COMPOSED PRODUCT AND ITS APPLICATIONS

Monika Sangwan (Research scholar) Department of Mathematics,
Guru Jambheshwar University of Science and Technology,
Hisar-125001(India)
Email. monika.gjust@gmail.com

ABSTRACT In this paper, we define composed product and its application for the case q=p^s be a power of a prime number p, and F$_q$ be the finite field with q elements.

INTRODUCTION

1.1 Composed Products and applications. Let q=p^s be a power of a prime number p, and let F$_q$ be the finite field with q elements. The multiplicative version of composed product of two polynomials f, g∈ F$_q$[x] (or composed multiplication for short) defined by

$$(\text{fog})=\prod_{\alpha}\prod_{\beta}(x-\alpha\beta)$$

Where the product $\prod_{\alpha}\prod_{\beta}$ runs over all roots of α, β of f, g respectively, was first introduced by Selmer (1966) [7] for the purpose 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 $a, a_0, a_1,..., a_{k-1}$ be given elements in F$_q$. Then a sequence S= $\{s_0, s_1,...\}$ of elements $s_i \in F_q$ satisfying the relation

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

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 such as linear feedback shift registers (LFSR) are used to generate them. See chapter 8 in [6] 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 [4] 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 polynomial s with higher degrees are therefore preferred.

The polynomial

$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - ... - a \in F_q[x]$

is called the characteristic polynomial of S (see [6]). In 1973, Zierler and Mills [9] showed that the characteristic polynomial of a component wise multiplication of LRS's of 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 $...S_r$ with component wise multiplication, is given by $f_1 \circ f_2 \circ ... f_r$. We refer the reader to page 433-435 in [6] as well. Note that since the required minimal polynomials are the factors of the characteristic polynomials $f_1 \circ f_2 \circ ... f_r$ 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 $\in F_q[x]$ 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 [1] generalized composed multiplications and composed sums in the following.

Definition 1.1 [1] (**Composed Product**) Let G be a non-empty subset of the algebraic closure Γ_q of 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 $\sigma(\alpha\Diamond\beta) = \sigma(\alpha)\sigma(\beta)$ 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 [1] 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 $\circ$ g (respectively, $f\oplus g,$). Other less common examples are

(i) G = $\Gamma_q, \alpha\Diamond\beta=\alpha+\beta-c$, where $c\in F_q$ 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 $\Gamma_q, \alpha\Diamond\beta= f(\alpha,\beta)$ where f(x,y) is any fixed polynomial in F_q[x,y] such that for all $\alpha,\beta\in G$.

Let $M_G[q,x]$ be the set of all monic polynomials over F_q of degree ≥ 1 whose roots lie in G. It is also shown in [1] that the condition $\sigma(\alpha\Diamond\beta)=\sigma(\alpha)\Diamond\sigma(\beta)$ implies that $f\Diamond g\in F_q[x]$. Moreover, if $\Diamond$ is an associative (respectively, commutative) on $M_G[q,x]$. In particular, composed multiplications and sums of polynomials are associative and commutative in F_q[x]. In fact, $(G,\Diamond)$ is an abelian group for composed multiplication, composed addition, and the example in (i) or (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 ([2], [3], [6], [8]). One of the most popular methods of construction is the method of compositions of polynomials

(not to be confused with composed products) where an irreducible polynomial of 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 [3]. Perhaps one of the most applicable result in this area is the following.

1.3 **Theorem 1.2 (Cohen (1969).** Let f and g be two non-irreducible polynomials over F_q and P be an irreducible polynomial over F_q of degree n >0. Then the composition

$$F(x) = g(x)^n P(f(x)/g(x))$$

Is irreducible over F_q if and only if $f-\alpha g$ is irreducible over F_{q^n} for some root $\alpha \in F_{q^n}$ of P.

Note that theorem 1.2 used extensively in the past by several authors in order to produce iterative constructions of irreducible polynomials. See [3] for instance and the references there.

Recently, Kyuregyan-Kyureghyan provides another proof of Theorem 1.2 in [5] using the idea of composing factors of irreducible polynomials over extensions fields. Suppose f is an irreducible polynomial over F_q of degree n and $g(x)=\sum_{i=0}^{n/d} g_i x^i \in F_{q^d}[x]$ 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 $1 \le u \le d-1$. We denote $g = g^{(0)}$, and thus $f=\prod_{u=0}^{d-1} g^{(u)}$. Conversely, given an irreducible polynomial g of degree n/d over 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 F_q. It is an irreducible polynomial only when F_{q^d} is the smallest extension field of F_q containing the coefficients of g, i.e., when $F_q(g_0,...,g_k)=F_{q^d}$. In particular, they obtain the following.

Theorem 1.3 (Theorem 1, [5]). Let k>1, gcd(k,d)=1, and f be an irreducible polynomial of degree k over F_q. Further let $\alpha \neq 0$ and be an elements of F_{q^d} . Set g(x) := f(αx+β). Then the polynomial

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

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

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) [1], 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, [1]). 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.

Now 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.

Now we show that some cases of the construction in Theorem 1.3 are in fact composed products and therefore consequences of the result given below.

Proposition Let gcd(k,d)=1, and f be an irreducible polynomial of degree k over F_q. Further let $\alpha \neq 0$ and β be elements of F_{q^d}. Set g(x):=f(αx+β) and let

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

be a polynomial over F_q of degree n=dk. Then

(i) If $\alpha \in F_q$ and $F_q(\beta) = F_{q^d}$ then F is a composed sum of two irreducible polynomials with degree k and d respectively, hence irreducible.

(ii) If $\beta \in F_q$ and $F_q(\alpha) = F_{q^d}$, then F is a composed multiplication of two irreducible polynomials with degree k and d respectively, hence irreducible.

(iii) If $F_q(\alpha) = F_{q^d}$ and β=cα, where $c \in F_q$, then F is the result of a linear substitution operation x→(x + c) applied to an irreducible composed multiplication, and hence irreducible.

(iv) If α= -β+1 and $F_q(\alpha,\beta)=F_{q^d}$, then F is the circle product of two irreducible polynomials with degree k and s respectively, where s/d, hence irreducible.

(v) If α= β+1 and $F_q(\alpha,\beta)=F_{q^d}$, then F is the composed product of two irreducible polynomials with degree k and s respectively, where s/d, hence irreducible.

Proof. (i) Because If $\alpha \in F_q$, we write $\overline{f}$ (x)= f(αx). So $\overline{f}$ (x) is also an irreducible polynomial of degree k over F_q. Therefore, by Proposition ,

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

is the composed sum of $\overline{f}$ and the minimal polynomial of α^{-1} β (an irreducible polynomial of degree d).

(ii) In this case, let $\overline{f}$ (x)= f(x+β). So $\overline{f}$ (x) is also an irreducible polynomial of degree k over F_q.

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

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

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

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

is irreducible as well over 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 F_q

(iv)Let h be the minimal polynomial of – α^{-1}+1.Because $F_q(\alpha,\beta) = F_{q^d}$, there are s/d distinct conjugates of –α^{-1}+1 and thus the degree of g 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/d as a consequence of $F_q(\alpha,\beta) = F_{q^d}$,the polynomial F is the composed product of two irreducible polynomials of coprime degrees, and hence irreducible.

(vi) Here we define the composed product $\lozenge$ for G=Γ_q-{-1} by a $\lozenge$ 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 α^{-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/d as a consequence of $F_q(\alpha,\beta) = F_{q^d}$, the polynomial F is the composed product of two irreducible polynomials of coprime degrees, and hence irreducible.

REFERENCES

[1] J. V. Brawley and L. Carlitz (1987).Irreducible and the composed product for polynomials over a Finite Field, Discrete Math., 65, 115-139.

[2] S. D. Cohen (1969).On Irreducible Polynomials of certain types in Finite Field, Proc. Cambridge Philos. Soc. 66, 335-344.

[3] S. D. (2005).Explicit Theorems on Generating Polynomials over Finite Fields, Finite Fields Appl. 11, 337-357.

[4] Z. Gao and F. Fu (2009). The Minimal Polynomial over F_q of linear recurring Sequence over F_{q^m} . Finite Fields Appl. 15, no. 6, 774-784.

[5]M. K. Kyuregyan and G. H. Kyureghyan (2011). Irreducible Composition of Polynomials over Finite Fields, Designs, Codes and Cryptography, 61, no. 3, 301-314.

[6]R. Lidl and H. Niederreiter (1997).Finite Fields, in Encyclopedia of Mathematics and its Applications, 2nd ed., vol 20, Cambridge University Press, Cambridge.

[7]E. S. Selmer (1966).Linear Recurrence Relation over Finite Fields, Univ. of Bergen.

[8]R. Varshamov (1984).A General Method of Synthesizing Irreducible Polynomials over Galois Fields, Soviet Math. Dokl., 29, 334-336.

[9]N. Zierler and W. H. Mills (1973).Products of Linear Recurring Sequences, J. Algebra 27, 147-157.