Constructions of optimal locally recoverable codes via Dickson polynomials

Jian Liu[1], Sihem Mesnager[2], and Deng Tang[3]

[1] School of Cybersecurity, College of Intelligence and Computing, Tianjin University,
Tianjin, 300350, China
`jianliu.nk@gmail.com`
[2] Department of Mathematics, University of Paris VIII, University of Paris XIII,
CNRS, UMR 7539 LAGA and Telecom ParisTech, Paris, France
`smesnager@univ-paris8.fr`
[3] School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China
`dtang@foxmail.com`

Abstract. In 2014, Tamo and Barg have presented in a very remarkable paper a family of optimal linear locally recoverable codes (LRC codes) that attain the maximum possible distance (given code length, cardinality, and locality). The key ingredient for constructing such optimal linear LRC codes is the so-called r-good polynomials, where r is equal to the locality of the LRC code. In 2018, Liu et al. have presented two general methods of designing r-good polynomials by using function composition, which lead to three new constructions of r-good polynomials. Next, Micheli has provided a Galois theoretical framework which allows to produce r-good polynomials.

The well-known Dickson polynomials form an important class of polynomials which have been extensively investigated in recent years under different contexts. In this paper, we provide new methods of designing r-good polynomials based on Dickson polynomials. Such r-good polynomials provide new constructions of optimal LRC codes.

1 Introduction

Locally recoverable codes (LRC codes) have recently been a very attractive subject in the research on coding theory due to their theoretical appeal and applications in large-scale distributed storage systems, where a single storage node erasure is considered as a frequent error-event.

An LRC code is said to have *locality* r if the value at any codeword coordinate can be recovered by accessing at most r other coordinates. We refer to such a code as an (n, k, r) LRC code over finite field $\mathbb{F}_q$, if the code is of length n, which has q^k codewords and locality r. For an LRC code with locality r, if a symbol is lost due to a node failure, its value can be recovered by accessing the value of at most r other symbols.

Problems of constructing LRC codes and bounding their parameters have been the subject of a considerable number of publications. Research on bounds for LRC codes was initiated in [3] which showed that the minimal distance $d(\mathcal{C})$ of an (n,k,r) LRC code is bounded as follows: $d(\mathcal{C}) \leqslant n-k-\lceil k/r \rceil+2$. LRC codes achieving this bound with equality are called *optimal* LRC codes. Taking into account the size of the code alphabet, another upper bound on the minimum distance of (n,k,r) LRC codes was established by Cadambe and Mazumdar [1].

An ingenious idea in designing optimal LRC codes is due to Tamo and Barg [9]. By generalizing the Reed-Solomon codes, Tamo and Barg [9] constructed a family of optimal (n,k,r) LRC codes over a finite field of size that slightly exceeds the code length n. Their method can provide optimal LRC codes for a lot of feasible triplet of parameters (n,k,r). These optimal LRC codes are obtained from specially constructed polynomials over finite fields, called *r-good polynomials* (see Definition 1), that is to say, an r-good polynomial yields an optimal (n,k,r) LRC code with n divisible by $r+1$. However, there are only a few known constructions of r-good polynomials. In 2018, Liu et al. [6] have provided two general methods of designing r-good polynomials by using function composition, which lead to three new constructions of r-good polynomials. Very recently, Micheli [7] has provided a Galois theoretical framework which allows to produce r-good polynomials and showed that the construction of r-good polynomials can be reduced to a Galois theoretical problem over global function fields. The objection of this paper is to explore more polynomials which could be good candidates for being r-good polynomials. More specifically, we exploit Dickson polynomials to provide more families of r-good polynomials leading to the constructions of optimal LRC codes. This paper is structured as follows. Section 2 sets main notations, gives some background on polynomials and exponentials sums over finite fields, and reviews the known explicit constructions of r-good polynomials. In Section 3, we present new r-good polynomials via Dickson polynomials.

Due to the limit in space, proofs of the main results are left to the full version of the paper.

2 Preliminaries

2.1 Background and notation

Let p be a prime and $q=p^s$ be an s-th power of p with s being a positive integer. We denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_q^\star$ the cyclic group $\mathbb{F}_q \setminus \{0\}$. For positive integers t and s satisfying $t|s$, let $\mathrm{Tr}_t^s(\cdot): \mathbb{F}_{p^s} \rightarrow \mathbb{F}_{p^t}$ be the (relative) *trace function* defined as

$$\mathrm{Tr}_t^s(x)=x+x^{p^t}+x^{p^{2t}}+\cdots+x^{p^{s-t}}.$$

For $x \in \mathbb{F}_{p^s}$, we briefly use $\mathrm{Tr}(x)$ to denote the (absolute) trace of $x \in \mathbb{F}_{p^s}$ over $\mathbb{F}_p$, i.e., $\mathrm{Tr}_1^s(x)$, if there is no risk of confusion.

Proposition 1. ([8, Theorem 2.25]) *Let $\mathbb{F}_{p^s}$ be a finite extension of $\mathbb{F}_{p^t}$. Then, for $a \in \mathbb{F}_{p^s}$, the equation $x^{p^t}-x=a$ has solutions in $\mathbb{F}_{p^s}$ if and only if $\mathrm{Tr}_t^s(a)=0$.*

Proposition 2. ([8, Theorem 5.4]) *For a finite field* $\mathbb{F}_q$ *with characteristic* p*, define* $\zeta_p = e^{2\pi i/p}$*, then*

$$\sum_{c\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(cx)} = \begin{cases} 0, \text{ if } x \neq 0, \\ q, \text{ if } x = 0. \end{cases}$$

A q-ary function is from $\mathbb{F}_q$ to itself. The *extended Walsh-Hadamard transform* of a q-ary function F is defined as the complex function

$$\mathcal{W}_F(v; w, k) = \sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}(vF(x)+wx^k)}, \quad v \in \mathbb{F}_q^*,\ w \in \mathbb{F}_q, \quad k \text{ is an integer.}$$

For two q-ary functions F and G, the composition $G(F(\cdot))$ is denoted by $G \circ F$.

For $a, b \in \mathbb{F}_{p^s}$, the classical p-ary Kloosterman sum (see e.g. [8]) on $\mathbb{F}_{p^s}$ is defined as

$$K_s(a, b) = \sum_{x\in\mathbb{F}_{p^s}^*} \zeta_p^{\mathrm{Tr}\left(ax+bx^{-1}\right)} = \mathcal{W}_{x^{-1}}(b; a, 1). \tag{1}$$

Dickson polynomials (see e.g. [5]) form an important class of polynomials. For $b \in \mathbb{F}_q$ and integer $m \geqslant 1$, let

$$D_{m,b}(x) = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-b)^j x^{m-2j} \tag{2}$$

denote the Dickson polynomial of degree m over $\mathbb{F}_q$.

Definition 1. *A polynomial* F *over* $\mathbb{F}_{p^s}$ *is said to be an* r-good polynomial *if*

1. *the degree of* F *is* $r + 1$*,*
2. *there exist pairwise disjoint subsets* $\{A_1, \dots, A_l\}$ *of* $\mathbb{F}_{p^s}$ *with cardinality* $|A_i| = r + 1$ *for* $i = 1, \dots, l$*,* $l \geqslant 1$*, such that the restriction of* F *to each subset* A_i *is constant.*

2.2 Known explicit constructions of r-good polynomials

Let p be a prime and $\gcd(m, p) = 1$, then for any integer $t \geqslant 0$, $(mp^t - 1)$-good polynomials on $\mathbb{F}_{p^s}$ can be constructed if $p^s \equiv 1 (\mathrm{mod}\ m)$ and $p^t \equiv 1 (\mathrm{mod}\ m)$, see [9]. To the best of our knowledge, if $p^t \not\equiv 1 (\mathrm{mod}\ m)$, then for $m > 1$, constructions of $(mp^t - 1)$-good polynomials on the extension field of $\mathbb{F}_p$ have only been examined in [6]. Thus, constructing optimal LRC codes with locality mp^t, where $m > 1$, $\gcd(m, p) = 1$, and $p^t \not\equiv 1 (\mathrm{mod}\ m)$ attracts a lot of attention.

When we consider r-good polynomials on $\mathbb{F}_{p^s}$ with $r = mp^t - 1$, where $\gcd(m, p) = 1$, the following constructions are known.

- If $t > 0$ and $m = 1$, then the p^s-ary linear function

$$F_a(x) = \sum_{i=0}^{t} a_i x^{p^i} \tag{3}$$

is an r-good polynomial, where $a = (a_0, \ldots, a_t) \in (\mathbb{F}_{p^s})^{t+1}$, $a_0 \neq 0$, $a_t \neq 0$ (see [9, Proposition 3.2]). In fact, let $E_a = \{x \in \mathbb{F}_{p^s} \mid F_a(x) = 0\}$, then for every $x \in b + E_a$, $F_a(x) = F_a(b)$.

- If $t = 0$ and $p^s \equiv 1 (\mathrm{mod}\ m)$, then the p^s-ary power function
$$G_\gamma(x) = \gamma x^m \tag{4}$$
is an r-good polynomial, where $\gamma \in \mathbb{F}_{p^s}^*$ (see [9, Proposition 3.2]). In fact, let $U_m = \{x \in \mathbb{F}_{p^s} \mid x^m = 1\}$ and bU_m be the multiplicative coset with $b \in \mathbb{F}_{p^s}^*$, then for every $x \in bU_m$, $G_\gamma(x) = G_\gamma(b)$.
- If $t > 0$, $m > 1$, $p^s \equiv 1 (\mathrm{mod}\ m)$, and $p^t \equiv 1 (\mathrm{mod}\ m)$, then the p^s-ary function
$$F(x) = \left(\sum_{i=0}^{t/e} a_i x^{p^{ei}}\right)^m$$
is an r-good polynomial, where e is a divisor of t satisfying $p^e \equiv 1 (\mathrm{mod}\ m)$, $a_i \in \mathbb{F}_{p^s}$ satisfying $\sum_{i=0}^{t/e} a_i = 0$, $a_0 \neq 0$, and $a_{t/e} \neq 0$ (see [9, Theorem 3.3]).
- Denote by $\mathrm{Im}(F) = \{F(x) \mid x \in \mathbb{F}_{p^s}\}$ the image set of F. Let G_γ and F_a be defined as in (4) and (3) respectively. Suppose that $\mathbb{F}_{p^s}$ contains all the roots of F_a. Set $H(x) = F_a(G_\gamma(x)) = \sum_{i=0}^{t} a_i \gamma^{p^i} x^{mp^i}$. Then, H is an $(mp^t - 1)$-good polynomial over $\mathbb{F}_{p^s}$ if and only if $\mathcal{A} = \{b \in \mathbb{F}_{p^s} \setminus E_a \mid b + E_a \subseteq \mathrm{Im}(G_\gamma)\}$ is nonempty, where $E_a = \{x \in \mathbb{F}_{p^s} \mid F_a(x) = 0\}$ (see [6, Theorem 4]).
- Set $I(x) = G_1(F_a(x)) = \left(\sum_{i=0}^{t} a_i x^{p^i}\right)^m$. Then, I is an $(mp^t - 1)$-good polynomial over $\mathbb{F}_{p^s}$ if and only if $\mathcal{A}' = \{b \in \mathbb{F}_{p^s}^* \mid bU_m \subseteq \mathrm{Im}(F_a)\}$ is nonempty, where $U_m = \{x \in \mathbb{F}_{p^s} \mid x^m = 1\}$ (see [6, Theorem 4]).

3 Constructions of r-good polynomials via Dickson polynomials

3.1 r-Good polynomials from Dickson polynomials

In this subsection, we consider r-good polynomials via Dickson polynomials over the finite field $\mathbb{F}_q$.

If $x \in \mathbb{F}_q$, then for any $b \in \mathbb{F}_q^*$, x can be written as $x = u + b \cdot u^{-1}$ with $u \in \mathbb{F}_{q^2}^*$. More explicitly, define $M = \{u \in \mathbb{F}_{q^2}^* \mid u^{q+1} = b\}$, then for $u \in \mathbb{F}_{q^2}^*$, $x = u + b \cdot u^{-1} \in \mathbb{F}_q$ if and only if $u \in \mathbb{F}_q^* \bigcup M$ (see e.g.[4]). It is shown in [8] that for $x = u + b \cdot u^{-1}$ with $u \in \mathbb{F}_{q^2}^*$, the Dickson polynomial $D_{m,b}$ on x equals
$$D_{m,b}(x) = u^m + b^m \cdot u^{-m}. \tag{5}$$

Case 1: q odd In this part, for the finite field $\mathbb{F}_q$, we assume that q is odd.

Theorem 1. ([2, Theorem 9]) *For q odd, let $x_0 \in \mathbb{F}_q$, then the set of preimages of $D_{m,b}(x_0)$ with $b \in \mathbb{F}_q^*$ and integer $m \geqslant 1$ has $\gcd(m, q-1)$ elements, i.e.,*
$$|D_{m,b}^{-1}(D_{m,b}(x_0))| = \gcd(m, q-1),$$

if x_0^2-4b *is a square in* $\mathbb{F}_q$ *and* $D_{m,b}(x_0)\neq\pm 2b^{m/2}$*, where* $b^{1/2}$ *is a square root of* b *in* $\mathbb{F}_{q^2}^*$*.*

Remark 1. For $x_0\in\mathbb{F}_q$, denote $x_0=u_0+b\cdot u_0^{-1}$ for $u_0\in\mathbb{F}_{q^2}^*$. Note that for q odd, x_0^2-4b is a square in $\mathbb{F}_q$ if and only if $u_0\in\mathbb{F}_q^*$, and x_0^2-4b is a non-square in $\mathbb{F}_q$ if and only if $u_0\in M\setminus\mathbb{F}_q^*$, where $M=\{u\in\mathbb{F}_{q^2}^*\mid u^{q+1}=b\}$ (see e.g.[2]).

Remark 2. Let $m|(q-1)$ and $m\geqslant 3$ in Theorem 1. Then, it can be deduced from Theorem 9 in [2] that for $x_0\in\mathbb{F}_q$, $|D_{m,b}^{-1}(D_{m,b}(x_0))|=m$ if and only if x_0^2-4b is a square in $\mathbb{F}_q$ and $D_{m,b}(x_0)\neq\pm 2b^{m/2}$.

It is shown that $D_{m,b}(x)\neq\pm 2b^{m/2}$ if and only if $u^m\neq(b\cdot u^{-1})^m$, where $x=u+b\cdot u^{-1}$ (see [2, Lemma 7]). Suppose $b\in\xi^lU_m$ and $u\in\xi^iU_m$, where ξ is a primitive element of $\mathbb{F}_q$, and ξ^iU_m is the multiplicative coset of $U_m=\{x\in\mathbb{F}_q\mid x^m=1\}$ for $i\in\{0,1,\ldots,(q-1)/m-1\}$. Then, it can be easily proved that $u^m=\left(b\cdot u^{-1}\right)^m$ if and only if $2i\equiv l(\bmod\ (q-1)/m)$. Since the degree of $D_{m,b}$ is m, then from Theorem 1, we can prove the following theorem.

Theorem 2. *For* q *odd, let* $b\in\mathbb{F}_q^*$ *and integer* $m\geqslant 1$*. If* $m|(q-1)$*, then the Dickson polynomial* $D_{m,b}(x)$ *is an* $(m-1)$*-good polynomial.*

Theorem 3. *For* q *odd, let* $b\in\mathbb{F}_q^*$ *and integer* $m\geqslant 3$ *satisfying* $m|(q-1)$*. Then, the Dickson polynomial* $D_{m,b}(x)$ *is an* $(m-1)$*-good polynomial. Suppose* $b\in\xi^lU_m$ *for some* $l\in S=\{0,1,\ldots,(q-1)/m-1\}$*, where* ξ *is a primitive element of* $\mathbb{F}_q$*,* ξ^iU_m *is the multiplicative coset of* $U_m=\{x\in\mathbb{F}_q\mid x^m=1\}$*. Then, the only pairwise disjoint subsets of* $\mathbb{F}_q$ *with cardinality* m *such that* $D_{m,b}$ *is constant on each subset include*

$$D_i=\left\{u+b\cdot u^{-1}\;\middle|\;u\in\xi^iU_m\right\},\quad \textit{for } i\in I\subseteq S, \tag{6}$$

where

$$I=\begin{cases}\left\{0,1,\ldots,\frac{l}{2}-1,l+1,l+2,\ldots,\frac{l}{2}+\frac{q-1}{2m}-1\right\}, & \textit{if } l \textit{ is even, } \frac{q-1}{m} \textit{ is even,}\\ \left\{0,1,\ldots,\frac{l}{2}-1,l+1,l+2,\ldots,\frac{l}{2}+\frac{q-1}{2m}-\frac{1}{2}\right\}, & \textit{if } l \textit{ is even, } \frac{q-1}{m} \textit{ is odd,}\\ \left\{0,1,\ldots,\frac{l-1}{2},l+1,l+2,\ldots,\frac{l}{2}+\frac{q-1}{2m}-\frac{1}{2}\right\}, & \textit{if } l \textit{ is odd, } \frac{q-1}{m} \textit{ is even,}\\ \left\{0,1,\ldots,\frac{l-1}{2},l+1,l+2,\ldots,\frac{l}{2}+\frac{q-1}{2m}-1\right\}, & \textit{if } l \textit{ is odd, } \frac{q-1}{m} \textit{ is odd.}\end{cases} \tag{7}$$

The following corollary is a direct consequence of Theorem 3.

Corollary 1. *For* q *odd, let* $b\in\mathbb{F}_q^*$ *and integer* $m\geqslant 3$ *satisfying* $m|(q-1)$*. Suppose* $b\in\xi^lU_m$ *for some* $l\in\{0,1,\ldots,(q-1)/m-1\}$*, where* ξ *is a primitive element of* $\mathbb{F}_q$*. Then, the Dickson polynomial* $D_{m,b}(x)$ *is constant on exactly* $l_{D_{m,b}}$ *pairwise disjoint subsets with cardinality* m*, where*

$$l_{D_{m,b}}=\begin{cases}\frac{q-1}{2m}-1, & \textit{if } l \textit{ is even, } \frac{q-1}{m} \textit{ is even,}\\ \frac{q-1-m}{2m}, & \textit{if } l \textit{ is even, } \frac{q-1}{m} \textit{ is odd,}\\ \frac{q-1}{2m}, & \textit{if } l \textit{ is odd, } \frac{q-1}{m} \textit{ is even,}\\ \frac{q-1-m}{2m}, & \textit{if } l \textit{ is odd, } \frac{q-1}{m} \textit{ is odd.}\end{cases}$$

Case 2: *q* even In this part, for the finite field $\mathbb{F}_q$, we assume that q is even.

Theorem 4. ([2, Theorem 9']) *For q even, let $x_0 \in \mathbb{F}_q$, then the set of preimage of $D_{m,b}(x_0)$ with $b \in \mathbb{F}_q^*$ and integer $m \geqslant 1$ has $\gcd(m, q-1)$ elements, i.e.,*

$$|D_{m,b}^{-1}\left(D_{m,b}(x_0)\right)| = \gcd(m, q-1),$$

if $x^2 + x_0 x + b$ is reducible over $\mathbb{F}_q$ and $D_{m,b}(x_0) \neq 0$.

Remark 3. For $x_0 \in \mathbb{F}_q$, denote $x_0 = u_0 + b \cdot u_0^{-1}$ for $u_0 \in \mathbb{F}_{q^2}^*$. Then, $x^2 + x_0 x + b$ is reducible over $\mathbb{F}_q$ if and only if $u_0 \in \mathbb{F}_q^*$, and $x^2 + x_0 x + b$ is irreducible over $\mathbb{F}_q$ if and only if $u_0 \in M \setminus \mathbb{F}_q^*$, where $M = \{u \in \mathbb{F}_{q^2}^* \mid u^{q+1} = b\}$ (see e.g.[2]). Note that for q even, any element in $\mathbb{F}_q^*$ is a square.

Remark 4. Let $m|(q-1)$ and $m \geqslant 2$ in Theorem 4. Then, it can be deduced from Theorem 9' in [2] that for $x_0 \in \mathbb{F}_q$, $|D_{m,b}^{-1}\left(D_{m,b}(x_0)\right)| = m$ if and only if $x^2 + x_0 x + b$ is reducible over $\mathbb{F}_q$ and $D_{m,b}(x_0) \neq 0$.

Theorem 5. *For q even, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 1$. If $m|(q-1)$, then the Dickson polynomial $D_{m,b}(x)$ is an $(m-1)$-good polynomial.*

The following corollary is a direct consequence of Theorem 2 and Theorem 5.

Corollary 2. *A Dickson polynomial $D_{m,b}(x)$ is an $(m-1)$-good polynomial if $m|(q-1)$ for any q (even or odd).*

Theorem 6 below is indeed a special case of Theorem 3, since for q even, $(q-1)/m$ must be odd, and the condition $m \geqslant 2$ follows from Remark 4.

Theorem 6. *For q even, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 2$ satisfying $m|(q-1)$. Then, the Dickson polynomial $D_{m,b}(x)$ is an $(m-1)$-good polynomial. Suppose $b \in \xi^l U_m$ for some $l \in S = \{0, 1, \ldots, (q-1)/m - 1\}$, where ξ is a primitive element of $\mathbb{F}_q$, $\xi^i U_m$ is the multiplicative coset of $U_m = \{x \in \mathbb{F}_q \mid x^m = 1\}$. Then, the only pairwise disjoint subsets of $\mathbb{F}_q$ with cardinality m such that $D_{m,b}$ is constant on each subset include*

$$D_i = \left\{u + b \cdot u^{-1} \;\middle|\; u \in \xi^i U_m\right\}, \quad \text{for } i \in I \subseteq S, \tag{8}$$

where

$$I = \begin{cases} \left\{0, 1, \ldots, \frac{l}{2} - 1, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - \frac{1}{2}\right\}, & \text{if } l \text{ is even}, \\ \left\{0, 1, \ldots, \frac{l-1}{2}, l+1, l+2, \ldots, \frac{l}{2} + \frac{q-1}{2m} - 1\right\}, & \text{if } l \text{ is odd}. \end{cases} \tag{9}$$

The following corollary is a direct consequence of Theorem 6.

Corollary 3. *For q even, let $b \in \mathbb{F}_q^*$ and integer $m \geqslant 3$ satisfying $m|(q-1)$. Then, the Dickson polynomial $D_{m,b}(x)$ is constant on exactly*

$$l_{D_{m,b}} = \frac{q-1-m}{2m}$$

pairwise disjoint subsets with cardinality m.

3.2 Constructing r-good polynomials by function compositions $D_{m,b} \circ F_a$ and $F_a \circ D_{m,b}$

Employing Theorem 3 and Theorem 6, one can obtain the following theorem.

Theorem 7. *Denote by* $\mathrm{Im}(F) = \{F(x) \mid x \in \mathbb{F}_{p^s} = \mathbb{F}_q\}$ *the image set of* F. *Let* $D_{m,b}$ *and* F_a *be defined as in (2) and (3) respectively. For* $i \in \{0, 1, \ldots, (q-1)/m - 1\}$, *let* $D_i = \left\{u + b \cdot u^{-1} \;\middle|\; u \in \xi^i U_m\right\}$, *where* ξ *is a primitive element of* $\mathbb{F}_q$. *Suppose that* $m|(p^s - 1)$, $m \geqslant 3$, *and* $\mathbb{F}_q$ *contains all the roots of* F_a. *Then,*

1. $H(x) = D_{m,b} \circ F_a(x)$ *is an* $(mp^t - 1)$*-good polynomial over* $\mathbb{F}_q$ *if and only if* $\mathcal{A} = \{i \in \{0, 1, \ldots, q-2\} \mid i \bmod \frac{q-1}{m} \in I,\ D_i \subseteq \mathrm{Im}(F_a)\}$ *is nonempty, where* I *is defined in (7) and (9) for* q *odd and* q *even respectively.*
2. $H'(x) = F_a \circ D_{m,b}(x)$ *is an* $(mp^t - 1)$*-good polynomial over* $\mathbb{F}_q$ *if and only if* $\mathcal{A}' = \left\{c \in \mathbb{F}_q \mid c + E_a \subseteq D_{m,b}\left(\bigcup_{i \in I} D_i\right)\right\}$ *is nonempty, where* $E_a = \{x \in \mathbb{F}_{p^s} \mid F_a(x) = 0\}$ *and* I *is defined in (7) and (9) for* q *odd and* q *even respectively, and* $D_{m,b}\left(\bigcup_{i \in I} D_i\right) = \{D_{m,b}(x) \mid x \in \bigcup_{i \in I} D_i\}$.

Proof. Observe that H and H' are of degree mp^t.

1. *Sufficiency.* Assume $\mathcal{A} \neq \emptyset$. Then, there exists $i \in \mathcal{A}$ such that $D_i = \{u + bu^{-1} \mid u \in \xi^i U_m\} \subseteq \mathrm{Im}(F_a)$ for $i \bmod \frac{q-1}{m} \in I$. Hence, for any $\xi^i U_m$, there must exist $x \in \mathbb{F}_q$ such that $u + bu^{-1} = F_a(x)$, which is equivalent to saying that, for any $j \in \{0, 1, \ldots, m-1\}$, there must exist $x_{i,j} \in \mathbb{F}_q$ such that

$$\xi^{i + j \cdot \frac{q-1}{m}} + b \cdot \xi^{-i - j \cdot \frac{q-1}{m}} = F_a(x_{i,j}). \tag{10}$$

Since F_a is linear, i.e., $F_a(x + y) = F_a(x) + F_a(y)$ for any $x, y \in \mathbb{F}_q$, then for any $y \in E_a = \{x \in \mathbb{F}_q \mid F_a(x) = 0\}$, we have $F_a(x + y) = F_a(x)$. Thus, F_a is constant on $x + E_a$ for any $x \in \mathbb{F}_q$.

Define $A_i = \bigcup_{j=0}^{m-1} (x_{i,j} + E_a)$. We now prove that the subsets $x_{i,j} + E_a$, $j = 0, 1, \ldots, m-1$, are pairwise disjoint. Let $j_1, j_2 \in \{0, 1, \ldots, m-1\}$ and $j_1 \neq j_2$. Suppose that $y \in (x_{i,j_1} + E_a) \bigcap (x_{i,j_2} + E_a)$, then there exist $e_1, e_2 \in E_a$ such that $y = x_{i,j_1} + e_1 = x_{i,j_2} + e_2$, and thus $F_a(x_{i,j_1}) = F_a(x_{i,j_2})$. According to (10), we have

$$\xi^{i + j_1 \cdot \frac{q-1}{m}} + b \cdot \xi^{-i - j_1 \cdot \frac{q-1}{m}} = \xi^{i + j_2 \cdot \frac{q-1}{m}} + b \cdot \xi^{-i - j_2 \cdot \frac{q-1}{m}} \in D_i.$$

Since $i \bmod \frac{q-1}{m} \in I$, we know that $|D_i| = |U_m| = m$, which implies $j_1 = j_2$, a contradiction. Hence, $|A_i| = \sum_{j=0}^{m-1} |x_{i,j} + E_a| = m|E_a| = mp^t$, where the last equation is due to the facts that the degree of F_a is p^t and $\mathbb{F}_q$ contains all the roots of F_a. For $x \in A_i$, we have $F_a(x) \in D_i$. Since $D_{m,b}$ is constant on D_i, then the composition $H = D_{m,b} \circ F_a$ is constant on A_i. Since the degree of H is mp^t, we know that H is an $(mp^t - 1)$-good polynomial over $\mathbb{F}_q$.

Necessity. Suppose that $H = D_{m,b} \circ F_a(x)$ is a $(mp^t - 1)$-good polynomial. Then, there exists $c \in \mathbb{F}_q$ such that $|H^{-1}(c)| = mp^t$, which implies that there exists $U \subseteq \mathbb{F}_q$ such that $\{F_a(x) \mid x \in H^{-1}(c)\} = \{u + b \cdot u^{-1} \mid u \in U\}$. Since the cardinality of the kernel of F_a is equal to p^t, then we have

$$|U| = \left|\left\{F_a(x) \;\middle|\; x \in H^{-1}(c)\right\}\right| = \left|H^{-1}(c)\right| / p^t = m.$$

Also, we have that for any $u \in U$,

$$u^m + b^m \cdot u^{-m} = D_{m,b}(u + b \cdot u^{-1}) = D_{m,b}(F_a(x)) = c,$$

where $x \in H^{-1}(c)$ such that $u + b \cdot u^{-1} = F_a(x)$. According to Theorem 3 and Theorem 6, we know that the only pairwise disjoint subsets of $\mathbb{F}_q$ with cardinality m such that $D_{m,b}$ is constant are $D_i = \left\{u + b \cdot u^{-1} \;\middle|\; u \in \xi^i U_m\right\}$, $i \in I$. Since $|U| = m$ and for any $u \in U$, $D_{m,b}(u + b \cdot u^{-1}) = c$, then we have $U = \xi^i U_m$ for some $i \in I$. Therefore, $D_i = \{u + b \cdot u^{-1} \mid u \in U\} = \{F_a(x) \mid x \in H^{-1}(c)\} \subseteq \mathrm{Im}(F_a)$, where $i \bmod \frac{q-1}{m} \in I$, and thus $\mathcal{A}$ is nonempty.

2. *Sufficiency.* Assume $\mathcal{A}' \neq \emptyset$. Then, there exists $c \in \mathbb{F}_q$ such that $c + E_a \subseteq D_{m,b}\left(\bigcup_{i \in I} D_i\right) = \left\{\xi^{im} + b^m \cdot \xi^{-im} \;\middle|\; i \in I\right\}$. For any $e \in E_a$, there must exist $i_e \in I$ such that $c + e = \xi^{i_e m} + b^m \cdot \xi^{-i_e m}$. Define $B_e = \{\xi^{i_e + j(q-1)/m} + b \cdot \xi^{-i_e - j(q-1)/m} \mid j = 0, 1, \ldots, m-1\}$. It is easy to see that $B_{e_1} \bigcap B_{e_2} = \emptyset$ for any $e_1, e_2 \in E_a$ and $e_1 \neq e_2$, since $e_1 \neq e_2$ implies $i_{e_1} \neq i_{e_2}$ and thus $D_{i_{e_1}} \bigcap D_{i_{e_2}} = \emptyset$ (due to Theorem 3 and Theorem 6). Hence, $|\bigcup_{e \in E_a} B_e| = \sum_{e \in E_a} |B_e| = mp^t$, where the last equation is from $|B_e| = m$ since $i_e \in I$ for any $e \in E_a$. Then, for any $x \in B_e$, $e \in E_a$,

$$\begin{aligned} F_a(D_{m,b}(x)) =& F_a\left(D_{m,b}(\xi^{i_e + j(q-1)/m} + b \cdot \xi^{-i_e - j(q-1)/m})\right) \\ =& F_a(\xi^{i_e m} + b^m \cdot \xi^{-i_e m}) = F_a(c + e) = F_a(c), \end{aligned}$$

which implies $H' = F_a \circ D_{m,b}$ is constant on $\bigcup_{e \in E_a} B_e \subseteq \mathbb{F}_q$ with cardinality mp^t. Since the degree of H' is mp^t, we know that H' is an $(mp^t - 1)$-good polynomial over $\mathbb{F}_q$.

Necessity. Suppose that $H' = F_a \circ D_{m,b}$ is an $(mp^t - 1)$-good polynomial. Then, there exists $d \in \mathbb{F}_q$ such that $|H'^{-1}(d)| = mp^t$, which implies

$$\begin{aligned} H'^{-1}(d) &= \{x \in \mathbb{F}_q \mid F_a(D_{m,b}(x)) = d\} \\ &= \bigcup_{i \in I} \{x \in D_i \mid F_a(D_{m,b}(x)) = d\} \\ &= \bigcup_{\substack{i \in I \\ F_a(\xi^{im} + b \cdot \xi^{-im}) = d}} D_i. \end{aligned}$$

Define $J = \{i \in I \mid F_a(\xi^{im} + b \cdot \xi^{-im}) = d\}$. Then, since $|D_i| = m$ for $i \in I$, we have $mp^t = |H'^{-1}(d)| = m|J|$, and thus $|J| = p^t$. Set $B_d = \{\xi^{im} + b \cdot \xi^{-im}) \mid i \in J\} \subseteq D_{m,b}\left(\bigcup_{i \in I} D_i\right)$. Clearly, for any $z_1, z_2 \in B_d$, we have $F_a(z_1) - F_a(z_2) = 0$, and thus $z_1 - z_2 \in E_a$, which implies $B_d \subseteq c + E_a$ for some $c \in \mathbb{F}_q$. Since $J \subseteq I$, we know that $|B_d| = |J| = p^t$. Therefore, there exists $c \in \mathbb{F}_q$ such that $B_d = c + E_a \subseteq D_{m,b}\left(\bigcup_{i \in I} D_i\right)$, and thus $\mathcal{A}'$ is nonempty.

Now we specify the function F_a which is equal to $F_\alpha(x) = x^{p^t} - \alpha^{p^t - 1}x$. We derive the following results. The first one concerns the function composition $D_{m,b} \circ F_\alpha$.

Theorem 8. *Let* $F_\alpha(x) = x^{p^t} - \alpha^{p^t-1}x$*, where* $\mathbb{F}_{p^t} \subseteq \mathbb{F}_q = \mathbb{F}_{p^s}$*,* $\alpha \in \mathbb{F}_q$*. Then, for* $b \in \mathbb{F}_q^*$ *and integer* $m \geqslant 3$ *satisfying* $m|(q-1)$*,* $D_{m,b} \circ F_\alpha$ *is an* (mp^t-1)*-good polynomial if and only if there exists* $i \in I$ *such that*

$$\mathrm{Tr}_t^s\left(\alpha^{-p^t}\left(u_j + b \cdot u_j^{-1}\right)\right) = 0$$

holds for all $j = 0, 1, \ldots, m-1$*, where* I *is defined in (7) and (9) for* q *odd and* q *even respectively,* $u_j = \xi^{i+j(q-1)/m}$*, and* ξ *is a primitive element of* $\mathbb{F}_q$*.*

As a consequence, one can obtain the following result.

Corollary 4. *For* q *odd, let* $F_\alpha(x) = x^{p^t} - \alpha^{p^t-1}x$*, where* $\mathbb{F}_{p^t} \subsetneq \mathbb{F}_q = \mathbb{F}_{p^s}$*,* $\alpha \in \mathbb{F}_q$*. Let integer* $m \geqslant 3$ *such that* $m|(q-1)$ *and* $(q-1)/m$ *is even, and let* b *be a non-square in* $\mathbb{F}_q^*$*. Then,* $D_{m,b} \circ F_\alpha$ *is an* (mp^t-1)*-good polynomial if and only if* $N \geqslant m$*, where*

$$N = \frac{1}{p^{tm}} \sum_{\substack{c_i \in \mathbb{F}_{p^t} \\ i=1,\ldots,m}} K_s\left(\alpha^{-p^t}\left(\sum_{i=1}^{m} c_i \xi^{i(q-1)/m}\right), \alpha^{-p^t} b\left(\sum_{i=1}^{m} c_i \xi^{-i(q-1)/m}\right)\right), \tag{11}$$

$K_s(\cdot,\cdot)$ *is the Kloosterman sum on* $\mathbb{F}_q$*, and* ξ *is a primitive element of* $\mathbb{F}_q$*.*

The second result is dealing with the function composition $F_\alpha \circ D_{m,b}$.

Theorem 9. *For* q *odd, let* $F_\alpha(x) = x^{p^t} - \alpha^{p^t-1}x$*, where* $\mathbb{F}_{p^t} \subsetneq \mathbb{F}_q = \mathbb{F}_{p^s}$*,* $\alpha \in \mathbb{F}_q$*. Let integer* $m \geqslant 3$ *such that* $m|(q-1)$ *and* $(q-1)/m$ *is even, and let* b *be a non-square in* $\mathbb{F}_q^*$*, then* $F_\alpha \circ D_{m,b}$ *is an* (mp^t-1)*-good polynomial if and only if there exists* $(u_1, \ldots, u_{p^t}) \in \left(\mathbb{F}_q^*\right)^{p^t}$ *such that*

$$u_i^m + \left(bu_i^{-1}\right)^m - u_1^m - \left(bu_1^{-1}\right)^m = \alpha\theta^{i-2},$$

hold for all $i = 2, \ldots, p^t$*, where* θ *is a primitive element of* $\mathbb{F}_{p^t}$*.*

We now present several new r-good polynomials over $\mathbb{F}_{p^s}$ with $r = mp^t - 1$, where $m > 1$, $\gcd(m,p) = 1$, $p^t \not\equiv 1 (\mathrm{mod}\ m)$, and $p^s \equiv 1 (\mathrm{mod}\ m)$. Let l_F be the number of pairwise disjoint subsets with cardinality $r+1$ on which F is constant. The examples are found by MAGMA.

Example 1. Let $F_a(x) = x^{p^t} - a^{p^t-1}x$, where a is a primitive element of $\mathbb{F}_{p^s}$. Let $p = 3$, $t = 1$, $m = 4$. Define

$$H(x) = D_{m,-a} \circ F_a(x) = (x^3 - a^2x)^4 + a(x^3 - a^2x)^2 + 2a^2.$$

1. If $s = 4$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^4}$, and $l_H = 2$.
2. If $s = 6$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^6}$, and $l_H = 11$.
3. If $s = 8$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^8}$, and $l_H = 95$.
4. If $s = 10$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^{10}}$, and $l_H = 803$.

Example 2. Let $F_a(x) = x^{p^t} - a^{p^t-1}x$, where a is a primitive element of $\mathbb{F}_{p^s}$. Let $p = 3$, $t = 1$, $m = 4$. Define

$$H(x) = F_a \circ D_{m,-a}(x) = (x^4 + ax^2 + 2a^2)^3 - a^2(x^4 + ax^2 + 2a^2).$$

1. If $s = 8$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^8}$, and $l_H = 6$.
2. If $s = 10$, then $H(x)$ is a 11-good polynomial on $\mathbb{F}_{3^{10}}$, and $l_H = 34$.

4 Concluding remarks

In this paper, we explored the new methods on constructing r-good polynomials via combining Dickson polynomials with linear functions. We found that there may exist a large number of such r-good polynomials besides the known ones.

Acknowledgement. We would like to thank Gaojun Luo for the discussion on r-good polynomials via Dickson polynomials in Hangzhou, China.

References

1. V. R. Cadambe and A. Mazumdar, Bounds on the size of locally recoverable codes, *IEEE Transactions on Information Theory,* vol. 61, no. 11, pp. 5787–5794, 2015.
2. W. S. Chou, J. Gomez-Calderon, and G. L. Mullen, Value sets of Dickson polynomials over finite fields, *Journal of Number Theory,* vol. 30, no. 3, pp. 334–344, 1988.
3. P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, On the locality of codeword symbols, *IEEE Transactions on Information Theory,* vol. 58, no. 11, pp. 6925–6934, 2012.
4. H. Lausch and W. Nöbauer, *Algebra of Polynomials,* North-Holland, Amsterdam, 1973.
5. R. Lidl, G. L. Mullen, and G. Turnwald, Dickson Polynomials, *Pitman Monographs in Pure and Applied Mathematics*, vol. 65, Addison-Wesley, Reading, MA, 1993.
6. J. Liu, S. Mesnager, and L. Chen, New constructions of optimal locally recoverable codes via good polynomials, *IEEE Transactions on Information Theory,* vol. 64, no. 2, pp. 889–899, 2018.
7. G. Micheli, Constructions of locally recoverable codes which are optimal. arXiv:1806.11492 [cs.IT], 2018.
8. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, New York: Cambridge University Press, 1997.
9. I. Tamo and A. Barg, A family of optimal locally recoverable codes, *IEEE Transactions on Information Theory,* vol. 60, no. 8, pp. 4661–4676, 2014.