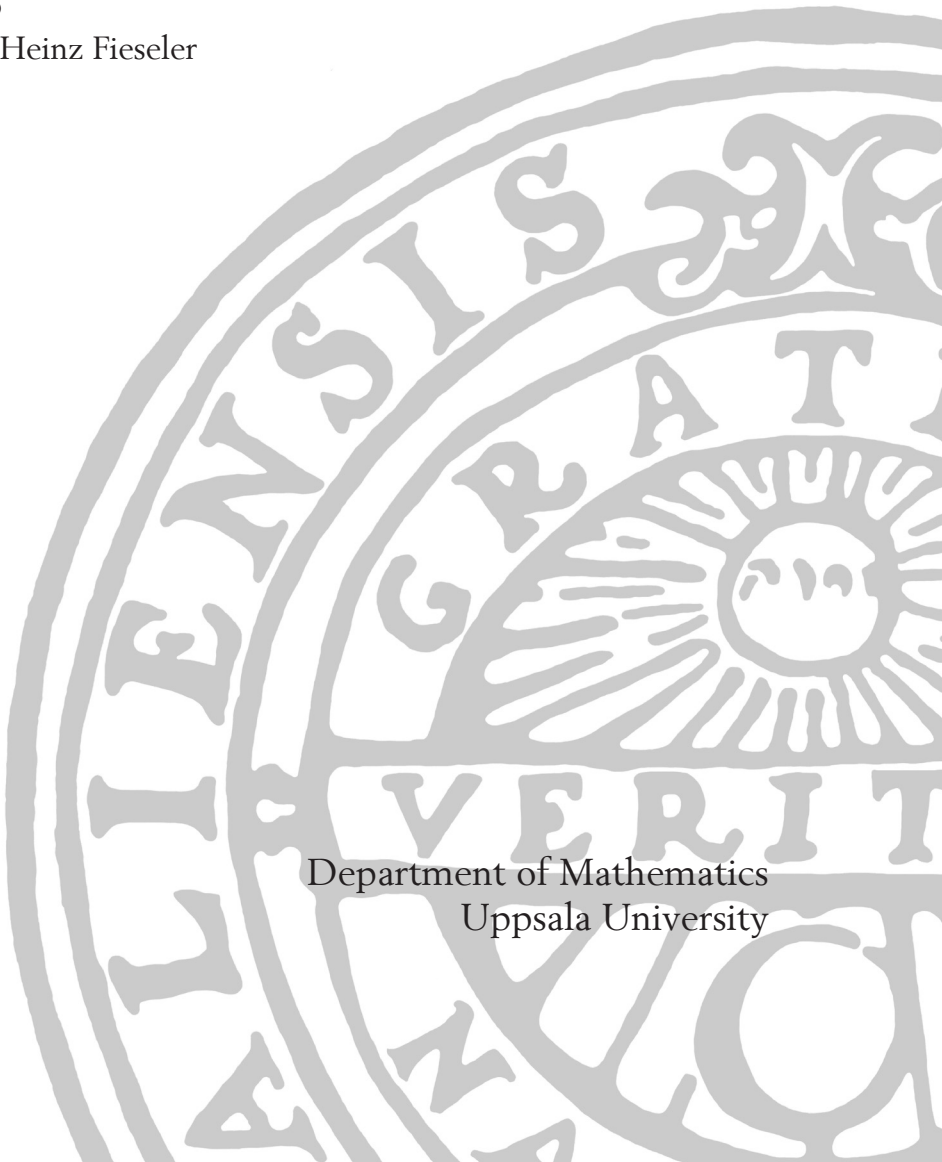
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2014:17

Construction of Irreducible Polynomials over Finite Fields

Gustav Hammarhjelm

Examensarbete i matematik, 15 hp
Handledare och examinator: Karl-Heinz Fieseler
Maj 2014



Department of Mathematics
Uppsala University

Construction of irreducible polynomials over finite fields

Gustav Hammarhjelm

May 22, 2014

Contents

Abstract

In this paper we investigate some results on the construction of irreducible polynomials over finite fields. Basic results on finite fields are introduced and proved. Several theorems proving irreducibility of certain polynomials over finite fields are presented and proved. Two theorems on the construction of special sequences of irreducible polynomials over finite fields are investigated in detail.

Acknowledgements

I would like to thank my supervisor Karl-Heinz Fieseler for guidance, inspiration and insightful comments. I would also like to thank my family for their support.

1 Introduction

The concept of a prime number is well known. The properties that make prime numbers interesting include (but are not limited to) the fact that a prime number does not admit any non-trivial factorization in integers and that if a prime number divides a product of numbers, it necessarily divides one of the factors. The first quality is what defines an irreducible element in any unital ring:

Definition 1.1. Let R be a commutative ring with unity and let $r \in R$. A non-zero, non-unit r is said to be *irreducible* if $r = ab$ for $a, b \in R$ implies a is a unit or b is a unit.

If one is challenged to find, explicitly, infinite sequences of distinct irreducible elements of a ring one can have various outcomes:

In the ring $\mathbb{Z}$ the irreducible elements are $\pm p$ where p is any prime number. As of today, as far as I know, nobody has come up with an explicit infinite sequence of distinct prime numbers.

The challenge turns out to be a rather modest one in some rings. For instance in $\mathbb{Q}[x]$, the polynomial ring over the field of rational numbers, it is very easy to explicitly define sequences of irreducible elements, e.g. the sequence $x^n - 2$ where n is a non-zero natural number, using Eisenstein's criterion.

In this text we will consider the setting when R is the polynomial ring $\mathbb{F}_q[x]$ over a finite field $\mathbb{F}_q$. A non-constant polynomial $f(x)$ of $\mathbb{F}_q[x]$ is called *irreducible over* $\mathbb{F}_q$ if $f(x) = g(x)h(x)$ for polynomials $g(x), h(x) \in \mathbb{F}_q[x]$ implies $g(x)$ or $h(x)$ is a unit, i.e. $g(x)$ or $h(x)$ is in $\mathbb{F}_q$, according to the definition of irreducibility. We will show that it is indeed possible (but requires more work than in $\mathbb{Q}[x]$) to generate infinite sequences of irreducible elements of strictly increasing degrees over $\mathbb{F}_q[x]$ for various finite fields $\mathbb{F}_q[x]$.

The existence of such sequences are not only valuable for recreational purposes, they may also be used for applications in mathematics. Indeed, one important role of irreducible polynomials is that one can explicitly construct fields using irreducible polynomials through factor rings. If one wants to make explicit calculations in say a finite field, it is often required to find an irreducible polynomial, in order to get information of the structure of the field. This is important for applications of field theory, for instance error correcting codes.

In this text we shall, after presenting some auxiliary results, investigate some ways of recognizing irreducible polynomials over finite fields. In the last part, we carefully investigate a theorem on the construction of infinite sequences of irreducible polynomials of increasing degree over finite fields.

2 Basic results on finite fields

Firstly, some notation that will be used in the text. If F and K are fields $F > K$ expresses that F is a field extension of K (or K is a subfield of F). If the extension is finite, then $[F : K]$ denotes the dimension of F over K, when F is considered a vector space over K. If $\alpha_1, \ldots, \alpha_n$ are algebraic over F then $F(\alpha_1, \ldots, \alpha_n)$ is the extension of F obtained by adjoining $\alpha_1, \ldots, \alpha_n$ to F. $F[x]$ denotes the polynomial ring over F and $\mathbb{F}_q$ denotes the finite field of q elements, $\mathbb{F}_q^*$ its multiplicative group.

Some fundamental results of algebra shall be used frequently, but will not be proved here, for instance that there is a finite field of p^n elements for each prime p and each positive natural number n, unique up to isomorphism, as well as the tower law for finite extensions and that the multiplicative group of a finite field is cyclic.

Theorem 2.1. *Let $\mathbb{F}$ be a finite field of characteristic p. Then*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

for $a, b \in \mathbb{F}, n \in \mathbb{N}_{>0}$.

Proof. By the binomial theorem for commutative rings

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

where each $p \mid \binom{p}{k}$ for each $0 < k < p$ so $(a+b)^p = a + b$. Now $(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p$ and the first result follows by induction. For the second result

$$(a-b)^{p^n} = (a + (-b))^{p^n} = a^{p^n} + (-b)^{p^n}.$$

Now if p is odd, $(-1)^{p^n} = -1$, if p is even $-1 = 1$ so in either case we have obtained the other result. □

Theorem 2.2. *Let $\mathbb{F}_q$ be a finite field and let $f \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$,* $\deg f = n$. *Then the splitting field of f is $\mathbb{F}_{q^n}$. Furthermore, if α is a zero of f, then the other zeros of f are given by $\alpha^q, \ldots, \alpha^{q^{n-1}}$.*

Proof. The theorem is trivial if $n = 1$ so assume $n > 1$. Let α be a zero in the splitting field of f, $\alpha \neq 0$ since $f(x)$ irreducible. $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$ so $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^n}$. Now, suppose $f(x) = \sum_{k=0}^{n} a_k x^k$, so that $f(\alpha) = \sum_{k=0}^{n} a_k \alpha^k = 0$. By theorem 2.1, for $0 < i < n$

$$0 = \left(\sum_{k=0}^{n} a_k \alpha^k \right)^{q^i} = \sum_{k=0}^{n} a_k^{q^i} \alpha^{kq^i} = f(\alpha^{q^i}),$$

since $a_k^q = a_k$, as $a_k \in \mathbb{F}_q$. It remains to show that $\alpha^{q^i} = \alpha^{q^j}$, $0 \leq i, j < n$ implies $i = j$ (so that we really have obtained n distinct zeros of f), until we, with clear conscience, may declare $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^n}$ the splitting field of f.

To this end, we use the fact that an irreducible polynomial $f(x)$ of degree m over a finite field $\mathbb{F}_q$ divides $x^{q^n} - x$ if and only if $m \mid n$. If $m \mid n$ then $\mathbb{F}_{q^m} < \mathbb{F}_{q^n}$ and as $\mathbb{F}_{q^n}$ consists of the zeros of $x^{q^n} - x$ each zero of $f(x)$ is a zero of $x^{q^n} - x$ so $f(x)$ divides this polynomial.

Conversely, if $f(x) \mid x^{q^n} - x$ and β is a zero of $f(x)$ in $\mathbb{F}_{q^m}$, we have the equality $\mathbb{F}_{q^m} = \mathbb{F}(\beta)$ since $f(x)$ is irreducible of degree m, then α is a zero of $x^{q^n} - x$ as well and thus $\alpha \in \mathbb{F}_{q^n}$. Therefore we have

$$\mathbb{F}_q < \mathbb{F}_{q^m} < \mathbb{F}_{q^n}$$

and $m \mid n$ by the tower law of finite field extensions.

Now, for a contradiction, assume $\alpha^{q^i} = \alpha^{q^j}$, $0 \leq i, j < n$. Then, since $\alpha \neq 0$ we have

$$\alpha^{q^i} = \alpha^{q^j} \iff \alpha^{q^i(q^{j-i}-1)} = 1 \iff (\alpha^{q^{j-i}-1})^{q^i} = 1$$

by raising the right hand side to the power q^{n-i} and multiplying with α we get $\alpha^{q^{j-i}} = \alpha$ since $\alpha^{q^{j-i}-1} \in \mathbb{F}_{q^n}$. Thus, α is a zero of $x^{j-i} - x$ and so $m \mid j - i$ with $0 < j - i < m$ which is absurd. □

Remark 2.3. We have seen in the proof of the last theorem that an irreducible polynomial over a finite field of degree m must have m distinct zeros. With this information we can deduce that polynomials of certain forms are never irreducible.

Let $\mathbb{F}_q$ be a field of characteristic p and consider the polynomial $x^p + a$ for some $a \in \mathbb{F}_q$. Let α be a zero of $x^p + a = 0$ with $\alpha \in \mathbb{F}_{q^p}$. Then $(x - \alpha)^p = x^p - \alpha^p = x^p + a$ and we see that the only zero of $x^p + a = 0$ is α and since $p > 1$ the polynomial $x^p + a$ must be reducible over $\mathbb{F}_q$ since if it would be irreducible, it would have p distinct zeros.

Definition 2.4. Let F be a field and K be a subfield of F. An automorphism σ of F is an automorphism of F *over* K if $\sigma(a) = a$ for all $a \in K$.

Theorem 2.5. *Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, $m > 1$ be finite fields. Then the automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are precisely $\sigma_i, i = 1, \ldots, m$ where $\sigma_i(\alpha) = \alpha^{q^i}$ for all $\alpha \in \mathbb{F}_{q^m}$.*

Proof. That σ_i are indeed automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is easily seen.

Suppose φ is an automorphism $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let θ be a generator of the multiplicative group of $\mathbb{F}_{q^m}$. If we can determine the image of θ, we determine the automorphism completely. φ is a linear mapping of $\mathbb{F}_{q^m}$ viewed as a vector space over $\mathbb{F}_q$. Now let f be the minimal polynomial of θ over $\mathbb{F}_q$, $\deg f = m$. Since φ is linear, we have $0 = \varphi(f(\theta)) = f(\varphi(\theta))$. By theorem 2.2 $\varphi(\theta) = \theta^{q^k}$ for some $k \in \{1, \ldots, m\}$ and so the result follows. □

Remark 2.6. If K is a field and F a finite extension of K, then the extension is called *normal* if $[F : K] = |\mathrm{Aut}(F/K)|$, where $\mathrm{Aut}(F/K)$ is the group of automorphisms of F over K. Such extensions are of great importance in Galois theory. By the above theorem, we see that a finite extension of a finite field is always normal.

Later in the text we shall need the concept of a normal basis of a finite field over a subfield. The definition of this concept is presented here.

Definition 2.7. Let $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$ be finite fields. A *normal basis* of F over K is a basis of F over K of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ for some $\alpha \in F$.

Remark 2.8. In terms of our above automorphisms $\sigma_i(\alpha) = \alpha^{q^i}$ of F over K, $0 \leq i < m$, a normal basis of F over K is a basis of F over K of the form $\{\alpha, \sigma_1(\alpha), \ldots, \sigma_{m-1}(\alpha)\}$ for some $\alpha \in F$.

The two following theorems are used to prove that every finite field has a normal basis over any subfield. First a result from linear algebra, whose proof will be omitted, but can be found in [4]:

Theorem 2.9. *Let F be a field and V a finite dimensional F-vector space,* $\dim V = n$*, and let $T : V \to V$ be a linear map. V is T-cyclic, i.e. there is a basis of V of the form $\{v, T(v) \ldots, T^{n-1}(v)\}$ for some $v \in V$ if and only if the characteristic polynomial χ_T of T equals the minimal polynomial μ_T of T.*

The following result is stated and proven in [3].

Theorem 2.10. [3] *Let G be a group. Let $\varphi_1, \ldots, \varphi_m$ be distinct homomorphisms from G to $\mathbb{F}_q^*$ and let $a_1, \ldots, a_m \in \mathbb{F}_q$, not all zero. Then $\varphi_1, \ldots, \varphi_m$ are linearly independent i.e. there exists $g \in G$ s.t.*

$$a_1\varphi_1(g) + \ldots + a_m\varphi_m(g) \neq 0.$$

The theorem that shows that every finite field has a normal basis over any subfield follows beautifully from the last two results.

Theorem 2.11. [3] *Let $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$ be finite fields. Then there exists a normal basis of F over K.*

Proof. We consider the automorphisms $\sigma_i(\alpha) = \alpha^{q^i}$ of F over K, where $0 \leq i < m$. These are m distinct group homomorphisms from F^* to F^*. Furthermore, σ_i are linear maps of F considered as a vector space over K. The statement that F has a normal basis over K is equivalent with saying that F is σ_1-cyclic. We therefore investigate the minimal and characteristic polynomial of σ_1, denoted μ and χ respectively.

$f(x) = x^m - 1$ clearly satisfies $f(\sigma_1) = 0 \in \mathrm{End}(F)$. We now show that there is no polynomial $g(x)$ of degree less than m such that $g(\sigma_1) = 0 \in \mathrm{End}(F)$. To this end, let $g(x) \neq 0$ be given, $\deg g < m$. Then, $g(\sigma_1)$ assumes the form

$$a_0\sigma_1^0 + a_1\sigma_1^1 + \ldots + a_{m-1}\sigma_1^{m-1} = a_0\sigma_0 + a_1\sigma_1 + \ldots + a_{m-1}\sigma_{m-1}$$

where $a_0, \ldots, a_{m-1} \in F$ are not all zero, and we may apply the previous theorem to conclude that there is $a \in F$ s.t. $g(\sigma_1)(a) \neq 0$ and thus $g(\sigma_1) \neq 0$. We may now conclude that the minimal polynomial μ of σ_1 is of degree m. Since χ is of degree m, both are monic, and $\mu \mid f(x)$, $\mu \mid \chi$ we must have $\mu = \chi = f$.

By theorem 2.9 we know that F is σ_1-cyclic, when viewed as a vector space over K, i.e. there is $a \in F$ such that $\{a, \sigma_1(a), \ldots, \sigma_1^{m-1}(a)\}$ is a basis of F over K. This is the desired normal basis of F over K. □

The following is a well-known test for determining whether an element α of a field $\mathbb{F}_q$ of odd characteristic is a quadratic residue or not, i.e. whether it exists $\beta \in \mathbb{F}_q$ with $\beta^2 = \alpha$ or not, and will be used later in the text:

Theorem 2.12. *Let $\mathbb{F}$ be a finite field of odd characteristic, $|\mathbb{F}| = q$. Then $\alpha \in \mathbb{F}^*$ is a quadratic non-residue of $\mathbb{F}$ if and only if $\alpha^{(q-1)/2} = -1$.*

Proof. For any non-zero α, $\left(\alpha^{(q-1)/2}\right)^2 - 1 = 0$ so $\alpha^{(q-1)/2} = \pm 1$, since in a field $x^2 - 1 = 0$ has only two solutions. Let θ be a generator of the multiplicative group of $\mathbb{F}$, then $\alpha = \theta^k$ for some natural number k. If k is even, then $\alpha = (\theta^{k/2})^2$ is a quadratic residue in $\mathbb{F}$ and $\alpha^{(q-1)/2} = \theta^{k\cdot(q-1)/2} = (\theta^{k/2})^{q-1} = 1$.

If on the other hand $\alpha = \theta^{2k+1}$ for some k, α is a quadratic non residue in $\mathbb{F}$, then

$$\alpha^{(q-1)/2} = (\theta^{2k}\theta)^{(q-1)/2} = (\theta^k)^{q-1}\theta^{(q-1)/2} = -1,$$

since $\theta^{(q-1)/2}$ must be -1 as θ is a generator of the multiplicative group of $\mathbb{F}$. □

Remark 2.13. A consequence of this theorem is that a non-zero element of a finite field of odd characteristic is a quadratic non-residue if and only if it is an odd power of the generator of the multiplicative group. From this it can be derived that the product of a quadratic non-residue and a non-zero quadratic residue is again a quadratic non-residue, as well as that the product of two quadratic residues is again a quadratic residue and finally that the product of two quadratic non-residues is a quadratic residue.

Furthermore, it is seen that the number of non-zero quadratic residues equals the number of quadratic non-residues which is $(q-1)/2$, which is seen through the characterization of non-zero elements as odd or even powers of the generator of the multiplicative group.

2.1 The reciprocal of a polynomial

Later in the text, especially when constructing sequences of irreducible polynomials, the major part of the polynomials dealt with will consist of self-reciprocal polynomials, a notion which will be defined here.

Definition 2.14. The *reciprocal* of a non-zero polynomial $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{F}_q[x]$ of degree n, denoted f^*, is the polynomial $f^*(x) = \sum_{k=0}^{n} a_k x^{n-k}$. A polynomial is called *self-reciprocal* if $f^*(x) = f(x)$.

For a polynomial $f(x) \in \mathbb{F}_q[x]$ we will often denote $f^*(x)$ by $x^n f(1/x)$, which is to be intepreted as an element of $\mathbb{F}_q(x)$, the field of quotients of $\mathbb{F}_q[x]$. Upon calculation in $\mathbb{F}_q(x)$ one indeed finds that $f^*(x) = x^n f(1/x)$ and so $x^n f(1/x) \in \mathbb{F}_q[x]$.

Remark 2.15. Here follows some remarks about reciprocal polynomials:

1. If $f(x) = \sum_{k=0}^{n} a_k x^k$ is self-reciprocal then there is a symmetry in the coefficients of f i.e. $a_k = a_{n-k}$ for $k = 0, \ldots, n$. The converse holds as well.

2. For $f(x), g(x) \in \mathbb{F}_q[x]$ we have

   $$(fg)^* = x^{\deg fg} f(1/x)g(1/x) = x^{\deg f} f(1/x) x^{\deg g} g(1/x) = f^* g^*$$

   and in particular $(cf)^* = cf^*$ for $c \in \mathbb{F}_q$. If $f(0) \neq 0$ then $(f^*)^* = f$.

3. Let $f \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$, $f(0) \neq 0$. Then f^* is irreducible over $\mathbb{F}_q$.

   Proof. Since $f(0) \neq 0$ then $\deg(f) = \deg(f^*)$ and so $(f^*)^* = f$. Suppose $f^* = gh$. Then $f = (f^*)^* = (gh)^* = g^* h^*$ which implies that g^* or h^* is constant. Suppose w.l.o.g. that $h^*(x) = x^{\deg(h)} h(1/x)$ is constant. Thus we must have that $h(x) = ax^n$ for some $a \in \mathbb{F}_q, n \in \mathbb{N}$. $n > 0$ would imply that $f^*(0) = 0$ which leads to $\deg(f) < \deg(f^*)$, contradiction. Thus $n = 0$ and f^* is irreducible. □

2.2 The Möbius inversion formula

Definition 2.16. Let $\omega(n)$ be the arithmetic function with $\omega(n) = \sum_{p|n} 1$, so that $\omega(n)$ is the number of distinct primes that divide n. Now set

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square free,} \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.17. [7]. *$\mu(n)$ is a multiplicative arithmetic function and $\sum_{d|n} \mu(d)$ is 0 if $n > 1$ and 1 if $n = 1$.*

Theorem 2.18. The Möbius inversion formula part I, [7]. *If F, f are arithmetic functions with $F(n) = \sum_{d|n} f(d)$ for all $n \in \mathbb{N}_{>0}$ then $f(n) = \sum_{d|n} \mu(d)F(n/d)$ for all $n \in \mathbb{N}_{>0}$.*

Proof. Let I be the set of ordered pairs (a, b) with $ab|n$.

$$\begin{aligned} \sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \mu(d) \sum_{e|(n/d)} f(e) = \sum_{d|n} \sum_{e|(n/d)} \mu(d)f(e) \\ &= \sum_{(d,e)\in I} \mu(d)f(e) = \sum_{e|n} f(e) \sum_{d|(n/e)} \mu(d) = f(n), \end{aligned}$$

since $\sum_{d|n} \mu(d)$ is 0 if $n > 1$ by the previous theorem. □

Theorem 2.19. The Möbius inversion formula part II, [7]. *If F, f are arithmetic functions with $f(n) = \sum_{d|n} \mu(d)F(n/d)$ for all $n \in \mathbb{N}_{>0}$ then $F(n) = \sum_{d|n} f(d)$ for all $n \in \mathbb{N}_{>0}$.*

Example 2.20. Let $\varphi : \mathbb{N} \to \mathbb{C}$ be Euler's totient function. Then $\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$.

Proof. One can verify that $\sum_{d|n} \varphi(d) = n =: F(n)$ for all $n \in \mathbb{N}$ (by for instance observing that φ is multiplicative and that the identity holds for prime powers). Set $\varphi(n) = f(n)$. Applying a Möbius inversion to the identity

$$\sum_{d|n} f(d) = \sum_{d|n} \varphi(d) = n = F(n)$$

yields the desired result. □

Theorem 2.21. *Let $\mathbb{F}_q$ be a finite field. Let $I_q(n)$ denote the number of irreducible monic polynomials over $\mathbb{F}_q$ of degree n. Then*

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

Proof. Let n be given. Form the polynomial $g(x) = x^{q^n} - x$, whose splitting field is $\mathbb{F}_{q^n}$ since all elements of $\mathbb{F}_{q^n}$ are zeros of $g(x)$. Let f be monic, irreducible over $\mathbb{F}_q$ of degree $d \mid n$. $\mathbb{F}_{q^d}$ is the splitting field of f by theorem 2.2. Since $d \mid n$, $\mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^n}$ and thus the zeros of f are contained in the set of zeros of g and consequently $f \mid g$ since all zeros of f are simple.

Now let $f \mid g$, f monic and irreducible over $\mathbb{F}_q$. Now it is demonstrated that $\deg f = d \mid n$. If α is a zero of f then $\alpha^{q^d-1} = 1$ since the splitting field of f is $\mathbb{F}_{q^d}$. Since $f \mid g$ the zeros of f are contained in the set of zeros of g and therefore $\mathbb{F}_{q^d}$ is a subfield of $\mathbb{F}_{q^n}$ and so $d \mid n$.

We have now demonstrated that $x^{q^n} - x$ is the product of all irreducible monic polynomials over $\mathbb{F}_q$ with degrees dividing n. Therefore we have $q^n = \sum_{d|n} I_q(d)d$. Setting $F(n) = q^n$, $f(n) = nI_q(n)$ and applying a Möbius inversion yields the desired result. □

3 Finding irreducible polynomials (examples)

Here are some examples of how one could go about finding the elusive irreducible polynomials.

Theorem 3.1. *Let p be a prime. The polynomial $f(x) = x^p - x + a \in \mathbb{F}_q[x]$, $q = p^n$ with $n \geq 1$, is irreducible over $\mathbb{F}_q$ if and only if it has no zeros in $\mathbb{F}_q$.*

Proof. Let α be a zero of f in some extension field of $\mathbb{F}_q$. Since for all $b \in \mathbb{F}_p$, b is a zero of $x^p - x$, and by theorem 2.1, $\alpha + b$ is a zero of f for every $b \in \mathbb{F}_p$. These are all zeros of f. Thus, the splitting field of f is $\mathbb{F}_q(\alpha)$. Let $p(x)$ be an irreducible factor of f (over $\mathbb{F}_q$) so that $\mathbb{F}_q[x]/(p(x))$ is a field. Then $p(\alpha + b) = 0$ for some (possibly several) $b \in \mathbb{F}_p$ and we must have $\mathbb{F}_q[x]/(p(x)) \cong \mathbb{F}_q(\alpha)$. Thus, for any irreducible factor p of f we have $\mathbb{F}_q[x]/(p(x)) \cong \mathbb{F}_q(\alpha)$, which implies that all irreducible factors have the same degree. If the number of irreducible factors are k and each is of degree n then we must have $kn = p$. But, by assumption, f has no zeros in $\mathbb{F}_q$. Therefore $n > 1$ and we must have $k = 1$ so f is irreducible.

The converse is trivial. □

Granted theorem 3.1 we can easily establish that the representation of a finite field as a factor ring is not unique. For instance, if $p = 5$, then both $x^5 - x + 1, x^5 - x + 2$ are irreducible over $\mathbb{F}_5$ so we have

$$\mathbb{F}_5[x]/(x^5 - x + 1) \cong \mathbb{F}_5[x]/(x^5 - x + 2) \cong \mathbb{F}_{5^5}.$$

The following theorem unveils an interesting way of forging two irreducible polynomials, yielding another irreducible polynomial of higher degree:

Theorem 3.2. *Let $\mathbb{F}$ be a finite field and let $f, g \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$, where $\deg f = m, \deg g = n$, $\gcd(m, n) = 1$ and $m, n > 1$. Then the polynomials*

$$h_\times(x) = \prod_{f(\alpha)=0} \prod_{g(\beta)=0} (x - \alpha\beta), h_+(x) = \prod_{f(\alpha)=0} \prod_{g(\beta)=0} (x - (\alpha + \beta))$$

are irreducible over $\mathbb{F}_q$ of degree mn, where the products range over all zeros of f, g in the splitting fields of f and g.

Proof. The statement is proved for $h_\times(x)$, the proof for $h_+(x)$ works analogously. Let α_1 be a zero of f in the splitting field $\mathbb{F}_{q^m}$ of f and let β_1 be a zero of f in the splitting field $\mathbb{F}_{q^n}$ of g. $(\alpha_1\beta_1)^{q^m-1} = \beta_1^{q^m-1} \in \mathbb{F}_q(\alpha_1\beta_1)$ since $\alpha_1 \in \mathbb{F}_{q^m}$ by theorem 2.2. Thus $(\beta_1^{q^m-1})^{q^{r-m}} = \beta_1^{q^r-q^{r-m}} = \beta_1^{-q^{m-r}} \in \mathbb{F}_q(\alpha_1\beta_1)$ where r is chosen so that r is a multiple of n greater than m. We claim that $m - r$ is not a multiple of n since otherwise $n \mid m$, contradiction. Thus $(\beta_1^{-q^{r-m}})^{-1} = \beta_1^{q^{r-m}}$ is a zero of g by theorem 2.2 belonging to $\mathbb{F}_q(\alpha_1\beta_1)$ and therefore $\beta_1 \in \mathbb{F}_q(\alpha_1\beta_1)$ by the same theorem and consequently $\alpha_1 \in \mathbb{F}_q(\alpha_1\beta_1)$. Thus $\mathbb{F}_q < \mathbb{F}_q(\alpha_1) < \mathbb{F}_q(\alpha_1\beta_1)$. By the tower law for finite field extensions we have

$$[\mathbb{F}_q(\alpha_1\beta_1) : \mathbb{F}_q] = [\mathbb{F}_q(\alpha_1\beta_1) : \mathbb{F}_q(\alpha_1)][\mathbb{F}(\alpha_1) : \mathbb{F}_q]$$

so $m = \deg(\alpha_1, \mathbb{F}_q) | \deg(\alpha_1\beta_1, \mathbb{F}_q)$ and in the same way $n = \deg(\beta_1, \mathbb{F}_q) | \deg(\alpha_1\beta_1, \mathbb{F}_q)$. Since m, n are relatively prime $mn | \deg(\alpha_1\beta_1, \mathbb{F}_q)$ and since

$$mn \geq [\mathbb{F}_q(\alpha_1, \beta_1) : \mathbb{F}_q] \geq [\mathbb{F}_q(\alpha_1\beta_1) : \mathbb{F}_q] = \deg(\alpha_1\beta_1, \mathbb{F}_q)$$

we have $mn = \deg(\alpha_1\beta_1, \mathbb{F}_q)$. Now, if we can show $h_\times(x) \in \mathbb{F}_q[x]$, $h_\times(x)$ must be irreducible since $\deg h_\times = mn$ and it has $\alpha_1\beta_1$ as a zero. First, observe that $\mathbb{F}_q(\alpha_1) \cap \mathbb{F}_q(\beta_1) = \mathbb{F}_q$, for if the intersection were greater, with an element $\gamma \notin \mathbb{F}_q$ then $\deg(\gamma, \mathbb{F}_q) > 1$ and

$$\deg(\gamma, \mathbb{F}_q) | \deg(\alpha_1, \mathbb{F}_q) = m, \deg(\gamma, \mathbb{F}_q) | \deg(\beta_1, \mathbb{F}_q) = n$$

contradicting the fact that m, n are relatively prime. Now

$$h_\times(x) = \prod_{f(\alpha)=0} \prod_{g(\beta)=0} (x - \alpha\beta) = \prod_{g(\beta)=0} \prod_{f(\alpha)=0} \beta(\beta^{-1}x - \alpha) = \prod_{g(\beta)=0} \beta^m f(\beta^{-1}x),$$

since $f(x) = \prod_{f(\alpha)=0}(x - \alpha)$. Thus $h_\times(x) \in (\mathbb{F}_q(\beta_1))[x]$, as $\mathbb{F}_q(\beta_1)$ is the splitting field of g, by theorem 2.2. In a similiar manner, one finds that $h_\times(x) \in (\mathbb{F}_q(\alpha_1))[x]$ so $h_\times(x) \in (\mathbb{F}_q(\alpha_1) \cap \mathbb{F}_q(\beta_1))[x] = \mathbb{F}_q[x]$. □

Example 3.3. Let $f(x) = x^2 + x + 1, g(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. These polynomials fulfil the hypothesis of the last theorem. We find their composition $h_\times(x)$. We see from the proof of the theorem that

$$h_\times(x) = \prod_{f(\alpha)=0} \alpha^3 g(\alpha^{-1}x)$$

where the product ranges over the zeros of $f(x)$ in $\mathbb{F}_4$, call them α_1, α_2. With this notation we find

$$h_\times(x) = (x^3 + \alpha_1^2 x + \alpha_1^3)(x^3 + \alpha_2^2 x + \alpha_2^3),$$

and after further simplification

$$h_\times(x) = x^6 + (\alpha_1^2 + \alpha_2^2)x^4 + (\alpha_1^3 + \alpha_2^3)x^3 + (\alpha_1^2\alpha_2^2)x^2 + (\alpha_1^2\alpha_2^3 + \alpha_1^3\alpha_2^2)x + \alpha_1^3\alpha_2^3.$$

Since $f(x) = (x + \alpha_1)(x + \alpha_2) = x^2 + x + 1$ we obtain $\alpha_1\alpha_2 = 1, \alpha_1 + \alpha_2 = 1$. Using these identities, we eventually find

$$h_\times(x) = x^6 + x^4 + x^2 + x + 1,$$

irreducible over $\mathbb{F}_2$ of degree 6.

We conclude this section by presenting a way of how one can obtain new irreducible polynomials from given ones via automorphisms.

Let $\mathbb{F}_q$ be a finite field and let σ be an automorphism of $\mathbb{F}_q$. Given such σ define

$$\overline{\sigma} : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$$

as

$$\overline{\sigma}(f(x)) = \sum_{k=0}^{n} \sigma(a_k)x^k$$

where $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{F}_q[x]$. We claim that $\overline{\sigma}$ is a homomorphism. Obviously, for polynomials $f(x), g(x)$ we have $\overline{\sigma}(f(x) + g(x)) = \overline{\sigma}(f(x)) + \overline{\sigma}(g(x))$. We now verify that $\overline{\sigma}(f(x)g(x)) = \overline{\sigma}(f(x))\overline{\sigma}(g(x))$ when $g(x)$ is a monomial ax^n and the claim follows since $\overline{\sigma}$ is an additive homomorphism. Suppose $f(x) = \sum_{k=0}^{n} a_k x^k$, then

$$\overline{\sigma}(f(x)ax^n) = \overline{\sigma}\left(\sum_{k=0}^{n} a \cdot a_k x^{k+n}\right) = \sum_{k=0}^{n} \sigma(a \cdot a_k)x^{k+n} = \sigma(a)x^n \sum_{k=0}^{n} \sigma(a_k)x^k = \overline{\sigma}(f(x))\overline{\sigma}(ax^n).$$

This shows that $\overline{\sigma}$ indeed is a homomorphism. Furthermore, $\overline{\sigma}$ is an isomorphism, since it has an inverse given by

$$\overline{\sigma}^{-1} = \overline{\sigma^{-1}}.$$

We can now state and prove a theorem on how one might produce new irreducible polynomials from known ones through automorphisms.

Theorem 3.4. *A polynomial $f(x) \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$ if and only if $\overline{\sigma}(f(x))$ is irreducible over $\mathbb{F}_q$, where $\overline{\sigma}$ is defined as above using any automorphism $\sigma : \mathbb{F}_q \to \mathbb{F}_q$.*

Proof. Suppose $f(x)$ is reducible, $f(x) = g(x)h(x)$, $\deg g, \deg h > 0$, then, since

$$\overline{\sigma}(f(x)) = \overline{\sigma}(g(x)h(x)) = \overline{\sigma}(g(x))\overline{\sigma}(h(x))$$

and σ is an automorphism, in particular $\sigma(a) \neq 0$ for $a \neq 0$, $\deg g = \deg \overline{\sigma}(g)$ and $\deg h = \deg \overline{\sigma}(h)$ which shows that $\overline{\sigma}(f(x))$ is reducible.

If $\overline{\sigma}(f(x))$ is reducible for some σ then as above $f(x) = \overline{\sigma}^{-1}(\overline{\sigma}(f(x)))$ is reducible. □

Now, if we start with fields $F = \mathbb{F}_{q^m} > \mathbb{F}_q = K$ and a non-trivial automorphism of F over K, for instance, $\sigma_i(\alpha) = \alpha^{q^i}$ for $1 \leq i < m$ and an irreducible polynomial $f(x) \in F[x]$ having not all coefficients in the set $F' \subset F$ of elements left fixed by σ_i, then we end up with a new irreducible polynomial given by $\overline{\sigma_i}(f(x))$. Later in the text we shall illustrate this by giving an example of how the latest theorem can be used to generate a new sequence of irreducible polynomials from a given one.

4 Sequences of irreducible polynomials

In this section a theorem on the construction of certain sequences of irreducible polynomials over finite fields shall be studied in detail. The goal is to present a proof of the following theorem:

Theorem 4.1. *Let q be the power of an odd prime p and let $f_1 \in \mathbb{F}_q$ be monic and irreducible over $\mathbb{F}_q[x]$ of degree m, with m even if $p \equiv 3 \mod 4$, such that $f_1(1)f_1(-1)$ is not a quadratic residue of $\mathbb{F}_q$, then the monic polynomials defined recursively by*

$$f_{n+1}(x) = (2x)^{m2^{n-1}} f_n\left(\frac{x^2+1}{2x}\right)$$

are all irreducible over $\mathbb{F}_q$.

This theorem is a slight modification of a theorem presented on page 45 of [8]. The statement of the theorem in [8] is identical to the one above, with the exception that the assumption m even if $p \equiv 3 \mod 4$ is dropped. As we will later see in this text, this assumption cannot be omitted.

Theorem 4.1 was proven in [2] by S.D. Cohen who expanded on results obtained by H. Meyn in [5]. We shall follow the approaches of these documents closely in this section, and study the arguments used in detail, in order to achieve a proof of theorem 4.1.

Firstly, we shall introduce important concepts used in both papers, before presenting a way of constructing sequences of irreducible polynomials over fields of characteristic 2 of growing degree. This will be followed by a section devoted to the proof of theorem 4.1, which concerns finite fields of odd characteristic.

4.1 The Q-transformation and the trace

One fruitful approach in the quest of finding sequences of irreducible polynomials is presented in [5]. The idea is to look at a certain transformation $Q : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$, $Q(f) = f^Q$ and determine conditions under which there is an inheritance of irreducibility when f is transformed to f^Q. The transformation is as follows:

Definition 4.2. Let $f \in \mathbb{F}_q[x]$ be a polynomial. Let $f^Q(x) = x^{\deg f} f(x+1/x)$ interpreted as an element in $\mathbb{F}_q(x)$, but actually an element of $\mathbb{F}_q[x]$. More precisely, if $f(x) = \sum_{k=0}^{n} a_k x^k$, $a_n \neq 0$, then $f^Q(x) = \sum_{k=0}^{n} a_k (x^2+1)^k x^{n-k}$. The mapping $f(x) \mapsto f^Q(x)$ will occasionally be referred to as the Q-transform.

Remark 4.3. Note that if $\deg f = n$ then $\deg f^Q = 2n$ and that $(f^Q)^* = f^Q$, i.e. f^Q is self-reciprocal.

Furthermore, if $f \in \mathbb{F}_q[x]$ and $a \in \mathbb{F}_q$ then we see from the definition of $f^Q(x)$ that we have

$$(af(x))^Q = af^Q(x).$$

More generally, if $f(x) = g(x)h(x)$, $g, h \in \mathbb{F}_q[x]$, then

$$f^Q(x) = x^{\deg f} f(x+1/x) = x^{\deg g} x^{\deg h} g(x+1/x)h(x+1/x) = g^Q(x)h^Q(x),$$

so that f^Q is irreducible only when f is.

There is also a correspondence between all polynomials of degree n and all self-reciprocal polynomials of degree n. If we count the polynomials of degree n over $\mathbb{F}_q$ we find that there are exactly $q^n(q-1)$. By the remark following definition 2.14 a polynomial $\sum_{k=0}^{2n} a_k x^k$ is self reciprocal if and only if $a_{2n-k} = a_k$ for all $0 \leq k \leq 2n$. Therefore, when constructing an irreducible polynomial of degree $2n$, the polynomial is determined by choosing $a_0, \ldots, a_n$ with the only restriction $a_0 \neq 0$. Thus, there are exactly $q^n(q-1)$ self-reciprocal polynomials of degree $2n$ over $\mathbb{F}_q$. Furthermore, if f is of degree n, as noted above f^Q is self-reciprocal of degree $2n$, and, as will now be shown, the mapping $f \mapsto f^Q$ is injective.

Suppose $f^Q(x) = g^Q(x)$, $f, g \in \mathbb{F}_q[x]$. Clearly f, g must have the same degrees, n say, so in other words, we have

$$x^n f(x + 1/x) = x^n g(x + 1/x).$$

Let $0 \neq \beta \in \overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$. In order to show injectivity, it suffices to show that $f(\beta) = g(\beta)$ and that $g(0) = f(0)$. Let $\alpha \in \overline{\mathbb{F}_q}$ be a zero of $x + 1/x = \beta \iff x^2 - \beta x + 1 = 0$. Then $\alpha \neq 0$ and

$$f^Q(\alpha) = g^Q(\alpha) \iff \alpha^n f(\alpha + 1/\alpha) = \alpha^n g(\alpha + 1/\alpha) \iff f(\beta) = g(\beta).$$

It remains to show that $f(0) = g(0)$, i.e. that the constant terms of f, g agree. But the constant term of $f(x)$ is the coefficient of the highest term in $f^Q(x)$, and likewise for g, and since $f^Q = g^Q$, $f(0) = g(0)$, so $f(x) = g(x)$ and $f \mapsto f^Q$ is injective (actually bijective, since domain and image are finite).

The next theorem plays an important role both in a construction of sequences of irreducible polynomials over fields of characteristic 2, as well as in the proof of theorem 4.1, which is our goal to prove. It gives a necessary and sufficient condition for when f^Q is irreducible if f is.

Theorem 4.4. (Lemma 5 of [5]). *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ with* $\deg f = n$. *Then f^Q is irreducible over $\mathbb{F}_q$ if and only if $g(x) = x^2 - \beta x + 1 \in \mathbb{F}_{q^n}[x]$ is irreducible over $\mathbb{F}_{q^n}$, where β is any zero of f.*

Remark 4.5. If $x^2 - \beta x + 1 \in \mathbb{F}_{q^n}[x]$ is irreducible for some zero β of $f(x)$ then it is irreducible for any other zero of $f(x)$. By theorem 2.2 the other zeros are $\beta^q, \ldots, \beta^{q^{n-1}}$ which can be expressed in terms of the automorphism $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ given by $\sigma(\alpha) = \alpha^q$ for $\alpha \in \mathbb{F}_{q^n}$ as $\sigma(\beta), \ldots, \sigma^{n-1}(\beta)$. Therefore $x^2 - \sigma^k(\beta)x + 1$ are all irreducible over $\mathbb{F}_{q^n}$ for $1 \leq k \leq n-1$ by theorem 3.4 which proves the claim.

Proof. Suppose $g(x)$ is irreducible over $\mathbb{F}_{q^n}$. Firstly, we show that 0 is not a zero of f^Q. If it would be, then the constant term of f^Q would be 0. But the constant term of f^Q is that of x^n in f, obviously non-zero. Now, let $\alpha \neq 0$ be a zero of f^Q. Our aim is to show that $\deg(\alpha, \mathbb{F}_q) = 2n = \deg f^Q$. Since $0 = f^Q(\alpha) = \alpha^n f(\alpha + 1/\alpha)$ we find that $f(\alpha + 1/\alpha) = 0$, since $\alpha \neq 0$. Let $\beta = \alpha + 1/\alpha$, $\deg(\beta, \mathbb{F}_q) = n$. Furthermore $g(\alpha) = 0$. Since $g(x)$ is assumed to be irreducible over $\mathbb{F}_{q^n}$, $\mathbb{F}_{q^n}[x]/(g(x))$ is a field, isomorphic to $(\mathbb{F}_q(\beta))(\alpha) = \mathbb{F}_q(\alpha)$ and we have, by the tower law for finite field extensions

$$[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q(\beta)][\mathbb{F}_q(\beta) : \mathbb{F}_q] = 2n$$

so $\deg(\alpha, \mathbb{F}_q) = 2n = \deg f^Q$ and we have deduced that f^Q must be irreducible.

If, on the other hand, $f^Q(x)$ is irreducible over $\mathbb{F}_q$, and α is a zero of f^Q, so that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = 2n$, then, by setting $\beta = \alpha + 1/\alpha$, $f(\beta) = 0$, we see that for $g(x) = x^2 - \beta x + 1$, $g(\alpha) = 0$. If g would be reducible α would be a zero of some linear polynomial of $\mathbb{F}_{q^n}[x]$ and so $\alpha \in \mathbb{F}_{q^n}$ contradicting that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = 2n$. □

Quite a lot of work is dedicated to transforming the above necessary and sufficient condition for when f^Q inherits irreducibility of f to a more applicable one. This is done through analyzing the irreducibility of $x^2 - \beta x + 1 \in \mathbb{F}_{q^n}[x]$ and the analysis depends strongly on whether the characteristic of the field is odd or not. So while the above theorem holds for any characteristic it will be transformed to give other conditions for inheritance of irreducibility depending on the characteristic of $\mathbb{F}_q$ as we shall later see.

In Meyn's paper [5] the notion of the *trace* of an element plays an important role in the search of sequences of irreducible polynomials over fields of characteristic 2, as it allows better usage of theorem 4.4. This notion is introduced here as it is valid for finite fields of any characteristic.

Definition 4.6. Let $\mathbb{F}_{q^m} = F, \mathbb{F}_q = K$ be finite fields. Let $\alpha \in F$. The *trace* of α over K is denoted and defined as

$$\mathrm{Tr}_{F/K}(\alpha) = \sum_{k=0}^{m-1} \alpha^{q^k}.$$

Remark 4.7. If $\alpha \in F > K$ then $\mathrm{Tr}_{F/K}(\alpha) \in K$. For let f be the minimal polynomial of α over K. Then $\deg f = d \mid m$, $F = \mathbb{F}_{q^m}$. By theorem 2.2 the elements $\alpha, \ldots, \alpha^{d-1}$ are the zeros of f. Now, by setting $\prod_{k=1}^{m-1}(x - \alpha^{q^k}) = g(x) = f(x)^{m/d} \in K[x]$, one sees that the second highest coefficient of g is $-\mathrm{Tr}_{F/K}(\alpha)$ so this element must be in K.

Alternatively, we observe that the trace of $\alpha \in F$ over K an element of K left invariant by all automorphisms of F over K. Thus $\mathrm{Tr}_{F/K}(\alpha) \in K$, by the theory of Galois.

In particular, if $\mathbb{F}_{q^m} = F, \mathbb{F}_q = K$ are finite fields, and the degree of the minimal polynomial of α over K is equal to m (so that $F = K(\alpha)$), then $-\mathrm{Tr}_{F/K}(\alpha)$ equals the coefficient of x^{m-1} in $f(x)$.

Some properties of the trace ([3] page 55):

- $\mathrm{Tr}_{F/K} : F \to K$ is linear (F considered a vector space over K).
- $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$, for all $\alpha \in F$.
- The trace function is *transitive*, i.e. if $K < F < L$ are finite fields fields and $\alpha \in L$ then $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha))$.

4.2 Sequences of irreducible polynomials over finite fields of characteristic 2

To be able to use theorem 4.4, one utilizes another irreducibility condition for $x^2-\beta x+1 \in \mathbb{F}_{2^n}[x]$, which is presented shortly. First, an example from [6] on how the trace can be used to show irreducibility of quadratic polynomials over fields of characteristic 2.

Theorem 4.8. *Let $F = \mathbb{F}_{2^k}$, $K = \mathbb{F}_2$, and let $f(x) = x^2 + x + \beta \in F[x]$. $f(x)$ has a zero in F, is not irreducible over F, if and only if $Tr_{F/K}(\beta) = 0$. In other words $f(x)$ is irreducible over F if and only if $Tr_{F/K}(\beta) = 1$.*

Proof. From theorem 2.11 we get that F has a normal basis over K, i.e. a basis of the form $\{\alpha^{2^i} : 0 \leq i < k\}$ for some $\alpha \in F$. So if there is a solution y of $f(x) = 0$, with $y \in F$, we may write $y = \alpha y_0 + \ldots + \alpha^{2^{k-1}} y_{k-1}, \beta = \alpha b_0 + \ldots + \alpha^{2^{k-1}} b_{k-1}$. Now

$$y^2 = (\alpha y_0 + \ldots + \alpha^{2^{k-1}} y_{k-1})^2 = \alpha^2 y_0^2 + \ldots + (\alpha^{2^{k-1}})^2 y_{k-1}^2$$

which is equal to $\alpha y_{k-1} + \alpha^2 y_1 \ldots + \alpha^{2^{k-1}} y_{k-2}$ since $y_i \in \mathbb{F}_2$ andless $(\alpha^{2^{k-1}})^2 = \alpha^{2^k} = \alpha$. By the condition that $y^2 + y = \beta$, and comparison of coefficients, we obtain $y_0 + y_{k-1} = b_0, y_1 + y_0 = b_1, \ldots, y_{k-1} + y_{k-2} = b_{k-1}$. Adding all those equations, we obtain $0 = \sum_{i=0}^{k-1} 2y_i = \sum_{i=0}^{k-1} b_i$. The claim is now that $\mathrm{Tr}_{F/K}(\beta) = \sum_{i=0}^{k-1} b_i$. By linearity of the trace $\mathrm{Tr}_{F/K}(\beta) = \sum_{i=0}^{k-1} b_i \mathrm{Tr}_{F/K}(\alpha^{q^i})$ and by the other property of the trace mentioned in remark 4.7 we have $\mathrm{Tr}_{F/K}(\alpha^{q^i}) = \mathrm{Tr}_{F/K}(\alpha)$ for all i in the sum. So, it only remains to show that $\mathrm{Tr}_{F/K}(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^i} = 1$, but this follows since $\mathrm{Tr}_{F/K}(\alpha) \in K$ and so $\mathrm{Tr}_{F/K}(\alpha) = 0$ or $\mathrm{Tr}_{F/K}(\alpha) = 1$ but the first situation cannot arise since $\{\alpha, \ldots, \alpha^{2^{k-1}}\}$ is a basis of F over K.

Now, suppose $\mathrm{Tr}_{F/K}(\beta) = 0$. Then we can construct solutions y of the equation by letting $y_0 = a, y_1 = a + b_1, y_2 = a + b_1 + b_2, \ldots, y_{m-1} = a + b_1 + \ldots + b_{m-1}$, $a = 0, 1$, as shown in [6]. □

We now turn to the promised irreducibility condition for $g(x) = x^2-\beta x+1 = x^2+\beta x+1$ over $\mathbb{F}_{2^n}$, aided by the last result.

Theorem 4.9. *Let $K = \mathbb{F}_2$ and $0 \neq \beta \in \mathbb{F}_{2^k} = F$. Then the equation $x^2 + \beta x + 1 = 0$ has a solution in F if and only if $\mathrm{Tr}_{F/K}(\frac{1}{\beta}) = 0$; consequently, $x^2 + \beta x + 1$ is irreducible over F if and only if $\mathrm{Tr}_{F/K}(\frac{1}{\beta}) = 1$).*

Proof. Suppose the equation $x^2 + x + \frac{1}{\beta}$ has solutions $\xi, \eta \in F$, a situation which occurs if and only if $\mathrm{Tr}_{F/K}(\frac{1}{\beta}) = 0$ by the previous theorem. Then, obviously, ξ, η are non-zero, $\xi\eta = \frac{1}{\beta}$, $\xi + \eta = 1$, and it is verified that $\frac{\xi}{\eta}$ is a solution of $x^2 + \beta x + 1 = 0$:

$$\left(\frac{\xi}{\eta}\right)^2 + \beta \cdot \frac{\xi}{\eta} + 1 = \frac{\xi^2 + \beta\xi\eta + \eta^2}{\eta^2} = \frac{(\xi + \eta)^2 + 1}{\eta^2} = 0.$$

Thus, if $\mathrm{Tr}_{F/K}(\frac{1}{\beta}) = 0$, then $x^2 + \beta x + 1 = 0$ has a solution in F.

Now suppose $x^2 + \beta x + 1 = 0$ has a solution in F. Since $\beta \neq 0$, this equation is equivalent to $\frac{1}{\beta}x^2 + x + \frac{1}{\beta} = 0$. Suppose this equation has a solution a. Then $\frac{a}{\beta}$ is a solution of $x^2 + x + \frac{1}{\beta^2} = 0$, which implies that $\mathrm{Tr}_{F/K}(\frac{1}{\beta^2}) = 0$, by the previous theorem. By the virtue of a property possessed by the trace $0 = \mathrm{Tr}_{F/K}(\frac{1}{\beta^2}) = \mathrm{Tr}_{F/K}(\frac{1}{\beta})$. □

The following theorem connects the most recent theorem with theorem 4.4 in order to obtain conditions for when irreducibility of f^Q is inherited by the irreducibility of f:

Theorem 4.10. (Theorem 6 of [5]). *Let $F = \mathbb{F}_{2^k}$, $k > 0$, $K = \mathbb{F}_2$, and let $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$ be irreducible over F. Then $f^Q(x)$ is irreducible over F if and only if $\mathrm{Tr}_{F/K}(a_1/a_0) = 1$.*

Proof. Let $L = \mathbb{F}_{2^{nk}}$. Let β be a zero of f, $\beta \in L$. By the previous theorem and theorem 4.4 $f^Q(x)$ is irreducible over F if and only if $\mathrm{Tr}_{L/K}(\frac{1}{\beta}) = 1$. f^* is irreducible over F by remark 2.15 and $f^*(1/\beta) = 0$ (recall that $f^*(x) = x^n f(1/x)$). Furthermore $f^*(x)/a_0$ is monic and irreducible over F of degree n with $1/\beta$ as a zero and therefore it is the minimal polynomial for $1/\beta$ over F. By the remark 4.7 we have $\mathrm{Tr}_{L/F}(1/\beta)$ is the coefficient of x^{n-1} in $f^*(x)/a_0$, namely a_1/a_0. Since the trace function is transitive, i.e. if $K < F < L$ are finite fields fields and $\alpha \in L$ then $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(\alpha))$, we find that

$$1 = \mathrm{Tr}_{L/K}(1/\beta) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(1/\beta)) = \mathrm{Tr}_{F/K}(a_1/a_0).$$

□

Remark 4.11. In $\mathbb{F}_2$, given an irreducible polynomial f, f^Q is irreducible if and only if the linear term of f has coefficient 1. And clearly, in any field of characteristic 2, the linear term of f must have non-zero coefficient a_1 in order for f^Q to be irreducible, since otherwise $Tr_{F/K}(a_1/a_0) = 0$, regardless of the value of $a_0 \neq 0$.

Example 4.12. Let α be a root of $x^3 + x + 1 \in \mathbb{F}_2[x]$, so that $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$. Then α, as can be verified, is a generator of $\mathbb{F}_8^*$. Then consider $x + \alpha \in \mathbb{F}_8[x]$, irreducible. $\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(1/\alpha) = 1$, so $f^Q(x)$ is irreducible over $\mathbb{F}_8$. However, $f^Q(x) = x^2 + \alpha x + 1$ and $\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\alpha/1) = 0$ so f^{Q^2} must be reducible over $\mathbb{F}_8$. Indeed

$$f^{Q^2} = x^4 + \alpha x^3 + x^2 + \alpha x + 1 = (x^2 + \alpha^5 x + \alpha^6)(x^2 + \alpha^6 x + \alpha).$$

In the light of the above example, we request conditions which assure that if a polynomial f satisfies the requirements of theorem 4.10, then f^Q also satisfies those requirements. It turns out, that it is sufficient to require an extra property of f, namely self-reciprocality.

Theorem 4.13. *Let $F = \mathbb{F}_{2^k}$, $k > 0$, $K = \mathbb{F}_2$. If a polynomial $f(x) = x^n + a_1 x^{n-1} + \ldots + a_1 x + 1 \in F[x]$ is self-reciprocal and irreducible over F and satisfies $Tr_{F/K}(a_1) = 1$, then $f^Q(x) = x^{2n} + b_1 x^{2n-1} + \ldots + b_1 x + 1 \in F[x]$ satisfies $Tr_{F/K}(b_1) = 1$.*

Proof. f being self-reciprocal implies that there is a certain symmetry in its coefficients, namely $a_k = a_{n-k}$ for $k = 0, \ldots, n$. Now we need only to observe that since f exhibits this symmetry in its coefficients the linear terms and constant terms of f^Q will be the same as for f, so $b_1 = a_1$. This is readily seen from the definition of f^Q, $f^Q(x) = \sum_{k=0}^{n} a_k (x^2 + 1)^k x^{n-k} = a_n + a_{n-1} x + \ldots = 1 + a_1 x + \ldots$. □

Now we have uncovered a weakness of the polynomial in the example preceding the last theorem, namely that the polynomial under scrutiny failed to be self-reciprocal.

Theorem 4.13 now ascertains that, if we start with a polynomial fulfilling all criteria, we can generate an infinite sequence of irreducible polynomials by repeatedly applying the Q-transform, since the assumptions in theorem 4.13 guarantee that theorem 4.10 can be applied repeatedly.

Example 4.14. Here follows some examples of when the theorem can be applied.

1. The simplest self-reciprocal, irreducible polynomial that comes to mind is $x+1 \in \mathbb{F}_{2^k}[x]$. We calculate the required trace in order to see whether or not theorems 4.10 and 4.13 apply, i.e. we must calculate the trace of 1:

$$\mathrm{Tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(1) = \sum_{i=0}^{k-1} 1^{2^j} = k$$

which is 1 if k odd and 0 if k even. So our theorems tell us that the Q-transform applied to $x+1$ yields infinitely many irreducible polynomials over $\mathbb{F}_{2^k}$ precisely when k is odd. The sequence originating from $x+1$ will be a sequence of irreducible polynomials of degree a power of 2 over any field $\mathbb{F}_{2^k}$ with k odd, and the first few elements are

$$x+1,\ x^2+x+1, x^4+x^3+x^2+x+1,\ x^8+x^7+x^6+x^4+x^2+x+1$$
$$x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+x^3+x^2+x+1$$

2. If we consider $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ where α is a zero of x^2+x+1, irreducible over $\mathbb{F}_2$, then

$$\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\alpha^{-1}) = \mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2}(\alpha) = \alpha+\alpha^2 = \alpha+\alpha+1 = 1$$

and so the theorems apply to the two self reciprocal irreducible polynomials

$$f_1(x) := x^2+\alpha x+1,\ f_2(x) := x^2+\alpha^{-1}x+1.$$

Irreducibility of $f_1(x), f_2(x)$ holds due to theorem 4.9 and thus we can iterate the Q-transform to those polynomials, and we obtain

$$f_1^Q(x) = x^4+\alpha x^3+x^2+\alpha x+1,$$
$$f_1^{Q^2}(x) = x^8+\alpha x^7+\alpha x^6+\alpha x^4+\alpha x^2+\alpha x+1.$$
$$f_2^Q(x) = x^4+\alpha^{-1}x^3+x^2+\alpha^{-1}x+1,$$
$$f_2^{Q^2}(x) = x^8+\alpha^{-1}x^7+\alpha^{-1}x^6+\alpha^{-1}x^4+\alpha^{-1}x^2+\alpha^{-1}x+1.$$

3. The only polynomial over $\mathbb{F}_8$ of degree 2 on which theorem 4.13 is applicable is x^2+x+1, since every other self reciprocal polynomial $x^2+\beta x+1$ fails to satisfy

$$\mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta^{-1}) = \mathrm{Tr}_{\mathbb{F}_8/\mathbb{F}_2}(\beta) = 1$$

which has to be satisfied in order to apply theorems 4.9 and 4.13.

A natural question now arises, is there always a choice for a polynomial satisfying theorem 4.13? This question is partially dealt with in the case of underlying field $\mathbb{F}_2$ in the paper by Meyn, [5], where it is shown that there exists a monic irreducible self reciprocal polynomial of degree $4m$ and the linear coefficient is 1 for every odd m.

4.3 Sequences of irreducible polynomials over finite fields of odd characteristic

While in the case of characteristic 2, the transform $f \mapsto f^Q$ succeeded in rendering sequences of irreducible polynomials, when certain conditions were imposed on the initial polynomial, it turns out that in the case of odd characteristic, we need to modify our transform slightly in order to generate such sequences over finite fields of general odd characteristic.

If $\mathbb{F}_q$ is of odd characteristic, one can obtain an irreducibility criterion for $g(x) = x^2 - \beta x + 1 \in \mathbb{F}_q[x]$, in order to use theorem 4.4 as follows. Since $g(x)$ is of degree 2 it is irreducible over $\mathbb{F}_q$ if and only if it has no zeros in $\mathbb{F}_q$. By rewriting $g(x) = 0$ as $(2x - \beta)^2 = \beta^2 - 4$, by rearrangements and completion of squares (enabled by odd characteristic), we see that $g(x)$ is irreducible over $\mathbb{F}_q$ if and only if $\beta^2 - 4$ is a quadratic non-residue of $\mathbb{F}_q$.

The above theorem and the preceding irreducibility criterion of $x^2 - \beta x + 1$ can be used to prove the following theorem of [5] (here proved in greater detail):

Theorem 4.15. *Let $\mathbb{F}_q$ be a finite field of odd characteristic and let $f(x) \in \mathbb{F}_q[x]$ be an irreducible monic polynomial over $\mathbb{F}_q$ of degree n. Then f^Q is irreducible over $\mathbb{F}_q$ if and only if $f(2)f(-2)$ is a quadratic non-residue of $\mathbb{F}_q$.*

Proof. By theorem 4.4 f^Q is irreducible if and only if $g(x) = x^2 - \beta x + 1$ is irreducible over $\mathbb{F}_{q^n}$, where β is a zero of f in $\mathbb{F}_{q^n}$ (the splitting field of f). This happens if and only if $\beta^2 - 4$ is a quadratic non-residue of $\mathbb{F}_{q^n}$, by theorem 2.12 if and only if $(\beta^2 - 4)^{(q^n-1)/2} = -1$.

By theorems 2.1 and 2.2, for $a \in \mathbb{F}_q$

$$f(a) = \prod_{\{\gamma : f(\gamma)=0\}} (a - \gamma) = \prod_{k=0}^{n-1} (a - \beta^{q^k}) = \prod_{k=0}^{n-1} (a - \beta)^{q^k} = (a - \beta)^{1+q+\ldots+q^{n-1}} = (a - \beta)^{(q^n-1)/(q-1)},$$

where the first product ranges over all zeros γ of f in the splitting field of f. Because of this we have $\beta^2 - 4$ is a quadratic non-residue of $\mathbb{F}_{q^n} \iff (\beta^2 - 4)^{(q^n-1)/2} = -1 \iff ((2 - \beta)(-2 - \beta))^{(q^n-1)/2} = -1 \iff (((2 - \beta)(-2 - \beta))^{(q^n-1)/(q-1)})^{(q-1)/2} = -1 \iff (f(2)f(-2))^{(q-1)/2} = -1 \iff f(2)f(-2)$ is a quadratic non-residue of $\mathbb{F}_q$. □

This theorem corresponds to theorem 4.10 in the sense that it provides transformation of the abstract necessary and sufficient condition of when f^Q inherits irreducibility from f given in theorem 4.4 into a more practical one. The condition in 4.10 was to verify a trace property of a certain element in the field of coefficients $\mathbb{F}_q$ of the polynomial under consideration. We succeeded in finding a similar condition here as well, namely to verify that a certain element in $\mathbb{F}_q$ is a quadratic non-residue. This should be compared to the task of using 4.4 for practical purposes, where one has to determine the irreducibility of a quadratic polynomial over an extension field of $\mathbb{F}_q$.

Using theorem 4.15 we can define our first sequence of irreducible polynomials over fields of odd characteristic.

Example 4.16. Let $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$, which is irreducible. Furthermore $f(2)f(-2) = f(-1)f(1) = -1$ which is a quadratic non-residue of $\mathbb{F}_3$. Now, if f^{Q^n} denotes repeated application of $f \mapsto f^Q$ n times, then

$$f^{Q^{n+1}}(2)f^{Q^{n+1}}(-2) = 2^{\deg f^{Q^n}}(-2)^{\deg f^{Q^n}} f^{Q^n}(2 + 2^{-1}) f^{Q^n}(-2 + (-2)^{-1}) = f^{Q^n}(-2) f^{Q^n}(2),$$

since $\deg f^{Q^n}$ is even (we define $f^{Q^0} := f$). Thus, by induction and theorem 4.15, the sequence defined by

$$f_{n+1}(x) = f_n^Q(x),$$

with $f_1(x) = f(x)$, is a sequence of irreducible polynomials over $\mathbb{F}_3$, $\deg f_n = 2^n$, the first few being

$$\begin{aligned} f_2(x) &= x^4 + 2x^3 + x^2 + 2x + 1, f_3(x) = x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^3 + 2x^2 + 2x + 1, \\ f_4(x) &= x^{16} + 2x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + 2x^9 + x^8 + 2x^7 + x^6 + x^4 + x^3 + x^2 + 2x + 1. \end{aligned}$$

We note that this process will succeed in general: Let $f(x) \in \mathbb{F}_{3^k}[x]$ be irreducible of even degree s.t. $f(2)f(-2) = f(-1)f(1)$ is a quadratic non-residue of $\mathbb{F}_{3^k}$. Then $f^{Q^n}(x)$ are irreducible for $n \in \mathbb{N}$. This is true because

$$f^{Q^{n+1}}(2)f^{Q^{n+1}}(-2) = 2^{\deg f^{Q^n}}(-2)^{\deg f^{Q^n}} f^{Q^n}(2 + 2^{-1}) f^{Q^n}(-2 + (-2)^{-1}) = f^{Q^n}(-2) f^{Q^n}(2)$$

so the claim follows by induction and theorem 4.15.

Observe that the induction step heavily depended on that the characteristic was 3.

Here is an example of a situation when repeated application of the Q-transform fails to produce more than one irreducible polynomial regardless of the starting polynomial.

Example 4.17. Let $f(x) \in \mathbb{F}_{5^k}[x]$, where $k \in \mathbb{N}_{>0}$, be irreducible, s.t. $f(2)f(-2)$ is a quadratic non-residue of $\mathbb{F}_{5^k}$. Thus, f^Q is irreducible by theorem 4.15. However,

$$f^Q(2)f^Q(-2) = 2^{\deg f}(-2)^{\deg f} f(2 + 2^{-1}) f(-2 + (-2)^{-1}) = f(0)^2$$

which is a quadratic residue, hence f^{Q^2} is not irreducible by theorem 4.15.

In order to prove theorem 4.1 we introduce a new polynomial transformation, involving the Q-transform.

Definition 4.18. Let $\mathbb{F}_q$ be a finite field of odd characteristic. Given a polynomial $f \in \mathbb{F}_q[x]$ of degree n, let $f^R(x) = 2^n f^Q(2^{-1}x) = (2x)^n f(2^{-1}(x + 1/x))$. Furthermore, for a polynomial f, let $\lambda(f) = f(1)f(-1)$.

Remark 4.19. Looking at $f^R(x) = 2^n f^Q(2^{-1}x)$ we see that the factor 2^n exists only for normalization purposes. The crucial difference between the R-transform and the Q-transform is the introduction of 2^{-1} in $f^Q(2^{-1}x)$ which shifts the zeros of the polynomial f somehow and will have a large impact on the success of producing infinite sequences of irreducible polynomials.

From $f^R(x) = (2x)^n f(2^{-1}(x + 1/x))$ it is seen that $f^R(x)$ is a self-reciprocal polynomial of degree twice that of $f(x)$. Since $f^R(x) = 2^n f^Q(2^{-1}x)$ we deduce from remark 4.3 that $f \mapsto f^R$ is an bijective mapping from the set of polynomials of degree n to the set of self-reciprocal polynomials of degree $2n$. This mapping will occasionally be referred to as the R-transform. Thus, every self reciprocal polynomial $f(x)$ of degree $2n$ over $\mathbb{F}_q$ can be written $f(x) = g^R(x)$ for some $g(x) \in \mathbb{F}_q[x]$. This will be used in the sequel. Furthermore, the R-transform of a product is the product of the R-transforms, so f^R is irreducible only if f is.

Since the R-transform of a monic polynomial f and the number of monic polynomials of degree n equals the number of self-reciprocal polynomials of degree n we have that f is monic if and only if f^R is monic.

The success of producing sequences of irreducible polynomials using the Q-transform relied heavily on the connection between $f(2)f(-2)$ and $f^Q(2)f^Q(-2)$ and in general it is hard to say sensible things about this connection. To illustrate this, if we start with an irreducible polynomial $f(x)$ over $\mathbb{F}_{11}$ where $f(2)f(-2)$ is a quadratic non-residue, then in order to apply the Q-transform once more, we must assert that $f^Q(2)f^Q(-2) = (-4)^{\deg f} f(2 + 2^{-1})f(-2 + (-2)^{-1}) = (-4)^{\deg f} f(3)f(-3)$ is a quadratic non-residue. In general, there need not be any connection between the non-quadratic nature of $f(2)f(-2)$ and the properties of $f(3)f(-3)$.

However, in the case of the R-transform, there is a rather clear connection between $\lambda(f)$ and $\lambda(f^R)$ on which our success of producing sequences of irreducible polynomials is heavily dependent.

Note that with our new notation, theorem 4.1 states precisely that the sequence defined by $f_{n+1}(x) = f_n^R(x)$ is a sequence of irreducible polynomials under certain conditions.

The following lemmata constitute the proof of theorem 4.1 in Cohen's paper [2]:

Lemma 4.20. *If f is a polynomial over $\mathbb{F}_q$, a finite field of odd characteristic p,* $\deg f = n$, *then*

- *if $p \equiv 1 \mod 4$ and if $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$, then $\lambda(f^R)$ is a quadratic non-residue of $\mathbb{F}_q$ as well.*
- *if n is even, and if $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$, then $\lambda(f^R)$ is a quadratic non-residue of $\mathbb{F}_q$ as well.*

Proof. $\lambda(f^R) = f^R(1)f^R(-1) = (-1)^n 2^{2n} f(1)f(-1) = (-1)^n 2^{2n}\lambda(f)$. If n is even, this clearly is a quadratic non-residue of $\mathbb{F}_q$. If $p \equiv 1 \mod 4$, -1 is a quadratic residue of $\mathbb{F}_q$, so $\lambda(f^R)$ is a quadratic non-residue. □

Lemma 4.21. *Let f be an irreducible polynomial over $\mathbb{F}_q$, a finite field of odd characteristic,* $\deg f = n$. *Then f^R is irreducible over $\mathbb{F}_q$ if and only if $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$.*

Proof. Let $g(x) = 2^n f(2^{-1}x)$, so that $f^R(x) = g^Q(x)$ i.e. if we show that $g^Q(x)$ is irreducible then $f^R(x)$ is irreducible. $g(x)$ is irreducible, for otherwise $2^n f(2^{-1}x) = r(x)s(x)$, for some $r(x), s(x) \in \mathbb{F}_q[x]$ with $0 < \deg r, s < n$, and $f(x) = 2^{-n}s(2x)g(2x)$, contradicting irreducibility of f. By theorem 4.15, $g^Q(x)$ is irreducible if and only if $g(2)g(-2)$ is a quadratic non-residue of $\mathbb{F}_q$ and $g(2)g(-2) = 2^{2n}\lambda(f)$ proves the claim. □

Those lemmata provide a proof of this version of theorem 4.1:

Theorem 4.22. *Let $f_1(x)$ be a monic irreducible polynomial over $\mathbb{F}_q$, a finite field of odd characteristic p,* $\deg f_1 = n$, *with n even if $p \equiv 3 \mod 4$, and with $\lambda(f)$ a quadratic non-residue of $\mathbb{F}_q$. Then the sequence of polynomials defined by*

$$f_{m+1}(x) = f_m^R(x),\ m \in \mathbb{N}_{>0}$$

is a sequence of monic irreducible polynomials over $\mathbb{F}_q$, with $\deg f_m = n2^{m-1}$.

Remark 4.23. However, it is *not* the case that the theorem succeeds if the required evenness of m if $p \equiv 3 \mod 4$ is neglected, as will now be shown. Take $x^3 + 2 \in \mathbb{F}_7[x]$, which is irreducible over $\mathbb{F}_7$, since it has no zeros in $\mathbb{F}_7$. Also $\lambda(f) = 3$, which is a quadratic non-residue of $\mathbb{F}_7$ since $3^3 = 27 = -1$ in $\mathbb{F}_7$. Now $f^R(x) = x^6 + 3x^5 + 2x^3 + 3x^2 + 1$, $\lambda(f^R) = 1$, and furthermore

$$\begin{aligned} f^{R^2}(x) &= x^{12} + 4x^{10} + 2x^9 - x^8 - x^7 - x^5 - x^4 + 2x^3 + 4x^2 + 1 \\ &= (x^6 + 3x^5 + 3x^3 + 2x^2 - x - 2)(x^6 + 4x^5 - x^4 + 2x^3 + 2x + 3) \end{aligned}$$

which is not irreducible!

Actually, the theorem will invariably fail if the initial polynomial is of odd degree when $\operatorname{char} \mathbb{F}_q \equiv 3 \mod 4$. For if we start with $f(x) \in \mathbb{F}_q[x]$ which is irreducible over $\mathbb{F}_q$ of odd degree m where $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$ then $\lambda(f^R) = (-1)^n 2^{2n} \lambda(f)$ which actually is a quadratic residue of $\mathbb{F}_q$ due remark 2.13.

The following theorem shows that every irreducible, self reciprocal polynomial of degree $2n$ arises by taking the R-transform of an irreducible polynomial of degree n on which theorem 4.22 can (possibly) be applied.

Theorem 4.24. *Let $f(x) \in \mathbb{F}_q[x]$ be monic, self-reciprocal and irreducible of degree $2n$ over the finite field $\mathbb{F}_q$. Then there is $g(x) \in \mathbb{F}_q[x]$, monic of degree n s.t. $g(x)$ is irreducible over $\mathbb{F}_q$ and*

$$f(x) = g^R(x), \lambda(g) \text{ a quadratic non-residue of } \mathbb{F}_q.$$

Proof. By remark 4.19 we find that $f(x) = g^R(x)$ for some monic $g(x)$ of degree n since the R-transform is a bijective mapping from the set of polynomials of degree n to the set of self-reciprocal polynomials of degree $2n$. In addition, the R-transform of a polynomial is irreducible only if the polynomial transformed is irreducible. Thus, $g(x)$ must be irreducible. Furthermore, since

$$g^R(x) = 2^n g((2^{-1}x))^Q = (2^n g(2^{-1}x))^Q := h^Q(x)$$

where $h(x) = 2^n g(2^{-1}x)$, is irreducible, we must have, by theorem 4.15, that $h(2)h(-2)$ is a quadratic non-residue of $\mathbb{F}_q$ and since

$$h(2)h(-2) = 2^n g(1) 2^n g(-1) = 2^{2n} \lambda(g)$$

we have deduced that $\lambda(g)$ is a quadratic non-residue of $\mathbb{F}_q$. □

From the previous theorem we can derive this corollary:

Corollary 4.25. *Let $\mathbb{F}_q$ be a finite field, where $\operatorname{char} \mathbb{F}_q = p \equiv 1 \mod 4$. If $f(x) \in \mathbb{F}_q[x]$ is self-reciprocal and irreducible of even degree, then $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$.*

Proof. By theorem 4.24 we can find $g(x) \in \mathbb{F}_q[x]$ irreducible s.t. $g(x)^R = f(x)$ where $\lambda(g)$ is a quadratic non-residue of $\mathbb{F}_q$. By lemma 4.20 we find that $\lambda(g^R) = \lambda(f)$ is a quadratic non-residue of $\mathbb{F}_q$. □

Now, at last, an example of when theorem 4.22 works:

Example 4.26. Consider the polynomial $x^2+2 \in \mathbb{F}_5$, irreducible, and let α satisfy $\alpha^2+2 = 0$ i.e. $\alpha^2 = 3$. Then $\mathbb{F}_{25} \cong \mathbb{F}_5(\alpha)$. As can be verified, α has order 8 in $\mathbb{F}_{25}^*$ and $2-\alpha$ has order 3. Thus $\theta := \alpha(2-\alpha) = 2(1+\alpha)$ has order $3 \cdot 8 = 24$ and generates $\mathbb{F}_{25}^*$.

We now attempt to find a polynomial $f(x)$ of the form $x+\beta$ where $\beta \in \mathbb{F}_{25}$ such that $\lambda(f) = (1+\beta)(-1+\beta)$ is a quadratic non-residue of $\mathbb{F}_{25}$ so that theorem 4.22 is applicable. It turns out that $\beta = \theta + 1$ is a good choice, since $-1+\beta = \theta$ is a quadratic non-residue and $1+\beta$ is a quadratic residue, as shown through the following calculation

$$(1+\beta)^{(25-1)/2} = (2(\alpha+2))^{12} = \ldots = 1.$$

Thus their product $\lambda(f)$ is a quadratic non-residue and theorem 4.22 applies: For instance

$$f^R(x) = 2(2^{-1}x+\beta)^Q = 2x(2^{-1}(x+1/x)+\beta) = x^2+2\beta x+1 = x^2+(1-\alpha)x+1$$

is irreducible over $\mathbb{F}_{25}$.

We now show that theorem 3.4 can be applied to obtain a "parallell" sequence of irreducible polynomials to the sequence generated by $f(x)$. As has been shown, $f^R(x) = x^2+(1-\alpha)x+1$ is irreducible. Now, there is a non-trivial automorphism of $\mathbb{F}_{25}$ over $\mathbb{F}_5$, namely the one defined by $\sigma(\theta) = \theta^5$. Hence

$$g(x) := \overline{\sigma}(f^R(x)) = x^2+\sigma(1-\alpha)x+1 = x^2+(1-\alpha^5)x+1 = x^2+(1+\alpha)x+1$$

is another irreducible (self reciprocal) polynomial of degree 2 over $\mathbb{F}_{25}$ by theorem 3.4.

Now, by theorem 4.24 it holds that $g(x) = h^R(x)$ for some irreducible polynomial $h(x)$ satisfying $\lambda(h)$ not a quadratic residue of $\mathbb{F}_{25}$. Since the R-transform is a bijective mapping from the set of polynomials of degree n to the set of self reciprocal polynomials of degree $2n$ we must have $h(x) \neq f(x)$ and thus $h(x)$ can be used to generate a "parallell" sequence of polynomials to the sequence generated by $f(x)$ through theorem 4.22.

It can indeed be calculated that

$$h(x) = x-2-2\alpha \neq f(x) = x-2+2\alpha$$

and that

$$\lambda(h) = (-1-2\alpha)(2-2\alpha) = 3\alpha$$

is a quadratic non-residue, since $(3\alpha)^{12} = \alpha^{12} = 3^6 = (3^2)^3 = (-1)^3 = -1$.

Theorem 4.24 allows us to deduce that there is $f(x) \in \mathbb{F}_q[x]$ of degree n with $\lambda(f)$ a quadratic non-residue of $\mathbb{F}_q$ to which theorem 4.22 may be applied, provided that there is a monic self-reciprocal polynomial of degree $2n$. The number of such polynomials is given by formulae presented in [5], but here we will be content with presenting a polynomial that exhibits properties regarding irreducible self reciprocal polynomials similar to those exhibited by $x^{q^n}-x$ regarding irreducible polynomials of degree $d \mid n$.

4.4 The polynomial $x^{q^n+1} - 1$

We will conclude the text by investigating the polynomial $x^{q^n+1} - 1$ whose irreducible factors are in close kinship with irreducible self-reciprocal polynomials. We will see that most of the irreducible factors of $x^{q^n+1} - 1$ are self-reciprocal and in order to show this we need the following two results on the identification and properties of self-reciprocal polynomials:

1. Let $f(x) \in \mathbb{F}_q[x]$ be irreducible of even degree and let its set of zeros be closed under inversion, i.e. if $f(\alpha) = 0$ then $f(\alpha^{-1}) = 0$ for $0 \neq \alpha$ in the splitting field of $f(x)$. Then $f(x)$ is self-reciprocal.

   Proof. From $f^*(x) = x^{\deg f} f(1/x)$ we see that $0 = \alpha^{\deg f} f(1/\alpha) = f^*(\alpha)$ so $f(x)$ and $f^*(x)$ have the same set of zeros. Thus, since f is irreducible and hence has only simple zeros, we may write $f(x) = cf^*(x)$ for some $c \in \mathbb{F}_q$. Using remark 2.15 we find $f^* = (cf^*)^* = c(f^*)^* = cf$ which gives $c^{-1} = c$ so that $c = \pm 1$. Since the degree of f is even of degree $2m$ say, there is a coefficient, namely that of x^m, call it a_m, left unchanged when mapping f to f^*. This means that we must have $a_m = ca_m$ so if $a_m \neq 0$ we must have $c = 1$. If $a_m = 0$ and $c = -1$ we get $a_k = -a_{2m-k}$ for $0 \leq k \leq 2m$ which implies $f(1) = 0$, contradiction to $f(x)$ being irreducible. Thus $c = 1$ and $f(x) = f^*(x)$. □

2. If $f(x) \in \mathbb{F}_q[x]$ is irreducible and self-reciprocal with $\deg(f) = m > 1$, then m is even.

   Proof. Let α be a zero of f in the splitting field $\mathbb{F}_{q^m}$ of f. Then, $\alpha \neq 0$ since f is irreducible. Since $0 = f(\alpha) = f^*(\alpha) = \alpha^n f(\alpha^{-1})$, α^{-1} is also a zero of f. Since we can pair each zero α with another zero α^{-1} and we have $\alpha^{-1} \neq \alpha$ (for otherwise $\alpha = \pm 1$) and since inverses are unique there must be an even number of distinct zeros of f in $\mathbb{F}_{q^m}$ and so m is even. □

Now let $\mathbb{F}_q$ be a finite field and consider the polynomial

$$h_{q,n}(x) = x^{q^n+1} - 1 \in \mathbb{F}_q[x].$$

We list some properties of $h_{q,n}(x)$:

- If $\alpha \in \mathbb{F}_q$ is a zero of $h_{q,n}(x)$ then $\alpha \in \{\pm 1\}$:

  $$\alpha^{q^n+1} - 1 = \alpha^{q^n-1}\alpha^2 - 1 = \alpha^2 - 1 = 0$$

  so α is a zero of $x^2 - 1$.

- Let $f(x)$ be irreducible and self reciprocal of degree $2n$, then $f(x) \mid h_{q,n}(x)$. Let α be a zero of $f(x)$. Then the zeros of $f(x)$ are $\{\alpha, \alpha^q, \ldots, \alpha^{q^{2n-1}}\}$and since $f(x)$ is self reciprocal there exists $1 \leq j \leq 2n - 1$ s.t. $\alpha^{-1} = \alpha^{q^j}$. We find that α is a zero of

  $$h_j(x) = x^{q^j+1} - 1.$$

For any polynomials $x^c - 1, x^d - 1$ we have $x^c - 1 \mid x^d - 1$ if $c \mid d$ because

$$(y-1)(y^{n-1} + y^{n-2} + \ldots + y^2 + y + 1) = y^n - 1$$

for y in any commutative ring and $n \in \mathbb{N}$. Apply with $y = x^c$ and $n = d/c$. Therefore

$$h_j(x) \mid x^{q^{2j}-1} - 1 = x^{(q^j+1)(q^j-1)} - 1$$

We now have that $f(x) \mid h_j(x)$ and $h_j(x) \mid x^{q^{2j}-1} - 1$ which implies $f(x) \mid x^{q^{2j}-1} - 1$. Thus, as seen in the proof of theorem 2.2, we get $2n \mid 2j$ and so $n \mid j$ and thus $n = j$ in other words $h_{q,n}(x) = h_j(x)$ so we have shown $f(x) \mid h_{q,n}(x)$.

- Now let $f(x)$ be an irreducible factor of $h_{q,n}(x)$ of degree $m \geq 2$. Let α be a zero of $f(x)$. Since $f(x) \mid h_{q,n}(x)$ we have that $\alpha^{q^n+1} = 1$ and thus $\alpha^{-1} = \alpha^{q^n}$. By theorem 2.2 the element α^{q^n} is a zero of $f(x)$. Thus the set of zeros of $f(x)$ is closed under inversion and by remark 2.15, $f(x)$ is self reciprocal of even degree, $m = 2d$ say. Since $f(x)$ divides $h_{q,n}(x)$ it divides $x^{q^{2n}-1} - 1$ as shown above and thus $2d \mid 2n$ and $d \mid n$.

What we can conclude from this information is that every irreducible factor of $h_{q,n}(x) = x^{q^n+1} - 1$ of degree 1 is either $x - 1$ or $x + 1$ (they actually occur with multiplicity at most 1, this can be shown by introducing the concept of the derivative of a polynomial, but will not be done here, see [1] for instance). Any irreducible factor of degree higher than 1 of $h_{q,n}(x)$ is of even degree and self reciprocal with degree dividing $2n$.

The properties of $h_{q,n}(x)$ suggest that if one wants to find irreducible self reciprocal polynomials of even degree one should investigate the divisors of $h_{q,n}(x)$.

What Meyn does in his paper [5] to determine a formula for the number of self-reciprocal irreducible polynomials of certain degree is very similar to what was done in theorem 2.21, namely to apply a Möbius inversion to a certain identity involving $h_{q,n}(x)$, in particular, there are self-reciprocal irreducible polynomials of degree 4 over any $\mathbb{F}_p$ where p is prime congruent 3 modulo 4, which implies that there are suitable starting polynomials for theorem 4.22 of degree 2.

The following argument shows that there are suitable starting polynomials of degree 1 over $\mathbb{F}_p$, p prime and $p \equiv 1 \mod 4$:

We seek a polynomial $f(x) = x + \alpha$ s.t. $\lambda(f)$ is a quadratic non-residue of $\mathbb{F}_p$ i.e. s.t. $\lambda(f) = \alpha^2 - 1$ is a quadratic non-residue. Thus, it suffices to find $\beta \in \mathbb{F}_p$ s.t. $\beta = \alpha^2$ is a quadratic residue but $\beta - 1 = \alpha^2 - 1$ is not. Suppose for a contradiction that there is no such β. Then, for every β that is a quadratic residue, $\beta - 1$ is a quadratic residue as well. Hence the set $\{\beta - n : n \in \mathbb{N}\}$ must consist only of quadratic residues. However, $\{\beta - n : n \in \mathbb{N}\} = \mathbb{F}_p$ which is a contradiction, since by remark 2.13 there are exactly $(p-1)/2 > 0$ quadratic non-residues of $\mathbb{F}_p$.

We are now guaranteed the existence of polynomials satisfying all requirements of theorem 4.22 for any field $\mathbb{F}_p$, p prime. Consequently, it is possible to generate infinite sequences of irreducible polynomials over $\mathbb{F}_p[x]$, p prime, which suffices if one wants to find explicit descriptions of certain field extensions of $\mathbb{F}_p[x]$.

To conclude the text, we observe that even though we have no explicit starting polynomial for the application of theorem 4.22 in any given case we have a good candidate polynomial $h_{q,n}(x)$ to look for such in its set of divisors. A task of this sort can be given to a computer and seems to be a rather small effort when the reward is an entire infinite sequence of irreducible polynomials!

References

[1] A. A. Albert *Fundamental concepts of higher algebra*, The University of Chicago Press, 1956.

[2] S. D. Cohen *The explicit construction of irreducible polynomials over finite fields*, Designs, codes, and cryptography vol 2, 1992.

[3] R. Lidl, H. Niederreiter *Finite Fields. Encyclopedia of Mathematics and its applications 20*, Cambridge University Press, 2008.

[4] Lars-Åke Lindahl *Linjär Algebra*, Fjärde upplagan, Matematiska institutionen, Uppsala Universitet, 2009.

[5] H. Meyn *On the Construction of Irreducible Self-Reciprocal Polynomials Over Finite Fields*, Applicable algebra in engineering, communication and computing vol 1, 1990.

[6] F. J. MacWilliams, N. J. A. Sloane *The theory of error correcting codes*, North-Holland, 1978.

[7] I. Niven, H. S. Zuckerman, H. L. Montgomery *An introduction to the theory of numbers*, Wiley, Fifth Edition, 1991.

[8] I. Shparlinski: *Finite Fields. Theory and computation*, Kluwer Academic Publishers, 1999.