Complete permutation polynomials from reversed Dickson polynomials and their applications in Cryptography

Jiaqi Fang 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

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

We present complete permutation polynomials arising from reversed Dickson polynomials over $\mathbb{F}_p$. Moreover, we explain an application of complete permutation polynomials in Cryptography.

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:

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

RDPs of the second kind

The nth reversed Dickson polynomial of the second kind is defined by

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

where $a \in \mathbb{F}_p$ is a parameter. The recurrence relation of Dickson polynomials of the second kind $E_n(x,a)$ is given by

$$E_0(x,a) = 1, \ E_1(x,a) = x,$$

$$E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a), \ \text{for } n \geq 2.$$

Permutation Polynomials

A *permutation polynomial* (PP) over $\mathbb{Z}_p$ is a polynomial that permutes the elements of $\mathbb{Z}_p$. For example, consider the polynomial $g(x) = 5x + 1$ and evaluate it at each element of $\mathbb{Z}_7$. Then, in characteristic 7, we have

$$g(0) = 1, \ g(1) = 6, \ g(2) = 4, \ g(3) = 2, \ g(4) = 0, \ g(5) = 5, \ g(6) = 3.$$

Since $g(x)$ permutes the elements of $\mathbb{Z}_7$, $g(x)$ is a permutation polynomial of $\mathbb{Z}_7$.

Complete Permutation Polynomials

A polynomial $f(x)$ is called a *complete permutation polynomial* (CPP) if both $f(x)$ and $f(x) + x$ are permutation polynomials.

Consider the polynomial $h(x) = g(x) + x = 6x + 1$ and evaluate it at each element of $\mathbb{F}_7$. Then, in characteristic 7, we have

$$h(0) = 1, \ h(1) = 0, \ h(2) = 6, \ h(3) = 5, \ h(4) = 4, \ h(5) = 3, \ h(6) = 2.$$

Since both $g(x)$ and $g(x)+x$ permute the elements of $\mathbb{Z}_7$, $g(x)$ is a complete permutation polynomial of $\mathbb{Z}_7$.

Results

1. Clearly, $D_0(1,x)$ is a CPP over $\mathbb{Z}_3$.
2. Let $n \geq 1$. Then, $D_n(1,x)$ is a CPP over $\mathbb{Z}_3$ if and only if $n \equiv 2, 6 \pmod 8$.
3. Let p be an odd prime. If $n = 2, 2p$, then $D_n(1,x)$ is a CPP of $\mathbb{F}_p$.
4. Let $p > 3$ be an odd prime. If $n = 3, 3p$, then $D_n(1,x)$ is a CPP of $\mathbb{F}_p$.
5. Let $p \equiv 1 \pmod{12}$. If $n = p + 1$, then $D_n(1,x)$ is a CPP of $\mathbb{F}_p$.
6. Let $p \equiv 5 \pmod{12}$. If $n = p + 1$, then $D_n(1,x)$ is not a CPP of $\mathbb{F}_p$.
7. Let $p \equiv 1 \pmod{12}$. If $n = p + 2$, then $D_n(1,x)$ is CPP of $\mathbb{F}_p$.
8. Let $p \equiv 7 \pmod{12}$. If $n = p + 2$, then $D_n(1,x)$ is not CPP of $\mathbb{F}_p$.
9. Since $D_{p+2}(1,x) = D_{2p+1}(1,x)$ for all $x \in \mathbb{F}_p$. We have the following:
   (a) Let $p \equiv 1 \pmod{12}$. If $n = 2p + 1$, then $D_n(1,x)$ is CPP of $\mathbb{F}_p$.
   (b) Let $p \equiv 7 \pmod{12}$. If $n = 2p + 1$, then $D_n(1,x)$ is not CPP of $\mathbb{F}_p$.
10. $E_n(1,x)$ is a CPP over $\mathbb{Z}_3$ if and only if $n \equiv 3, 15 \pmod{24}$.
11. The third reversed Dickson polynomial of the second kind $E_3(1,x)$ is a CPP for any $p \geq 3$ since $E_3(1,x) = 1 - 2x$ and $E_3(1,x) + x = 1 - x$ are both PPs of $\mathbb{F}_p$.

Conjectures

Conjecture 1 Let p be an odd prime and let $1 \leq n \leq p^2 - 1$. Then $D_n(1,x)$ is a CPP on $\mathbb{F}_p$ if and only if

$$n = \begin{cases} 2, 2p, 3, 3p, p+1, p+2, 2p+1 & \text{if } p \equiv 1 \pmod{12}, \\ 2, 2p, 3, 3p & \text{if } p \equiv 3 \pmod 4 \text{ or } p \equiv 5 \pmod{12}. \end{cases}$$

Conjecture 2 Let $p \geq 5$. Then, $E_n(1,x)$ is a CPP of $\mathbb{F}_p$ if and only if $n \equiv 3 \pmod{p(p^2-1)}$.

Applications in Cryptography

Check Digit System is a form of redundancy check used for error detection on identification numbers such as ISBN numbers.

ISBN 978-0-13-601970-1

9780136019701

A **single error** refers to an error in which only one digit of a number is incorrect.

$$\cdots a \cdots \to \cdots b \cdots$$

A **twin error** refers to when two adjacent digits were swapped.

$$\cdots aa \cdots \to \cdots bb \cdots$$

By mapping a set of input values through a **CPP**, we transform them into another set of values, then single errors or twin errors will map to different values, and these discrepancies can be detected when the transformed data is reversed.

Future Plans

We plan on studying self-reciprocal polynomials from Dickson Polynomials, which has many applications in the Coding Theory. Self-reciprocal polynomials are polynomials whose coefficients form a **palindrome**.

Definition

The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f(\frac{1}{x})$, i.e. if

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

then

$$f^*(x) = a_n + a_{n-1}x + a_{n-2}x^2 + \ldots + a_0x^n.$$

A polynomial $f(x)$ is called self-reciprocal if $f^*(x) = f(x)$, i.e. if $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, a_n \neq 0$, is self-reciprocal, then $a_i = a_{n-i}$ for $0 \leq i \leq n$.

Example $f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$

Acknowledgements

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