A Study of Polynomials $g_{n,p}$ and Their Applications in Cryptography

Zhiyan Jiang and Neranga Fernando
Department of Mathematics and Computer Science, College of the Holy Cross

Introduction

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

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

We study the algebraic properties of a family of polynomials defined by functional equations. Moreover, we investigate complete permutation polynomials defined by functional equations over finite fields $\mathbb{F}_p$.

Polynomial g

The nth polynomial $g_{n,p}$ is given by the explicit expression

$$g_{n,p}(x) = \sum_{\frac{n}{p} \le l \le \frac{n}{p-1}} \frac{n}{l} \binom{l}{n-l(p-1)} x^{n-l(p-1)} \quad \in \mathbb{Z}[x],$$

where n is the index of the polynomial. The recurrence relation of polynomial g_n is given by

$$g_{n,p} = 0, \text{ for } 0 \le n \le p-1, \;\; g_{p-1,p} = -1,$$

$$g_{n,p} = x g_{n-p,p} + g_{n-p+1,p}, \text{ for } n \ge p.$$

Permutation Polynomials

A polynomial $f \in \mathbb{F}_p[x]$ is called a *permutation polynomial* of $\mathbb{F}_p$ if the associated mapping $x \mapsto f(x)$ from $\mathbb{F}_p$ to $\mathbb{F}_p$ is a permutation of $\mathbb{F}_p$.

For example, consider the polynomial $h(x) = 2x+1$ over $\mathbb{F}_5$. If we evaluate the polynomial $h(x)$ at each value in $\mathbb{F}_5$, we get

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

Since $h(x)$ permutes every element of $\mathbb{F}_5$, $h(x)$ is a permutation polynomial (PP) over $\mathbb{F}_5$.

If both $f(x)$ and $f(x) + x$ are permutation polynomials over $\mathbb{F}_p$, then we call $f(x)$ a complete permutation polynomial over $\mathbb{F}_p$.

For instance, $h(x) + x = 3x + 1$ is a PP over $\mathbb{F}_5$. Thus, $h(x)$ is a *complete permutation polynomial* (CPP).

We study CPPs over finite fields arising from a particular family of polynomials: polynomial $g_{n,p}$. This family of polynomials was introduced by Xiang-dong Hou in 2012. **[?]**

$$g_{n,p} = \begin{cases} 0 & \text{if } w_q(n) < p \\ -1 & \text{if } w_p(n) = p \\ \alpha_0 x^{p^0} + (\alpha_0 + \alpha_1) x^{p^1} + \ldots + (\alpha_0 + \ldots + \alpha_{t-1}) x^{p^{t-1}} + \delta & \text{if } w_p(n) = p. \end{cases}$$

where

$$\delta = \begin{cases} 1 & \text{if } p = 2, \\ 0 & \text{if } p > 2. \end{cases}$$

New findings on patterns of polynomials

Inspired by [1, Theorem 3.3], we discovered a new formula that generates polynomial $g_{n,p}$ with $w_p(n) = p + m$, where m is a non-negative integer with no upper bound and $w_p(n)$ is the base p weight of n. Let k be a non-negative integer and $p > 3$.

$$g_{(m+2)p-1+k(p-1)}(x) = ((p-1) - S_k) x^{m+1},$$

where

$$S_k = \sum_{n=2}^{k+1} \binom{n+m-1}{m}.$$

We also discovered that this applies for cases of $w_q(n) = p^l + m$, where l is any positive integer, and we are currently exploring the use of this newly discovered generator to find new patterns of specific indices of the polynomial.

On Complete Permutation Polynomials

The polynomial $g_{p^2-2,p}$ is not a complete permutation polynomial. We have

$$g_{p^p-2,p} = (p-1) x^{p-2}.$$

Let $h(x) = g(x) + x$. Then we have

$$h(x) = \begin{cases} -x^{-1} + x & \text{if } x \in \mathbb{F}_p^*, \\ 0 & \text{if } x = 0. \end{cases}$$

Since $h(1) = 0$ and $h(0) = 0$, $h(x)$ is not a PP of $\mathbb{F}_p$. Therefore $g(x)$ is not a CPP.

Future plans on verifying Polynomials

The following table gives a list of indices of the CPPs generated by the polynomial $g_{n,p}$:

A	B	C	D	E	F	G	H	I	J	K
	3	5	7	9	11	13	15	17	19	23
2p-1	x+2	4x	6x		10x	12x		16x	18x	22x
2p+1	x	0	0		0	0		0	0	0
2p+2	2+2x^2	4	0		0	0		0	0	0
3p-1	2+2x^2	4x^2	6x^2	8x^2	10x^2	12x^2	14x^2	16x^2	18x^2	22x^2
3p+1	2	4	0	0	0	0		0	0	0
3p+2	x	2x	0		0	0		0	0	0
4p-1	x	4x^3	6x^3	8x^3	10x^3	12x^3		16x^3	18x^3	22x^3
4p+1	0	x	0		0	0		0	0	0
4p+2	2+x^2	4x^2	6		0	0		0	0	0
5p-1	2+x^2	4+4x^4	3x^2	8x^4	10x^4	12x^4	14x^4	16x^4	18x^4	22x^4
5p+1	2+x^2	0	6		0	0		0	0	0
5p+2	2x	0	2x		0	0		0	0	0
6p-1	2x	3x	6x^5		10x^5	12x^5		16x^5	18x^5	22x^5
6p+1	2x	0	x		0	0		0	0	0
6p+2	2+2x^2	4	6x^2	8	0	0		0	0	0
7p-1	2+2x^2	3x^2	6+6x^6	8x^6	10x^6	12x^6	14x^6	16x^6	...	...
7p+1	2+x^2	4	0	0	0					
7p+2	2x	x	0	2x	0					
8p-1	2x	3x^3	5x		10x^7		14x^7			
8p+1	2x	0	0		0					
8p+2	2+x^2	x^2	0		0					
9p-1	2+x^2	4+3x^4	5x^2	8+8x^8	10x^8			16x^8		
9p+1	2	x^2	2							
9p+2	0	4x^3	0							
10p-1										
10p+1										
10p+2										
11p-1					10+10x^10					

The indices follow the patterns $mp - 1$, $mp + 1$ and $mp + 2$, where $m \ge 2$ is an integer.

Some verification

Here are the generalizations of three polynomials derived from the table:

For $p \ge 3$, we have

$$g_{p^2-1} = (p-1) + (p-1) x^{p-1}.$$

For $p \ge 5$, we have

$$g_{kp-1} = (p-1) x^{\frac{p-1}{2}}, \text{ where } k = \tfrac{p+1}{2}.$$

For $p \ge 7$ such that $p \equiv 3 \pmod 4$,

$$g_{kp-1} = (p-1) x^{kp-2}, \text{ where } k = \tfrac{p+5}{4}.$$

Future Plans

In our growing needs of electric commerce and electric bookkeeping, it is evident that more accurate, more complicated verification tools should be developed to ensure the currency of the data and the accuracy of the data input, respectively. Using complete permutation polynomials is an effective way of verification:

- Mobile payment may use systems similar to the QR code system and ISBN system. Maintaining the code currency ensures no other people can use the screenshot of the payment page for their uses. The polynomial g can find a unique prime number to coordinate with every 5 second interval of the day in order to make every unique code.
- It is hard to find a complete polynomial generated at a large index– without a p shared by the two sides of the communication, finding the specific polynomial will cost considerably more time–we can impose a time limit on the operator's console to weed out the communications which, during access, excesses the time limit required to access each digit generated by elements within $\mathbb{F}_p$ into the polynomial.

Single-input errors and double-errors are commonplace errors one can make when inputting a series of digits. Having the digit checking system makes sure the end result confirms with the expectations. Moreover, we plan on investigating the applications of polynomial g in the area of Latin Squares, Elliptic Curve Cryptography, and the behaviour of the polynomial when $n < 0$.

Acknowledgements

We thank the Weiss Summer Science Research program for the support. We would also like to thank Dr. Dan Kennedy '68 for his generous donation to make this possible.

References

X. Hou, *A new approach to permutation polynomials over finite fields* **18** (2012), 492 – 521