Abstract. We study the variance of sums of indicator functions of $s$th-power-free polynomials in arithmetic progression and in short-intervals in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of $q$ elements in the limit $q \to \infty$. We use a recent equidistribution result due to N.Katz to express these variances, in terms of matrix integrals over the unitary group, and evaluate them.

1. Introduction

The goal of this note is to investigate the fluctuation of sums of $s$th-power-free polynomials for $s \geq 2$ in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of $q$ elements, in the limit $q \to \infty$. Denote by $\alpha_s$, the indicator function of $s$th-power-free polynomials. We study the variance of the sum of $\alpha_s$ in arithmetic progression and in short interval, in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$ of $q$ elements, in the limit $q \to \infty$.

2. $s$th-power-free polynomials

Let $\mathbb{F}_q$ be a finite field of an odd cardinality $q$, and $\mathcal{M}_n$ be the set of all monic polynomials of degree $n$ with coefficients in $\mathbb{F}_q$. A polynomial in $\mathbb{F}_q$ is a $s$th-power-free polynomial if every root has multiplicity of at most $s-1$. We denote by $\alpha_s$ the indicator function of $s$th-power-free polynomials. i.e.,

\begin{equation}
\alpha_s = \begin{cases} 
1 & \text{if } f \text{ is } s\text{-power-free} \\
0 & \text{otherwise.}
\end{cases}
\end{equation}

The mean value of $\alpha_s$ over all monic polynomials of degree $n$ is defined to be

$$\langle \alpha_s \rangle := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \alpha_s(f)$$

Let $\text{Poly}^s_n(\mathbb{F}_q)$ denote the set of $s$th-power-free monic polynomials of degree $n > 1$. Then the total number of monic $s$th-power-free polynomials of degree $n > 1$ is given by

$$|\text{Poly}^s_n(\mathbb{F}_q)| = \begin{cases} 
q^n - q^{n-s+1} & \text{if } n \geq s \\
q^n & \text{if } 0 < n < s \\
1 & \text{if } n = 0
\end{cases}$$

The generating function for the number of monic $s$th-power-free polynomial of degree $n$ is

$$\sum_{n=0}^{\infty} \sum_{f \in \mathcal{M}_n} \alpha_s(f)u^n = \frac{Z(u)}{Z(u^s)}$$
where $Z(u)$ is the Zeta function of $\mathbb{F}_q[t]$, given by the product over monic irreducible polynomials in $\mathbb{F}_q[t]$: 
\[
Z(u) = \prod_p (1 - u^\deg_p)^{-1} = \frac{1}{1 - qu}
\]
Therefore by expanding and comparing coefficients, we have,
\[
\sum_{f \in \mathcal{M}_n} \alpha_s(f) = q^n(1 - \frac{1}{q^s - 1})
\]

2.1. **Arithmetic progression.** Let $Q \in \mathbb{F}_q[t]$ be a square-free polynomial of positive degree. The sum of $\alpha_s$ over all monic polynomials of degree $n$ lying in the arithmetic progressions $f \equiv A \mod Q$ is
\[
S_{\alpha_s;n;Q}(A) := \sum_{f \in \mathcal{M}_n, \ f = A \mod Q} \alpha_s(f)
\]
The average of this sum when we vary $A$ over residue classes coprime to $Q$ is
\[
\langle S_{\alpha_s;n;Q} \rangle = \frac{1}{\Phi(Q)} \sum_{f \in \mathcal{M}_n, \ (f,Q) = 1} \alpha_s(f)
\]
where $\Phi(Q)$ is the number of invertible residues modulo $Q$. Variance of $S_{\alpha_s;n;Q}$ is defined to be the average of the squared difference between $S_{\alpha_s;n;Q}$ and its mean value.
\[
Var(S_{\alpha_s;n;Q}) = \frac{1}{\Phi(Q)} \sum_{A \mod Q} |S_{\alpha_s;n;Q} - \langle S_{\alpha_s;n;Q} \rangle|^2
\]

2.2. **Short intervals.** A short interval in $\mathbb{F}_q[t]$ is a set of the form
\[
I(A;h) = \{ f : ||f - A|| \leq q^h \}
\]
where $A \in \mathcal{M}_n$ and $0 \leq h \leq n - 2$ and the norm is
\[
||f|| := \|\mathbb{F}_q[t]/(f)\| = q^{\deg f}.
\]
The cardinality of such a short interval is
\[
\#I(A;h) = q^{h+1} := H.
\]
We define for $1 \leq h < n$ and $A \in \mathcal{M}_n$
\[
N_{\alpha_s;h}(A) := \sum_{f \in I(A;h)} \alpha_s(f)
\]
be the number of $s$th-power-free polynomials in the interval $I(A;h)$. The mean value of $N_{\alpha_s;h}$ when we average over $A \in \mathcal{M}_n$ is
\[
\langle N_{\alpha_s;h} \rangle := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} N_{\alpha_s;h}
\]
The variance of $N_{\alpha_s;h}$ by definition is given by,
\[
Var(N_{\alpha_s;h}) := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |N_{\alpha_s;h} - \langle N_{\alpha_s;h} \rangle|^2
\]
In section 4 we compute the variance of $S_{\alpha_s;n;Q}$ and $N_{\alpha_s;h}$.
3. Dirichlet Characters and Katz’s equidistribution results

We recall standard material from Section 3 of [1] and Section 3 of [2]. For, $Q(t) \in \mathbb{F}_q[t]$, a polynomial of positive degree, $\Phi(Q)$ is defined as the order of the group $(\mathbb{F}_q[t]/Q)^\times$, that is the number of residues modulo $Q$ which are coprime to $Q$. A Dirichlet character modulo $Q$ is a homomorphism:

$$\chi : (\mathbb{F}_q[t]/(Q))^\times \to \mathbb{C}^\times.$$ 

One can extend $\chi$ to $\mathbb{F}_q[t]$ by defining it to vanish on polynomials which are not coprime to $Q$. A Dirichlet character needs to satisfy the following:

- $\chi(fg) = \chi(f)\chi(g)$ for all $f, g \in \mathbb{F}_q[t]$
- $\chi(f + hQ) = \chi(f)$ for all $f, h \in \mathbb{F}_q[t]$
- $\chi(f) = \chi(g)$ for all $f, g \in \mathbb{F}_q[t]$ such that $f \equiv g \mod Q$

We denote by $\Gamma(Q)$ the group of all Dirichlet characters modulo $Q$. Note that $|\Gamma(Q)|$ is the Euler totient function $\Phi(Q)$. The orthogonality relations for Dirichlet characters are:

$$\frac{1}{\Phi(Q)} \sum_{\chi \mod Q} \chi(f)\chi(g) = \begin{cases} 1 & \text{if } f \equiv g \mod Q \\ 0 & \text{otherwise.} \end{cases}$$

From this a standard argument shows that,

$$\frac{1}{\Phi(Q)} \sum_{A \mod Q} \chi_1(A)\chi_2(A) = \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{otherwise.} \end{cases}$$

Recall that a Dirichlet character $\chi$ is even if $\chi(cf) = \chi(f)$ for all scalars $c \in \mathbb{F}_q^\times$, and we say that $\chi$ is “odd” otherwise. The trivial character is denoted by $\chi_0$. A character $\chi$ is primitive if there is no proper divisor $Q' | Q$ so that $\chi(F) = 1$ whenever $F$ is coprime to $Q$ and $F = 1 \mod Q'$.

- $\Gamma_{\text{prim}}(Q)$ - the set of all primitive characters mod $Q$, $|\Gamma_{\text{prim}}(Q)| := \Phi_{\text{prim}}(Q)$
- $\Gamma_{\text{even}}(Q)$ - the set of primitive even characters mod $Q$, $|\Gamma_{\text{even}}(Q)| := \Phi_{\text{even}}(Q)$
- $\Gamma_{\text{odd}}(Q)$ - the set of primitive odd characters mod $Q$, $|\Gamma_{\text{odd}}(Q)| := \Phi_{\text{odd}}(Q)$
- $\Gamma_{d-\text{prim}}(Q)$ - the set of all characters $\chi$ modulo $Q$ such that $\chi^d$ is primitive for the fixed integer $d > 0$, $|\Gamma_{d-\text{prim}}(Q)| := \Phi_{d-\text{prim}}(Q)$.

As $q \to \infty$ almost all characters are primitive in the sense that,

$$\frac{\Phi_{\text{prim}}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right),$$

the implied constant depending only on $\deg Q$.

Moreover as $q \to \infty$ with degree $Q$ fixed, almost all characters are primitive and odd.

$$\frac{\Phi_{\text{odd}}(Q)}{\Phi(Q)} = 1 + O\left(\frac{1}{q}\right),$$

the implied constant depending only on degree $Q$.

For the number of primitive even characters, we consider the polynomial $Q(t)$ of the form, $Q(t) = t^m, m \geq 2$. Then, the number of primitive even characters modulo $t^m$ is $\Phi_{\text{even}}((t^m)) = q^{m-2}(q - 1)$, there are $O(q^{m-2})$ non-primitive even characters mod $T^m$.

**Dirichlet $L$-function.** The $L$-function $L(u, \chi)$ associated to a Dirichlet character $\chi$ mod $Q$ is defined as the product over all monic irreducible polynomials in $\mathbb{F}_q[t]$:

$$L(u, \chi) = \prod_{p \mid Q} (1 - \chi(p)u^{\deg p})^{-1}.$$
The product is absolutely convergent for $|u| < 1/q$. If $\chi = \chi_0$ is the trivial character modulo $Q$, then

$$L(u, \chi_0) = Z(u) \prod_{p \mid Q} (1 - u^{\deg p}),$$

where

$$Z(u) = \prod_{\text{prime}} (1 - u^{\deg p})^{-1} = \frac{1}{1 - qu}$$

is the Zeta function of $\mathbb{F}_q[t]$. Also set $\zeta_q(s) := Z(q^{-s})$. If $Q \in \mathbb{F}_q[t]$ is a polynomial of $\deg Q \geq 2$, and $\chi \neq \chi_0$ a nontrivial character mod $Q$, then the $L$ function $L(u, \chi)$ is a polynomial in $u$ of degree $\deg Q - 1$. Moreover if $\chi$ is an even character, then there is a trivial zero at $u = 1$. We may factor $L(u, \chi)$ in terms of inverse roots:

$$L(u, \chi) = \prod_{j=1}^{\deg Q - 1} (1 - \alpha_j(\chi)u).$$

The Riemann Hypothesis proved by Andre Weil (1948), asserts that for each (nonzero) inverse root, either $\alpha_j(\chi) = 1$ or $|\alpha_j(\chi)| = q^{\frac{1}{2}}$. If $\chi$ is primitive and odd character modulo $Q$, then all inverse roots $\alpha_j$ have absolute value $q^{\frac{1}{2}}$ and for $\chi$ primitive and even the same holds except for the trivial zero at 1. We then write the nontrivial inverse roots as $\alpha_j = q^{\frac{1}{2}} e^{i\theta_j}$ and the $L$-function (for a primitive character $\chi$) is

$$L(u, \chi) = (1 - \lambda_\chi u)^{-1} \det(I - uq^{\frac{1}{2}} \Theta_\chi)$$

$\Theta_\chi$, a unitary matrix given by, $\Theta_\chi = \diag(e^{i\theta_1}, ..., e^{i\theta_N})$ which determines a unique conjugacy class in the unitary group $U(N)$, where $N = \deg Q - 1$ and $\lambda_\chi = 0$ for odd character $\chi$ and $N = \deg Q - 2$ and for $\chi$ even, $\lambda_\chi = 1$. The unitary matrix $\Theta_\chi$ is called the unitarized Frobenius matrix of $\chi$.

Katz equidistribution results.

**Theorem 3.1.** (1) [1] Fix $m \geq 4$. The unitarized Frobenii $\Theta_\chi$ for the family of even primitive characters mod $T^{m+1}$ become equidistributed in the projective unitary group $PU(m - 1)$ of size $m - 1$, as $q$ goes to $\infty$.

(2) [3] If $m \geq 5$ and in addition the characteristics of the fields $\mathbb{F}_q \geq 2s + 1$, then the set of conjugacy classes $(\Theta_\chi, \Theta_{\chi^2}, ..., \Theta_{\chi^s})$ become equidistributed in the space of conjugacy classes of the product $(PU(m - 1))^s$ as $q$ goes to infinity.

This theorem enables us to replace the average over primitive even characters modulo $T^{n-h}$ by a matrix integral over the projective unitary group $PU(n - h - 2)$ (in equation (4.11)).

**Theorem 3.2.** (1) [2] Fix $m \geq 2$. Suppose we are given a sequence of finite fields $\mathbb{F}_q$ and squarefree polynomials $Q(T) \in \mathbb{F}_q[T]$ of degree $m$. As $q \to \infty$, the conjugacy classes $\Theta_\chi$ with $\chi$ running over all primitive odd characters modulo $Q$, are uniformly distributed in the unitary group $U(m - 1)$.

(2) [1] If in addition $s \geq 2$ and we restrict characteristics of fields $\mathbb{F}_q$ is bigger than $s$, then the collection of $s$-tuples of conjugacy classes $\Theta_{\chi_1}, \Theta_{\chi_2}, ..., \Theta_{\chi^s}$ with $\chi$ running over all characters such that $\chi_1, \chi_2, ..., \chi^s$ are primitive odd characters modulo $Q$, become equidistributed in the space of conjugacy classes of the $s$-fold product $U(m - 1)^s$.

This theorem enables us to replace the average over primitive odd characters modulo polynomial $Q$ of fixed degree $N + 1$ by a matrix integral over the unitary group $U(N)$ (in equation (5.8)).
4. Variance in short intervals

The mean value. The mean value of \( N_{\alpha,s,h} \), when we average over \( A \in \mathcal{M}_n \) is

\[
\langle N_{\alpha,s,h} \rangle := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} N_{\alpha,s,h}(A)
\]

\[
= \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \sum_{f \in I(A; h)} \alpha_s(f)
\]

\[
= q^{h+1} \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \sum_{f \in I(A; h)} \alpha_s(f)
\]

\[
= q^{h+1} (\alpha_s)_n
\]

In the rest of this section, we evaluate the variance of the number of \( s \)-power-free polynomials in short intervals given by \( N_{\alpha,s,h} \). We apply, [Lemma 5.4, [5]] which gives an expression for the variance of the short interval sums in terms of sums of certain arithmetic function \( \alpha \), which is nice in the sense, \( \alpha \) is even, \( \alpha \) is multiplicative and symmetric i.e., \( \alpha(f^n) = \alpha(f) \), if \( f(0) \neq 0 \) under the map defined by, \( f^*(t) := t^{deg(f)} f(\frac{1}{t}) \), twisted by primitive even Dirichlet characters. For such an \( \alpha \), as \( q \to \infty \), Lemma 5.4, [5] gives,

\[
(4.1) \quad \text{Var}(N_{\alpha}) = \frac{1}{\Phi_{ev}(T_{n-h})^2} \sum_{\chi \mod T^n \chi \neq \chi_0 \text{even}} |\sum_{m=0}^{n} \alpha(T^{n-m}) \mathcal{M}(m; \alpha \chi)|^2
\]

Here \( \Phi_{ev}(f) \) denotes the number of even primitive characters modulo \( f \in \mathbb{F}_q[t] \) and \( \mathcal{M}(m; \alpha \chi) := \sum_{f \in \mathcal{M}_n} \alpha(f) \chi(f) \).

Since the indicator function for \( s \)-power-free polynomial \( \alpha_s \) satisfies all conditions of \( \alpha \), we safely use [Lemma 5.4, [5]]. Hence we have the following result.

**Lemma 4.1.** As \( q \to \infty \)

\[
(4.2) \quad \text{Var}(N_{\alpha,s,h}) = \frac{1}{\Phi_{ev}(T_{n-h})^2} \sum_{\chi \mod T^n \chi \neq \chi_0 \text{even}} \sum_{m_1,m_2=n-s+1}^{n} \mathcal{M}(m_1, \alpha_s \chi) \mathcal{M}(m_2, \alpha_s \chi)
\]

where \( \Phi_{ev}(f) \) denotes the number of even primitive characters modulo \( f \in \mathbb{F}_q[t] \) and \( \mathcal{M}(n; \alpha_s \chi) := \sum_{f \in \mathcal{M}_n} \alpha_s(f) \chi(f) \).

**Proof.** By the definition of \( \alpha_s \), we have

\[
(4.3) \quad \alpha_s(t^{n-m}) = \begin{cases} 
1, & \text{for } m = n - s + 1, \ldots, n - 1, n \\
0, & \text{otherwise}
\end{cases}
\]

From the expression for Variance, (See, equation (4.1) and Lemma 4.1) we have,

\[
(4.4) \quad \frac{1}{\Phi_{ev}(T_{n-h})} \sum_{\chi \mod T^n \chi \neq \chi_0 \text{even}} \sum_{m_1,m_2=0}^{n} \alpha_s(t^{n-m_1}) \alpha_s(t^{n-m_2}) \mathcal{M}(m_1, \alpha_s \chi) \mathcal{M}(m_2, \alpha_s \chi)
\]

combining the definition of \( \alpha_s \) (4.3) and with equation (4.4) the result (4.2) follows. \( \Box \)
Hence, by expanding and comparing coefficients we have,

\[ \sum_{m \geq 0} \mathcal{M}(m; \alpha_s \chi) u^m = \frac{L(u, \chi)}{L(u^s, \chi^s)} \]

For an even primitive character \( \chi \mod t^{n-h} \), \( L(u, \chi) \) has a trivial zero at \( u = 1 \), hence we may write (see equation (3.3))

\[ L(u, \chi) = (1 - u) \det(I - uq^{1/2} \Theta_\chi) \]

\[ L(u^s, \chi^s) = (1 - u^s) \det(I - u^s q^{1/2} \Theta_{\chi^s}) \]

and writing (with \( N = \deg Q - 1 \))

\[ \det(I - uq^{1/2} \Theta_\chi) = \sum_{j=0}^{N} \text{tr} \Lambda_j(\chi) q^{1/2} u^j \]

\[ \frac{1}{\det(I - uq^{1/2} \Theta_\chi)} = \sum_{l=0}^{\infty} \text{tr} \text{Sym}^l(\chi) q^{1/2} u^l \]

Abbreviate as follows:

\[ \Lambda_i(\chi) := \text{tr} \Lambda_i(\Theta_\chi), \text{Sym}^i(\chi) = \text{tr} \text{Sym}^i(\Theta_\chi) \]

where \( \Theta_\chi \in U(n - h - 2) \) is the unitarized Frobenius class. Therefore the generating function of \( \mathcal{M}(n; \alpha_s \chi) \) for \( \chi \mod t^{n-h} \) such that, \( \chi, \ldots, \chi^s \) are primitive and even can be written as follows:

\[ \frac{L(u, \chi)}{L(u^s, \chi^s)} = \frac{(1 - u) \left( \sum_{j=0}^{N} \Lambda_j(\chi) q^{1/2} u^j \right) \left( \sum_{k \geq 0} u^{ks} \right) \left( \sum_{l \geq 0} \text{Sym}^l(\chi^s) q^{1/2} u^l \right)}{(1 - u^s) \left( \sum_{k \geq 0} u^{ks} \right) \left( \sum_{l \geq 0} \text{tr} \text{Sym}^l(\chi^s) q^{1/2} u^l \right)} \]

\[ = \sum_{m \geq 0} \left( \sum_{j+k+l=m \atop 0 \leq j \leq N \atop l,k \geq 0} \Lambda_j(\chi) \text{Sym}^l(\chi^s) q^{1/2} - \sum_{j+k+l=s-1 \atop 0 \leq j \leq N \atop l,k \geq 0} \Lambda_j(\chi) \text{Sym}^l(\chi^s) q^{1/2} \right) u^m \]

Hence, by expanding and comparing coefficients we have,

\[ \mathcal{M}(m, \alpha_s \chi) = S_\chi(m) - S_\chi(m-1) \]

where for \( m \geq 0 \)

\[ S_\chi(m) := \sum_{j+k+l=m \atop 0 \leq j \leq N \atop l,k \geq 0} \Lambda_j(\chi) \text{Sym}^l(\chi^s) q^{1/2} \]

Now back to the variance formula, See, Lemma 4.1, equation (4.1), we can split the sum into two parts: the sum over \( \chi \not\equiv \chi_0 \mod t^{n-h} \), \( \chi \in \Gamma_{\text{prim}}^{\text{ev}}(t^{n-h}) \) and the sum over even, non primitive characters \( \mod t^{n-h} \). The first sum will give the main term, since most of the even characters are also primitive and the second sum will give an error term.

**Lemma 4.2.** Let \( \chi \) be a primitive even character \( \mod t^{n-h} \). Then for any \( n \), we have

\[ \sum_{m=0}^{n} \alpha_s(t^{n-m}) \mathcal{M}(m, \alpha_s \chi) = \sum_{m=n-s+1}^{n} \mathcal{M}(m, \alpha_s \chi) \]
Theorem 4.3. Let $\chi \mod s$. Hence the equation (4.8).

\[
\alpha_s(t^{n-m}) = \begin{cases} 
1 & \text{if } m = n - s + 1, \ldots, n \\
0 & \text{if } m = n - s, \ldots, 0.
\end{cases}
\]

Hence the equation (4.8). \qed

Proof. This follows directly from the definition of $\alpha_s(t^{n-m})$ since,

By using the equidistribution result Theorem 3.1 (ii) we get

For $\chi$ even and primitive consider inner sum in the variance formula: Hence we get,

The largest power of $q$ is obtained in the first sum, Hence the contribution of even primitive characters to the variance formula is

where $\Phi_{ev}$ is the lower order term of $\alpha_s(t^{n-m})$ by the choice of $j, k, l$, hence negligible. The above sum after substituting for

is

By using the equidistribution result Theorem 3.1 (ii) we get

It is well known that $\Lambda_j$ and $\text{Sym}_j$ are distinct irreducible representations of the unitary group $U(N)$, and hence one gets [Section 4.6.6]

\[
\int_{U(N)} \overline{\text{tr} \Lambda_j(U)} \overline{\text{tr} \Lambda_i(U)} dU = \delta_{j,i}
\]

and

\[
\int_{U(N)} \overline{\text{tr} \text{Sym}_j(U)} \overline{\text{tr} \text{Sym}_k(U)} dU = \delta_{j,k}
\]
Now, using equations (4.12), sum in equation (4.10) becomes:

\[
\frac{H}{q^n \varphi(n)} \sum_{\chi \equiv \chi_0 \text{ primitive, even}} q^{j+l} |\Lambda_j(\chi) \text{Sym}^l(\chi^*)|^2 \sim \frac{H}{q^n} \sum_{0 \leq j \leq n \atop l,k \geq 0} q^{j+l}
\]

Next, it remains to evaluate the sum:

\[
S(n) := \sum_{j+l=n \atop 0 \leq j \leq n-h-2} q^{j+l}
\]

The highest power of \( q \) is obtained when

\[
j = n - h - 2
\]

then

\[
l = \frac{n - N}{s} = \frac{h + 2}{s}
\]

Therefore, the largest power of \( q \) is:

\[
q^{\frac{s(n-h-2)+h+2}{s}}
\]

There are \( O(q^{n-h-2}) \) non primitive even characters mod \( n-h \). From the above calculation, it follows that, the sum over all nonprimitive characters is estimated to be, \( O(q^{-2(n-h-1)} \cdot q^{n-h-2} \cdot q^{\frac{s(n-h-2)+h+2}{s}}) \). Hence, as \( q \to \infty \)

\[
S(n) \sim q^{\frac{s(n-h-2)+h+2}{s}} \quad \text{for} \quad n \equiv N + \lambda_j \mod{s} \quad \text{and} \quad \lambda_j \in \{0, 1, 2, \ldots, (s-1)\}
\]

(4.13)

\[
S(n) \sim \begin{cases} 
q^{\frac{s(n-h-2)+h+2}{s}}, & n \equiv N \mod{s} \\
q^{\frac{s(n-h-2)+h+2-\lambda_j}{s}}, & n \not\equiv N \mod{s}
\end{cases}
\]

Therefore substituting the value \( S(n) \) in equation (4.9), we get

\[
\text{Var}(N_{\alpha_s;h}) \sim \frac{H}{q^n} S(n)
\]

(4.14)

\[
\text{Var}(N_{\alpha_s;h}) \sim \begin{cases} 
q^{\frac{h+2-\lambda_j}{s}}, & n \equiv N \mod{s} \\
q^{\frac{h+2-\lambda_j}{s}}, & n \not\equiv N \mod{s}
\end{cases}
\]

This completes proof of Theorem 4.3.

5. Variance in arithmetic progressions

Given a polynomial \( Q \in \mathbb{F}_q[t] \), the average of \( S_{\alpha_s;n;Q} \) when we vary \( A \) over residue classes coprime to \( Q \) equals to

\[
\langle S_{\alpha_s;n;Q} \rangle = \frac{1}{\Phi(Q)} \sum_{f \in M_n \atop (f,Q)=1} \alpha_s(f) = \frac{1}{\Phi(Q)} \sum_{f \in M_n} \chi_0(f) \alpha_s(f)
\]

(5.1)
We present a formula for variance of $S_{\alpha,n;Q}$ using Dirichlet characters, [5, sec 4.1]. We start with the following expansion, using the first orthogonality relation for Dirichlet characters on arithmetic progression:

\[(5.2)\]

\[
S_{\alpha,n;Q} = \frac{1}{\Phi(Q)} \sum_{f \in M_n} \alpha_s(f) + \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0} \chi(A)\mathcal{M}(n, \alpha_s\chi)
\]

where

\[
\mathcal{M}(n, \alpha_s\chi) = \sum_{f \in M_n} \alpha_s(f)\chi(f)
\]

Contribution of trivial character is equal to the average of $S_{\alpha,n;Q}(A)$. Therefore,

\[
S_{\alpha,n;Q} - \langle S_{\alpha,n;Q} \rangle = \frac{1}{\Phi(Q)} \sum_{\chi \neq \chi_0 \mod Q} \chi(A)\mathcal{M}(n, \alpha_s\chi)
\]

using the above and the second orthogonality relation for Dirichlet character, we have the following expression for the variance.

\[(5.3)\]

\[
Var(S_{\alpha,n;Q}) = \langle |S_{\alpha,n;Q} - \langle S_{\alpha,n;Q} \rangle |^2 \rangle = \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \alpha_s\chi)|^2
\]

**Theorem 5.1.** Let $Q$ be a prime polynomial and set $N := \deg Q - 1$, then in the limit $q \to \infty$ the following holds:

Proof. The generating function of $\mathcal{M}(n; \alpha_s\chi)$ is

\[
\sum_{n=0}^{\infty} \mathcal{M}(n; \alpha_s\chi)u^n = \frac{L(u, \chi)}{L(u^s, \chi^s)}
\]

If both $\chi, \chi^s$ are primitive odd characters (which happens for almost all $\chi$), then from equation 3.3

\[
L(u, \chi) = \det(I - uq^{\frac{1}{2}}\Theta_{\chi})
\]

\[
L(u^s, \chi^s) = \det(I - u^sq^{\frac{1}{2}}\Theta_{\chi}^s)
\]

and writing (with $N = \deg Q - 1$)

\[(5.4)\]

\[
\det(I - uq^{\frac{1}{2}}\Theta_{\chi}) = \sum_{j=0}^{N} \text{tr} \Lambda_j(\chi)q^{\frac{1}{2}}u^j
\]

\[
\frac{1}{\det(I - q^{\frac{1}{2}}u^s\Theta_{\chi}^s)} = \sum_{l=0}^{\infty} \text{tr} \text{Sym}^l(\chi^s)q^{\frac{1}{2}}u^{sl}
\]

Abbreviate as follows:

\[
\Lambda_i(\chi) := \text{tr} \Lambda_i(\Theta_{\chi}), \text{Sym}^i(\chi) = \text{tr} \text{Sym}^i(\Theta_{\chi})
\]

Hence for $n \geq N$, we have,

\[(5.6)\]

\[
\mathcal{M}(n, \alpha_s\chi) = \sum_{\substack{j + sl = n \\ 0 \leq j \leq N \\ l \geq 0}} \Lambda_j(\chi)\text{Sym}^k(\chi^s)q^{\frac{j+sl}{2}}
\]
Therefore, by using the formula for the variance, given in (5.3), we have
\[
Var(S_{\alpha; n; Q}) = \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \alpha_s \chi)|^2
\]
\[
= \frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} \left| \sum_{j+s,l=0}^{j<s,l=n} j+l \right|^2
\]
(5.7)

We invoke Theorem 3.2(ii) which asserts, the collection of $s$-tuples of conjugacy classes $\Theta_\chi, \Theta_{\chi^2}, \ldots, \Theta_{\chi^s}$ are uniformly distributed in $U(\deg Q - 1)$,
\[
\frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} \left| \sum_{j+s,l=0}^{j<s,l=n} j+l \right|^2
\]
\[
\sim \frac{1}{\Phi(Q)} \int_{U(N)} \left| \int_{\mathbb{C}} q^{j+l} \left| trA_j(U_1)trA_l(U_2) \right|^2 dU_1dU_2 \right|
\]
(5.8)

From equations (4.12) we arrive at
\[
\frac{1}{\Phi(Q)^2} \sum_{\chi \neq \chi_0} |\mathcal{M}(n; \alpha_s \chi_j)|^2 \sim \frac{1}{\Phi(Q)} \sum_{j+sl=n \atop 0<j\leq N} q^{j+l}
\]
(5.9)

Next, we want to evaluate
\[
S(n) := \sum_{j+sl=n \atop 0<j\leq N} q^{j+l} = \sum_{j+nl=n \atop j \equiv n \mod s} q^{n+j(s-1)}/s
\]
The highest power of $q$ is attained when $j = N$. Hence,
\[
S(n) \sim q^{n+N(s-1)-\lambda_j}/s, \text{ for } n \equiv N + \lambda_j \mod s \text{ and } \lambda_j \in \{0, 1, 2 \ldots (s-1)\}
\]
(5.10)

Therefore,
\[
S(n) \sim \begin{cases} 
q^{n+N(s-1)}/s, & n \equiv N \mod s \\
q^{n+N(s-1)-\lambda_j}/s, & n \not\equiv N \mod s
\end{cases}
\]
(5.11)

The number of even characters is $\Phi_{ev}(Q) = \frac{\Phi(Q)}{q-1}$ and the number of non-primitive characters is $O(\Phi(Q)/q)$, hence the number of characters which are not odd and primitive is $O(\Phi(Q)/q)$. Hence,
\[
Var(S_{\alpha;n;Q}) \sim \begin{cases} 
\frac{1}{\Phi(Q)} q^{n+N(s-1)}/s, & n \equiv N \mod s \\
\frac{1}{\Phi(Q)} q^{n+N(s-1)-\lambda_j}/s, & n \not\equiv N \mod s
\end{cases}
\]

6. Acknowledgement

The author would like to thank Prof. Soumya Das, Department of Mathematics, IISc, Bangalore, for many helpful discussions and suggestion while writing the manuscript. This research work was supported by the Department of Science and Technology, Government of India, under the Women Scientist Scheme [SR/WOS-A/PM-31-2016].
REFERENCES

[1] N. Katz, Witt vectors and a question of Keating and Rudnick. Int. Math. Res. Not. IMRN, no.16, 3613638.
[2] N. Katz, On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor. Int. Math. Res. Not. IMRN 2013, no.14, 32213249.
[3] N. Katz, Witt vectors and a question of Entin Keating and Rudnick about primitive Dirichlet characters with squarefree conductor. Int. Math. Res. Not. IMRN, no.14, 595975.
[4] N. Katz, On two questions of Entin Keating and Rudnick about primitive Dirichlet characters. Int. Math. Res. Not. IMRN 2013, no.15, 6046069.
[5] 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.
[6] E. Roditty-Gershon, Square-full polynomials in short intervals and in arithmetic progressions. Res. Number Theory 3(2017), 3:3. MR359721.

Department of Mathematics, Indian Institute of Science, Bangalore, India. E-mail address: psushma@iisc.ac.in, sushmapalimar@gmail.com.