Fixed Points and Cycle Types of Reversed Dickson Permutation Polynomials

Haoming Wu and Neranga Fernando
Department of Mathematics and Computer Science, College of the Holy Cross

Introduction

Let p be a prime number. Then the finite prime field with characteristic p is given by

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}.$$

We investigate fixed points and cycle types of permutation polynomials arising from reversed Dickson polynomials over $\mathbb{F}_p$.

Reversed Dickson Polynomials

The nth reversed Dickson polynomial (RDP) of the first kind is given by the explicit expression

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

where $a \in \mathbb{F}_p$ is a parameter.

The recurrence relation of reversed Dickson polynomials is given by

$$D_0(a,x) = 2,\ D_1(a,x) = a,$$
$$D_n(a,x) = aD_{n-1}(a,x) - xD_{n-2}(a,x) \text{ for } n \geq 2.$$

Here are the next few reversed Dickson polynomials:

- $D_2(1,x) = 1 - 2x$
- $D_3(1,x) = D_2(1,x) - xD_1(1,x) = (1-2x) - x = 1 - 3x$
- $D_4(1,x) = D_3(1,x) - xD_2(1,x) = 1 - 16x + 2x^2$
- $D_5(1,x) = D_4(1,x) - xD_3(1,x) = 1 - 125x + 5x^2$

Permutation Polynomials and Fixed Points

A *permutation polynomial* (PP) over $\mathbb{F}_p$ is a polynomial that permutes the elements of $\mathbb{F}_p$.

Example 1 Consider the polynomial $g(x) = x^3 + 1$ and evaluate it at each element of $\mathbb{F}_5$. Then, in characteristic 5, we have

$$g(0) = 1,\ g(1) = 2,\ g(2) = 4,\ g(3) = 3,\ g(4) = 0.$$

Since the polynomial $g(x)$ permutes the elements of $\mathbb{F}_5$, $g(x)$ is a permutation polynomial in $\mathbb{F}_5$.

A **fixed point** is a value that does not change under a given mapping.

In Example 1, there is only one fixed point which is 3.

Reversed Dickson Permutation Polynomials

- For any p, $D_2(1,x) = D_{2p}(1,x) = 1 + (p-2)x$ is a PP over $\mathbb{F}_p$.

  Example $D_2(1,x) = D_{26}(1,x) = 11x + 1$ is a PP over $\mathbb{F}_{13}$.

- For any p, $D_3(1,x) = D_{3p}(1,x) = 1 + (p-3)x$ is a PP over $\mathbb{F}_p$.

  Example $\mathrm{D}_3(1,x) = D_{39}(1,x) = 10x + 1$ is a PP over $\mathbb{F}_{13}$.

- When $p \equiv 1$ or $5 \pmod{12}$, $D_{p+1}(1,x) = \frac{1}{2} + \frac{1}{2}(1-4x)^{\frac{p+1}{2}}$ is a PP of $\mathbb{F}_p$.

  Example $D_6(1,x) = 3x^3 + 4x^2 + 4x + 1$ is a PP of $\mathbb{F}_5$.

- When $p \equiv 1$ or $7 \pmod{12}$, $D_{p+2}(1,x) = \frac{1}{2}(1-4x)^{\frac{p+1}{2}} + \frac{1}{2} - x$ is a PP over $\mathbb{F}_5$.

  Example $D_9(1,x) = 2x^4 + 5x^3 + 6x^2 + 5x + 1$ is a PP of $\mathbb{F}_7$.

- When $p \equiv 1$ or $7 \pmod{12}$, $D_{2p+1}(1,x) = \frac{1}{2}(1-4x)^{\frac{p+1}{2}} + \frac{1}{2} - x$ is a PP over $\mathbb{F}_7$.

  Example $D_{27}(1,x) = 11x^7 + 10x^6 + 12x^5 + 8x^4 + 11x^3 + 12x^2 + 11x + 1$ is a PP of $\mathbb{F}_{13}$.

Results on Fixed Points

1. Let $p \geq 3$ be an odd prime and $n \in \{2, 2p\}$. Then, the reversed Dickson permutation polynomial $D_n(1,x)$ has exactly one fixed point.
2. Let $p > 3$ be an odd prime and $n \in \{3, 3p\}$. Then, the reversed Dickson permutation polynomial $D_n(1,x)$ has exactly one fixed point.
3. Let $p \equiv 5 \pmod{12}$. The permutation polynomial $D_{p+1}(1,x)$ has no fixed point.
4. Let $p \equiv 1 \pmod{12}$. Then the permutation polynomial $D_{p+1}(1,x)$ has exactly one fixed point, and the permutation polynomials $D_{p+2}(1,x)$ and $D_{2p+1}(1,x)$ have exactly $\frac{p+1}{2}$ fixed points.
5. Let $p \equiv 7 \pmod{12}$. Then the reversed Dickson permutation polynomials $D_{p+2}(1,x)$ and $D_{2p+1}(1,x)$ have exactly $\frac{p+1}{2}$ fixed points.

Cycle Types

In Example 1, we have

$$0 \to 1,\ 1 \to 2,\ 2 \to 4,\ 4 \to 0,$$

This is a four-cycle which can be written as $(0\,1\,2\,4)$. The fixed point is 3. Thus, the cycle type of the permutation induced by $g(x)$ over $\mathbb{F}_5$ is $(4, 1)$, where 4 stands for the four-cycle and 1 stands for the fixed point.

Results on Cycle Types

1. Let $p \equiv 7 \pmod{12}$. Then the reversed Dickson permutation polynomials $D_{p+2}(1,x)$ and $D_{2p+1}(1,x)$ have exactly $\frac{p+1}{2}$ fixed points.
2. Let $p > 3$ be a prime and $j \in \mathbb{Z}^+$ such that $j \mid p-1$. Then, the cycle type of the permutation polynomials $D_2(1,x)$ and $D_{2p}(1,x)$ is $(\underbrace{\frac{p-1}{j}, ..., \frac{p-1}{j}}_{j \text{ times}}, 1)$, where $\mathrm{ord}_p(-2) = \frac{p-1}{j}$. In particular, if -2 is a primitive root modulo p, i.e. $j = 1$, then the cycle type of the permutation polynomials $D_2(1,x)$ and $D_{2p}(1,x)$ is $(p-1, 1)$.
3. Let $p = 3$. Then the cycle type of the permutation polynomials $D_2(1,x)$ and $D_{2p}(1,x)$ is (3).
4. Let $p > 3$ be a prime and $j \in \mathbb{Z}^+$ such that $j \mid p-1$. Then the cycle type of the permutation polynomials $D_3(1,x)$ and $D_{3p}(1,x)$ is $(\underbrace{\frac{p-1}{j}, ..., \frac{p-1}{j}}_{j \text{ times}}, 1)$ where $\mathrm{ord}_p(-3) = \frac{p-1}{j}$. In particular, if -3 is a primitive root modulo p, then the cycle type of the permutation polynomials $D_3(1,x)$ and $D_{3p}(1,x)$ is $(p-1, 1)$.
5. Let $p \geq 3$. Then the cycle type of the polynomial $D_2(1,x) + x$ is $(\underbrace{2, ..., 2}_{\frac{p-1}{2}\text{times}}, 1)$.
6. Let $p \equiv 1 \pmod{12}$ or $p \equiv 7 \pmod{12}$. Let $j \in \mathbb{Z}^+$ such that $j \mid p-1$. Then the permutation polynomials $D_{p+2}(1,x)$ and $D_{2p+1}(1,x)$ have the cycle type $(\underbrace{\frac{p-1}{j}, ..., \frac{p-1}{j}}_{\frac{j}{2} \text{ times}}, \underbrace{1, ..., 1}_{\frac{p+1}{2}\text{times}})$ whenever $\mathrm{ord}_p(-3) = \frac{p-1}{j}$.

Future Plans

Let X be a non-empty set, and let $\triangleright : X \times X \mapsto X$ be a binary operation. The pair $(X, \triangleright)$ is called a quandle if it satisfies the following axioms:
1. For all $x \in X$, $x \triangleright x = x$.
2. For all $x, y \in X$, $\beta_y(x) = x \triangleright y$ is invertible.
3. For all $x, y, z \in X$, $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

Example 2 Let $X = \mathbb{Z}_3$. For $x, y \in X$, define $x \triangleright y = 2y - x \pmod 3$.

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Acknowledgements

The authors would like to thank the Weiss Summer Research Program at College of the Holy Cross for the support.