left(\frac{n(n-1)}{2}c_0^2 + nc_1\right)t^{n-2} + \cdots,$$

$$\delta(t)^{n-2} = t^{n-2} + (n-2)c_0t^{n-3} + \cdots,$$

$$\delta(t)^{n-3} = t^{n-3} + \cdots.$$

Since $\gcd(n,q) = 1$ and $t^n = f(\delta(t)) = \delta(t)^n + \gamma\delta(t)^{n-2} + \cdots$, comparing the coefficients we get $c_0 = 0$ and $nc_1 + \gamma = 0$.

Theorem 14. *If* $[M : \mathbb{F}_q(x)] = 2$ *and* $\gcd(n,q) = 1$*, then* $f(T) = D_n(T+b,a) - D_n(b,a)$ *for some* $a, b \in \mathbb{F}_q$.

Proof. Without loss of generality, assume that the coefficients of degree $n-1$ of f is 0. Then there is a root $\delta(t) = t + \sum_{j\geq 0} c_j/t^j \in \overline{\mathbb{F}_q}((t))$ of $f(T) - t^n$, where $c_0 = 0$ and $c_1 \in \mathbb{F}_q$. The roots of $f(T) - t^n$ are given by $u_0 = \delta(t), u_1 = \delta(\omega t), \ldots, u_{n-1} = \delta(\omega^{n-1}t)$ for a primitive n-th root ω of unity in $\mathbb{F}_{q^2}$, as shown in Theorem **??**. For an integer i, if $u_i \in \mathbb{F}_q(u_0)$, then $u_i = \alpha u_0 + \beta$ for some $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \neq 0$, as discussed in Proposition **??**. It follows that $\beta = 0$ and $\omega^i = \alpha = \omega^{-i}$, which means $\omega^i = -1$ with $n = 2i$.

Now suppose that $u_i \notin \mathbb{F}_q(u_0)$, and let u_j for some integer j be its conjugate with respect to $\mathbb{F}_q(u_0)$. For $r_1, r_0, s_2, s_1, s_0 \in \mathbb{F}_q$, denote by

$$T^2 + (r_1u_0 + r_0)T + s_2u_0^2 + s_1u_0 + s_0 \tag{4}$$

the minimal polynomial of u_i and u_j over $\mathbb{F}_q(u_0)$. Computing the coefficients of $\delta(\omega^i t)^2 + (r_1u_0 + r_0)\delta(\omega^i t) + s_2u_0^2 + s_1u_0 + s_0$ in t and the same for j leads to

$$\omega^{2i} + r_1\omega^i + s_2 = \omega^{2j} + r_1\omega^j + s_2 = 0, \tag{5}$$

$$r_0\omega^i + s_1 = r_0\omega^j + s_1 = 0, \tag{6}$$

$$2c_1 + c_1r_1(\omega^i + \omega^{-i}) + 2c_1s_2 + s_0 = 2c_1 + c_1r_1(\omega^j + \omega^{-j}) + 2c_1s_2 + s_0 = 0. \tag{7}$$

It follows immediately from (**??**) that $r_0 = s_1 = 0$. Assume $c_1 r_1 \neq 0$. Then multiplying (**??**) by ω^i or ω^j yields a quadratic equation with two roots ω^i and ω^j, as well as (**??**). Thus $s_2 = 1$ and $2c_1 + 2c_1 s_2 + s_0 = c_1 r_1^2$. Note that $\omega^i \cdot \omega^j = s_2 = 1$ and $\omega^i + \omega^j = -r_1$, so

$$s_0 = c_1 r_1^2 - 4c_1 = c_1((\omega^i + \omega^j)^2 - 4) = c_1(\omega^i - \omega^{-i})^2.$$

By (**??**) we know

$$u_i u_{-i} = s_2 u_0^2 + s_1 u_0 + s_0 = u_0^2 + c_1(\omega^i - \omega^{-i})^2,$$

and meanwhile

$$(-1)^n u_0 u_1 \cdots u_{n-1} = -t^n = -f(u_0).$$

Consequently, if n is odd, then

$$\begin{aligned} f(u_0) =& u_0 \prod_{i=1}^{n-1} u_i = u_0 \prod_{i=1}^{\frac{n-1}{2}} u_i u_{-i} \\ =& u_0 \prod_{i=1}^{\frac{n-1}{2}} (u_0^2 + c_1(\omega^i - \omega^{-i})^2) \\ =& D_n(u_0, c_1). \end{aligned}$$

If n is even, then

$$\begin{aligned} f(u_0) =& - u_0 \prod_{i=1}^{n-1} u_i = -u_0 u_{n/2} \prod_{i=1}^{\frac{n}{2}-1} u_i u_{-i} \\ =& u_0^2 \prod_{i=1}^{\frac{n}{2}-1} (u_0^2 + c_1(\omega^i - \omega^{-i})^2) \\ =& D_n(u_0, c_1) - D_n(0, c_1). \end{aligned}$$

It remains to discuss the case $c_1 r_1 \neq 0$. Note that c_1 does not depend on the choice of i, j, but r_1 does. If $c_1 = 0$, then $s_1 = s_0 = 0$ by (**??**) and (**??**), and thus $u_i u_j = s_2 u_0^2$. This holds for any i such that $u_i \notin \mathbb{F}_q(u_0)$, so $f(u_0)$ is a product of monomials in u_0, namely, $f(u_0) = D_n(u_0, 0)$. Now suppose $c_1 \neq 0$ and $r_1 = 0$. Then $s_2 = -\omega^{2i}$ and $s_0 = -2c_1(1 - \omega^{2i})$. The function field $\mathbb{F}_q(u_0, u_i)/\mathbb{F}_q(u_0)$ is defined by

$$u_i^2 - \omega^{2i} u_0^2 - 2c_1(1 - \omega^{2i}) = 0.$$

If $s_2 = 1$, then $\omega^{-i} = \omega^j = -\omega^i$, and $s_0 = -4c_1 = c_1(\omega^i - \omega^{-i})^2$, and the same result follows. If $s_2 \neq 1$, then u_i is not the conjugate of u_{-i}. Recall that $\omega^i + \omega^j = r_1 \neq 0$ implies $\omega^i \cdot \omega^j = s_2 = 1$ for any choice of i, j. Therefore, the conjugate of $u_{-i} = \delta(\omega^{-i} t)$ is $\delta(-\omega^i t)$. Then by the same argument, $\mathbb{F}_q(u_0, u_{-i})/\mathbb{F}_q(u_0)$ is defined by

$$u_{-i}^2 - \omega^{-2i} u_0^2 - 2c_1(1 - \omega^{-2i}) = 0.$$

If q is odd, then $\mathbb{F}_q(u_0, u_i) \neq \mathbb{F}_q(u_0, u_{-i})$ (to see this, compare their discriminants), which gives rise to a contradiction. If q is even, then $\mathbb{F}_q(u_0, u_i)/\mathbb{F}_q(u_0)$ is inseparable, also a contradiction. □

Theorem 15. *Suppose $f(T) = D_n(T, a) - D_n(0, a)$ for $a \in \mathbb{F}_q^*$, $n > 2$ with $\gcd(n, q) = 1$. If $q \equiv \pm 1 \pmod{n}$, then $[M : \mathbb{F}_q(x)] = 2$. Moreover, the full constant field of $M/\mathbb{F}_q$ is $\mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod{n}$.*

Proof. Let $t_1 = t^n + \frac{a^n}{t^n} - D_n(0, a)$, and $\omega \in \overline{\mathbb{F}_q}$ a primitive n-th root of unity. Then the n distinct roots of $f(T) - t_1 \in \mathbb{F}_q(t_1)[T]$ are given by $u_i = \omega^i t + a(\omega^i t)^{-1}$, $i = 0, \ldots, n-1$. Suppose $q \equiv \pm 1 \pmod{n}$. Then for $2 \leq i < n$, it is viable to write $\omega^i = \alpha_i \omega + \beta_i$ for some $\alpha_i, \beta_i \in \mathbb{F}_q$. If $q \equiv 1 \pmod{n}$, set $\alpha_i = \frac{\omega^{-i} - \omega^i}{\omega^{-1} - \omega}$, and then $\omega^{-i} = \omega^i + \alpha_i(\omega^{-1} - \omega) = \alpha_i \omega^{-1} + \beta_i$. If $q \equiv -1 \pmod{n}$, then $\omega^q = \omega^{-1}$ and $\omega^{-i} = (\alpha_i \omega + \beta_i)^q = \alpha_i \omega^{-1} + \beta_i$. It follows that $\omega^i t + a(\omega^i t)^{-1} = \alpha_i(\omega t + a(\omega t)^{-1}) + \beta_i(t + at^{-1})$, which means the splitting field of $f(T) - t_1$ over $\mathbb{F}_q(t_1)$ is $\mathbb{F}_q(u_0, u_1)$.

Next we prove that $[\mathbb{F}_q(u_0, u_1) : \mathbb{F}_q(u_0)] = 2$. One can verify that

$$u_1^2 - (\omega + \omega^{-1}) u_0 u_1 + u_0^2 + a(\omega - \omega^{-1})^2 = 0,$$

so u_1 is integral over $\mathbb{F}_q[u_0]$, and a fortiori, over $\mathbb{F}_{q^2}[u_0]$. If $u_1 \in \mathbb{F}_{q^2}(u_0)$, then $u_1 \in \mathbb{F}_{q^2}[u_0]$, since $\mathbb{F}_{q^2}[u_0]$ as a UFD is integrally closed. Noting that t is transcendental over $\mathbb{F}_{q^2}$, we have $u_1 = c_1 u_0 + c_0$ for some $c_1, c_0 \in \mathbb{F}_{q^2}$. Comparing the coefficients yields $\omega = c_1$ and $\omega^{-1} a = c_1 a$, so $\omega^2 = 1$ and $n = 2$. Thus $u_1 \notin \mathbb{F}_{q^2}(u_0)$, and consequently $[\mathbb{F}_q(u_0, u_1) : \mathbb{F}_q(u_0)] = 2$. If the full constant field of $\mathbb{F}_q(u_0, u_1)/\mathbb{F}_q$ is not $\mathbb{F}_q$, then it must be $\mathbb{F}_{q^2}$. In this case $\mathbb{F}_{q^2}(u_0) \subseteq \mathbb{F}_q(u_0, u_1)$ and $[\mathbb{F}_{q^2}(u_0) : \mathbb{F}_q(u_0)] = 2$. Hence $\mathbb{F}_q(u_0, u_1) = \mathbb{F}_{q^2}(u_0)$, but $u_1 \notin \mathbb{F}_{q^2}(u_0)$, a contradiction. Then the full constant field is $\mathbb{F}_q$.

Suppose now that the full constant field of $M/\mathbb{F}_q$ is $\mathbb{F}_q$. Then $\omega + \omega^{-1} = (u_1 + u_{n-1})/u_0 \in \mathbb{F}_q$, as it is an algebraic element over $\mathbb{F}_q$ in M. The polynomial $T^2 - (\omega + \omega^{-1})T + 1$ in $\mathbb{F}_q[T]$ has roots ω and ω^{-1}, so we have either $\omega^q = \omega$ or $\omega^q = \omega^{-1}$. This implies $q \equiv 1 \pmod{n}$ or $q \equiv -1 \pmod{n}$. □

Remark 16. Note that in [**?**], Cohen and Matthews have discussed the monodromy groups of Dickson polynomials. Notably, they showed that Dickson polynomials have a dihedral group as monodromy group in some cases. However, the converse was not considered and our results cannot be derived from [**?**]. Furthermore, note that a small mistake has been incorporated in [**?**] since $q^2 \equiv 1 \pmod{n}$ is not equivalent to $q \equiv \pm 1 \pmod{n}$ when n is not a prime.

Remark 17. Let $f(T) = D_n(T, a)$ for some $a \in \mathbb{F}_q^*$. By Theorem **??**, whenever there is a root $\alpha \in \mathbb{F}_q$ of $f(T) - c$ for $c \in \mathbb{F}_q$, every irreducible factor of $f(T) - c$ has degree 1 or 2. Furthermore, if n is odd, then $f(T) - c$ is either product of linear factors, or product of $T - \alpha$ and quadratic irreducible polynomials over $\mathbb{F}_q$. To see this, note that for the n roots $x, y_1, \ldots, y_{n-1}$ of $f(T) - t$, none of them except x belongs to $\mathbb{F}_q(x)$. If $\beta \in \mathbb{F}_q$ is another root of $f(T) - c$, then all other roots of $f(T) - c$ belong to $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_q$. If n is even, it is not hard to draw

a similar conclusion that $f(T) - c$ is product of $(T-\alpha)(T+\alpha)$ and quadratic irreducible polynomials over $\mathbb{F}_q$.

Now that it has been shown that $[M : \mathbb{F}_q(x)] = 2$ for Dickson polynomials, it is natural to ask what the exact value of $\mathcal{G}(f)$ is. Before that, we need a basic fact about squares in a finite field.

Lemma 18. *For fixed $c \in \mathbb{F}_q^*$, the number of $b \in \mathbb{F}_q$ such that $b^2 + c$ is a square in $\mathbb{F}_q^*$ is $\frac{q-3}{2}$ if $-c$ is a square in $\mathbb{F}_q^*$, and $\frac{q-1}{2}$ otherwise.*

Theorem 19. *If $f(T) = D_n(T, a) - D_n(0, a)$ for $a \in \mathbb{F}_q^*$, $n > 2$ with $\gcd(n, q) = 1$ and $q \equiv \pm 1 \pmod{n}$, then*

$$\mathcal{G}(f) = \begin{cases} \left\lfloor \frac{q-3}{2n} \right\rfloor & \text{if } q \text{ is odd and } q \equiv \eta(a) \equiv 1 \pmod{n}, \\ \left\lfloor \frac{q+1}{2n} \right\rfloor & \text{if } q \text{ is odd and } q \equiv \eta(a) \equiv -1 \pmod{n}, \\ \left\lfloor \frac{q}{2n} \right\rfloor & \text{otherwise,} \end{cases}$$

where η is the quadratic character of $\mathbb{F}_q^*$.

Proof. Let $\mathbb{F}_q(x, y)$ be the function field defined by $y^2 - (\omega + \omega^{-1})xy + x^2 + a(\omega - \omega^{-1})^2 = 0$. It is indeed the splitting field of $f(T) - t \in \mathbb{F}_q(t)[T]$. If a rational place of $\mathbb{F}_q(t)$ splits completely in $\mathbb{F}_q(x)$, then it also splits completely in $\mathbb{F}_q(x, y)$ by Lemma **??**, so there are n rational places (other than the infinite one) of $\mathbb{F}_q(x)$ splitting completely in $\mathbb{F}_q(x, y)$. Conversely, suppose that $(x - b)$, a place of $\mathbb{F}_q(x)$ for some $b \in \mathbb{F}_q$, splits completely in $\mathbb{F}_q(x, y)$. If $(x - b)$ is unramified in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$, then the place P of $\mathbb{F}_q(t)$ lying below $(x - b)$ splits completely in $\mathbb{F}_q(x)$, for $\mathbb{F}_q(x, y)/\mathbb{F}_q(t)$ is Galois, in which P splits completely. If $(x-b)$ is ramified, then obviously P can not split completely. Therefore it suffices to count the number of $b \in \mathbb{F}_q$ such that $(x-b)$ is unramified in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ and splitting completely in $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$.

Denote by ν the number of $b \in \mathbb{F}_q$ such that $(x - b)$ splits completely in $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$; that is, $T^2 - (\omega + \omega^{-1})bT + b^2 + a(\omega - \omega^{-1})^2$ has two distinct factors in $\mathbb{F}_q[T]$. When q is even, that is equivalent to $b \neq 0$ and

$$\begin{aligned} 0 &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{b^2 + a(\omega - \omega^{-1})^2}{(\omega + \omega^{-1})^2 b^2}\right) \\ &= \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left((\omega + \omega^{-1})^{-2}\right) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}\left(\frac{a}{b^2}\right). \end{aligned}$$

Here we are using the fact that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\alpha) = 0$ for $\alpha \in \mathbb{F}_q$, if and only if $\beta^2 - \beta = \alpha$ for some $\beta \in \mathbb{F}_q$. Then clearly either $\nu = \frac{q-2}{2}$, or $\nu = \frac{q}{2}$. When q is odd, $(x - b)$ splits completely in $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$ if and only if the quadratic discriminant

$$\begin{aligned} &(\omega + \omega^{-1})^2 b^2 - 4(b^2 + 4a(\omega - \omega^{-1})^2) \\ =&((\omega + \omega^{-1})^2 - 4)b^2 - 4a(\omega - \omega^{-1})^2 \\ =&(\omega - \omega^{-1})^2(b^2 - 4a) \end{aligned}$$

is a square in $\mathbb{F}_q^*$. Note that if $\omega \notin \mathbb{F}_q$, then $(\omega - \omega^{-1})^2$ is a non-square in $\mathbb{F}_q$. In this case the number ν is obtained from Lemma **??**, as

$$\nu = \begin{cases} \frac{q-3}{2} & \text{if } q \equiv \eta(a) \equiv 1 \pmod{n}, \\ \frac{q-1}{2} & \text{if } q \equiv -\eta(a) \pmod{n}, \\ \frac{q+1}{2} & \text{if } q \equiv \eta(a) \equiv -1 \pmod{n}. \end{cases}$$

Meanwhile, $(x-b)$ is ramified in $\mathbb{F}_q(x)/\mathbb{F}_q(t)$ if and only if $(x-b)$ is a zero of $f'(x)$, i.e. $f'(b) = 0$. There are at most $n-1$ such places. Finally we have

$$\frac{\nu - n + 1}{n} \leq \mathcal{G}(f) \leq \frac{\nu}{n}.$$

There is only one integer in the interval $\left[\frac{\nu-n+1}{n}, \frac{\nu}{n}\right]$. Note that if $q \equiv \pm 1 \pmod{n}$, then $\left\lfloor \frac{q-1}{2n} \right\rfloor = \left\lfloor \frac{q}{2n} \right\rfloor$, and if in addition q is even, then $\left\lfloor \frac{q-2}{2n} \right\rfloor = \left\lfloor \frac{q}{2n} \right\rfloor$. The desired result then follows. □

Remark 20. In [**?**], the case $q \equiv 1 \pmod{n}$ has been discussed, where the formula is obtained by studying the value sets of Dickson polynomials over finite fields. Here we can generalize it to all cases, with proof using the language of function fields. In particular, if $q \not\equiv 1 \pmod{n}$ and $q \not\equiv -1 \pmod{n}$, then $\mathcal{G}(f) = 0$, since the full constant field of $M/\mathbb{F}_q$ is not $\mathbb{F}_q$.

4.2 Powers of Linearized Polynomials

In Proposition **??**, it is shown that powers of linearized polynomials are likely to have minimal Galois groups. The following proposition is actually a generalization.

Proposition 21. *Let $f(T) = (h(T))^k$, where $h(T) = \sum_{b \in B}(T-b)$, $n = kp^l$ for some integers k, l, with B an additive subgroup of order p^l in $\mathbb{F}_q$. If $q \equiv 1 \pmod{k}$, with ω a primitive k-th root of unity in $\mathbb{F}_q$, let j be the least positive integer such that $\omega^j = c_0 + c_1\omega + \cdots + c_{j-1}\omega^{j-1}$ for some $c_i \in \mathbb{F}_q$ with $c_i B = B$, $0 \leq i < j$. Then*

1. *$[M : \mathbb{F}_q(x)] \leq p^{l(j-1)}$;*
2. *there exists some $t_0 \in \mathbb{F}_q$ such that $f(T) - t_0$ splits completely (without multiple roots) in $\mathbb{F}_q[T]$ if and only if there exists $u_0 \in \mathbb{F}_q$ with $u_0\mathbb{F}_{p^d} \subseteq \{h(\alpha) \mid \alpha \in \mathbb{F}_q\}$ and $p^{l+d} \leq q$, where d is the least positive integer such that $p^d \equiv 1 \pmod{k}$;*
3. *$\frac{d}{\gcd(d,l)} \leq j \leq d$, and the lower bound is achieved if $B = \mathbb{F}_{p^l}$.*

Proof. (1) Let $u = h(x)$. For $1 \leq i < j$, choose an element y_i such that $h(y_i) = \omega^i u$. Clearly $f(y_i + b_0) = u^k = f(x)$ for any $b_0 \in B$ and $[\mathbb{F}_q(x, y_i) : \mathbb{F}_q(x)] \leq p^l$. Accordingly $[\mathbb{F}_q(x, y_1, \ldots, y_{j-1}) : \mathbb{F}_q(x)] \leq p^{l(j-1)}$. If $cB = B$ for some $c \in \mathbb{F}_q$,

then B is a vector space over $\mathbb{F}_p(c)$, and thus $c \in \mathbb{F}_{p^l}$. Let $y_j = c_0x + c_1y_1 + \cdots + c_{j-1}y_{j-1}$, so that

$$\begin{aligned} h(y_j) =& h(c_0x) + h(c_1y_1) + \cdots + h(c_{j-1}y_{j-1}) \\ =& c_0^{p^l} h(x) + c_1^{p^l} h(y_1) + \cdots + c_{j-1}^{p^l} h(y_{j-1}) \\ =& \left(c_0 + c_1\omega + \cdots + c_{j-1}\omega^{j-1}\right) u \\ =& \omega^j u. \end{aligned}$$

Similarly we have $y_{j+1} = c_0y_1 + c_1y_2 + \cdots + c_{j-1}y_j$ with $h(y_{j+1}) = \omega^{j+1}u$, and so on. By adding each element of B to $x, y_1, \ldots, y_{n-1}$, we obtain n distinct roots of $f(T) - t$. Thus $M = \mathbb{F}_q(x, y_1, \ldots, y_{j-1})$ and $[M : \mathbb{F}_q(x)] \leq p^{l(j-1)}$. This completes the proof.

(2) Note that $f(T) - t_0$ splits completely in $\mathbb{F}_q[T]$ if and only if $t_0 = u_0^k$ for some $u_0 \in \mathbb{F}_q$ and $h(T) - \omega^i u_0$ splits completely for any integer i. The latter is equivalent to $\omega^i u_0 \in E$, where $E = \{h(\alpha) \mid \alpha \in \mathbb{F}_q\}$ is a vector space over $\mathbb{F}_p$. Meanwhile $\mathbb{F}_{p^d}$ is the smallest subfield of $\mathbb{F}_q$ containing ω, as well as the smallest vector space over $\mathbb{F}_p$ in $\mathbb{F}_q$ containing $1, \omega, \ldots, \omega^{k-1}$, for the minimal polynomial of ω over $\mathbb{F}_p$ has degree d. It follows that $u_0\mathbb{F}_{p^d} \subseteq E$. Comparing the dimensions we have $p^{l+d} \leq q$.

(3) Let $\mathbb{F}_{p^e}$ for some integer e be the largest subfield of $\mathbb{F}_q$ over which B is a vector space. Then it is clear that e divides l, and $cB = B$ if and only if $c \in \mathbb{F}_{p^e}$; hence j is the degree of ω over $\mathbb{F}_{p^e}$, which is exactly the least positive integer such that $p^{ej} \equiv 1 \pmod{k}$. This implies $j = \frac{d}{\gcd(d,e)}$, and the inequality follows. □

With the notation above, we give an example.

Example 22. Let $q = 64$, $n = 6$, $k = 3$ and $B = \{0, c\}$ for some $c \in \mathbb{F}_q^*$. Since $\omega^2 + \omega + 1 = 0$, applying the proposition we have $[M : \mathbb{F}_q(x)] \leq 2$, but $\omega B \neq B$, so $M \neq \mathbb{F}_q(x)$. It turns out that $[M : \mathbb{F}_q(x)] = 2$. On the other hand, ω lies in $\mathbb{F}_4$ and $c^2\mathbb{F}_4 \subseteq c^2\mathbb{F}_{32} = \{c^2\alpha(\alpha - 1) \mid \alpha \in \mathbb{F}_q\} = \{\alpha(\alpha - c) \mid \alpha \in \mathbb{F}_q\}$, so there exists a rational place of $\mathbb{F}_q(t)$ splitting completely in $\mathbb{F}_q(x)$, and hence in M. Then the full constant field of $M/\mathbb{F}_q$ is $\mathbb{F}_q$. This example shows that without the assumption $\gcd(n, q) = 1$, Theorem **??** is not valid.

5 Conclusions

This paper has discussed a property of polynomials over finite fields with applications to locally recoverable codes and turned to characterize the corresponding Galois groups over function fields. For a polynomial of degree n with $[M : \mathbb{F}_q(x)]$ being a specific integer, some of its properties have been presented in terms of the polynomial factorization and the arithmetic of q and n. Besides, there are also some specific forms of polynomials with good properties, especially the Dickson polynomials. In most cases, we also proved that such polynomials are unique. The results may be applied to other research on polynomials over finite fields and

their corresponding function fields. However, there are still many polynomials for which it is difficult to give a more precise condition with respect to their Galois groups or splitting fields. This may be an interesting and challenging problem.

Acknowledgement

The authors sincerely thank the anonymous referees and the Associate Editor for their constructive and valuable comments, which have improved the quality of the paper highly. The work of the first author is supported by the China Scholarship Council. The funding corresponds to the scholarship for the Ph.D. thesis of the first author in Paris, France.

References

1. Chen, R., Mesnager, S., Zhao, C.A.: Good polynomials for optimal lrc of low locality. Des. Codes Cryptogr **7**(89), 1639–1660 (2021)
2. Cohen, S.D.: The distribution of polynomials over finite fields. Acta Arithmetica **3**(17), 255–271 (1970)
3. Cohen, S.D., Matthews, R.W.: Monodromy groups of classical families over finite fields. Finite Fields and Applications, London Math Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge (233), 59–68 (1996)
4. Lidl, R., Mullen, G.L., Turnwald, G.: Dickson polynomials. Longman, London-Harlow-Essex (1993)
5. Liu, J., Mesnager, S., Chen, L.: New constructions of optimal locally recoverable codes via good polynomials. IEEE Transactions on Information Theory **64**(2), 889–899 (2018)
6. Liu, J., Mesnager, S., Tang, D.: Constructions of optimal locally recoverable codes via dickson polynomials. Designs, codes and cryptography. To appear (2020)
7. Micheli, G.: Constructions of locally recoverable codes which are optimal. IEEE Transactions on Information Theory **66**(1), 167–175 (2020)
8. Stichtenoth, H.: Algebraic function fields and codes, vol. 254. Springer Science & Business Media (2009)
9. Tamo, I., Barg, A.: A family of optimal locally recoverable codes. IEEE Transactions on Information Theory **60**(8), 4661–4676 (2014)