ITERATES OF POLYNOMIALS AND SIMULTANEOUS PRIME SPECIALIZATION

SUSHMA PALIMAR

Abstract. R.W.K. Odoni showed that the Galois group of the n-th iterate of the generic monic polynomial of degree \( d \geq 2 \) in fields of characteristic zero is the \( n \)-folded iterated wreath product of the symmetric group \( S_d \). This result was extended to the fields of positive characteristic by Juul. Let \( \mathbb{F}_q \) be a finite field with \( q \) elements and \( q \) be a power of a prime \( p > 2 \), \( k = \mathbb{F}_q \), be an algebraic closure of \( \mathbb{F}_q \). We prove that, given \( F(t,x) \in k[t][x] \), an irreducible monic polynomial in \( x \) of degree \( n > 0 \), which is separable over \( k(t) \) and a generic monic polynomial \( \Phi(a_0, \ldots, a_{d-1}, t) \) in \( t \) of degree \( d \geq 2 \), with algebraically independent coefficients \( a = (a_0, \ldots, a_{d-1}) \), the Galois group of the \( m \)-th iterate of the composite polynomial \( F(t, \Phi(a, t)) \) over \( k(a_0, \ldots, a_{d-1}) \) is the \( m \) folded iterated wreath product of the symmetric group \( S_{nd} \). This result when applied to an explicit form of Chebotarev density theorem over function fields resembles, the polynomial analogue of the Bateman-Horn conjecture and the Chowla’s conjecture on the autocorrelation of the Möbius function, in the limit of a large finite field. These are presented here.

1. Introduction

Birch and Swinnerton Dyer showed that the Galois group of a polynomial \( x^n + x + t \), \( n > 1 \), over the field \( \overline{\mathbb{F}}_p(t) \), (the algebraic closure of prime field \( \mathbb{F}_p \) of \( p \) elements of rational functions in the variable \( t ) \), is the symmetric group \( S_n \) of order \( n \), unless, \( p \mid 2n(n-1) \) while answering a question posed by Chowla. In 1966 Sarvadaman Chowla [12] conjectured that, number of polynomials of the form

\[
x^n + x + d
\]

which are irreducible modulo \( p \) is asymptotic to \( \frac{2}{n} \), as \( p \to \infty \) for fixed \( n \). This was proved independently by S.D. Cohen [13] in 1970 and R. Ree [36] in 1971, that, for any prime power \( q \), the number of \( d \) such that \( x^n + x + d \) is irreducible is indeed \( \frac{2}{n} + O(q^{\frac{1}{2}}) \) with the implied constant depending only on \( n \). One of the ingredient in the proof is the fact that the Galois group of the polynomial \( x^n + x + t \in \mathbb{F}_q[t,x] \) over the function field \( \mathbb{F}_q(t) \) is the symmetric group \( S_n \) of order \( n \). The connection of these problems to Galois theory is established via the Chebotarev density theorem.

2010 Mathematics Subject Classification. 11T06,11T55,12F10, 37P15.

Key words and phrases. Galois groups; wreath product; Odoni’s conjecture; prime specializations; Bateman-Horn Conjecture; autocorrelation.
1.1. Galois groups of iterates. Let $K$ be a Hilbertian field and $\phi(x) \in K[x]$ be a polynomial of degree $d > 1$. For a fixed $n \in \mathbb{N}$, let

$$\phi^n = \underbrace{\phi \circ \cdots \circ \phi}_{n \text{ times}}$$

denote the $n$-th iterate of $\phi$, the $n$-fold composition of $\phi$ with itself. For $t \in K$, the set of preimages of $t$ is the set of roots of $\phi^n(x) - t = 0$, i.e.,

$$\phi^{-n}(t) = \{ \alpha \in \overline{K} | \phi^n(\alpha) = t \}$$

Let $K_n/K$ denote the splitting field of $\phi^n(x) - t$ over $K$. $K_n$ is obtained from $K_{n-1}$ by adjoining the roots of $\phi(x) - \beta_i$, where $\beta_1, \ldots, \beta_{d^{n-1}}$ are the $d^{n-1}$ distinct roots of $\phi^{n-1}(x) - t = 0$. Denote, $K = K_0$, then, there is a containment $K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n \subset \cdots$ and so on. The $d^n$ roots of the $n$th iterate of $\phi$ can be identified with $d^n$ vertices at level $n$ of the $d$-ary rooted tree $T$, in such a way that Galois group of $\phi^n$ embeds in $\text{Aut}(T_n)$, where $\text{Aut}(T_n)$ is the group of automorphism of the $d$-ary rooted tree of height $n$. A standard result in group theory is that, $\text{Aut}(T_n) \cong [S_d]^n$, the $n$-fold iterated wreath product of the symmetric group $S_d$. We call the relative Galois extension $K_n/K_{n-1}$ is maximal when $\text{Gal}(K_n/K_{n-1}) = S_d^{d^{n-1}}$ and the extension $K_n/K$ is maximal when $\text{Gal}(K_n/K) = \text{Aut}(T_n)$. Then it follows by induction and comparison of degrees that, $\text{Gal}(K_n/K) \cong [S_d]^n$ for all $n \in \mathbb{N}$. (Jones, [20]).

**Conjecture 1.1.** [Conjecture 7.5, Odoni, [30]] For any Hilbertian field $F$ of characteristic 0, there is a monic polynomial $f(x) \in F[x]$ of degree $d \geq 2$ such that,

$$\text{Gal}(f^n(x), F) \cong [S_d]^n, n \geq 1 \quad (1.2)$$

Odoni himself proved that $\phi(x) = x^2 - x + 1$ over a field $K$ of characteristic 0 has surjective arboreal representation ([30]). Conjecture 1.1 was proved over an algebraically closed field $F$ of characteristic $p > 0$ by Juul, [22]. While,Looper, [27] established this result over the field $F = \mathbb{Q}$, and all prime degrees $d$. Looper’s result was independently extended in [23, 8, 10]. Kadets [23], showed that Odoni’s conjecture holds over any number field. Specer [40] proved Odoni’s conjecture for all number fields, more generally, for all algebraic extensions $K/\mathbb{Q}$ that are unramified outside of a finite set of primes.

1.2. Preliminaries.

**Definition 1.** Hilbert Irreducibility Theorem. [Fried & Jarden [29], Chapter 12]. Suppose that $f(\mathbf{X}, \mathbf{t})$, where $\mathbf{X} = (X_1, \ldots, X_r), \mathbf{t} = (t_1, \ldots, t_s)$ and $r, s \geq 1$ is a polynomial in $r + s$ indeterminates with coefficients in a Hilbertian field $K$. If $f$ is irreducible in $K(\mathbf{X}, \mathbf{t})$, then Hilbert Irreducibility theorem asserts that, there exists infinitely many specializations $\mathbf{t} \mapsto \alpha$, given by $H := \alpha = (\alpha_1, \ldots, \alpha_s) \in K^s$ for which $f(\alpha_1, \ldots, \alpha_r, x)$ is irreducible in $K[\mathbf{X}]$. Further if $r = s = 1$, then for almost all specializations $f(\mathbf{X}, \alpha)$...
Let \( d \) be a regular extension. Denote, \( \text{Gal}(k/k) \) the Galois group acting on the zeros of \( F \) \( k \) denotes the splitting field of \( F \) \( t \), \( \Phi(t) \) be algebraically independent variables and, \( \Phi(a) = k[a][t] \). Let \( \Phi(a) = k(a)[t] \) be a generic monic polynomial of degree \( d \geq 2 \). Then the polynomial \( F(t, \Phi(a, t)) \in k(a)[t] \). Then denote, \( r \) is fixed and \( p \nmid r(r - 1). \)

**Remark 1.** Let \( L \) be the splitting field of \( \Phi(a, t) \) over \( k(a) \). Then \( L/F_q \) is a regular extension.

**Theorem 2.1.** Let \( F(t, x) \in k[t][x] \) be a monic, irreducible polynomial in \( x \), separable over \( k(t) \) of degree \( n > 0 \). Then \( F(t, \Phi(a, t)) \) \( k(a)[t] \) is a polynomial in \( t \) with indeterminates \( a_0, \ldots, a_{d-1} \) as coefficients. Denote, \( r = \deg_t(F(t, \Phi(a, t))) \), such that, \( r \) is fixed and \( p \nmid r(r - 1). \). Then, the Galois group of the polynomial \( F(t, \Phi(a, t)) \) over \( k(a) \) (regarded as a group of permutation on the zeros of \( F(t, \Phi(a, t)) \)) is the symmetric group \( S_r \) on \( r \) letters.

\[
\text{Gal}(F(t, \Phi(a, t)), k(a)) = S_r. \tag{2.2}
\]

Suppose, \( M \) is the splitting field of \( F(t, \Phi(a, t)) \) over \( F_q(a) \). Then, \( S_r \cong \text{Gal}(F(t, \Phi(a, t)), k(a)) \). \( k(a) \) is contained in \( S_r \leq \text{Gal}(F(t, \Phi(a, t)), F_q(a)) = S_r. \)

\[
\text{Gal}(M/F_q(a)) = \text{Gal}(M/F_q(a)) = S_r \tag{2.3}
\]

Thus, replacing \( q \) by any large power of \( p \) and \( M \) by \( M/F_q \), we have that, \( \text{Gal}(M/F_q(a)) = \text{Gal}(M/F_q(a)) = S_r \)
Theorem 2.2. Under the hypothesis of Theorem 2.1, for a fixed $m \in \mathbb{N}$, the Galois group of the $m$-th iterate of polynomial $F(t, \Phi(a, t))$ over $k(a)$ (regarded as a group of permutation on the zeros of $F^m(t, \Phi(a, t))$) is the $m$-folded iterated wreath product of the symmetric group $S_r$. That is,

$$\text{Gal}(F^m(t, \Phi(a, t)), k(a)) = [S_r]^m$$

The proof of Theorem 2.2 proceeds by induction steps, by showing that for a fixed $m \in \mathbb{N}$, the splitting field $K_m$ of $F^m(t, \Phi(a, t))$ over $K_{m-1}$ is the compositum of $r^{m-1}$ linearly disjoint splitting fields over $K_{m-1}$. Then it follows that

$$\text{Gal}(K_m/K_{m-1}) = S_r^{m-1} \text{ for } m \geq 1.$$  

This is done in Proposition 3.4 and Corollary 3.4.

Remark 2. We may note that, Theorems 2.1 and Theorem 2.2 hold over any algebraically closed field $k$ of characteristic $p \geq 0$ and not just over $\mathbb{F}_q$.

In §4 and §5 we give two applications of Theorem 2.2 along with an appropriate versions of the Chebotarev Density Theorem. We first show that Theorem 2.2 resembles the Schinzel Hypothesis H for polynomials with coefficients in $\mathbb{F}_q(a)$. Schinzel’s Hypothesis H asserts that finitely many irreducible polynomials over integers simultaneously assume prime values infinitely often unless there is a local obstruction. The quantitative analogue of the Schinzel Hypothesis H is the Bateman-Horn conjecture. A detailed study on polynomial analogue of the Schinzel Hypothesis H over $\mathbb{F}_q(t)$ is done in §5. The quantitative result of the Theorem 2.2 bears resemblance to the function field analogue of Bateman-Horn conjecture for polynomials over $\mathbb{F}_q(t)$.

This is discussed in §4.3. Besides this, Theorem 2.2 further implies that, for a fixed $m \in \mathbb{N}$, the iterates $F^{\phi_i}(t, \Phi(a, t))$ for $1 \leq i \leq m$ are irreducible over $\mathbb{F}_q(a)$. Therefore, $F(t, \Phi(a, t))$ is a stable polynomial over $\mathbb{F}_q(a)$. The asymptotic for the number of stable polynomials over finite fields bears resemblance to the function field analogue of the Chowla’s conjecture on the autocorrelation of the M"obius function in $\mathbb{F}_q[t]$. This is discussed in §5. We find the asymptotics of these conjectures for fixed $m, r, \deg(F^{\phi_i}(t, \Phi(a, t)))$ for $1 \leq i \leq m$ and $q \to \infty$.

2.1. Gal($F(t, \Phi(a, t)), k(a)$) is a transitive subgroup of $S_r$.

Proposition 2.1. Suppose $F(t, x)$ in $k[t][x]$ is a monic irreducible polynomial in $x$ and separable over $k(t)$. Then the composite polynomial $F(t, \Phi(a, t))$ is a monic, irreducible polynomial in $t$ and separable over $k(a)$.

Proof. By definition, $k(t)$ is Hilbertian. Given that, $F(t, x) \in k[t][x]$ is irreducible in $x$, Hilbert irreducibility theorem guarantees (Definition 1), the existence of infinitely many monic polynomials $g(t) = t^d + t^{d-1}c_{d-1} + \cdots + c_0 \in \mathbb{F}_q[t]$ of bounded degree $d$, such that, the polynomials $F(t, g(t))$
is irreducible in $k[t]$. This implies, for any generic monic polynomial $\Phi(a, t)$ defined in (2.1), the composite polynomial $F(t, \Phi(a, t))$ is irreducible over $k(a)$.

By [Uchida [42] §1], any Hilbertian field is separably Hilbertian. As, $F(t, x) \in k[t][x]$ is separable over $k(t)$, the discriminant $\text{disc}_x(F(t, x))$ is a nonzero function of $t$. By [Rudnik 37, Theorem 1.1], if $F(t, x) \in \mathbb{F}_q[t][x]$ is separable, with square-free content of bounded degree and height, then in the limit $q \to \infty$ for almost all monic polynomials $g(t) \in \mathbb{F}_q(t)$ of bounded degree, the polynomial $F(t, g(t))$ is separable (square-free) in $\mathbb{F}_q[t]$ and do not have multiple roots in any extension of $\mathbb{F}_q(t)$. Accordingly, for the generic polynomial $\Phi(a, t)$ defined in (2.1), the composite polynomial $F(t, \Phi(a, t))$ is absolutely irreducible and separable over $k(a)$, so that the Galois group $\text{Gal}(F(t, \Phi(a, t)), k(a))$ is a transitive subgroup of $S_r$, symmetric group on $r$ letters.

$\square$

2.2. Critical points of $F(t, \Phi(a, t)) \in k(a)[t]$ are distinct. The separability of $F(t, \Phi(a, t))$ over $k(a)$ implies,

$$\text{Disc}_t(F(t, \Phi(a, t))) = \pm \text{Resultant}(F(t, \Phi(a, t)), \frac{d}{dt}F(t, \Phi(a, t))) \neq 0. \quad (2.7)$$

Hence, $F(t, \Phi(a, t))$ has no multiple (double) roots, in any extension of $k(a)$. That is, the system of equations

$$\begin{cases}
\frac{d}{dt}F(t, \Phi(a, t))|_{t=\rho} = 0 \\
\frac{d}{dt}F(t, \Phi(a, t))|_{t=\eta} = 0 \\
F(t, \Phi(a, t))|_{t=\rho} = F(t, \Phi(a, t))|_{t=\eta}
\end{cases} \quad (2.8)$$

do not have a solution for distinct roots $\rho, \eta$ of $F(t, \Phi(a, t)) = 0$ in the algebraic closure $\Omega$ of $k(a)$, which means, the critical points of $F(t, \Phi(a, t))$ are distinct, [Rudnik 37, Theorem 1.3].

Remark 3. We note that, $F(t, \Phi(a, t)) \in k(a)[t]$ is separable over $k(a)$, with $r-1$ distinct critical values $\alpha_1, \ldots, \alpha_{r-1}$, so $F(t, \Phi(a, t))$ is a Morse polynomial of degree $r$ in $t$ [Theorem 4.4.1 [35]].

2.3. Galois group of $F(t, \Phi(a, t))$ over $k(a)$ contains a transposition. We recall the following standard theorem on local fields.

**Theorem 2.3** (Theorem 11.7, Sutherland [41]). Let $K$ be a global field with a nontrivial absolute value $| \cdot |$, and let $\hat{K}$ be the completion of $K$ with respect to $| \cdot |$. Every finite separable extension $\hat{L}$ of $\hat{K}$ is the completion of a finite separable extension $L$ of $K$ with respect to an absolute value that restricts to $| \cdot |$. Moreover, one can choose $L$ so that $\hat{L}$ is the compositum of $L$ and $\hat{K}$ and further, $[\hat{L} : \hat{K}] = [L : K]$.

Every finite extension of local fields $\hat{L}/\hat{K}$ necessarily corresponds to an extension of global fields $L/K$. The following proposition is an adaptation of [Lemma 5, Smith 39].
**Proposition 2.2.** Let $L$ denote the splitting field of $F(t, \Phi(a,t))$ over $k(a)$. The Galois group $G$ of $F(t, \Phi(a,t))$ over $k(a)$ contains a transposition.

**Proof.** We know that, $L/k(a)$ is a Galois extension and $G$ is a transitive subgroup of $S_r$. From (2.8) we know that, $F(t, \Phi(a,t))$ do not have double roots in any extension of $k(a)$, and for any prime $P$ of $\mathbb{F}_q(a)$, every irreducible factor of $F(t, \Phi(a,t))$ mod $P$ has ramification index less than 3. Hence, the only primes ramifying in $L$ are the primes dividing $D$. Let $P \neq 0$ be any prime dividing the discriminant $D$ of $F(t, \Phi(a,t))$. Clearly, $P$ is a ramified prime in $L$ and the factorization of $F(t, \Phi(a,t))$ modulo $P$ is,

$$\tilde{F} \equiv \bar{f}_1^2 \bar{f}_2 \ldots \bar{f}_n \mod P$$

(2.9)

Each of $\bar{f}_i, i \geq 2$ is monic and relatively prime to $\bar{f}_1 \mod P$ and $\bar{f}_2, \ldots, \bar{f}_n$ are irreducible. By Hensel’s Lemma, $F(t, \Phi(a,t))$ is factored over the completion $\hat{K}$ of $k(a)$ with respect to non trivial absolute value (prime ideal) $P$ as

$$F = g_1 \cdots g_n$$

(2.10)

with each $g_i$ having coefficients in $\hat{K}$ and, $g_i \equiv \bar{f}_i \mod P, i \geq 2$ and $g_1 \equiv \bar{f}_1^2 \mod P$. Let $\mathfrak{p}$ be a prime of $L$ lying above $P$ and $\hat{L}$ be an extension of $\hat{K}$. Clearly, $\hat{L}$ is the completion of $L$ with respect to $\mathfrak{p}$ containing $\hat{K}$, and the extension of local fields $\hat{L}/\hat{K}$ is a Galois extension. For $i \geq 2$, the roots of $g_i = 0$ generate unramified extension over $\hat{K}$ and $g_1$ is irreducible of degree 2 over $\hat{K}$. Thus, the inertia group of $\hat{L}$ over $k(a)$ is generated by transposition of the roots of $g_1 = 0$ and leaves the roots of $g_i$ fixed for $i \geq 2$. Accordingly, $G$ contains a transposition.

**Remark 4.** Proposition 2.2 holds true under any specialization (separable, irreducible) $a_i \mapsto c \in k$. Then the Galois group of the specialized polynomial contains a transposition. Now, $G$ contains a transposition, by the fact that, Galois groups cannot increase under (separable) specialization of parameters.

2.4. **Galois group of $F(t, \Phi(a,t))$ over $k(a)$** is doubly transitive and primitive. A permutation group $G$ acting on a set $\Omega = \{1, 2, \ldots, n\}$ is transitive, if $\forall i, j \in \Omega$, there exists a $\sigma \in G$, such that, $\sigma(i) = j$. More generally, $G$ is $k$-transitive for a positive integer $k \leq n$ if, for any $k$-tuple of pairwise distinct points $i_1, \ldots, i_k$ in $\Omega$ and pairwise distinct points $j_1, \ldots, j_k$ in $\Omega$ there is an element $\sigma$ of $G$, such that, $\sigma(i_l) = j_l$ for $1 \leq l \leq k$. Clearly a $k$-transitive group is also $k-1$ transitive.

$F(t, \Phi(a,t))$ is a polynomial in $t$ of degree $r > 2$, irreducible and separable over $k(a)$. Let $\alpha_1, \ldots, \alpha_r$ be the $r$ distinct roots of $F(t, \Phi(a,t)) = 0$ and as before let $L$ be the splitting field of $F(t, \Phi(a,t))$ over $k(a)$, that is $L = k(a)(\alpha_1, \ldots, \alpha_r)$. $F(t, \Phi(a,t))$ splits into $r$ linear factors $(t - \alpha_1) \ldots (t - \alpha_r)$ in $L[t]$. Since the roots of $F(t, \Phi(a,t)) = 0$ are distinct, any two linear factors $(t - \alpha_i)$ and $(t - \alpha_j)$ for $i \neq j$ are pairwise coprime in $L[t]$ and any $\alpha_i$ for $1 \leq i \leq r$ is transcendental over $k(a)$. To prove double transitivity of the
Galois group of $F(t, \Phi(a, t))$ over $k(a)$, we follow the method of “throwing away roots” [Abhyankar [11] §4]. Thus, we remove a root of $F(t, \Phi(a, t)) = 0$, say $t = \alpha_1$ and get,

$$F_1(a, t) = \frac{F(t, \Phi(a, t))}{(t - \alpha_1)} \in k(a)(\alpha_1)[t]$$

(2.11)

Obviously, $F_1(a, t)$ is irreducible in $k(a)(\alpha_1)[t]$ and separable over $k(a)(\alpha_1)$. Consequently $F(t, \Phi(a, t))$ and $F_1(a, t)$ are irreducible in $k(a)[t]$ and $k(a)(\alpha_1)[t]$ respectively. This means, the stabilizer of the root $t = \alpha_1$ in the Galois group of $F_1(a, t)$, acts transitively on other roots, implying the Galois group of $F(t, \Phi(a, t))$ over $k(a)$ is doubly transitive.

**Proposition 2.3.** The Galois group $G$ of $F(t, \Phi(a, t))$ over $k(a)$ is primitive.

**Proof.** Since any doubly transitive group action is primitive, $G$ is primitive. □

A result due to Marggraof (Marggraf or Marggraaf) stated in [W. Burnside, §140, p.197] is that a primitive permutation group $G$, which contains a cycle fixing $k$ points is $k + 1$-fold transitive [§3, G.A. Jones [21]]. This is stated in Wielandt, [43], Theorem 13.8 as below.

**Theorem 2.4.** Suppose, $G$ is a primitive group of degree $n$, which contains a cycle fixing $k$ points, then $G$ is $(n - d + 1)$-fold transitive.

**Theorem 2.5.** [43], Theorem 10.1 Let $k = 1, 2, 3 \ldots$. Every $(k + 1)$-fold transitive group is $k$-fold primitive. Every $k$-fold primitive group is $k$-fold transitive and every group of which is a subgroup is $k$-fold primitive.

**Theorem 2.6.** [43], Theorem 13.3] If a primitive permutation group contains a transposition, it is a symmetric group.

2.5. **Proof of Theorem 2.1.** Claim: $\text{Gal}(F(t, \Phi(a, t)), k(a)) \cong S_r$.

**Proof.** We know that, $F(t, \Phi(a, t)) \in k(a)[t]$ is a polynomial in $t$ of degree $r$ and,

$$G = \text{Gal}(F(t, \Phi(a, t)), k(a)) = \text{Gal}(L/k(a)).$$

The Galois group $G$ is a transitive subgroup of $S_r$ and contains a transposition. In addition, $G$ is doubly transitive, hence primitive. Thus $G$ is a primitive permutation group containing a transposition. Therefore $G = S_r$. □

It follows that $\text{Gal}(F(t, \Phi(a, t)), \mathbb{F}_q(a)) \cong S_r$ as well. So, the splitting field $M$ of $F(t, \Phi(a, t))$ over $\mathbb{F}_q(a)$ is a geometric extension, [shown in (2.4)]. Let $f(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_0 \in \mathbb{F}_q[t]$ be the specialized polynomial of degree $d \geq 2$ under suitable irreducible, separable specializations $(a_0, \ldots, a_{d-1}) \mapsto (c_0, \ldots, c_{d-1}) \in \mathbb{F}_q^d$ for the generic polynomial $\Phi(a, t)$. Thus applying an effective version of the Chebotarev Density Theorem for geometric function field extensions we have the following result:

\[ \text{Iterates of polynomials} \]
Theorem 2.7. Assume the hypothesis of Theorem 2.1. Then, the number of monic irreducible polynomials \( f(t) \in \mathbb{F}_q[t] \) of degree \( d \geq 2 \) such that \( F(t, f(t)) \) is irreducible in \( \mathbb{F}_q[t] \), which is
\[
\# \{ f(t) \in \mathbb{F}_q[t] \mid \deg(f) = d \geq 2 : F(t, f(t)) \in \mathbb{F}_q[t] \text{ is irreducible} \}
\]
\[
= \frac{q^d}{r} + O_r(q^{d-\frac{1}{2}}), \quad q \to \infty
\]  
(2.12)

the implied constant depends only on \( r \).

The estimate (2.12) is standard, due to a more general explicit version of Chebotarev density theorem \([2], \text{Theorem A.4}\) by Andrade et. al. Pollack [Theorem 2, [34]] establishes (2.12) using the methods of Cohen [Theorem 3, [14]] and Ree [36]. Cohen and Ree derive this independently to settle Chowla’s conjecture [12]. Their result uses Chebotarev density theorem for function fields which in turn depends on Weil’s profound result on the Riemann hypothesis for curves.

2.6. Linearly disjoint Galois extensions.

Definition 3. Two algebraic sub-extensions \( K, L \) of \( \Omega/k \) are linearly disjoint if and only if \( K \otimes_k L \) is a field.

Definition 4. A field extension \( L/k \) is said to be regular if \( k \) is algebraically closed in \( L \) equivalently, \( L \otimes_k \overline{k} \) is an integral domain, \( \overline{k} \) is the algebraic closure of \( k \); i.e., \( L, \overline{k} \) are linearly disjoint over \( k \).

Theorem 2.8. [Cohn [16], Theorem 5.5, Theorem 5.5']

(1) Let \( K/k, L/k \) be two extensions of which one is normal and one is separable. Then \( K \otimes_k L \) is a field, if and only if \( K \cap L = k \).

(2) Further, \( K \otimes_k L \) is a field, if and only if \( K, L \) have no isomorphic subfield properly containing \( k \).

3. Galois groups of iterates of composition of polynomials

As before, \( k = \overline{\mathbb{F}}_q, \text{char } \mathbb{F}_q = p > 2 \) and \( F(t, \Phi(a, t)) \in k(a) \) is a polynomial in \( t \) of degree \( r > 2 \), whose coefficients are algebraically independent variables over \( \mathbb{F}_q \), and \( \gcd(p, r(r - 1)) = 1 \).

In the sequel, we set, \( K_0 = k(a), F^0(t, \Phi(a, t)) \) as \( F(t, \Phi(a, t)) \) and \( K_1 \), the splitting field of \( F(t, \Phi(a, t)) \) over \( k(a) \). For a fixed \( n \in \mathbb{N} \), the \( n \)th iterate of \( F(t, \Phi(a, t)) \) is
\[
F^n(t, \Phi(a, t)) := F^{n-1}(F(t, \Phi(a, t)))
\]
and \( K_n \) is the splitting field of \( F^n(t, \Phi(a, t)) \) over \( k(a) \) which is the constant field extension of \( k(a) \) contained in a fixed algebraic closure \( \Omega \) of \( k(a) \). Aim of this section is to show that for a fixed \( n \in \mathbb{N} \), the relative Galois extension \( K_n/K_{n-1} \) is maximal, i.e., \( \text{Gal}(K_n/K_{n-1}) \cong S_r^{n-1} \). We know that, critical points of \( F(t, \Phi(a, t)) \in k(a)[t] \) are distinct by (2.8). We assume without loss of generality that, for any two distinct critical points, \( \gamma, \delta \) of \( F(t, \Phi(a, t)) \)
Lemma 3.1. (Capelli’s Lemma) Let \( K \) be a field and \( f(x), g(x) \) in \( K[x] \) be polynomials. Let \( \beta \) be a root of \( f(x) \). Then every root of \( g(x) - \beta \) is a root of \( f(g(x)) \). If \( \alpha \) is a root of \( f(g(x)) \), then \( g(\alpha) \) is a root of \( f(x) \). Then, \( f(g(x)) \) is irreducible in \( K[x] \) if and only if \( f(x) \) is irreducible in \( K[x] \) and \( g(x) - \beta \) is irreducible in \( K(\beta)[x] \) for every root \( \beta \) of \( f(x) \).

Remark 5. We may note that, \( F(t, \Phi(a, t)) \) is a Morse polynomial, (Remark [3] and the Galois group of \( F(t, \Phi(a, t)) \) over \( k(a) \) is \( S_r \). Then for any indeterminate \( \alpha \), the Galois group of \( F(t, \Phi(a, t)) - \alpha \) over \( k(a)(\alpha) \) is \( S_r \).

This result is due to Hilbert, stated in [38, Theorem 4.4.5].

Suppose, \( \alpha_1, \ldots, \alpha_r \) are the \( r \) distinct roots of \( F(t, \Phi(a, t)) = 0 \). Then,

\[
F^{o2}(t, \Phi(a, t)) = F(F(t, \Phi(a, t))) = \prod_{i=1}^{r} F(t, \Phi(a, t)) - \alpha_i \in K_1[t] \quad (3.1)
\]

Each of \( r \) polynomials,

\[
F(t, \Phi(a, t)) - \alpha_1, \ldots, F(t, \Phi(a, t)) - \alpha_r \quad (3.2)
\]

are of degree \( r \) in \( t \), which are distinct, monic, irreducible, separable and pairwise relatively prime in \( K_1[t] \). Then by Hilbert’s result,

\[
\text{Gal}(F(t, \Phi(a, t)) - \alpha_i, k(a)(\alpha_i)) \cong S_r \quad \text{for } 1 \leq i \leq r \quad (3.3)
\]

Consequently, the following Proposition follows by induction steps.

Proposition 3.1. For a fixed \( n \in \mathbb{N} \), the \( n \)-th iterate \( F^{o n}(t, \Phi(a, t)) \) of \( F(t, \Phi(a, t)) \) decomposes to \( r^{n-1} \) polynomials of degree \( r \) in \( t \) which are non associate, monic, irreducible, separable and are pairwise relatively prime over \( K_{n-1} \), and their splitting fields are linearly disjoint over \( k(a) \).

Proof. For \( n = 1 \), \( F^{o1}(t, \Phi(a, t)) \) has \( r \) distinct roots. Then, \( F^{o2}(t, \Phi(a, t)) \) splits to \( r \) linear factors which are monic, irreducible, separable and pairwise relatively prime over \( K_1 \) and the result holds true [see, (3.1)]. Let us assume that, the result holds true for all \( m < n \). Let \( \alpha_1, \ldots, \alpha_{r^{n-1}} \) be the \( r^{n-1} \) distinct roots of \( F^{o n-1}(t, \Phi(a, t)) = 0 \) in some algebraic closure of \( k(a) \). Here, \( K_{n-1} \) is the splitting field of \( F^{o n-1}(t, \Phi(a, t)) \) over \( k(a) \). We may note that,

\[
F^{o n}(t, \Phi(a, t)) = F^{o n-1}(F(t, \Phi(a, t))) = \prod_{i=1}^{r^{n-1}} F(t, \Phi(a, t)) - \alpha_i \quad (3.4)
\]

We may note that, each of \( \alpha_i \) is transcendental over \( k(a) \), and the \( r^{n-1} \) polynomials on the right of (3.4), are of degree \( r \) in \( t \), which are monic, irreducible, separable and pairwise relatively prime over \( K_{n-1} \). Let \( M_i \) be the splitting field of \( F(t, \Phi(a, t)) - \alpha_i \) over \( k(a)(\alpha_i) \), for \( 1 \leq i \leq r^{n-1} \). Since the polynomials \( F(t, \Phi(a, t)) - \alpha_i \) are distinct and are relatively prime in \( K_{n-1}[t] \),
they have distinct ramifications in the Galois extensions $M_1/k(a)(\alpha_1), \ldots, M_{n-1}/k(a)(\alpha_{n-1})$, respectively. Hence, their splitting fields $M_1, \ldots, M_{n-1}$ are linearly disjoint over $k(a)$ and the claim follows.

3.1. Linearly disjoint splitting fields over $K_{n-1}$. From Proposition 3.1 and by (3.3),

$$\text{Gal}(F(t, \Phi(a, t)) - \alpha_i, k(a)(\alpha_i)) = \text{Gal}(M_i/k(a)(\alpha_i)) \cong S_r, \text{ for } 1 \leq i \leq r^{n-1}$$

(3.5)

Denote,

$$M = M_1 \cdots M_{n-1}$$

(3.6)

Similarly denote,

$$M_i' := M_i K_{n-1} \text{ for } 1 \leq i \leq r^{n-1}$$

(3.7)

For distinct roots, $\alpha_1, \ldots, \alpha_{n-1}$ of $F^{\circ n-1}(t, \Phi(a, t))$ there is a distinct ramification of $F(t, \Phi(a, t)) - \alpha_i$ in $M_i$, for $1 \leq i \leq r^{n-1}$, implies, $M_1' \cdots M_{n-1}'$ are linearly disjoint over $K_{n-1}$ for $1 \leq i \leq r^{n-1}$. Consequently, from

$$F^{\circ n}(t, \Phi(a, t)) = \prod_{i=1}^{r^{n-1}} F(t, \Phi(a, t)) - \alpha_i \in K_{n-1}[t]$$

(3.8)

it follows that $K_n$, the splitting field of $F^{\circ n}(t, \Phi(a, t))$ is the compositum of $r^{n-1}$ linearly disjoint splitting fields $M_1'/K_{n-1} \cdots M_{n-1}'/K_{n-1}$. Thus,

$$K_n = M_1' \cdots M_{n-1}'$$

(3.9)

that is,

$$K_n = M \cdot K_{n-1}$$

Proposition 3.2. For a fixed $n \in \mathbb{N}$, any prime $P$ of $k(a)$ ramifying in $K_n$, does not ramify in $K_{n-1}$.

Proof. From the discussion in (3.3) the polynomials $F(t, \Phi(a, t)) - \alpha_1, \ldots, F(t, \Phi(a, t)) - \alpha_{n-1}$ are distinct, separable and relatively prime over $K_{n-1}$ with respective splitting fields $M_1' \cdots M_{n-1}'$, which are linearly disjoint over $K_{n-1}$. The “only” primes ramifying in $K_n$ are the prime divisors of the $\text{disc}(F(t, \Phi(a, t)) - \alpha_i)$, discriminant of $F(t, \Phi(a, t)) - \alpha_i$ for $1 \leq i \leq r^{n-1}$. Obviously, distinct ramification implies, primes ramifying in $M_i'$ does not ramify in $M_j'$ for $i \neq j$. Also, from the above discussion, $K_{n-1}$ is the compositum of $r^{n-2}$ linearly disjoint splitting fields $L_1', \ldots, L_{r^{n-2}}'$ over $K_{n-2}$. So, if a prime $P$, ramifying in $K_n$, also ramifies in $K_{n-1}$, then it ramifies in one of the $L_i'$ for $1 \leq i \leq r^{n-2}$, which is a contradiction for $M_1', \ldots, M_{n-1}'$ being linearly disjoint over $K_{n-1}$. Hence the claim follows.

The following result is standard, which is reminiscent of the second isomorphism theorem. [Proposition 3.1, VIII §3, Lang, Algebra [25]], [Proposition 2.6 in K. Conrad [17]], [Theorem 6.2.2, Robert B. Ash [4] (last two references are expository article on Galois theory)]
Proposition 3.3. The Galois group \( \text{Gal}(M_i'/K_{n-1}) \cong S_r \), for \( 1 \leq i \leq r^{n-1} \) where, \( M_i' = M_iK_{n-1} \).

Proof. We may note from \( \S 3.1 \) that,  
\[ \text{Gal}(F(t, \Phi(a), t) - \alpha_i, k(\alpha_i)) = \text{Gal}(M_i/k(\alpha_i)) \cong S_r, \quad 1 \leq i \leq r^{n-1} \]

In the following diamond diagram,

\[
\begin{array}{ccc}
M_iK_{n-1} & \text{Gal}(M_i/K_{n-1}) & k(\alpha_i) \\
M_i & \text{Gal}(M_i/\text{K}_{n-1}) & M_i \cap K_{n-1} \\
& & \text{Gal}(M_i/k(\alpha_i)) \cong S_r \\
\end{array}
\]

Note that, \( M_i/k(\alpha_i) \) is a finite Galois extension and, \( K_{n-1}/k(\alpha_i) \) is a normal extension, hence, \( \text{Gal}(M_iK_{n-1}/K_{n-1}) \) is a normal subgroup of \( \text{Gal}(M_i/k(\alpha_i)) = S_r \). We may note that,

\[ \text{Gal}(M_iK_{n-1}/K_{n-1}) \cong \text{Gal}(M_i/M_i \cap K_{n-1}) \] \hspace{1cm} (3.10)

but,

\[ \text{Gal}(M_i/M_i \cap K_{n-1}) = \text{Gal}(M_i/k(\alpha_i)) = S_r. \] \hspace{1cm} (3.11)

Combining (3.10) and (3.11),

\[ \text{Gal}(M_iK_{n-1}/K_{n-1}) = \text{Gal}(M_i'/K_{n-1}) = S_r \] \hspace{1cm} (3.12)

\[ \square \]

3.2. Distinct ramification and Square-free discriminants. Let us recall, for a fixed \( n \in \mathbb{N} \),

\[ F^{\circ n}(t, \Phi(a), t) = \prod_{i=1}^{r^{n-1}} F(t, \Phi(a), t) - \alpha_i, \quad F(t, \Phi(a), t) - \alpha_i \in K_{n-1}[t]. \] \hspace{1cm} (3.13)

Denote  
\[ d_i = \text{disc}_t(F(t, \Phi(a), t) - \alpha_i) \]

the discriminant of \( F(t, \Phi(a), t) - \alpha_i \). For, \( 1 \leq i \leq r^{n-1} \), \( \text{Gal}(F(t, \Phi(a), t) - \alpha_i, k(\alpha_i)) = S_r \), the symmetric group of order \( r \). Hence, discriminants, \( d_1, \ldots, d_{r^{n-1}} \) are square free. Distinct ramification of \( F(t, \Phi(a), t) - \alpha_i \) in \( M_i' \) implies, the discriminants \( d_1, \ldots, d_{r^{n-1}} \) are relatively prime, so, the product of \( d_i \cdot d_j \) is squarefree for \( i \neq j \), so \( d_1, \ldots, d_{r^{n-1}} \) are square independent. We know that, \( M_i', \ldots, M_{r^{n-1}}' \) are linearly disjoint over \( K_{n-1} \). Denote by \( E_i' \), the unique quadratic extension of \( K_{n-1} \) inside \( M_i' \) given by \( E_i' = K_{n-1}(\sqrt{d_i}) \).
for \(1 \leq i \leq r^{n-1}\). This is the fixed field of \(A_r\) in \(M'_i\), where, \(A_r\) is the alternating group on \(r\) letters, which is a normal subgroup of \(S_r\). Since, \(d_1, \ldots, d_{r^{n-1}}\) are squarefree as well as relatively prime in \(k(a)\), the unique quadratic extensions, \(E'_1, \ldots, E'_{r^{n-1}}\) are linearly disjoint over \(K_{n-1}\). Now let us start proving Theorem 2.2.

**Proposition 3.4.** For a fixed \(n \in \mathbb{N}\), the relative Galois extension \(K_n/K_{n-1}\) is maximal, that is
\[
\text{Gal}(K_n/K_{n-1}) \cong S_r^{n-1}
\]

*Proof.* We may note that, the result holds true for \(n = 1\).

\[
\text{Gal}(F^{01}(t, \Phi(a,t)), k(a)) = \text{Gal}(K_1/K_0) \cong S_r.
\]

For \(n > 1\), proof follows from [Lang, 25, VI, §1.14 1.15]. Assume the result holds true for all \(m < n\).

By equation (3.9) and Proposition 3.2, \(K_n\) is the compositum of \(M'_1 \cdot \cdots \cdot M'_{r^{n-1}}\), and \(M'_1, \ldots, M'_{r^{n-1}}\) are linearly disjoint over \(K_{n-1}\) with \(\text{Gal}(M'_i/K_{n-1}) \cong S_r\) for \(1 \leq i \leq r^{n-1}\). This is best visualized in the diamond diagram below.

\[
\begin{array}{c}
K_n \\
\downarrow \\
M'_1 \\
\downarrow \\
K_{n-1} \\
\downarrow \\
M'_{r^{n-1}}
\end{array}
\]

Then,
\[
\text{Gal}(K_n/K_{n-1}) \cong \text{Gal}(M'_1/K_{n-1}) \times \cdots \times (M'_{r^{n-1}}/K_{n-1})
\]
\[
\sigma \mapsto (\sigma|_{M'_1}, \ldots, \sigma|_{M'_{r^{n-1}}}) \text{ is an isomorphism.}
\]

This gives,
\[
\text{Gal}(K_n/K_{n-1}) \cong S_r^{n-1}; \text{ } K_n \text{ has degree } (r!)^{n-1} \text{ over } K_{n-1}. \quad (3.14)
\]

Thus, \(\text{Gal}(K_n/K_{n-1})\) is maximal as claimed for all \(n \geq 1\). \qed

**Corollary 3.1.** For a fixed \(n \in \mathbb{N}\) the Galois extension \(K_n/k(a)\) is maximal.

*Proof.* Maximalirty of \(K_n/K_{n-1}\) implies, any prime of \(k(a)\), which ramifies in \(K_n\), does not ramify in \(K_{n-1}\) and does not ramify in any subextension of \(K_n\). From the expression,
\[
[K_n : k(a)] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : k(a)]
\]

it follows that,
\[
[K_n : k(a)] = (r!)^{n-1} \cdot (r!)^{n-2} \cdots (r!) \cdot r! = |S_r|^n
\]

That is,
\[
\text{Gal}(K_n/k(a)) \cong [S_r]^n. \quad (3.15)
\]

Hence, the Galois extension \(K_n/k(a)\) is maximal for \(n \geq 1\). \qed
Proposition 3.4 and Corollary 3.4 together completes Theorem 2.2.

4. Applications

In this section we see that the quantitative version of Theorem 2.2 resembles the analogue of the Bateman-Horn conjecture and the Chowla conjecture on the autocorrelation of Möbius function in $\mathbb{F}_q[t]$.

**Conjecture 4.1.** ([7]) (Polynomial analogue of Schinzel Hypothesis H). Let $f_1(t, x), \ldots, f_r(t, x)$ be non constant irreducible polynomials in $\mathbb{F}_q[t][x]$ which are separable over $\mathbb{F}_q(t)$ of $\deg_x(f_i(t, x)) > 0$. Suppose that, there is no prime $P \in \mathbb{F}_q[t]$ for which every $g(t) \in \mathbb{F}_q[t]$, satisfies

$$f_1(g(t)) \ldots f_r(g(t)) \equiv 0 \mod P$$

Then the specializations $f_1(g(t)), \ldots, f_r(g(t))$ are simultaneously irreducible for infinitely many monic polynomials $g(t) \in \mathbb{F}_q[t]$.

The quantitative version of Schinzel Hypothesis is the Bateman-Horn Conjecture.

**Theorem 4.1.** ([7], [34]) (Polynomial analogue of Bateman-Horn Conjecture.) Let $n$, $B$ be positive integers, $p$ a prime such that $p \nmid 2n$, $q$ a power of $p$. Suppose, $f_1(x), \ldots, f_r(x) \in \mathbb{F}_q[x]$ be non-associate irreducible polynomials such that $\sum \deg(f_i) \leq B$. Then the number of degree $n$ monic $g(t) = t^n + \cdots \in \mathbb{F}_q[t]$ for which all of the $f_i(g(t))$ are irreducible in $\mathbb{F}_q[t]$ is

$$\frac{q^n}{n^r} + O_n, B \left(q^{n-B} \right). \tag{4.1}$$

The function field analogue of the Bateman-Horn conjecture is studied in detail and resolved over (large) finite fields in [34] by Pollack by supposing degree of $f_1, \ldots, f_r$ bounded by $B$ and letting $q^n \to \infty$ (i.e., either $q \to \infty$ or $n \to \infty$), where $n = \deg(g(t))$. Since the asserted constant in Pollack’s theorem is of order of magnitude $(n!)^B$, the asymptotic (4.1) is ineffective when $n \to \infty$, but works when $q \to \infty$ and $n$ is fixed. Bary-Soroker resolved this conjecture for $q \to \infty$, keeping $\deg(g)$ fixed, (Theorem 1.4, [7]), which overcomes the drawback of Pollack’s assumption $n \to \infty$. Both the authors treated the case $f_i$ independent of $t$, i.e., $f_i \in \mathbb{F}_q[x]$. As a further improvement to [2] and [34], Entin [6] resolved Bateman-Horn conjecture for both monic and non monic polynomials $f_i(t, x) \in \mathbb{F}_q[t][x]$ which are irreducible in $x$, separable over $\mathbb{F}_q(t)$, for fixed quantities, $\deg(f_i(t, g(t)))$, $r$ and $q \to \infty$.

4.1. Frobenius classes and cycle structure. Let $p$ be a prime number which is fixed, and $\mathbb{F}_p$, an algebraic closure of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The fundamental tool in the theory of finite fields is the Frobenius map $\text{Frob}: \mathbb{F}_p \to \mathbb{F}_p$, which is defined by $\text{Frob}(\alpha) = \alpha^p$, which is a field automorphism of $\mathbb{F}_p$. This map permutes the roots of any polynomial $g$ that has coefficients in $\mathbb{F}_p$. Galois theory for finite fields alludes to the statement that, the cycle pattern of $\text{Frob}$ viewed as a permutation of the zeroes of $g$, is the same.
as the decomposition type of $g$ over $\mathbb{F}_p$ provided $g$ is separable polynomial (squarefree). A lucid explanation on Chebotarev and his density theorem is done in [26], by Lenstra and Stevenhagen.

Let $\mathcal{M}_n \subset \mathbb{F}_q[t]$ be the collection of all monic polynomials of degree $n$ over $\mathbb{F}_q$ and $f \in \mathcal{M}_n$ be a separable polynomial of degree $n > 0$. We say that its cycle structure is $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$, if in the decomposition $f = \prod_i P_i$ into prime factorization, we have $\#\{i : \deg(P_i) = j\} = \lambda_j$. Thus we get a partition of $n$. Here, $\lambda_1(f)$ is the number of roots of $f \in \mathbb{F}_q[t]$ and $f$ is irreducible if and only if $\lambda_n(f) = 1$.

The cycle structure of a permutation $\sigma$ of $n$ letters is the partition $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_n)$ of $n$, if in the decomposition of $\sigma$ as a product of disjoint cycles, there are $\lambda_j$ cycles of length $j$ and $\sum j\lambda_j = n$. Here $\lambda_1$ is the number of fixed points of $\sigma$ and $\lambda_n = 1$ if and only if $\sigma$ is an $n$-cycle.

For each partition $\lambda \vdash n$, the probability that a random permutation has cycle structure $\sigma$ is given by Cauchy’s formula

$$p(\lambda) = \frac{\# \{ \sigma \in S_n : \lambda(\sigma) = \lambda \}}{\# S_n} = \prod_{j=1}^{\infty} \frac{1}{j^{\lambda_j} \cdot \lambda_j!} \quad (4.2)$$

As $q \to \infty$ the distribution over $\mathcal{M}_n$ of factorization types tends to the distribution of cycle types in $S_n$ [2].

**Theorem 4.2. (Chebotarev Density Theorem)** Let $F$ be a global field, let $K$ be a finite Galois extension of $F$, and let $G = \text{Gal}(K/F)$. For any conjugacy class $C$ of $G$, the Dirichlet density of the set of primes $\mathfrak{p}$ of $F$ for which $\text{Frob}(K/F) = C$ exists and is equal to $\#C/\#G$. Furthermore, if $F$ is a number field or $F$ is a function field whose constant field is algebraically closed in $K$, then the natural density of this set also exists and is equal to $\#C/\#G$.

**4.2. Irreducibility of $F^{\text{gen}}(t, f(t))$ over $\mathbb{F}_q$.** Suppose for some fixed $m \in \mathbb{N}$,

$$\text{Gal}(F^{\text{gen}}(t, \Phi(a, t)), k(a)) = \text{Gal}(K_m/k(a)) \cong [S_r]^m.$$  

Let $L$ be the splitting field of $F^{\text{gen}}(t, \Phi(a, t))$ over $\mathbb{F}_q(a)$. Then it follows that

$$\text{Gal}(F^{\text{gen}}(t, \Phi(a, t)), \mathbb{F}_q(a)) = \text{Gal}(L/\mathbb{F}_q(a)) \cong [S_r]^m \quad (4.3)$$

as well. Thus, the splitting field $L$ of $F^{\text{gen}}(t, \Phi(a, t))$ over $\mathbb{F}_q(a)$ is a geometric extension. Let $\mathbb{F}_{q^m}$ be the algebraic closure of $\mathbb{F}_q$ in $L$. Let $C$ be a conjugacy class of $\text{Gal}(L/\mathbb{F}_q(a))$, every element of which restricts down to the $q$-th power map on $\mathbb{F}_{q^m}$. For $c = (c_0, \ldots, c_{d-1}) \in \mathbb{F}_q^d$, let

$$P = (a_0 - c_0, \ldots, a_{d-1} - c_{d-1})$$

be any prime of $\mathbb{F}_q(a)$, which does not ramify in $L$. Let $\lambda$ be any cycle pattern in $[S_r]^m$. Let $C$ be the corresponding conjugacy class in $[S_r]^m$. As before, for some specialization $a = (a_0, \ldots, a_{d-1}) \mapsto c = (c_0, \ldots, c_{d-1}) \in \mathbb{F}_q^d$, let $f(t) \in \mathbb{F}_q[t]$, be a specialized polynomial in $\mathbb{F}_q[t]$ of degree $d \geq 2$ of the
generic polynomial $\Phi(a, t)$. The polynomial $F^{com}(t, f(t)) \in \mathbb{F}_q[t]$ has a cycle pattern $\lambda_{F^{com}}$ if and only if, $\text{Frob}(L/\mathbb{F}_q)$ has cycle pattern $\lambda$. Thus, by an explicit version of the Chebotarev Density Theorem for geometric function field extensions, (\cite{2}, Theorem 3.1) the number of $f(t) \in \mathbb{F}_q[t]$ of degree $d \geq 2$ such that $F^{com}(t, f(t))$ is squarefree with cycle pattern $\lambda$ is

$$\frac{|C|}{|[S_r]^m|} q^d + O_{r, \deg F^{com}}(q^{d-1/2})$$

Here, the implied constant depends only on $r$, $\deg F^{com}$ and $p(\lambda)$ is the probability of random permutation in $[S_r]^m$ having cycle structure $\lambda$. By [Lemma 13, \cite{32}], irreducibility of $F^{com}(t, f(t))$ over $\mathbb{F}_q$ is equivalent to the group $\text{Gal}(L/\mathbb{F}_q(a))$ containing a conjugacy class $C$ of size $|S_r|^m$. Then, the number of $f(t) \in \mathbb{F}_q[t]$ of degree $d \geq 2$ such that $F^{com}(t, f(t))$ is irreducible in $\mathbb{F}_q[t]$ with cycle structure $\lambda$ is

$$\frac{|C|}{|[S_r]^m|} q^d + O_{r, \deg F^{com}}(q^{d-1/2})$$

4.3. **Simultaneous irreducibility of** $F^{oi}(t, f(t)), \ldots, F^{com}(t, f(t))$ **over** $\mathbb{F}_q$.

**Remark 6.** *For the rest of the paper the asymptotic big $O$ notation implies a constant depending only on $r,m$ and $\deg F^{oi}$ for $1 \leq i \leq m$.*

Suppose for some fixed $m \in \mathbb{N}$ let, $\text{Gal}(F^{com}(t, \Phi(a, t)), k(a)) = [S_r]^m$. Then

$$\text{Gal}(F^{oi}(t, \Phi(a, t)), k(a)) \cong [S_r]^i \text{ for } 1 \leq i \leq m$$

As before, for any element $c = (c_0, \ldots, c_{d-1}) \in \mathbb{F}_q^d$, let

$$P = (a_0 - c_0, \ldots, a_{d-1} - c_{d-1})$$

be any prime of $\mathbb{F}_q(a)$. Then, it follows from Proposition \cite{32} that, if $P$ is unramified in $K_m$, then, $P$ stays prime in each of $K_j, j = 1, \ldots, m - 1$. Further if a prime $P$ of $\mathbb{F}_q(a)$ ramifies in $K_m$, then it does not ramify in $K_{m-1}$ or in any other subextension of $K_m$. As, each of $F(t, \Phi(a, t)), \ldots, F^{com}(t, \Phi(a, t))$ have distinct ramification in $K_m$, it follows that, product of discriminants,

$$\text{disc}_i(F^{oi}(t, \Phi(a, t))) \cdot \text{disc}_j(F^{oi}(t, \Phi(a, t))) \text{ for } i \neq j, \ 1 \leq i, j \leq m$$

is square-free, so they are square independent in $k(a)$. The irreducibility of $F^{com}(t, \Phi(a, t))$ over $k(a)$ implies $F(t, \Phi(a, t)), \ldots, F^{com-1}(t, \Phi(a, t))$ are simultaneously irreducible over $k(a)$. Let $L_i$ be the splitting field of $F^{oi}(t, \Phi(a, t))$ over $\mathbb{F}_q(a)$ for $1 \leq i \leq m$. Then $L_i$ is a geometric extension as
well. Hence, irreducibility of $F^{o_{m}}(t, \Phi(a, t))$ over $\mathbb{F}_{q}(a)$ implies, $F(t, \Phi(a, t)), \ldots, F^{o_{m-1}}(t, \Phi(a, t))$ are simultaneously irreducible over $\mathbb{F}_{q}(a)$. Let $\mathbb{F}_{q^{i}}$ be the field of constants of $\mathbb{F}_{q}$ in $L_i$. Hence, an asymptotic for fixed $r, m, \deg F^{o_{i}}$ for $1 \leq i \leq m$ such that, simultaneous irreducibility of $F^{o_{m}}(t, f(t)), \ldots, F(t, f(t))$ in $\mathbb{F}_{q}[t]$ is obtained when $q \to \infty$. Thus, this result is similar to the function field analogue of Bateman-Horn conjecture over large finite fields. Set
\[
\mathcal{F} = F^{o_{1}}(t, \Phi(a, (t))) \cdots F^{o_{m}}(t, \Phi(a, (t)))
\] 
(4.7)

Let $L$ be the splitting field of $\mathcal{F}$ over $\mathbb{F}_{q}(a)$. Clearly $\mathcal{F}$ is a monic separable polynomial. Each of $F^{o_{i}}(t, \Phi(a, (t)))$ for $1 \leq i \leq m$ are monic, distinct, irreducible and separable polynomials with disjoint ramifications in $L$ and we have containment $L_1 \subset L_2 \subset \cdots \subset L_m = L$ and, $L/\mathbb{F}_{q}(a)$ is a geometric extension with full field of constants $\mathbb{F}_{q}^{m}$, where $r^{m}$ is the least common multiple of $r, \ldots, r^{m}$. The map
\[
\text{Gal}(L/\mathbb{F}_{q}(a)) \cong \text{Gal}(L_1/\mathbb{F}_{q}(a)) \times \cdots \times \text{Gal}(L_m/\mathbb{F}_{q}(a))
\] 
(4.8)
\[
\sigma \mapsto (\sigma|L_1, \ldots, \sigma|L_m)
\] 
is an isomorphism (Theorem 1.3, [33]).

A conjugacy class in $S_r \times \cdots \times [S_r]^{m}$ is the Cartesian product of a conjugacy class in $S_r$, a conjugacy class in $[S_r]^{2}$ and so on. Let $(\lambda_1, \ldots, \lambda_m)$ be any cycle pattern in $S_r \times \cdots \times S_r$ and $C_1 \times \cdots \times C_m$ be the Cartesian product of corresponding conjugacy classes in $S_r \times [S_r]^{2} \times \cdots \times [S_r]^{m}$. Suppose the prime $P = (a_0 - c_0, \ldots, a_{d-1} - c_{d-1})$ of $\mathbb{F}_{q}(a)$ does not ramify in any of $L_1, \ldots, L_m$. We may note that, the polynomial $F^{o_{i}}(t, f(t)) \in \mathbb{F}_{q}[t]$ has a cycle pattern $\lambda_{F^{o_{i}}}$ if and only if, $\text{Frob}(L_i/\mathbb{F}_{q}(a))$ has cycle pattern $\lambda_i$ for $1 \leq i \leq m$. Then, by [2, Theorem 3.1], number of irreducible polynomials $f(t) \in \mathbb{F}_{q}[t]$ such that $F^{o_{1}}(t, f(t)), \ldots, F^{o_{m}}(t, f(t))$ are squarefree with cycle pattern $(\lambda_1, \ldots, \lambda_m)$ is
\[
\frac{|C_1|}{|S_r|} \cdot \frac{|C_2|}{|S_r|^2} \cdots \frac{|C_m|}{|S_r|^m} \cdot q^{d} + O_{r, m, \deg F^{o_{i}}(t, \Phi(a, t)))}(q^{d-\frac{1}{2}})
\] 
(4.9)
\[
= p(\lambda_1) \cdots p(\lambda_m) q^{d} + O_{r, m, \deg F^{o_{i}}(t, \Phi(a, t)))}(q^{d-\frac{1}{2}})
\]
where, $p(\lambda_i)$ is the probability of random permutation in $[S_r]^{i}$, having cycle structure $\lambda_i$ and the implied constant depends only on $r, m, \deg F^{o_{i}}$ for $1 \leq i \leq m$. Therefore, the number of $f(t) \in \mathbb{F}_{q}[t]$ such that $\mu(F^{o_{i}}(t, f(t))) = \pm 1$ for $1 \leq i \leq m$, is
\[
\frac{1}{2m} q^{d} + O_{r, m, \deg F^{o_{i}}}(q^{d-\frac{1}{2}})
\] 
(4.10)
where $\mu$ is the M"{o}bius function for $\mathbb{F}_{q}[t]$. Thus, $F^{o_{1}}(t, f(t)), \ldots, F^{o_{m}}(t, f(t))$ are simultaneously irreducible over $\mathbb{F}_{q}$ if and only if $\text{Gal}(L/\mathbb{F}_{q}(a))$ contains a conjugacy class $C$ of size
\[
\frac{|S_r|}{r} \cdot \frac{|S_r|^2}{r^2} \cdots \frac{|S_r|^m}{r^m}
\] 
(4.11)
Then, the number of monic polynomials \( f(t) = t^d + c_d t^{d-1} + \cdots + c_1 t + c_0 \) in \( \mathbb{F}_q[t] \), of degree \( d \geq 2 \) such that \( F^{\circ i}(t, f(t)), \ldots, F^{\circ m}(t, f(t)) \) is irreducible in \( \mathbb{F}_q[t] \) with cycle structure \( (\lambda_1, \ldots, \lambda_m) \) is,

\[
\frac{q^d}{r \cdots r^m} + O_{r,m, \deg F^{\circ i}}(q^{d-1/2})
\]

(4.12)

Thus we have,

**Theorem 4.3. (Bateman-Horn conjecture for iterated polynomials over large finite fields.)** Suppose that, for fixed \( m, r \in \mathbb{N} \), \( \text{Gal}(F^{\circ m}(t, \Phi(a, t)), \mathbb{F}_q(a)) = [S_r]^m \). Then in the limit \( q \to \infty \), the number of monic polynomials \( f(t) \in \mathbb{F}_q[t] \) of degree \( d \geq 2 \) such that \( F^{\circ i}(t, f(t)) \), for \( 1 \leq i \leq m \) are simultaneously irreducible over \( \mathbb{F}_q \) is

\[
\prod_{i=1}^{m} \deg F^{\circ i}(t, \Phi(a, t)) + O_{r,m, \deg F^{\circ i}}(q^{d-1/2})
\]

(4.13)

the implicit constant in the \( O \)-notation depends only on \( r, m, \deg F^{\circ i} \) for \( 1 \leq i \leq m \).

5. Stability of \( F(t, f(t)) \) over \( \mathbb{F}_q \)

A polynomial \( f \in \mathbb{F}_q[x] \) is said to be stable if all the iterates of \( f(x) \), given by \( f^{\circ n}(x), n \geq 2 \) are irreducible over \( \mathbb{F}_q \). For a fixed \( m \in \mathbb{N} \), let us assume the hypothesis of Theorem 2.2. Then,

\[ \text{Gal}(F^{\circ i}(t, \Phi(a, t)), \mathbb{F}_q(a)) \cong [S_r]^i \text{ for } 1 \leq i \leq m \]

(5.1)

Thus the iterates \( F^{\circ i}(t, \Phi(a, t)) \) for \( 1 \leq i \leq m \) are irreducible and square-free over \( \mathbb{F}_q(a) \). Hence, we conclude that \( F(t, \Phi(a, t)) \) is a stable polynomial over \( \mathbb{F}_q(a) \) as well. The necessary and sufficient condition for the stability of quadratic polynomials over the finite field \( \mathbb{F}_q \) of characteristic \( p \neq 2 \) is resolved in [3, Theorem 5]. Jones and Boston, [Proposition 2.3, 19] proved that any quadratic polynomial \( f(x) \in \mathbb{F}_q[x] \) is said to be stable, if and only if the adjusted critical orbit of \( f \) contains no squares. i.e., the set defined by

\[
\{ -f(\gamma) \} \cup \{ f^{\circ n}(\gamma_1), \ldots, f^{\circ n}(\gamma_k) | n \geq 2 \}
\]

contains no squares, where \( \gamma_i \) are the critical points. This result holds true for polynomials of arbitrary degree \( d \geq 2 \) over \( \mathbb{F}_q \). The asymptotic for the stability of quadratic polynomial over finite fields is given by Ostafe and Shparlinski [31]. The authors proved critical orbit of quadratic polynomials, over a finite field \( \mathbb{F}_q \) of \( q \) elements is of length \( O(q^{3/4}) \). Perez, et.al [32] generalized this result for polynomials of degree \( d > 0 \) given by \( f(X) = c_d X^d + \cdots + c_0 \in \mathbb{F}_q[X] \) such that, for a fixed \( k \in \mathbb{N} \), the number of stable polynomials is \( O(q^{d+1}/2^K + d^K q^{d+1/2}) \). Thus, the non trivial estimate for the stability of \( F(t, f(t)) \) over \( \mathbb{F}_q \) is given here:
Theorem 5.1. Suppose that, for fixed \( m \in \mathbb{N} \), \( \text{Gal}(\mathbb{F}_{q^m}(t, \Phi(a, t)), \mathbb{F}_q(a)) = \mathbb{F}_{p^m} \). Then in the limit \( q \to \infty \), the number of monic polynomials \( f(t) \in \mathbb{F}_q[t] \), of degree \( d \geq 2 \) such that, \( F^{\circ i}(t, f(t)) \) are square-free for \( 1 \leq i \leq m \)
\[
\frac{q^d}{2m}(1 + O_{r, m, \deg F^{\circ i}}(q^{-1/2}))
\]
the implied constant depend only on \( r, m, \deg F^{\circ i} \) for \( 1 \leq i \leq m \).

i.e., for fixed \( r, m, \deg F^{\circ i} \), for \( 1 \leq i \leq r \) and \( q \to \infty \) we have,
\[
\#\{f(t) \in \mathbb{F}_q[t], \deg f(t) = d \geq 2|\mu(F^{\circ i}(t, f(t))) = \pm 1 \text{ for } 1 \leq i \leq m\}
\]
\[
\frac{q^d}{2m}(1 + O_{m, r, \deg F^{\circ i}}(q^{-1/2}))
\]

Here, \( \mu \) denotes the M"obius function for \( \mathbb{F}_q[t] \) and the implied constant depends only on \( m, r, \deg F^{\circ i} \) for \( 1 \leq i \leq m \). Consequently, we note that, estimate in \( (5.3) \) follows directly from equation \( (4.10) \), for the number of polynomials \( f(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_0 \in \mathbb{F}_q[t] \) of arbitrary degree \( d \) such that, \( F(t, f(t)), \ldots, F^{\circ m}(t, f(t)) \) is square-free for fixed \( r, m, \deg(F^{\circ i}), 1 \leq i \leq m \) and \( q \to \infty \).

Besides, we note that, Theorem 5.1 can be considered as the polynomial analogue of the generalized Chowla conjecture on the autocorrelation of the M"obius function for polynomials in \( \mathbb{F}_q[t] \), which was resolved by Carmon and Rudnick (Theorem 1.1, [11]) for odd characteristic over large finite fields \( \mathbb{F}_q \). Authors show that, given \( r \) distinct monic polynomials of degree \( n > 0 \) in \( \mathbb{F}_q[x] \), the pairwise square independence of discriminants of these polynomials implies the polynomials are squarefree. Authors use Pellet’s formula and Weil bound for multiplicative character sums to prove the claim in \( (5.3) \).

The product of discriminants \( \text{disc}_i(F^{\circ i}(t, \Phi(a, t))) \cdot \text{disc}_j(F^{\circ j}(t, \Phi(a, t))) \) are pairwise square free for \( 1 \leq i, j \leq m \) for \( i \neq j \) in \( \mathbb{F}_q(a) \) means, the \( m \) iterated polynomials \( F^{\circ i}(t, \Phi(a, t)), 1 \leq i \leq m \) are simultaneously square-free over \( \mathbb{F}_q(a) \). This is due to Pellet’s formula, which states that for a polynomial ring \( \mathbb{F}_q[x] \), with \( q \) odd, the M"obius function \( \mu(F) \) can be computed from the discriminant \( \text{disc}(F) \) of \( F(x) \) as \( \mu(F) = (-1)^{\deg(F)} \chi_2(\text{disc}(F)) \) where \( \chi_2 \) is the quadratic character of \( \mathbb{F}_q \). Then applying Weil bound for multiplicative character sums, the estimate \( (5.3) \) is reclaimed.

6. Acknowledgment

The author thanks Prof. Soumya Das, Department of Mathematics, IISc, Bangalore, for many constructive discussion and encouragement which lead to this paper.

References

[1] S.S. Abhyankar, Galois Theory on the line in nonzero characteristic. Bull. Amer. Math. Soc.(N.S.), 27, 1, 1992.
[2] J.C. Andrade, L. Bary-Soroker and Z. Rudnick, Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$. Philos Trans A Math Phys Eng Sci. vol. 373, 2014.

[3] M. Ayad D. L. McQuillan Irreducibility of the iterates of a quadratic polynomial over a field. Acta Arithmetica, 93(1):87-97, 2000.

[4] Robert B. Ash, Abstract Algebra: The Basic Graduate Year.

[5] A.O. Bender and O. Wittenberg, A potential analogue of Schinzel Hyothesis for polynomials with coefficients in $\mathbb{F}_q[t]$. Int. Math. Res. Not., 36, 2237-2248, 2005.

[6] Alexei Entin On the Bateman-Horn Conjecture for polynomials over large finite fields. Compositio Math. 152:2525-2544, 2016.

[7] L. Bary-Soroker, Irreducible values of polynomials. Adv. Math., 229(2):854-874, 2012.

[8] Robert B. Ash, Abstract Algebra: The Basic Graduate Year.

[9] N. Boston and R. Jones, Arboreal Galois Representations Geom. Dedicata, 124, 2007.

[10] W. Burnside, Theory of Groups of finite order. C. J. Clay and Sons, Cambridge University Press Warehouse, London, 1897.

[11] D. Carmon, Z. Rudnick, The autocorrelation of the Mobius function and Chowla’s conjecture for the rational function field, The Quarterly Journal of Mathematics, doi:10.1093/qmath/has047, 2013.

[12] S. Chowla, A note on the construction of finite Galois fields $\mathbb{GF}(p^n)$ J. Math. Anal. Appl. 15, 53-54, 1966.

[13] S. D. Cohen, The distribution of polynomials over finite field. Acta Arith., 17, 255-271, 1970.

[14] S. D. Cohen, Uniform distribution of polynomials over finite field. J. London Math. Soc. 6, 93(102), 1972.

[15] S. D. Cohen, Polynomial Factorisation, graphs, designs and codes. Contemporary Mathematics, 168, 1994.

[16] P. M. Cohn, Algebra, 2nd ed., John Wiley & Sons, England, 1991.

[17] K. Conrad, The Galois correspondence at work. Available at https://kconrad.math.uconn.edu.

[18] K. Conrad, Irreducible values of polynomials: a non-analogy, Number Fields and Function Fields: Two Parallel Worlds, 71-85, Progress in Mathematics, 239, Birkhauser, Basel, 2005.

[19] R. Jones N. Boston. Settled polynomials over finite fields Proc. Amer. Math. Soc., 140:1849-1863, 2012.

[20] R. Jones, Galois representations from pre-image trees: an arboreal survey, Pub. Math. Besancon, 107-136, 2013.

[21] G. A. Jones, Primitive permutation groups containing a cycle, arXiv:1209.5169v1, 2012.

[22] J. Juul, Iterates of generic polynomials and generic rational functions, Trans. Amer. Math. Soc. 371, 809-831, 2019.

[23] B. Kadets, Large Arboreal Galois Representations, J. Number Theory, Volume 210, May 2020.

[24] J. P. Keating and Z. Rudnick, The variance of the number of prime polynomials in short intervals and in residue classes. Int. Math. Res. Not. IMRN, page 30 pp., 2012.

[25] S. Lang, Algebra, Revised Third edition, Springer, 2005.

[26] P. Stevenhagen and H. W. Lenstra Chebotarev and his density theorem The Math. Intelligencer, 18, pages, 26-37, 1996.

[27] N. Looper, Dynamical Galois groups of trinomials and Odoni’s conjecture Bull. Lond. Math. Soc. 51(2), 2019.

[28] K. K. Madhu, Galois theory and polynomial orbits, Ph.D. Thesis, University of Rochester, 2011.

[29] F. Michael and J. Moshe, Field Arithmetic, 3rd revised ed., Springer, Germany, 2008.
7. Declarations

7.1. Funding. This research work was funded by the Department of Science and Technology, Government of India, under the Women Scientist Scheme [SR/WOS-A/PM-31-2016] and [SR/WOS-A/PM-76-2021].

7.2. Data availability. Data sharing not applicable to this article as no data sets were generated or analysed during the current study.

7.3. Conflict of interest. The author declares there is no conflict of interest regarding the publication of this paper.

Department of Mathematics, Indian Institute of Science, Bangalore, Karnataka, India.

Email address: sushmapalimar@gmail.com