Self-reciprocal polynomials arising from reversed Dickson polynomials

Neranga Fernando

Department of Mathematics
Northeastern University
Boston

AMS Fall Eastern Sectional Meeting
State University of New York at Buffalo, Buffalo, NY

September 17, 2017

Introduction

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

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

then

$$f^*(x) = a_n + a_{n-1} x + a_{n-2} x^2 + \cdots + a_0 x^n.$$

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

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

Example 2 Let $g(x) = 1 + 2x + 3x^2 + 3x^3 + 2x^4 + x^5$.

An application in coding theory

Let C be a code of length n over R, where R is either a ring or a field. Consider the codeword $c = (c_0, c_1, \ldots, c_{n-2}, c_{n-1})$ in C, and denote its reverse by c^r which is given by $c^r = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$.

If τ denotes the cyclic shift, then $\tau(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$. A code C is said to be a *cyclic code* if the cyclic shift of each codeword is also a codeword.

Example The code $C = \{000, 110, 101, 011\}$ is a cyclic code.

An application in coding theory (contd.)

The codeword

$$c = (c_0, c_1, \ldots, c_{n-1})$$

can be represented by the polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

The cyclic shifts of c correspond to the polynomials

$$x^i f(x) \pmod{x^n - 1} \text{ for } i = 0, 1, \ldots, n-1.$$

Example The codeword $v = 1101000$ can be represented by the polynomial $v(x) = 1 + x + x^3$. Here $n = 7$. Then the codeword 1000110 is represented by the polynomial

$$x^4 v(x) = x^4 + x^5 + x^7 \equiv 1 + x^4 + x^5 \pmod{1 + x^7}.$$

An application in coding theory (contd.)

Among all non-zero codewords in a cyclic code C, there is a unique codeword whose corresponding polynomial $g(x)$ has minimum degree and divides $x^n - 1$. The polynomial $g(x)$ is called the generator polynomial of the cyclic code C.

In 1964, James L. Massey studied reversible codes over finite fields and showed that the cyclic code generated by the monic polynomial $g(x)$ is reversible if and only if $g(x)$ is self-reciprocal.

J. L. Massey, *Reversible codes*, Information and Control **7** (1964), 369 – 380.

Background

Let p be a prime and q a power of p.

Let $\mathbb{F}_q$ be the finite field with q elements.

The n-th reversed Dickson polynomial of the first kind $D_n(a,x)$ is defined by

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

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

X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009), 748 – 773.

Background (contd.)

$$D_n(1,x) = \left(\frac{1}{2}\right)^{n-1} f_n(1-4x),$$

where

$$f_n(x) = \sum_{j\geq 0} \binom{n}{2j} x^j.$$

X. Hou, T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl. **16** (2010), 436 – 448.

Background (contd.)

The n-th reversed Dickson polynomial of the second kind $E_n(a, x)$ can be defined by

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

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

S. Hong, X. Qin, W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational*, Finite Fields Appl. **37** (2016), 54 – 71.

Background (contd.)

$$E_n(1, x) = \frac{1}{2^n} f_{n+1}(1 - 4x),$$

where

$$f_n(x) = \sum_{j \geq 0} \binom{n}{2j+1} x^j.$$

S. Hong, X. Qin, W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational*, Finite Fields Appl. **37** (2016), 54 – 71.

Background (contd.)

Reversed Dickson polynomials of the third kind $T_n(1,x)$ can be written explicitly as follows.

$$T_n(1,x) = \frac{1}{2^{n-1}} f_n(1-4x),$$

where

$$f_n(x) = \sum_{j\geq 0} \binom{n}{2j+1} x^j.$$

F., *Reversed Dickson polynomials of the third kind*. arXiv:1602.04545

Background (contd.)

For $a \in \mathbb{F}_q$, the n-th Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(x,a)$ is defined by

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

and $D_{0,k}(x,a) = 2-k$.

Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl. **18** (2012), 814 – 831.

Background (contd.)

For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

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

and $D_{0,k}(a,x) = 2-k$.

Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl. **18** (2012), 814 – 831.

Background (contd.)

When p is odd, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(1,x)$ can be written as

$$D_{n,k}(1,x) = \left(\frac{1}{2}\right)^n f_{n,k}(1-4x),$$

where

$$f_{n,k}(x) = k \sum_{j\geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j\geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x]$$

for $n \geq 1$ and

$$f_{0,k}(x) = 2-k.$$

F., *Reversed Dickson polynomials of the* $(k+1)$*-th kind over finite fields*, J. Number Theory **172** (2017), 234 – 255.

Self-reciprocal polynomials over $\mathbb{Z}$

Recall that for $n \geq 1$,

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x].$$

Theorem Let $n > 1$ be even. $f_{n,k}(x)$ is a self-reciprocal if and only if $k \in \{0, 2\}$.

Theorem Let $n > 1$ be odd. $f_{n,k}(x)$ is a self-reciprocal if and only if $k = 1$ or $n = 3$ when $k = 3$.

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Recall again that for $n \geq 1$,

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x].$$

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} x^j - k \sum_{j \geq 0} \binom{n-1}{2j+1} x^{j+1} + 2 \sum_{j \geq 0} \binom{n}{2j} x^j$$

Let n be even.

$$(k(n-1)+2) + \sum_{j=1}^{\frac{n}{2}-1} \left[k \binom{n-1}{2j+1} - k \binom{n-1}{2j-1} + 2 \binom{n}{2j} \right] x^j + (2-k)\, x^{\frac{n}{2}}.$$

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Replace the constant term by the coefficient of $x^{\frac{n}{2}}$ above and define $g_{n,k}$ to be

$$g_{n,k}(x) := (2-k) + \sum_{j=1}^{\frac{n}{2}-1} \left[k\binom{n-1}{2j+1} - k\binom{n-1}{2j-1} + 2\binom{n}{2j} \right] x^j + (2-k)\, x^{\frac{n}{2}}.$$

Also, replace the coefficient of $x^{\frac{n}{2}}$ by the constant term and define $h_{n,k}$ to be

$$h_{n,k}(x) := (k(n-1)+2) + \sum_{j=1}^{\frac{n}{2}-1} \left[k\binom{n-1}{2j+1} - k\binom{n-1}{2j-1} + 2\binom{n}{2j} \right] x^j + (k(n-1)+2)\, x^{\frac{n}{2}}$$

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Theorem Let $n > 1$ be even. $g_{n,k}$ and $h_{n,k}$ are self-reciprocal if and only if $k = 0$.

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Recall again that for $n \geq 1$,

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x].$$

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} x^j - k \sum_{j \geq 0} \binom{n-1}{2j+1} x^{j+1} + 2 \sum_{j \geq 0} \binom{n}{2j} x^j$$

Let n be odd.

$$(k(n-1)+2) + \sum_{j=1}^{\frac{n-1}{2}-1} \left[k \binom{n-1}{2j+1} - k \binom{n-1}{2j-1} + 2 \binom{n}{2j} \right] x^j + (-k(n-1)+2n)\, x^{\frac{n-1}{2}}.$$

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Replace the constant term by the coefficient of $x^{\frac{n-1}{2}}$ and define $g^*_{n,k}$ to be

$$g^*_{n,k}(x) := (-k(n-1)+2n) + \sum_{j=1}^{\frac{n-1}{2}-1} \left[k\binom{n-1}{2j+1} - k\binom{n-1}{2j-1} + 2\binom{n}{2j} \right] x^j + (-k(n-1)+2n)\, x^{\frac{n-1}{2}}.$$

Also, replace the coefficient of $x^{\frac{n-1}{2}}$ by the constant term and define $h^*_{n,k}$ to be

$$h^*_{n,k}(x) := (k(n-1)+2) + \sum_{j=1}^{\frac{n-1}{2}-1} \left[k\binom{n-1}{2j+1} - k\binom{n-1}{2j-1} + 2\binom{n}{2j} \right] x^j + (k(n-1)+2)$$

Self-reciprocal polynomials over $\mathbb{Z}$ (contd.)

Theorem Let $n > 1$ be odd. $g^*_{n,k}$ and $h^*_{n,k}$ are self-reciprocal if and only if $k = 1$

Self-reciprocal polynomials in odd characteristic

Let $n > 1$, p be an odd prime, and $0 \leq k \leq p-1$. Consider

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{F}_p[x].$$

Theorem Assume that n is even. Then $f_{n,k}(x)$ is a self-reciprocal if and only if one of the following holds:

(i) $k = 0$.

(ii) $k = 2$ and $n \neq (2\ell)p$, where $\ell \in \mathbb{Z}^+$.

Self-reciprocal polynomials in odd characteristic (contd.)

Let $n > 1$, p be an odd prime, and $0 \leq k \leq p-1$. Consider

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{F}_p[x].$$

Theorem Assume that $n > 0$ is odd. Then $f_{n,k}(x)$ is a self-reciprocal if and only if one of the following holds:

(i) $n = 1$ for any k.

(ii) $k = 0$ and $n = p^{\ell}$, where $\ell \in \mathbb{Z}^+$.

(iii) $n = 3$ and $k = 3$ when $p > 3$.

(iv) $k = 1$ and $n + 1 \neq (2\ell)p$, where $\ell \in \mathbb{Z}^+$.

Self-reciprocal polynomials in odd characteristic (contd.)

Corollary If $k = 0$ and $n > 2$ with $n \equiv 2 \pmod 4$, then $f_{n,k}(x)$ is not an irreducible self-reciprocal polynomial.

Corollary If $k = 2$ and $n \neq (2\ell)p$ with $n \equiv 0 \pmod 4$, where $\ell \in \mathbb{Z}^+$, then $f_{n,k}(x)$ is not an irreducible self-reciprocal polynomial.

Corollary If $k = 1$ and $n + 1 \neq (2\ell)p$ with $n \equiv 3 \pmod 4$, where $\ell \in \mathbb{Z}^+$, then $f_{n,k}(x)$ is not an irreducible self-reciprocal polynomial.

In characteristic 2

Recall that for $n \geq 1$,

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x].$$

When $p = 2$, we have

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) \in \mathbb{F}_2[x].$$

Theorem Let $n > 1$ and $k = 1$. Then $f_{n,k}(x)$ is a self-reciprocal if and only if n is even.

Corollary If $n > 2$ with $n \equiv 2 \pmod 4$, then $f_{n,k}(x)$ is not an irreducible self-reciprocal polynomial.

Remark Note that when $n = 2$, $f_{n,k} = x + 1$ which is irreducible.

Coterm polynomials

Coterm polynomials were introduced by Oztas, Siap, and Yildiz in *Reversible codes and applications to DNA*, Lecture Notes in Comput. Sci., 8592, Springer, Heidelberg, 2014.

Let R be a commutative ring with identity.

Definition Let $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in R[x]/(x^n - 1)$ be a polynomial, with $a_i \in R$. If for all $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$, we have $a_i = a_{n-i}$, then $f(x)$ is said to be a coterm polynomial over R.

If $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_n \neq 0$, is a self-reciprocal polynomial, then the removal of the term a_nx^n from $f(x)$ gives a coterm polynomial.

Coterm Polynomials from reversed Dickson polynomials

$$f_{n,k}(x) = k \sum_{j\geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j\geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x].$$

Theorem Let $n \geq 4$ be even and define

$$C_{n,k}(x) := f_{n,k}(x) - 2x^{\frac{n}{2}} \quad \text{and} \quad G_{n,k}(x) := g_{n,k}(x) - 2x^{\frac{n}{2}},$$

where $g_{n,k}(x)$ is the polynomial defined in a previous slide. If $k = 0$, then $C_{n,k}(x)$ and $G_{n,k}(x)$ are coterm polynomials over $\mathbb{Z}$. Moreover, define

$$H_{n,k}(x) := f_{n,k}(x) - 2n\, x^{\frac{n}{2}-1} \quad \text{for } n \geq 6 \text{ even.}$$

If $k = 2$, then $H_{n,k}(x)$ is a coterm polynomial over $\mathbb{Z}$.

Coterm Polynomials from reversed Dickson polynomials (contd.)

Theorem Let $n > 3$ be odd. Define

$$C_{n,k}(x) := f_{n,k}(x) - (n+1)x^{\frac{n-1}{2}} \quad \text{and} \quad G^*_{n,k}(x) := g^*_{n,k}(x) - (n+1)x^{\frac{n-1}{2}},$$

where $g^*_{n,k}(x)$ is the polynomial defined in a previous slide. If $k = 1$, then $C_{n,k}(x)$ and $G^*_{n,k}(x)$ are coterm polynomials over $\mathbb{Z}$.

Let p be an odd prime.

Theorem Let $n \geq 4$ be even. Define

$$C_{n,k}(x) := f_{n,k}(x) - 2\,x^{\frac{n}{2}}.$$

If $k = 0$ and $w_p(n) \neq 2$, where $w_p(n)$ is the base p weight of n, then $C_{n,k}(x)$ is a coterm polynomial over $\mathbb{F}_p$.

Coterm Polynomials from reversed Dickson polynomials (contd.)

Theorem Let $n \geq 6$ be even. Define

$$C_{n,k}(x) := f_{n,k}(x) - 2n\, x^{\frac{n}{2}-1}.$$

If $k = 2$, $n \neq (2\ell_1)p$, where $\ell_1 \in \mathbb{Z}^+$, and $n \neq p^{\ell_2} + 1$, where $\ell_2 \in \mathbb{Z}^+$, then $C_{n,k}(x)$ is a coterm polynomial over $\mathbb{F}_p$.

Theorem Let $n > 3$ be odd. Define

$$C_{n,k}(x) := f_{n,k}(x) - (n+1)x^{\frac{n-1}{2}}.$$

If $k = 1$, $n + 1 \neq (2\ell_1)p$, where $\ell_1 \in \mathbb{Z}^+$, and $n \neq p^{\ell_2}$, where $\ell_2 \in \mathbb{Z}^+$, then $C_{n,k}(x)$ is a coterm polynomial over $\mathbb{F}_p$.

Remark In characteristic 2, $f_{n,k}(x) - x^{\frac{n}{2}}$ is a coterm polynomial over $\mathbb{F}_2$ if $n \geq 4$ is even and $n \neq 2^{\ell}$, where $\ell \in \mathbb{Z}^+$.

For further details

F., *Self-reciprocal polynomials and coterm polynomials*. arXiv:1606.07750

Acknowledgement

- Sartaj Ul Hasan at Defence Research and Development Organisation, Delhi, India.
- Boris Tsvelikhovsky at Northeastern University.

Thank you!