Beyond Binary: Crosscorrelation of Higher Order Character Sequences

Mriganka Dey[*1,2], Sampa Dey[†3], Sampurna Pal[‡4], Subhabrata Samajder[§1], and Rana Barua[¶1]

[1] *Institute for Advancing Intelligence (IAI), TCG-CREST, Kolkata, India*
[2] *Department of Computer Science, RKMVERI, Belur, India*
[3] *Statistic and Mathematics Unit, Indian Statistical Institute, Kolkata, India*
[4] *Department of Mathematics and Statistics, IIT Kanpur, Kanpur, India*

July 22, 2026

Abstract

The arithmetic crosscorrelation of pseudorandom sequences is a key measure of their suitability for cryptographic and communication applications. While prior work has addressed this quantity for binary sequences, the non-binary setting has remained largely unexplored. This paper initiates a systematic study of the arithmetic crosscorrelation of non-binary pseudorandom sequences constructed from higher-order multiplicative characters over finite fields. For two sequences of coprime periods P and Q, defined via r-th order characters of polynomials of degree d, we show that the joint local patterns of the sequences are asymptotically uniformly distributed, and use this to derive an explicit bound on the arithmetic crosscorrelation $C^A_{S,T}(\tau)$. Specifically, we establish

$$\mathcal{N}\big(C^A_{S,T}(\tau)\big) \;=\; O\Big(\big(\varphi(r)dP^{1/2}Q(\log P)^2\big)^{\varphi(r)}\Big)$$

for all shifts τ, for r-th order character sequences, where $\varphi(\cdot)$ is the *Euler totient function* and $\mathcal{N}(\cdot)$ denotes the norm function. To the best of our knowledge, this work establishes the first nontrivial upper bounds on the arithmetic crosscorrelation of non-binary pseudorandom sequences, thereby extending the results of Chen et al. [IEEE IT'22] and Yan and Ke [ePrint: 2026/616], which were obtained exclusively for the Legendre sequence.

1 Introduction

Pseudorandom numbers are outputs of deterministic algorithms, but behave like truly random numbers in the sense that they show statistical properties that are similar or very close to the statistical properties exhibited by truly random numbers. Although the measure of randomness of a pseudorandom sequence can be formally defined in terms of Kolmogorov complexity, it was subsequently shown that Kolmogorov complexity is *uncomputable*. Therefore, to show that a given sequence of numbers exhibits nice pseudorandom properties, the following two approaches are normally taken. First approach is to study its various statistical properties and

[*]mriganka.dey.86@tcgcrest.org
[†]sampa.math@gmail.com
[‡]sampu.andul@gmail.com
[§]subhabrata.samajder@tcgcrest.org
[¶]rana.barua@tcgcrest.org

show that these properties do not deviate "too much" from those of a truly random sequence of the same length. Whereas the second approach, which is used in areas like cryptography, defines pseudorandom numbers in the following manner. Given a polynomial-length sequence of pseudorandom numbers, it is difficult for any algorithm (called distinguishers) having polynomial computational power to tell apart the pseudorandom number sequence from that of a truly random sequence of the same length.

The unpredictable nature of pseudorandom sequences is a desirable feature that finds application across many different areas. For example, (computationally) unpredictable sequences are needed for cryptography, whereas uncorrelated sequences are useful in wireless communications [1] and radar systems [2]. For example, Barker codes, which are binary sequences with the ideal autocorrelation property such that the absolute values of the off-peak (non-cyclic) autocorrelation coefficients are upper bounded by 1, are used in technologies like the radar [2], mobile phones [1], telemetry [35], ultrasound imaging and testing [42, 13], GPS [25] and Wi-Fi [31].

In cryptographic applications, unpredictability is essential, and this is closely related to having low and well-controlled autocorrelation values, which prevent an adversary from exploiting structural patterns in the sequence. One such application is to translate the notions of *confusion* and *diffusion*, introduced by Shannon in his seminal work [34], to properties of Boolean functions [6]. Particularly, research in symmetric-key cryptanalysis has shown that to prevent certain types of attacks, the underlying Boolean function needs to possess certain properties. A basic tool for this is the crosscorrelation between two n-variable boolean functions f and g, which is defined as the cyclic crosscorrelation between the sequences $(f(0), f(1), \ldots, f(2^{n-1}))$ and $(g(0), g(1), \ldots, g(2^{n-1}))$, i.e., $C_{f,g}(u) = \sum_{x\in\{0,1\}^n}(-1)^{f(x)\oplus g(x\oplus u)}$ [32] with $C_{f,g}(0)$ referred to as the correlation between f and g. Recall that an S-box is a vectorial Boolean function from $\{0,1\}^n \to \{0,1\}^m$ and in many symmetric-key designs they provide one of the possible (if not the only) sources of confusion, as mentioned by Shannon. To prevent attacks like linear cryptanalysis, ideally, one would like the crosscorrelation between an arbitrary combination of the S-box output and any linear combination of the input to be zero. However, this is not possible due to Parseval's theorem. Hence, the design of cryptographically "nice" S-boxes involves studying the correlation and crosscorrelation properties of S-boxes [32].

The (statistical) pseudorandomness of a sequence can be quantified through a variety of measures. Among the most general is the correlation measure of order μ, introduced by Mauduit and Sàrközy [27, 7, 26, 28, 29, 30, 33], which has since been the subject of extensive investigation. Arithmetic crosscorrelation, originally introduced by Mandelbaum [24], constitutes another prominent measure of pseudorandomness. Traditional methods of constructing pseudorandom sequences include shift register-based constructions, which play a vital role in fields such as communications, radar, and stream ciphers [14, 15]. In the 1990s, Klapper and Goresky [21] introduced the *feedback with carry shift register (FCSR)* sequences, which can be viewed as an arithmetic analogue of the well-studied *linear feedback shift register (LFSR)* based pseudorandom sequences. These constructions further highlight the deep connection between algebraic structure and correlation measures, making arithmetic crosscorrelation and autocorrelation fundamental tools in assessing the cryptographic strength and practical applicability of pseudorandom sequences.

1.1 Related Works

Pseudorandom sequences play a fundamental role in cryptography due to their wide-ranging applications in the design of secure cryptographic primitives. In a pioneering work, Damgård [10] investigated the randomness properties of Legendre and Jacobi sequences, laying the foundation

for a rich line of research on the cryptographic hardness of Legendre and higher-order character sequences. In recent years, Gibbs and Wu [9] established the one-wayness of the Legendre symbol under the Quadratic Residuosity assumption by proving the existence of a weak pseudorandom function (wPRF) derived from the Legendre sequence. Extending this line of work, Dey et al. [12] recently demonstrated that quartic character sequences also possess one-wayness under the same assumption by constructing a weak pseudorandom function based on the quartic character. This naturally leads to the question of understanding the statistical pseudorandomness properties of Legendre and quartic character sequences under various pseudorandomness measures, among which arithmetic autocorrelation is a particularly significant one.

It is worth emphasizing that extending these results to the r-th power residue symbol presents several non-trivial challenges. Beyond the inherent technical difficulties, two fundamental requirements must be met. First, there must exist an efficient deterministic algorithm for computing the r-th power residue symbol. Second, the cyclotomic ring of integers $\mathbb{Z}[\zeta_r]$, where ζ_r denotes a primitive r-th root of unity, should be *norm-Euclidean* (to be defined later), as this property is crucial for carrying out the underlying arithmetic efficiently.

Furthermore, to ensure that the r-th power residue symbol is defined unambiguously, it must be evaluated with respect to a distinguished generator of each prime ideal, known as a *primary prime*. In principle, the P-th power residue symbol, for an odd prime $P \leq 13$, can be computed using the generic algorithm of Caranay and Scheidler [6, § 7]. However, obtaining an efficient implementation for a fixed value of P remains a difficult problem. Explicit deterministic algorithms are currently available only for a handful of small exponents, including the fourth power residue symbol [39], the eighth power residue symbol [23, Chapter 9], the eleventh power residue symbol [20], and the thirteenth power residue symbol [5]. De Boer and Pagano [11] later proposed a generic algorithm for arbitrary power residue symbols. However, their approach is inherently probabilistic, rendering it unsuitable for most cryptographic applications. Consequently, the deterministic computation of the ninth power residue symbol, as well as arbitrary higher-order power residue symbols beyond the thirteenth, remains an important open problem.

In a significant development, Brier *et al.* [4] introduced a unified and simplified framework for computing primary elements in P-th cyclotomic fields, encompassing and generalizing all previously known constructions. Building on this framework, they presented efficient deterministic algorithms for computing the P-th power residue symbol for every prime $P \in \{3, 5, 7, 11, 13\}$. They also developed efficient deterministic algorithms for computing the ninth and sixteenth power residue symbols, substantially extending the range of residue symbols that can be evaluated efficiently in practice.

The concept of arithmetic autocorrelation was first introduced by Mandelbaum [24] in his investigation of arithmetic codes. This notion was subsequently broadened by Goresky and Klapper [16, 15], who extended it to arithmetic crosscorrelation in the framework of their study of FCSR sequences. A recent result due to Hofer, Merai and Winterhof [18] demonstrates that binary sequences whose higher-order correlation measures are sufficiently small cannot simultaneously possess large arithmetic autocorrelation — a quantity that measures the crosscorrelation of a sequence with a shifted copy of itself. The authors further remarked that this result admits a natural extension to the non-binary setting. Subsequently, Chen et al. [8] demonstrated that binary sequences with coprime periods admit constant arithmetic crosscorrelation, and established an upper bound on the arithmetic crosscorrelation of Legendre sequences. Recently, Yan and Ke [41] derived an upper bound for the arithmetic crosscorrelation of binary sequences with coprime periods constructed using the *generalized Legendre symbol*. They additionally demonstrated that non-binary sequences with coprime periods also exhibit constant arithmetic

crosscorrelation. However, the authors left the question of deriving the arithmetic crosscorrelation for non-binary sequences open.

1.2 Our Contribution

Let ζ_r be a primitive r-th root of unity, the ring $\mathbb{Z}[\zeta_r]$ denote the integral closure of $\mathbb{Z}$ in the r-th cyclotomic extension field $\mathbb{Q}(\zeta_r)$. Our primary contribution is to develop a general analytic framework for sequences constructed from *r-th order multiplicative characters* over finite fields. Let $S = (s_i)_{i\geq 0}$ and $T = (t_i)_{i\geq 0}$ be two sequences of coprime periods P and Q, respectively, defined by r-th order characters evaluated on polynomial functions of arguments, i.e., $\chi_\pi(f(x))$ and $\chi_\rho(g(x))$, where χ_π is some r-th order character and f is a polynomial of degree d over the finite field $\mathbb{F}_P$ with $\pi \mid P$, and χ_ρ is some r-th order character and g is a polynomial of degree d over the finite field $\mathbb{F}_Q$ with $\rho \mid Q$. We study the arithmetic crosscorrelation $C^A_{S,T}(\tau)$ by analyzing the distribution of joint local patterns of the form

$$(s_{n-k}, \ldots, s_n, t_{n-k}, \ldots, t_n),$$

and establish that these patterns are asymptotically uniformly distributed.

We define the r-th order residue of $\alpha \in \mathbb{Z}[\zeta_r]$ with respect to a prime $\pi \in \mathbb{Z}[\zeta_r]$ such that $\pi \mid P$ and P is an integer prime congruent to 1 (mod r), as $\alpha^{\frac{P-1}{r}} \mod \pi$. Notice that this means that $\mathbb{Z}[\zeta_r]$ must be an Euclidean domain such that α can be written as $\alpha = \beta \cdot \pi + \xi$, where $0 \leq \mathcal{N}(\xi) < \mathcal{N}(\pi)$ and $\mathcal{N}(\cdot)$ is an absolute field norm of $\mathbb{Q}(\zeta_r)$. In other words, $\mathbb{Z}[\zeta_r]$ needs to be *norm-Euclidean*. However, recall that $\mathbb{Z}[\zeta_r]$ is not necessarily norm-Euclidean. But, for $r \in \{3, 4, 5, 6\}$, the rings $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\omega]$ (Eisenstein integers), $\mathbb{Z}[\zeta_4] = \mathbb{Z}[i]$ (Gaussian integers), $\mathbb{Z}[\zeta_5]$, and $\mathbb{Z}[\zeta_6]$ are all known to be norm-Euclidean, where $i = \sqrt{-1}$, $\omega = \frac{-1+i\sqrt{3}}{2}$. In fact, the complete list of norm-Euclidean cyclotomic rings $\mathbb{Z}[\zeta_r]$ (except for $r \not\equiv 2 \bmod 4$) with *class number*[1] 1 is known to be exactly those with $r \in \{1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 20, 21, 24\}$, as mentioned by Lemmermeyer [22, Section 8]. In Theorem 3, we obtain a nontrivial upper bound that holds for the before mentioned arbitrary r-th power residue characters and get explicit upper bound for $r \in \{3, 4, 5, 6\}$.

Our primary contribution is to develop a general analytic framework for sequences constructed from *r-th order multiplicative characters* over finite fields. Let $S = (s_i)_{i\geq 0}$ and $T = (t_i)_{i\geq 0}$ be two sequences of coprime periods P and Q, respectively, defined by r-th order characters evaluated on polynomial functions of arguments, i.e., $\chi_\pi(f(x))$ and $\chi_\rho(g(x))$, where χ_π is some r-th order character and f is a polynomial of degree d over the finite field $\mathbb{F}_P$ with $\pi \mid P$ and χ_ρ is some r-th order character and g is a polynomial of degree d over the finite field $\mathbb{F}_Q$ with $\rho \mid Q$. We study the arithmetic crosscorrelation $C^A_{S,T}(\tau)$ by analyzing the distribution of joint local patterns of the form

$$(s_{n-k}, \ldots, s_n, t_{n-k}, \ldots, t_n),$$

and establish that these patterns are asymptotically uniformly distributed.

Our approach combines a power-basis decomposition over the underlying field of multiplicative characters with sharp bounds on character sums. A key technical ingredient is the application of the Weil bound [38] to suitably constructed polynomial arguments, which enables us to

[1]Let R be a Dedekind domain, and $I(R)$ denote the group of nonzero fractional ideals of R. If $P(R) \subseteq I(R)$ denotes the subgroup of nonzero principal fractional ideals, then the quotient group $\mathrm{Cl}(R) := I(R)/P(R)$ is called the *ideal class group* of R, and its order $h_R := |\mathrm{Cl}(R)|$ is called the *class number* of R.

control correlations among shifted evaluations of the underlying sequences. As a consequence, we prove that for all shifts τ,

$$\mathcal{N}\left(C^{A}_{S,T}(\tau)\right) \;=\; O\left(\varphi(r)dP^{1/2}Q(\log P)^2\right)^{\varphi(r)},$$

where d is the degree of the defining polynomial and $\mathcal{N}(\cdot)$ denotes the underlying field norm. To the best of our knowledge, this is the *first nontrivial upper bound* on the arithmetic crosscorrelation of non-binary sequences.

Although prior works have primarily focused on binary sequences, especially those constructed from quadratic characters, little is known quantitatively about sequences derived from higher-order characters. Our work, therefore significantly generalizes and strengthens the earlier results of Chen et al. [8] and Yan and Ke [41]. In particular, while it is known that sequences with coprime periods exhibit constant arithmetic crosscorrelation, our results provide explicit quantitative bounds in the non-binary setting and reveal the underlying distributional structure responsible for this phenomenon. Recently, Yan and Ke [40] proved that ternary, quaternary, and 6-ary sequences with ideal arithmetic autocorrelation do not exist. Therefore, our results when viewed together with the result of Yan and Ke [40] establish that although the arithmetic autocorrelation for the ternary, quaternary, and 6-ary power residue sequences are greater than zero, the deviation is not too much.

2 Preliminaries

We use the standard notation for sets of numbers: $\mathbb{N}$ denotes the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Q}$ the rationals, $\mathbb{R}$ the reals, and $\mathbb{C}$ the complex numbers. In this work, we say that $f(x) = O(g(x))$, if there exists an absolute constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for all large values of x. We use the notation $x := a$ to denote that x is defined as a. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, 2, \ldots, n\}$, whereas for $m, n \in \mathbb{Z}$ with $m < n$, $[m, n]$ denotes the set $\{m, m+1, \ldots, n\}$. Denote by $\mathbb{F}_P$ the finite field with P elements, where P is a prime, and by $\overline{\mathbb{F}}_P$ its algebraic closure. Finally, let log denote the logarithm to the base 2.

A sequence $(u_n)_{n\geq 0}$ is called *eventually periodic* if there exist integers $\ell \geq 0$ and $\tau \geq 1$ such that

$$u_{n+\tau} \;=\; u_n, \quad \forall\; n \geq \ell.$$

The smallest such τ is called the *period*, and ℓ is called the *pre-period*. Denote by $S = (s_j)_{j\geq 0}$ and $T = (t_j)_{j\geq 0}$, two periodic sequences in $\{0, 1, 2, \ldots, r-1\}$ with periods P and Q, respectively, such that $\gcd(P, Q) = 1$. Let $N = PQ$ be the common period of S and T. For a fixed integer τ, represent

$$S(r) \;=\; \sum_{j=0}^{\infty} s_j r^j, \quad T^{(\tau)}(r) \;=\; \sum_{j=0}^{\infty} t_{j+\tau} r^j$$

and let $S(r) - T^{(\tau)}(r) = \sum_{j=0}^{\infty} u_j r^j$ be the (eventually periodic) r-adic expansion. Let ℓ be the length of the pre-period, then the *arithmetic crosscorrelation* $C^{A}_{S,T}(\tau)$ of S and T is defined as

$$C^{A}_{S,T}(\tau) \;:=\; \sum_{j=\ell}^{\ell+N-1} \zeta_r^{u_j} \;=\; \sum_{j=0}^{r-1} N_j \zeta_r^j,$$

where N_j counts the number of times j appears in one full period of the r-adic expansion of $S(r) - T^{(\tau)}(r)$.

2.1 Characters

The *(multiplicative) character* χ of a finite abelian group G (written multiplicatively) of order $\text{ord}(G)$ with identity element 1_G is a multiplicative group homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. That is $\chi : G \to U$ such that for any $g_1, g_2 \in G$, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. It is easy to verify that for any $g \in G$, $\chi(1_G) = 1$ and $\chi(g)^{\text{ord}(G)} = 1$. So χ maps into the $\text{ord}(G)$-th roots of unity. Also, $\chi(g^{-1}) = \overline{\chi(g)}$ for every $g \in G$, where $\overline{z}$ denotes the complex conjugate of any $z \in \mathbb{C}$. The character that fixes all values to the identity $1 \in U$, i.e., $\chi(g) = 1$ for all $g \in G$ is called the *trivial* or the *principal* character of G and is denoted by $\chi_0(\cdot)$. All other characters of G are called *non-trivial* or *non-principal*. For a character χ define the associated *conjugate character* $\overline{\chi}(g) := \overline{\chi(g)} = \chi^{-1}(g)$ for all $g \in G$.

For a positive integer N, let $\mathbb{Z}_N^*$ denote the multiplicative group of integers modulo N that are coprime to N. Then, recall that a ***Dirichlet Character*** of modulus N is a group homomorphism $\chi : \mathbb{Z}_N^* \to \mathbb{C}^*$, i.e. for any $n_1, n_2 \in \mathbb{Z}_N^*$, $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$. That is $G = \mathbb{Z}_N^*$ with $\text{ord}(G) = \varphi(N)$ and U is cyclic group containing all the N-th roots of unity, where $\varphi(\cdot)$ denotes the Euler's totient function. Thus, a (Dirichlet) character is called *principal* if it takes the value 1 on every element of $\mathbb{Z}_N^*$. Characters are extended to functions $\chi : \mathbb{Z} \to \mathbb{C}$ by defining $\chi(a) = 0$ whenever $\gcd(a, N) \neq 1$.

2.2 Some Definitions and Results From Algebraic Number Theory

We start by describing the basic algebraic setup, the so-called *AKLB setup*, that we will be working on. Let A be an integral domain and K be its corresponding fraction field. Consider a finite separable extension L of K. Let B denote the integral closure of A in L. Next, recall that a commutative ring R is called *Noetherian* if it satisfies the *ascending chain condition (A. C. C.) on ideals* if every infinite increasing chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in R terminates, i.e., there is a positive integer m such that $I_k = I_m$ for all $k \geq m$. A *Dedekind domain* is then defined as an integral domain A that satisfies the following conditions.

(a) A is a Noetherian ring

(b) A is integrally closed

(c) Every non-zero prime ideal of A is maximal.

A principal ideal domain satisfies all the above three conditions and is therefore a Dedekind domain.

In our case, we will consider the Dedekind domain $\mathbb{Z}$ to be our base ring A. Then K denotes the fractional field of $\mathbb{Z}$, which is $\mathbb{Q}$. Consider L to be the number field of degree n. Then B will denote the *ring of integers* of L. In the AKLB setup, if A is a Dedekind domain, then so is B. Thus, the ring of integers of a number field is a Dedekind domain.

Consider the AKLB setup and let P be a prime ideal in A. Assume that PB (lifting P to B) factors in B into prime ideals as $PB = \prod_{i=1}^{g} P_i^{e_i}$, where e_i is called the *ramification index* of P_i over P (or over A). A prime ideal P in A *ramifies* in B (or in L) if $e_i > 1$ for at least one $i \in [g]$. The field A/P is a subfield of B/P_i for all i and B/P_i is a finite extension of A/P. The degree f_i of extension is called the *relative degree* or the *residue class degree* or the *inertial degree* of P_i over P (or over A). Also, B/PB is an n-dimensional vector space over A/P, where recall that n is the degree of extension of L/K.

Theorem 1 (Ram-rel Identity [3, Section 4.1.6])**.** $\sum_{i=1}^{g} e_i f_i = [B/PB : A/P] = n$.

Additionally, assume that L is also normal, and hence Galois. Denote the *Galois group* of L over K by $\mathrm{Gal}(L/K)$. Thus, in the factorization $PB = \prod_{i=1}^{g} P_i^{e_i}$ of the non-zero prime ideal P, the ramification indices e_i are same for all $i \in [g]$, as are their relative degrees f_i. That is the Ram-Rel identity simplifies to $efg = n$, where $e_i = e$, $f_i = f$ for all $i \in [g]$ and $n = [L : K] = |\mathrm{Gal}(L/K)|$.

2.3 The r-th Cyclotomic Ring of Integers

Let $r \geq 3$ be a positive integer and let $\zeta_r = e^{2\pi \mathrm{i}/r}$ denote a primitive r-th root of unity. The *r-th cyclotomic field* is the field extension

$$\mathbb{Q}(\zeta_r) \;:=\; \left\{ \sum_{k=0}^{\varphi(r)-1} a_k\, \zeta_r^k \;\middle|\; a_k \in \mathbb{Q} \right\},$$

where $\varphi(r)$ is the Euler's totient function. The minimal polynomial of ζ_r over $\mathbb{Q}$ is the *r-th cyclotomic polynomial*

$$\Phi_r(x) \;=\; \prod_{\substack{1 \leq k \leq r \\ \gcd(k,r)=1}} \left(x - \zeta_r^k\right) \;\in\; \mathbb{Z}[x],$$

which is monic, irreducible over $\mathbb{Q}$, and satisfies $\mathbb{Q}(\zeta_r) \cong \mathbb{Q}[x]/\langle \Phi_r(x) \rangle$ with $[\mathbb{Q}(\zeta_r) : \mathbb{Q}] = \varphi(r)$.

The *(cyclotomic) ring of integers* of $\mathbb{Q}(\zeta_r)$, denoted by $\mathbb{Z}[\zeta_r]$, consists of all elements of $\mathbb{Q}(\zeta_r)$ which are roots of some monic polynomial with coefficients in $\mathbb{Z}$ and as such

$$\mathbb{Z}[\zeta_r] \;=\; \left\{ \sum_{k=0}^{\varphi(r)-1} a_k\, \zeta_r^k \;\middle|\; a_k \in \mathbb{Z} \right\}.$$

It is a free $\mathbb{Z}$-module of rank $\varphi(r)$ with basis $\{1, \zeta_r, \ldots, \zeta_r^{\varphi(r)-1}\}$. For $\alpha \in \mathbb{Z}[\zeta_r]$, the *field norm* is

$$\mathcal{N}(\alpha) \;:=\; \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} \sigma(\alpha) \;\in\; \mathbb{Z},$$

and it is multiplicative, i.e., $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, where $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$ denotes the *Galois group* of $\mathbb{Q}(\zeta_r)$ over $\mathbb{Q}$, which consists of the $\varphi(r)$ field automorphisms $\sigma_k : \zeta_r \mapsto \zeta_r^k$ for $\gcd(k, r) = 1$. In particular $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q}) \cong \mathbb{Z}_r^\star$ (see [19, Proposition 13.2.1] or [37, Theorem 2.5]). The *canonical embedding* $\sigma : \mathbb{Q}(\zeta_r) \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the injective ring homomorphism given by

$$\sigma(x) \;:=\; (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)),$$

where r_1 denotes the number of *real embeddings*, i.e., $\sigma_i(\mathbb{Q}(\zeta_r)) \subset \mathbb{R}$ and r_2 denotes the number of *complex embeddings*. Next, recall the following few examples of norms in the r-th cyclotomic ring of integers.

- $r = 3$**:** In this case, $\zeta_3 = \omega$, which implies that the 3-rd cyclotomic ring of integers is $\mathbb{Z}[\omega]$, called the set of Eisenstein integers. Norm of an element $\alpha = a + \omega b \in \mathbb{Z}[\omega]$ is defined as $\mathcal{N}(\alpha) := a^2 - ab + b^2$.
- $r = 4$**:** In this case, $\zeta_4 = \mathrm{i}$, which implies that the 4-th cyclotomic ring of integers is $\mathbb{Z}[\mathrm{i}]$, called the set of Gaussian integers. Norm of an element $\alpha = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]$ is defined as $\mathcal{N}(\alpha) := a^2 + b^2$.

- $r = 5$**:** In this case, 5-th cyclotomic ring of integers is $\mathbb{Z}[\zeta_5]$. Norm of an element $\alpha = a + \zeta_5 b + \zeta_5^2 c + \zeta_5^3 d \in \mathbb{Z}[\zeta_5]$ is defined as $\mathcal{N}(\alpha) := u^2 - (uv + uw) + 3vw - (v^2 + w^2)$, where $u = a^2 + b^2 + c^2 + d^2,\ v = ab + bc + cd,\ w = ac + ad + bd$.
- $r = 6$**:** In this case, $\zeta_6 = -\omega^2$, which implies that the 6-th cyclotomic ring of integers is $\mathbb{Z}[-\omega^2] = \mathbb{Z}[\omega]$. Norm of an element $\alpha = a + \omega b \in \mathbb{Z}[\omega]$ is defined as $\mathcal{N}(\alpha) := a^2 - ab + b^2$.

The group of units $\mathbb{Z}[\zeta_r]^\star$ is characterised by Dirichlet's Unit Theorem [3, Theorem 6.2.1], which states the group B^* of units of a number field L is isomorphic to $G \times \mathbb{Z}^s$, i.e., $B^* \cong G \times \mathbb{Z}^s$, where G is the cyclic group consisting of all roots of unity in L, $s = r_1 + r_2 - 1$, r_1 denotes the number of real embeddings and r_2 denotes the number of complex embeddings of L, s is called the *unit rank* of the number field L. Also, an element $x \in B$ belongs to B^* if and only if $\mathcal{N}(x) = \pm 1$ [3, Lemma 6.1.1].

For $r \geq 3$, the number field $L = \mathbb{Q}(\zeta_r)$, $r_1 = 0$ and $r_2 = \varphi(r)/2$, so applying Dirichlet's Unit Theorem, we get

$$\mathbb{Z}[\zeta_r]^\star \ \cong\ \mu_r \times \mathbb{Z}^{\varphi(r)/2\,-\,1},$$

where μ_r is the finite group of roots of unity in $\mathbb{Z}[\zeta_r]$. In particular, for $r \in \{3, 4, 6\}$ the *free rank*, i.e., $s = \varphi(r)/2 - 1$ is zero and the unit group is finite. Notice that, for $r = 4$ we have $\mathbb{Z}[\mathrm{i}]^\star = \{\pm 1, \pm \mathrm{i}\}$, for $r = 3, 6$ we get $\mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$. Whereas for $r \geq 5$ and $r \neq 6$, there exist infinitely many units. Two elements $\alpha, \beta \in \mathbb{Z}[\zeta_r]$ are called *associates* if they differ by a unit factor, i.e., there exists a $u \in \mathbb{Z}[\zeta_r]^*$ such that $\alpha = u\beta$. We write $\alpha \sim \beta$ to denote that α and β are associates of each other.

2.4 r-th order Residue Symbol

Let $P \in \mathbb{Z}$ be a prime and $d \geq 0$ be the largest integer such that $P^d \mid r$. Suppose $h = \varphi(P^d)$ and let $f \geq 1$ denote the multiplicative order of p modulo r/P^d, i.e., $P^f \equiv 1 \pmod{r/P^d}$. Since, $\mathbb{Q}(\zeta_r)$ is a $\varphi(r)$ degree Galois extension of $\mathbb{Q}$, we have $\langle P \rangle = \mathfrak{P}_1^h \cdots \mathfrak{P}_g^h$ and $f = [\mathbb{Z}[\zeta_r]/\mathfrak{P}_i : \mathbb{Z}/\langle P \rangle]$ for all $i \in [g]$. Then from the Ram-Rel identity for Galois extensions, we have $hfg = \varphi(r)$ which implies that $g = \varphi(r)/(hf)$.

Take a prime $P \in \mathbb{Z}$ such that $P \equiv 1 \mod r$. Then, $d = 0$ which implies that $h = 1$ and by the choice of P, we have $P \equiv 1 \pmod{r/P^0} \equiv 1 \pmod{r}$, hence $f = 1$. Together they imply that $g = \varphi(r)$. Thus, $\langle P \rangle = \mathfrak{P}_1 \cdots \mathfrak{P}_{\varphi(r)}$ and these prime ideals in $\mathbb{Z}[\zeta_r]$ are called *conjugates* of one another. Take $\langle \pi \rangle = \mathfrak{P}_i$ for any $i \in [g]$. Then $\mathcal{N}(\pi) = P$. Consider the map

$$\left(\tfrac{\cdot}{\pi}\right) : \mathbb{Z}[\zeta_r] \longrightarrow \{\zeta_r^0, \ldots, \zeta_r^{r-1}\},$$

defined by

$$\left(\tfrac{Z}{\pi}\right) \ \equiv\ Z^{\frac{P-1}{r}} \pmod{\pi},$$

This function, denoted by $\chi_\pi(\cdot)$, is called the *r-th order residue symbol*. By convention, if $\pi \mid Z$, then $\left(\frac{Z}{\pi}\right) = 0$.

The restriction of χ_π to $\mathbb{Z}$ defines a Dirichlet character of order r. We can define a map by,

$$\phi : \{\zeta_r^0, \ldots, \zeta_r^{r-1}\} \ \longrightarrow\ \{0, \ldots, r-1\}, \quad \zeta_r^k \ \longmapsto\ k \pmod{r}$$

Define the *r-th order character sequences* in modulus P by $S = (s_j)_{j \geq 0}$ such that each $s_j = \phi(\chi_\pi(x_j))$, for some $x_j \in \mathbb{F}_P$.

To use the division algorithm on the number field $\mathbb{Q}(\zeta_r)$, we first need to show that $\mathbb{Q}(\zeta_r)$ is indeed *norm-Euclidean*. Recall that an algebraic number field K is called *norm-Euclidean* if

the absolute value of the norm is an Euclidean function, where recall that f is an *Euclidean function* on a ring R, if $f : R \to \mathbb{R}_{\geq 0}$ and satisfies the following two conditions.

(a) $f(\alpha) = 0$ if and only if $\alpha = 0$.

(b) For all $\alpha, \beta \in R \setminus \{0\}$, there exists a $\gamma \in R$ such that $f(\alpha - \beta\gamma) < f(\beta)$.

3 r-th order Character Bounds

Let π and ρ be distinct cyclotomic primes with norms $\mathcal{N}(\pi) = P$ and $\mathcal{N}(\rho) = Q$, where $P < Q$ along with $P \equiv Q \equiv 1 \mod r$. Denote by χ_π and χ_ρ the multiplicative characters of order r modulo π and ρ, respectively. Define the r-th order character sequences $(s_j)_{j\geq 0}$ and $(t_j)_{j\geq 0}$ by

$$s_j \;=\; \phi(\chi_\pi(f(j))) \quad \text{and} \quad t_j \;=\; \phi(\chi_\rho(g(j))),$$

where $f \in \mathbb{F}_P[x],\ g \in \mathbb{F}_Q[x]$.

We first recall a version of the Weil bound [38] for multiplicative characters, which is due to Wan [36] and is reproduced next.

Theorem 2 (Weil bound [36, Corollary 2.3])**.** *Let $f_1(x), \ldots, f_n(x)$ be n monic pairwise prime polynomials in $\mathbb{F}_P[x]$ whose largest square-free divisors have degree d_i for $1 \leq i \leq n$. Let $\chi_1, \ldots, \chi_n$ be nontrivial multiplicative characters of the finite field $\mathbb{F}_P$. Assume that for some $1 \leq i \leq n$, the polynomial $f_i(x)$ is not of the form $g(x)^{\mathrm{ord}(\chi_i)}$ in $\mathbb{F}_P[x]$, where $\mathrm{ord}(\chi_i)$ denotes the order of χ_i. Then we have the estimate*

$$\left| \sum_{x \in \mathbb{F}_P} \chi_1\big(f_1(x)\big) \cdots \chi_n\big(f_n(x)\big) \right| \;\leq\; \left(\sum_{i=1}^{n} d_i - 1 \right) \sqrt{P}.$$

Following the arguments of [36] and [17], we prove the following lemma, which is a version of Theorem 2 where for any $k \geq 0$, a square-free degree d monic polynomial f, we define $f_i(x) := f(x - i)$ with f_i, f_j $(i \neq j)$ co-prime in $\mathbb{F}_P$ and $i, j \in A \subseteq \{0, 1, \ldots, k\}$.

Lemma 1. *Let $P \equiv 1 \pmod r$ be a prime, and let $f \in \mathbb{F}_P[x]$ be a square-free polynomial of positive degree d such that, for every pair of distinct integers $j, j' \in \{0, 1, \ldots, k\}$, the translates $f(x - j)$ and $f(x - j')$ are coprime in $\mathbb{F}_P[x]$ (equivalently, $f(x)$ and $f(x + t)$ share no common root in algebraic closure $\overline{\mathbb{F}}_P$ of $\mathbb{F}_P$, for any $0 < |t| \leq k$). Let χ_π be a multiplicative character modulo P of order r. Then for any nonempty subset $A \subseteq \{0, 1, \ldots, k\}$ and any exponents $a_j \in \{1, \ldots, r - 1\}$ for $j \in A$, we have*

$$\left| \sum_{\ell=0}^{P-1} \prod_{j \in A} \chi_\pi^{a_j}\big(f(\ell - j)\big) \right| \;\leq\; \big((k+1)d - 1\big)\sqrt{P} \;=\; O(kd\sqrt{P}).$$

Proof of Lemma 1. For each $j \in A$, define the shifted polynomial

$$f_j(x) \;:=\; f(x - j) \in \mathbb{F}_P[x].$$

Now f is square-free, which implies that the roots of $f_j(x)$ are also distinct as they are the roots of f shifted by j. Substituting $x = \ell$ in the sum, we may rewrite

$$S \;:=\; \sum_{\ell=0}^{P-1} \prod_{j \in A} \chi_\pi^{a_j}\big(f(\ell - j)\big) \;=\; \sum_{x \in \mathbb{F}_P} \prod_{j \in A} \chi_j\big(f_j(x)\big),$$

where we set $\chi_j := \chi_\pi^{a_j}$ for each $j \in A$. The proof then proceeds via the following steps.

Step 1: Each χ_j is a nontrivial multiplicative character. Since χ_π is a multiplicative character, then for $x, y \in \mathbb{F}_P^*$ we have $\chi_\pi(xy) = \chi_\pi(x)\chi_\pi(y)$. Hence,

$$\chi_j(xy) \;=\; \big(\chi_\pi(xy)\big)^{a_j} \;=\; \big(\chi_\pi(x)\big)^{a_j}\big(\chi_\pi(y)\big)^{a_j} \;=\; \chi_j(x)\chi_j(y).$$

Thus, $\chi_j = \chi_\pi^{a_j}$ is again a multiplicative character modulo P. Moreover, since χ_π has order exactly r in the character group, the power $\chi_\pi^{a_j}$ has order

$$\operatorname{ord}(\chi_j) = \frac{r}{\gcd(r, a_j)}.$$

As $1 \le a_j \le r-1$, we have $\gcd(r, a_j) < r$, so $\operatorname{ord}(\chi_j) \ge 2$. In particular, χ_j is nontrivial.

Step 2: The f_j's ($j \in A$) are pairwise coprime. Since $A \subseteq \{0, 1, \ldots, k\}$, the shifts $j, j' \in A$ with $j \ne j'$ are distinct elements of $\{0, \ldots, k\}$. By hypothesis, $f(x-j)$ and $f(x-j')$ are coprime in $\mathbb{F}_P[x]$ for any such pair. Therefore, f_j and $f_{j'}$ are also pairwise coprime.

Step 3: The largest square-free divisor of each f_j has degree d. By Step 1's analogue for polynomials: since f is square-free by hypothesis, so is each translate $f_j(x) = f(x-j)$. *Hence f_j is equal to its own largest square-free divisor, which has degree $d_j = \deg(f_j) = d \;\forall\; j \in A$.*

Step 4: The non-degeneracy hypothesis of the Weil bound holds. We must check that for some (in fact every) $i \in A$, the polynomial f_i is not of the form $g(x)^{\operatorname{ord}(\chi_i)}$ for any $g \in \mathbb{F}_P[x]$. Since f_i is square-free of degree $d \ge 1$ and $\operatorname{ord}(\chi_i) \ge 2$ by Step 1, therefore f_i cannot be a perfect $\operatorname{ord}(\chi_i)$-th power of any nonconstant polynomial (a nontrivial power would force repeated irreducible factors), nor can it be a power of a constant (since $\deg f_i = d \ge 1 > 0$). Hence, the hypothesis of Theorem 2 holds for every $i \in A$.

Step 5: Apply the Weil bound. All hypotheses of Theorem 2 are now verified with $n = |A|$, $Q = P$, characters $\{\chi_j\}_{j\in A}$, and polynomials $\{f_j\}_{j\in A}$ each having largest square-free divisor of degree $d_j = d$. Therefore

$$|S| \;\le\; \left(\sum_{j\in A} d_j - 1\right)\sqrt{P} \;=\; \big(|A|\,d - 1\big)\sqrt{P}.$$

Step 6: Bound $|A|$ and conclude. Since $A \subseteq \{0, 1, \ldots, k\}$, we have $|A| \le k+1$, and so

$$|S| \;\le\; \big((k+1)d - 1\big)\sqrt{P}.$$

As $(k+1)d - 1 \le (k+1)d \le 2kd$ for all $k \ge 1$, this yields

$$|S| \;\le\; 2kd\sqrt{P}.$$

That is,

$$\left|\sum_{\ell=0}^{P-1}\prod_{j\in A}\chi_\pi^{a_j}\big(f(\ell - j)\big)\right| \;=\; O(kd\sqrt{P}),$$

as claimed.

□

4 Arithmetic Crosscorrelation of Non-binary Sequences

his section gives the main result of this paper, whereby we show that the arithmetic crosscorrelation of sequences generated from the r-th residue symbol does not deviate too much from uniform. The proof technique used is similar to that of Yan and Ke [41].

We first consider $k+1$ length sequences $(s_{\ell-k},\ldots,s_\ell)$ and $(t_{\ell-k},\ldots,t_\ell)$ generated by two characters $\chi_\pi(\cdot)$ and $\chi_\rho(\cdot)$ corresponding to integer primes P and Q, respectively such that $P \equiv Q \equiv 1 \pmod r$. In particular, let $s_j = \phi(\chi_\pi(f(j)))$ and $t_{j'} = \phi(\chi_\rho(g(j')))$ for some square-free polynomials f and g of degree d satisfying the conditions of Lemma 1, where $j \in \mathbb{F}_P$ and $j' \in \mathbb{F}_Q$. Notice that by varying the shift ℓ and considering different monic square-free polynomials f and g, considering the squences $(s_{\ell-k},\ldots,s_\ell)$ and $(t_{\ell-k},\ldots,t_\ell)$ is akin to considering all possible $k+1$ length squences generated by the characters $\chi_\pi(\cdot)$ and $\chi_\rho(\cdot)$, respectively. Then in order to derive an upper bound on the arithmetic crosscorrelation between the sequence $(s_j)_{j=\ell-k}^{\ell}$ and $(t_\ell)_{j=\ell-k}^{\ell}$, first consider the concatenated squence $(s_{\ell-k},\ldots,s_\ell,t_{\ell-k},\ldots,t_\ell)$ of length $2k+2$. We then count the number of times a particular pattern of $2k+2$ length sequence is generated by this concatenated sequence. This is achived by first considering an arbitrary r-ary sequence of length $2k+2$, i.e., $\vec{e} = (e_0,\ldots,e_k,e_{k+1},\ldots,e_{2k+1}) \in \{0,1,\ldots,r-1\}^{2k+2}$. Then we divide the sequence $\vec{e}$ in two parts $(e_0,\ldots,e_k)$ and $(e_{k+1},\ldots,e_{2k+1})$, and check if both $s_{l-k+j} = e_j$ and $t_{l-k+j} = e_{k+1+j}$ for all $j \in [0,k]$ (see Figure 1). This is summarized in Lemma 2, where we count the number of such sequences $\vec{e}$ which is equal to the $(s_{\ell-k},\ldots,s_\ell,t_{\ell-k},\ldots,t_\ell)$, where ℓ varies from 0 to $PQ-1$ and PQ is the period of the sequence $(s_{\ell-k},\ldots,s_\ell,t_{\ell-k},\ldots,t_\ell)$.

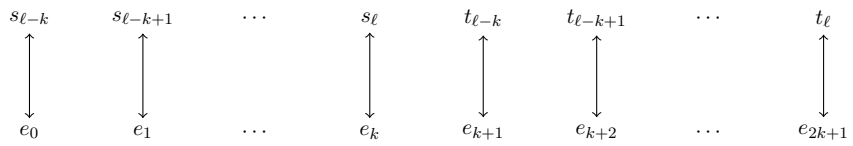

Figure 1: A pictorial representation of the proof idea used in Lemma 2.

Lemma 2. *Let P and Q be distinct odd primes such that $P \equiv Q \equiv 1 \pmod r$ with $P < Q$ and let $f \in \mathbb{F}_P[x]$ and $g \in \mathbb{F}_Q[x]$ be polynomials of degree d each satisfying the hypothesis of Lemma 1. Define the sequences*

$$s_\ell \;=\; \phi(\chi_\pi(f(\ell))), \quad t_\ell \;=\; \phi(\chi_\rho(g(\ell)))$$

of periods P and Q, and assume that both χ_π and χ_ρ are mulltiplicatie characters of order r modulo P and Q, respectively. For any $k \geq 0$ and any pattern $\vec{e} \in \{0,\ldots,r-1\}^{2k+2}$, define the number

$$\Sigma_k(\vec{e}) \;=\; \#\{\ell = 0,1,\ldots,PQ-1 : (s_{\ell-k},\ldots,s_\ell,t_{\ell-k},\ldots,t_\ell) = \vec{e}\}.$$

Then

$$\Sigma_k(\vec{e}) \;=\; \frac{PQ}{r^{2k+2}} + O\left(r^{-k}kdP^{1/2}Q\right)$$

for $k \leq \min\left\{\frac{\log P}{2\log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}\right\}$, and $2^{d-\lfloor 2\log r\rfloor} < Q$.

In particular, if $d = 1$ (classical rth order character sequences), then we get

$$\Sigma_k(\vec{e}) = \frac{PQ}{r^{2k+2}} + O\left(r^{-k}kP^{1/2}Q\right).$$

Proof of Lemma 2. Write $\vec{e} = (e_0, \ldots, e_{2k+1})$. For integers $\ell, j \leq k$, assume that $P \nmid f(\ell - j)$ and $Q \nmid g(\ell - j)$. We define the following indicator function

$$\mathbb{1}_{\phi(\chi_\pi(x))=h} \;=\; \frac{1}{r}\sum_{m=0}^{r-1} \zeta_r^{-mh}\chi_\pi(x)^m, \tag{1}$$

where note that when $\chi_\pi(x) = \zeta_r^h$, then the value of the expression is 1 and when $\chi_\pi(x) \neq \zeta_r^h$, the value of the expression is equal to

$$\frac{1}{r}\sum_{m=0}^{r-1}(\zeta_r^{-h}\chi_\pi(x))^m \;=\; \frac{(\zeta_r^{-h}\chi_\pi(x))^r - 1}{r(\zeta_r^{-h}\chi_\pi(x) - 1)} \;=\; \frac{1-1}{r(\zeta_r^{-h}\chi_\pi(x) - 1)} = 0.$$

Similarly, for any $y \in \mathbb{Z}_Q^\star$ we have

$$\mathbb{1}_{\phi(\chi_\rho(y))=h'} \;=\; \frac{1}{r}\sum_{m=0}^{r-1} \zeta_r^{-mh'}\chi_\rho(x)^m. \tag{2}$$

Then $\Sigma_k(\vec{e})$ can be written as

$$\Sigma_k(\vec{e}) \;=\; \left|\sum_{\ell=0}^{PQ-1}\prod_{j=0}^{k} \mathbb{1}_{s_{\ell-j}=e_j}\cdot\mathbb{1}_{t_{\ell-j}=e_{k+1+j}}\right| + O(kd(P+Q)),$$

where the error $O(kd(P+Q))$ arises from those indices ℓ for which there exists some $j \in \{0, 1, \ldots, k\}$ such that $\gcd(f^{a_j}(\ell - j), P) > 1$ or $\gcd(g^{b_j}(\ell - j), Q) > 1$. Moreover, using (1) and (2), we can write

$$\begin{aligned}
A \;&=\; \sum_{\ell=0}^{PQ-1}\prod_{j=0}^{k} \mathbb{1}_{s_{\ell-j}=e_j}\cdot\mathbb{1}_{t_{\ell-j}=e_{k+1+j}} \\
&=\; \frac{1}{r^{2k+2}}\sum_{\ell=0}^{PQ-1}\prod_{j=0}^{k}\left(\sum_{a_j=0}^{r-1}\zeta_r^{-a_je_j}\,\chi_\pi(f(\ell-j))^{a_j}\right)\left(\sum_{b_j=0}^{r-1}\zeta_r^{-b_je_{k+1+j}}\,\chi_\rho(g(\ell-j))^{b_j}\right) \\
&=\; \frac{1}{r^{2k+2}}\sum_{\vec{a},\vec{b}\in\{0,\ldots,r-1\}^{k+1}}\left(\prod_{j=0}^{k}\zeta_r^{-a_je_j}\right)\left(\prod_{j=0}^{k}\zeta_r^{-b_je_{k+1+j}}\right)S(\vec{a},\vec{b}) \\
&=\; \frac{1}{r^{2k+2}}\left[S(\vec{0},\vec{0}) + \sum_{\substack{\vec{a},\vec{b}\in\{0,\ldots,r-1\}^{k+1}\\ \text{s.t. } \vec{a}\neq\vec{0}\neq\vec{b}}}\left(\prod_{j=0}^{k}\zeta_r^{-a_je_j}\right)\left(\prod_{j=0}^{k}\zeta_r^{-b_je_{k+1+j}}\right)S(\vec{a},\vec{b})\right],
\end{aligned}$$

which implies that

$$A - \frac{S(\vec{0},\vec{0})}{r^{2k+2}} \;=\; \frac{1}{r^{2k+2}} \sum_{\substack{\vec{a},\vec{b}\in\{0,\ldots,r-1\}^{k+1}\\ \text{s.t. } \vec{a}\neq\vec{0}\neq\vec{b}}} \left(\prod_{j=0}^{k} \zeta_r^{-a_j e_j}\right)\left(\prod_{j=0}^{k} \zeta_r^{-b_j e_{k+1+j}}\right) S(\vec{a},\vec{b})$$

$$\implies \left|A - \frac{S(\vec{0},\vec{0})}{r^{2k+2}}\right| \;\leq\; \left|\frac{1}{r^{2k+2}} \sum_{\substack{\vec{a},\vec{b}\in\{0,\ldots,r-1\}^{k+1}\\ \text{s.t. } \vec{a}\neq\vec{0}\neq\vec{b}}} \left(\prod_{j=0}^{k} \zeta_r^{-a_j e_j}\right)\left(\prod_{j=0}^{k} \zeta_r^{-b_j e_{k+1+j}}\right) S(\vec{a},\vec{b})\right|$$

$$\implies \left|A - \frac{S(\vec{0},\vec{0})}{r^{2k+2}}\right| \;\leq\; \frac{1}{r^{2k+2}} \sum_{\substack{\vec{a},\vec{b}\in\{0,\ldots,r-1\}^{k+1}\\ \text{s.t. } \vec{a}\neq\vec{0}\neq\vec{b}}} \left|S(\vec{a},\vec{b})\right|,$$

where

$$S(\vec{a},\vec{b}) \;=\; \sum_{\ell=0}^{PQ-1} \left(\prod_{j=0}^{k} \chi_\pi(f(\ell-j))^{a_j}\right)\left(\prod_{j=0}^{k} \chi_\rho(g(\ell-j))^{b_j}\right)$$

such that $\vec{a} = (a_0,\ldots,a_k)$, and $\vec{b} = (b_0,\ldots,b_k)$. Note that, $\Sigma_k(\vec{e}) = |A| + O(kd(P+Q))$.

Set $U = \{j :\; a_j \neq 0\}$ and $V = \{j :\; b_j \neq 0\}$. Now, depending on whether V and U are empty or not, we have the following 4 cases.

Case 1: $U = V = \emptyset$**.** That is for all j, we have $a_j = b_j = 0$, which implies that $\chi_\pi^{a_j}(f(\ell-j)) = \chi_\rho^{b_j}(g(\ell-j)) = 1$ for all j. Therefore,

$$S(\vec{0},\vec{0}) \;=\; \sum_{i=0}^{PQ-1} 1 \;=\; PQ.$$

Therefore, its contribution to $\Sigma_k(\vec{e})$ is $\frac{1}{r^{2k+2}} \cdot PQ$.

Case 2: $U \neq \emptyset, V = \emptyset$**.** Since $b_j \equiv 0 \;\forall\; j$, therefore $\chi_\rho^{b_j}(g(\ell-j)) = 1$ for all j. Now, by the Chinese Remainder Theorem ($\gcd(P,Q) = 1$), the sum can be factored as

$$S(\vec{a},\vec{0}) \;=\; Q \cdot \sum_{\ell=0}^{P-1} \prod_{j=0}^{k} \chi_\pi(f(\ell-j))^{a_j} \;=\; Q \cdot \sum_{\ell=0}^{P-1} \chi_\pi^{a_j}\left(\prod_{j\in U} f(\ell-j)\right),$$

where the product inside χ_π runs only over $j \in U$, since for $j \notin U$ $\chi_\pi^{a_j} = \chi_\pi^0 = 1$. Applying the Lemma 1 we get

$$\left|\sum_{l=0}^{P-1} \chi_\pi^{a_j}\left(\prod_{j\in U} f(l-j)\right)\right| \;\leq\; \big((k+1)d-1\big)\, P^{1/2} \;=\; O(kd\, P^{1/2}).$$

Therefore,

$$|S(\vec{a},\vec{0})| \;=\; O(kd\, QP^{1/2}).$$

The number of tuples $\vec{a} \in \{0,\ldots,r-1\}^{k+1}$ with $U \neq \emptyset$ is $r^{k+1}-1$, while $\vec{b} = \vec{0}$ is a fixed tuple. Then, the fraction of tuples $(\vec{a},\vec{b})$ such that $\vec{a} \neq \vec{0}$ and $\vec{b} = \vec{0}$ is $\frac{r^{k+1}-1}{r^{2k+2}}$. Therefore the total contribution of Case 2 to $\Sigma_k(\vec{e})$ is bounded by

$$\frac{(r^{k+1}-1)\cdot O(kd\, QP^{1/2})}{r^{2k+2}} \;\leq\; \frac{O(kd\, QP^{1/2})}{r^{k+1}} \;=\; O(r^{-k}\, kd\, P^{1/2}Q).$$

Case 3: $V \neq \emptyset,\ U = \emptyset$**.** By the same argument as in Case 2 with the roles of P and Q interchanged, we get

$$|S(\vec{0}, \vec{b})| \ = \ \left| P \cdot \sum_{\ell=0}^{Q-1} \chi_\rho^{b_j} \left(\prod_{j \in V} g(\ell - j) \right) \right| \ = \ O(kd\, PQ^{1/2}).$$

The total contribution of Case 3 to $\Sigma_k(\vec{e})$ is therefore bounded by

$$\frac{(r^{k+1} - 1) \cdot O(kd\, PQ^{1/2})}{r^{2k+2}} \ = \ O(r^{-k}\, kd\, PQ^{1/2}).$$

Case 4: $U \neq \emptyset,\ V \neq \emptyset$**.** Since U indexes characters modulo P, V indexes characters modulo Q, and $\gcd(P, Q) = 1$, then applying the Chinese Remainder Theorem one can factorize $S(\vec{a}, \vec{b})$ as follows.

$$S(\vec{a}, \vec{b}) \ = \ \left(\sum_{\ell=0}^{P-1} \prod_{j \in U} \chi_\pi^{a_j}(f(\ell - j)) \right) \cdot \left(\sum_{\ell=0}^{Q-1} \prod_{j \in V} \chi_\rho^{b_j}(g(\ell - j)) \right).$$

Then, applying Lemma 1 to each factor independently, we get

$$|S(\vec{a}, \vec{b})| \ = \ O(k^2 d^2\, (PQ)^{1/2}).$$

The number of pairs $(\vec{a}, \vec{b})$ with $U \neq \emptyset$ and $V \neq \emptyset$ is at most $(r^{k+1} - 1)^2 < r^{2k+2}$ and the fraction of such pairs is $\frac{(r^{k+1}-1)^2}{r^{2k+2}}$. Then the total contribution of Case 4 to $\Sigma_k(\vec{e})$ is bounded by

$$O\left(\frac{(r^{k+1})^2 \cdot k^2 d^2 (PQ)^{1/2}}{r^{2k+2}} \right) \ = \ O(k^2 d^2 (PQ)^{1/2}).$$

Summing the contributions from Cases 1 to 4, we get

$$\begin{aligned} \left| A - \frac{PQ}{r^{2k+2}} \right| \ &= \ O\left(r^{-k} kd\, P^{1/2} Q \right) + O\left(r^{-k} kd PQ^{1/2} \right) + O\left(k^2 d^2 (PQ)^{1/2} \right) \\ \implies \quad |A| \ &= \ \frac{PQ}{r^{2k+2}} + O\left(r^{-k} kd\, P^{1/2} Q \right) + O\left(r^{-k} kd PQ^{1/2} \right) + O\left(k^2 d^2 (PQ)^{1/2} \right), \end{aligned}$$

where the second implication follows from the definition of $O(\cdot)$. Hence, we get the following

$$\Sigma_k(\vec{e}) \ = \ \frac{PQ}{r^{2k+2}} + O\left(r^{-k} kd\, P^{1/2} Q \right) + O\left(r^{-k} kd PQ^{1/2} \right) + O\left(k^2 d^2 (PQ)^{1/2} \right) + O(kd(P+Q)),$$

where recall that the $O(kd(P+Q))$-term arises from those ℓ indices for which there exists some $j \in \{0, 1, \ldots, k\}$ such that $\gcd(f^{a_j}(\ell - j), P) > 1$ or $\gcd(g^{b_j}(\ell - j), Q) > 1$.

Next, we identify the range of k for which the dominant error term is $r^{-k} kd P^{1/2} Q$, where we assume without loss of generality that $P < Q$. The four error terms are

$$E_1 \ = \ r^{-k} kd\, P^{1/2} Q, \quad E_2 \ = \ r^{-k} kd\, PQ^{1/2}, \quad E_3 \ = \ k^2 d^2 (PQ)^{1/2}, \quad E_4 \ = \ kd(P+Q).$$

This gives rise to the following three cases.

Case 1: E_1 dominates E_2. Since $P < Q$, we have $Q^{1/2} > P^{1/2}$. So

$$\frac{E_1}{E_2} \;=\; \frac{Q^{1/2}}{P^{1/2}} \;>\; 1,$$

and $E_2 = O(E_1)$ always holds when $P < Q$.

Case 2: E_1 dominates E_4. The condition $E_1 \geq E_4$ implies that

$$r^{-k}kd\,P^{1/2}Q \;\geq\; kd(P+Q) \quad \Rightarrow \quad (r^{-k}\sqrt{P}-1)Q \;\geq\; P,$$

which implies that $r^{-k}P^{1/2} \geq 1$, or equivalently

$$k \;\leq\; \frac{\log P}{2\log r}.$$

Case 3: E_1 dominates E_3. The condition $E_1 \geq E_3$ requires

$$r^{-k}kd\,P^{1/2}Q \;\geq\; k^2d^2(PQ)^{1/2},$$

which implies that $r^{-k}Q^{1/2} \geq kd$, or equivalently

$$k\log r \;\leq\; \tfrac{1}{2}\log Q - \log(kd).$$

Since $k \leq \frac{\log P}{2\log r}$ (from Case 2), we have $\log k \leq \log\log P - \log(2\log r)$ and from $2^{d-\lfloor 2\log r\rfloor} < Q$ we have $d \leq \log(Qr^2)$. This condition is therefore satisfied whenever

$$k \;\leq\; \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}.$$

Combining all the above three conditions, we get that E_1 dominates all other error terms provided

$$k \;\leq\; \min\left\{\frac{\log P}{2\log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}\right\}.$$

In particular, if $d = 1$ (classical r-th order character sequences), then we get

$$\Sigma_k(\vec{e}) = \frac{PQ}{r^{2k+2}} + O\left(r^{-k}kP^{1/2}Q\right).$$

□

The next lemma studies the boundary case, i.e., when $K = \min\left\{\frac{\log P}{2\log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}\right\}$. In particular, we show that under the condition that $r \leq (\log P)^2$ and $Q \geq 2^8$, $r^{-K} \leq r^{-\lfloor K\rfloor} = O(P^{-\frac{1}{2}}(\log P)^2)$. This implies that the error term in Lemma 2 becomes equal to $O(r^{-\lfloor K\rfloor} \cdot KdP^{1/2}Q) = O((\log P)^2 \cdot KdQ) = O\left(\frac{(\log P)^3 d\,Q}{\log r}\right)$, since $K = \min\left\{\frac{\log P}{2\log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}\right\} \leq \frac{\log P}{2\log r}$.

Lemma 3. *Let P and Q $(\geq 2^8)$ be distinct odd primes with $2 < P < Q$, with $r \leq (\log P)^2$*

$$K \;=\; \min\left\{\frac{\log P}{2\log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}\right\},$$

and let $M = \lfloor K\rfloor$, then $r^{-M} = O(P^{-\frac{1}{2}}(\log P)^2)$.

Proof of Lemma 3. Since $M = \lfloor K \rfloor$, we have $K - 1 < M \leq K$, which implies that $r^{-K} \leq r^{-M} < r^{-K+1}$. Let $A = \frac{\log P}{2 \log r}$ and $B = \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r}$.

Case 1: If $A \leq B$, then $K = A$. Hence, $r^{-K} = r^{-A} = P^{-\frac{1}{2}}$.

Case 2. If $B < A$, let $x = \log Q$, $y = \log P$. Then $B < A$ implies

$$\begin{aligned} \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r} &< \frac{\log P}{2\log r} \\ \implies \log Q - \log P &< 2(\log\log Q + \log\log P) \\ \implies x - y &< 2(\log x + \log y) \end{aligned}$$

Since for any $x \geq 8$, $5\log x < 2x$ and for any $y > 0$, $\log y < y$, we have

$$\begin{aligned} x &< y + 2(\log x + \log y) < y + 2\log y + \frac{4x}{5} \\ \implies x &< 15y \\ \implies \log Q &= O(\log P). \end{aligned}$$

Then we get

$$\begin{aligned} r^{-K} = r^{-B} &= Q^{-\frac{1}{2}} \log Q \log P \\ &= P^{-\frac{1}{2}} \left(\frac{P}{Q}\right)^{\frac{1}{2}} \log Q \log P \\ &< P^{-\frac{1}{2}} \log Q \log P = O\left(P^{-\frac{1}{2}} (\log P)^2\right). \end{aligned}$$

From both cases, we obtain

$$r^{-K} = O\left(P^{-\frac{1}{2}} (\log P)^2\right).$$

Since $r \leq (\log P)^2$, it follows that

$$r^{-M} \leq r^{-K+1} = r\, r^{-K} \leq r O\left(P^{-\frac{1}{2}} (\log P)^2\right) = O\left((\log P)^2 P^{-\frac{1}{2}} (\log P)^2\right).$$

As $(\log P)^2$ is negligible compared to $P^{\frac{1}{2}}(\log P)^2$, we conclude that

$$r^{-M} = O\left(P^{-\frac{1}{2}} (\log P)^2\right).$$

□

Finally, using the results of Lemma 2 and 3, we derive an upper bound on the norm of the arithmetic crosscorrelation of sequences generated from the generalized r-th order residue symbols. In particular, we show that if the degree d and $\varphi(r)$ are small, then the norm of arithmetic crosscorreplation is $O(\mathsf{poly}(P^{1/2}Q(\log P)^2))$, where poly denotes some polynomial of degree $\varphi(r)$.

Theorem 3. *Let $S = (s_\ell)_{\ell \geq 0}$ and $T = (t_\ell)_{\ell \geq 0}$ be two sequences generated from the generalized r-th order residue symbols with coprime periods P and Q, where P and Q satisfy the conditions of Lemma 2 and 3. Then, for $Q \geq 2^8$ and $2^{d - \lfloor 2\log r \rfloor} < Q$, the arithmetic crosscorreltaion $C^A_{S,T}$ satisfies*

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = O\left(\left(\varphi(r) d P^{1/2} Q (\log P)^2\right)^{\varphi(r)}\right),$$

for $0 \le \tau < PQ$, *where* $\varphi(\cdot)$ *is the* Euler's Totient function. *In particular, for* $r \in \{3, 4, 6\}$ *we have*

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; O\left(4d^2PQ^2(\log P)^4\right),$$

and for $r = 5$ *we have*

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; O\left(256d^4P^2Q^4(\log P)^8\right).$$

Proof of Theorem 3. By the definition of arithmetic crosscorrelation, we have

$$C^A_{S,T}(\tau) \;=\; \sum_{j=0}^{r-1} N_j \zeta_r^j$$

From the work of Yan and Ke [41, Theorem 3], it follows that the arithmetic crosscorrelation of two non-binary sequences with coprime periods is independent of the shift τ. Therefore, we may set $\tau = 0$. Furthermore, without loss of generality, we can assume $S(r) \ge T^{(0)}(r)$, where

$$S(r) \;=\; \sum_{\ell=0}^{PQ-1} s_\ell r^\ell, \quad T^{(0)}(r) \;=\; \sum_{\ell=0}^{PQ-1} t_\ell r^\ell.$$

Write

$$S(r) - T^{(0)}(r) \;=\; \sum_{\ell=0}^{PQ-1} (s_\ell - t_\ell) r^\ell \;=\; \sum_{\ell=0}^{PQ-1} w_\ell r^\ell$$

with $w_\ell \in \{0, 1, \ldots, r-1\}$ for all $\ell \in [0, PQ-1]$. Since the r-adic representation is unique, therefore, for a given $S(r)$ and $T^{(0)}(r)$ the values of w_ℓ's are unique. Hence, in order to compute $\mathcal{N}(C^A_{S,T})$ it is necessary to estimate the number of indices ℓ for which $w_\ell = 1$. The computations for the other cases, i.e., when $w_\ell \in \{0, 2, \ldots, r-1\}$ are similar.

Assume there exist integers $n \ge k \ge 1$ and $a \in \{0, 1, \ldots, r-1\}$ such that

$$\begin{pmatrix} s_{n-k} & s_{n-k+1} & \cdots & s_{n-1} & s_n \\ t_{n-k} & t_{n-k+1} & \cdots & t_{n-1} & t_n \end{pmatrix} \;=\; \begin{pmatrix} a & x_1 & \cdots & x_{k-1} & y \\ b & x_1 & \cdots & x_{k-1} & z \end{pmatrix}, \tag{3}$$

for some $y, z \in \{0, 1, \ldots, r-1\}$. That is, consider the sequences $(s_{n-k}, s_{n-k+1}, \ldots, s_{n-1}, s_n)$ and $(t_{n-k}, t_{n-k+1}, \ldots, t_{n-1}, t_n)$ such that $s_{n-k} = a \ne b = t_{n-k}$, $s_i = t_i = x_{i-(n-k)}$ for all $i \in [n-k+1, n-1]$, $s_n = y$ and $t_n = z$. Consider the following table for $a - b \bmod r$, where the value of the column value represents the value of $a - b \bmod r$ and the carry of the column carry represents the corresponding borrow.

a, b	value	carry
$0 \le a, b \le r-1$	$(a-b) \bmod r$	$\begin{cases} 0, & a \ge b, \\ 1, & a < b \end{cases}$

So for the case $a > b$, the carry coming from the least significant k-digits is 0. Therefore, from the table above, we get

$$w_n = \begin{cases} 0 & \text{if } z \equiv y \mod r \\ 1 & \text{if } z \equiv y - 1 \mod r \\ \vdots & \vdots \\ r-1 & \text{if } z \equiv y - r + 1 \mod r \end{cases}$$

For the case $a < b$, the carry coming from the least significant k-digits is 1. Therefore, from the table above, we get

$$w_n = \begin{cases} 0 & \text{if } z \equiv y-1 \mod r \\ 1 & \text{if } z \equiv y-2 \mod r \\ \vdots & \vdots \\ r-1 & \text{if } z \equiv y \mod r \end{cases}$$

For the block $(s_{n-k}, s_{n-k+1}, \ldots, s_n)$, each coordinate can take any of the r possible values independently, and hence there are r^{k+1} possible choices in total. Observe that for indices $j = 1, 2, \ldots, k-1$, we impose the condition

$$s_{n-k+j} \;=\; t_{n-k+j}.$$

Therefore, once the values of s_{n-k+j} are fixed for these indices, the corresponding values of t_{n-k+j} are uniquely determined. Next, for the last coordinate, for each fixed value of y, there exists a unique value of z satisfying the required congruence condition, i.e., $w_n = 1$. Finally, the condition $a \neq b$ ensures that for each fixed value of $a \in \{0, 1, \ldots, r-1\}$, there are exactly $r-1$ possible choices for b. Thus, in total for this particular pattern of sequences satisfying equation (3) there exists $r^{k+1} \cdot (r-1)$ distinct patterns $\vec{e} \in \{0, 1, \ldots, r-1\}^{2k+2}$ such that

$$(s_{n-k}, s_{n-k+1}, \cdots, s_n, t_{n-k}, t_{n-k+1}, \cdots, t_n) \;=\; \vec{e}$$

implies $w_n = 1$. Hence for every $k = 1, 2, \ldots$ there are at least

$$(r-1) \cdot r^{k+1} \frac{PQ}{r^{2k+2}} + O\left(\frac{(r-1) \cdot r^{k+1}}{r^k} k d P^{1/2} Q\right) \;=\; \frac{(r-1)PQ}{r^{k+1}} + O\left(k d P^{1/2} Q\right)$$

distinct integers n in every fixed interval of length PQ such that $w_n = 1$. Choose the value,

$$M = \left\lfloor \min\left\{ \frac{\log P}{2 \log r}, \frac{\frac{1}{2}\log Q - \log\log Q - \log\log P}{\log r} \right\} \right\rfloor \leq \log P$$

. By Lemma 3, for $n \in [0, PQ-1]$ with $w_n = 1$, we have the number N_1

$$\begin{aligned} N_1 \;&\geq\; \sum_{k=1}^{M} \frac{(r-1)PQ}{r^{k+1}} + O\left(\sum_{k=1}^{M} k d P^{\frac{1}{2}} Q\right) \;=\; \frac{(r-1)PQ}{r^2} \sum_{k=1}^{M} r^{-(k-1)} + O\left(M^2 d P^{1/2} Q\right) \\ &=\; \frac{(r-1)PQ}{r^2} \cdot \frac{1 - r^{-M}}{1 - \frac{1}{r}} + O\left(M^2 d P^{1/2} Q\right) \;=\; \frac{PQ}{r}\left(1 - r^{-M}\right) + O\left(M^2 d P^{1/2} Q\right) \\ &=\; \frac{PQ}{r} + O\left(r^{-M} PQ + M^2 d P^{1/2} Q\right) \;=\; \frac{PQ}{r} + O\left(P^{1/2} Q (\log P)^2 + (\log P)^2 \cdot d P^{1/2} Q\right) \\ &=\; \frac{PQ}{r} + O\left(d P^{1/2} Q (\log P)^2\right), \end{aligned}$$

Analogously, the counts $N_0, N_2, \ldots, N_{r-1}$ for which $w_n = j$, $j \in \{0, 2, \ldots, r-1\}$, satisfy the same lower bound by similar arguments. In particular,

$$N_j \;\geq\; \frac{PQ}{r} + O\left(d P^{1/2} Q (\log P)^2\right),$$

for all $j \in \{0, 1, \ldots, r-1\}$. Since $\sum_{j=0}^{r-1} N_j = PQ$, we have $N_0 + N_1 + \cdots + N_{r-1} = PQ$, and each $N_j \geq \frac{PQ}{r} + O\left(d P^{1/2} Q (\log P)^2\right)$. So there exists constants $c_j > 0$ such that the following holds

$$N_j \;\geq\; \frac{PQ}{r} - c_j d P^{1/2} Q (\log P)^2.$$

Now $N_j = PQ - \sum_{k\neq j} N_k$, so we have

$$N_j \leq PQ - \sum_{k\neq j}\left(\frac{PQ}{r} - c_j dP^{1/2}Q(\log P)^2\right) \;=\; \frac{PQ}{r} + C_j dP^{1/2}Q(\log P)^2,$$

where $C_j = \sum_{k\neq j} c_j$. Therefore for $j \neq k \in \{0,1,\ldots,r-1\}$,

$$|N_j - N_k| \;=\; O\left(dP^{1/2}Q(\log P)^2\right). \tag{4}$$

Next, we compute $\mathcal{N}\left(C^A_{S,T}(\tau)\right)$ for $r \in \{3,4,5,6\}$ separately.

Case I ($r = 3$): In this case, the arithmetic crosscorrelation is given by

$$C^A_{S,T}(\tau) \;=\; N_0\omega^0 + N_1\omega^1 + N_2\omega^2 \;=\; N_0 + N_1 + N_2(-1-\omega) \;=\; (N_0 - N_2) + \omega(N_1 - N_2).$$

So, we have

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; (N_0 - N_2)^2 - (N_0 - N_2)(N_1 - N_2) + (N_1 - N_2)^2.$$

From Equation 4 we get,

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; O\left(3\left(dP^{1/2}Q(\log P)^2\right)^2\right) \;=\; O\left(\left(2dP^{1/2}Q(\log P)^2\right)^2\right).$$

Case II ($r = 4$): In this case, the arithmetic crosscorrelation is given by

$$C^A_{S,T}(\tau) \;=\; N_0 + N_1 i + N_2 i^2 + N_3 i^3 \;=\; (N_0 - N_2) + i(N_1 - N_3).$$

So, we have

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; (N_0 - N_2)^2 + (N_1 - N_3)^2.$$

From Equation 4 we get,

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; O\left(2\left(dP^{1/2}Q(\log P)^2\right)^2\right) \;=\; O\left(\left(2dP^{1/2}Q(\log P)^2\right)^2\right).$$

Case III ($r = 5$): In this case, the arithmetic crosscorrelation is given by

$$C^A_{S,T}(\tau) \;=\; N_0 + N_1\zeta_5 + N_2\zeta_5^2 + N_3\zeta_5^3 + N_4\zeta_5^4,$$

using the minimal polynomial relation $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$, i.e. $\zeta_5^4 = -1 - \zeta_5 - \zeta_5^2 - \zeta_5^3$, we get

$$C^A_{S,T}(\tau) \;=\; (N_0 - N_4) + (N_1 - N_4)\zeta_5 + (N_2 - N_4)\zeta_5^2 + (N_3 - N_4)\zeta_5^3.$$

So, we have

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; X_1^2 - (X_1X_2 + X_1X_3) + 3X_2X_3 - (X_2^2 + X_3^2),$$

where

$$\begin{aligned} X_1 &= (N_0 - N_4)^2 + (N_1 - N_4)^2 + (N_2 - N_4)^2 + (N_3 - N_4)^2 \\ X_2 &= (N_0 - N_4)(N_1 - N_4) + (N_1 - N_4)(N_2 - N_4) + (N_2 - N_4)(N_3 - N_4) \\ X_3 &= (N_0 - N_4)(N_2 - N_4) + (N_0 - N_4)(N_3 - N_4) + (N_1 - N_4)(N_3 - N_4). \end{aligned}$$

From Equation 4 we get,

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) \;=\; O\left(\left(4dP^{1/2}Q(\log P)^2\right)^4\right).$$

Case IV ($r = 6$)**:** In this case, the arithmetic crosscorrelation is given by

$$\begin{aligned} C^A_{S,T} &= N_0\zeta_6^0 + N_1\zeta_6^1 + N_2\zeta_6^2 + N_3\zeta_6^3 + N_4\zeta_6^4 + N_5\zeta_6^5 \\ &= N_0 + N_1(1+\omega) + N_2\omega + N_3(-1) + N_4(-1-\omega) + N_5(-\omega) \\ &= (N_0 + N_1 - N_3 - N_4) + \omega(N_1 + N_2 - N_4 - N_5) \end{aligned}$$

So, we have

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = (N_0+N_1-N_3-N_4)^2-(N_0+N_1-N_3-N_4)(N_1+N_2-N_4-N_5)+(N_1+N_2-N_4-N_5)^2.$$

From Equation 4 we get,

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = O\left(\left(2dP^{1/2}Q(\log P)^2\right)^2\right).$$

For a general integer r, let

$$C^A_{S,T}(\tau) = \sum_{j=0}^{r-1} N_j\zeta_r^j \in \mathbb{Z}[\zeta_r].$$

Since the field norm from $\mathbb{Q}(\zeta_r)$ to $\mathbb{Q}$ is the product of all Galois conjugates, and using the identity $\sum_{j=0}^{r-1}\zeta^j = 0$ we get

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} \sigma\left(\sum_{j=0}^{r-1} N_j\zeta_r^j\right) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} \sigma\left(\sum_{j=0}^{r-2}(N_j - N_{r-1})\zeta_r^j\right).$$

For every Galois automorphism σ,

$$\begin{aligned} \left|\sigma\left(\sum_{j=0}^{r-2}(N_j - N_{r-1})\zeta_r^j\right)\right| &= \left|\sum_{k=0}^{\varphi(r)-1} M_k\zeta_r^k\right| \quad [\text{where } M_k = \mathsf{poly}(|N_j - N_{j'}|) \text{ with degree 1}] \\ &\le \sum_{k=0}^{\varphi(r)-1} |M_k| = O\left(\varphi(r)dP^{1/2}Q(\log P)^2\right) \quad [\text{Using Equation 4}]. \end{aligned}$$

Hence,

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = \prod_{\sigma} O\left(\varphi(r)dP^{1/2}Q(\log P)^2\right) = O\left(\left(\varphi(r)dP^{1/2}Q(\log P)^2\right)^{\varphi(r)}\right),$$

where the implied constant depends only on r.

Combining all, we get

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = O\left(\left(\varphi(r)dP^{1/2}Q(\log P)^2\right)^{\varphi(r)}\right), \qquad 0 \le \tau < PQ.$$

In particular, for $r \in \{3, 4, 6\}$ we have $\varphi(r) = 2$ and for $r = 5$ we have $\varphi(r) = 4$. For $r = 2$ (i.e., $\varphi(2) = 1$), our bound simplifies to

$$\mathcal{N}\left(C^A_{S,T}(\tau)\right) = O\left(dP^{1/2}Q(\log P)^2\right),$$

thereby recovering the bound of Yan and Ke [41, Theorem 2] for the generalized Legendre character sequences. □

5 Conclusion

In this paper, we initiated the study of the arithmetic crosscorrelation of non-binary pseudorandom sequences constructed from higher-order multiplicative characters over finite fields. We established the asymptotic uniform distribution of joint local patterns and derived the first explicit non-trivial upper bounds on the arithmetic crosscorrelation of such sequences. Our results generalize the known bounds for binary Legendre-type sequences to a broad class of higher-order character sequences, thereby providing new insights into their pseudorandomness properties and potential cryptographic applications. Future work includes extending these results to other norm-Euclidean cyclotomic fields and investigating arithmetic crosscorrelation measures for more general higher-order character sequences.

References

[1] 802.11b White Paper. Vocal Technologies. Retrieved 16 July, 2026.

[2] Majid Alotaibi. Low noise moving target detection in high resolution radar using binary codes. *EURASIP Journal on Adva2021nces in Signal Processing*, 2021(8), 2021. DOI: 10.1186/s13634-020-00716-0.

[3] Robert B Ash. *A course in algebraic number theory*. Courier Corporation, 2010.

[4] Eric Brier, Rémi Géraud-Stewart, Marc Joye, and David Naccache. Primary Elements in Cyclotomic Fields with Applications to Power Residue Symbols, and More. Cryptology ePrint Archive, Paper 2021/1106, 2021.

[5] Eric Brier and David Naccache. The thirteenth power residue symbol. Cryptology ePrint Archive, Paper 2019/1176, 2019.

[6] Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT 2000, page 507–522, Berlin, Heidelberg, 2000. Springer-Verlag.

[7] Julien Cassaigne, Christian Mauduit, and András Sárközy. On Finite Pseudorandom Binary Sequences. VII. The Measures of Pseudorandomness. *Acta Arith.*, 103(2):97–118, 2002.

[8] Zhixiong Chen, Zhihua Niu, and Arne Winterhof. Arithmetic crosscorrelation of pseudorandom binary sequences of coprime periods. *IEEE Transactions on Information Theory*, 68(11):7538–7544, 2022.

[9] Henry Corrigan-Gibbs and David J. Wu. The pseudorandomness of legendre symbols under the quadratic-residuosity assumption. In Benny Applebaum and Huijia Rachel Lin, editors, *Theory of Cryptography - 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1-5, 2025, Proceedings, Part III*, Lecture Notes in Computer Science, pages 298–322. Springer, 2025.

[10] Ivan Damgård. On the randomness of legendre and jacobi sequences. In Shafi Goldwasser, editor, *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, Lecture Notes in Computer Science, pages 163–172. Springer, 1988.

[11] Koen de Boer and Carlo Pagano. Calculating the power residue symbol and ibeta: Applications of computing the group structure of the principal units of a p-adic number field completion. In *Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, page 117–124, New York, NY, USA, 2017. Association for Computing Machinery.

[12] Mriganka Dey, Sampa Dey, Sampurna Pal, Subhabrata Samajder, and Rana Barua. Beyond quadratic: Unlocking pseudorandomness with quartic character. 2026.

[13] Zeng Fan, John Rudlin, Giorgos Asfis, and Hongying Meng. Convolution of Barker and Golay Codes for Low Voltage Ultrasonic Testing. *Technologies*, 7(4):72, 2019. DOI: 10.3390/technologies7040072.

[14] S.W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[15] M. Goresky and A. Klapper. Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Transactions on Information Theory*, 43(4):1342–1345, 1997.

[16] Mark Goresky and Andrew Klapper. *Algebraic Shift Register Sequences*. Cambridge University Press, Cambridge, UK, 2012.

[17] Louis Goubin, Christian Mauduit, and András Sárközy. Construction of large families of pseudorandom binary sequences. *Journal of Number Theory*, 106(1):56–69, May 2004.

[18] Richard Hofer, László Mérai, and Arne Winterhof. *Measures of Pseudorandomness: Arithmetic Autocorrelation and Correlation Measure*, pages 303–312. Springer International Publishing, Cham, 2017.

[19] Kenneth Ireland and Michael Ira Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.

[20] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The eleventh power residue symbol. *Journal of Mathematical Cryptology*, 15(1):111–122, 2021.

[21] Andrew Klapper and Mark Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptol.*, 10(2):111–147, March 1997.

[22] Franz Lemmermeyer. The euclidean algorithm in algebraic number fields. *Expositiones Mathematicae*, 1995. Updated survey version.

[23] Franz Lemmermeyer. *Reciprocity Laws*. Springer Berlin Heidelberg, 2000.

[24] D. Mandelbaum. Arithmetic codes with large distance. *IEEE Transactions on Information Theory*, 13(2):237–242, 1967.

[25] Shota Matsuyuki and Akio Tsuneda. A Study on Aperiodic Auto-Correlation Properties of Concatenated Codes by Barker Sequences and NFSR Sequences. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 664–666, 2018. DOI: 10.1109/ICTC.2018.8539367.

[26] Christian Mauduit and Andras Sarkbzy. On Finite Pseudorandom Sequences of k Symbols. *Indagationes Mathematicae*, 13(1):89–101, 2002.

[27] Christian Mauduit and András Sárközy. On Finite Pseudorandom Binary Sequences. I. Measure of Pseudorandomness, the Legendre Symbol. *Acta Arith.*, 82(4):365–377, 1997.

[28] Christian Mauduit and András Sárközy. On Finite Pseudorandom Binary Sequences: II. The Champernowne, Rudin–Shapiro, and Thue–Morse Sequences, A Further Construction. *Journal of Number Theory*, 73(2):256–276, 1998.

[29] Christian Mauduit and András Sárközy. On Finite Pseudorandom Binary Sequences, V. On (n α) and (n 2α) Sequences. *Monatshefte für Mathematik*, 129(3):197–216, 2000.

[30] Christian Mauduit and András Sárközy. On Finite Pseudorandom Binary Sequences, VI, (On Sequences). *Monatshefte für Mathematik*, 130(4):281–298, 2000.

[31] Jan Mikulka and Stanislav Hanus. CCK and Barker Coding Implementation in IEEE 802.11b Standard. In *2007 17th International Conference Radioelektronika*, pages 1–4, 2007. DOI: 10.1109/RADIOELEK.2007.371484.

[32] Palash Sarkar and Subhamoy Maitra. Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes. *Theory of Computing Systems*, 35(1):39–57, 2002.

[33] A. Sárközy. A finite pseudorandom binary sequence. *Studia Sci. Math. Hungar.*, 38:377–384, 2001.

[34] C. E. Shannon. Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[35] Irv D. Siegel. Development of a Set of Optimum Synchronization Codes for a Unique Decoder Mechanization. Master's thesis, Department: Electrical and Computer Engineering, University of Missouri-Rolla, USA, 1971.

[36] Daqing Wan. Generators and Irreducible Polynomials Over Finite Fields. *Mathematics of Computation*, 66(219):1195–1212, 1997.

[37] Lawrence C Washington. *Introduction to cyclotomic fields*. Springer Science & Business Media, 2012.

[38] André Weil. On Some Exponential Sums. *Proceedings of the National Academy of Sciences*, 34(5):204–207, 1948.

[39] André Weilert. Fast computation of the biquadratic residue symbol. *Journal of Number Theory*, 96(1):133–151, 2002.

[40] Feifei Yan and Pinhui Ke. Notes on the ideal arithmetic correlations of n-ary sequences. Cryptology ePrint Archive, Paper 2026/1383, 2026.

[41] Feifei Yan and Pinhui Ke. On the properties of arithmetic crosscorrelation for sequences with coprime periods. Cryptology ePrint Archive, Paper 2026/616, 2026.

[42] Heng Zhao, Larry Y. L. Mo, and Shangkai Gao. Barker-coded ultrasound color flow imaging: theoretical and practical design considerations. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, 54(2):319–331, 2007. DOI: 10.1109/TUFFC.2007.246.