Self-reciprocal polynomials and reversed Dickson polynomials

Neranga Fernando

Department of Mathematics
Rose–Hulman Institute of Technology
Terre Haute, Indiana

May 6, 2021

Outline of the talk

1. Background

Outline of the talk

1. Background
2. Self-reciprocal polynomials

Outline of the talk

Outline of the talk

Outline of the talk

1. Background
2. Self-reciprocal polynomials
   - 2.1 Introduction
   - 2.2 Definition of a self-reciprocal polynomial
   - 2.3 An introduction to coding theory

Outline of the talk

1. Background
2. Self-reciprocal polynomials
   2.1 Introduction
   2.2 Definition of a self-reciprocal polynomial
   2.3 An introduction to coding theory
   2.4 Cyclic codes

Outline of the talk

Outline of the talk

Outline of the talk

1. Background
2. Self-reciprocal polynomials
   2.1 Introduction
   2.2 Definition of a self-reciprocal polynomial
   2.3 An introduction to coding theory
   2.4 Cyclic codes
   2.5 An application of self-reciprocal polynomials in coding theory
   2.6 Self-reciprocal polynomials over $\mathbb{Z}$
   2.7 Self-reciprocal polynomials in odd characteristic

Outline of the talk

1. Background
2. Self-reciprocal polynomials
   2.1 Introduction
   2.2 Definition of a self-reciprocal polynomial
   2.3 An introduction to coding theory
   2.4 Cyclic codes
   2.5 An application of self-reciprocal polynomials in coding theory
   2.6 Self-reciprocal polynomials over $\mathbb{Z}$
   2.7 Self-reciprocal polynomials in odd characteristic
   2.8 Self-reciprocal polynomials in even characteristic

Outline of the talk

Background

Let p be a prime, q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements.

Background

Let p be a prime, q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements.

Dickson polynomials

Background

Let p be a prime, q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements.

Dickson polynomials

Leonard Eugene Dickson (1897)

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

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

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

Background (contd.)

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**, 748 – 773, (2009).

Background (contd.)

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

Background (contd.)

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

where

$$f_n(x) = \sum_{j \geq 0} \binom{n}{2j} x^j \ \in \mathbb{Z}[x].$$

Background (contd.)

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

where

$$f_n(x) = \sum_{j\geq 0} \binom{n}{2j} x^j \ \in \mathbb{Z}[x].$$

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

Background (contd.)

Schur (1923)

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

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

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

Background (contd.)

The n-th reversed Dickson polynomial of the second kind $E_n(x, a)$ 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, 54 –71 (2016).

Background (contd.)

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

Background (contd.)

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

where

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

Background (contd.)

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

where

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

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

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.)

Reversed Dickson Polynomials of the $(k+1)$-th kind

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

Background (contd.)

Reversed Dickson Polynomials of the $(k+1)$-th kind

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

- $D_{n,0}(a,x) = D_n(a,x)$ and $D_{n,1}(a,x) = E_n(a,x)$.

Background (contd.)

Reversed Dickson Polynomials of the $(k+1)$-th kind

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

- $D_{n,0}(a,x) = D_n(a,x)$ and $D_{n,1}(a,x) = E_n(a,x)$.
- Only need to consider $0 \leq k \leq p-1$ in characteristic p.

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

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

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

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

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

Introduction

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

Introduction

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

- Its coefficients form a palindrome.

Introduction

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

- Its coefficients form a palindrome.
- Such polynomials are called self-reciprocal polynomials.

Introduction

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

- Its coefficients form a palindrome.
- Such polynomials are called self-reciprocal polynomials.

Question: How can we define self-reciprocal polynomials?

Introduction (contd.)

Let's consider a different polynomial.

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

Introduction (contd.)

Let's consider a different polynomial.

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

- The degree of the polynomial $f(x)$ is 4.

Introduction (contd.)

Let's consider a different polynomial.

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

- The degree of the polynomial $f(x)$ is 4.
- $f\left(\frac{1}{x}\right) = 1 + \frac{2}{x} + \frac{3}{x^2} + \frac{2}{x^3} + \frac{1}{x^4}.$

Introduction (contd.)

Let's consider a different polynomial.

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

- The degree of the polynomial $f(x)$ is 4.
- $f\left(\frac{1}{x}\right) = 1 + \frac{2}{x} + \frac{3}{x^2} + \frac{2}{x^3} + \frac{1}{x^4}$.
- Multiply $f(\frac{1}{x})$ by $x^{\deg(f)}$, i.e. x^4, to obtain

$$x^4 f\left(\frac{1}{x}\right) = x^4 + 2x^3 + 3x^2 + 2x + 1.$$

Introduction (contd.)

Let's consider a different polynomial.

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

- The degree of the polynomial $f(x)$ is 4.
- $f\left(\frac{1}{x}\right) = 1 + \frac{2}{x} + \frac{3}{x^2} + \frac{2}{x^3} + \frac{1}{x^4}$.
- Multiply $f(\frac{1}{x})$ by $x^{\deg(f)}$, i.e. x^4, to obtain

$$x^4 f\left(\frac{1}{x}\right) = x^4 + 2x^3 + 3x^2 + 2x + 1.$$

- The polynomial $x^{\deg(f)}\, f(\frac{1}{x})$ is called the reciprocal of $f(x)$ and we denote it by $f^*(x)$.

Introduction (contd.)

Let's consider a different polynomial.

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

- The degree of the polynomial $f(x)$ is 4.
- $f\left(\frac{1}{x}\right) = 1 + \frac{2}{x} + \frac{3}{x^2} + \frac{2}{x^3} + \frac{1}{x^4}$.
- Multiply $f(\frac{1}{x})$ by $x^{\deg(f)}$, i.e. x^4, to obtain

$$x^4 f\left(\frac{1}{x}\right) = x^4 + 2x^3 + 3x^2 + 2x + 1.$$

- The polynomial $x^{\deg(f)}\, f(\frac{1}{x})$ is called the reciprocal of $f(x)$ and we denote it by $f^*(x)$. Note that $f(x) = x^{\deg(f)}\, f(\frac{1}{x})$.

Definition of a self-reciprocal polynomial

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

Definition of a self-reciprocal polynomial

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

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

Definition of a self-reciprocal polynomial

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

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

Definition of a self-reciprocal polynomial

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 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_n \neq 0$, is self-reciprocal, then $a_i = a_{n-i}$ for $0 \leq i \leq n$.

Coding Theory

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another.

Information Source $\rightarrow$ **Encoder** $\rightarrow$ **Channel (Noise)** $\rightarrow$ **Decoder** $\rightarrow$ **Information Sink**

Coding Theory (contd.)

• The information to be sent is transmitted by a sequence of zeros and ones which are called digits.

Coding Theory (contd.)

- The information to be sent is transmitted by a sequence of zeros and ones which are called digits.
- A *word* is a sequence of digits.

Coding Theory (contd.)

- The information to be sent is transmitted by a sequence of zeros and ones which are called digits.
- A *word* is a sequence of digits.
- The *length* of a word is the number of digits in the word.

Coding Theory (contd.)

• The information to be sent is transmitted by a sequence of zeros and ones which are called digits.

• A *word* is a sequence of digits.

• The *length* of a word is the number of digits in the word.

Example 0110101 is a word of length seven.

Coding Theory (contd.)

• A *binary code* is a set C of words. The term “binary” refers to the fact that only two digits, 0 and 1, are used, i.e. the digits are elements of $\mathbb{Z}_2$.

Coding Theory (contd.)

• A *binary code* is a set C of words. The term "binary" refers to the fact that only two digits, 0 and 1, are used, i.e. the digits are elements of $\mathbb{Z}_2$.

• The code consisting of all words of length two is

$$C = \{00, 10, 01, 11\}.$$

Coding Theory (contd.)

• A *binary code* is a set C of words. The term "binary" refers to the fact that only two digits, 0 and 1, are used, i.e. the digits are elements of $\mathbb{Z}_2$.

• The code consisting of all words of length two is

$$C = \{00, 10, 01, 11\}.$$

• A *block code* is a code having all its words of the same length; this number is called the *length* of a code.

Coding Theory (contd.)

Let C be a block code of length n. 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 $c^r = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$.

Coding Theory (contd.)

Let C be a block code of length n. 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 $c^r = (c_{n-1}, c_{n-2}, \ldots, c_1, c_0)$.

Example The reverse of the codeword 0110101 is 1010110.

Cyclic Codes

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

Cyclic Codes

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

Cyclic Codes (contd.)

The codeword

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

can be represented by the polynomial

Cyclic Codes (contd.)

The codeword

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

can be represented by the polynomial

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

Cyclic Codes (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

Cyclic Codes (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

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

Cyclic Codes (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 $v(x) = 1 + x + x^3$.

Cyclic Codes (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 $n = 7$.

Cyclic Codes (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

Cyclic Codes (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

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

An application of self-reciprocal polynomials in coding theory

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.

An application of self-reciprocal polynomials in coding theory

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.

Recall $f_{n,k}(x)$

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

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

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

For $n \geq 1$, we have

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

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

For $n \geq 1$, we have

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

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

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

For $n \geq 1$, we have

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

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 $n \geq 1$,

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

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

Recall again that for $n \geq 1$,

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

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

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

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

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 $n \geq 1$,

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

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

Recall again that for $n \geq 1$,

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

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

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

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

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 $0 \le k \le p-1$. Consider

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

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 $\ell \in \mathbb{Z}^+$.

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.

Thank you!