AAECC 1, 43–53 (1990)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

On the Construction of Irreducible Self-Reciprocal Polynomials Over Finite Fields

Helmut Meyn
I.M.M.D., Informatik 1, Universität Erlangen-Nürnberg, Martensstraße 3, D-8520 Erlangen, FRG

Abstract. The transformation $f(x) \mapsto f^Q(x) := x^{\deg(f)} f(x + 1/x)$ for $f(x) \in \mathbb{F}_q[x]$ is studied. Simple criteria are given for the case that the irreducibility of f is inherited by the self-reciprocal polynomial f^Q. Infinite sequences of irreducible self-reciprocal polynomials are constructed by iteration of this Q-transformation.

Keywords: Polynomials, Self-reciprocal, Finite fields, Quadratic transformations

1. Introduction

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.

Self-reciprocal polynomials over finite fields are used to generate reversible codes with a read-backward property (J. L. Massey [13], S. J. Hong and D. C. Bossen [10], A. M. Patel and S. J. Hong [15]). The fact that self-reciprocal polynomials are given by specifying only half of their coefficients is of importance (E. R. Berlekamp [2]). Also, there is an intimate connection between irreducible self-reciprocal polynomials over $\mathbb{F}_q$ and the class of primitive self-complementary necklaces consisting of beads coloured with q colours (R. L. Miller [14] and the references given there). The numbers of these polynomials are at the same time the numbers of certain symmetry types of periodic sequences (E. N. Gilbert and J. Riordan [8]). Furthermore, we demonstrate how self-reciprocal irreducible polynomials can be used to construct certain infinite subfields $GF(q^{n \cdot 2^\infty})$ of the algebraic closure of $\mathbb{F}_q$.

Every self-reciprocal *irreducible* polynomial of degree $n \geqq 2$ has even degree. On the other hand any polynomial f of degree n may be transformed into a self-reciprocal polynomial f^Q of degree $2n$ given by $f^Q(x) = x^n f(x + 1/x)$. It is natural to ask under which conditions the irreducibility of f is inherited by f^Q.

For the smallest field $\mathbb{F}_2$, R. R. Varshamov and G. A. Garakov [16] gave the following answer:

If $f \in \mathbb{F}_2[x]$ is irreducible then f^Q is irreducible if and only if
the linear coefficient of f is one, i.e. $f'(0) = 1$.

This means in particular that the number of self-reciprocal irreducible monic (*srim*) polynomials of degree $2n$ ($n \geqq 1$) over $\mathbb{F}_2$ is equal to the number of irreducible monic polynomials of degree n with linear coefficient equal to 1. The method of proof in [16], however, does not suggest what criterion might look like an appropriate generalization to the case of any larger field $\mathbb{F}_q$.

In this paper we show how a different approach leads to a simple proof of their result and allows a generalization to any even or odd q. Due to the quadratic nature of the transformation $f \mapsto f^Q$ the conditions for f depend for even q on the trace function and for odd q on quadratic residues in $\mathbb{F}_q^*$.

The second section introduces the subject of *srim* polynomials in greater detail. We want to call attention to the fact that the product of all *sirm* polynomials of fixed degree has structural properties very similar to those of the product of all irreducible monic polynomials 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 third section presents the generalization, mentioned above, of the criterion of Varshamov and Garakov. Note that in general the conditions to be exploited cannot be read off as easily from the sequence of coefficients of f as in the case with $\mathbb{F}_2$. The final section shows how infinite sequences of *srim* polynomials can be defined in principle. In the case of characteristic 2 a simple criterion allows the construction of such sequences. Concerning fields of odd order, however, our discussion is incomplete due to a number of number-theoretic questions which we have not settled.

2. The Role 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
$$\alpha \mapsto \alpha^{-1} \ (\alpha \neq 0).$$
- If $f \in \mathbb{F}_q[x]$ is irreducible and if the set of roots of f is closed under inversion, then
$$f^*(x) = \begin{cases} -f(x) & \text{if} \quad f(x) = x - 1 \wedge q \neq 2 \\ f(x) & \text{otherwise.} \end{cases}$$
- 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 single 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* $2n$ ($n \geqq 1$) *over* $\mathbb{F}_q$ *is a factor of the polynomial*
$$H_{q,n}(x) := x^{q^n+1} - 1.$$

ii) *Each irreducible factor of degree* $\geqq 2$ *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 $H_{q,j}(x) | x^{q^{2j}-1} - 1$. On the other hand $f(x) | x^{q^{2n}-1} - 1$, so that $2n | 2j$. It follows that $j = n$.

ii) Let g be an irreducible factor of degree $\geqq 2$ 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 a factor of $H_{q,d}$. Because of $H_{q,d} | H_{q,n}$ we have $q^d + 1 | q^n + 1$, which is possible only in the case when n/d is odd. □

If we define $R_{q,n}(x)$ as the product of all *srim* polynomials of degree $2n$ ($n \geqq 1$) over $\mathbb{F}_q$ then Theorem 1 takes the form:

$$H_{q,n}(x) = (x^{1+e_q} - 1) \prod_{\substack{d|n \\ n/d \text{ odd}}} R_{q,d}(x) \tag{1}$$

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*

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

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 $n = 2^s$ ($s \geqq 0$), i.e.

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

Example. By Eq. (2) the product $R_{4,2}(x)$ of all *srim* polynomials of degree 4 over $\mathbb{F}_4$ is equal to $(x^{17} + 1)/(x + 1)$. A complete factorization of this polynomial over $\mathbb{F}_4$ gives the four *srim* polynomials of degree 4: $x^4 + \omega x^3 + x^2 + \omega x + 1$; $x^4 + \omega^2 x^3 + x^2 + \omega^2 x + 1$; $x^4 + x^3 + \omega x^2 + x + 1$; $x^4 + x^3 + \omega^2 x^2 + x + 1$. Here ω denotes a primitive element of $\mathbb{F}_4 : \omega + \omega^2 = 1$.

Making use 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 $\mathbb{F}_q$.*

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

Remarks

- Note the analogy of this procedure to the usual determination of the number $N_q(n)$ of all irreducible monic polynomials of fixed degree n over $\mathbb{F}_q$:

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

(Lidl/Niederreiter [11]). The role 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.

- Carlitz determined the numbers $S_q(n)$ in his paper [4]. In [5] Cohen gave a simplified proof of Theorem 3 avoiding the distinction between even and odd q. The treatment of self-reciprocal polynomials in Cohen [6] is very similar to that given here.

- As is well known (Miller [14]), Eq. (3) has an interpretation as the number of all primitive self-complementary necklaces of length n in q colours – this holds even if q is not a prime power. This is proved by means of de Brujin's method of counting.

- For further references to the literature on self-reciprocal polynomials see the notes of Chap. 3, p. 132 in Lidl/Niederreiter [11].

3. Construction of Irreducible Self-Reciprocal Polynomials

In Galois theory it is occasionally useful to remark that for any self-reciprocal $f(x)$ of even degree $2n$, $x^{-n}f(x)$ is a polynomial $g(y)$ of degree n in $y := x + 1/x$. Proceeding in the reverse direction we use this quadratic transformation to construct self-reciprocal polynomials (Carlitz [4], Miller [14], Andrews [1], and Cohen [6]).

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

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

Remark. The coefficients of f can be retrieved uniquely from the coefficients of f^Q by an inversion formula (Andrews [1]).

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 $\alpha + 1/\alpha$ is a root of f, by definition of f^Q. The irreducibility of f implies that $\alpha + 1/\alpha$ has degree n, i.e.

$$(\alpha + 1/\alpha)^{q^n} = \alpha + 1/\alpha \quad (n \text{ minimal!}). \tag{4}$$

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 the minimality of n in (4). □

Remark. Garbe introduced in [7] the *level* of a polynomial f which was subsequently identified by Cohen [6] as the order of f^Q. The question if there are polynomials of maximum order and maximum level was answered by Cohen in [6]: For fields of *even* order q and every n there is a primitive polynomial f of degree n over $\mathbb{F}_q$ such that f^Q is irreducible of order $q^n + 1$ and there is a primitive polynomial f of degree n such that f^Q factorizes as a product of two primitive polynomials.

The property of the transformation $f \mapsto f^Q$ as stated in Lemma 4 can be put in a different way:

- If $n > 1$ then

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

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

- Furthermore, this relation allows a different way to deduce the formula in Theorem 3 for the number of *srim* polynomials. (For the proof of these claims Götz [9].)

Remark. Because of the lemma just proved we can proceed as follows if we want to construct a *srim* polynomial of degree $2n$ over $\mathbb{F}_q$:

i) generate a monic irreducible polynomial f of degree n
ii) transform f into f^Q
iii) test, if

$$gcd(x^{q^n-1} - 1, f^Q(x)) = 1$$

which is equivalent to

$$x^{q^n} \equiv x \,(\mathrm{mod}\, f^Q(x)).$$

If the *gcd* is different from 1 then start from i) anew.

Confronted with this situation we ask for a priori conditions for f which guarantee that f^Q is irreducible.

At the beginning of the investigations we note the following simple lemma which is also used by Cohen in [5] in a more general form:

Lemma 5. *Let f be an irreducible polynomial of degree n over $\mathbb{F}_q$. Then f^Q is irreducible if and only if the polynomial*

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

is irreducible, where β is any root of f.

Proof. Let α be a root of f^Q; then $\beta := \alpha + 1/\alpha$ is a root of f. So β has degree n over $\mathbb{F}_q$, because f is irreducible by assumption. On the other hand, α is a root of the polynomial g as defined above. Consequently, α is of degree $2n$ over $\mathbb{F}_q$ exactly when g is irreducible. □

Lemma 5 tells us that an answer to our question will depend on the properties of quadratic extensions.

At first we shall deal with the case of characteristic 2 so that the *trace* function will play a decisive role.

Theorem 6. *If $f(x) = x^n + \cdots + a_1x + a_0 \in \mathbb{F}_{2^k}[x]$ $(k \geqq 1)$ is an irreducible polynomial, then $f^Q(x)$ is irreducible if and only if the absolute trace of a_1/a_0 is equal to* 1.

Proof. In order to simplify notation we define

$$F := \mathbb{F}_2, \quad K := \mathbb{F}_{2^k}, \quad L := \mathbb{F}_{2^{nk}}.$$

The status of quadratic equations in characteristic 2 is well known: For $\alpha, \beta, \gamma \in L$ the equation $\alpha x^2 + \beta x + \gamma = 0$ has

- one solution in case $\beta = 0$
- no solution in case $\beta \neq 0 \wedge \mathrm{Tr}_{L/F}(\alpha \cdot \gamma / \beta^2) = 1$
- two solutions in case $\beta \neq 0 \wedge \mathrm{Tr}_{L/F}(\alpha \cdot \gamma / \beta^2) = 0$

(MacWilliams and Sloane [12], p. 277).

This information combined with Lemma 5 leads to: f^Q is irreducible if and only if the discriminant $\mathrm{Tr}_{L/F}(1/\beta^2)$ of Eq. (5) $g = 0$ is equal to 1.

Because of

$$\mathrm{Tr}_{L/F}(1/\beta^2) = (\mathrm{Tr}_{L/F}(1/\beta))^2$$

we get the condition $\mathrm{Tr}_{L/F}(1/\beta) = 1$.

The transitivity of the trace function gives

$$\mathrm{Tr}_{L/F}(1/\beta) = \mathrm{Tr}_{K/F}(\mathrm{Tr}_{L/K}(1/\beta)) = 1.$$

On the other hand $\mathrm{Tr}_{L/K}(1/\beta)$ is the second-highest coefficient of the *monic* reciprocal of $f(x)$: $x^n + (a_1/a_0)x^{n-1} + \cdots + 1/a_0$. Thus the absolute trace of a_1/a_0 must be 1. □

Corollary 7. (Varshamov and Garakov). *If $f(x) = x^n + \cdots + a_1x + 1 \in \mathbb{F}_2[x]$ is irreducible then $f^Q(x)$ is irreducible if and only if a_1 is equal to* 1.

Proof. The trace function is the identity. □

Example. In $\mathbb{F}_4$ the elements with trace equal to 0 are 0 and 1. Therefore we get the following rule: the Q-image of the irreducible polynomial $f(x) = x^n + \cdots + a_1x + a_0 \in \mathbb{F}_4[x]$ is irreducible if and only if $a_0 \neq a_1$ and $a_1 \neq 0$. For instance, the Q-images of $x^2 + \omega x + 1, x^2 + \omega^2 x + 1, x^2 + x + \omega$, and $x^2 + x + \omega^2$ are the 4 *srim* polynomials of degree 4 over $\mathbb{F}_4$ as given (in the same order) in the example after Lemma 2. The corresponding rules for $\mathbb{F}_8, \mathbb{F}_{16}, \ldots$ depend on the particular primitive element one uses and are not expressible by the coefficients of f alone.

When the characteristic of the field $\mathbb{F}_q$ is odd we find a necessary and sufficient condition for the irreducibility of f^Q which reflects even less directly the properties of the coefficients of f:

Theorem 8. *Let q be an odd prime power. If f is an irreducible monic polynomial of degree n over $\mathbb{F}_q$ then f^Q is irreducible if and only if the element $f(2)\cdot f(-2)$ is a non-square in $\mathbb{F}_q$.*

Proof. By Lemma 5 f^Q is irreducible if and only if the polynomial g is irreducible which in the case of odd characteristic is equivalent to

$$\beta^2 - 4 \text{ is a non-square in } \mathbb{F}_{q^n}.$$

Again, this condition for β is equivalent to the condition given in the theorem as the following computation shows:

$$\begin{aligned}
&\beta^2 - 4 \text{ is a non-square in } \mathbb{F}_{q^n}\\
&\quad \Leftrightarrow (\beta^2-4)^{(q^n-1)/2} = -1 \Leftrightarrow \{[(2-\beta)(-2-\beta)]^{(q^n-1)/(q-1)}\}^{(q-1)/2} = -1\\
&\quad \Leftrightarrow \{f(2)\cdot f(-2)\}^{(q-1)/2} = -1 \Leftrightarrow f(2)\cdot f(-2) \text{ is a non-square in } \mathbb{F}_q. \quad \square
\end{aligned}$$

Example. Over the field $\mathbb{F}_5$ there are 10 irreducible monic polynomials of degree 2. Six of them yield by evaluation

$$f(2)\cdot f(-2) \notin \{\pm 1\} = (\mathbb{F}_5^*)^2.$$

These polynomials are $x^2+x+2, x^2+2x+3, x^2+2x+4, x^2+3x+3, x^2+3x+4$ and x^2+4x+2. The Q-images of these 6 polynomials are exactly the 6 *srim* polynomials of degree 4 over $\mathbb{F}_5$.

Remark. In their paper Varshamov and Garakov [16] assert on p. 409 that "almost" all of their results could be generalized to "higher characteristics". Götz [9] has given a proof of Corollary 7 which avoids the complicated induction arguments used by these authors and he points out that the crucial fact they use is:

$$((1 + x + x^2 + \cdots + x^{2^{n-1}})^*)^Q = (x^{2^n+1} + 1)/(x + 1)$$

which heavily depends on the $\mathbb{F}_2$-arithmetic.

4. Iterated Presentations

In this section we shall show how one can construct infinite sequences of irreducible polynomials by iterated application of the Q-transformation. With possible exception of the first polynomial all polynomials in each sequence are self-reciprocal.

The constructions provide examples of what Brawley and Schnibben in [3] call iterated presentations:

Definition. An *iterated presentation* of $GF(q^N)$ over $GF(q)$, N a Steinitz number, is a pair of sequences $(d_i, p_i(x))$ consisting of a specified divisor sequence $d_0 = 1, d_1, d_2, \ldots$ converging to N and a specified sequence of polynomials $f_1(x), f_2(x), \ldots$ such that for all $i \geqq 0$, $f_{i+1}(x)$ is an irreducible polynomial of degree d_{i+1}/d_i over $GF(q^{d_i})$.

In the examples to follow d_1 will be a specified number n and the quotients d_{i+1}/d_i will be 2 for all $i \geqq 1$. Also, we shall present the intermediate fields by irreducible polynomials over $GF(q)$ of degree $d_i = 2^{i-1}\cdot n$, which is an obviously equivalent procedure. Accordingly, the fields we are going to present are of the type $GF(q^{n\cdot 2^\infty})$.

We first deal with the case of characteristic 2.

Theorem 9. *The Q-transform of a* srim *polynomial* $f(x) = x^n + a_1 x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{F}_{2^k}[x]$ *with* $\mathrm{Tr}(a_1) = 1$ *is a* srim *polynomial of the same kind, i.e.* $f^Q(x) = x^{2n} + \tilde{a}_1 x^{2n-1} + \cdots + \tilde{a}_1 x + 1$ *satisfies* $\mathrm{Tr}(\tilde{a}_1) = 1$.

Proof. We use the following notation:

$$F := \mathbb{F}_2, \quad K := \mathbb{F}_{2^k}, \quad L := \mathbb{F}_{2^{nk}}, \quad G := \mathbb{F}_{2^{2nk}}.$$

By Theorem 6 f^Q is irreducible. If α is a root of f^Q then $\beta := \alpha + 1/\alpha$ is a root of f and α is a root of the irreducible polynomial $g(x) := x^2 + \beta x + 1 \in L[x]$ (Lemma 5). We have to following identities:

$$\mathrm{Tr}_{G/L}(\alpha) = \beta; \quad \mathrm{Tr}_{G/K}(\alpha) = \tilde{a}_1; \quad \mathrm{Tr}_{L/K}(\beta) = a_1$$

which combine by transitivity to

$$\mathrm{Tr}_{K/F}(\tilde{a}_1) = \mathrm{Tr}_{K/F}\,\mathrm{Tr}_{G/K}(\alpha) = \mathrm{Tr}_{K/F}\,\mathrm{Tr}_{L/K}(\beta) = \mathrm{Tr}_{K/F}(a_1) = 1. \quad \square$$

Examples

1. Starting with $m_1(x) = x^2 + x + 1$ over $\mathbb{F}_2$ and defining $m_{i+1}(x) = m_i(x)^Q (i \geq 1)$ we get an infinite sequence of irreducible polynomials over $\mathbb{F}_2$ of degrees 2^i. This sequence was used recently by D. Wiedemann [17] (also [3]) to construct an iterated presentation of the infinite field $GF(2^{2^\infty})$, a subfield of the algebraic closure of $\mathbb{F}_2$. We note in passing that Wiedemann posed the question if for all i the order of $m_i(x)$ is the maximum possible, namely $2^{2^{i-1}} + 1$, the $(i-1)^{\text{th}}$ Fermat number.

2. If we start with the *srim* polynomial of degree 10:

$$m_1(x) = x^{10} + x^9 + x^5 + x + 1 \in \mathbb{F}_2[x]$$

we get an iterated presentation of $GF(2^{5\cdot 2^\infty})$.

3. If we want to define the field $GF(2^{3\cdot 2^\infty})$ we can start with the polynomial of degree 12:

$$x^{12} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1 \in \mathbb{F}_2[x].$$

(Note that $x^6 + x^3 + 1$ is the only *srim* polynomial of degree 6 over $\mathbb{F}_2$!)

More generally, we are able to give an iterated presentation of the infinite field $GF(2^{n\cdot 2^\infty})$ for any *odd n* via the following procedure: We start with an irreducible polynomial of degree n over $\mathbb{F}_2$ such that both the second-highest and the linear coefficient are 1 (call these polynomials of type A). The Q-transformation applied to such a polynomial gives a *srim* polynomial with linear coefficient equal to 1. The iterated application of Q will then lead to the desired sequence of extensions according to Theorem 9.

We show that polynomials of type A exist in the case $n = 2\cdot m, m$ *odd*, which is sufficient for our purposes. (In fact, there is computational evidence that polynomials of type A exist for all degrees $\geqq 4$ and that the numbers of these polynomials increase quite rapidly, but we were not able to give an explicit counting formula for them.)

Suppose on the contrary that any irreducible polynomial over $\mathbb{F}_2$ of degree n with linear coefficient 1 is of type B, i.e. has second-highest coefficient 0. Let B^* be the set of reciprocals of the polynomials in B. By assumption, $B\cap B^*=\emptyset$. By Corollary 7 we know that $card(B)$ is equal to the number of *srim* polynomials of degree $2n$. But now $2\cdot card(B)=\frac{1}{2m}\sum_{d|m}\mu(d)2^{2m/d}$ already exceeds (without taking into account polynomials of type $x^n+0\cdot x^{n-1}+\cdots+0\cdot x+1$!) the number of *all* irreducible polynomials:

$$N_2(n)=\frac{1}{n}\sum_{d|n}\mu(d)2^{n/d}=\frac{1}{2m}\sum_{d|m}\mu(d)2^{2m/d}-\frac{1}{2m}\sum_{d|m}\mu(d)2^{m/d}.$$

This contradiction shows that A cannot be empty.

When p is an odd prime the conditions under which an irreducible polynomial $f(x)\in\mathbb{F}_p[x]$ generates an infinite sequence of irreducible polynomials by iterated application of Q are much more complicated. In fact, the following investigation should be understood as a more experimental attempt to demonstrate the problems involved.

The condition on f^Q that makes f^{Q^2} irreducible is:

$$f^Q(2)\cdot f^Q(-2)=2^{2n}(-1)^n f(5/2)\cdot f(-5/2) \text{ is a non-square.}$$

The condition on f^{Q^2} that makes f^{Q^3} irreducible is:

$$f^{Q^2}(2)\cdot f^{Q^2}(-2)=10^{2n}(-1)^n f(29/10)\cdot f(-29/10) \text{ is a non-square.}$$

Continuing in this way we get a sequence of conditions in which f has to be evaluated at the points $\pm\Psi_p^r(1)$ for $r\geqq 1$ where Ψ_p denotes the finite mapping $\Psi_p\colon a\mapsto a+1/a \pmod p$ and Ψ_p^r denotes the r^{th} iteration of Ψ_p. Obviously, $\Psi_p(a)=a+a^{p-2}$, so that Ψ_p is also defined for 0.

We list a few elementary properties of this mapping which we need in the sequel:

(i) Due to the symmetry $\Psi_p(-a)=-\Psi_p(a)$ we identify Ψ_p with the mapping induced on the set of unordered pairs $(a,-a)$.
(ii) Any element of $\mathbb{F}_p$ which has a Ψ_p-preimage has exactly two of them with the only exception of $(2,-2)$. As a consequence, $(2,-2)$ is contained in a Ψ_p-cycle if and only if this is true for $(1,-1)$.
(iii) $(1,-1)$ has no Ψ_p-preimage if and only if -3 is a non-square in $\mathbb{F}_p$, i.e. $p\equiv -1 \pmod 6$.
(iv) If $p\equiv 1 \pmod 6$ then 1 has a Ψ_p-preimage but may not generate a Ψ_p-cycle. 37 is the first prime of this type.
(v) We call a prime p *Q-singular* if 0 is the final point of the Ψ_p-orbit of 1 (otherwise we call it *Q-regular*). Necessarily such a prime is $\equiv 1 \pmod 4$ and $\equiv \pm 1 \pmod{10}$ (when greater than 5), to mention only the simplest congruences to be satisfied. For these primes the Q-iteration with irreducible outcome comes to an end after

finitely many steps. In order to give an idea of the frequency we list the Q-singular primes not greater than 10,000:5, 29, 41, 89, 101, 109, 269, 421, 509, 521, 709, 929, 941, 1549, 1861, 2281, 2521, 2749, 2801, 2909, 3121, 3169, 3469, 5821, 5881, 7109, 8069, 8969, 9041, 9181.

In order to generate an infinite sequence of *srim* polynomials over a field with Q-regular characteristic p one has to

1. determine the length l_p of the Ψ_p-orbit of 1 and to
2. find an irreducible polynomial $f(x)$ that satisfies the conditions:

$$f(2)\cdot f(-2) \quad \textit{and} \quad (-1)^n\cdot f(\Psi_p^r(1))\cdot f(\Psi_p^r(-1))$$
$$\textit{are non-squares} \pmod p \textit{ for all } r=1,\dots,l_p+1.$$

It appears to be difficult to find general propositions concerning these two tasks, so at present we have to content ourselves with giving examples in some special cases.

When we are sure that neither p is Q-singular nor 1 is contained in a Ψ_p-cycle then we can use the following alternative to define infinite sequences of *srim* polynomials:

Theorem 10. *If p is a prime satisfying $p\equiv 3 \pmod 4$ and $p\equiv 5 \pmod 6$ then* (i) *any irreducible polynomial $f(x)\in\mathbb{F}_p[x]$ of* even *degree n such that $f(\Psi_p^r(1))\cdot f(\Psi_p^r(-1))$ is a* non-square *for all $r\geqq 1$ defines an iterated presentation of $GF(p^{n\cdot 2^\infty})$.*
(ii) *any polynomial of* odd *degree n such that $f(2)\cdot f(-2)$ is a* non-square *and $f(\Psi_p^r(1))\cdot f(\Psi_p^r(-1))$ is a* square *for all $r\geqq 2$ defines an iterated presentation of $GF(p^{n\cdot 2^\infty})$.*

Note that we do not claim the general availability of the polynomials needed in Theorem 10.

Example. For $p=11$ the Ψ_{11}-orbit of 1 is $1\to 2\to(-3)\to 4\leftrightarrow(-4)$. The polynomial x^2+x+6 may be taken as an example for the case (i) of the theorem whereas for (ii) the polynomial $x+5$ is suitable.

Finally, if 1 generates a Ψ_p-cycle then we have to make sure that the conditions "$f(2)\cdot f(-2)$ *is a non-square*" and "$(-1)^n\cdot f(2)\cdot f(-2)$ *is a non-square*" are compatible.

This means that for $p\equiv 3 \pmod 4$ the degree n has to be even.

The case of the two smallest Q-regular primes is particularly easy:

If $f(x)\in\mathbb{F}_3[x]$ is irreducible of even *degree such that $f(1)\cdot f(-1)=-1$ then $f(x)$ generates an infinite sequence of* srim *polynomials by Q-iteration.*

As an example one might take $x^2+x+2\in\mathbb{F}_3[x]$.

If $f(x)\in\mathbb{F}_7[x]$ is irreducible of even *degree such that $f(1)\cdot f(-1)$ and $f(2)\cdot f(-2)$ are both non-squares* (mod 7) *then $f(x)$ generates an infinite sequence of* srim *polynomials by Q-iteration.*

As an example one might take $x^2+x-1\in\mathbb{F}_7[x]$.

We close by reviewing the open questions which arose in this section:

- What is the number of polynomials of type A?
- Is there a characterization of the Q-singular primes?
- For which primes p is the Ψ_p-orbit of 1 cyclic?
- For which pairs (p, d) do there exist irreducible polynomials over $\mathbb{F}_p, p$ odd, of degree d which give rise to an infinite sequence of self-reciprocal irreducibles?

Acknowledgements. The author is grateful to the referee for his helpful suggestions and comments, especially for the simplification of the proof of Thereom 8 and reference to the papers [5], [7], and [6].

References

1. Andrews, G. E.: Reciprocal polynomials and quadratic transformations. Utilitas Math. **28**, 255–264 (1985)
2. Berlekamp, E. R.: Bit-serial Reed-Solomon encoders. IEEE Trans. Inform. Theory **IT-28**, 869–874 (1982)
3. Brawley, J. V., Schnibben, G. E.: Infinite algebraic extensions of finite fields. Contemporary Mathematics, vol. **95**, American Math. Soc., Providence, Rhode Island 1989
4. Carlitz, L.: Some theorems on irreducible reciprocal polynomials over a finite field. J. Reine Angew. Math. **227**, 212–220 (1967)
5. Cohen, S. D.: On irreducible polynomials of certain types in finite fields. Proc. Camb. Phil. Soc. **66**, 335–344 (1969)
6. Cohen, S. D.: Polynomials over finite fields with large order and level. Bull. Korean Math. Soc. **24**, 83–96 (1987)
7. Garbe, D.: On the level of irreducible polynomials over Galois fields. J. Korean Math. Soc. **22**, 117–124 (1985)
8. Gilbert, E. N., Riordan, J.: Symmetry types of periodic sequences. Illinois J. Math. **5**, 657–665 (1961)
9. Götz, W.: Selbstreziproke Polynome über endlichen Körpern. Diploma thesis, Erlangen (1989)
10. Hong, S. J., Bossen, D. C.: On some properties of self-reciprocal polynomials. IEEE Trans. Inform. Theory **IT-21** 462–464 (1975)
11. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20, Reading, MA: Addison-Wesley 1983
12. MacWilliams, F. J., Sloane, N. J. A.: The theory of error-correcting codes. Amsterdam: North-Holland 1977
13. Massey, J. L.: Reversible codes. Information Control **7**, 369–380 (1964)
14. Miller, R. L.: Necklaces, Symmetries and Self-Reciprocal Polynomials. Discrete Math. **22**, 25–33 (1978)
15. Patel, A. M., Hong, S. J.: Optimal rectangular code for high density magnetic tapes. IBM J. Res. Develop. **18**, 579–588 (1974)
16. Varshamov, R. R., Garakov, G. A.: On the Theory of Selfdual Polynomials over a Galois Field (Russian). Bull. Math. Soc. Sci. Math. R. S. Roumanie, (N.S.) **13**, 403–415 (1969)
17. Wiedemann, D.: An Iterated Quadratic Extension of GF(2). Fibonacci Quart. **26**, 290–295 (1988)

Received January 6, 1990; revised version March 29, 1990

Note added in proof. H. Niederreiter has answered completely the question about polynomials of type A in his paper "An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field" (forthcoming).