A Generalized Counting and Factoring Method for Polynomials over Finite Fields

Ronald C. Mullin
Joseph L. Yucas
and
Gary L. Mullen

Abstract

We discuss a transform on the set of rational functions over the finite field F_q. For a subclass of these functions, the transform yields a polynomial and its factorization as a product of the set of monic irreducible polynomials all of which share a common property P that depends on the choice of rational function. A general formula is derived from the factorization for the number of monic irreducible polynomials of degree n having property P. However it is also possible in some instances to exploit the properties of the factorization to obtain a "closed" form of the answer more directly. We illustrate the method with four examples, two of which appear in the literature. In particular, we give alternative proofs for a result of L. Carlitz on the number of monic irreducible self-reciprocal polynomials and a remarkable result of S. D. Cohen on the number of $(r, m)-$polynomials, that is, monic irreducible polynomials of the form $f(x^r)$ of degree mr. We also give a generalization of the factorization of $x^{q-1} - 1$ over F_q that includes the factorization of $x^{(q-1)^2} - 1$. The new results concern translation invariant polynomials, which lead to a consideration of the orders of elements in $\overline{F}_q$, the algebraic closure of F_q. We show that there are an infinite number of $\theta \in \overline{F_q}$ such that $ord(\theta)$ and $ord(r(\theta))$ are related, in the sense that given one, one can infer information about the other.

1 Introduction

For q a prime power, let F_q denote the finite field of order q. In this paper we discuss a general method of counting irreducible polynomials with various properties over finite fields. In particular, we provide a single framework with which to obtain counting results concerning the number of monic self-reciprocal, and translation invariant irreducible polynomials over finite fields, as well as results concerning quadratically irreducible and other kinds of irreducible polynomials over finite fields. Our method, while much more general, is reminiscent of the following example.

For a positive integer $n \geq 1$ consider the polynomial $C_q(n,x) = x^{q^n} - x \in F_q[x]$. It is well known that

$$x^{q^n} - x = \prod_{\alpha \in F_{q^n}} (x - \alpha) = \prod_{d|n} MI(q,d),$$

where $MI(q,d)$ denotes the product of all monic irreducible polynomials of degree d over F_q, see for example Theorem 3.20 of [8]. While the above factorizations are of interest in themselves, the more important use is that they allow us to obtain a formula for the number of monic irreducible polynomials of degree n over F_q.

By taking degrees on both sides of this equation and then applying Möbius inversion, this equation leads to the well known formula

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

for the number of monic irreducible polynomials of degree n over the finite field F_q, where of course μ is the Möbius function from elementary number theory.

Another similar formula is the following:

Let $SMRI(q,k)$ denote the set of monic irreducible self-reciprocal polynomials of degree k over F_q. Then Carlitz [2] showed that

$$\#SRMI(q,2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)(q^{n/d} - 1)$$

if q is odd, and

$$\#SRMI(q,2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d}$$

if q is even.

We also have that if $n = 2^v t$, $v \geq 0$, t odd, then

$$\#SMRI(q,2n) = \begin{cases} \frac{1}{2n}(q^n - 1) & n = 1,\ q \text{ odd}, \\ \frac{t}{2n} N_{q^{n/t}}(t) & \text{otherwise.} \end{cases}$$

We note that in [3], the author obtains the above formulae using a simpler method in addition to obtaining other results. The main point of this paper is that it contains a method of producing factorizations and enumerative formulas, both old and new, from a unified theory. In this regard we need two concepts, replicators which are studied in section 2 and k-normal rational functions which are discussed in section 3. The main result of this paper occurs in section 4 and several illustrative special cases are briefly discussed in section 5. In section 6 we discuss polynomials which are quadratically irreducible.

The following notation and terminology will be used throughout the remainder of this paper. The ring of polynomials in a single variable x with coefficients in F_q will be denoted by $F_q[x]$ and $F_q(x)$ will denote the field of rational functions over F_q. By a rational function $r = f/g$, we mean a function for which $g \neq 0$ and r is *reduced* so that $(f, g) = 1$. The *degree* of r is defined to be the maximum of the degrees of the polynomials f and g.

2 Replicators

A rational function $r(x) = f(x)/g(x)$ over F_q is said to be a *replicator* over F_q if for every $n \geq 1$, $x^{q^n-1} - 1$ divides $f(x)^{q^n} - f(x)g(x)^{q^n-1}$. In this case, we write

$$f(x)^{q^n} - f(x)g(x)^{q^n-1} = (x^{q^n-1} - 1)\hat{r}(n, x)$$

for some polynomial $\hat{r}(n, x) \in F_q[x]$. The polynomial $\hat{r}(n, x)$ is said to be the *n-th order transform* of $r(x)$.

As an example let $r(x) = x^2$. Since $(x^2)^{q^n} - x^2 = (x^{q^n-1} - 1)(x^{q^n+1} + x^2)$, we see that $r(x)$ is a replicator over F_q for every q and the n-th order transform of $r(x)$ is $x^{q^n+1} + x^2$. We will see later that one can replace x^2 above with any polynomial and still obtain a replicator. On the other hand, the rational function $r(x) = x/(x - 1)$ is not a replicator over F_q for any q since $x - 1$ does not divide $x^{q^n} - x(x - 1)^{q^n-1}$.

We now proceed with some general remarks on replicators.

Lemma 1

$$x^{(q^n-1)k} - 1 = (x^{q^n-1} - 1)\sum_{j=0}^{k-1} x^{(q^n-1)j}$$

Proof: The sum telescopes.

■

For $g \in F_q[x]$ let

$$I_g = \{f \in F_q[x] : x^{q^n-1} - 1 \text{ divides } f^{q^n} - fg^{q^n-1} \text{ for all n}\}.$$

That is, I_g is the collection of all polynomials f for which f/g is a replicator.

Proposition 2 *I_g is an ideal of $F_q[x]$.*

Proof: If $f_1^{q^n} - f_1 g^{q^n-1} = (x^{q^n-1}-1)h_1$ and $f_2^{q^n} - f_2 g^{q^n-1} = (x^{q^n-1}-1)h_2$, then

$$\begin{aligned}(f_1+f_2)^{q^n} - (f_1+f_2)g^{q^n-1} &= f_1^{q^n} + f_2^{q^n} - f_1 g^{q^n-1} - f_2 g^{q^n-1} \\ &= (x^{q^n-1}-1)(h_1+h_2).\end{aligned}$$

Also, if $f^{q^n} - fg^{q^n-1} = (x^{q^n-1}-1)h$ then

$$\begin{aligned}(x^k f)^{q^n} - x^k f g^{q^n-1} &= x^k(x^{(q^n-1)k} f^{q^n} - f g^{q^n-1}) \\ &= x^k(x^{(q^n-1)k} f^{q^n} - f^{q^n} + f^{q^n} - f g^{q^n-1}) \\ &= x^k(f^{q^n}(x^{(q^n-1)k} - 1) + (x^{q^n-1}-1)h) \\ &= x^k(x^{q^n-1}-1)(f^{q^n}\sum_{j=0}^{k-1} x^{(q^n-1)j} + h)\end{aligned}$$

by Lemma 1.

■

Proposition 3 *Suppose that a polynomial $g \in F_q[x]$ can be written $g(x) = x^k p(x)$ with $p(0) \neq 0$ and $p(x)$ square-free. Then $I_g =< p >$, the principal ideal generated by p.*

Proof: First notice that

$$p^{q^n} - pg^{q^n-1} = p^{q^n} - x^{(q^n-1)k}p^{q^n} = -p^{q^n}(x^{(q^n-1)k} - 1).$$

By Lemma 1 we see that $p \in I_g$ and hence $< p > \subseteq I_g$. Suppose $f \in I_g$ and let r be an irreducible factor of p. Let $d = deg(r)$. Then there exists $h \in F_q[x]$ such that $f^{q^d} - fg^{q^d-1} = (x^{q^d-1}-1)h$, i.e., $f(f^{q^d-1} - g^{q^d-1}) = (x^{q^d-1}-1)h$. Since r divides $x^{q^d-1}-1$ and r divides g we see that r divides f. Consequently, p divides f and $I_g \subseteq < p >$.

■

Corollary 4 *If $g = x^k$, $k \geq 0$, then f/g is a replicator for every $f \in F_q[x]$. In particular, every polynomial is a replicator over F_q for every q.*

For a fixed positive integer n, define the mapping $\phi : F_q[x] \to F_q[x]$ by

$$\phi(f) = \hat{f}(n, x).$$

Proposition 5 *The mapping ϕ is linear.*

Proof: For $f_1, f_2 \in F_q[x]$,

$$\frac{(f_1+f_2)^{q^n}-(f_1+f_2)}{x^{q^n-1}-1} = \frac{f_1^{q^n}-f_1}{x^{q^n-1}-1} + \frac{f_2^{q^n}-f_2}{x^{q^n-1}-1}.$$

Also for $a \in F_q$,

$$\frac{(af)^{q^n}-af}{x^{q^n-1}-1} = \frac{af^{q^n}-af}{x^{q^n-1}-1} = a\frac{f^{q^n}-f}{x^{q^n-1}-1}.$$

■

In the next proposition we compute the n-th order transform for any polynomial.

Proposition 6 *Suppose $f = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ is in $F_q[x]$. Then*

$$\hat{f}(n,x) = \sum_{k=1}^{m} a_k x^k \sum_{j=0}^{k-1} x^{(q^n-1)j}.$$

Proof: By the previous proposition it suffices to compute $\phi(x^k)$.

$$\phi(x^k) = \frac{x^{q^n k}-x^k}{x^{q^n-1}-1} = x^k\frac{x^{(q^n-1)k}-1}{x^{q^n-1}-1} = x^k\sum_{j=0}^{k-1}x^{(q^n-1)j}$$

by Lemma 1.

■

3 K-normal rational functions

Let k be a positive integer. A rational function $r(x) = f(x)/g(x)$ over F_q is said to be k-normal if for every $n \geq 1$ and for each $\lambda \in F_{q^n}$, the degrees of the factors of the associated polynomial $f(x)-\lambda g(x)$ divide k, and for some λ, at least one factor has degree equal to k. In particular, if $f(x)-\lambda g(x)$ is irreducible for some λ and $f(x)-\lambda g(x)$ is either irreducible or factors into linear factors for all other λ, then $r(x)$ is k-normal, where k is the degree of $r(x)$.

As examples, linear rational functions are trivially seen to be 1-normal and quadratic rational functions are 1 or 2-normal over F_q for every q.

If q is a prime power, let r be a divisor of $q-1$. Then $f(x) = x^r$ is r-normal over F_q. This fact is a corollary of the following lemma.

Lemma 7 *Let q be a prime power. Let λ be an element of order e in F_q^*, and let r be a divisor of $q-1$. Let $d = (r,(q-1)/e)$, and let $\tilde{r} = r/d$. Then there exist distinct elements $\delta_0, \delta_1, \ldots, \delta_{d-1} \in F_q$ such that $x^r - \lambda = \prod_{j=0}^{d-1}(x^{\tilde{r}} - \delta_j)$, where δ_j is a primitive d^{th} root of unity in F_q^* and $x^{\tilde{r}} - \delta_j$ is irreducible over F_q.*

Proof: Suppose that $\lambda \in F_q^*$ and α is a generator of F_q^*. Since λ has order e, then λ can be written as $\lambda = \alpha^{(\frac{q-1}{e})k}$ where $(e,k) = 1$. Note that by the definition of d, $(q-1)/de$ is an integer.

For the factorization of $x^r - \lambda$, let $\delta = \alpha^{(\frac{(q-1)}{de})k}$. Now $\omega = \alpha^{\frac{q-1}{d}}$ is a primitive d^{th} root of unity in F_q^*, so let $\delta_j = \alpha^{(\frac{(q-1)}{de})k}\omega^j$, $j = 0, 1, \ldots, d-1$. The δ_j are distinct, and since $\delta_j^d = \lambda$, then

$$\begin{aligned} x^r - \lambda &= (x^{\tilde{r}})^d - \lambda \\ &= \prod_{j=0}^{d-1}(x^{\tilde{r}} - \delta_j). \end{aligned}$$

It remains to show that $x^{\tilde{r}} - \delta_j$ is irreducible over F_q for $j = 0, 1, \ldots d-1$. Let h_j denote the order of $\delta_j = \delta\omega^j$. Note that if $q \equiv 3 \pmod 4$, then $4 \nmid r$. Therefore, in order to show reducibility, it is sufficient to show that if s is a prime that divides $\tilde{r}$, then s divides h_j but not $(q-1)/h_j$ (see [8] Theorem 3.75, p.124).

Let $\eta = \alpha^{\frac{q-1}{de}}$, so η has order de. We first show that $x^{\tilde{r}} - \eta$ is irreducible over F_q. Let s be a prime that divides r, and suppose that ℓ, u, and v are such that $s^\ell || q-1$, $s^u || e$, and $s^v || r$. Then $s^{\ell-u} || (q-1)/e$. If $v \leq \ell - u$, then $s^v || d$, and $s|\not{\tilde{r}}$. This is always the case if $u = 0$, so the any prime divisor of $\tilde{r}$ is also a divisor of e, and therefore these are the only primes that play a role in deciding the irreducibility of $x^{\tilde{r}} - \delta_j$. On the other hand, if $v > \ell - u$, then $s^{\ell-u} || d$, and $s^\ell || de$, and $s | \tilde{r}$, but $s \nmid (q-1)/de$. Since every prime that divides $\tilde{r}$ also divides r, then $x^{\tilde{r}} - \eta$ is irreducible.

Now consider the irreducibility of $x^{\tilde{r}} - \delta_j$. Note that $\delta_j = \alpha^{(\frac{q-1}{de})ej+k}$, and the order of δ_j depends on any prime divisors of $ej + k$ that also divide de. However it is still possible to show that $x^{\tilde{r}} - \delta_j$ is irreducible over F_q, since we need only consider primes that divide e and $ej + k$. But if s is prime that divides e, then $s \nmid (ej + 1)$ since $(e,k) = 1$. Therefore $x^{\tilde{r}} - \delta_j$ is irreducible, as required.

■

Corollary 8 *Let q be a prime power, and let r be a divisor of $q-1$. Then $f(x) = x^r$ is r-normal over F_q.*

Proof: Suppose that $r | q-1$ and that $\lambda \in F_{q^n}$, and consider $g = x^r - \lambda$. If $\lambda = 0$, then all the irreducible factors of g are of degree one. If $\lambda \neq 0$, then by the previous lemma, all irreducible factors of g have degree r/d for some divisor d of r, as required.

■

The proof of the following is immediate.

Corollary 9 *Let q be a prime power and λ be an element of order e in F_q^*, and $f = (q-1)/e$. Then there exist distinct elements $\delta_0, \delta_1, \ldots, \delta_{f-1} \in F_q$ such that $x^{q-1} - \lambda = \prod_{j=0}^{f-1}(x^e - \delta_j)$, where $x^e - \delta_j$ is irreducible.*

Proposition 10 *The polynomial $x^q - x$ is q-normal over F_q.*

Proof: This follows from the fact that the polynomial $x^q - x - \lambda$ factors according to Theorem 3.80 of [8], into irreducible polynomials whose degrees divide q.

■

4 The main theorem

For a polynomial $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ over F_{q^n} we define the following sequence of polynomials:

$$p^{(j)}(x) = x^m + a_{m-1}^{q^j} x^{m-1} + \cdots + a_1^{q^j} x + a_0^{q^j}.$$

Notice that $p^{(s)}(x) = p(x)$ where s is the least common multiple of the degrees of the coefficients of $p(x)$.

Define the spin $S_p(x)$ of the polynomial $p(x)$ by

$$S_p(x) = \prod_{j=0}^{s-1} p^{(j)}(x).$$

It is not hard to check that the following lemma holds.

Lemma 11 *For polynomials $f, g \in F_q[x]$, the spin of the polynomial $f(x) - \lambda g(x)$ is the polynomial $\prod_{i=1}^{d} f(x) - \lambda^{q^i} g(x)$, where d is the degree of λ.*

Lemma 12 *Suppose $p(x)$ is an irreducible polynomial over F_{q^n} of degree d and let $\alpha \in F_{q^{dn}}$ be a root of $p(x)$. Then $S_p(x)$ is the minimal polynomial of α over F_q.*

Proof: First notice that $p(x)$ factors as $p_1(x)p_2(x)$ if and only if $p^{(j)}(x)$ factors as $p_1^{(j)}(x)p_2^{(j)}(x)$, and hence $p^{(j)}(x)$ is irreducible for each j. Next, notice that the d distinct roots of $p^{(j)}(x)$ are $\alpha^{q^j}, \alpha^{q^{n+j}}, \cdots, \alpha^{(d-1)n+j}$. Hence $S_p(x)$ has the same roots as the minimal polynomial of α over F_q. Since these roots are distinct, we have equality.

■

We now obtain the following generalization of Theorem 3.7 of [9].

Lemma 13 *Let $f, g \in F_q[x]$ and suppose $\lambda \in F_{q^n}$ has degree d and minimal polynomial $h(x)$ over F_q. Then the factorization of $g^d h(f/g)$ into irreducible factors over F_q is given by $\prod_p S_p(x)$, where p ranges over all irreducible factors of $f - \lambda g$.*

Proof: The polynomial $h(x)$ has the factorization $h(x) = \prod_{i=1}^{d}(x - \lambda^{q^i})$ over the extension field F_{q^n}. Thus

$$g^d h(f/g) = g^d \prod_{i=1}^{d}(f(x)/g(x) - \lambda^{q^i}) = \prod_{i=1}^{d}(f - \lambda^{q^i} g) = \prod_{p} S_p(x).$$

■

Now let $r(x) = f(x)/g(x)$ be a k-normal replicator over F_q and suppose $p(x)$ is an irreducible factor of $f - \lambda g$ for $\lambda \in F_{q^n}$ of degree d with minimal polynomial $h(x)$ over F_q. We say that $S_p(x)$ is hard for $r(x)$ if the degree of $S_p(x)$ does not divide n.

Write

$$f^{q^n} - f g^{q^n - 1} = (x^{q^n - 1} - 1)G(n, x)\bar{r}(n, x),$$

where $\bar{r}(n, x)$ is the factor of $f^{q^n} - f g^{q^n - 1}$ of largest degree which is squarefree and satisfies $(C_q(n, x), \bar{r}(n, x)) = 1$. Further let $G(n) = deg(G(n, x))$.

Let $HMI(q, n, r(x))$ denote the collection of all monic irreducible polynomials of degree n which are hard for $r(x)$. Then we obtain the following factorization of $\bar{r}(n, x)$.

Theorem 14 *Let $r(x)$ be a k-normal replicator over F_q of degree m. Then*

$$\bar{r}(n, x) = \prod h(x), (*)$$

where the product is over all $h(x) \in HMI(q, d, r(x))$ with d dividing n but d not dividing n/k.

Proof: Recall that

$$x^{q^n} - x = \prod_{d|n} h(x)$$

where $h(x)$ runs over all monic irreducible polynomials of degree d dividing n. Hence

$$f^{q^n} - f g^{q^n - 1} = g^{q^n}((f/g)^{q^n} - f/g)$$

$$= g^{q^n} \prod_{d|n} h(f/g) = \prod_{d|n} g^{q^d} h(f/g) = \prod_{d|n} \prod_{p} S_p(x)$$

by the previous lemma. Consequently,

$$(x^{q^n - 1} - 1)G(n, x)\bar{r}(n, x) = \prod_{d|n} \prod_{p} S_p(x).$$

Dividing each side by $(x^{q^n-1}-1)G(n,x)$ yields the theorem.

■

We now obtain the following counting formula.

Corollary 15

$$\#HMI(q,kn,r(x)) = \frac{1}{kn} \sum_{\substack{d|n \\ d\nmid(n/k)}} \mu(n/d)[(m-1)q^n - G(d)+1]$$

$$= \frac{1}{kn} \sum_{\substack{d|n \\ k\nmid d}} \mu(d)[(m-1)q^{n/d} - G(n/d)+1].$$

Proof: By taking degrees of equation (*) we have

$$mq^n - (q^n-1) - G(n) = \sum_{\substack{d|n \\ d\nmid(n/k)}} dN(d),$$

where $N(d)$ is the number of monic irreducible polynomials over F_q of degree d which are hard for $r(x)$. Applying Möbius inversion leads to the corollary.

■

A notation in a summation of the form $\sum_{\substack{d|n \\ d\nmid k}} F(n,d)$ can be simplified when k is a prime power. Note that n can be written uniquely as $n = k^a n_1$ where $a \geq 0$ and $k \nmid n_1$, and let n_1 be called the $k-free$ part of n, written $k-free(n)$. Then by definition,

$$\sum_{\substack{d|n \\ d\nmid k}} F(n,d) = \sum_{d|k-free(n)} F(n,d) = \sum_{d|n_1} F(k^a n_1, d).$$

In particular, if q is a prime power, then

$$\sum_{d|q-free(n)} \mu(d)q^{n/d} = \sum_{d|n_1} \mu(d) q^{k^a n_1},$$

so

$$\sum_{d|q-free(n)} \mu(d)q^{n/d} = n_1 N_{q^{k^a}}(n_1) = n_1 N_{q^{n/n_1}}(n_1).$$

5 Special cases

A polynomial $f \in F_q[x]$ is said to be translation invariant if $f(x+\alpha) = f(x)$ for all $\alpha \in F_q$.

1. Let $TIMI(q,m)$ denote the set if all monic irreducible translation invariant polynomials of degree m in $F_q[x]$. The following theorem is useful for calculating the cardinality of $TIMI(q,m)$.

Theorem 16 *Let f be an irreducible translation-invariant polynomial of degree m in $F_q[x]$. Then there is an irreducible polynomial $g \in F_q[x]$ such that $f(x) = g(x^q - x)$.*

Proof: Suppose that $f \in F_q[x]$ is irreducible and translation-invariant of degree n. Let $R \subset F_{q^n}$ denote the set of roots of f. Let θ be a root of f, and let $X(\theta) = \{\theta+\alpha : \alpha \in F_q\}$ and $X^*(\theta) = \{\theta+\alpha : \alpha \in F_q^*\}$. Since f is translation-invariant, then $X(\theta) \subseteq R$. Consider the relation defined on R by the rule "for $\theta_1, \theta_2 \in R$, $\theta_1 \sim \theta_2$ if and only if $\theta_1 - \theta_2 \in F_q$". This is an equivalence relation on R, and its equivalence classes are the sets $X(\theta)$. Each class contains q elements, so $q|n$, say $n = qt$, where t is the number of equivalence classes.

For any root θ and any $\alpha \in F_q$, θ and $\theta + \alpha$ are algebraic conjugates. Let u be the least positive integer such that $\theta^{q^u} \in X^*(\theta)$, and suppose that $\theta^{q^u} = \theta + \beta$ where $\beta \in F_q$. Then $(\theta^{q^u})^{q^u} = (\theta + \beta)^{q^u} = \theta + 2\beta$. Similarly $\theta^{q^{su}} = \theta + s\beta$, $s = 0, 1, \ldots$. In particular $\theta^{q^{qu}} = \theta$, so qu is a multiple of n, therefore $u \geq n/q(= t)$.

Let $\theta_i = \theta^{q^i}, i = 0, 1, \ldots n-1$, so in particular, $\theta = \theta_0$. Then $(\theta_i)^{q^u} = (\theta^{q^u})^{q^i} = (\theta + \beta)^{q^i} = \theta_i + \beta$. This implies that u is the least positive integer such that $\theta_i^{q^u} \in X^*(\theta_i)$, for any i, since if there were a u_1 satisfying $0 \leq u_1 < u$ such that $\theta_1^{q^{u_1}} \in X^*(\theta_1)$, a similar computation would show that $\theta^{q^{u_1}} \in X^*(\theta)$, a contradiction of the definition of u. This implies that $X(\theta_0), X(\theta_1), \ldots, X(\theta_{u-1})$ are distinct equivalence classes, because if some $X(\theta_i) = X(\theta_j)$ where $0 \leq i < j \leq u - 1$, then $(\theta_i)^{q^{j-i}} \in X(\theta_i)$, where $0 \leq j - i < u$, which contradicts the fact u is the least positive integer such that $(\theta_i)^{q^{j-i}} \in X(\theta_i)$. Therefore there must be at least u distinct equivalence classes, so $u \leq n/q(= t)$, and we have $u = t$.

Let $P(\theta) = \prod_{y \in X(\theta)} y$. Then $P(\theta) = \prod_{\alpha \in F_q} (\theta - \alpha) = \theta^q - \theta$.

Note that

$$(\theta^q - \theta)^{q^t} = (\theta^{q^t})^q - \theta^{q^t} = (\theta + \beta)^q - (\theta + \beta) = \theta^q - \theta.$$

Therefore the degree of $P(\theta)$ over F_q is a divisor of t. But $P(\theta_i) = P(\theta_j)$ implies that $\theta_i^q - \theta_i = \theta_j^q - \theta_j$, that is, $P(\theta_0), P(\theta_1), \ldots, P(\theta_{t-1})$ constitutes a set of t distinct algebraic conjugates over F_q, so

$$g(x) = \prod_{i=0}^{t-1}(x - P(\theta_i)) = \prod_{i=0}^{t-1}(x - (\theta_i^q - \theta_i))$$

is an irreducible polynomial of degree t over F_q. Further

$$\begin{aligned} g(x^q - x) &= \prod_{i=0}^{t-1}(x^q - x - (\theta_i^q - \theta_i)) = \prod_{i=0}^{t-1}(x^q - \theta_i^q - (x - \theta_i)) \\ &= \prod_{i=0}^{t-1}((x - \theta_i)^q - (x - \theta_i)) = \prod_{i=0}^{t-1}\prod_{\alpha \in F_q}(x - \theta_i - \alpha) = f(x), \end{aligned}$$

as required.

As was noted earlier, the polynomial $x^q - x$ is q-normal replicator of degree q over F_q. It can be easily verified that

$$\begin{aligned} f^{q^n} - fg^{q^{n-1}} &= (x^q - x)^{q^n} - (x^q - x) \\ &= (x^{q^{n-1}} - 1)x[(x^{q^n} - x)^{q-1} - 1]. \end{aligned}$$

Therefore $\tilde{r}(n, x) = x$ and $G(n) = 1$.

This provides an example of a new result obtained by the mechanism of this paper, namely

$$\#TIMI(q, m) = \begin{cases} (q-1)/qn) \sum\limits_{d|q-free(n)} \mu(d)q^{n/d} \text{ if } q|m, \\ \qquad 0 \text{ otherwise.} \end{cases}$$

and for the case of $m = qn$, let $n = q^a n_1$ where $a \geq 0$ and $q \nmid n_1$. Then

$$\#TIMI(q, qn) = ((q-1)n_1/qn)N_{q^n/n_1}(n_1).$$

In [13] Shparlinski showed that in general for an element $\alpha \in F_q$, there is no connection between the multiplicative order of α and the multiplicative order of $\alpha + 1/\alpha$. In fact, he showed that under some rather mild conditions, the orders can in fact be independent of each other. This work on the orders of α and $\alpha + 1/\alpha$ was motivated by the question of whether an optimal normal basis generator is always primitive; we refer to [12] for a discussion of such generators.

We now show that under some highly constrained conditions, there can be a relation between the orders of α and $\beta = \alpha + 1/\alpha$ in a finite field. In the following we show that if α is a root of a translation invariant polynomial over F_2, then there is a relation between $ord(\alpha)$ and $ord(\beta)$. In particular, we prove the following.

Proposition 17 *If α is a root of a translation invariant irreducible polynomial of degree $2k$ over F_2 and $\beta = \alpha + 1/\alpha$, then $ord(\beta) = ord(\alpha)$ if k is even, and $ord(\beta) = ord(\alpha)/(ord(\alpha), 3)$ if k is odd.*

Proof: Let α be a root of a monic translation invariant polynomial $f(x)$ of positive degree over F_2, and let $\beta = \alpha + 1/\alpha$. Then $f(x)$ is a polynomial in $x(x+1)$ and so it has degree $2k$ with $k > 0$. Over the field F_2, $\bar{r}(x) = x^{2^k} + x + 1$, and so by Theorem 12, $f(x)$ divides $\bar{r}(n,x)$ and hence $\alpha^{2^k} = \alpha + 1$. After squaring and dividing by α, we have $\alpha^{2^{k+1}-1} = \alpha + 1/\alpha = \beta$.

We have that $ord(\beta) = ord(\alpha)/(ord(\alpha), 2^{k+1} - 1)$. Moreover $(2^{2k} - 1, 2^{k+1} - 1) = 3$ if k is odd, and equals 1 if k is even. Since $\alpha \in F_{2^{2k}}, ord(\alpha)$ divides $2^{2k} - 1$ and hence $(ord(\alpha), 2^{k+1} - 1) = 3$ if k is odd and 3 divides $ord(\alpha)$ otherwise.

■

Proposition 17 shows that infinitely often, there is direct relation between the order of θ and $r(\theta)$, where $r(x) = x + x^{-1}$. We show that a similar statement is true for any rational function over F_q apart from those that are essentially constant, that is, for all rational functions not of the form $\alpha f(x)/f(x)$ where $\alpha \in F_q$. Clearly it is sufficient to prove the result for rational functions in their reduced form.

Suppose that $r(x) = f(x)/g(x)$ is a non-constant reduced rational function over the field F_q. Let $\overline{F}_q$ denote the algebraic closure of F_q, and suppose that $\theta \in \overline{F}_q$ is not a root of either of the polynomials $f(x)$ or $g(x)$. Then θ is said to be a power-mate of r if $ord(\theta) = ord(r(\theta))$. Let $PM(q,r)$ denote the set of power-mates of r. We show that the set $PM(q,r)$ is infinite.

Theorem 18 *Suppose that $r(x)$ is a non-constant reduced rational function over the field F_q. Then $PM(q,r)$ is infinite.*

Proof: Let p be the characteristic of F_q.

Case 1: The function $r(x)$ is a polynomial. In this case suppose that r is a non-constant polynomial. If r is a p-th power, say $r = r_1^{p^t}$ for some polynomial r_1 since r is not constant then it can be written as $r = r_2^{p^u}$ where r_2 is a polynomial that is not a p-th power. It follows that $ord(r(\theta)) = ord(r_2(\theta))$ for any $\theta \in \overline{F}_q$ that is not a root of r. Therefore it is sufficient to establish the result for polynomials that are not p-th powers.

Suppose that $r(x)$ is not a p-th power. Let n be an integer satisfying $q^n > \deg(r)$. Let $h_n(x) = x^{q^n} - r(x)$. Then $h_n'(x) = -r'(x)$ where $r' \neq 0$, and any repeated factor of h_n, including any repeated factor x, is also a factor of $r'(x)$. Also any factor of multiplicity t in $r'(x)$ occurs with multiplicity at most $t+1$ in $h_n(x)$. Let $deg(r') = d_1$. If $s \geq 1$, then

$2s \geq s+1$, thus d, the total degree of the product of factors with multiplicity $t \geq 2$ in $h_n(x)$, satisfies $d \leq 2d_1$.

Assume that $PM(q,r)$ is a finite set, and let $MPM(q,r)$ denote the set of minimal polynomials of the elements of $PM(q,r)$. Then $MPM(q,r)$ can be partitioned into two disjoint sets, S_1 and S_2, where $S_1 = \{m \in MPM(q,r) : m|r'\} \cup \{x\}$ and $S_2 = \{m \in MPM(q,r) : m \nmid r'\}$. Let d_2 denote the sum of the degrees of the members of S_2. Note that d_1 and d_2 do not depend on n. Let n_1 be an integer satisfying $q^{n_1} > 2d_1 + d_2 + 1$, where the summand 1 is included to cover the eventuality that x is a factor of multiplicity 1 in r. Since $\deg(h_{n_1}(x)) > 2d_1 + d_2 + 1$, then $h_{n_1}(x)$ must be divisible by an irreducible polynomial $g(x)$ that does not occur in $PM(q,r)$. Let θ be a root of $g(x)$. Then $\theta^{q^{n_1}} = r(\theta)$, and since θ and $\theta^{q^{n_1}}$ are algebraic conjugates, then $ord(\theta) = ord(\theta^{q^{n_1}})$, so $\theta \in PM(q,r)$, which contradicts the fact that $PM(q,r)$ is finite.

Case 2: The function $r(x)$ is not a polynomial. In this case $r(x)$ can be written uniquely in the form $r(x) = f(x)/g(x)$ where $g(x)$ is a non-constant monic polynomial. Using an argument similar to that in Case 1, we may assume without loss of generality that g is not a p-th power. Recall that if $r = f/g$, then $\deg(r) = \max\{\deg(f), \deg(g)\}$. Let n be an integer satisfying $q^n > \deg(r)$. Let $h_n(x) = g(x)x^{q^n} - f(x)$ viewed as a polynomial over F_q. Then $h_n'(x) = x^{q^n}g'(x) - f'(x)$, where $g' \neq 0$.

Again assume that $PM(q,r)$ is a finite set, and let $MPM(q,r)$ denote the set of minimal polynomials of the elements of $PM(q,r)$. Let m be any monic irreducible factor m of h_n other than $m(x) = x$, and let θ be any root of $m \in \overline{F}_q$. Then $\theta \neq 0$ and $g(\theta)\theta^{q^n} - f(\theta) = 0$. If $g(\theta) = 0$, then $f(\theta) = 0$, which is impossible since $(f,g) = 1$. Similarly $f(\theta) \neq 0$. So $\theta^{q^n} = f(\theta)/g(\theta)$, and since θ and θ^{q^n} are conjugates then $m \in MPM(q,r)$ and therefore all monic irreducible factors lie in $MPM(q,r) \cup \{x\}$.

Let a and b be any two distinct integers such that $q^b > q^a > \deg(r)$. Let m be any polynomial divides h_a' and h_b' with multiplicities $k_a \geq 2$ and $k_b \geq 2$ respectively. Then m divides $G = (h_a'(x), h_b'(x))$ with multiplicity $k_{a,b} = \min(k_a, k_b)$. But G divides $D = h_b'(x) - h_a'(x) = (x^{q^b} - x^{q^a})g'(x) = (x^{q^b - q^a} - 1)x^{q^a}g'(x)$. Clearly $x^{q^b - q^a} - 1$ has no repeated factors, so any polynomial $m \in MPM(q,r)$ that appears with multiplicity $t_m \geq 1$ in $g'(x)$, can occur with multiplicity at most $u_m = t_k + 1$ in G, and any polynomial $m \in MPM(q,r)$ that does not divide $g'(x)$ occurs with multiplicity $u_m \leq 1$ in G. Further, let u_x denote multiplicity of the factor x in $f(x)$. If c is any integer satisfying $q^c > \deg(r)$, the multiplicity of x in h_c is u_x, and therefore the multiplicity of x in h_c' is at most u_x.

Let $S_1 = \{m \in MPM(q,r) : m|g'\}$, $S_2 = \{m \in MPM(q,r) : m \nmid g'\}$ and $S = S_1 \cup S_2 \cup \{x\}$. For any polynomial $m \in S$, we define the value $v(m)$ of m as follows. If $m \in S_1$, then $v(m) = 2$, if $m \in S_2$, then $v(m) = u_m + 1$, and $v(x) = u_x$. Note that no polynomial m of S can appear in both h_a and h_b with multiplicity greater than $v(m)$.

Let $s_v = \sum_{m \in S} v(m) \deg(m)$, and let s^* and n^* be the least integers satisfying $q^{s^*} > s_v$ and $q^{n^*} > \deg(r)$, respectively, and let $n_0 = \max\{s^*, n^*\} + 1$, and let $n_i = n_0 + i$, $i = 0, 1, 2, \cdots$. As noted above, for $i \geq 0$, all monic irreducible divisors of h_{n_i} lie in S. For $m \in S$ and $i \geq 0$, let $w_i(m)$ denote the multiplicity of the polynomial m as a factor of h_{n_i}. Since $q^{n_i} > q^{s^*} > s_v$, then there must be at least one $m \in S$ such that $w_0(m) > v(m)$. Let $W_0 = \{m : w_0(m > v(m)\}$. Since $w_0(x) = v(x)$, then $x \notin W_0$, so $W_0 \subseteq MPM(q,r)$. Similarly, there must exist an $m_1 \in MPM(q,r)$ such that $w_1(m_1) > v(m_1)$. If $m_1 \in W_0$, then m_1 has a multiplicity that is greater than $v(m_1)$ in both the factorization of h_{n_0} and h_{n_1}, a contradiction. Let $W_1 = W_0 \cup \{m \in MPM(q,r) : w_1(m) > v(m)\}$. Continuing in this way, construct $W_0, W_1, W_2 \cdots$, with $W_0 \subsetneq W_1 \subsetneq W_2 \cdots \subset MPM(q,r)$. Since $MPM(q,r)$ is finite, there exists a j such that $W_j = MPM(q,r)$. Thus no factor m of $h_{n_{j+1}}$ can occur with multiplicity $w_{j+1}(m) > v(m)$, a contradiction of the assumption that $PM(q,r)$ is finite.

∎

By combining the methods of Proposition 17 and Theorem 18, it is possible to obtain other relations between the orders of θ and $r(\theta)$ for infinite classes of θ similar to those obtained in Theorem 18.

2: The enumerative result for translation invariant polynomials can be generalized as follows. Let $F_{q'}$ be a subfield of F_q. A polynomial $f \in F_q[x]$ is said to be $F_{q'}$- *subfield translation invariant* if $f(x + \alpha) = f(x)$ for all $\alpha \in F_{q'}$, where $F_{q'}$ is viewed as a subfield of F_q. For brevity, if q' is specified, the polynomial is said to be *subfield invariant.*

Although every translation invariant polynomial in $F_q[x]$ is $F_{q'}$- *subfield* translation invariant for every subfield, the converse is not true. For example, let α be a root of $x^2 + x + 1$ in F_4. Then $x^2 + x + \alpha$ and $x^2 + x + \alpha + 1$ are F_2- *subfield* translation invariant, but they are not translation invariant. (They are the only F_2-subfield translation invariant monic irreducible polynomials of degree 2 over F_4.)

Let $STIMI(q', q, m)$ denote the set of all monic irreducible subfield translation invariant polynomials of degree m in $F_q[x]$.

The following theorem is useful for calculating the cardinality of $STIMI(q', q, m)$.

Theorem 19 *Let f be an irreducible $F_{q'}$-subfield translation invariant polynomial of degree m in $F_q[x]$, then there is an irreducible polynomial $g \in F_q[x]$ such that $f(x) = g(x^{q'} - x)$.*

The proof of this theorem is the proof of Theorem 16 mutatis mutandis.

It can be shown that the polynomial $x^{q'} - x$ is q'-normal replicator of degree q' over F_q.

Note that

$$\begin{aligned} f^{q^n} - fg^{q^{n-1}} &= (x^{q'} - x)^{q^n} - (x^{q'} - x) \\ &= (x^{q^{n-1}} - 1)x[(x^{q^n} - x)^{q'-1} - 1]. \end{aligned}$$

Hence $\tilde{r}(n,x) = x$ and $G(n) = 1$. Therefore

$$\#STIMI(q',q,m) = \begin{cases} (q'-1)/q'n) \prod_{d|q'-free\ n} \mu(d)q^{n/d} \text{ if } q'|m, \\ \qquad 0 \text{ otherwise.} \end{cases}$$

If $m = q'n$, the result can be written in terms of $N_q(n)$, the number of monic irreducible polynomials of degree n over F_q. Let $n = q'^a n_1$ where $a \geq 0$ and $q' \nmid n_1$, then it is easily shown that

$$\#STIMI(q',q,m) = ((q'-1)n_1/q'n)N_{q^{n/n_1}}(n_1).$$

3. Consider $r(x) = \frac{x^2+1}{x}$. The rational function $r(x)$ is a 2-normal replicator over F_q of degree $m = 2$. Thus

$$f^{q^n} - fg^{q^n-1} = (x^2+1)^{q^n} - (x^2+1)x^{q^n-1} = (x^{q^n-1} - 1)(x^{q^n+1} - 1).$$

Here,

$$\hat{r}(n,x) = x^{q^n+1} - 1,$$

$$G(n,x) = \begin{cases} x^2 - 1 & \text{if } q \text{ is odd} \\ x+1 & \text{if } q \text{ is even} \end{cases}.$$

and

$$G(n) = \begin{cases} 2 & \text{if } q \text{ is odd} \\ 1 & \text{if } q \text{ is even} \end{cases}.$$

We note that these results agree with those from page 75 of [6]; see also [10]. By Corollary 15 we obtain the result on the number of monic irreducible self-reciprocal polynomials over F_q given in the introduction of this paper:

$$\#SRMI(q,2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)(q^{n/d} - 1)$$

if q is odd and

$$\#SRMI(q,2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)q^{n/d}$$

if q is even.

If $n = 2^v t$, $v \geq 0$, t odd, then

$$\#SMRI(q,2n) = \begin{cases} \frac{1}{2n}(q^n - 1) & n = 1,\ q \text{ odd}, \\ \frac{t}{2n}(N_{q^{n/t}}(t)) & \text{otherwise.} \end{cases}$$

This is a result of the fact that $\sum_{d|n}\mu(d)=1$ if $n=1$ and is zero otherwise, and the properties of n being $2-free$, as discussed earlier.

4. A monic irreducible binomial over the field F_q is an irreducible polynomial of the form $x^r-\lambda$ where $\lambda\in F_q^*$. Let $B(r,q)$ denote the set of all monic irreducible binomials of degree r in $F_q[x]$, and let $P(r,q)$ denote the product of all elements in $B(r,q)$. We use the fact that $f(x)=x^r$ is r-normal over F_q to determine $\#B(r,q)$, the cardinality of the set $B(r,q)$. This result is related to a result of S. D. Cohen [3] on counting (r,m)-polynomials, that is, irreducible polynomials of the form $p(x^r)$, where p is a monic (necessarily irreducible) polynomial of degree m in $F_q[x]$. This will be discussed after the determination of $\#B(r,q)$.

As usual, the method produces a factorization that is normally used to produce a "sum over divisors" formula. However, in this instance the closed form of the answer is that of a product. Rather than using sums to produce the answer, we use the factorization itself to lead directly to the product, illustrating the flexibility of the method.

In the following we let $Q_d(x)$ denote the cyclotomic polynomial of order d when it is defined over F_q.

Theorem 20 *Suppose that the integer $r>1$ and the field F_q are given. Let r' be the squarefree part of r. Then*
(1) $x^{(q-1)^2}-1=\prod_{d|q-1}P(d,q)$, and
(2) If $r'|q-1$ and either $4\nmid q+1$, or $4|q+1$ but $4\nmid r$, then $\#B(r,q)=(\varphi(r)/r)(q-1)$. Otherwise $\#B(r,q)=0$.

Proof: If $f(x)=x^r$, then

$$f^q-fg^{q-1}=x^{qr}-x^r=(x^{r(q-1)}-1)x^r,$$

and $G(1,x)=x^r$ and $\overline{r}(1,x)=(x^{r(q-1)}-1)/(x^{q-1}-1)$.
But

$$(x^{r(q-1)}-1)=\prod_{\lambda\in F_q^*}(x^r-\lambda),$$

and since it is r-normal over F_q, then $\overline{r}(1,x)$ is the product of the monic irreducible polynomials in F_q that are hard for $f(x)$. But by the definition of hardness, an irreducible factor of a monic binomial $x^r-\lambda$, is hard for $f(x)=x^r$ if its degree does not divide 1. By Lemma 7, the degrees of the irreducible factors of are divisors of r. Moreover it is easily seen that for any irreducible binomial $g(x)=x^d-\lambda'$ such that $d|r$, there is a λ such that $g(x)|x^r-\lambda$. Since $\overline{r}(1,x)$ has no repeated proper factors, then

$$\overline{r}(1,x)=\prod_{\substack{d|r,\\ d\neq 1}}P(d,q),$$

and therefore

$$x^{r(q-1)} - 1 = \prod_{d|r} P(d,q).$$

In particular

$$(*) \prod_{d|q-1} Q_d(x^{q-1}) = x^{(q-1)^2} - 1 = \prod_{d|q-1} P(d,q),$$

where $Q_d(x)$ is the d-th cyclotomic polynomial over F_q.

Part (2): By Corollary 9, the irreducible factors of $Q_d(x^{q-1})$ all have degree d. Equating sets of irreducible factors of the same degree in the products in equation $(*)$ yields $P(d,q) = Q_d(x^{q-1})$ for any d that divides $q-1$.

Let λ be any member of F_q^*. Now any prime that divides r also divides of r', so under the above hypotheses, $x^r - \lambda$ is irreducible over F_q if and only if $x^{r'} - \lambda$ is irreducible over F_q, so $\#B(r,q) = \#B(r',q)$. Since $P(r',q) = Q_{r'}(x^{q-1})$ and $Q_{r'}(x)$ has degree $\phi(r')$, then $r'(\#B(r,q)) = \phi(r')(q-1)$, and the result holds for r'. If $r = \prod_{j=1}^{w} p_i^{a_i}$ is the canonical prime decomposition of r, then $\varphi(r) = p_1^{a_1-1}p_2^{a_2-1}\cdots p_w^{a_w-1}\prod_{j=1}^{w} p_i^{a_i}$, therefore $\varphi(r)/r = \varphi(r')/r'$, so the result holds for r as required. It is easily shown that if the hypotheses fail then $x^r - \lambda$ is reducible, which completes the proof.

∎

The notion of an (r,m)-polynomial, that is, an irreducible polynomial of the form $p(x^r)$, where p is a monic irreducible polynomial of degree m in $F_q[x]$ was introduced by Cohen in [Cohen, 1968], where the number of such polynomials was determined. Let $L_r(rm,q)$ denote the number of (r,m)-polynomials over F_q. Clearly every monic irreducible polynomial of degree m in $F_q[x]$ is a $(1,m)$ polynomial, and conversely, and therefore $L_1(1m,q) = N_q(m)$, so the problem is to determine $L_r(rm,q)$ for $r > 1$.

For $r = 1$, the polynomial $f(x) = x$ is a $(1,1)$-polynomial but is not a monic irreducible binomial. But for $r > 1$, every $(r,1r)-$polynomial is a monic irreducible binomial and conversely. Thus for $r > 1$, we have $L_r(r1,q) = \#B(r,q)$.

As above, let r' denote the squarefree part of r, and suppose $r > 1$. It follows from Theorem 18 that if $r'|q-1$ and either $4 \nmid q+1$, or $4|q+1$ but $4 \nmid r$, then $L_r(r1,q) = (\varphi(r)/r)(q-1)$, otherwise $L_r(r1,q) = 0$. This result was first established by Cohen (by other methods) and is central to his proof of his theorem below.

The following is required for the statement of the theorem. Suppose that q is a prime power and $r > 1$ is an integer such that $(r,q) = 1$. Let k denote the order of q mod r', that is, k is the least positive integer such that $q^k \equiv 1 \bmod r'$. If m is a positive integer, then $r'|q^m - 1$ if and only if $k|m$. Then m can be written in the form

$$m = kn_1n,$$

where $(r,n) = 1$ and $n_1'|r$.

Theorem 21 *(Cohen) Suppose that integers* $r > 1$, $m > 0$, *and a field* F_q *are given. Then, if* $r'|q^m - 1$, $4 \nmid (r, q^m + 1)$ *and* m *is written in the form* $m = kn_1n$ *as above, we have*

$$L_r(rm,q) = \begin{cases} (\varphi(r)/rm)(q^m - 1) & n = 1, \\ (n\varphi(r)/rm)N_{q^{m/n}}(n) & n > 1. \end{cases}$$

Otherwise we have $L_r(rm,q) = 0$.

For the sake of completeness, we include a proof of Cohen's result in terms of monic irreducible binomials. The formulae are written as products, and in the case $n = 1$, our proof avoids summations.

Proof: Case 1 Suppose that $n = 1$. Let $p(x)$ be a monic irreducible polynomial of degree m in $F_q[x]$. Then, as in the proof of Theorem 20, $p(x^r)$ is an (r,m)-polynomial if and only if it is an (r',m)-polynomial, which is the case if and only if $x^{r'} - \lambda$ is irreducible over F_{q^m} where λ is a zero of $p(x)$ in F_{q^m}. So we can restrict our initial consideration to r'. Since $k|m$, then $r'|q^m - 1$, and $\#B(r',q^m) = (\varphi(r')/r')(q^m - 1)$. Suppose that $x^{r'} - \nu$ is a factor of $P(r',q^m)$, and suppose that η is of degree $t < m$. Then $r'|q^t - 1$, so $k|t$ and $t = k\nu$ where $\nu|n_1$. If $t = 1$, then clearly μ is of degree $m(= k)$. If $t > 1$, let s be a prime such that $s|(n_1/t)t$. Then $s|r'$, and therefore $x^{r'} - \nu$ factors over $F_{q^{st}}$, contradicting the fact that $x^{r'} - \nu$ is irreducible over F_{q^m}. Therefore ν is of degree m. Let f be the minimal polynomial of ν over F_q, then $f(x^{r'}) = \prod_{i=0}^{m-1}(x^{r'} - \nu^{q^i})$ over F_{q^m}, and therefore f is an (r',m)-polynomial over F_q and conversely. Therefore, over F_q, we have $P(r',q^m) = \prod_{f \in S(r',m,q)} f(x)$. So $L_{r'}(r'm,q) = \#B(r',q^m)/m = (\varphi(r')/r'm)(q^m - 1)$. The result for general r follows from the fact that $\varphi(r)/r = \varphi(r')/r'$.

Case 2 Suppose that $n > 1$. Again we can restrict our initial consideration to the case of r'. Suppose that $\nu \in F_{q^m}$ is such that $x^{r'} - \nu$ is irreducible over F_{q^m}, and that ν is of degree t. Then $k|t$ and $t = kd$ where $d|n_1n$. As in Case 1, if d is divisible by a prime divisor of r', then $x^{r'} - \nu$ cannot be irreducible, so $(d, n_1) = 1$, and $d|n$, so $t = kn_1d$.

Consider F_{q^m} as an extension of $F_{q^{kn_1}}$. Again

$$\#B(r',q^m) = (\varphi(r')/r')(q^m - 1).$$

Let $S_t = \{\nu : x^{r'} - \mu \in B(r', q^m), \deg(\nu) = t\}$. Then, as above,

$$\prod\nolimits_{\mu \in S_t} (x^{r'} - \eta) = \prod\nolimits_{f \in S(r',t,q)} f(x)$$

over F_q, so $\#S_t = tL_{r'}(r't, q)$.

Thus $\sum_{d|n} kn_1 dL_{r'}(r'kn_1 d, q) = (\varphi(r')/r')(q^{kn_1 n} - 1)$.

As noted by Cohen, Möbius inversion of this equation yields

$$kn_1 nL_{r'}(r'kn_1 n, q) = (\varphi(r')/r') \sum\nolimits_{d|n} \mu(d)(q^{kn_1 n/d} - 1),$$

and since $\sum_{d|n} \mu(d) = 0$ for $n > 1$, then

$$mL_{r'}(r'm, q) = (\varphi(r')/r') \sum\nolimits_{d|n} \mu(d)(q^{kn_1/d} - 1).$$

Generalizing from r' to r completes the proof.

6 Quadradically irreducible polynomials

Assume that q is an odd prime power and let S denote the collection of all monic self-reciprocal irreducible polynomials over F_q of degree $2d$ where d runs over all divisors of n for which n/d is odd.

From Section 3, part 3 (see also Jungnickel [6] page 75,) we have the following factorization

$$\frac{x^{q^n+1} - 1}{x^2 - 1} = \prod_{f \in S} f.$$

Let $s = \frac{q^n-1}{2}$. We have

$$x^{q^n+1} - 1 = (x^2 - 1) \sum_{i=0}^{s} x^{2i}$$

since the right hand side telescopes.

Let P_n denote the collection of all polynomials over F_q of degree n and let S_{2n} denote the collection of all self-reciprocal polynomials over F_q of degree $2n$. Define

$$\Phi : P_n \to S_{2n}$$

by

$$f(x) \to x^n f(x + x^{-1}),$$

where $n = \deg f$.

A self-reciprocal polynomial $b(x)$ of degree $2n$ can be written as

$$b(x) = \sum_{i=0}^{n-1} b_i(x^{2n-i} + x^i) + b_n x^n.$$

Define

$$\Psi : S_{2n} \rightarrow P_n$$

by

$$b(x) \rightarrow \sum_{i=0}^{n-1} b_i D_{n-i}(x, 1) + b_n,$$

where for $a \in F_q$, the Dickson polynomial $D_n(x, a)$ of degree $n \geq 1$ and parameter a is defined by

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

see [7] page 8, or [8] page 355.

It is shown in [4] that the function Ψ is multiplicative and is the inverse of Φ. Define $D_0(x, 1) := 1$ if 4 divides $q^n - 1$ and $D_0(x, 1) := 0$ otherwise. Then we have the following factorization

$$\sum_{i=0}^{s} x^{2i} = \prod_{f \in S} f$$

so

$$\sum_{i=0}^{s} D_{2i}(x, 1) = \prod_{f \in S} \Psi(f).$$

A monic irreducible polynomial f of degree n over F_q is said to be quadratically irreducible if $x^2 - \lambda x + 1$ is irreducible over F_{q^n} for any root $\lambda \in F_{q^n}$ of f. We now obtain

Proposition 22 *For a monic irreducible polynomial f of degree n over F_q, the following statements are equivalent:*

1. f is quadratically irreducible over F_q.

2. $f(2)f(-2)$ is a non-square in F_q.

3. $\lambda^2 - 4$ is a non-square in F_{q^n} for one (and hence all) roots λ of f.

4. $\Phi(f)$ is irreducible over F_q.

5. $f = \Psi(g)$ for some monic self-reciprocal irreducible polynomial g of degree $2n$ over F_q.

Proof: The equivalence of statements 1, 2, 3, and 4 is in [10]. The equivalence of 4 and 5 follows since from [11], Ψ is the inverse of Φ.

Let J denote the collection of all quadratically irreducible polynomials over F_q of degree d, where d runs over all divisors of n for which n/d is odd. We are able to obtain the following factorization of the polynomial $\sum_{i=0}^{s} D_{2i}(x,1)$:

$$\sum_{i=0}^{s} D_{2i}(x,1) = \prod_{f \in J} f.$$

Let $N(n,q)$ denote the number of quadratically irreducible polynomials over F_q of degree n. It follows easily that

$$N(n,q) = \frac{1}{2n} \sum_{\substack{d|n \\ d \ odd}} \mu(d)(q^{n/d} - 1).$$

Remark: The function Φ gives a bijection between the set of quadratically irreducible polynomials over F_q of degree n and the set of monic self reciprocal irreducible polynomials of degree $2n$ thus the formula for $N(n,q)$ above can also be obtained easily.

In the case when $q = 2$, if in the above we replace

$$\frac{x^{q^n+1} - 1}{x^2 - 1}, \sum_{i=0}^{s} x^{2i}, D_0, \sum_{i=0}^{s} D_{2i}(x,1)$$

with

$$\frac{x^{2^n+1} - 1}{x - 1}, \sum_{i=0}^{2^n} x^i, 1, \sum_{i=0}^{2^n} D_i(x,1)$$

respectively, then we obtain,

Proposition 23 *For a monic irreducible polynomial f of degree n over F_2, the following statements are equivalent:*

1. f is quadratically irreducible over F_2.

2. The trace of f is 1 *and the trace of its linear coefficient is also* 1.

3. $\Phi(f)$ is irreducible over F_2.

4. $f = \Psi(g)$ for some monic self-reciprocal irreducible polynomial of degree $2n$ over F_2.

In addition

$$\sum_{i=0}^{2^n} D_i(x,1) = \prod_{f\in J} f$$

and

$$N(n,2) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d}.$$

References

[1] L. Carlitz, A theorem of Dickson on irreducible polynomials, Proc. Amer. Math. Soc. 3(1952), 693-700.

[2] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. reine und angew. Math. 227(1967), 212-220.

[3] S.D. Cohen, On irreducible polynomials of certain types in finite fields, Proc. Cambridge Philos. Soc. 66(1969), 335-344.

[4] R.W. Fitzgerald and J.L. Yucas, Factors of Dickson polynomials over finite fields, Finite Fields Appl. 11(2005), 724-737.

[5] S. Gao and G.L. Mullen, Dickson polynomials and irreducible polynomials over finite fields, J. Number Thy. 49(1994), 118-132.

[6] D. Jungnickel, Finite Fields, Bibliographisches Institut & F.A. Brockhaus AG, Manheim, 1993.

[7] R. Lidl, G.L. Mullen, and G. Turnwald, Dickson Polynomials, Longman Scientific & Technical, Essex, England, 1993.

[8] R. Lidl and H. Niederreiter, Finite Fields, Sec. ed., Cambridge Univ. Press, Cambridge, 1997.

[9] A.J. Menezes, Editor, Applications of Finite Fields, Kluwer Acad. Pub., Boston, 1993.

[10] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Alg. in Eng., Comm. and Comp. 1(1990), 43-53.

[11] G.L. Mullen and J.L. Yucas, Self-reciprocal irreducible polynomials over finite fields, Designs, Codes and Cryptography 33(2004), 275-281.

[12] R.C. Mullin, I. Onyszchuk, S.A. Vanstone, and R.M. Wilson, Optimal normal bases in $GF(p^n)$, Discrete Appl. Math. 22(1988/1989), 149-161.

[13] I. Shparlinski, On the multiplicative orders of γ and $\gamma+\gamma^{-1}$ in finite fields, Finite Fields Appl. 7(2001), 327-331.

Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL 33431, Email: rmullin@fau.edu; and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, N2L 3G1, Canada, Email: rcmullin@uwaterloo.ca.

Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, U.S.A., Email: jyucas@math.siu.edu

Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, U.S.A., Email: mullen@math.psu.edu