COMPOSED PRODUCTS AND FACTORS OF CYCLOTOMIC POLYNOMIALS OVER FINITE FIELDS

ALEKSANDR TUXANIDY AND QIANG WANG

ABSTRACT. Let $q = p^s$ be a power of a prime number p and let $\mathbb{F}_q$ be a finite field with q elements. This paper aims to demonstrate the utility and relation of composed products to other areas such as the factorization of cyclotomic polynomials, construction of irreducible polynomials, and linear recurrence sequences over $\mathbb{F}_q$. In particular we obtain the explicit factorization of the cyclotomic polynomial $\Phi_{2^n r}$ over $\mathbb{F}_q$ where both $r \geq 3$ and q are odd, $\gcd(q, r) = 1$, and $n \in \mathbb{N}$. Previously, only the special cases when $r = 1,\ 3,\ 5$, had been achieved. For this we make the assumption that the explicit factorization of Φ_r over $\mathbb{F}_q$ is given to us as a known. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the factorization of $n \in \mathbb{N}$ into powers of distinct primes $p_i,\ 1 \leq i \leq s$. In the case that the multiplicative orders of q modulo all these prime powers $p_i^{e_i}$ are pairwise coprime, we show how to obtain the explicit factors of Φ_n from the factors of each $\Phi_{p_i^{e_i}}$. We also demonstrate how to obtain the factorization of Φ_{mn} from the factorization of Φ_n when q is a primitive root modulo m and $\gcd(m, n) = \gcd(\phi(m), \mathrm{ord}_n(q)) = 1$. Here ϕ is the Euler's totient function, and $\mathrm{ord}_n(q)$ denotes the multiplicative order of q modulo n. Moreover, we present the construction of a new class of irreducible polynomials over $\mathbb{F}_q$ and generalize a result due to Varshamov (1984) [23].

1. INTRODUCTION

1.1. **Composed Products and Applications.** Let $q = p^s$ be a power of a prime p, and $\mathbb{F}_q$ be a finite field with q elements. The multiplicative version of composed products of two polynomials $f,\ g \in \mathbb{F}_q[x]$ (or *composed multiplication* for short) defined by

$$(f \odot g)(x) = \prod_{\alpha} \prod_{\beta} (x - \alpha\beta)$$

where the product $\prod_\alpha \prod_\beta$ runs over all roots $\alpha,\ \beta$ of $f,\ g$ respectively, was first introduced by Selmer (1966) [19] for the purposes of studying linear recurrence sequences (LRS). Informally, LRS's are sequences whose terms depend linearly on a finite number of its predecessors; thus a famous example of a LRS is the Fibonacci sequence whose terms are the sum of the previous two terms. Let k be a positive integer and let $a, a_0, \ldots, a_{k-1}$ be given elements in $\mathbb{F}_q$. Then a sequence $S = \{s_0, s_1, \ldots\}$ of elements $s_i \in \mathbb{F}_q$ satisfying the relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n + a, \qquad n = 0, 1, \ldots$$

is a LRS. If $a = 0$, then S is called a *homogeneous* LRS. If we let $k = 2,\ a = 0,\ a_0 = a_1 = 1$ and $s_0 = 0,\ s_1 = 1$ then S becomes the (homogeneous) Fibonacci sequence. LRS's have applications in coding theory, cryptography, and other areas of electrical engineering where electric switching circuits

Key words and phrases. factorization, composed products, cyclotomic polynomials, construction of irreducible polynomials, Dickson polynomials, linear recurring sequences, linear feedback shift registers, linear complexity, stream cipher theory, finite fields.

Aleksandr Tuxanidy wishes to dedicate his work here to Dr. E. Lorin and Dr. Q. Wang for their support and guidance throughout the years 2010, 2011. In particular, they made him believe in himself as a student once more. The research of Qiang Wang is partially supported by NSERC of Canada.

such as linear feedback shift registers (LFSR) are used to generate them. See Chapter 8 in [15] for this and a general introduction. In particular, the matter of the linear complexity of a LRS, and more generally, the linear complexity of the component wise multiplication of LRS's, is of great importance in stream cipher theory, a branch in cryptography; here a higher complexity is preferred. See [12] for instance and the references contained therein. Since the linear complexity of a LRS is given by the degree of the minimal polynomial of the LRS, minimal polynomials with higher degrees are therefore preferred.

The polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a \in \mathbb{F}_q[x]$$

is called the *characteristic polynomial of* S (see [15]). In 1973, Zierler and Mills [28] showed that the characteristic polynomial of a component wise multiplication of homogeneous LRS's is the composed multiplication of the characteristic polynomials of the respective LRS's. That is, if $S_1, S_2, \ldots, S_r$ are homogeneous LRS's with respective characteristic polynomials $f_1, f_2, \ldots, f_r$, then the characteristic polynomial of $S_1 S_2 \cdots S_r$, with component wise multiplication, is given by $f_1 \odot f_2 \odot \cdots \odot f_r$. We refer the reader to page 433-435 in [15] as well. Note that since the required minimal polynomials are factors of the characteristic polynomials $f_1 \odot f_2 \odot \cdots \odot f_r$ of LRS's, the study of factorizations of composed products has an important significance. Thus composed products have applications in stream cipher theory, LFSR, and LRS in general.

Similarly, the *composed sum* of $f, g \in \mathbb{F}_q[x]$ is defined by

$$(f \oplus g)(x) = \prod_{\alpha} \prod_{\beta} (x - (\alpha + \beta))$$

where the product runs over all the roots α of f and β of g, including multiplicities.

In 1987, Brawley and Carlitz [6] generalized composed multiplications and composed sums in the following.

Definition 1.1. [6] **(Composed Product)** *Let G be a non-empty subset of the algebraic closure Γ_q of $\mathbb{F}_q$ with the property that G is invariant under the Frobenius automorphism $\alpha \mapsto \sigma(\alpha) = \alpha^q$ (i.e., if $\alpha \in G$, then $\sigma(\alpha) \in G$). Suppose a binary operation $\diamond$ is defined on G satisfying $\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta)$ for all $\alpha, \beta \in G$. Then the* composed product *of f and g, denoted by $f \diamond g$, is the polynomial defined by*

$$(f \diamond g)(x) = \prod_{\alpha} \prod_{\beta} (x - (\alpha \diamond \beta)),$$

where the $\diamond$-products run over all roots α of f and β of g.

Observe that $\deg(f \diamond g) = (\deg f)(\deg g)$ clearly. Moreover, in [6] it is noted that when $G = \Gamma_q - \{0\}$ (respectively, Γ_q) and $\diamond$ is the usual multiplication (respectively, addition) then $f \diamond g$ becomes $f \odot g$ (respectively, $f \oplus g$). Other less common examples are

(i) $G = \Gamma_q$, $\alpha \diamond \beta = \alpha + \beta - c$ where $c \in \mathbb{F}_q$ is fixed.

(ii) $G = \Gamma_q - \{1\}$, $\alpha \diamond \beta = \alpha + \beta - \alpha\beta$ (sometimes called the *circle product*), and

(iii) $G =$ any σ-invariant subset of Γ_q, $\alpha \diamond \beta = f(\alpha, \beta)$ where $f(x, y)$ is any fixed polynomial in $\mathbb{F}_q[x, y]$ such that $f(\alpha, \beta) \in G$ for all $\alpha, \beta \in G$.

Let $M_G[q, x]$ be the set of all monic polynomials over $\mathbb{F}_q$ of degree ≥ 1 whose roots lie in G. It is also shown in [6] that the condition $\sigma(\alpha \diamond \beta) = \sigma(\alpha) \diamond \sigma(\beta)$ implies that $f \diamond g \in \mathbb{F}_q[x]$. Moreover, if $\diamond$ is an associative (respectively, commutative) product on G, the composed product is associative (respectively, commutative) on $M_G[q, x]$. In particular, composed multiplications and sums of polynomials are associative and commutative in $\mathbb{F}_q[x]$. In fact, $(G, \diamond)$ is an abelian group for the composed multiplication, composed addition, and the examples in (i), (ii).

1.2. **Irreducible Constructions.** The construction of irreducible polynomials over finite fields is currently a strong subject of interest with important applications in coding theory, cryptography and complexity theory ([8], [9], [14], [15], [23]). One of the most popular methods of construction is the method of composition of polynomials (not to be confused with composed products) where an irreducible polynomial of a higher degree is produced from a given irreducible polynomial of lower degree by applying a substitution operator. For a recent survey of previous results up to the year 2005 on this subject see [9]. Perhaps one of the most applicable results in this area is the following.

Theorem 1.2 (**Cohen (1969)**). *Let f and g be two non-zero relatively prime irreducible polynomials over $\mathbb{F}_q$ and P be an irreducible polynomial over $\mathbb{F}_q$ of degree $n > 0$. Then the composition*

$$F = g^n P\left(f/g\right)$$

is irreducible over $\mathbb{F}_q$ if and only if $f - \alpha g$ is irreducible over $\mathbb{F}_{q^n}$ for some root $\alpha \in \mathbb{F}_{q^n}$ of P.

Note that Theorem 1.2 has been used extensively in the past by several authors in order to produce iterative constructions of irreducible polynomials. See [9] for instance and the references there.

Recently, Kyuregyan-Kyureghyan provides another proof of Theorem 1.2 in [14] using the idea of composing factors of irreducible polynomials over extension fields. Suppose f is an irreducible polynomial over $\mathbb{F}_q$ of degree n and $g(x) = \sum_{i=0}^{n/d} g_i x^i \in \mathbb{F}_{q^d}[x]$ is a factor of f. Then all the remaining factors are

$$g^{(u)}(x) = \sum_{i=0}^{n/d} g_i^{q^u} x^i,$$

where $1 \leq u \leq d-1$. We denote $g = g^{(0)}$, and thus $f = \prod_{u=0}^{d-1} g^{(u)}$. Conversely, given an irreducible polynomial g of degree $k = n/d$ over $\mathbb{F}_{q^d}$, we can form the product $f = \prod_{u=0}^{d-1} g^{(u)}$. However, f is not always an irreducible polynomial over $\mathbb{F}_q$. It is an irreducible polynomial only when $\mathbb{F}_{q^d}$ is the smallest extension field of $\mathbb{F}_q$ containing the coefficients of g, i.e., when $\mathbb{F}_q(g_0, \ldots, g_k) = \mathbb{F}_{q^d}$. In particular, they obtain the following.

Theorem 1.3 (**Theorem 1,** [14]). *Let $k > 1$, $\gcd(k, d) = 1$, and f be an irreducible polynomial of degree k over $\mathbb{F}_q$. Further let $\alpha \neq 0$ and β be elements of $\mathbb{F}_{q^d}$. Set $g(x) := f(\alpha x + \beta)$. Then the polynomial*

$$F = \prod_{u=0}^{d-1} g^{(u)}$$

of degree $n = dk$ is irreducible over $\mathbb{F}_q$ if and only if $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_{q^d}$.

We note that besides the above results there are others that are, perhaps, equally applicable in this area. In particular, a result due to Brawley and Carlitz (1987) [6], is also instrumental in the construction of irreducible polynomials of relatively higher degree from given polynomials of relatively lower degrees.

Theorem 1.4 (**Theorem 2,** [6]). *Suppose that $(G, \diamond)$ is a group and let $f, g \in M_G[q, x]$ with $\deg f = m$ and $\deg g = n$. Then the composed product $f \diamond g$ is irreducible if and only if f and g are both irreducible with $\gcd(m, n) = 1$.*

In Section 2 we construct irreducible polynomials through the use of composed products. First, we show that for some choices of α, β, the product of irreducible polynomials in Theorem 1.3, F, is in fact a composed product, and therefore can be derived from Theorem 1.4. Moreover, we obtain several concrete constructions of irreducible polynomials (Theorem 2.9 and Theorem 2.11) where Theorem 2.11 generalizes a classical result due to Varshamov [23] (see also Theorem 3 [14]) and both Theorems 2.9, 2.11, use cyclotomic polynomials as one of two inputs of composed products.

1.3. **Factorization of Cyclotomic Polynomials.** Let Φ_n denote the n-th cyclotomic polynomial

$$\Phi_n(x) = \prod_{0<j\leq n,\ (j,n)=1} \left(x - \xi_n^j\right)$$

where ξ_n is a primitive n-th root of unity. Clearly, $x^n - 1 = \prod_{d|n} \Phi_d(x)$ and the Mobius Inversion Formula gives $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$ where μ is the Mobius function. Cyclotomic polynomials have been studied extensively since they first appeared in the 18th century works of Euler, Lagrange, Gauss, and others, and to this day continue to be a strong subject of interest in Mathematics ([2], [21], [27]). This is a class of polynomials which naturally arise in the classical 2000 year old Greek problem of Cyclotomy which concerns the division of the circumference of the unit circle into n equal parts, a problem that was finally solved by Gauss at the turn of the 19th century.

It is well known the fact that all cyclotomic polynomials are irreducible over the field of rational numbers; this is not the case over finite fields. In fact, Φ_n decomposes into $\phi(n)/d$ irreducibles over $\mathbb{F}_q$ of the same degree $d = \mathrm{ord}_n(q)$ (see Theorem 2.47 in [15]). The first steps in the factorization of cyclotomic polynomials over finite fields were made in the 19th century by Gauss, Pellet and others who restricted their studies to the prime fields $\mathbb{F}_p$ (p.77, [15]). More recently, Fitzgerald and Yucas (2005) [10] discovered a relationship between the factorization of cyclotomic polynomials and that of Dickson polynomials of the first and second kind. This provides us with an alternative method to factor a Dickson polynomial when we know the factorization of the corresponding cyclotomic polynomial. However, the problem of the explicit factorization of cyclotomic polynomials over finite fields still remains open.

We now give a brief survey of some of the past accomplishments regarding the factorization of cyclotomic polynomials over finite fields; these are especially related to our quest to factor $\Phi_{2^n r}$. The factorization of Φ_{2^n} over $\mathbb{F}_q$ when $q \equiv 1 \pmod 4$ can be found for example in [15] and is stated here in Theorem 3.10; the more difficult case when $q \equiv 3 \pmod 4$ was achieved in 1996 by Meyn [16]. More recently, Fitzgerald and Yucas (2007) [11] gave the factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ for the special cases where r is an odd prime and $q \equiv \pm 1 \pmod r$ is odd. As a result, the factorizations over $\mathbb{F}_q$ of $\Phi_{2^n 3}$, and the Dickson polynomials of the first and second kind $D_{2^n 3}$, $E_{2^n 3-1}$, respectively, are thus obtained. In 2011, L. Wang and Q. Wang [26] went a step further and gave the factorization of $\Phi_{2^n 5}$ over $\mathbb{F}_q$.

In this paper we obtain the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ for arbitrary $r \geq 3$ odd and q odd such that $\gcd(q, r) = 1$. Thus, we generalize the results in [11] and [26]. We make the assumption that the explicit factorization of Φ_r is given to us as a known. When $q = p$ and r is an odd prime (distinct from p) one may use for instance the results due to Stein (2001) [20] to compute the factors of Φ_r efficiently. We achieve our result by applying the theory of composed products as well as by using, and refining in some cases, some of the techniques and results in [26] now generalized for arbitrary odd number $r > 1$. In particular, we refine the following result of theirs. Let $v_2(k)$ denote the highest power of 2 dividing k.

Theorem 1.5 (**Theorem 2.2,** [26])**.** *Let $q = p^s$ be a power of an odd prime p, let $r \geq 3$ be any odd number such that $\gcd(r, q) = 1$, and let $L := L_{\phi(r)} = v_2\left(q^{\phi(r)} - 1\right)$ be the highest power of 2 dividing $q^{\phi(r)} - 1$. Then, for any $n > L$, if $\Phi_{2^L r} = \prod_i f_i$ is the corresponding factorization over $\mathbb{F}_q$, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by $\Phi_{2^n r}(x) = \prod_i f_i(x^{2^{n-L}})$.*

Thus it only remains to factor $\Phi_{2^n r}$ when $1 \leq n \leq L$. We improve the result stated above by giving a smaller bound $K = v_2(q^{d_r} - 1) \leq L$, when $d_r := \mathrm{ord}_r(q)$ is even or $q \equiv 1 \pmod 4$; here K has the same properties as L just described, i.e., if the factorization of $\Phi_{2^K r}$ is known, then for $n > K$ we obtain the factorization of $\Phi_{2^n r}$ by applying the substitution $x \to x^{2^{n-K}}$ to each of the irreducible factors of $\Phi_{2^K r}$. In the case d_r is odd and $q \equiv 3 \pmod 4$, we show that the corresponding bound is $v_2(q+1) < L$. Consequently, it only remains to factor $\Phi_{2^n r}$ when $1 \leq n \leq K$ or $1 \leq n \leq v_2(q+1)$, respectively. We also show that K and $v_2(q+1)$ are the smallest such bounds can be in these cases.

In order to obtain the irreducible factors when $1 \leq n \leq L$, the authors of [26] employed the properties $\Phi_{2r}(x) = \Phi_r(-x)$, and $\Phi_{2^n r}(x) = \Phi_{2^{n-1}r}(x^2),\ n > 1$, of cyclotomic polynomials, together with an iteration of L steps that consists of the following strategy:

1. Obtain the factorization for $n = 0, 1$.
2. For $1 < n \leq L$ and each irreducible factor $h_{n-1}(x)$ of $\Phi_{2^{n-1}r}(x)$, factor $h_{n-1}(x^2)$ into irreducibles; these are all the irreducible factors of $\Phi_{2^n r}(x)$.

   If $n = L$, stop.

First, note that since $q > 1$ is odd, we may write $q = 2^A m \pm 1$, for some $A \geq 2$, and some m odd. Some of our improvements to the above are as follows: In the case $n \leq A$ or $d_r = \mathrm{ord}_r(q)$ odd, we give the explicit factorization of $\Phi_{2^n r}$ without the need of any iterations. On the other hand, in the case d_r is even and $n > A$, we use a similar strategy to step 2, where we replace L by K. We show that in the case d_r even it is enough to iterate for at most $v_2(d_r) < L$ steps starting at $n = A$. This is quite significant as $L = A + v_2(\phi(r))$, and so if A is large, say when $q = 2^A - 1$ is a large Mersenne prime, then L is large. However, as discussed, we only need to iterate for at most $v_2(d_r)$ steps which is relatively much smaller. We remark that, similarly as done in [26], whenever d_r is even or $q \equiv 1 \pmod 4$ the factorization of $\Phi_{2^n r}$ can also be formulated in terms of a system of non-linear recurrence relations for $n \leq K$. For small finite fields and small d_r, this can be computed fairly fast.

As the reader can infer from the previous discussion on the properties of the bounds K and $v_2(q+1)$, the irreducible factors of these cyclotomic polynomials $\Phi_{2^n r}$ are sparse polynomials with a relatively small fixed amount of non-zero coefficients and a relatively much higher (as high as needed) degree. For applications of sparse polynomials in LRS, efficient implementation of LFSR, and in finite field arithmetic, see for instance [3], [13], and [25]. Moreover, as another consequence to our factorization, we obtain infinite families of irreducible polynomials.

We show in Section 3.1 that cyclotomic polynomials are composed multiplications of other cyclotomic polynomials of lower order. In particular, $\Phi_{2^n r} = \Phi_{2^n} \odot \Phi_r$. As a result, we now have at our disposal additional tools such as the results due to Brawley and Carlitz (1987) [6] which we quote in Section 2.1; these are instrumental to our results. We remark that none of the previous authors listed above in our survey considered this insight. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ be the factorization of $n \in \mathbb{N}$ into powers of distinct primes $p_i,\ 1 \leq i \leq s$. In the case that the orders of q modulo all these prime powers $p_i^{e_i}$ are pairwise coprime, in Theorem 3.1 we show how to obtain the factorization of Φ_n from the factorizations of each $\Phi_{p_i^{e_i}}$. In Theorem 3.3 we demonstrate how to obtain the factorization of Φ_{mn} from the factorization of Φ_n when q is a primitive root modulo m and $\gcd(m, n) = \gcd(\phi(m), \mathrm{ord}_n(q)) = 1$.

Note that if $S = \{s_k\},\ T = \{t_k\}$, are homogeneous LRS's with characteristic polynomials $\Phi_{2^n},\ \Phi_r$, respectively, then the characteristic polynomial of $ST = \{s_k t_k\}$ is $\Phi_{2^n r} = \Phi_{2^n} \odot \Phi_r$ by our previous discussion on composed products. We obtain that for n strictly greater than the corresponding bound K or $v_2(q+1)$, the linear complexity of such ST is of the form $2^{z(n)} d_r$ where $z(n) = n - K$ or $z(n) = n - v_2(q+1) + 1$, respectively. Thus by letting $n \to \infty$, the LRS ST will have a linear complexity approaching infinity. As previously discussed, this is very desirable in stream cipher theory.

The rest of this paper goes as follows. In Section 2.1 we discuss a few more properties of composed products and show that some cases of the Kyuregyan-Kyureghyan's construction are composed products. In Section 2.2 we give some results regarding the constructions of irreducible polynomials; for this we made use of a theorem on the irreducibility of composed products, due to Brawley and Carlitz (1987). We consider Theorem 2.11 our main result in this section. As a corollary, this generalizes a result due to Varshamov (1984). As another consequence to Theorem 2.11, in Theorem 3.3 we show how to obtain the factorization of Φ_{mn} from the factorization of Φ_n when q is a primitive root modulo m and $\gcd(m, n) = \gcd(\phi(m), \mathrm{ord}_n(q)) = 1$. In Sections 3.1 and 3.2 we give a number of results and notations,

respectively, which we later use in order to obtain the factorization of $\Phi_{2^n r}$. Then in Sections 3.3 and 3.4 we give the factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ when $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$, respectively. Finally in Appendix A we give a table of examples for Theorem 2.11 and two tables of examples in Appendix B testing the recurrence relations in Theorems 3.11 and 3.13.

2. Irreducible Composed Products and Cyclotomic Polynomials

In this section we apply Theorem 2.3, due to Brawley and Carlitz [6], in the construction of new classes of irreducible polynomials of higher degrees from irreducible polynomials of lower degrees. We devote most of our attention to polynomials of the form $f \odot \Phi_n$. We consider Theorem 2.11 our main result in this section. As a corollary, this generalizes a result due to Varshamov (1984) [23]. As another consequence to Theorem 2.11 we show in Theorem 3.3 how to obtain the factorization of Φ_{mn} from the factorization of Φ_n when q is a primitive root modulo m and $\gcd(m,n) = \gcd(\phi(m), \operatorname{ord}_n(q)) = 1$. First, in Section 2.1 we give a number of known results in the theory of composed products which are instrumental.

2.1. Composed Products.

We need the following known results regarding composed products.

Proposition 2.1 ([7]). *Let $f,\ g \in \mathbb{F}_q[x]$. Then*

$$(f \odot g)(x) = \prod_{\alpha} \alpha^n g\left(\alpha^{-1} x\right)$$

and

$$(f \oplus g)(x) = \prod_{\alpha} g(x - \alpha)$$

where the products $\prod_\alpha$ run over all the roots α of f.

Proof.

$$\begin{aligned}(f \odot g)(x) &= \prod_{\alpha}\prod_{\beta}(x - \alpha\beta) = \prod_{\alpha}\prod_{\beta}\alpha\left(\alpha^{-1}x - \beta\right) = \prod_{\alpha}\alpha^n g\left(\alpha^{-1}x\right).\\ (f \oplus g)(x) &= \prod_{\alpha}\prod_{\beta}(x - (\alpha+\beta)) = \prod_{\alpha}\prod_{\beta}((x-\alpha)-\beta) = \prod_{\alpha} g(x-\alpha). \quad \square\end{aligned}$$

Proposition 2.2 ([6]). *Let $f_i,\ 1 \le i \le s,\ g_j,\ 1 \le j \le t$, be polynomials over $\mathbb{F}_q$. Then*

$$\prod_i f_i \diamond \prod_j g_j = \prod_i \prod_j f_i \diamond g_j.$$

As we remarked earlier, $(G, \diamond)$ is an abelian group when $\diamond$ is the composed multiplication $\odot$, composed sum $\oplus$, or composed circle product $\otimes$. Theorem 1.4 therefore deduces the following consequence.

Theorem 2.3 ([6]). *Let $f,\ g \in \mathbb{F}_q[x]$ of degree $m,\ n$, respectively. Then $f \odot g$, $f \oplus g$, $f \otimes g$ are irreducible over $\mathbb{F}_q$ if and only if $f,\ g$ are irreducible over $\mathbb{F}_q$ and $\gcd(m,n) = 1$.*

One can show that, in particular, the irreducibility of composed multiplications, composed sums, and other cases, follows from Theorem 1.3 due to Kyuregyan-Kyureghyan [14] (when $k > 1$). We however ask if Theorem 1.3 can on the other hand be obtained from irreducible composed products, described in Theorem 2.3. In the following we show that some cases of the construction in Theorem 1.3 are indeed composed products. Note that as a bonus one can now drop the requirement $k > 1$ of Theorem 1.3 in these cases.

Proposition 2.4. *Let* $\gcd(k,d)=1$*, and* f *be an irreducible polynomial of degree* k *over* $\mathbb{F}_q$*. Further let* $\alpha\neq 0$ *and* β *be elements of* $\mathbb{F}_{q^d}$*. Set* $g(x):=f(\alpha x+\beta)$ *and let*

$$F=\prod_{u=0}^{d-1} g^{(u)}$$

be a polynomial over $\mathbb{F}_q$ *of degree* $n=dk$*. Then*

(i) if $\alpha\in\mathbb{F}_q$ *and* $\mathbb{F}_q(\beta)=\mathbb{F}_{q^d}$*, then* F *is a composed sum of two irreducible polynomials with degrees* k *and* d *respectively, hence irreducible.*

(ii) if $\beta\in\mathbb{F}_q$ *and* $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^d}$*, then* F *is a composed multiplication of two irreducible polynomials with degrees* k *and* d *respectively, hence irreducible.*

(iii) if $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^d}$ *and* $\beta=c\alpha$*, where* $c\in\mathbb{F}_q$*, then* F *is the result of a linear substitution operation* $x\to(x+c)$ *applied to an irreducible composed multiplication, and hence irreducible.*

(iv) if $\alpha=-\beta+1$ *and* $\mathbb{F}_q(\alpha,\beta)=\mathbb{F}_{q^d}$*, then* F *is the composed circle product of two irreducible polynomials with degrees* k *and* s *respectively, where* $s\mid d$*, hence irreducible.*

(v) if $\alpha=\beta+1$ *and* $\mathbb{F}_q(\alpha,\beta)=\mathbb{F}_{q^d}$*, then* F *is the composed product of two irreducible polynomials with degrees* k *and* s *respectively, where* $s\mid d$*, hence irreducible.*

Proof. (i) Because $\alpha\in\mathbb{F}_q$, we write $\bar{f}(x)=f(\alpha x)$. So $\bar{f}(x)$ is also an irreducible polynomial of degree k over $\mathbb{F}_q$. Therefore, by Proposition 2.1,

$$F(x)=\prod_{u=0}^{d-1} f^{(u)}(\alpha x+\beta)=\prod_{u=0}^{d-1}\bar{f}^{(u)}(x+\alpha^{-1}\beta)$$

is the composed sum of $\bar{f}$ and the minimal polynomial of $\alpha^{-1}\beta$ (an irreducible polynomial of degree d).

(ii) In this case, let $\bar{f}(x)=f(x+\beta)$. So $\bar{f}(x)$ is also an irreducible polynomial of degree k over $\mathbb{F}_q$.

$$F(x)=\prod_{u=0}^{d-1} f^{(u)}(\alpha x+\beta)=\prod_{u=0}^{d-1}\bar{f}^{(u)}(\alpha x).$$

Hence all the roots of F are the product of roots of $\bar{f}$ and roots of the minimal polynomial of α^{-1}; moreover, both are irreducible polynomials over $\mathbb{F}_q$. Therefore F is the irreducible composed multiplication of $\bar{f}$ and the minimal polynomial of α^{-1} (both have coprime degrees).

(iii) Note that $\prod_{u=0}^{d-1}\alpha^{-kq^u} f\left(\alpha^{q^u}x\right)$ is an irreducible composed multiplication over $\mathbb{F}_q$. Thus, since $\prod_{u=0}^{d-1}\alpha^{-kq^u}\in\mathbb{F}_q^*$, it must be that

$$H(x)=\prod_{u=0}^{d-1} f\left(\alpha^{q^u}x\right)=\prod_{u=0}^{d-1} f^{(u)}(\alpha x)$$

is irreducible as well over $\mathbb{F}_q$. But then

$$H(x+c)=\prod_{u=0}^{d-1} f^{(u)}(\alpha(x+c))=\prod_{u=0}^{d-1} f^{(u)}(\alpha x+\beta)=F(x)$$

is irreducible over $\mathbb{F}_q$.

(iv) Let h be the minimal polynomial of $-\alpha^{-1}+1$. Because $\mathbb{F}_q(\alpha,\beta)=\mathbb{F}_{q^d}$, there are $s\mid d$ distinct conjugates of $-\alpha^{-1}+1$ and thus the degree of h is s. We denote an arbitrary root of f and h by α_f and α_h respectively. Then an arbitrary root of $F(x)=\prod_{u=0}^{d-1} f^{(u)}(\alpha x+\beta)$ can be written as

$$\alpha^{-1}(\alpha_f-\beta)=\alpha^{-1}(\alpha_f+\alpha-1)=\alpha^{-1}\alpha_f+1-\alpha^{-1}=(1-\alpha_h)\alpha_f+\alpha_h=\alpha_f+\alpha_h-\alpha_f\alpha_h.$$

Because h has degree $s\mid d$ as a consequence of $\mathbb{F}_q(\alpha,\beta)=\mathbb{F}_{q^d}$, the polynomial F is the composed circle product of two irreducible polynomials of coprime degrees, and hence irreducible.

(v) Here we define the product $\diamond$ for $G = \Gamma_q - \{-1\}$ by $a \diamond b = a + b + ab$, which forms an abelian group similar to the group corresponding to the circle product. Similarly, let h be the minimal polynomial of $\alpha^{-1} - 1$ and denote an arbitrary root of f and h by α_f and α_h respectively. Then an arbitrary root of $F(x) = \prod_{u=0}^{d-1} f^{(u)}(\alpha x + \beta)$ can be written as

$$\alpha^{-1}(\alpha_f - \beta) = \alpha^{-1}(\alpha_f - \alpha + 1) = \alpha^{-1}\alpha_f - 1 + \alpha^{-1} = (1 + \alpha_h)\alpha_f + \alpha_h = \alpha_f + \alpha_h + \alpha_f\alpha_h.$$

Because h has degree $s \mid d$ as a consequence of $\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_{q^d}$, the polynomial F is the composed product of two irreducible polynomials of coprime degrees, and hence irreducible. □

2.2. **Irreducible Constructions.** In this subsection we use the composed multiplication to construct some new classes of irreducible polynomials. We first recall the definition of *order* of a polynomial.

Definition 2.5 ([15])**.** *Let $f \in \mathbb{F}_q[x]$ be a non-zero polynomial. Then the least positive integer e for which f divides $x^e - 1$ is called the* order *of f and is denoted by* $\mathrm{ord}(f)$.

Proposition 2.6 (**Theorem 3.3,** [15])**.** *Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n, and with $f(0) \neq 0$. Then $\mathrm{ord}(f)$ is equal to the order of any root of f in the multiplicative group $\mathbb{F}_{q^n}^*$.*

Lemma 2.7. *Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n belonging to order t, and let r be a positive integer. Then $f(x) \mid f(x^r)$ implies $r \equiv q^i \pmod t$ for some $i \in [0, n-1]$. Furthermore, let α be a root of f and assume $r \equiv q^i \pmod t$ as above. Then the sets*

$$R = \{\alpha^{r^k q^u};\ 0 \leq u \leq n-1\},\ F = \{\alpha^{q^u};\ 0 \leq u \leq n-1\}$$

are equal for any $k \geq 0$.

Proof. Recall that the roots of f are α^{q^u}, $0 \leq u \leq n-1$ and note $q^n \equiv 1 \pmod t$ because $t \mid q^n - 1$. Moreover, $q^n \equiv 1 \pmod t$ implies that for any $m \geq 0$ there exists an $s \in [0, n-1]$ such that $q^m \equiv q^s \pmod t$. We have: $f(x) \mid f(x^r)$ implies $f(\alpha^{q^u r}) = 0$ for all $u \in [0, n-1]$ giving $\alpha^{q^u r} = \alpha^{q^j}$, some $j \in [0, n-1]$; hence $q^u r \equiv q^j \pmod t$ and so $r \equiv q^{n+j-u} \equiv q^i \pmod t$, some $i \in [0, n-1]$.

Next, assume $r \equiv q^i \pmod t$ for some $i \in [0, n-1]$. We show that $R = F$. Clearly, $r^k q^u \equiv q^{ik+u} \equiv q^j \pmod t$ for some $j \in [0, n-1]$. Thus, $\alpha^{r^k q^u} = \alpha^{q^j} \in F$; hence $R \subseteq F$. Now let $\alpha^{q^u} \in F$. Note that $r \equiv q^i \pmod t$ implies $r^k \equiv q^l \pmod t$ for some $l \in [0, n-1]$. If $u \geq l$, then $r^k q^{u-l} \equiv q^u \pmod t$, so $\alpha^{q^u} = \alpha^{r^k q^{u-l}} \in R$. If $u < l$, write $r^k \equiv q^{u+s} \pmod t$, where $0 < s = l - u \leq n-1$. Then $r^k q^{n-s} \equiv q^{u+s+(n-s)} \equiv q^u \pmod t$, and hence $\alpha^{q^u} = \alpha^{r^k q^{n-s}} \in R$. Therefore $R = F$. □

Lemma 2.8 (**Exercise 10.12,** [24])**.** *Let r be an odd prime number and q a prime power. Suppose that q is a primitive root modulo r and $r^2 \nmid \left(q^{r-1} - 1\right)$. Then the polynomial*

$$\Phi_r(x^{r^k}) = x^{(r-1)r^k} + x^{(r-2)r^k} + \cdots + x^{r^k} + 1$$

is irreducible over $\mathbb{F}_q$ for each $k \geq 0$.

Proof. First, recall that the hypotheses imply that q is a primitive root modulo r^k, $k \geq 1$. Then $\Phi_{r^{k+1}}$, $k \geq 0$, is irreducible over $\mathbb{F}_q$. Thus, if we show $\Phi_{r^{k+1}}(x) = \Phi_r(x^{r^k})$, the result is achieved. Indeed,

$$\Phi_{r^{k+1}}(x) = \prod_{d \mid r^{k+1}} \left(x^{r^{k+1}/d} - 1\right)^{\mu(d)} = \frac{x^{r^{k+1}} - 1}{x^{r^k} - 1} = \Phi_r\left(x^{r^k}\right).$$ □

The following result is the construction of a new infinite family of irreducible polynomials over $\mathbb{F}_q$.

Theorem 2.9. *Let r be a prime number and let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n such that*

(i) $f(x) \mid f(x^r)$
(ii) q *is a primitive root modulo* r
(iii) $\gcd(n, r-1) = 1$.

We have:

(a) The polynomial $F(x) = f(x^r)\left(f(x)\right)^{-1} = \left(f \odot \Phi_r\right)(x)$ *is irreducible over* $\mathbb{F}_q$ *of degree* $n(r-1)$.

(b) If r *is an odd prime such that* $r^2 \nmid \left(q^{r-1}-1\right)$ *and* $\gcd(n, r(r-1)) = 1$, *then* $F\left(x^{r^k}\right) = \left(f \odot \Phi_{r^{k+1}}\right)(x)$, $k \geq 0$, *is an irreducible polynomial over* $\mathbb{F}_q$ *of degree* $nr^k(r-1)$.

Proof. (a) Condition (i) and Lemma 2.7 imply that

$$f(x) = \prod_{u=0}^{n-1}\left(x - \alpha^{q^u}\right) = \prod_{u=0}^{n-1}\left(x - \alpha^{rq^u}\right).$$

As a result,

$$F(x) = \frac{f(x^r)}{f(x)} = \prod_{u=0}^{n-1}\left(\frac{x^r - \alpha^{rq^u}}{x - \alpha^{q^u}}\right).$$

Note that

$$\frac{x^r - \alpha^{rq^u}}{x - \alpha^{q^u}} = x^{r-1} + \alpha^{q^u}x^{r-2} + \cdots + \alpha^{(r-1)q^u} = \alpha^{(r-1)q^u}\Phi_r\left(\alpha^{-q^u}x\right).$$

Condition (ii) implies that Φ_r is irreducible over $\mathbb{F}_q$ of degree $r-1$ which is coprime to n by condition (iii). It only remains to observe that

$$F(x) = \prod_{u=0}^{n-1}\alpha^{(r-1)q^u}\Phi_r\left(\alpha^{-q^u}x\right) = \left(f \odot \Phi_r\right)(x)$$

by Proposition 2.1. Now Theorem 2.3 completes the proof of (a).

We now prove (b): Lemma 2.8 gives $\Phi_r\left(x^{r^k}\right) = \Phi_{r^{k+1}}(x)$ is irreducible over $\mathbb{F}_q$ of degree $r^k(r-1)$ which is coprime to n by assumption. By condition (i), Lemma 2.7, and Proposition 2.1, we obtain

$$\begin{aligned} F\left(x^{r^k}\right) &= \prod_{u=0}^{n-1}\alpha^{(r-1)q^u}\Phi_r\left(\alpha^{-q^u}x^{r^k}\right) = \prod_{u=0}^{n-1}\alpha^{r^k(r-1)q^u}\Phi_r\left(\alpha^{-r^kq^u}x^{r^k}\right) \\ &= \prod_{u=0}^{n-1}\alpha^{r^k(r-1)q^u}\Phi_{r^{k+1}}\left(\alpha^{-q^u}x\right) = \left(f \odot \Phi_{r^{k+1}}\right)(x). \end{aligned}$$

Noting that $f \odot \Phi_{r^{k+1}}$ is irreducible over $\mathbb{F}_q$ of degree $nr^k(r-1)$ by Theorem 2.3, we thus obtain the result. □

Example 2.1. *We give an example where conditions (i), (ii), (iii) are satisfied. As shown in Lemma 2.7, if* $f(x) \mid f(x^r)$, *then* $r \equiv q^i \pmod{t}$ *for some* $i \in [0, n-1]$, *where* t *is the order of* f. *Moreover, we need* $\mathrm{ord}_t(q) = n$ *(see Lemma 2.10),* $\mathrm{ord}_r(q) = \phi(r)$ *and* $\gcd(n, \phi(r)) = 1$. *The reader can verify that when* $(q, n, t, r, f(x)) = \left(2, 3, 7, 11, x^3 + x^2 + 1\right)$ *all the conditions are met. Furthermore,* $11^2 \nmid \left(2^{10} - 1\right)$ *and* $\gcd(3, 11 \cdot 10) = 1$, *so part (b) also holds in this case.*

We generalize the last result further in the following theorem. This also generalizes a result due to Varshamov (1984) which we state in Corollary 2.12. We need the following well known fact.

Lemma 2.10 (Theorem 3.5, [15]). *Let* f *be an irreducible polynomial over* $\mathbb{F}_q$ *of degree* n *belonging to order* t. *Then the multiplicative order of* q *modulo* t *is* n.

Theorem 2.11. *Let $m \in \mathbb{N}$ and assume that q is a primitive root modulo m. Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n such that $\gcd(n, \phi(m)) = 1$ with f belonging to order t. If m and t are even, further assume that n is the multiplicative order of q modulo $t/2$. For each positive divisor d of m define the polynomials R_d, Ψ_d over $\mathbb{F}_q$ as follows: Set $x^d \equiv R_d(x) \pmod{f(x)}$, and $\Psi_d(x) = \sum_{i=0}^{n} \Psi_{d,i} x^i$, where Ψ_d is the non-zero polynomial of minimal degree satisfying the congruence*

$$\sum_{i=0}^{n} \Psi_{d,i} \left(R_d(x)\right)^i \equiv 0 \pmod{f(x)}.$$

Then the polynomials $\Psi_d,\ d \mid m$, are irreducible over $\mathbb{F}_q$ of degree n. Furthermore,

$$F_m(x) = \prod_{d|m} \Psi_d\left(x^d\right)^{\mu(m/d)} = \left(f \odot \Phi_m\right)(x)$$

is an irreducible polynomial over $\mathbb{F}_q$ of degree $n\phi(m)$ belonging to order $\operatorname{lcm}(t, m)$.

Proof. We first prove that for each positive divisor d of m, Ψ_d is irreducible over $\mathbb{F}_q$ of degree n. Now, let $\alpha \in \mathbb{F}_{q^n}$ be a root of f. Then the congruence relations $\sum_{i=0}^{n} \Psi_{d,i} \left(R_d(x)\right)^i \equiv 0 \pmod{f(x)}$ and $x^d \equiv R_d(x) \pmod{f(x)}$ imply that $R_d(\alpha) = \alpha^d$ is a root of Ψ_d. Thus, by the assumption of the minimality of the degree of Ψ_d we deduce that Ψ_d is the minimal polynomial of α^d over $\mathbb{F}_q$. As a result, Ψ_d is irreducible over $\mathbb{F}_q$.

We now prove $\deg(\Psi_d) = n$. Suppose $\deg(\Psi_d) = s_d \le n$. Note that $\operatorname{ord}(\Psi_d) = \operatorname{ord}\left(\alpha^d\right) = t/\gcd(d, t)$. Then by Lemma 2.10 we have $\operatorname{ord}_t(q) = n$, and $\operatorname{ord}_{t/\gcd(d,t)}(q) = s_d$. Since q is a primitive root modulo m, then m must be either $1,\ 2,\ 4,\ r^k$, or $2r^k$ for some odd prime r and some $k \ge 1$. We show that in all these cases $s_d = n$ for each $1 \le d \mid m$. Observe that Ψ_1 is the minimal polynomial of α which is f; hence $\Psi_1 = f$ and $s_1 = n$. Suppose $d = 2 \mid m$. If $\gcd(d, t) = 1$, then $s_2 = \operatorname{ord}_{t/\gcd(2,t)}(q) = \operatorname{ord}_t(q) = n$. Otherwise t is even and so $s_2 = \operatorname{ord}_{t/\gcd(2,t)}(q) = \operatorname{ord}_{t/2}(q) = n$ by the hypothesis for m even. Note that whenever $m > 2$ we can't have $\gcd(m, t) = m$ otherwise $q^n \equiv 1 \pmod{t}$ gives $q^n \equiv 1 \pmod{m}$ implying $\phi(m) \mid n$ contrary to $\gcd(n, \phi(m)) = 1$ and $\phi(m) > 1$. Thus whenever $m = 4$ we must have either $\gcd(m, t) = 1$ or $\gcd(m, t) = 2$. In both cases we obtain $s_4 = \operatorname{ord}_{t/\gcd(4,t)}(q) = \operatorname{ord}_t(q) = n$ or $s_4 = \operatorname{ord}_{t/2}(q) = n$ also by the hypothesis for m even. Consider the cases $m = r^k,\ 2r^k$, for some odd prime r, some $k \ge 1$. Let $d = r^j \mid m,\ 1 \le j \le k$. Either $r \mid \gcd\left(r^j, t\right)$ or $\gcd\left(r^j, t\right) = 1$. Suppose $r \mid \gcd\left(r^j, t\right)$. In particular, $r \mid t$. Note that $\phi(m) > 1$ is even and so the assumption $\gcd(n, \phi(m)) = 1$ implies n is odd. Moreover, because q is a primitive root modulo $m = r^k$ or $2r^k$, then q is a primitive root modulo r. Now, $q^n \equiv 1 \pmod{t}$ gives $q^n \equiv 1 \pmod{r}$ implying $\phi(r) = r - 1 \mid n$. But n is odd and $r - 1$ is even because r is odd. Thus we have reached a contradiction and so we must have $\gcd\left(r^j, t\right) = 1$. As a result we obtain $s_{r^j} = \operatorname{ord}_{t/\gcd(r^j,t)}(q) = \operatorname{ord}_t(q) = n$. At this point we have accounted for all possible positive divisors d of m and we thus conclude $s_d = n$ for each $1 \le d \mid m$; therefore

$$\Psi_d(x) = \prod_{u=0}^{n-1} \left(x - \alpha^{dq^u}\right).$$

Now, we know that Φ_m is irreducible over $\mathbb{F}_q$ since q is a primitive root modulo m. Moreover, $\deg(\Phi_m) = \phi(m)$ is coprime to n by assumption. Thus, by Theorem 2.3, $f \odot \Phi_m$ is irreducible over $\mathbb{F}_q$ of degree $n\phi(m)$. Furthermore, because the roots $\{\xi_m\}$ of Φ_m are the primitive m-th roots of unity, i.e., m is the least positive integer l such that $\xi_m^l = 1$, then $\operatorname{ord}(\xi_m) = m$. Hence, $\operatorname{ord}(f \odot \Phi_m) = \operatorname{ord}(\alpha\xi_m) = \operatorname{lcm}(t, m)$. In conclusion, if we show $F_m = f \odot \Phi_m$, the proof will be complete. First, recall

$$x^m - 1 = \prod_{k=0}^{m-1} \left(x - \xi_m^k\right) = \prod_{d|m} \Phi_d(x) = \prod_{d|m} \prod_{\substack{k=0 \\ \gcd(k,d)=1}}^{d-1} \left(x - \xi_d^k\right).$$

We have

$$\begin{aligned}\Psi_m\left(x^m\right) &= \prod_{u=0}^{n-1}\left(x^m-\alpha^{mq^u}\right)=\prod_{u=0}^{n-1}\prod_{k=0}^{m-1}\left(x-\alpha^{q^u}\xi_m^k\right)=\left(f\odot\left(x^m-1\right)\right)(x)=\left(f\odot\prod_{d\mid m}\Phi_d\right)(x)\\ &= \prod_{u=0}^{n-1}\prod_{d\mid m}\prod_{\substack{k=0\\ \gcd(k,d)=1}}^{d-1}\left(x-\alpha^{q^u}\xi_d^k\right)=\prod_{d\mid m}\prod_{u=0}^{n-1}\prod_{\substack{k=0\\ \gcd(k,d)=1}}^{d-1}\left(x-\alpha^{q^u}\xi_d^k\right)\\ &= \prod_{d\mid m}\left(f\odot\Phi_d\right)(x).\end{aligned}$$

By applying the Mobius Inversion Formula now we obtain the desired result. □

Remark 2.1. *Whenever the hypotheses in Theorem 2.11 are true, the proof shows, in particular, that the characteristic polynomial of each α^d, $1\le d\mid m$, is its minimal polynomial, and thus it is irreducible. Note that the condition "If m and t are even, further assume that n is the multiplicative order of q modulo $t/2$" is necessary to ensure that for any even positive divisor d of m, the characteristic polynomial of α^d is irreducible; this is true in most cases here. However, the reader can observe from the proof that if we define Ψ_d as the characteristic polynomial of α^d instead, F_m will still be irreducible.*

Remark 2.2. *Note that since m is either of $1,\ 2,\ 4,\ r^k,\ 2r^k$, and $\mu(c)=0$ whenever there exists some prime p such that $p^2\mid c$, then any F_m must be a product and division of at most four minimal polynomials Ψ_d evaluated at x^d. Since one of these must be the given $\Psi_1=f$, we only need to compute at most three minimal (or characteristic, see above) polynomials. Thus, this may provide an alternative more efficient way to compute $f\odot\Phi_m$ versus other known general methods for computing composed products. See* [7] *for known methods of computing composed products efficiently. We further remark that our formula $F_m=f\odot\Phi_m$ holds even if $\gcd(n,\phi(m))\neq 1$, although F_m is not irreducible in this case.*

Remark 2.3. *Theorem 2.9 (a) is a corollary of Theorem 2.11. Indeed,*

$$F(x)=\frac{f\left(x^r\right)}{f(x)}=\left(f\odot\Phi_r\right)(x)=F_r(x).$$

Theorem 2.11 generalizes a result due to Varshamov (1984) which was given without a proof. For an independent proof of Corollary 2.12 we refer the reader to Theorem 3 in [14].

Corollary 2.12 (Varshamov (1984)). *Let r be an odd prime number which does not divide q and $r-1$ be the order of q modulo r. Further, let $n\in\mathbb{N}$ such that $\gcd(n,r-1)=1$, and let f be an irreducible polynomial of degree n over $\mathbb{F}_q$ belonging to order t. Define the polynomials R and ψ over $\mathbb{F}_q$ as follows: Set $x^r\equiv R(x)\pmod{f(x)}$ and $\psi(x)=\sum_{u=0}^{n}\psi_u x^u$, where ψ is the nonzero polynomial of minimal degree satisfying the congruence*

$$\sum_{u=0}^{n}\psi_u\left(R(x)\right)^u\equiv 0\pmod{f(x)}.$$

Then the polynomial ψ is an irreducible polynomial of degree n over $\mathbb{F}_q$ and

$$F(x)=\left(f(x)\right)^{-1}\psi\left(x^r\right)$$

is an irreducible polynomial of degree $(r-1)n$ over $\mathbb{F}_q$. Moreover, F belongs to order rt.

Proof. In Theorem 2.11, let $m=r$. Then F_r is an irreducible polynomial over $\mathbb{F}_q$ of degree $\phi(r)n=(r-1)n$ belonging to order $\operatorname{lcm}(r,t)$. Recall from the proof of Theorem 2.11 that if an odd prime r divides m, then $\gcd(r,t)=1$. Thus F_r belongs to order $\operatorname{lcm}(r,t)=rt$. Let α be a root of f. The definition of ψ

implies it is the minimal polynomial of α^r which is Ψ_r; thus $\psi = \Psi_r$ and so ψ is irreducible over $\mathbb{F}_q$ of degree n. It only remains to observe

$$F_r(x) = \prod_{d|r} \Psi_d\left(x^d\right)^{\mu(r/d)} = \frac{\Psi_r\left(x^r\right)}{\Psi_1(x)} = \frac{\psi\left(x^r\right)}{f(x)} = F(x). \qquad \square$$

Corollary 2.13. *Let r be an odd prime and assume q is a primitive root modulo r such that $r^2 \nmid \left(q^{r-1}-1\right)$. Let f be an irreducible polynomial over $\mathbb{F}_q$ of degree n such that $f(x) \mid f\left(x^r\right)$ and $\gcd\left(n, r(r-1)\right) = 1$. Then for $k \geq 0$,*

$$F_r\left(x^{r^k}\right) = F_{r^{k+1}}(x)$$

is an irreducible polynomial over $\mathbb{F}_q$ of degree $nr^k(r-1)$.

Proof. Let $F(x) = (f(x))^{-1} f\left(x^r\right) = \left(f \odot \Phi_r\right)(x)$ as in Theorem 2.9. Then $F\left(x^{r^k}\right)$ is irreducible over $\mathbb{F}_q$ of degree $nr^k(r-1)$ by Theorem 2.9 (b). It only suffices to note that by Remark 2.3 and Theorem 2.9 (b) we have

$$F_r\left(x^{r^k}\right) = F\left(x^{r^k}\right) = \left(f \odot \Phi_{r^{k+1}}\right)(x) = F_{r^{k+1}}(x). \qquad \square$$

3. Explicit Factorization of the Cyclotomic Polynomial $\Phi_{2^n r}$

In this section we present new results, Theorems 3.8, 3.11, 3.13, of the explicit factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ where q is odd, $n \in \mathbb{N}$, and $r \geq 3$ is any odd number such that $\gcd(q, r) = 1$. Previously, only $\Phi_{2^n 3}$ and $\Phi_{2^n 5}$ had been factored in [11] and [26], respectively. We also show how to obtain the factorization of Φ_n in a special case in Theorem 3.1, and how to obtain the factorization of Φ_{mn} from the given factorization of Φ_n when q is a primitive root modulo m and $\gcd(m, n) = \gcd(\phi(m), \mathrm{ord}_n(q)) = 1$.

3.1. Preliminaries.

The following result shows that cyclotomic polynomials are in fact composed multiplications of other cyclotomic polynomials. Moreover, it shows how we may obtain the factorization of Φ_n in a special case.

Theorem 3.1. *Let $n = p_1^{e_1} p_2^{e_2} \ldots p_s^{e_s}$ be the complete factorization of $n \in \mathbb{N}$. Let $\Phi_{p_1^{e_1}} = \prod_i f_{1_i}$, $\Phi_{p_2^{e_2}} = \prod_j f_{2_j}, \ldots,$ $\Phi_{p_s^{e_s}} = \prod_k f_{s_k}$ be the corresponding factorizations over $\mathbb{F}_q$. Then*

$$\begin{aligned} \Phi_n &= \Phi_{p_1^{e_1}} \odot \Phi_{p_2^{e_2}} \odot \cdots \odot \Phi_{p_s^{e_s}} \\ &= \prod_i \prod_j \cdots \prod_k \left(f_{1_i} \odot f_{2_j} \odot \cdots \odot f_{s_k}\right). \end{aligned}$$

Moreover, if the multiplicative orders of q modulo all these primes powers $p_i^{e_i}$ are pairwise coprime, then this is the complete factorization of Φ_n over $\mathbb{F}_q$.

Proof. For brevity's sake, let $F = \Phi_{p_1^{e_1}} \odot \cdots \odot \Phi_{p_s^{e_s}}$. By definition,

$$F(x) = \prod_{\xi_{p_1^{e_1}}} \cdots \prod_{\xi_{p_s^{e_s}}} \left(x - \xi_{p_1^{e_1}} \cdots \xi_{p_s^{e_s}}\right)$$

where the products $\prod_{\xi_{p_i^{e_i}}}$ run over all primitive $p_i^{e_i}$-th roots of unity $\xi_{p_i^{e_i}}$. Note that each $\xi_{p_1^{e_1}} \xi_{p_2^{e_2}} \cdots \xi_{p_s^{e_s}}$ is a root of Φ_n. Indeed, $\mathrm{ord}(\xi_{p_1^{e_1}} \cdots \xi_{p_s^{e_s}}) = p_1^{e_1} \cdots p_s^{e_s} = n$ as $\mathrm{ord}(\xi_{p_i^{e_i}}) = p_i^{e_i}$ and the p_i's are coprime; thus each $\xi_{p_1^{e_1}} \cdots \xi_{p_s^{e_s}}$ is a primitive n-th root of unity, and hence a root of Φ_n. Furthermore, both polynomials are monic and $\deg(F) = \prod_{i=1}^s \phi(p_i^{e_i}) = \phi(\prod_{i=1}^s p_i^{e_i}) = \phi(n) = \deg \Phi_n$. Now, recall that all the roots of a cyclotomic polynomial are distinct. If we show that all roots $\xi_{p_1^{e_1}} \xi_{p_2^{e_2}} \cdots \xi_{p_s^{e_s}}$ of F are distinct, the desired result $\Phi_n = F$ must then follow. Suppose $\xi_{p_1^{e_1}}^{i_1} \cdots \xi_{p_s^{e_s}}^{i_s} = \xi_{p_1^{e_1}}^{j_1} \cdots \xi_{p_s^{e_s}}^{j_s}$ is a root of

F. Then $\xi_{p_1^{e_1}}^{i_1-j_1}\cdots\xi_{p_{s-1}^{e_{s-1}}}^{i_{s-1}-j_{s-1}} = \xi_{p_s^{e_s}}^{j_s-i_s}$. In particular, $\operatorname{ord}(\xi_{p_1^{e_1}}^{i_1-j_1}\cdots\xi_{p_{s-1}^{e_{s-1}}}^{i_{s-1}-j_{s-1}}) = \operatorname{ord}(\xi_{p_s^{e_s}}^{j_s-i_s})$. Moreover, $\operatorname{ord}(\xi_{p_1^{e_1}}^{i_1-j_1}\cdots\xi_{p_{s-1}^{e_{s-1}}}^{i_{s-1}-j_{s-1}}) \mid p_1^{e_1}\cdots p_{s-1}^{e_{s-1}}$ and $\operatorname{ord}(\xi_{p_s^{e_s}}^{j_s-i_s}) \mid p_s^{e_s}$. But then, as $\gcd(p_1^{e_1}\cdots p_{s-1}^{e_{s-1}},\ p_s^{e_s}) = 1$, we must have $\xi_{p_s^{e_s}}^{j_s-i_s} = 1$. Since $p_s^{e_s} > 1$ and $0 < i_s, j_s < p_s^{e_s}$, necessarily $i_s = j_s$. Similarly, by induction we can show $i_k = j_k,\ 1 \le k \le s$. Thus, $\Phi_n = F$.

The second statement of the theorem follows from Proposition 2.2, the associativity of composed multiplications, and Theorem 2.3 combined with the fact that the degrees of the irreducible factors f_i of $\Phi_{p_i^{e_i}}$ are $\operatorname{ord}_{p_i^{e_i}}(q)$. □

Example 3.1. *Let $q = 11,\ n = 595 = 5\cdot 7\cdot 17$. As $\operatorname{ord}_5(q) = 1,\ \operatorname{ord}_7(q) = 3,\ \operatorname{ord}_{17}(q) = 16$ are pairwise coprime, then by Theorem 3.1 the complete factorization of Φ_{595} over $\mathbb{F}_{11}$ is given by*

$$\Phi_{595} = \prod_i \prod_j \prod_k (f_i \odot g_j \odot h_k)$$

where the $f_i,\ g_j,\ h_k$ are the irreducible factors of $\Phi_5,\ \Phi_7,\ \Phi_{17}$, respectively, over $\mathbb{F}_{11}$.

We have the following corollary to Theorem 3.1.

Corollary 3.2. *Let $m,\ n \in \mathbb{N}$ be coprime. Then $\Phi_{mn} = \Phi_m \odot \Phi_n$. Further, let $\Phi_m = \prod_i f_i,\ \Phi_n = \prod_j g_j$ be the respective factorizations over $\mathbb{F}_q$. Then*

$$\Phi_{mn} = \prod_i \prod_j (f_i \odot g_j).$$

Moreover, if $\gcd(\operatorname{ord}_m(q), \operatorname{ord}_n(q)) = 1$, then this is the complete factorization of Φ_{mn} over $\mathbb{F}_q$.

Proof. The result is clear if $m = 1$ or $n = 1$. Assume $m = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\ n = p_{k+1}^{e_{k+1}}p_{k+2}^{e_{k+2}}\cdots p_s^{e_s}$ are complete factorizations of $m,\ n$ over $\mathbb{N}$. Then by Theorem 3.1 we have

$$\Phi_m = \Phi_{p_1^{e_1}} \odot \cdots \odot \Phi_{p_k^{e_k}}, \qquad \Phi_n = \Phi_{p_{k+1}^{e_{k+1}}} \odot \cdots \odot \Phi_{p_s^{e_s}},$$

giving

$$\Phi_m \odot \Phi_n = (\Phi_{p_1^{e_1}} \odot \cdots \odot \Phi_{p_k^{e_k}}) \odot (\Phi_{p_{k+1}^{e_{k+1}}} \odot \cdots \odot \Phi_{p_s^{e_s}}) = \Phi_{p_1^{e_1}} \odot \cdots \odot \Phi_{p_s^{e_s}} = \Phi_{mn}.$$

The second statement follows immediately from Proposition 2.2 and Theorem 2.3 combined with the fact that the degrees of the irreducible factors $f_i,\ g_j$ are $\operatorname{ord}_m(q),\ \operatorname{ord}_n(q)$ respectively. □

In particular, whenever r is odd we have $\Phi_{2^n r} = \Phi_{2^n} \odot \Phi_r$. Thus whenever the factorizations of $\Phi_m,\ \Phi_n$ are known, and $\gcd(m,n) = \gcd(\operatorname{ord}_m(q), \operatorname{ord}_n(q)) = 1$, we can obtain all the irreducible factors of Φ_{mn} by computing each $f_i \odot g_j$. This is a significant tool in the factorization of polynomials which we will use frequently in order to obtain some of the following results.

The following result shows how we may obtain the factorization of Φ_{mn} from the factorization of Φ_n whenever q is a primitive root modulo m and $\gcd(m,n) = \gcd(\phi(m), \operatorname{ord}_n(q)) = 1$. Recall that Φ_n decomposes into $\phi(n)/\operatorname{ord}_n(q)$ irreducible factors over $\mathbb{F}_q$ of the same degree $\operatorname{ord}_n(q)$ whenever $\gcd(q,n) = 1$.

Theorem 3.3. *Let $m,\ n \in \mathbb{N},\ \gcd(m,n) = \gcd(\phi(m), d_n) = 1$, where $d_n = \operatorname{ord}_n(q)$. Assume q is a primitive root modulo m. Let $\Phi_n = \prod_{i=1}^{\phi(n)/d_n} f_i$ be the corresponding factorization over $\mathbb{F}_q$. Then the factorization of Φ_{mn} over $\mathbb{F}_q$ is given by*

$$\Phi_{mn}(x) = \prod_{i=1}^{\phi(n)/d_n} \left(\prod_{d\mid m} \Psi_{i,d}\left(x^d\right)^{\mu(m/d)} \right)$$

where each $\Psi_{i,d}$ is the minimal polynomial of $\xi_{n,i}^d$ with $\xi_{n,i}$ a root of f_i.

Proof. Since q is a primitive root modulo m, Φ_m is irreducible over $\mathbb{F}_q$. Note $\gcd(d_n, \phi(m)) = 1$ implies each polynomial $f_i \odot \Phi_m$ is irreducible over $\mathbb{F}_q$ by Theorem 2.3. Then by Corollary 3.2 and Theorem 2.11 the complete factorization of Φ_{mn} over $\mathbb{F}_q$ is given by

$$\Phi_{mn}(x) = \prod_{i=1}^{\phi(n)/d_n} (f_i \odot \Phi_m)(x) = \prod_{i=1}^{\phi(n)/d_n} \left(\prod_{d|m} \Psi_{i,d}\left(x^d\right)^{\mu(m/d)} \right)$$

as required. □

Remark 3.1. *Note that the irreducible factors of Φ_{mn} are expressed in terms of the minimal polynomials $\Psi_{i,d}$ over $\mathbb{F}_q$ of $\xi_{n,i}^d$, where the root $\xi_{n,i}$ of f_i is a primitive n-th root of unity. We remark that it is not necessary to compute the minimal polynomials: Since $\gcd(m,n) = 1$, then $\gcd(d,n) = 1$ for each $d \mid m$; hence $\xi_{n,i}^d$ is a primitive n-th root of unity, and so it must be a root of some irreducible factor f_j of Φ_n. But then $\Psi_{i,d} = f_j$.*

As a particular consequence, we can now let Φ_n be as in Theorems 3.10, 3.11, 3.12, 3.13, etc, and then use the respective factorizations $\prod_i f_i$ given there to factor Φ_{mn}. This is now merely a matter of computation.

On the other hand, in the case that we do not know the factorization of Φ_n, we can let $S = \{\xi_{n_i}\}_{i=1}^{\phi(n)/d_n}$ be a set of pairwise non-conjugate primitive n-th roots of unity ξ_n. Then we can write the complete factorization of Φ_{mn} over $\mathbb{F}_q$ as

$$\Phi_{mn}(x) = \prod_{i=1}^{\phi(n)/d_n} \left(\prod_{d|m} \Psi_{i,d}\left(x^d\right)^{\mu(m/d)} \right) = \prod_{\xi_{n_i} \in S} \left(\prod_{d|m} \Psi_{i,d}\left(x^d\right)^{\mu(m/d)} \right)$$

where $\Psi_{i,d}$ is the minimal polynomial of $\xi_{n_i}^d$. Indeed, ξ_{n_i} is a root of $\Psi_{i,1} = f_i$, and for non-conjugates ξ_{n_i}, ξ_{n_j}, we have $f_i \neq f_j$; finally, there are $|S| = \phi(n)/d_n$ irreducible factors f_i of Φ_n.

Lemma 3.4 (**Theorem 3.35,** [15])**.** *Let f_1, $f_2, \ldots,$ f_N be all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $(q^m - 1)/e$. Assume also that $q^m \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$. Then $f_1(x^t)$, $f_2(x^t), \ldots,$ $f_N(x^t)$ are all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et.*

Lemma 3.5 (**Exercise 2.57,** [15])**.**
(a) $\Phi_{2n}(x) = \Phi_n(-x)$ for $n \geq 3$ and n odd.
(b) $\Phi_{mt}(x) = \Phi_m(x^t)$ for all positive integers m that are divisible by the prime t.
(c) $\Phi_{mt^k}(x) = \Phi_{mt}\left(x^{t^{k-1}}\right)$ if t is a prime and m, k are arbitrary positive integers.

Note that Lemma 3.5 implies that, in particular, for $n \geq 2$, $\Phi_{2^n r}(x) = \Phi_{2^{n-1} r}(x^2)$. Observe that if $\Phi_{2^{n-1}r} = \prod_i h_i$ is the corresponding factorization, then $\Phi_{2^n r}(x) = \Phi_{2^{n-1}r}\left(x^2\right) = \prod_i h_i\left(x^2\right)$. *This means that we can obtain all the irreducible factors of $\Phi_{2^n r}$ by factoring each $h_i\left(x^2\right)$.*

Let $v_2(k)$ denote the highest power of 2 dividing k.

Lemma 3.6 (**Proposition 1,** [4])**.** *For $i \geq 1$,*

$$\begin{aligned} v_2\left(q^i - 1\right) &= v_2(q-1) + v_2\left(q^{i-1} + q^{i-2} + \cdots + 1\right) \\ &= \begin{cases} v_2(q-1) + v_2(i) + v_2(q+1) - 1, & \text{if } i \text{ is even} \\ v_2(q-1), & \text{if } i \text{ is odd.} \end{cases} \end{aligned}$$

Lemma 3.7. *Let $q = p^s$ be a power of an odd prime p, let $r \geq 3$ be any odd number coprime to q, and let $d_r = \operatorname{ord}_r(q)$. If $q \equiv 1 \pmod 4$, write $q = 2^A m + 1$, $A \geq 2$, m odd. Otherwise if $q \equiv 3 \pmod 4$, write $q = 2^A m - 1$, $A \geq 2$, m odd. Set $K := v_2\left(q^{d_r} - 1\right)$. Then if d_r is even, in both cases cases of q we have*

$K = A + v_2(d_r) > A \geq 2$. *If* d_r *is odd and* $q \equiv 1 \pmod 4$, *then* $K = A$. *If* d_r *is odd and* $q \equiv 3 \pmod 4$, *then* $K = 1$.

Proof. First assume d_r is even. Then $v_2(d_r) > 0$, and so $A + v_2(d_r) > A \geq 2$. If $q \equiv 1 \pmod 4$, we have $q - 1 = 2^A m$ and $q + 1 = 2\left(2^{A-1}m + 1\right) = 2m'$, where m' is odd. Thus $v_2(q-1) = A$, and $v_2(q+1) = 1$. Hence, $K = v_2(q-1) + v_2(d_r) + v_2(q+1) - 1 = A + v_2(d_r)$.

If $q \equiv 3 \pmod 4$, we have $q - 1 = 2\left(2^{A-1}m - 1\right)$ and $q + 1 = 2^A m$. Thus $v_2(q-1) = 1$ and $v_2(q+1) = A$. Hence, $K = v_2(q-1) + v_2(d_r) + v_2(q+1) - 1 = A + v_2(d_r)$.

Now if d_r is odd, by Lemma 3.6, $K = v_2(q-1)$. If $q \equiv 1 \pmod 4$, then $K = A$. Otherwise, if $q \equiv 3 \pmod 4$, then $K = 1$. □

The following result represents an improvement over Theorem 1.5 in [26]. Later on we use it often in the following sections.

Theorem 3.8. *Let* $q = p^s$ *be a power of an odd prime* p, *let* $r \geq 3$ *be any odd number such that* $\gcd(r, q) = 1$. *Let* $d_r = \mathrm{ord}_r(q)$. *If* d_r *is odd, further assume* $q \equiv 1 \pmod 4$. *Set* $K := v_2\left(q^{d_r} - 1\right)$. *Then for* $n \leq K$ *and any irreducible factor* h_n *of* $\Phi_{2^n r}$, *we have* $\deg(h_n) = d_r$. *Furthermore, if* $0 < n < K$ *strictly, then* $h_n\left(x^2\right)$ *decomposes into precisely two irreducible factors of degree* d_r *which are irreducible factors of* $\Phi_{2^{n+1}r}$. *On the other hand, for any* $n > K$, *if* $\Phi_{2^K r} = \prod_i h_{K_i}$ *is the corresponding factorization over* $\mathbb{F}_q$, *the complete factorization of* $\Phi_{2^n r}$ *over* $\mathbb{F}_q$ *is given by* $\Phi_{2^n r}(x) = \prod_i h_{K_i}(x^{2^{n-K}})$.

Proof. Since $q^{d_r} \equiv 1 \pmod r$ and $K = v_2\left(q^{d_r} - 1\right)$, we have $q^{d_r} \equiv 1 \pmod{2^K r}$. Let $n \leq K$. It is true that $q^{d_r} \equiv 1 \pmod{2^n r}$. Let $d_n = \mathrm{ord}_{2^n r}(q)$. Then $d_n \mid d_r$. On the other hand, $q^{d_n} \equiv 1 \pmod{2^n r}$ gives $q^{d_n} \equiv 1 \pmod r$ implying $d_r \mid d_n$. Consequently, $d_n = d_r$. Recalling that the degree of each irreducible factor of $\Phi_{2^n r}$ is $\mathrm{ord}_{2^n r}(q) = d_n$, we conclude that for $n \leq K$, each irreducible factor of $\Phi_{2^n r}$ has degree d_r.

For $0 < n < K$, let h_n be an irreducible factor (of degree d_r) of $\Phi_{2^n r}$. Then $h_n\left(x^2\right)$ has degree $2d_r$ and is a factor of $\Phi_{2^{n+1}r}$ clearly. Because $n + 1 \leq K$, then $h_n\left(x^2\right)$ must decompose into an amount z of irreducibles of degree d_r. But this is possible only if $z = 2$.

Note $e = 2^K r$ is the order of $\Phi_{2^K r}$ and thus the order of any irreducible factor h_K of it. By definition, $2^{K+1} \nmid \left(q^{d_r} - 1\right)$. Hence, $2 \nmid \left(q^{d_r} - 1\right)/e$, and by Lemma 3.4, $h_K\left(x^2\right)$ is irreducible over $\mathbb{F}_q$. If d_r is even, then $K > 2$ by Lemma 3.7. If d_r is odd, then $q \equiv 1 \pmod 4$ by assumption, and so $K = A \geq 2$ by Lemma 3.7. Then $2^2 = 4 \mid \left(q^{d_r} - 1\right)$. As a result, for $n > K$, Lemma 3.4 gives $h_K\left(x^{2^{n-K}}\right)$ is irreducible over $\mathbb{F}_q$. Because

$$\Phi_{2^n r}(x) = \Phi_{2^K r}\left(x^{2^{n-K}}\right) = \prod_i h_{K_i}\left(x^{2^{n-K}}\right),$$

where $\Phi_{2^K r} = \prod_i h_{K_i}$ is the corresponding factorization, the factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is complete. □

Whenever d_r is even, or $q \equiv 1 \pmod 4$, the bound $K = v_2\left(q^{d_r} - 1\right)$ in Theorem 3.8 represents an improvement over the bound $L = v_2\left(q^{\phi(r)} - 1\right)$ of Theorem 1.5 due to L. Wang and Q. Wang [26]. This is because $K \leq L$ as $\left(q^{d_r} - 1\right) \mid \left(q^{\phi(r)} - 1\right)$. Moreover, it is clear that K is the smallest bound with the property that $\Phi_{2^n r}(x) = \prod_i h_{K_i}\left(x^{2^{n-K}}\right)$ is the corresponding factorization over $\mathbb{F}_q$ for $n > K$. In Theorem 3.13 we will show that, in particular, when d_r is odd and $q \equiv 3 \pmod 4$, the corresponding bound is $v_2(q+1) = A$. That is, if $\Phi_{2^A r} = \prod_i h_{A_i}$ is the corresponding factorization, then for $n > A$ the factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by $\Phi_{2^n r}(x) = \prod_i h_{A_i}\left(x^{2^{n-A}}\right)$.

3.2. **Notations.** We use the following notations. Let $\Omega(r)$ be the set of primitive r-th roots of unity and let U_n be the set of primitive 2^n-th roots of unity. Similarly as done in [26] we let the expression

$$\prod_{a\in A}\cdots\prod_{b\in B} f_i(x,a,\ldots,b)$$

denote the product of *distinct* polynomials $f_i(x,a,\ldots,b)$ satisfying conditions $a\in A,\ldots,b\in B$. For example, if we let g_w be an irreducible factor of Φ_r with root w, say in $\mathbb{F}_{q^{d_r}}$, then in the product $\prod_{w\in\Omega(r)} g_w$ we take g_w and not any of $g_{w^{q^i}}$ as $g_w = g_{w^{q^i}}$ in this case.

Recall the *elementary symmetric polynomials* S_i defined by

$$S_i(x_1,x_2,\ldots,x_n) = \sum_{k_1<k_2<\cdots<k_i} x_{k_1}x_{k_2}\ldots x_{k_i}$$

for any $i=1,2,\ldots,n$, with $S_0=1$. The following proposition is a well known fact.

Proposition 3.9 (**Theorem 3, Section 4.5,** [18])**.** *Write $S_i = S_i(x_1,x_2,\ldots,x_n)$ for $1\le i\le n$. Then*

$$\prod_{i=1}^{n}(x-x_i) = \sum_{i=0}^{n}(-1)^i S_i x^{n-i}.$$

From now on for any proper element $w\in\mathbb{F}_{q^n}$, i.e. $\mathbb{F}_q(w)=\mathbb{F}_{q^n}$, we use the notation $S_{i,w} = S_i\left(w,w^q,\ldots,w^{q^{n-1}}\right)$.

3.3. **Factorization of $\Phi_{2^n r}$ when $q\equiv 1 \pmod 4$.** In this section and the following we make the assumption that the explicit factorization of Φ_r is given to us as a known. One may use for instance the results due to Stein (2001) to compute the factors of Φ_r efficiently when $q=p$ and r is an odd prime distinct to p. First, we need the following well known theorem concerning the factorization of Φ_{2^n} when $q\equiv 1 \pmod 4$ which follows from Theorems 2.47 and 3.35 in [15].

Theorem 3.10 ([15])**.** *Let $q\equiv 1 \pmod 4$, i.e. $q=2^A m+1$, $A\ge 2$, m odd. Let U_n denote the set of primitive 2^n-th roots of unity.*

(a) If $2\le n\le A$, then $\mathrm{ord}_{2^n}(q)=1$ and Φ_{2^n} is the product of 2^{n-1} irreducible linear factors over $\mathbb{F}_q$:

$$\Phi_{2^n}(x) = \prod_{u\in U_n}(x+u).$$

(b) If $n>A$, then $\mathrm{ord}_{2^n}(q)=2^{n-A}$ and Φ_{2^n} is the product of 2^{A-1} irreducible binomials over $\mathbb{F}_q$ of degree 2^{n-A} :

$$\Phi_{2^n}(x) = \prod_{u\in U_A}\left(x^{2^{n-A}}+u\right).$$

First recall that whenever $\gcd(q,n)=1$, Φ_n decomposes into $\phi(n)/\mathrm{ord}_n(q)$ irreducibles over $\mathbb{F}_q$ of degree $\mathrm{ord}_n(q)$ (Theorem 2.47, [15]). In particular, Φ_r decomposes into irreducibles of degree $d_r := \mathrm{ord}_r(q)$ over $\mathbb{F}_q$ when q, r are coprime.

We now give the factorization of $\Phi_{2^n r}$ when $q\equiv 1 \pmod 4$.

Theorem 3.11. *Let $q\equiv 1 \pmod 4$, say $q=2^A m+1$, $A\ge 2$, m odd. Let $r\ge 3$ be odd such that $\gcd(q,r)=1$, and let $d_r=\mathrm{ord}_r(q)$.*

1. If $n=1$, then

$$\Phi_{2r}(x) = \prod_{w\in\Omega(r)}\left(\sum_{i=0}^{d_r} S_{i,w}x^{d_r-i}\right)$$

is the complete factorization of Φ_{2r} *over* $\mathbb{F}_q$.
2. If $2 \leq n \leq A$, *then*

$$\Phi_{2^n r}(x) = \prod_{u \in U_n} \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} u^i S_{i,w} x^{d_r - i} \right)$$

is the complete factorization of $\Phi_{2^n r}$ *over* $\mathbb{F}_q$.
3. If $n > A$, *we have:*
(a) If d_r *is odd, then*

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} u^i S_{i,w} x^{2^{n-A}(d_r - i)} \right).$$

is the complete factorization of $\Phi_{2^n r}$, $n > A$, *over* $\mathbb{F}_q$.
(b) If d_r *is even, then:*
(i) For $A < n \leq K$, *the complete factorization of* $\Phi_{2^n r}$ *over* $\mathbb{F}_q$ *is given by*

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(x^{d_r} + \sum_{i=1}^{d_r} a_{n_i} x^{d_r - i} \right)$$

where each a_{n_i}, $1 \leq i \leq d_r$, *satisfies the following system of non-linear recurrence relations*

$$\left\{ \sum_{i+j=2k} (-1)^j a_{n_i} a_{n_j} = a_{(n-1)_k}, \qquad 1 \leq k \leq d_r \right\}$$

with initial values $a_{A_k} = u^k S_{k,w}$, $1 \leq k \leq d_r$, *where* $a_{n_i} = 0$ *for* $i > d_r$, *and* $a_{n_0} = 1$.
(ii) For $n > K$, *the complete factorization of* $\Phi_{2^n r}$ *over* $\mathbb{F}_q$ *is given by*

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(x^{2^{n-K} d_r} + \sum_{i=1}^{d_r} a_{K_i} x^{2^{n-K}(d_r - i)} \right)$$

where each a_{K_i}, $1 \leq i \leq d_r$, *is as obtained in (i).*

Proof. Let

$$\Phi_r(x) = \prod_{w \in \Omega(r)} g_w(x) = \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} (-1)^i S_{i,w} x^{d_r - i} \right)$$

be the factorization of Φ_r over $\mathbb{F}_q$.
1. $(n = 1)$: Because g_w is irreducible over $\mathbb{F}_q$, $g_w(-x)$ is irreducible over $\mathbb{F}_q$. By Lemma 3.5,

$$\Phi_{2r}(x) = \Phi_r(-x) = \prod_{w \in \Omega(r)} g_w(-x) = \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} (-1)^{d_r} S_{i,w} x^{d_r - i} \right).$$

Note that, in the case d_r odd, the number of irreducible factors of Φ_{2r}, which is $\phi(r)/d_r$, is even. Thus it follows that we may write the factorization above as

$$\Phi_{2r}(x) = \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} S_{i,w} x^{d_r - i} \right).$$

The factorization is complete.
2. By Theorem 3.10 (a) and Corollary 3.2 we have

$$\Phi_{2^n r}(x) = \left(\Phi_{2^n} \odot \Phi_r \right)(x) = \prod_{u \in U_n} \prod_{w \in \Omega(r)} \left((x + u) \odot g_w \right)(x).$$

By Proposition 2.1,

$$\begin{aligned}((x+u)\odot g_w)(x) &= (-u)^{d_r} g_w\left((-u)^{-1}x\right) = (-u)^{d_r}\sum_{i=0}^{d_r}(-1)^i S_{i,w}(-u)^{i-d_r}x^{d_r-i}\\ &= \sum_{i=0}^{d_r} S_{i,w}u^i x^{d_r-i}.\end{aligned}$$

Noting that each $(x+u)\odot g_w$ is irreducible over $\mathbb{F}_q$ by Theorem 2.3, these factors give us a complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ for $2\le n\le A$.

3 (a): Since $q\equiv 1 \pmod 4$ and d_r is odd, Lemma 3.7 gives $K=A$; consequently if $\Phi_{2^A r}=\prod_i h_{A_i}$ is the corresponding factorization over $\mathbb{F}_q$, then Theorem 3.8 gives that for $n>A$, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by $\Phi_{2^n r}(x)=\prod_i h_{A_i}\left(x^{2^{n-A}}\right)$. Thus it only remains to make the substitution $x\to x^{2^{n-A}}$ in each irreducible factor h_{A_i} obtained in Part 2 as the statement in the theorem shows.

(b) (i) ($A<n\le K$ and d_r even): Let h_{n-1} be an irreducible factor of $\Phi_{2^{n-1}r}$. By Theorem 3.8, $\deg(h_{n-1})=d_r$ and $h_{n-1}\left(x^2\right)$ decomposes into two irreducibles of degree d_r which are irreducible factors of $\Phi_{2^n r}$. Let $h_{n-1}\left(x^2\right)=f_n(x)g_n(x)$ be the corresponding factorization. First, we show $g_n(x)=f_n(-x)$. Let α be a root of f_n. We claim that $-\alpha$ is not a root of f_n. On the contrary, suppose $f_n(-\alpha)=0$. Then $-\alpha=\alpha^{q^i}$ for some $i\in[0,d_r-1]$ implies $-1=\alpha^{q^i-1}$ and $1=\alpha^{2\left(q^i-1\right)}$. But then $\mathrm{ord}(\alpha)=2^n r \mid 2\left(q^i-1\right)$ and so $r\mid\left(q^i-1\right)$. However, this contradicts $\mathrm{ord}_r(q)=d_r>i$. Therefore $f_n(-\alpha)\neq 0$. Now, we have

$$f_n(-\alpha)g_n(-\alpha)=h_{n-1}\left((-\alpha)^2\right)=h_{n-1}\left(\alpha^2\right)=f_n(\alpha)g_n(\alpha)=0.$$

As $f_n(-\alpha)\neq 0$, necessarily $g_n(-\alpha)=0$. Thus both $f_n(-x),\ g_n(x)$ have $-\alpha$ as a root. But then since both $f_n(-x),\ g_n(x)$ are monic irreducible polynomials over $\mathbb{F}_q$ of degree d_r, it must be that $g_n(x)=f_n(-x)$. Therefore $h_{n-1}(x^2)=f_n(x)f_n(-x)$ is the corresponding factorization. We may write

$$h_{n-1}(x)=x^{d_r}+\sum_{k=1}^{d_r}a_{(n-1)_k}x^{d_r-k}$$

and

$$f_n(x)=x^{d_r}+\sum_{i=1}^{d_r}a_{n_i}x^{d_r-i}$$

for some coefficients $a_{(n-1)_k},\ a_{n_i}\in\mathbb{F}_q$. Now, $h_{n-1}(x^2)=f_n(x)f_n(-x)$ gives

$$\begin{aligned}x^{2d_r}+\sum_{k=1}^{d_r}a_{(n-1)_k}x^{2(d_r-k)} &= \left(x^{d_r}+\sum_{i=1}^{d_r}a_{n_i}x^{d_r-i}\right)\left(x^{d_r}+\sum_{j=1}^{d_r}a_{n_j}(-1)^j x^{d_r-j}\right)\\ &= x^{2d_r}+\sum_{k=1}^{2d_r}\sum_{i+j=k}(-1)^j a_{n_i}a_{n_j}x^{2d_r-k}\\ &= x^{2d_r}+\sum_{k=1}^{d_r}\sum_{i+j=2k}(-1)^j a_{n_i}a_{n_j}x^{2(d_r-k)}.\end{aligned}$$

The last equality followed from the fact that the coefficients of odd powers of x in $h_{n-1}(x^2)$ are 0. Comparing coefficients on each side we see that each $a_{n_i},\ 1\le i\le d_r$, satisfies the following system of

non-linear equations

$$\left\{ \sum_{i+j=2k} (-1)^j a_{n_i} a_{n_j} = a_{(n-1)_k}, \qquad 1 \le k \le d_r \right\}.$$

We know the system must have a solution, otherwise $h_{n-1}(x^2) \neq f_n(x) f_n(-x)$ contrary to the previous arguments. Moreover, the solution must be unique by the uniqueness of factorizations. Furthermore, the reader can see that we can obtain the coefficients of f_n, and hence of $f_n(-x)$, by a recursion where the initial values are the coefficients $a_{A_k} = u^k S_{k,w},\ 1 \le k \le d_r$ of an irreducible factor of $\Phi_{2^A r}$ which we already know from Part 1. Next, we show that we can obtain all the irreducible factors of $\Phi_{2^n r}$ in this way. We claim that for any two distinct initial-value sets $I = \{u_i^k S_{k,w}\},\ J = \{u_j^k S_{k,w}\}$, all the irreducible factors generated by I and J are distinct. By induction on n where $A < n \le K$: Let $g_A,\ h_A$ be the distinct irreducible factors of $\Phi_{2^A r}$ corresponding to I and J. Then in particular $g_A(x^2) \neq h_A(x^2)$. As each of these decomposes into two irreducible factors of the form $f_{A+1}(x),\ f_{A+1}(-x)$, then all four irreducible factors must be distinct. Otherwise if they share an irreducible factor, say $f_{A+1}(-x)$, then necessarily they must share $f_{A+1}(x)$ resulting in $g_A(x^2) = h_A(x^2)$, a contradiction. Similarly one can show that the inductive step follows from the inductive hypothesis. The claim now follows. Consequently, if we let $s = n - A$, then each initial-value set $\{u^k S_{k,w}\}$ corresponding to an irreducible factor g_A of $\Phi_{2^A r}$ will generate a total of 2^s distinct irreducible factors of $\Phi_{2^n r}$. Since there are $\phi(2^A r)/d_r$ irreducible factors of $\Phi_{2^A r}$, the initial-value sets generate a total of $2^s \phi(2^A r)/d_r = 2^{s+A-1}\phi(r)/d_r = 2^{n-1}\phi(r)/d_r = \phi(2^n r)/d_r$ distinct irreducible factors of $\Phi_{2^n r}$, as desired. The factorization is complete.

(ii) $(n > K)$: If $\Phi_{2^K r} = \prod_i h_{K_i}$ is the corresponding factorization, then by Theorem 3.8, for $n > K$, we obtain $\Phi_{2^n r}(x) = \prod_i h_{K_i}\left(x^{2^{n-K}}\right)$ as its complete factorization. Since each h_{K_i} is already known from Part (i), it only remains to make the substitution $x \to x^{2^{n-K}}$ in each h_{K_i} to obtain each irreducible factor of $\Phi_{2^n r}$, as the statement in the theorem shows. The proof of (ii) is complete. □

Remark 3.2. *In order to obtain each irreducible factor of $\Phi_{2^n r}$, for any $n \in \mathbb{N}$, we require at most $v_2(d_r)$ iterations of the system of non-linear recurrence relations in (i): For $n \le A$, the explicit factorization is already given in Parts 1 and 2. However, for $A < n \le K$ and d_r even, the system of non-linear recurrence relations in (i) must iterate for $n - A$ steps. In the case $A < n = K$, the system will iterate for the maximum number of steps $K - A$. By Lemma 3.7, this equals $v_2(d_r)$.*

Remark 3.3. *We can also formulate the factorization of $\Phi_{2^n r},\ 1 \le n \le K$, in terms of the non-linear recurrence relation in (i) with initial values corresponding to $n = 1$. For small finite fields and small d_r, this can be computed fairly fast.*

Remark 3.4. *Let $n > K$, let $S = \{s_k\},\ T = \{t_k\}$ be homogeneous LRS's with characteristic polynomials $\Phi_{2^n},\ \Phi_r$ respectively. Then as discussed earlier, the characteristic polynomial of $ST = \{s_k t_k\}$ is $\Phi_{2^n r} = \Phi_{2^n} \odot \Phi_r$. Since all irreducible factors of $\Phi_{2^n r},\ n > K$, have degree $2^{n-K} d_r$, the minimal polynomial of ST must have degree $2^{n-K} d_r$. This is the linear complexity of ST. Note that if we let $n \to \infty$, the linear complexity of the corresponding LRS ST approaches infinity.*

For the subcases $q \equiv 1 \pmod 4$ with $q \equiv \pm 1 \pmod r$ and thus $d_r = 1,\ 2$, where r is an odd prime, Theorem 3.11 becomes Theorem 1, Parts 2 and 4 in Fitzgerald and Yucas (2007) [11].

3.4. **Factorization of $\Phi_{2^n r}$ when $q \equiv 3 \pmod 4$.** We need the following result due to Meyn (1996) [16].

Theorem 3.12 (**Theorem 1,** [16])**.** *Let $q \equiv 3 \pmod 4$, i.e. $q = 2^A m - 1,\ A \ge 2,\ m$ odd. Let $n \ge 2$.*

(a) If $n \le A$, then Φ_{2^n} is the product of 2^{n-2} irreducible trinomials over $\mathbb{F}_q$:

$$\Phi_{2^n}(x) = \prod_{u \in U_n} \left(x^2 + \left(u + u^{-1}\right) x + 1\right).$$

(b) If $n > A$, then Φ_{2^n} is the product of 2^{A-2} irreducible trinomials over $\mathbb{F}_q$:

$$\Phi_{2^n}(x) = \prod_{u \in U_A} \left(x^{2^{n-A+1}} + \left(u - u^{-1}\right) x^{2^{n-A}} - 1 \right).$$

We are now ready to give the factorization of $\Phi_{2^n r}$ when $q \equiv 3 \pmod 4$.

Theorem 3.13. *Let $q \equiv 3 \pmod 4$, i.e. $q = 2^A m - 1$, $A \geq 2$, m odd. Let $r \geq 3$ be odd such that $\gcd(q, r) = 1$, and let $d_r = \mathrm{ord}_r(q)$.*
1. If $n = 1$, then

$$\Phi_{2r}(x) = \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} S_{i,w} x^{d_r - i} \right)$$

is the complete factorization of Φ_{2r} over $\mathbb{F}_q$.
2. If $2 \leq n \leq A$, we have:
(i) If d_r is odd, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by

$$\Phi_{2^n r}(x) = \prod_{u \in U_n} \prod_{w \in \Omega(r)} \left(\sum_{k=0}^{2d_r} \sum_{i+j=k} S_{i,w} S_{j,w} u^{i-j} x^{2d_r - k} \right).$$

(ii) If d_r is even, $\Phi_{2^n r}$ decomposes into irreducibles of degree d_r over $\mathbb{F}_q$ so that

$$\Phi_{2^n r}(x) = \prod_{u \in U_n} \prod_{w \in \Omega(r)} \left[\left(x^{d_r} + \sum_{i=1}^{d_r} a_{n_i} x^{d_r - i} \right) \left(x^{d_r} + \sum_{j=1}^{d_r} b_{n_j} x^{d_r - j} \right) \right]$$

is the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$, where each a_{n_i}, $b_{n_j} \in \mathbb{F}_q$, $1 \leq i, j \leq d_r$, satisfies the following system of equations

$$\left\{ \sum_{i+j=k} a_{n_i} b_{n_j} = \sum_{i+j=k} S_{i,w} S_{j,w} u^{i-j}, \qquad 1 \leq k \leq 2d_r \right\},$$

with $a_{n_i}, b_{n_j} = 0$ if $i > d_r$ or $j > d_r$, and $a_{n_0} = b_{n_0} = 1$.
3. If d_r is odd, then for $n > A$ the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(\sum_{k=0}^{2d_r} \sum_{i+j=k} u^{i-j} S_{i,w} S_{j,w} x^{2^{n-A}(2d_r - k)} \right).$$

4. If d_r is even, we have:
(iii) For $A < n \leq K$, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(x^{d_r} + \sum_{i=1}^{d_r} a_{n_i} x^{d_r - i} \right)$$

where each a_{n_i}, $1 \leq i \leq d_r$, satisfies the following system of non-linear recurrence relations

$$\left\{ \sum_{i+j=2k} (-1)^j a_{n_i} a_{n_j} = a_{(n-1)_k}, \qquad 1 \leq k \leq d_r \right\}$$

with initial values a_{A_k}, $1 \leq k \leq d_r$, as obtained in (ii), where $a_{n_i} = 0$ for $i > d_r$, and $a_{n_0} = 1$.

(iv) For $n > K$, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by

$$\Phi_{2^n r}(x) = \prod_{u\in U_A}\prod_{w\in\Omega(r)}\left(x^{2^{n-K}d_r} + \sum_{i=1}^{d_r} a_{K_i} x^{2^{n-K}(d_r-i)}\right)$$

where each $a_{K_i},\ 1 \le i \le d_r$, is as obtained in (iii).

Proof. Let

$$\Phi_r(x) = \prod_{w\in\Omega(r)} g_w(x) = \prod_{w\in\Omega(r)}\left(\sum_{i=0}^{d_r}(-1)^i S_{i,w} x^{d_r-i}\right)$$

be the factorization of Φ_r over $\mathbb{F}_q$.
1. $(n = 1)$: Similar to Part 1 in Theorem 3.11.
2. $(2 \le n \le A)$: By Theorem 3.12 (a) we have

$$\begin{aligned}
\Phi_{2^n r}(x) &= \prod_{u\in U_n}\prod_{w\in\Omega(r)}\left(\left(x^2 + \left(u + u^{-1}\right)x + 1\right)\odot g_w\right)(x)\\
&= \prod_{u\in U_n}\prod_{w\in\Omega(r)}(-u)^{d_r} g_w\left((-u)^{-1}x\right)(-u)^{-d_r} g_w(-ux)\\
&= \prod_{u\in U_n}\prod_{w\in\Omega(r)}\left(\sum_{i=0}^{d_r}(-1)^i S_{i,w}(-u)^{i-d_r}x^{d_r-i}\right)\left(\sum_{j=0}^{d_r}(-1)^j S_{j,w}(-u)^{d_r-j}x^{d_r-j}\right)\\
&= \prod_{u\in U_n}\prod_{w\in\Omega(r)}\left(\sum_{k=0}^{2d_r}\sum_{i+j=k} S_{i,w}S_{j,w}u^{i-j}x^{2d_r-k}\right). \qquad (*)
\end{aligned}$$

First, note that these factors in $(*)$ are over $\mathbb{F}_q$ as the composed product of polynomials over $\mathbb{F}_q$ are polynomials over $\mathbb{F}_q$. We have:

(i) If d_r is odd, then $\gcd(2, d_r) = 1$ and so each factor $\left(x^2 + \left(u + u^{-1}\right)x + 1\right)\odot g_w$ is irreducible by Theorem 2.3; hence the factorization is complete.

(ii) If d_r is even, then in particular $A < A + v_2(d_r) = K$. Then by Theorem 3.8 each factor in $(*)$ of $\Phi_{2^n r}$ must decompose into two irreducibles of degree d_r. Thus, for some coefficients $a_{n_i},\ b_{n_j} \in \mathbb{F}_q$ we must have

$$\begin{aligned}
\sum_{k=0}^{d_r}\sum_{i+j=k} S_{i,w}S_{j,w}u^{i-j}x^{2d_r-k} &= \left(x^{d_r} + \sum_{i=1}^{d_r} a_{n_i}x^{d_r-i}\right)\left(x^{d_r} + \sum_{j=1}^{d_r} b_{n_j}x^{d_r-j}\right)\\
&= x^{2d_r} + \sum_{k=1}^{2d_r}\sum_{i+j=k} a_{n_i}b_{n_j}x^{2d_r-k}.
\end{aligned}$$

Comparing coefficients on each side we see that each $a_{n_i},\ b_{n_j},\ 1 \le i,\ j \le d_r$, satisfies the following system of equations

$$\left\{\sum_{i+j=k} a_{n_i}b_{n_j} = \sum_{i+j=k} S_{i,w}S_{j,w}u^{i-j}, \qquad 1 \le k \le 2d_r\right\}$$

which has a solution. We stress that the solution must be unique by the uniqueness of factorizations. Hence the result follows.

3. ($n > A$ and d_r odd): Since $\gcd\left(2^{n-A+1}, d_r\right) = 1$, the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ is given by

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(\left(x^{2^{n-A+1}} + \left(u - u^{-1}\right) x^{2^{n-A}} - 1 \right) \odot g_w \right)(x).$$

Since the computation of the composed product above is somewhat more involved this time, we proceed as follows: First note that for $n > A$ all irreducible factors of $\Phi_{2^n r}$ have degree $2^{n-A+1} d_r$. It then follows that if a factor of $\Phi_{2^n r}$ has degree $2^{n-A+1} d_r$, it must be an irreducible factor. Because $q = 2^A m - 1$, we know that $2^A \mid (q+1)$ and $q^2 - 1 = (q+1)(q-1)$ imply that if $u \in U_A$, then $u^{q+1} = 1$ and so $u \in \mathbb{F}_{q^2}$. Note that since $q \equiv 3 \pmod 4$, then $q^2 \equiv 1 \pmod 4$. Then by Theorem 3.11, Part 3 (a), the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_{q^2}$ is given by

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(\sum_{i=0}^{d_r} u^i S_{i,w} x^{2^{n-A}(d_r - i)} \right). \qquad (**)$$

Let $Z_u(x) = \sum_{i=0}^{d_r} u^i S_{i,w} x^{2^{n-A}(d_r-i)}$ above, and since $u^q = u^{-1}$, consider its conjugate

$$\overline{Z}_u(x) = \sum_{j=0}^{d_r} u^{-j} S_{j,w} x^{2^{n-A}(d_r - j)}.$$

First, note that $u^{-1} \in U_A$ and $(**)$ imply $\overline{Z}_u$ is an irreducible factor of $\Phi_{2^n r}$ over $\mathbb{F}_{q^2}$. Moreover, $Z_u \neq \overline{Z}_u$. Indeed, observe that $u^{d_r} \neq u^{-d_r}$, otherwise $u^{2d_r} = 1$, and so $\mathrm{ord}(u) = 2^A$ gives $2^A \mid 2d_r$ contrary to $A \geq 2$ and d_r odd. Then $u^{d_r} S_{d_r,w} \neq u^{-d_r} S_{d_r,w}$. As these are the coefficients of x^0 in $Z_u(x)$, $\overline{Z}_u(x)$, respectively, necessarily $Z_u \neq \overline{Z}_u$.

We have

$$Z_u(x)\overline{Z}_u(x) = \sum_{k=0}^{2d_r} \sum_{i+j=k} u^{i-j} S_{i,w} S_{j,w} x^{2^{n-A}(2d_r - k)}.$$

Note from Part 2 and $(*)$ above that for $u \in U_A$ we have $\sum_{i+j=k} u^{i-j} S_{i,w} S_{j,w} \in \mathbb{F}_q$ (since the composed products of polynomials over $\mathbb{F}_q$ are polynomials over $\mathbb{F}_q$). Thus $Z_u \overline{Z}_u \in \mathbb{F}_q[x]$, it has degree $2^{n-A+1} d_r$, and is a factor of $\Phi_{2^n r}$ clearly. But then $Z_u \overline{Z}_u$ must be irreducible over $\mathbb{F}_q$; hence the complete factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ must be

$$\Phi_{2^n r}(x) = \prod_{u \in U_A} \prod_{w \in \Omega(r)} \left(\sum_{k=0}^{2d_r} \sum_{i+j=k} u^{i-j} S_{i,w} S_{j,w} x^{2^{n-A}(2d_r - k)} \right)$$

as required.

4. (iii) Similar to the proof of (i) in Theorem 3.11.
   (iv) Similar to the proof of (ii) in Theorem 3.11. □

Remark 3.5. *See Remark 3.2 after Theorem 3.11. Furthermore, comparing the factorizations in Parts 2 (i) and 3, we see that the factors in Part 3 can be obtained from the factors in Part 2 (i) by the substitution* $x \to x^{2^{n-A}}$. *Thus, for* $n > A = v_2(q+1)$, *if* $\Phi_{2^A r} = \prod_k h_{A_k}$ *is the corresponding factorization, then* $\Phi_{2^n r}(x) = \prod_k h_{A_k}(x^{2^{n-A}})$ *is the complete factorization over* $\mathbb{F}_q$. *Moreover, it is easy to see that* $A = v_2(q+1)$ *is the smallest such bound with this property.*

Remark 3.6. *In the case* d_r *is even, see Remarks 3.3 and 3.4 after Theorem 3.11.*

Remark 3.7. *Let* $n > A$, *let* $S = \{s_k\}$, $T = \{t_k\}$ *be homogeneous LRS's with characteristic polynomials* Φ_{2^n}, Φ_r *respectively. Then as discussed earlier, the characteristic polynomial of* $ST = \{s_k t_k\}$ *is* $\Phi_{2^n r} = \Phi_{2^n} \odot \Phi_r$. *Suppose* d_r *is odd. Since all irreducible factors of* $\Phi_{2^n r}$, $n > A$, *have degree* $2^{n-A+1} d_r$, *the*

minimal polynomial of ST must have degree $2^{n-A+1}d_r$. *This is the linear complexity of ST. Note that if we let* $n \to \infty$, *the linear complexity of the corresponding LRS ST approaches infinity.*

For the subcases $q \equiv 3 \pmod 4$ with $q \equiv \pm 1 \pmod r$, and thus $d_r = 1,\ 2$, where r is an odd prime, Theorem 3.13 becomes Theorem 1, Parts 1 and 3 in Fitzgerald and Yucas (2007) [11].

4. Conclusion

In this paper we gave the factorization of the cyclotomic polynomial $\Phi_{2^n r}$ over $\mathbb{F}_q$ where both $r \geq 3$, q are odd and $\gcd(q, r) = 1$. Previously, only $\Phi_{2^n 3}$ and $\Phi_{2^n 5}$ had been factored in [11] and [26], respectively. As a result we have obtained infinite families of irreducible sparse polynomials from these factors. However, it would be desirable to obtain the time complexities of the non-linear recurrence relation in Theorem 3.11 (i) (Theorem 3.13 (iii) is similar) and we leave it for a future study. Furthermore, we showed how to obtain the factorization of Φ_n in a special case (see Theorem 3.1). We also showed in Theorem 3.3 how to obtain the factorization of Φ_{mn} from the factorization of Φ_n when q is a primitive root modulo m and $\gcd(m, n) = \gcd(\phi(m), \mathrm{ord}_n(q)) = 1$.

The factorization of Φ_{2^n} was already given in [15] when $q \equiv 1 \pmod 4$ and in [16] when $q \equiv 3 \pmod 4$. It is natural to consider the generalization of Theorem 3.8 to allow for other cases (besides 2^n); this is currently in progress. It is expected that these irreducible factors will be sparse as well. Note that we can allow q to be even in this case by forcing r to be odd. This is significant as the fields $\mathbb{F}_{2^s}$ are the most commonly used in modern engineering.

In Section 2 we considered irreducible composed products of the form $f \odot \Phi_m$. In particular, we derived the construction of a new class of irreducible polynomials in Theorem 2.11. It is natural to consider other classes of polynomials and substitute them for Φ_m and see what the result may be.

We also gave formulas for the linear complexity of ST when $\Phi_{2^n},\ \Phi_r$ are characteristic polynomials of the homogeneous LRS's $S,\ T$, respectively. We showed that by letting $n \to \infty$, the linear complexity of ST will approach infinity.

Another matter of interest is the factorization of composed products. Since the minimal polynomial of a LRS, say ST, is an irreducible factor of some composed product, this has applications in stream cipher theory, LFSR and LRS in general. D. Mills (2001) [17] had already studied the factorization of arbitrary composed products. In particular, if $\deg f = m$ and $\deg g = n$ with $f,\ g$ irreducible over $\mathbb{F}_q$, Mills gave $d = \gcd(m, n)$ as an upper bound for the number of irreducible factors that $f \diamond g$ could decompose into. He also gave the possible degrees that these irreducible factors may attain. As a result, we now know the possible linear complexities that ST could attain. On the other hand his work was generalized for two arbitrary irreducible polynomials f and g. In the case that at least one of these polynomials belongs to a certain class of polynomials with well defined properties, we wonder if it could be possible to obtain more precise information regarding the number of irreducible factors and their degrees. For instance, in the case of $f \odot \Phi_m$, can we know precisely the degrees of the irreducible factors? Can we know precisely in how many irreducible factors does $f \odot \Phi_m$ decompose into? Note that the subject of the factorization of composed products is one for which very little research has been done. Currently, the authors were able to find only one paper [17] on this matter and they feel this is a topic that has been somewhat neglected.

References

[1] T. M. Apostol (1976). *Introduction to Analytic Number Theory*, Springer-Verlag New York Inc.

[2] A. S. Bamunoba (2010). *Cyclotomic Polynomials*, African Institute for Mathematical Sciences, Stellenbosch University, South Africa. Available at: http://users.aims.ac.za/∼bamunoba/bamunoba.pdf

[3] E. R. Berlekamp (1982). *Bit-serial Reed-Solomon Encoders*, IEEE Trans. Info. Theory **28**, 869-874.

[4] F. R. Beyl (1977). *Cyclic Subgroups of the Prime Residue Group*, Amer. Math. Monthly **84**, 46-68.

[5] I. Blake, S. Gao and D. Mills (1991). *Factorization of Polynomials of the type* $f\left(x^t\right)$, presented at the International Conference on Finite Fields, Coding Theory, and Advances in Comm. and Computing, Las Vegas.

[6] J. V. Brawley and L. Carlitz (1987). *Irreducibles and the Composed Product for Polynomials over a Finite Field*, Discrete Math., **65**, 115-139.
[7] J. V. Brawley, S. Gao and D. Mills (1997). *Computing Composed Products of Polynomials*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), 1-15, Contemp. Math., **225**, Amer. Math. Soc., Providence, RI.
[8] S. D. Cohen (1969). *On Irreducible Polynomials of certain types in Finite Fields*, Proc. Cambridge Philos. Soc. **66**, 335-344.
[9] S. D. Cohen (2005). *Explicit Theorems on Generator Polynomials over Finite Fields*, Finite Fields Appl. **11**, 337-357.
[10] R. W. Fitzgerald and J. L. Yucas (2005). *Factors of Dickson Polynomials over Finite Fields*, Finite Fields Appl. **11**, no. 4, 724-737.
[11] R. W. Fitzgerald and J. L. Yucas (2007). *Explicit Factorization of Cyclotomic and Dickson Polynomials over Finite Fields*, Arithmetic of Finite Fields, *Lecture Notes in Comput. Sci.* **4547**, Springer, Berlin, 1-10.
[12] Z. Gao and F. Fu (2009). *The Minimal Polynomial over $\mathbb{F}_q$ of Linear Recurring Sequence over $\mathbb{F}_{q^m}$*. Finite Fields Appl. **15**, no. 6, 774-784.
[13] S. Golomb and G. Gong (2005). *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press.
[14] M. K. Kyuregyan and G. H. Kyureghyan (2011). *Irreducible Compositions of Polynomials over Finite Fields*, Designs, Codes and Cryptography, **61**, no. 3, 301-314.
[15] R. Lidl and H. Niederreiter (1997). *Finite Fields*, in Encyclopedia of Mathematics and its Applications, 2nd ed., vol 20, Cambridge University Press, Cambridge.
[16] H. Meyn (1996). *Factorization of the Cyclotomic Polynomials $x^{2^n}+1$ over Finite Fields*, Finite Fields Appl. **2**, 439-442.
[17] D. Mills (2001). *Factorizations of Root-based Polynomial Compositions*, Discrete Math. **240**, no. 1-3, 161-173.
[18] W. K. Nicholson (1999). *Introduction to Abstract Algebra*, 2nd ed., John Wiley & Sons, Inc.
[19] E. S. Selmer (1966). *Linear Recurrence Relations over Finite Fields*, Univ. of Bergen.
[20] G. Stein (2001). *Using the Theory of Cyclotomy to factor Cyclotomic Polynomials over Finite Fields*, Math. Comp. **70**, no. 235, 1237-1251.
[21] B. Sury (1999). *Cyclotomy and Cyclotomic Polynomials: The story of how Gauss narrowly missed becoming a philologist*, RESONANCE, 41-53. Available at: www.springerlink.com/index/h44xt1p4p42m3987.pdf
[22] A. Tuxanidy (2011). *Composed Products and Factorization of Cyclotomic Polynomials over Finite Fields*, Honours Project, Carleton University.
[23] R. Varshamov (1984). *A General Method of Synthesizing Irreducible Polynomials over Galois Fields*, Soviet Math. Dokl., **29**, 334-336.
[24] Z. Wan (2003). *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Co. Pte. Ltd.
[25] M. Wang and I. F. Blake (1989). *Bit-serial Multiplication in Finite Fields*, IEEE Trans. Comput. **38**, 1457-1460.
[26] L. Wang and Q. Wang (2011). *On Explicit Factors of Cyclotomic Polynomials over Finite Fields*, Designs, Codes and Cryptography, Springer Netherlands.
[27] L. C. Washington (1982). *Introduction to Cyclotomic Fields*, Springer-Verlag New York Inc.
[28] N. Zierler and W. H. Mills (1973). *Products of Linear Recurring Sequences*, J. Algebra **27**, 147-157.

Appendix A. Samples of Irreducible Polynomials F_m

We provide a table of examples for Theorem 2.11. MAPLE software was used in the computations.

Table 1. Table of (irreducible) samples of F_m from Theorem 2.11 outputed on inputs (m, q, n) and f.

(m, q, n)	$f(x)$	$F_m(x)$
$(2, 3, 6)$	$x^6 + 2x^4 + x^3 + 2x + 1$	$x^6 + x^5 + 2x^4 + x^3 + x + 2$
$(2, 5, 5)$	$x^5 + 3x^4 + 4x^3 + 4x + 2$	$x^5 + 2x^4 + 4x^3 + 4x + 3$
$(4, 3, 9)$	$x^9 + x^7 + x^6 + x + 1$	$x^{18} + x^{16} + x^{14} + x^{12} + 2x^{10} + x^8 + x^6 + x^2 + 1$
$(4, 7, 3)$	$x^3 + 4x^2 + 1$	$x^6 + 2x^4 + 6x^2 + 1$
$(3^2, 5, 5)$	$x^5 + 3x^4 + 4x^2 + x + 1$	$x^{30} + 3x^{27} + 3x^{24} + 3x^{21} + 3x^{18} + x^{15} + 2x^9 + 4x^6 + 2x^3 + 1$
$(7^2, 3, 5)$	$x^5 + x^4 + x^2 + 2x + 2$	$x^{210} + 2x^{203} + \cdots + 1$
$(6, 5, 9)$	$x^9 + 4x^8 + 3x^7 + x^5 + 3x^4 + 4x^2 + 2x + 3$	$x^{18} + 4x^{17} + 3x^{16} + 2x^{15} + 3x^{14} + x^{11} + x^{10} + 2x^9 + 4x^8 + x^7 + x^6 + x^5 + 2x^4 + 3x^3 + 2x^2 + x + 4$
$(10, 3, 5)$	$x^5 + x^3 + x^2 + 2x + 2$	$x^{20} + 2x^{18} + x^{17} + 2x^{16} + x^{15} + x^{14} + x^{12} + 2x^{10} + 2x^8 + x^7 + 2x^3 + 2x^2 + x + 1$
$(3^2, 2, 5)$	$x^5 + x^2 + 1$	$x^{30} + x^{27} + x^{21} + x^6 + 1$
$(3^3, 2, 5)$	$x^5 + x^2 + 1$	$x^{90} + x^{81} + x^{72} + x^{45} + x^{27} + x^9 + 1$

Appendix B. Recursive Computations

We provide the following tables of examples for Theorems 3.11 (i) and 3.13 (iii). The coefficients $(a_{n_1}, a_{n_2}, \ldots, a_{n_6})$ are the coefficients of the irreducible factors of $\Phi_{2^n r}$ over $\mathbb{F}_q$ for $q = 5,\ 19,\ r = 7,\ n \leq K = 3$, calculated by using the recurrence relations in Theorems 3.11 (i) and 3.13 (iii). In particular, the tables show that these recursive relations, now with initial values corresponding to $n = 1$, may be used to obtain the factors of $\Phi_{2^n r}$ when $n \leq A$ as well. MAPLE software was used in the computations.

Table 2. Factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ where $r = 7,\ q = 5,\ n \leq K = 3$

n	1	2	3
$(a_{n_1}, a_{n_2}, \ldots, a_{n_6})$	(4, 1, 4, 1, 4, 1)	(2, 4, 3, 1, 2, 4) (3, 4, 2, 1, 3, 4)	(1, 4, 3, 2, 4, 2) (4, 4, 2, 2, 1, 2) (2, 1, 4, 2, 3, 3) (3, 1, 1, 2, 2, 3)

Table 3. Factorization of $\Phi_{2^n r}$ over $\mathbb{F}_q$ where $r = 7,\ q = 19,\ n \leq K = 3$

n	1	2	3
$(a_{n_1}, a_{n_2}, \ldots, a_{n_6})$	(18, 1, 18, 1, 18, 1)	(8, 3, 8, 3, 8, 1) (11, 3, 11, 3, 11, 1)	(2, 6, 10, 13, 2, 18) (17, 6, 9, 13, 17, 18) (8, 9, 18, 10, 8, 18) (11, 9, 1, 10, 11, 18)

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.

E-mail address: attorres@connect.carleton.ca

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, Canada.

E-mail address: wang@math.carleton.ca