Contemporary Mathematics

Dickson permutation polynomials that decompose in cycles of the same length

Ivelisse M. Rubio, Gary L. Mullen, Carlos Corrada, and Francis N. Castro

Abstract. In this paper we study permutations of finite fields $\mathbf{F}_q$ given by Dickson polynomials. For certain families of Dickson permutation polynomials we give the necessary and sufficient conditions on the degree of the polynomial in order to obtain a permutation that decomposes in cycles of the same length.

1. Introduction

Consider $\mathbf{F}_q$, the finite field of $q = p^f$ elements, where p is a prime number. The *Dickson polynomial* $D_i(x, a)$ of degree i is defined as:

$$D_i(x,a) := \sum_{j=0}^{\lfloor i/2 \rfloor} \frac{i}{i-j} \binom{i-j}{j} (-a)^j \, x^{i-2j}.$$

It is known that the Dickson monomial of degree i, $D_i(x, 0) := x^i$ produces a permutation of $\mathbf{F}_q$ if and only if $\gcd(i, q-1) = 1$. Also, for $a \neq 0$, the Dickson polynomial of degree i, $D_i(x, a)$, produces a permutation of $\mathbf{F}_q$ if and only if $\gcd(i, q^2-1) = 1$.

Using the fact that Dickson permutation polynomials $D_i(x, a)$ are closed under composition of polynomials if and and only if $a = 0, 1, -1$, in [**LM**], Lidl and Mullen studied the cycle structure of Dickson permutation polynomials where $a = 0, 1, -1$. Permutation monomials x^i with all the cycles of the same length (ignoring the fixed points) were characterized by Rubio and Corrada in [**RC**]. For the sake of completeness we include the following theorem that characterizes the permutation monomials that decompose in cycles of the same length.

Theorem 1.1. *Let $q - 1 = p_1^{k_1} \dots p_r^{k_r}$ and suppose that $\gcd(i, q-1) = 1$. The permutation of $\mathbf{F}_q$ given by x^i has cycles of the same length j if and only if one of the following holds for each $l = 1, \dots, r$:*

1991 *Mathematics Subject Classification.* Primary 12E10; Secondary 11T06.

Key words and phrases. Dickson polynomials, permutations, finite fields, cyclic decomposition.

The first author was partially supported by the National Security Agency, Grant Number H98230-04-C-0486, and by the ADVANCE Institutional Transformation Program, NSF Grant SBE-0123654.

1. $i \equiv 1 \pmod{p_l^{k_l}}$
2. $j = \mathrm{ord}_{p_l^{k_l}}(i)$ *and* $j \,|\, (p_l - 1)$
3. $j = \mathrm{ord}_{p_l^{k_l}}(i)$, $k_l \geq 2$ *and* $j = p_l$.

In this work we characterize Dickson permutation polynomials $D_i(x,1)$ and $D_i(x,-1)$ that decompose in cycles of the same length. With this characterization one can construct Dickson permutations with a prescribed cycle length as we will see in Section 4. Being able to construct permutations with certain cycle structure may prove to be very important in applications like turbo-like coding or low-density parity-check codes (LDPC) where cycles or lack thereof are fundamental for the performance of the codes. We also characterize Dickson permutation polynomials that decompose in cycles of length two. These types of permutations are their own inverse and are useful in applications to coding theory because the same technology used for encoding can be used for decoding. We are currently undertaking the task of distinguishing which of the permutations described here provide good interleavers for these applications.

From now on j will denote a positive integer and $(n,m) = \gcd(n,m)$ denotes the greatest common divisor of n and m. We say that a permutation *decomposes in cycles of length* j if all of the nontrivial cycles of the permutation have length j. Also, we say that j is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$ if j is the smallest integer such that $i^j \equiv 1 \pmod{t}$ or $i^j \equiv -1 \pmod{t}$.

2. Dickson Permutation Polynomials $D_i(x,1)$

The cycle structure of Dickson permutation polynomials $D_i(x,1)$ is determined by the following theorem proved in [**LM**].

THEOREM 2.1. *Let j be a positive integer and let $D_i(x,1)$ permute $\mathbf{F}_q$. Then $D_i(x,1)$ has a cycle of length j if and only if $q-1$ or $q+1$ has a divisor t such that j is the smallest integer with $i^j \equiv \pm 1 \pmod{t}$. Moreover the number M_j of such cycles is*

$$jM_j = \frac{\big(q+1, i^j+1\big) + \big(q-1, i^j+1\big) + \big(q+1, i^j-1\big) + \big(q-1, i^j-1\big)}{2} - \epsilon - \sum_{k|j, k<j} kM_k,$$

where

$$\epsilon = \begin{cases} 1 & \text{if } p = 2, \text{ or } p \text{ is odd and } i \text{ is even} \\ 2 & \text{if } p \text{ is odd and } i \text{ is odd.} \end{cases}$$

Note that this theorem gives a formula for counting the number of fixed points of the permutation (also see Theorems 3.35 and 3.36 in [**LMT**]). The number of points of $\mathbf{F}_q$ fixed by the permutation $D_i(x,1)$ is:

$((q+1, i+1) + (q-1, i+1) + (q+1, i-1) + (q-1, i-1))/2 - \epsilon$, where ϵ is as defined in Theorem 2.1.

The following corollary to Theorem 2.1 characterizes the Dickson permutation polynomials $D_i(x,1)$ that decompose in cycles of the same length j.

COROLLARY 2.2. All non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x,1)$ have cycles of length j if and only if for every divisor t of $q-1$, $i \equiv \pm 1 \pmod{t}$ or j is the smallest integer with $i^j \equiv \pm 1 \pmod{t}$

and for every divisor s of $q+1$, $i \equiv \pm 1 \pmod{s}$ or j is the smallest integer with $i^j \equiv \pm 1 \pmod{s}$.

One can use the above corollary to obtain Dickson permutation polynomials $D_i(x,1)$ that decompose in cycles of length j but this would imply checking the conditions for every divisor of $q+1$ and $q-1$. Also, if one wants to use the corollary to find the exponents i with this property, one will have to do an exhaustive search. It seems difficult to use a direct application of the Chinese Remainder Theorem to reformulate Corollary 2.2 in terms of the prime power divisors of $q-1$ and $q+1$. More conditions are needed in the situations presented in Lemmas 2.15 and 2.16. These lemmas are used in Theorem 2.17 to give the necessary and sufficient conditions on the highest power of the primes dividing $q-1$ and $q+1$ to obtain Dickson permutation polynomials that decompose in cycles of the same length.

The following definitions and notations will be used on the rest of the paper:

DEFINITION 2.3. Suppose that $\gcd(i,t)=1$. Denote by $j = \mathrm{ord}_t(i)$ the smallest integer j such that $i^j \equiv 1 \pmod{t}$.

DEFINITION 2.4. Suppose that $\gcd(i,t)=1$. Denote by $j = \mathrm{ord}_t^-(i)$ the smallest integer j such that $i^j \equiv -1 \pmod{t}$.

The conditions in the above corollary are related to these definitions but it is important to note that $j = \mathrm{ord}_t(i)$ does not imply that j is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$. The following lemmas, which are very easy to prove, relate $\mathrm{ord}_t(i)$ and $\mathrm{ord}_t^-(i)$.

LEMMA 2.5. *If* $\mathrm{ord}_t^-(i)$ *exists, then* $\mathrm{ord}_t^-(i) \leq \mathrm{ord}_t(i)$.

LEMMA 2.6. *Suppose that* $\mathrm{ord}_t^-(i)$ *exists. Then,* $\mathrm{ord}_t^-(i) = \mathrm{ord}_t(i)$ *if and only if* $t = 2$ *and* $i \equiv 1 \pmod{2}$.

LEMMA 2.7. *Let* p *be a prime,* $p^k \neq 2$*, and suppose that* $\mathrm{ord}_{p^k}^-(i)$ *exists. Then* $j = \mathrm{ord}_{p^k}^-(i)$ *implies that* $2j = \mathrm{ord}_{p^k}(i)$.

Since we want to reduce the conditions in Corollary 2.2 from any divisor of $q+1$ and $q-1$ to only the highest powers of the primes dividing $q+1$ and $q-1$, we need to relate $\mathrm{ord}_{p_l^{k_l}}(i)$ to $\mathrm{ord}_{p_l^h}(i)$ for $h < k_l$ and $\mathrm{ord}_{p_l^{k_l}}^-(i)$ to $\mathrm{ord}_{p_l^h}^-(i)$ for $h < k_l$. Also, for $l \neq m$, we need to relate $\mathrm{ord}_{p_l^{k_l}}(i)$ to $\mathrm{ord}_{p_m^{k_m}}(i)$ and $\mathrm{ord}_{p_l^{k_l}}^-(i)$ to $\mathrm{ord}_{p_m^{k_m}}^-(i)$. The relations needed for our results are shown in the following lemmas.

LEMMA 2.8. *Let* p *be a prime and suppose that* $p = \mathrm{ord}_{p^k}(i)$ *for some* $k \geq 2$. *Then either* $2 = p = \mathrm{ord}_{p^l}(i)$ *for* $2 \leq l \leq k$ *or* $i \equiv 1 \pmod{p^l}$ *for* $1 \leq l < k$.

PROOF. It is easy to see that the result follows for $k = 2, 3$.

Let $p = 2$ and $k \geq 4$. Suppose that $2 = \mathrm{ord}_{2^k}(i) = \mathrm{ord}_{2^{k-1}}(i)$ and $i \equiv 1 \pmod{2^{k-2}}$. Then $2^2 | (i-1)$ and, since $2 = \mathrm{ord}_{2^{k-1}}(i)$ implies that $2^{k-1} \nmid (i-1)$, one must have that $2^2 | (i+1)$. This implies that $4|2$ which is absurd. Hence, $2 = p = \mathrm{ord}_{p^l}(i)$ for $2 \leq l \leq k$ or $i \equiv 1 \pmod{2^l}$ for $1 \leq l < k$.

Now let $p \neq 2$ and $p = \mathrm{ord}_{p^k}(i)$. Then, $i \equiv \alpha^{\frac{\varphi(p^k)}{p}} \pmod{p^k}$ for some α a primitive root mod p^k. This implies that $i \equiv \alpha^{p^{k-2}(p-1)} \equiv \alpha^{\varphi(p^l)p^{k-l-1}} \equiv 1 \pmod{p^l}$, for $1 \leq l < k$. □

LEMMA 2.9. *Let p be a prime and suppose that $p = \mathrm{ord}^-_{p^k}(i)$ for some $k \geq 2$. Then $p \neq 2$ and $i \equiv -1 \pmod{p^l}$ for $1 \leq l < k$.*

PROOF. If $2 = \mathrm{ord}^-_{2^k}(i)$ for some $k \geq 2$, then $2^2|(i^2+1)$ and i is odd. This implies that $2|(i-1)$ and $2|(i+1)$ and hence $2^2|(i^2-1)$. But this implies that $4|2$, which is impossible. Therefore $2 \neq \mathrm{ord}^-_{2^k}(i)$ for $k \geq 2$

Suppose now that $p \neq 2$ and $p = \mathrm{ord}^-_{p^k}(i)$. Then $i \equiv \alpha^{\frac{\varphi(p^k)}{2p}} \pmod{p^k}$ for some α a primitive root mod p^k, and, since $p \neq 2$, $i \equiv \alpha^{\frac{\varphi(p^l)}{2}p^{k-l-1}} \equiv -1 \pmod{p^l}$ for $1 \leq l < k$.

□

The following lemmas are similar to results presented in [**RC**] for the case of permutation monomials and their proofs are omitted.

LEMMA 2.10. *Let p be a prime. Then $j = \mathrm{ord}_{p^k}(i)$ and $j|(p-1)$ if and only if $j = \mathrm{ord}_{p^l}(i)$ for all $l \leq k$.*

LEMMA 2.11. *Let p be a prime, j odd and $k \geq 2$. Then $j = \mathrm{ord}^-_{p^k}(i)$ and $j|(p-1)$ if and only if $j = \mathrm{ord}^-_{p^l}(i)$ for all $l \leq k$.*

LEMMA 2.12. *Let p be a prime and j even. Then $j = \mathrm{ord}^-_{p^k}(i)$ and $2j|(p-1)$ if and only if $j = \mathrm{ord}^-_{p^l}(i)$ for all $l \leq k$.*

LEMMA 2.13. *Let $j = \mathrm{ord}^-_s(i)$, $j = \mathrm{ord}^-_t(i)$ and $\gcd(s,t) = 1$. Then $j = \mathrm{ord}^-_{st}(i)$.*

LEMMA 2.14. *Let $j = \mathrm{ord}^-_s(i)$, $i \equiv -1 \pmod{t}$, j odd and $\gcd(s,t) = 1$. Then $j = \mathrm{ord}^-_{st}(i)$.*

The next two lemmas will be combined to obtain the main theorem of this section.

LEMMA 2.15. *Let $n = q-1 = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ be the prime factorization of n. Suppose that $\gcd(i, q^2-1) = 1$. If all the non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x,1)$ have the same length j, then $i \equiv \pm 1 \pmod{n}$, or exactly one of the following hold for all $l = 1, \dots, r$.*

(1) *Either*
   (a) $i \equiv -1 \pmod{p_l^{k_l}}$ *and* (*j odd or $p_l^{k_l} = 2$*), or*
   (b) $j = \mathrm{ord}^-_{p_l^{k_l}}(i)$, *and* (*$j$ odd and $j|(p_l-1)$, or $2j|(p_l-1)$*), or*
   (c) $j = \mathrm{ord}^-_{p_l^{k_l}}(i)$, $k_l \geq 2$ *and* $j = p_l \neq 2$.

(2) $i \not\equiv 1 \pmod{n}$, *j odd and either*
   (a) $i \equiv 1 \pmod{p_l^{k_l}}$, *or*
   (b) $j = \mathrm{ord}_{p_l^{k_l}}(i)$ *and* $j|(p_l-1)$, *or*
   (c) $j = \mathrm{ord}_{p_l^{k_l}}(i)$, $k_l \geq 2$ *and* $j = p_l$.

(3) $i \not\equiv \pm 1 \pmod{n}$, $j = 2$ *and either*
   (a) $i \equiv -1 \pmod{p_l^{k_l}}$, *or*
   (b) $i \equiv 1 \pmod{p_l^{k_l}}$, *or*
   (c) $2 = \mathrm{ord}_{p_l^{k_l}}(i)$, $k_l \geq 2$, *and* $p_l = 2$.

PROOF. Suppose that all the cycles have length j, or are fixed points. Suppose that $i \not\equiv \pm 1 \pmod{q-1}$. By Corollary 2.2, $j = \mathrm{ord}_t(i)$, or $j = \mathrm{ord}_t^-(i)$ or $i \equiv \pm 1 \pmod{t}$ for all t that divides $q-1$. This holds in particular for all $t = p_l^{k_l}$, $l = 1, \ldots, r$. We first show that if $p_l^{k_l}$ divides $q-1$, then it satisfies either (a), (b), or (c) in one of the cases of the lemma. This is, we need to show that:

i. If $1 \neq j = \mathrm{ord}_{p_l^{k_l}}(i)$ and $j \not| (p_l - 1)$, then $j = p_l$ and $k_l \geq 2$.
ii. If $1 \neq j = \mathrm{ord}_{p_l^{k_l}}(i)$, then j odd or $i \equiv -1 \pmod{p_l^{k_l}}$ or $j = p_l = 2, k_l \geq 2$.
iii. For $l \neq m$, if $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ and $i \equiv -1 \pmod{p_m^{k_m}}$, then j is odd, or $p_m^{k_m} = 2$.
iv. If $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ and $j \not| (p_l - 1)$, then $j = p_l \neq 2$ and $k_l \geq 2$.
v. If $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ and $2j \not| (p_l - 1)$, then $j = p_l \neq 2$ and $k_l \geq 2$.

- **Proof of i:** This result follows from Theorem 2 in [**RC**].
- **Proof of ii:** Suppose that $1 \neq j = \mathrm{ord}_{p_l^{k_l}}(i)$ and j even. Then $j = 2h$ and $p_l^{k_l} | (i^h - 1)(i^h + 1)$. Since all the cycles have the same length j, one must have that $h = 1$ and $j = 2$. Suppose that $i \not\equiv -1 \pmod{p_l^{k_l}}$. Then, since $2 = \mathrm{ord}_{p_l^{k_l}}(i)$, one has that $p_l^{k_l} \not| (i-1)$ and $p_l^{k_l} \not| (i+1)$. Therefore $p_l | (i+1)$ and $p_l | (i-1)$, which implies that $p_l = 2 = j$. Since $2^{k_l} \not| (i-1)$, one must have that $k_l \geq 2$.
- **Proof of iii:** Suppose that $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$, $i \equiv -1 \pmod{p_m^{k_m}}$, and j is even. Then $i^j \equiv 1 \pmod{p_m^{k_m}}$. Since all the cycles have the same length, we have that $p_m^{k_m} p_l^{k_l} | (i^j - 1)$ or $p_m^{k_m} p_l^{k_l} | (i^j + 1)$. Therefore $p_l^{k_l} = 2$ or $p_m^{k_m} = 2$. If $p_l^{k_l} = 2$, then $i \equiv 1 \pmod{p_l^{k_l}}$ and this is a contradiction.
- **Proof of iv:** Suppose that $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ and $j \not| (p_l - 1)$. If $k_l = 1$, then $p_l \neq 2$ and, by Lemma 2.7, $2j = \mathrm{ord}_{p_l}(i)$, $2j | (p_l - 1)$ and therefore $j | (p_l - 1)$, which is a contradiction. Hence $k_l \geq 2$.

  Lemmas 2.11 and 2.12 imply that $h = \mathrm{ord}^-_{p_l^s}(i)$ for some $s < k_l$ and $h < j$. But, since all the cycles have the same length j, $h = 1$ and $i \equiv -1 \pmod{p_l^s}$. Let s be the largest such that $j \neq \mathrm{ord}^-_{p_l^s}(i)$. Then, $j = \mathrm{ord}^-_{p_l^{s+1}}(i)$ and $2j = \mathrm{ord}_{p_l^{s+1}}(i)$. If $p_l = 2$, then $2^s | (i+1)$ and $2^{s+1} | (i^2 - 1)$. This implies that $j = 2 = p_l$, but this contradicts Lemma 2.9. Therefore p_l is odd. By Lemma 3 in Chapter 4 of [**IR**], one has that $i^{p_l} \equiv (-1)^{p_l} \equiv -1 \pmod{p_l^{s+1}}$. Hence, $i^{2p_l} \equiv 1 \pmod{p_l^{s+1}}$. This implies that $2j | 2p_l$ and $j = p_l$.
- **Proof of v:** Suppose $1 \neq j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ and $2j \not| (p_l - 1)$. If $j \not| (p_l - 1)$, then we get the result by iv. Suppose that $j | (p_l - 1)$. Then $p_l \neq 2$ and $2j = \mathrm{ord}_{p_l^{k_l}}(i)$. Since $2j \not| (p_l - 1)$, Lemma 2.10 implies that $h = \mathrm{ord}_{p_l^s}(i)$ for some $h < 2j$ and $s < k_l$. But, since the cycles have the same length, $h = 1$ and $i \equiv 1 \pmod{p_l^s}$. Therefore $i^j \equiv 1 \pmod{p_l^s}$ and $i^j \equiv -1 \pmod{p_l^s}$. This implies that $p_l^s = 2$ which is a contradiction.

We now need to show that the same case of the lemma holds for all $p_1^{k_1}, \ldots, p_r^{k_r}$. To see this it is enough to prove that, if $p_l^{k_l}$ and $p_m^{k_m}$ both divide $q-1$ for $l \neq m$, then:

vi. If $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$, then $j \neq \text{ord}^-_{p_m^{k_m}}(i)$. That is, if $p_l^{k_l}$ satisfies case 2 or case 3, then $p_m^{k_m}$ cannot satisfy case 1.

vii. If $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$, $i \not\equiv -1 \pmod{p_l^{k_l}}$ and $i \equiv -1 \pmod{p_m^{k_m}}$, then j is odd and $i \equiv 1 \pmod{p_m^{k_m}}$ (and we are in case 2), or $2 = j = p_l, k_l \geq 2$ (and we are in case 3).

viii. If $1 \neq j = \text{ord}^-_{p_l^{k_l}}(i)$ and $i \equiv 1 \pmod{p_m^{k_m}}$, then $i \equiv -1 \pmod{p_m^{k_m}}$ (and we have case 1).

- **Proof of vi:** Suppose that $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$ and $j = \text{ord}^-_{p_m^{k_m}}(i)$. Then, since all the cycles have the same length j, $i^j \equiv \pm 1 \pmod{p_l^{k_l} p_m^{k_m}}$. This implies that $p_l^{k_l} | (i^j + 1)$ or $p_m^{k_m} | (i^j - 1)$ and therefore $p_l^{k_l} = 2$ or $p_m^{k_m} = 2$. Hence $i \equiv 1 \pmod{p_l^{k_l}}$ or $i \equiv 1 \pmod{p_m^{k_m}}$, which is a contradiction to $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$ or $1 \neq j = \text{ord}^-_{p_m^{k_m}}(i)$.
- **Proof of vii:** Suppose that $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$ and $i \equiv -1 \pmod{p_m^{k_m}}$. Then, since all the cycles have the same length j, we have that $p_m^{k_m} p_l^{k_l} | (i^j - 1)$ or $p_m^{k_m} p_l^{k_l} | (i^j + 1)$.

  Suppose that $p_m^{k_m} p_l^{k_l} | (i^j - 1)$ and j is odd. Since $i \equiv -1 \pmod{p_m^{k_m}}$, we have that $i^j \equiv -1 \pmod{p_m^{k_m}}$. This implies that $p_m^{k_m} | (i^j - 1)$ and $p_m^{k_m} | (i^j + 1)$ and hence $p_m^{k_m} = 2$. Therefore $i \equiv 1 \pmod{p_m^{k_m}}$ and this follows under case 2 of the lemma.

  Suppose that $p_m^{k_m} p_l^{k_l} | (i^j - 1)$ and j is even. The same arguments in the proof of ii show that $p_l = 2 = j$ and $k_l \geq 2$.

  Suppose now that $p_m^{k_m} p_l^{k_l} | (i^j + 1)$. Then $p_l^{k_l} | (i^j + 1)$ and, since $p_l^{k_l} | (i^j - 1)$, we have that $p_l^{k_l} = 2$. This implies that $i \equiv 1 \pmod{p_l^{k_l}}$, a contradiction to $1 \neq j = \text{ord}_{p_l^{k_l}}(i)$.
- **Proof of viii:** The proof is similar to the proof of vii.

□

The next lemma deals with the divisors of $q+1$ and its proof is the same as the proof of Lemma 2.15.

LEMMA 2.16. *Let $n = q + 1 = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be the prime factorization of n. Suppose that $\gcd(i, q^2 - 1) = 1$. If all the non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x, 1)$ have the same length j, then $i \equiv \pm 1 \pmod{n}$, or exactly one of the cases of the above lemma holds for all $l = 1, \ldots, r$.*

The following theorem gives the necessary and sufficient conditions for a permutation $D_i(x, 1)$ to decompose in cycles of the same length.

THEOREM 2.17. *Let $q - 1 = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ and $q + 1 = p_{r+1}^{k_{r+1}} p_{r+2}^{k_{r+2}} \ldots p_s^{k_s}$ be the prime factorizations of $q - 1$ and $q + 1$. Suppose that $\gcd(i, q^2 - 1) = 1$. The permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x, 1)$ is the identity on $\mathbf{F}_q$ or all non-trivial cycles have the same length j if and only if $i \equiv \pm 1 \pmod{q-1}$ or exactly one of the cases in Lemma 2.15 holds for all $l = 1, 2, \ldots, r$, and $i \equiv$*

$\pm 1 \pmod{q+1}$ *or exactly one of the cases in Lemma 2.15 holds for all* $l = r+1, r+2, \ldots, s$.

PROOF. ($\Longrightarrow$) If the permutation is the identity on $\mathbf{F}_q$, then $i \equiv \pm 1 \pmod{q-1}$ and $i \equiv \pm 1 \pmod{q+1}$. If the permutation is not the identity and all the non-trivial cycles have length j then $j = \mathrm{ord}_{p_l^{k_l}}(i)$ or $j = \mathrm{ord}^-_{p_l^{k_l}}(i)$ for at least one $1 \leq l \leq s$ and Lemmas 2.15 and 2.16 show this direction of the statement.

($\Longleftarrow$) If $i \equiv \pm 1 \pmod{q-1}$ and $i \equiv \pm 1 \pmod{q+1}$ then $D_i(x,1)$ is the identity on $\mathbf{F}_q$. Suppose that $i \not\equiv \pm 1 \pmod{q-1}$ and case 1 of Lemma 2.15 holds for every $p_l^{k_l}$ that divides $q-1$. Lemmas 2.9, 2.11 and 2.12 guarantee that $j = \mathrm{ord}^-_{p_l^h}(i)$ or $i \equiv -1 \pmod{p_l^h}$ for all $l = 1, 2, \ldots, r$ and $h \leq k_l$. If $t|(q-1)$ Lemmas 2.13 and 2.14 guarantee that $j = \mathrm{ord}^-_t(i)$ or $i \equiv -1 \pmod{t}$. Since $\mathrm{ord}^-_t(i) \leq \mathrm{ord}_t(i)$, this implies that $i \equiv -1 \pmod{t}$ or j is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$.

Suppose that case 2 of Lemma 2.15 holds for every $p_l^{k_l}$ that divides $q-1$. Then, by arguments similar to those on the proof of Theorem 2 in [**RC**], one has that $j = \mathrm{ord}_t(i)$ or $i \equiv 1 \pmod{t}$. Since j is odd, we have that $\mathrm{ord}^-_t(i)$ does not exist and therefore $i \equiv \pm 1 \pmod{t}$ or j is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$.

Suppose that case 3 of Lemma 2.15 holds for every $p_l^{k_l}$ that divides $q-1$. Then $i \equiv \pm 1 \pmod{p_l^{k_l}}$ or $2 = \mathrm{ord}_{2^{k_l}}(i)$, $k_l \geq 2$. If $i \equiv \pm 1 \pmod{p_l^{k_l}}$, then $i \equiv \pm 1 \pmod{p_l^h}$ for all $h \leq k_l$. If $2 = \mathrm{ord}_{2^{k_l}}(i)$, $k_l \geq 2$, then, by Lemma 2.8 we have that $2 = \mathrm{ord}_{2^h}(i)$ or $i \equiv \pm 1 \pmod{p_l^h}$ for all $h \leq k_l$. Therefore $2 = \mathrm{ord}_t(i)$ or $i \equiv \pm 1 \pmod{t}$ for all $t|(q-1)$ and $i \not\equiv \pm 1 \pmod{q-1}$. This implies that $j = 2$ is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$ or $i \equiv \pm 1 \pmod{t}$.

The above arguments also apply for $q+1$. Therefore, if $D_i(x,1)$ is not the identity on $\mathbf{F}_q$ and j is such that one of the cases of Lemma 2.15 holds for all $p_s^{k_s}$ that divide $q-1$ or $i \equiv \pm 1 \pmod{q-1}$ and one of the cases of Lemma 2.15 holds for all $p_l^{k_l}$ that divide $q+1$ or $i \equiv \pm 1 \pmod{q+1}$, then we have that for every divisor t of $q-1$ and for every divisor s of $q+1$, $i \equiv \pm 1 \pmod{t}$ or j is the smallest integer such that $i^j \equiv \pm 1 \pmod{t}$, and $i \equiv \pm 1 \pmod{s}$ or j is the smallest integer such that $i^j \equiv \pm 1 \pmod{s}$. Therefore, by Corollary 2.2, all cycles have length j or 1. □

EXAMPLE 2.18. Consider the Dickson permutation polynomial $D_{31}(x,1)$ over $\mathbf{F}_{17}$ after reducing the exponents modulo 16:

$$D_{31}(x) = x^{15} + 3x^{13} + 9x^{11} + 11x^9 + 5x^7 + 8x^5 + 14x^3 + x.$$

For $p-1 = 17-1 = 16 = 2^4$, we have that $1 = \mathrm{ord}^-_{2^4}(31)$. The value of j cannot be determined by $p-1$; is determined by the divisors of $p+1$.

For $p+1 = 18 = 2 \cdot 3^2$, we have that $1 = \mathrm{ord}_2(31)$, $3 = \mathrm{ord}_{3^2}(31)$. Case 2 (a) and (c) are satisfied and $j = 3$.

Theorem 2.17 implies that all the cycles of the permutation induced by $D_{31}(x,1)$ have length $j = 3$. The number of fixed points is given by the formula after Theorem 2.1: $[(18,32) + (16,32) + (18,30) + (16,30)]/2 - 2 = 11$. The cyclic decomposition is in fact $(3,4,10)(7,14,13)$.

As we mentioned in the introduction, permutations that decompose in cycles of length two are useful in applications to coding theory. The following corollary characterizes the Dickson permutation polynomials $D_i(x,1)$ that decompose in cycles of length two and, hence, are their own inverse.

COROLLARY 2.19. Let $q-1 = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ and $q+1 = p_{r+1}^{k_{r+1}}p_{r+2}^{k_{r+2}}\dots p_s^{k_s}$ be the prime factorizations of $q-1$ and $q+1$. Suppose that $\gcd(i, q^2-1) = 1$. The permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x,1)$ is the identity on $\mathbf{F}_q$ or all the non-trivial cycles have length two if and only if one of the following holds for all $l = 1, 2, \dots, r$ and one of the following holds for all $l = r+1, r+2, \dots, s$:

(1) Either
   (a) $i \equiv 1 \pmod{p_l^{k_l}}$ and $p_l^{k_l} = 2$, or
   (b) $2 = \operatorname{ord}^-_{p_l^{k_l}}(i)$, and $4|(p_l-1)$.
(2) Either
   (a) $i \equiv \pm 1 \pmod{p_l^{k_l}}$, or
   (b) $2 = \operatorname{ord}_{p_l^{k_l}}(i), p_l = 2$, $k_l \geq 2$, and $i \not\equiv -1 \pmod{p_l^{k_l}}$.

We close this section with a nice approach to finding the necessary and sufficient conditions to obtain Dickson permutation polynomials with cycles of the same length suggested by Rex Matthews. We thank Rex Matthews for his idea, which can be stated as follows:

THEOREM 2.20. *Let $\mathbf{F}_q$ be a field with odd characteristic and let i be such that $\gcd(i, q^2-1) = 1$. All non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x,1)$ have length j if and only if $j = \operatorname{ord}_s^-(i)$ and $\gcd(i^t+1, s) = \gcd(i+1, s)$ for all $t < j$, or $j = \operatorname{ord}_s(i)$ and $\gcd(i^t-1, s) = \gcd(i-1, s)$ for all $t < j$, for $s = q-1$ and $s = q+1$.*

3. Dickson Permutation Polynomials $D_i(x,-1)$

We now consider the case $D_i(x,-1)$. Since for $p = 2$, $D_i(x,1) = D_i(x,-1)$, it is enough to consider $D_i(x,-1)$ for $\mathbf{F}_q$ with odd characteristic. Since $D_i(x,-1)$ is permutation polynomial if and only if $\gcd(i, q^2-1) = 1$, we will also consider i to be odd. Let $\nu_\rho(m)$ denote the highest power of ρ dividing $m \neq 0$ and set $\nu_\rho(0) = \infty$.

The cycle structure of Dickson permutation polynomials $D_i(x,-1)$ is determined by the following theorem proved in [**LM**].

THEOREM 3.1. *Let j be a positive integer and let $D_i(x,-1)$ permute $\mathbf{F}_q$. If i and q are odd, then $D_i(x,-1)$ has a cycle of length j if and only if $q-1$ or $q+1$ has a divisor t such that $j = \operatorname{ord}_t(i)$ or j is the smallest such that $2(i^j+1) \equiv 0 \pmod{t}$. Moreover the number K_j of such cycles is*

$$jK_j = \frac{a_1\left(2(q+1), i^j+1\right) + a_2\left(q-1, i^j+1\right) + a_3\left(q+1, (i^j-1)/2\right)}{2} + \frac{\left(q-1, i^j-1\right)}{2} - \epsilon - \sum_{m|j, m<j} mK_m,$$

where

$$\epsilon = \begin{cases} 2 & \text{if } i^j \equiv 1 \text{ and } q \equiv 1 \pmod 4 \\ 0 & \text{otherwise,} \end{cases} \qquad a_1 = \begin{cases} 1 & \text{if } \nu_2(i^j+1) = \nu_2(q+1) \\ 0 & \text{otherwise,} \end{cases}$$

$$a_2 = \begin{cases} 1 & \text{if } \nu_2(i^j+1) < \nu_2(q+1) \\ 0 & \text{otherwise,} \end{cases} \qquad a_3 = \begin{cases} 1 & \text{if } \nu_2(i^j+1) > \nu_2(q+1) \\ 0 & \text{otherwise.} \end{cases}$$

Note that this theorem gives us a formula for counting the number of fixed points of the permutation (also see Theorems 3.35 and 3.36 in [**LMT**]). The number of points of $\mathbf{F}_q$ fixed by the permutation $D_i(x,-1)$ is: $(a_1\,(2(q+1), i+1) + a_2\,(q-1, i+1) + a_3\,(q+1, (i-1)/2) + (q-1, i-1))/2 - \epsilon$, where ϵ, a_1, a_2, a_3 are as defined in Theorem 3.1.

The following corollary to Theorem 3.1 characterizes the Dickson permutation polynomials $D_i(x,-1)$ that decompose in cycles of the same length j.

COROLLARY 3.2. All the non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the polynomial $D_i(x,-1)$ have length j if and only if for every divisor t of $q-1$ we have that j is the smallest integer with $i^j \equiv 1 \pmod t$ or $2(i^j+1) \equiv 0 \pmod t$ or $i \equiv 1 \pmod t$ or $2(i+1) \equiv 0 \pmod t$, and, for every divisor s of $q+1$, j is the smallest integer with $i^j \equiv 1 \pmod s$ or $2(i^j+1) \equiv 0 \pmod s$ or $i \equiv 1 \pmod s$ or $2(i+1) \equiv 0 \pmod s$.

As in Section 2 we will reformulate the conditions in order to have Dickson permutation polynomials $D_i(x,-1)$ that decompose in cycles of the same length. Note that in this case, instead of requiring j to be the smallest integer such that $i^j \equiv -1 \pmod t$, it is required that $2(i^j+1) \equiv 0 \pmod t$. The following definition for the case $2(i^j+1) \equiv 0 \pmod t$ is similar to what was defined in Section 2 for $i^j \equiv -1 \pmod t$.

DEFINITION 3.3. Suppose that $\gcd(i,t) = 1$. Denote by $j = \mathrm{ord}_t^{-2}(i)$ the smallest integer j such that $2(i^j+1) \equiv 0 \pmod t$.

It is important to note that $j = \mathrm{ord}_t(i)$ does not imply that j is the smallest such that $i^j \equiv 1 \pmod t$ or $2(i^j+1) \equiv 0 \pmod t$.

Through a sequence of lemmas that we omit because their results and proofs are similar to those used in Section 2, we are able to state the next two lemmas. These lemmas lead to Theorem 3.6, which is a characterization of Dickson permutation polynomials $D_i(x,-1)$ that decompose in cycles of the same length.

LEMMA 3.4. *Let $\mathbf{F}_q$ be a field of odd characteristic and $n = q-1 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ be the prime factorization of n. Suppose that $\gcd(i, q^2-1) = 1$. If all the non-trivial cycles of the permutation of $\mathbf{F}_q$ given by the Dickson polynomial $D_i(x,-1)$ have the same length j, then $i \equiv 1 \pmod n$ or $2(i+1) \equiv 0 \pmod n$, or exactly one of the following hold for all $l = 1, \dots, r$.*

(1) *Either*
   (a) $2(i+1) \equiv 0 \pmod{p_l^{k_l}}$ *and* *(j odd or $p_l^{k_l} = 2, 4$), or*
   (b) $j = \mathrm{ord}_{p_l^{k_l}}^{-2}(i)$, *and (j odd and $j \mid (p_l - 1)$, or $2j \mid (p_l - 1)$), or*
   (c) $j = \mathrm{ord}_{p_l^{k_l}}^{-2}(i)$, $k_l \geq 2$ *and* $j = p_l \neq 2$.

(2) $i \not\equiv 1 \pmod n$, j *odd and either*
   (a) $i \equiv 1 \pmod{p_l^{k_l}}$, *or*
   (b) $j = \mathrm{ord}_{p_l^{k_l}}(i)$ *and* $j \mid (p_l - 1)$, *or*
   (c) $j = \mathrm{ord}_{p_l^{k_l}}(i)$, $k_l \geq 2$ *and* $j = p_l$.

(3) $2(i+1) \not\equiv 0 \pmod n, i \not\equiv 1 \pmod n$, $j = 2$ *and either*
   (a) $2(i+1) \equiv 0 \pmod{p_l^{k_l}}$, *or*

(b) $i \equiv 1 \pmod{p_l^{k_l}}$, *or*
(c) $2 = \mathrm{ord}_{p_l^{k_l}}(i), k_l \geq 2$ *and* $p_l = 2$.

The next lemma deals with the divisors of $q+1$.

LEMMA 3.5. *Let* $\mathbf{F}_q$ *be a field with odd characteristic and* $n = q+1 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *be the prime factorization of* n. *Suppose that* $\gcd(i, q^2-1) = 1$. *If all the non-trivial cycles of the permutation of* $\mathbf{F}_q$ *given by the Dickson polynomial* $D_i(x, -1)$ *have the same length* j, *then* $i \equiv 1 \pmod{n}$ *or* $2(i+1) \equiv 0 \pmod{n}$, *or exactly one of the cases in the above lemma holds for all* $l = 1, \dots, r$.

The following theorem gives the necessary and sufficient conditions for a permutation $D_i(x, -1)$ to decompose in cycles of the same length. The proof is very similar to the proof of Theorem 2.17.

THEOREM 3.6. *Let* $\mathbf{F}_q$ *be a field with odd characteristic and* $q-1 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ *and* $q+1 = p_{r+1}^{k_{r+1}} p_{r+2}^{k_{r+2}} \dots p_s^{k_s}$ *be the prime factorizations of* $q-1$ *and* $q+1$. *Suppose that* $\gcd(i, q^2-1) = 1$. *The permutation of* $\mathbf{F}_q$ *given by the Dickson polynomial* $D_i(x, -1)$ *is the identity on* $\mathbf{F}_q$ *or all the non-trivial cycles have the same length* j *if and only if* $i \equiv 1 \pmod{q-1}$ *or* $2(i+1) \equiv 0 \pmod{q-1}$ *or exactly one of the cases in Lemma 3.4 holds for all* $l = 1, 2, \dots, r$ *and* $i \equiv 1 \pmod{q+1}$ *or* $2(i+1) \equiv 0 \pmod{q+1}$, *and exactly one of the cases in Lemma 3.4 holds for all* $l = r+1, r+2, \dots, s$.

The following corollary characterizes the Dickson permutation polynomials $D_i(x, -1)$ that decompose in cycles of length two and, hence, are their own inverse.

COROLLARY 3.7. Let $\mathbf{F}_q$ be a field with odd characteristic. Also let $q-1 = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ and $q+1 = p_{r+1}^{k_{r+1}} p_{r+2}^{k_{r+2}} \dots p_s^{k_s}$ be the prime factorizations of $q-1$ and $q+1$. Suppose that $\gcd(i, q^2-1) = 1$. The permutation given by the Dickson polynomial $D_i(x, -1)$ is the identity in $\mathbf{F}_q$ or all the non-trivial cycles have length two if and only if one of the following holds for all $l = 1, 2, \dots, r$ and one of the following holds for all $l = r+1, r+2, \dots, s$:

(1) Either
  (a) $2(i+1) \equiv 0 \pmod{p_l^{k_l}}$ and $p_l^{k_l} = 2, 4$, or
  (b) $j = \mathrm{ord}^{-2}_{p_l^{k_l}}(i)$, and $4 | (p_l - 1)$.
(2) Either
  (a) $2(i+1) \equiv 0 \pmod{p_l^{k_l}}$, or
  (b) $i \equiv 1 \pmod{p_l^{k_l}}$, or
  (c) $2 = \mathrm{ord}_{p_l^{k_l}}(i)$, $k_l \geq 2$ and $p_l = 2$.

4. Construction of Dickson permutation polynomials that decompose in cycles of length j

Certain permutations of $\mathbf{F}_q$ that decompose in cycles of length two and are given by monomials x^i have been used to construct interleavers for turbo codes that have good performance ([**CR**]). As we have mentioned, being able to construct permutations with certain cycle structure may prove to be very important in applications such as turbo-like coding or low-density parity-check codes (LDPC) where cycles or lack thereof are fundamental for the performance of the codes.

Our results are algorithmic in the sense that, given a finite field $\mathbf{F}_q$ and a positive integer j, we can find the degrees i of all the Dickson permutation polynomials $D_i(x,1)$, $D_i(x,-1)$ that decompose in cycles of length j.

We designed an algorithm for constructing the set of all the degrees i such that $D_i(x,1) \in \mathbf{F}_q[x]$ decomposes in cycles of length j. The detailed algorithm can be found in

`http://epsilon.cnnet.upr.edu/irubio/Investigacion/permute.html`.

The main idea is to use primitive roots α_l in $\mathbb{Z}_{p_l{}^{k_l}}$, where $p_l \neq 2$, and $p_l^{k_l}|(q-1)$ or $p_l^{k_l}|(q+1)$ to get elements t_l such that $j = \operatorname{ord}_{p_l^{k_l}}(t_l)$ or $j = \operatorname{ord}^-_{p_l^{k_l}}(t_l)$. Note that $t_l = \alpha_l^{\frac{p_l^{k_l-1}(p_l-1)}{2j}c}$, where $\gcd(c,2j)=1$, is such that $j = \operatorname{ord}^-_{p_l^{k_l}}(t_l)$. Similarly, $t_l = \alpha_l^{\frac{p_l^{k_l-1}(p_l-1)}{j}c}$, where $\gcd(c,j)=1$, is such that $j = \operatorname{ord}_{p_l^{k_l}}(t_l)$. One uses the conditions on Theorem 2.17, the t_l's and the Chinese Remainder Theorem to obtain the desired exponents i.

Acknowledgements

The authors appreciate the careful review, corrections and helpful suggestions to this paper made by the referees. The first author is grateful to the UPR-Humacao ADVANCE Institutional Transformation Program for the continuous support and encouragement.

References

[CR] C. Corrada and I. Rubio, Deterministic Interleavers for Turbo Codes with Random-like Performance and Simple Implementation, *Proceedings of the 3rd International Symposium on Turbo Codes and Related Topics*, 2003, pp. 555–558.

[IR] K. Ireland, M. Rosen, *A Classical Introduciton to Modern Number Theory*, 2nd edition, Springer, 1991.

[LM] R. Lidl, G.L. Mullen, Cycle Structure of Dickson Permutation Polynomials, *Mathematical Journal of Okayama University* **33** (1991), 1–11.

[LMT] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman, Essex, 1993.

[RC] I. Rubio, C. Corrada, *Cyclic Decomposition of Permutations of Finite Fields Obtained Using Monomials*, Finite Fields and Applications, LNCS 2948, pp. 254-261, Springer-Verlag, 2004.

Department of Mathematics, University of Puerto Rico, Humacao, PR 00791
Current address: Department of Computer Science, University of Puerto Rico, Río Piedras, Box 23355, San Juan, PR 00931
E-mail address: `iverubio@uprrp.edu`

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802
E-mail address: `mullen@math.psu.edu`

Department of Computer Science, University of Puerto Rico, Río Piedras, Box 23355, San Juan, PR 00931
E-mail address: `ccorrada@gmail.com`

Department of Mathematics, University of Puerto Rico, Río Piedras, Box 23355, San Juan, PR 00931
E-mail address: `franciscastr@gmail.com`