Self-reciprocal Polynomials Over Finite Fields

by

Helmut Meyn[1] and Werner Götz[1]

Abstract. The *reciprocal* $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f(1/x)$. A polynomial is called *self-reciprocal* if it coincides with its reciprocal.

The aim of this paper is threefold: first we want to call attention to the fact that the product of all self-reciprocal irreducible monic (*srim*) polynomials of a fixed degree has structural properties which are very similar to those of the product of all irreducible monic polynomials of a fixed degree over a finite field $\mathbb{F}_q$. In particular, we find the number of all srim-polynomials of fixed degree by a simple Möbius-inversion.

The second and central point is a short proof of a criterion for the irreducibility of self-reciprocal polynomials over $\mathbb{F}_2$, as given by Varshamov and Garakov in [10]. Any polynomial f of degree n may be transformed into the self-reciprocal polynomial f^Q of degree $2n$ given by $f^Q(x) := x^n f(x + x^{-1})$. The criterion states that the self-reciprocal polynomial f^Q is irreducible if and only if the irreducible polynomial f satisfies $f'(0) = 1$.

Finally we present some results on the distribution of the traces of elements in a finite field. These results were obtained during an earlier attempt to prove the criterion cited above and are of some independent interest.

For further results on self-reciprocal polynomials see the notes of chapter 3, p. 132 in Lidl/Niederreiter [5].

1 The rôle of the polynomial $x^{q^n+1} - 1$

Some remarks on self-reciprocal polynomials are in order before we can state the main theorem of this section.

- If f is self-reciprocal then the set of roots of f is closed under the inversion map $\alpha \mapsto \alpha^{-1} \qquad (\alpha \neq 0)$.

[1]Universität Erlangen-Nürnberg, Informatik I, Martensstr. 3, D-91058 Erlangen

- If $f \in \mathbb{F}_q[x]$ is irreducible and if the set of roots of f is closed under inversion, then
$$f^*(x) = \begin{cases} -f(x) & \text{if } f(x) = x - 1 \wedge q \neq 2 \\ f(x) & \text{otherwise} \end{cases}$$
.

- If f is self-reciprocal and $f(-1) \neq 0$ then f has even degree.

As a consequence, self-reciprocal irreducible polynomials have even degree with the only exception of $f(x) = x + 1$. The following theorem provides the means for finding the product of all srim-polynomials of fixed degree:
Theorem 1

i) *Each srim-polynomial of degree* $2n \quad (n \geq 1)$ *over* $\mathbb{F}_q$ *is a factor of the polynomial*
$$H_{q,n}(x) := x^{q^n+1} - 1 \in \mathbb{F}_q[x].$$

ii) *Each irreducible factor of degree* ≥ 2 *of* $H_{q,n}(x)$ *is a srim-polynomial of degree* $2d$*, where* d *divides* n *such that* n/d *is odd.*

Proof:

i) If f is srim of degree $2n$ then $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{2n-1}}\}$ is the set of roots of f in $\mathbb{F}_{q^{2n}}$. Because this set is closed under inversion we have
$$\exists! j \in [0, 2n-1] : \alpha^{q^j} = \alpha^{-1}$$
which means that α is a root of $H_{q,j}$. Obviously $H_{q,j}(x) \mid x^{q^{2j}-1} - 1$. On the other hand $f(x) \mid x^{q^{2n}-1} - 1$, so that $2n \mid 2j$. It follows that $j = n$.

ii) Let g be an irreducible factor of degree ≥ 2 of $H_{q,n}$. As a consequence, a root α of g satisfies $\alpha^{q^n} = \alpha^{-1}$, i.e. the set of roots of g is closed under inversion. From this we know that g is self-reciprocal of even degree $2d$, say. By the arguments given in i) it follows that $2d$ divides $2n$ and g is both a factor of $H_{q,d}$ and $H_{q,n}$. The gcd of these polynomials is $x^{\gcd(q^n+1, q^d+1)} - 1$. It follows that n/d is odd. ⊠

If we define $R_{q,n}(x)$ as the product of all srim-polynomials of degree $2n$ $(n \geq 1)$ over $\mathbb{F}_q$ then Theorem 1 takes the form:
$$H_{q,n}(x) = (x^{1+e_q} - 1) \prod_{\substack{d \mid n \\ n/d \text{ odd}}} R_{q,d}(x) \tag{1}$$

where $e_q \equiv q \bmod 2$, i.e. $x^{1+e_q}-1$ collects the single linear factor $x+1$ if q is even resp. the two linear factors $(x+1)(x-1)$ if q is odd.
If we further use the 'normalization'

$$H^0_{q,n}(x) := H_{q,n}(x)/(x^{1+e_q}-1)$$

then we can invert the product-formula (1) by Möbius-inversion to get

Lemma 2 *The product $R_{q,n}(x)$ of all srim-polynomials of degree $2n$ satisfies*

$$R_{q,n}(x) = \prod_{\substack{d|n \\ d \,\mathrm{odd}}} H^0_{q,n/d}(x)^{\mu(d)} \tag{2}$$

Note that due to the fact that $\sum_{d|n}\mu(d) = 0$ for $n > 1$ the normalization is of concern only in the case $n = 2^s \quad (s \geq 0)$, i.e.

$$R_{q,n}(x) = \prod_{\substack{d|n \\ d \,\mathrm{odd}}} H_{q,n/d}(x)^{\mu(d)}, \quad \text{if n} \neq 2^{\text{s}} \quad (\text{s} \geq 0)$$

As a consequence of (2) we are able to count the number of srim-polynomials of fixed degree:

Theorem 3 *Let $S_q(n)$ denote the number of srim-polynomials of degree $2n$ over $\mathbb{F}_q$.*

$$S_q(n) = \begin{cases} \frac{1}{2n}(q^n-1) & \text{if } q \text{ is odd} \wedge n = 2^s \\ \\ \frac{1}{2n}\sum_{\substack{d|n \\ dodd}} \mu(d)\, q^{n/d} & \text{otherwise} \end{cases} \tag{3}$$

Remarks

- Carlitz determined the numbers $S_q(n)$ in his paper [2]. Our proof via Möbius-inversion avoids his lengthy calculations with L-series.
- Note the analogy of this procedure to the usual determination of the number of all irreducible polynomials of fixed degree n over $\mathbb{F}_q$:

  $$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)\, q^{n/d}$$

  (cf. Lidl/Niederreiter [5]). The rôle of $x^{q^n-1}-1$ in the case of irreducible polynomials is played by the polynomial $x^{q^n+1}-1$ in the case of self-reciprocal irreducible polynomials.

- As is well known (cf. Miller [9]), formula (3) has an interpretation as the number of all primitive self-complementary necklaces of length n in q colors - even if q is not a prime power. This is proved by means of de Brujin's method of counting.

2 Construction of irreducible self-reciprocal polynomials

In Galois theory it is occasionally useful to remark that for any self-reciprocal polynomial $f(x)$ of even degree $2n$, $x^{-n}f(x)$ is a polynomial $g(y)$ of degree n in $y := x + x^{-1}$. Proceeding in the reverse direction we use this substitution to construct self-reciprocal polynomials (cf. also Andrews [1], Carlitz [2] and Miller [9]).

Definition For $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_0 \neq 0 \neq a_n$ set

$$f^Q(x) := x^n f(x + x^{-1}) = \sum_{i=0}^{n} a_i (1 + x^2)^i x^{n-i}$$

The self-reciprocal polynomial f^Q of degree $2n$ has a simple behaviour with respect to reducibility:

Lemma 4 *If f is irreducible over $\mathbb{F}_q$ of degree $n > 1$ then* **either** *f^Q is a srim-polynomial of degree $2n$* **or** *f^Q is the product of a reciprocal pair of irreducible polynomials of degree n which are not self-reciprocal.*

Note: two polynomials g and h constitute a reciprocal pair if

$$\exists \gamma \in \mathbb{F}_q^* : g^*(x) = \gamma h(x)$$

Proof: If α is a root of f^Q then $\alpha + \alpha^{-1}$ is a root of f, by definition of f^Q. The irreducibility of f implies that $\alpha + \alpha^{-1}$ has degree n, i.e.

$$(\alpha + \alpha^{-1})^{q^n} = \alpha + \alpha^{-1} \qquad (n \text{ mimimal!}) \tag{4}$$

This is equivalent to $(\alpha^{q^n+1} - 1)(\alpha^{q^n-1} - 1) = 0$. So, **either** $(\alpha^{q^n+1} - 1) = 0$, which by Theorem 1 means that f^Q is irreducible. **Or** $(\alpha^{q^n-1} - 1) = 0$, which means that each irreducible factor of f^Q is of degree n. If such a factor would be srim (which would be possible only in case n even) then $\alpha^{q^{n/2}+1} - 1 = 0$ would contradict to the minimality of n in (4). ⊠

This property of the transformation $f \mapsto f^Q$ can be put in a different way:

- If $n > 1$ then

$$I_{q,n}^{Q}(x) = \frac{R_{q,n}(x) I_{q,n}(x)}{R_{q,n/2}(x)}$$

  where $R_{q,n/2}(x) = 1$ if n is odd and $I_{q,n}(x)$ denotes the product of all irreducible monic polynomials of degree n over $\mathbb{F}_q$.

- Furthermore, this relation allows a different way to deduce the formula in Theorem 3 for the number of srim-polynomials.

For the proofs of these two remarks cf. Götz [3].
It is natural to ask for conditions for the coefficients of f which guarantee that f^Q is irreducible. In the case of the smallest field ($q = 2$) Varshamov and Garakov [10] gave the following answer:
Theorem 5 *Let f be an irreducible polynomial over $\mathbb{F}_2$. Then f^Q is irreducible if and only if $f'(0) = 1$, i.e. the linear coefficient of f is 1.*
Proof: Let α be a root of f^Q; then $\beta := \alpha + \alpha^{-1}$ is a root of f. β has degree n over $\mathbb{F}_2$, because f is irreducible by assumption. On the other hand, α is a root of g, where

$$g(x) := x^2 - \beta x + 1 \in \mathbb{F}_{2^n}[x]. \tag{5}$$

The status of quadratic equations in characteristic 2 is well known
(cf. MacWilliams and Sloane [6], p. 277):
The polynomial $Ax^2 + Bx + C = 0$ has

- one solution in case $B = 0$
- no solution in case $B \neq 0 \wedge Tr(\frac{AC}{B^2}) = 1$
- two solutions in case $B \neq 0 \wedge Tr(\frac{AC}{B^2}) = 0$

Define $Tr(\frac{AC}{B^2})$ as the *discriminant* of the polynomial $Ax^2 + Bx + C = 0$.Then the discriminant of $g(x)$ is $Tr(\beta^{-2})$. Because Tr is the absolute trace, $Tr(\beta^{-2}) = Tr(\beta^{-1})$. But $Tr(\beta^{-1}) = 1$ means that the second highest coefficient in $f^*(x)$ is one. This is equivalent to $f'(0) = 1$. ⊠
Remark In their paper [10] Varshamov and Garakov assert on p. 409 that "almost" all of their results could be generalized to higher characteristics. Our proof of their criterion shows, that the crucial condition is the irreducibility of g in equation (5). Exactly this equation is also the starting point of Carlitz's counting arguments. How the irreducibility of g can be expressed in terms of the coefficients of f is by no means obvious. The condition $\beta^2 - 4 \notin \mathbb{F}_q^2$ (q odd) has to be investigated.

3 Trace-Polynomials over $\mathbb{F}_q$.

In their proof of Theorem 5 Varshamov and Garakov in [10] perform some calculations with polynomials which – in a first attempt to simplify their proof – led us to the following considerations.

Definition

i) For $\delta \in \mathbb{F}_q$ the *trace-polynomials* are defined by

$$T_{q,n}(x,\delta) := \begin{cases} \delta & \text{if } n = 0 \\ \delta + \sum_{i=0}^{n-1} x^{q^i} & \text{if } n > 0 \end{cases}$$

ii) $F_{q,n}(x,\delta)$ denotes the product of all irreducible monic polynomials of degree n over $\mathbb{F}_q$, which have their second-highest coefficient equal to δ.

Observation Obviously, we have the relation $F_{q,n}(x,\delta) \mid T_{q,n}(x,\delta)$.

The next lemma gives the structure of $T_{q,n}(x,\delta)$:

Lemma 6 *If $q = p^s$ is a prime power and $\delta \in \mathbb{F}_q$, then the trace-polynomials satisfy*

$$T_{q,n}(x,\delta) = \prod \left\{ F_{q,d}(x,\gamma) \; ; \; d \mid n \; , \; \gamma \in \mathbb{F}_q \; , \; \frac{n}{d} \cdot \gamma = \delta \; (\mathrm{mod} p) \right\}$$

Proof:

" $\supset$ " if f has the form $f(x) = x^d + \gamma x^{d-1} + \ldots$ and α is a root of f in $\mathbb{F}_{q^d}$ then by the transitivity of the trace:

$$\begin{aligned} Tr_1^n(\alpha) &= Tr_1^d(Tr_d^n(\alpha)) \\ &= Tr_1^d(\frac{n}{d}\alpha) = \frac{n}{d} \cdot (-\gamma) = -\delta \; (\mathrm{mod} p) \end{aligned}$$

" $\subset$ " if $g(x) \mid T_{q,n}(x,\delta)$ and g is irreducible of degree d, then d is a divisor of n because $(T_{q,n}(x,\delta))^q - T_{q,n}(x,\delta) = x^{q^n} - x$. For a root α of g define $\gamma := -Tr_1^d(\alpha)$ and so $g(x)$ is a factor of $F_{q,d}(x,\gamma)$. ⊠

By another application of the Möbius-inversion we find

Theorem 7

$$F_{q,n}(x,0) = \prod_{d|n} T_{q,n/d}(x,0)^{\mu(d)} \qquad \text{if } p \nmid n$$

$$F_{q,n}(x,0) = \prod_{d|n \,\wedge\, p \not| d} \left(T_{q,n/d}(x,0) \;/\; (x^{q^{n/pd}} - x)\right)^{\mu(d)} \qquad \text{if } p \mid n$$

$$F_{q,n}(x,\delta) = \prod_{d|n \,\wedge\, p \not| d} \left(T_{q,n/d}(x, d^{-1}(\mathrm{mod} p) \cdot \delta\right)^{\mu(d)} \qquad \text{if } \delta \neq 0$$

Remarks

- By combining Theorem 7 and Theorem 1, and with the help of a result which is valid for $\mathbb{F}_2$ only, Götz [3] has given an alternative proof of Theorem 5.
- For the case $q = 2$ and $\delta = 1$ Theorem 7 gives the remarkable information that over $\mathbb{F}_2$ there are exactly as many srim-polynomials of degree $2n$ as there are irreducible monic polynomials of degree n with linear coefficient equal to 1 (by taking reciprocals). Theorem 5 provides an explicit bijection between these two sets of polynomials.

Note added in proof [2]

The case of odd characteristic was solved in [8]. The results were presented in [4], § 2.7 and the proofs were further simplified in [7], § 3.3.

References

[1] G.E. Andrews
Reciprocal Polynomials and Quadratic Transformations
Utilitas Mathematica 28, (1985)

[2] L. Carlitz
Some Theorems on Irreducible Reciprocal Polynomials Over a Finite Field
J. reine angew. Math. 227 (1967), 212-220

[3] W. Götz
Selbstreziproke Polynome über endlichen Körpern
Diploma thesis, Erlangen, 1989

[2] for the electronic version

[4] D. Jungnickel
Finite Fields
Bibliographisches Institut, Mannheim, 1993

[5] R. Lidl / H. Niederreiter
Finite Fields
Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Mass., 1983

[6] F.J. MacWilliams / N.J.A. Sloane
The Theory of Error-Correcting Codes
North-Holland, Amsterdam, 1977

[7] A.J.Menezes (*Ed.*)
Applications of Finite Fields
Kluwer Academic, Boston, 1993

[8] H. Meyn
On the Construction of Irreducible Self-reciprocal Polynomials over Finite Fields
AAECC 1 (1990), 43-53

[9] R.L. Miller
Necklaces, Symmetries and Self-Reciprocal Polynomials
Discrete Mathematics 22 (1978), 25-33

[10] R.R. Varshamov / G.A. Garakov
On the Theory of Selfdual Polynomials over a Galois Field (Russian)
Bull. Math. Soc. Sci. Math. R.S. Roumanie, (N.S.), 13 (1969), 403-415