International Journal of Foundations of Computer Science
© World Scientific Publishing Company

Statistical Properties of the Arithmetic Correlation of Sequences*

Mark Goresky
School of Mathematics
Institute for Advanced Study

Andrew Klapper
Dept. of Computer Science
779A Anderson Hall, University of Kentucky
Lexington, KY, 40506-0046.
http://www.cs.uky.edu/∼klapper.

Received (Day Month Year)
Accepted (Day Month Year)
Communicated by (xxxxxxxxxx)

In this paper we study arithmetic correlations of sequences. Arithmetic correlations are the with-carry analogs of classical correlations. We analyze the arithmetic autocorrelations of non-binary ℓ-sequences, showing that they are nearly optimal. We analyze the expected auto- and cross-correlations of sequences with fixed shift, averaged over all seqeunces with a fixed period. We analyze the expected autocorrelations of a fixed sequence, averaged over all shifts.

Keywords: Feedback with carry shift registers, Correlations, pseudo-randomness, sequences.

1991 Mathematics Subject Classification:

1. Introduction

Sequences with good correlation properties are essential ingredients in a wide range of applications including CDMA systems and radar ranging. A great deal of research has gone into the design and generation of sequences and families of sequences with good correlation properties. For example, for CDMA we want large families of sequences with small pairwise correlations. Unfortunately, we also know that there are fundamental limits on the sizes of families of sequences with such properties [10].

In this paper we consider an arithmetic or "with-carry" analog of the correlation of sequences, previously introduced by the authors in the binary case [2]. In this paper we generalize this notion to non-binary sequences. We study the average

*Some of the results in this paper have appeared without proof in the conference SETA 2008 behavior of the arithmetic correlation of sequences, averaged in two different ways, and compare to the average behavior of the classical correlation function. The new notion of correlation is interesting in part because it is known (in the binary case) that they do not suffer from some of the constraints on sizes of families of sequences with good classical correlations. However, we do not as yet know of any significant applications of arithmetic correlations. Nonetheless, it is worthwhile studying properties of arithmetic correlations in hope that applications will come.

In previous work we have studied arithmetic auto- and cross-correlations (defined below) of a class of binary sequences called ℓ-sequences [2, 3, 5]. The arithmetic autocorrelations of these sequences were previously studied in the context of arithmetic coding [8, 9]. It is known that the shifted arithmetic autocorrelations of binary ℓ-sequences are identically zero and that the arithmetic cross-correlations of any two distinct decimations of a binary ℓ-sequence is identically zero.

In this paper we study the arithmetic correlations of possibly non-binary sequences. We show that the arithmetic autocorrelations of ℓ-sequences are at most one for a prime connection integer and at most two for a prime power connection integer. We also analyze the expected arithmetic auto- and cross-correlations of sequences with fixed shift, averaged over all sequences, and in the binary case we analyze the expected arithmetic autocorrelations of a fixed sequence, averaged over all shifts.

2. Balance and Classical Correlations

In his section we recall some basic facts about balance and classical notions of the correlation of sequences. Here and throughout the paper let $N \geq 2$ be a natural number. Let $\mathbf{a} = a_0, a_1, \cdots$ be a periodic sequence with $a_i \in \{0, 1, \cdots, N-1\}$, $i = 0, 1, \cdots$.

For each $i = 0, 1, \cdots, N-1$, let μ_i be the number of occurrences of i in one complete period of $\mathbf{a}$. Let

$$\zeta = e^{2\pi i/N}$$

be a complex primitive Nth root of 1. Let

$$Z(a) = Z(\mathbf{a}) = \sum_{i=0}^{N-1} \mu_i \zeta^i,$$

the *imbalance* of a or of $\mathbf{a}$.

The periodic sequence $\mathbf{a}$ is said to be *balanced* if $\mu_i = \mu_j$ for all i, j. It is *weakly balanced* if $Z(\mathbf{a}) = 0$.

For example, let $N = 3$ and $a = 3/5 = 0 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + 1 \cdot 3^5 + 0 \cdot 3^6 + 1 \cdot 3^7 + \cdots$. This sequence is periodic with period 4 from the 3^2 term on. Thus $\mu_0 = 1$, $\mu_1 = 2$, and $\mu_2 = 1$. We have $Z(\mathbf{a}) = 1 + 2\zeta + \zeta^2 = \zeta$. The sequence is not weakly balanced.

Lemma 1. *If the N-ary sequence* $\mathbf{a}$ *is balanced, then it is weakly balanced. If N is prime, then* $\mathbf{a}$ *is balanced if and only if it is weakly balanced.*

Proof. The element ζ is a root of the polynomial $x^N-1=(x-1)(x^{N-1}+\cdots+1)$, so it is a root of $x^{N-1}+\cdots+1$. This proves the first statement. If N is prime, then the latter polynomial is irreducible [7] . If the μ_i were not all equal, then we could form a linear combination of $Z(\mathbf{a})$ and $\sum_{i=0}^{N-1}\zeta^i$ whose value is zero and that does not include some power ζ^j, $j<N$. By multiplying by ζ^{N-j-1} we obtain a nontrivial integer linear combination of $1,\zeta,\cdots,\zeta^{N-2}$ that equals 0. Thus ζ is a root of a polynomial with integer coefficients and degree less than $N-1$. This is a contradiction. □

For any N-ary sequence $\mathbf{b}$, let $\mathbf{b}^\tau$ be the sequence formed by shifting $\mathbf{b}$ by τ positions, $b^\tau_i=b_{i+\tau}$.

Definition 2. *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be two eventually periodic sequences with period T and let $0\le\tau<T$. Then the sequence* $\mathbf{a}-\mathbf{b}^{(\tau)}$ *(term by term subtraction modulo N) is periodic and its period divides T. The* shifted cross-correlation *of* $\mathbf{a}$ *and* $\mathbf{b}$ *is*

$$\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)=Z(\mathbf{a}-\mathbf{b}^{(\tau)})=\sum_{i=0}^{T-1}\zeta^{a_i-b_{i+\tau}}=\sum_{0\le c<N}|\{0\le i<T: a_i-b_{i+\tau}\equiv c \pmod N\}|\zeta^c, \quad (1)$$

where the imbalance is taken over a full period of length T. When $\mathbf{a}=\mathbf{b}$*, the cross-correlation is called the* autocorrelation *of* $\mathbf{a}$ *and is denoted* $\mathcal{A}_{\mathbf{a}}(\tau)$*.*

The ordinary cross-correlation with shift τ of two N-ary sequences $\mathbf{a}$ and $\mathbf{b}$ of period T is the imbalance of the term by term difference of $\mathbf{a}$ and $\mathbf{b}^\tau$, or equivalently, of the coefficient sequence of the difference between the power series associated with $\mathbf{a}$ and the power series associated with $\mathbf{b}^\tau$. In the binary case this is the number of zeros minus the number of ones in one period of the bitwise exclusive-or of $\mathbf{a}$ and the τ shift of $\mathbf{b}$ [1]. The arithmetic cross-correlation is the with-carry analog of this [2].

The most widely used sequences for many applications in cryptography and communications are *m-sequences*. These are N-ary sequences of period N^k-1 generated by LFSRs of length k. It is well known that their autocorrelations with nonzero shift τ are all -1 (so-called *ideal autocorrelations*). Many researchers have studied cross-correlations of cyclically distinct m-sequences, but the the values are known only in a few cases (such as when m-sequence $\mathbf{a}$ is related to m-sequence $\mathbf{b}$ by $a_i=b_{(N^j+1)i}$, a so-called quadratic decimation).

The calculation of the expected auto- and cross-correlation (averaged over all sequences of a given period T) is straightforward.

Theorem 3. *For any τ, the expected autocorrelation, averaged over all sequences* $\mathbf{a}$ *of period T, is*

$$E_{\mathbf{a}}[\mathcal{A}_{\mathbf{a}}(\tau)]=0.$$

The expected cross-correlation, averaged over all pairs of sequences **a** *and* **b** *is*

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)] = 0.$$

Proof. The expected cross-correlation is U/N^{2T} where

$$\begin{aligned} U &= \sum_{\mathbf{a},\mathbf{b}} Z(\mathbf{a}-\mathbf{b}^{(\tau)}) \\ &= \sum_{\mathbf{a},\mathbf{b}} \sum_{i=0}^{T-1} \zeta^{a_i - b_{i+\tau}} \\ &= \sum_{i=0}^{T-1} \sum_{\substack{(\cdots,a_j,\cdots)\\ j\neq i}} \sum_{\substack{(\cdots,b_j,\cdots)\\ j\neq i+\tau}} \sum_{a_i} \sum_{b_{i+\tau}} \zeta^{a_i - b_{i+\tau}} \\ &= \sum_{i=0}^{T-1} N^{2T-2} \sum_{a_i} \zeta^{a_i} \sum_{b_{i+\tau}} \zeta^{-b_{i+\tau}} \\ &= 0. \end{aligned}$$

The calculation of expected autocorrelations is similar. □

A similar calculation gives the following.

Theorem 4. *For any τ, the second moment of the autocorrelation, averaged over all sequences* **a** *of period T, is*

$$E_{\mathbf{a}}[\mathcal{A}_{\mathbf{a}}(\tau)^2] = \begin{cases} T^2 \ \textit{if}\ \tau = 0 \\ 2T \ \textit{if}\ N = 2 \ \textit{and}\ T = 2\tau \\ T \quad \textit{else.} \end{cases}$$

The second moment of the cross-correlation, averaged over all sequences **a** *and* **b** *of period T, is*

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)^2] = T.$$

We can also average over all shifts. If x is a complex number, then we denote the complex conjugate of x by $\overline{x}$.

Theorem 5. *For any sequences* **a** *and* **b** *with period T , the expected cross-correlation, averaged over all shifts τ, is*

$$E_{\tau}[\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)] = \frac{Z(\mathbf{a})\overline{Z(\mathbf{b})}}{T}.$$

Proof. We have

$$E_{\tau}[\mathcal{C}_{\mathbf{a},\mathbf{b}}(\tau)] = \frac{1}{T} \sum_{\tau=0}^{T-1} \sum_{i=0}^{T-1} \zeta^{a_i - b_{i+\tau}}$$

$$= \frac{1}{T}\sum_{i=0}^{T-1}\zeta^{a_i}\sum_{\tau=0}^{T-1}\zeta^{-b_{i+\tau}}$$
$$= \frac{Z(\mathbf{a})\overline{Z(\mathbf{b})}}{T}$$

as claimed. □

Corollary 6. *For any sequence* $\mathbf{a}$ *with period* T *, the expected autocorrelation, averaged over all shifts* τ*, is*

$$E_\tau[\mathcal{C}_\mathbf{a}(\tau)] = \frac{|Z(\mathbf{a})|^2}{T}.$$

3. Arithmetic Correlations

Let $N \geq 2$ be a natural number. In this section we define a with carry analog of the usual notion of cross-correlations for N-ary sequences.

A fundamental tool we use is the notion of *N-adic numbers.* An N-adic number is a formal expression

$$a = \sum_{i=0}^{\infty} a_i N^i,$$

where $a_i \in \{0, 1, \cdots, N-1\}$, $i = 0, 1, \cdots$. The set $\hat{\mathbb{Z}}_n$ of N-adic numbers forms an algebraic ring and has been the subject of extensive study for over 100 years [5, 6]. The algebra — addition and multiplication — is defined with carries propagated to higher and higher terms, just as it is for ordinary nonnegative integers, but possibly involving infinitely many terms. It is easy to see that $\hat{\mathbb{Z}}_n$ contains all rational numbers u/q, $u, q \in \mathbb{Z}$, with q relatively prime to N and no other rational numbers. There is a one to one correspondence between N-adic numbers and infinite N-ary sequences. Under this correspondence the rational numbers u/q with q relatively prime to N correspond to the eventually periodic sequences. The rational numbers u/q with q relatively prime to N and $-q \leq u \leq 0$ correspond to the (strictly) periodic sequences. If $\mathbf{a}$ is periodic (resp., eventually periodic) then we say that the associated N-adic number is periodic (resp., eventually periodic). Note that, unlike power series, the sum and difference of strictly periodic N-adic numbers are eventually periodic but may not be strictly periodic.

Let $\mathbf{a}$ be an eventually periodic N-ary sequence and let

$$a = \sum_{i=0}^{\infty} a_i N^i$$

be the associated N-adic number.

Definition 7. *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be two eventually periodic sequences with period* T *and let* $0 \leq \tau < T$*. Let* a *and* $b^{(\tau)}$ *be the N-adic numbers whose coefficients are given by* $\mathbf{a}$ *and* $\mathbf{b}^\tau$*, respectively. Then the sequence of coefficients associated with* $a - b^{(\tau)}$ *is* *eventually periodic and its period divides T. The* shifted arithmetic cross-correlation *of* $\mathbf{a}$ *and* $\mathbf{b}$ *is*

$$\mathcal{C}^{A}_{\mathbf{a},\mathbf{b}}(\tau) = Z(a - b^{(\tau)}), \tag{2}$$

where the imbalance is taken over a full period of length T. When $\mathbf{a} = \mathbf{b}$, the arithmetic cross-correlation is called the arithmetic autocorrelation *of* $\mathbf{a}$ *and is denoted* $\mathcal{A}^{A}_{\mathbf{a}}(\tau)$.

If for all τ such that $\mathbf{a}$ and $\mathbf{b}^{\tau}$ are distinct we have $\mathcal{C}^{A}_{\mathbf{a},\mathbf{b}}(\tau) = 0$, then $\mathbf{a}$ and $\mathbf{b}$ are said to have *ideal arithmetic correlations.* A family of sequences is said to have ideal arithmetic correlations if every pair of sequences in the family has ideal arithmetic correlations.

4. ℓ-Sequences

In this section we consider the arithmetic autocorrelations of ℓ-sequences. These are the arithmetic analogs of m-sequences, a class of sequences that have been used in many applications. Recall that an m-sequence over a finite field F is the coefficient sequence of the power series expansion of a rational function $f(x)/q(x)$ such that the degree of f is less than the degree of q, q is irreducible, and x is a primitive element in the multiplicative group of $F[x]/(q)$. It is well known that the classical shifted autocorrelations of an m-sequence all equal -1. However, the cross-correlations of m-sequences are only known in a few special cases.

An N-ary ℓ-sequence $\mathbf{a}$ is the N-adic expansion of a rational number f/q where $\gcd(q, N) = 1$, $-q < f < 0$ (so that $\mathbf{a}$ is strictly periodic), and N is a primitive element in the multiplicative group of integers modulo q. This last condition means that the multiplicative order of N modulo q, $\mathrm{ord}_q(N)$, equals $\phi(q)$ (Euler's function). In particular it implies that q is a power of a prime number, $q = p^t$. For the remainder of this section we assume that N, $\mathbf{a}$, q, p, t and f satisfy all these conditions.

Quite a lot is known about ℓ-sequences, especially in the binary ($N = 2$) case. For example, we have the following is a remarkable fact about binary ℓ-sequences [2].

Theorem 8. *Suppose that* $\mathbf{a}$ *is a binary ℓ-sequence. If* $\mathbf{c}$ *and* $\mathbf{b}$ *are decimations of* $\mathbf{a}$*, then the arithmetic cross-correlation of* $\mathbf{c}$ *and* $\mathbf{b}$ *with shift τ is zero unless $\tau = 0$ and* $\mathbf{b} = \mathbf{c}$.

Our goal here is to determine the arithmetic autocorrelations of not necessarily binary ℓ-sequences. First we look at their imbalances.

Theorem 9. *Let* $\mathbf{a}$ *be an N-ary ℓ-sequence based on a connection integer $q = p^e$,* *p prime, $e \geq 1$. Then*

$$|Z(\mathbf{a})| \begin{cases} \leq 2 \textit{ for all } q \\ \leq 1 \textit{ if } q \textit{ is prime} \\ \leq 1 \textit{ if } e \geq 2 \textit{ and either } q \equiv 1 \pmod{N} \textit{ or } p^{e-1} \equiv 1 \pmod{N} \\ = 0 \textit{ if } q \textit{ is prime and } q \equiv 1 \pmod{N} \\ = 0 \textit{ if } e \geq 2,\ q \equiv 1 \pmod{N}, \textit{ and } p^{e-1} \equiv 1 \pmod{N} \end{cases}$$

One of the last two cases always holds when $N = 2$.

Proof. Let q be the minimal connection element of $\mathbf{a}$ and suppose q is prime. The distribution of occurrences of symbols in $\mathbf{a}$ is the same as the distribution of occurrences of symbols as the first symbols of the various shifts of $\mathbf{a}$. The rational representations of the shifts of $\mathbf{a}$ are the fractions $-u/q$ with $0 < u < q - 1$. An integer $b \in \{0, 1, \cdots, N-1\}$ occurs as the first element in the N-ary expansion of $-u/q$ if and only if

$$\frac{-u}{q} \equiv b \pmod{N}.$$

This holds if and only if

$$u \equiv -qb \pmod{N}$$

since q and N are relatively prime. Equivalently,

$$-ru \equiv b \pmod{N},$$

where $rq \equiv 1 \pmod{N}$ and $|r| < N/2$. Thus

$$|Z(\mathbf{a})| = \left| \sum_{u=1}^{q-1} \zeta^{-ru} \right|.$$

We have

$$\begin{aligned} |Z(\mathbf{a})| &= \left| \sum_{u=1}^{q-1} \zeta^{-ru} \right| \\ &= \left| \frac{(\zeta^{-r})^q - \zeta^{-r}}{\zeta^{-r} - 1} \right| \\ &= \left| \frac{\zeta^{-1} - \zeta^{-r}}{\zeta^{-r} - 1} \right| \\ &= \left| \frac{\zeta^{(r-1)/2} - \zeta^{-(r-1)/2}}{\zeta^{r/2} - \zeta^{-r/2}} \right| \\ &= \left| \frac{\sin(\pi(r-1)/N)}{\sin(\pi r/N)} \right|. \end{aligned} \tag{3}$$

We have

$$-\pi \frac{N+1}{2N} \leq \pi \frac{r-1}{N} < \pi \frac{r}{N} \leq \pi \frac{N-1}{2N} < \frac{\pi}{2}.$$

The sine function is increasing on the interval $[-\pi/2, \pi/2]$, so the expression in equation (3) is less than 1 if $-\pi/2 \leq \pi(r-1)/N$. The only other possibility is that $\pi(r-1)/N = -\pi(N+1)/(2N)$. In this case $\pi r/N = -\pi(N-1)/(2N)$ and the expression in equation (3) equals 1.

Now suppose that q is a power of a prime, $q = p^t$. We are led to the same sum, but we must subtract off the terms for which t divides f. A similar argument shows that the sum of these terms is at most one, so the imbalance is at most 2.

If $q \equiv 1 \pmod{N}$, then $r = 1$ and so the expression in equation (3) is zero. The statements for prime powers are proved similarly. If $N = 2$, then $q \equiv 1 \pmod{N}$. The last statement was also proved previously [2]. □

We can apply this result to estimate the autocorrelations of ℓ-sequences.

Theorem 10. *Let* $\mathbf{a}$ *be an* N*-ary* ℓ*-sequence with period* T *based on a prime connection integer* q*. Let* τ *be an integer that is not a multiple of* T*. Then* $|\mathcal{A}^A_{\mathbf{a}}(\tau)| \leq 1$*. If* $q \equiv 1 \pmod{N}$*, then* $\mathcal{A}^A_{\mathbf{a}}(\tau) = 0$*. This last statement holds when* $N = 2$*.*

Proof. The N-adic number associated with $\mathbf{a}$ is a fraction $-f/q$ as above. By an argument similar to the one in Section 5, the arithmetic autocorrelation of $\mathbf{a}$ with shift τ is the imbalance of the rational number

$$\frac{(N^{T-\tau}-1)f \pmod{q}}{q},$$

where the reduction modulo q is taken in the range $[-(q-1), 0]$. Since q is prime, this is again the rational number corresponding to an ℓ-sequence. The theorem then follows from Theorem 9. □

Note that this argument does not apply to ℓ-sequences with prime power connection integer since the numerator $(N^{T-\tau}-1)f$ may not be relatively prime to q.

5. Expected Arithmetic Correlation of a Fixed Shift

In this section we investigate the expected values of the arithmetic autocorrelations and cross-correlations and the second moments and variances of the cross-correlations for a fixed shift.

We need some initial analysis for general N-ary sequences. Fix a period T. As we have seen, the N-ary sequences of period T are the coefficient sequences $\mathbf{a}$ of rational numbers of the form

$$a = \frac{-f}{N^T - 1}$$

with $0 \leq f \leq N^T - 1$.

Lemma 11. *If* a *and* b *are distinct* N*-adic numbers whose coefficient sequences are periodic with period* T*, and* $a - b \in \mathbb{Z}$*, then* $\{a, b\} = \{0, -1\}$*.*

Proof. First note that the N-adic expansion of an integer is strictly periodic if and only if the integer is 0 or -1. Let $a = -f/(N^T - 1)$ and $b = -g/(N^T - 1)$ with $0 \leq f, g \leq N^T - 1$. Assume that $f > g$. Then $a - b = -(f - g)/(N^T - 1)$ is strictly periodic and nonzero, so $-1 = a - b = -(f - g)/(N^t - 1)$. Thus $f = g + (N^T - 1)$. The only possibility is that $f = N^T - 1$ and $g = 0$. That is, $a = -1$ and $b = 0$. The case when $g > f$ is similar. □

Next fix a shift τ. Then the τ shift of $\mathbf{a}$ corresponds to a rational number

$$a^{(\tau)} = c_{f,\tau} + \frac{-N^{T-\tau} f}{N^T - 1},$$

where $0 \leq c_{f,\tau} < N^{T-\tau}$ is an integer.

Now let $\mathbf{b}$ be another periodic N-ary sequence corresponding to the rational number

$$b = \frac{-g}{N^T - 1}.$$

Then the arithmetic cross-correlation between $\mathbf{a}$ and $\mathbf{b}$ with shift τ is

$$\begin{aligned} \mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau) &= Z\left(\frac{-f}{N^T - 1} - \left(c_{g,\tau} + \frac{-N^{T-\tau} g}{N^T - 1}\right)\right) \\ &= Z\left(\frac{N^{T-\tau} g - f}{N^T - 1} - c_{g,\tau}\right). \qquad (4) \end{aligned}$$

Theorem 12. *For any τ, the expected arithmetic autocorrelation, averaged over all sequences $\mathbf{a}$ of period T, is*

$$E_{\mathbf{a}}[\mathcal{A}^A_{\mathbf{a}}(\tau)] = \frac{T}{N^{T-\gcd(\tau,T)}}.$$

The expected cross-correlation, averaged over all pairs of sequences $\mathbf{a}$ and $\mathbf{b}$ is

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau)] = \frac{T}{N^T}.$$

Proof. If the τ shift of $\mathbf{b}$ equals $\mathbf{a}$, then $\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau) = T$. Otherwise a and $b^{(\tau)}$ are distinct periodic sequences. In particular, by Lemma 11 $a - b^{(\tau)}$ is an integer only if $\{a, b^{(\tau)}\} = \{0, -1\}$.

First we consider the autocorrelation. Let

$$S = \sum_{f=0}^{N^T-1} Z\left(\frac{(N^{T-\tau} - 1)f}{N^T - 1} - c_{f,\tau}\right).$$

It follows from equation (4) that the expected arithmetic autocorrelation is $E_{\mathbf{a}}[\mathcal{A}^A_{\mathbf{a}}(\tau)] = S/N^T$.

By the first paragraph of this proof $a - a^{(\tau)}$ is an integer only if $a^{(\tau)} = a$. When it is not an integer, the periodic part of

$$\frac{(N^{T-\tau} - 1)f}{N^T - 1} - c_{f,\tau}$$

is the same as the periodic part of

$$\frac{(N^{T-\tau}-1)f \pmod{N^T-1}}{N^T-1},$$

where we take the reduction modulo N^T-1 in the set of residues $\{-(N^T-2), -(N^T-3), \cdots, -1, 0\}$. In particular, this latter rational number has a strictly periodic N-adic expansion, so we can compute its contribution to S by considering the first T coefficients.

Let $d = \gcd(T, T-\tau) = \gcd(T, \tau)$. Thus $T = md$ for some integer m. Then $\gcd(N^T-1, N^{T-\tau}-1) = N^d-1$. The set of elements of the form $(N^{T-\tau}-1)f \pmod{N^T-1}$ is the same as the set of elements of the form $(N^d-1)f \pmod{N^T-1}$. Thus

$$S = \sum_{f=0}^{N^T-1} Z\left(\frac{(N^d-1)f \pmod{N^T-1}}{N^T-1}\right).$$

Now consider the contribution to S from the ith term in the expansion in each element in the sum, say corresponding to an integer f. If we multiply f by N^{T-i} modulo N^T-1, this corresponds to cyclically permuting the corresponding sequence to the right by $T-i$ places. This is equivalent to permuting to the left by i positions, so the elements in the ith place become the elements in the 0th place. Moreover, multiplying by N^{T-i} is a permutation modulo N^T-1, so the distribution of values contributing to S from the ith terms is identical to the distribution of values from the 0th term.

To count the contribution from the 0th position, let

$$D = \frac{N^T-1}{N^d-1}$$

and $f = u + vD$ with $0 < u < D$ and $0 \le v < N^d-1$. Then $(N^d-1)f \pmod{N^T-1} = (N^d-1)u \pmod{N^T-1} = (N^d-1)u - (N^T-1)$. Thus

$$\frac{(N^d-1)f \pmod{N^T-1}}{N^T-1} = \frac{(N^d-1)u}{N^T-1} - 1. \tag{5}$$

In particular, the contribution to S from the 0th position depends only on u. Thus we can count the contributions over all g with $0 < u < D$, and then multiply by N^d-1. The contribution from the 0th position for a particular u is given by reducing the right hand side of equation (5) modulo N. We have

$$\begin{aligned}\frac{(N^d-1)u}{N^T-1} - 1 &= (1+N^T+N^{2T}+\cdots)(N^d-1)u - 1\\ &\equiv -u-1 \pmod{N}.\end{aligned}$$

Since $-(1+N^d+N^{2d}+\cdots+N^{T-d}) \le -u-1 \le -2$, as u varies its reduction modulo N takes each value in $\{0, 1, \cdots, N-1\}$ exactly $N^{d-1}+N^{2d-1}+\cdots+N^{T-d-1}$ times.

It follows that the contribution to S from the sequences that are not equal to their τ shifts is a multiple of $1+\zeta+\cdots+\zeta^{N-1} = 0$.

Thus we need to count the number of sequences that are equal to their τ shifts. These are the sequences whose minimal periods are divisors of τ. Of course the minimal periods of such sequences are also divisors of T, so it is equivalent to count the sequences whose minimal period divides d. The number of such sequences is exactly N^d. Thus the expected autocorrelation is

$$E_{\mathbf{a}}[\mathcal{A}_{\mathbf{a}}^A(\tau)] = \frac{N^d T}{N^T}.$$

Now consider the expected cross-correlation. The set of τ shifts of all T-periodic sequences is just the set of all T-periodic sequences, so we can take $\tau = 0$. Thus $c_{g,\tau} = 0$. Let

$$R = \sum_{f,g=0}^{N^T-1} Z\left(\frac{g-f}{N^T-1}\right) = \sum_{f,g=0}^{N^T-1} Z\left(\frac{(g-f) \pmod{N^T-1}}{N^T-1}\right).$$

Here when we reduce modulo $N^T - 1$ we must take $(g-f) \pmod{N^T-1} = g-f$ if $g \le f$ and $(g-f) \pmod{N^T-1} = g - f - (N^T-1)$ if $f < g$. Thus

$$R = TN^T + \sum_{0\le g<f\le N^T-1} Z\left(\frac{g-f}{N^T-1}\right) + \sum_{0\le f<g\le N^T-1} Z\left(\frac{g-f-N^T+1}{N^T-1}\right), \quad (6)$$

where the first term on the right hand side accounts for the cases when $f = g$. By similar arguments to those in the derivation of the expected autocorrelations, we can reduce the calculation of the remaining two terms on the right hand side of equation (6) to counting the contributions from the 0th positions. The rational numbers have periodic expansions, so the reductions of these numbers modulo N are the coefficients of N^0 in the expansions of the numerators. That is, if $f = f_0 + Nf'$ and $g = g_0 + Ng'$ with $0 \le f_0, g_0 < N$, then

$$R = TN^T + T \cdot \sum_{0\le g<f\le N^T-1} \zeta^{g_0-f_0} + T \cdot \sum_{0\le f<g\le N^T-1} \zeta^{g_0-f_0-1}.$$

We have $g < f$ if and only if either $g' < f'$ or $g' = f'$ and $g_0 < f_0$. If we fix an f and consider all $g < f$ with $g' < f'$, then the g_0 is free to vary over $\{0, 1, \cdots, N-1\}$. Thus the contribution to R from such terms is zero. Similarly, if $f' < g'$ then the contribution is zero. Thus we only need to consider the cases when $f' = g'$. Since there are N^{T-1} choices of f', we have

$$\begin{aligned}
R &= TN^T + TN^{T-1} \sum_{f_0=0}^{N-1} \sum_{g_0=0}^{f_0-1} \zeta^{g_0-f_0} + TN^{T-1} \sum_{f_0=0}^{N-1} \sum_{g_0=f_0+1}^{N-1} \zeta^{g_0-f_0-1} \\
&= TN^T + TN^{T-1} \sum_{f_0=0}^{N-1} \sum_{g_0=0}^{f_0-1} \zeta^{g_0-f_0} + TN^{T-1} \sum_{f_0=0}^{N-1} \sum_{g_0=f_0}^{N-2} \zeta^{g_0-f_0} \\
&= TN^T + TN^{T-1} \sum_{f_0=0}^{N-1} \sum_{g_0=0}^{N-2} \zeta^{g_0-f_0}
\end{aligned}$$

$$= TN^T + TN^{T-1}\frac{\zeta^{-N}-1}{\zeta-1}\cdot\frac{\zeta^{N-1}-1}{\zeta-1}$$
$$= TN^T.$$

Thus

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau)] = \frac{R}{N^{2T}} = \frac{T}{N^T}.$$

This proves the theorem. □

Theorem 13. *Let $\tau \in \mathbb{Z}$, $d = \gcd(T,\tau)$, and $D = (N^T-1)/(N^d-1)$. The second moment of the arithmetic autocorrelation with shift τ, averaged over all sequences $\mathbf{a}$ of period T is*

$$E_{\mathbf{a}}[\mathcal{A}^A_{\mathbf{a}}(\tau)^2] = \begin{cases} \dfrac{(N^d-1)T(D+T-1)+T^2}{N^T} = T + \dfrac{T^2-T}{N^{T-d}} & \text{if } N \neq 2 \\ \dfrac{(N^d-1)T(D+T-N^d(T/d-1)-1)+T^2}{N^T} & \text{if } N = 2. \end{cases}$$

Proof. As in the computation of the expectation, we have

$$E_{\mathbf{a}}[\mathcal{A}^A_{\mathbf{a}}(\tau)^2] = \frac{1}{N^T}\sum_{f=0}^{N^T-1}\left|Z\left(\frac{(N^d-1)f \pmod{N^T-1}}{N^T-1}\right)\right|^2 = \frac{S}{N^T}.$$

If $T|\tau$ (so that $d=T$), then each term of the sum is $|Z(0)|^2 = T^2$, so the second moment is T^2. Assume from here on that T does not divide τ. Thus d is a proper divisor of T. We have

$$S = (N^d-1)\sum_{f=0}^{D-1}\left|Z\left(\frac{-(N^d-1)f}{N^T-1}\right)\right|^2 + |Z(0)|^2 = (N^d-1)\sum_{f=0}^{D-1}\left|Z\left(\frac{-(N^d-1)f}{N^T-1}\right)\right|^2 + T^2.$$

We write it this way because $-(N^d-1)f/(N^T-1) = -f/D$ has a strictly periodic N-adic expansion if $0 \le f < D$. Thus if $-(N^d-1)f/(N^T-1) = \sum_{i=0}^{\infty} g_i N^i$, then

$$|Z(f/D)|^2 = \sum_{0\le i,j<T} \zeta^{g_i - g_j}.$$

For any g with $0 \le g < N^T-1$, the first T coefficients in the N-adic expansion of $-g/(N^T-1)$ are the coefficients in the N-ary expansion of g. By arguments similar to the ones in the case of the expectation, we can take $i=0$ and introduce a multiplicative factor of T. Thus

$$S = (N^d-1)\sum_{\substack{0\le g<N^T-1 \\ g \text{ a multiple of } N^d-1}}\ \sum_{0\le i,j<T}\zeta^{g_i-g_j} + T^2$$
$$= (N^d-1)\sum_{0\le i,j<T}\ \sum_{\substack{0\le g<N^T-1 \\ g \text{ a multiple of } N^d-1}}\zeta^{g_i-g_j} + T^2$$

$$= (N^d-1)T\sum_{j=0}^{T-1}\sum_{\substack{0\le g<N^T-1\\ g\text{ a multiple of }N^d-1}}\zeta^{g_0-g_j}+T^2,$$

where $g=\sum_{i=0}^{T-1}g_iN^i$ with $0\le g_i<N$. Now fix j. Let

$$U_j=\sum_{\substack{0\le g<N^T-1\\ g\text{ a multiple of }N^d-1}}\zeta^{g_0-g_j}.$$

We compute all the U_js.

First suppose $j=0$. Then we have $\zeta^{g_0-g_j}=1$, and there are D such terms (one for each multiple g of N^d-1), so $U_0=D$.

Now suppose $j>0$. Suppose that $j=ed+k$ with $1\le k\le d$. Let g' be obtained from g by interchanging g_j and g_k. Then

$$g'=g+(g_k-g_j)(N^{ed+k}-N^k)=(g_k-g_j)N^k(N^{ed}-1)\equiv g \pmod{N^d-1}.$$

Thus the distribution of pairs (g_0,g_j) is the same as the distribution of pairs (g_0,g_k). It follows that

$$S=(N^d-1)T\sum_{j=0}^{T-1}U_j+T^2=(N^d-1)T\left(D+(T/d-1)U_d+T/d\sum_{j=1}^{d-1}U_j\right)+T^2.(7)$$

Suppose that $1\le j\le d-1$. For given g_0 and g_j we want to know the number of choices of the remaining g_ks that make g a multiple of N^d-1. For a given g let $x=g_0+g_1N+\cdots+g_{d-1}N^{d-1}$ and $y=g_d+g_{d+1}N+\cdots+g_{T-1}N^{T-1-d}$, so that $g=x+N^dy$. Thus $0\le y<N^{T-d}$. Let

$$V_x=\{y: N^d-1|x+N^dy \text{ and } 0\le y<N^{T-d}\}.$$

and let $E=(N^{T-d}-1)/(N^d-1)$. Fix x. Then $|\{y:0\le y<N^{T-d}\}|=E(N^d-1)+1$, so $|V_x|=E+1$ if $0\in V_x$, and $|V_x|=E$ otherwise. Since $0\le x<N^d$, $0\in V_x$ if and only if N^d-1 divides x, and this holds if and only if $x=0$ or $x=N^d-1$. For fixed g_0 and g_j, the remaining coefficients of x are arbitrary, unless $g_0=g_j=N-1$, in which case we cannot have all $g_i=N-1$. Thus if $(g_0,g_j)\ne(0,0)$, then the number of g with $N^d-1|g$ is $N^{d-2}E$. If $(g_0,g_j)=(0,0)$, then the number of g with $N^d-1|g$ is $N^{d-2}E+1$. It follows that $U_j=1$.

Now let $j=d$ and recall that $T=md$. First suppose that $m\ge 3$. For a given g let $x=g_0+g_1N+\cdots+g_{2d-1}N^{2d-1}$ and $y=g_{2d}+g_{2d+1}N+\cdots+g_{T-1}N^{t-1-2d}$, so that $g=x+N^{2d}y$. Thus $0\le y<N^{T-2d}$. Let

$$W_x=\{y: N^d-1|x+N^{2d}y \text{ and } 0\le y<N^{T-2d}\}.$$

and let $F=(N^{T-2d}-1)/(N^d-1)$. Fix x. Then $|\{y:0\le y<N^{T-2d}\}|=F(N^d-1)+1$, so $|V_x|=F+1$ if $0\in W_x$, and $|W_x|=F$ otherwise. Since $0\le x<N^{2d}$, $0\in W_x$ if and only if N^d-1 divides x. We next see when this occurs. Let $x'=(g_0+g_d)+(g_1+g_{d+1})N+\cdots+(g_{d-1}+g_{2d-1})N^{d-1}$. Then $N^d-1|x$ if and only if

$N^d-1|x'$. However $0 \le x' \le 2(N^d-1)$, so if $N^d-1|x'$ then $x' \in \{0, N^d-1, 2(N^d-1)\}$. If $x=0$, then $g_0=g_d=0$ and there is only one choice of the remaining g_i, $i<2d$ with $N^d-1|x$. If $x=2(N^d-1)$, then $g_0=g_d=N-1$. We would need all $g_i=N-1$, $i=0,\cdots,2d-1$, to have $N^d-1|x$. As before, we cannot have all $g_i=N-1$ since $g<N^T-1$. If $x=N^d-1$, then $g_0+g_d=N-1$ and we can choose the remaining g_i, $i<2d$ in any way with $g_i+g_{i+d}=N-1$. There are N^{d-1} such choices for each g_0 and $g_d=N-1-g_0$. Thus in we have

$$\begin{aligned} U_d &= 1+N^{d-1}\sum_{g_0=0}^{N-1}\zeta^{g_0-(N-1-g_0)} \\ &= 1+N^{d-1}\zeta\sum_{g_0=0}^{N-1}\zeta^{2g_0} \\ &= \begin{cases} 1-N^d & \text{if } N=2 \\ 1 & \text{otherwise,}\end{cases} \end{aligned}$$

since ζ^2 is a nontrivial root of 1 unless $N=2$.

Finally, let $m=2$. Let $x=(g_0+g_d)+g_1N+\cdots+g_{d-1}N^{d-1}$ and $y=g_{d+1}+g_{d+2}N+\cdots+g_{2d-1}N^{d-2}$. Thus $0\le y<N^{d-1}$. As above, N^d-1 divides g if and only if it divides $x+Ny$. The bounds on y imply that for each fixed x there is at most one y with N^d-1 dividing $x+Ny$. We want to know for which x there is one such y. That is, for which x there is a $y\in\{0,1,\cdots,N^{d-1}-1\}$ with $x\equiv -Ny \pmod{N^d-1}$. We have $y\in\{0,1,\cdots,N^{d-1}-1\}$ if and only if $Ny\in\{0,N,\cdots,N^d-N\}$ if and only if $-Ny \pmod{N^d-1}\in\{0,N^d-1-N,\cdots,N-1\}$. We also have $0\le x\le N^d+N-2$. If $0\le x\le N^d-2$, then we must have $x\in\{0,N^d-1-N,\cdots,N-1\}$. The first possibility is $x=0$, whence $g_0=g_1=\cdots=g_d=0$. Each of the remaining elements of this set are congruent to $N-1$ modulo N, so each has $g_0+g_d=N-1$. So for each choice of g_0 there are $N^{d-1}-1$ values of $x<N^d-1$ with $g_d=N-1-g_0$ for which there is a y with N^d-1 dividing $x+Ny$. If $N^d-1\le x\le N^d+N-2$, Then we must have $x-(N^d-1)\in\{0,N^d-1-N,\cdots,N-1\}$. That is, $x=N^d-1$ or $x\in\{2(N^d-1)-N,\cdots,N^d+N-2\}$. In the latter case this means $x=N^d+N-2$. If $x=N^d-1$, then $g_0+g_d=N-1$ and $g_1=\cdots=g_{d-1}=N-1$, so we get one additional g with $g_0+g_d=N-1$. If $x=N^d+N-2$, then $g_0=\cdots=g_d=N-1$, but as before this makes g too large. It follows that U_d takes the same values as when $m\ge 3$.

Combining all this we see that

$$S=\begin{cases}(N^d-1)T(D+T-1)+T^2=N^TT+N^d(T^2-T) & \text{if } N\neq 2\\ (N^d-1)T(D+T-N^d(T/d-1)-1)+T^2 & \text{if } N=2.\end{cases}$$

The theorem follows. □

Corollary 14. *Let $\tau\in\mathbb{Z}$, $d=\gcd(T,\tau)$, and $D=(N^T-1)/(N^d-1)$. The variance of the arithmetic autocorrelation with shift τ, averaged over all sequences* **a** *of period*

T is

$$V[\mathcal{A}^A_{\mathbf{a}}(\tau)^2] = \begin{cases} T + \dfrac{T^2 - T}{N^{T-d}} - \dfrac{T^2}{N^{2(T-d)}} & \textit{if } N \neq 2 \\ T + \dfrac{T^2 - T - (N^d - 1)(T/d - 1)}{N^{T-d}} - \dfrac{T^2}{N^{2(T-d)}} & \textit{if } N = 2. \end{cases}$$

Theorem 15. *For any shift τ, the second moment of the arithmetic cross-correlation, averaged over all pairs of sequences* $\mathbf{a}$ *and* $\mathbf{b}$ *is*

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau)^2] = T\frac{N^T + 1 - T}{N^T}.$$

The variance is

$$V_{\mathbf{a},\mathbf{b}}[\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau)] = T\frac{(N^T+1)(N^T-T)}{N^{2T}}.$$

Proof. As in the computation of the expectation, we can reduce to the case when $\tau = 0$. We let

$$P = \sum_{f,g=0}^{N^T-1} \left| Z\left(\frac{(g-f) \pmod{N^T-1}}{N^T-1}\right)\right|^2,$$

so that the second moment is P/N^{2T}. We proceed by determining the number of pairs f, g with

$$g - f \equiv -h \pmod{N^T - 1} \quad \text{and} \quad 0 \leq f, g \leq N^T - 1 \tag{8}$$

for each h with $0 \leq h \leq N^T - 1$. As we have seen, if $h = N^T - 1$, then equation (8) only holds for $g = 0$ and $f = N^T - 1$. Let $h < N^T - 1$. For every $f < N^T - 1$ there is exactly one $g < N^T - 1$ satisfying equation (8), namely $f - h \pmod{N^T - 1}$. For $g = N^T - 1$ there is one $f < N^T - 1$ satisfying equation (8), namely $f = h$. For $f = N^T - 1$ there is one g with $1 \leq g \leq N^T - 1$ satisfying equation (8), namely $g = N^T - 1 - h$. This accounts for all choices of f and g, and we see that for $0 \leq h < N^T - 1$ there are $N^T + 1$ pairs f, g satisfying equation (8), and for $h = N^T - 1$ there is one such pair.

Let us first compute as if all h occurred equally often. We switch to thinking about N-ary T-tuples $\mathbf{h} = (h_0, h_1, \cdots, h_{T-1})$ representing single periods. If each h occurred $N^T + 1$ times, then each $\mathbf{h}$ would occur $N^T + 1$ times as single periods of $-h/(N^t - 1)$s. This would give a total contribution to P of

$$\begin{aligned} (N^T+1)\sum_{\mathbf{h}}\left|\sum_{i=0}^{T-1}\zeta^{h_i}\right|^2 &= (N^T+1)\sum_{\mathbf{h}}\sum_{i=0}^{T-1}\sum_{j=0}^{T-1}\zeta^{h_i-h_j} \\ &= (N^T+1)\sum_{i=0}^{T-1}\sum_{\mathbf{h}}\zeta^{h_i-h_i} + (N^T+1)\sum_{i\neq j}\sum_{\mathbf{h}}\zeta^{h_i-h_j} \\ &= TN^T(N^T+1) + (N^T+1)\sum_{i\neq j}N^{T-2}\sum_{h_i,h_j}\zeta^{h_i-h_j} \end{aligned}$$

$$= TN^T(N^T+1).$$

But we have over counted since the T-tuple $\mathbf{h} = (N-1, N-1, \cdots, N-1)$, corresponding to the N-adic number -1 and the numerator $h = N^T - 1$, only occurs once. For this value of h we have $|Z(-1)|^2 = T^2$, so in fact

$$P = TN^T(N^T+1) - T^2N^T = TN^T(N^T+1-T).$$

It follows that

$$E_{\mathbf{a},\mathbf{b}}[\mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau)^2] = \frac{P}{N^{2T}} = T\frac{N^T+1-T}{N^T}$$

as claimed. The claimed value of the variance follows. □

6. Expected Arithmetic Autocorrelation of a Fixed Binary Sequence

In this section we fix a binary sequence and find the expected arithmetic autocorrelation, averaged over all shifts. This time the answer is very different from that in the classical case. We let $\mathbf{a}$ be a periodic N-ary sequence with period T and associated N-adic number $-f/(N^T-1)$.

As in Section 5 if we let

$$S = \sum_{\tau=0}^{T-1} Z\left(\frac{(N^{T-\tau}-1)f}{N^T-1} - c_{f,\tau}\right).$$

then from equation (4) the expected arithmetic autocorrelation is $E_\tau[\mathcal{A}^A_{\mathbf{a}}(\tau)] = S/T$.

Theorem 16. *Suppose that the minimum period of* $\mathbf{a}$ *is* T *and* $\tau \not\equiv 0 \pmod{T}$. *Then*

$$Z\left(\frac{(N^{\tau}-1)f}{N^T-1} - c_{f,T-\tau}\right) = -Z\left(\frac{(N^{T-\tau}-1)f}{N^T-1} - c_{f,\tau}\right).$$

Proof. Note that if w is a rational but is not an integer, then for any integer c the eventual periodic part of w is the same as the eventual periodic part of $w+c$ and is the same as the eventual periodic part of Nw. Also, it is the bit-wise complement of the eventual periodic part of $-w$.

Let $d = \gcd(T,\tau) = \gcd(T, T-\tau) < T$. We claim that $(N^{T-\tau}-1)f/(N^T-1)$ is not an integer. Suppose to the contrary that it is an integer. Then $(N^T-1)/(N^d-1)$ divides f, say

$$f = \frac{N^T-1}{N^d-1}g,$$

with $g \in \mathbb{Z}$. It follows that

$$\frac{-f}{N^T-1} = \frac{-g}{N^d-1},$$

from which it follows that $\mathbf{a}$ has period dividing $d < T$, a contradiction. Similarly, $(N^{\tau}-1)f/(N^T-1)$ is not an integer.

From this we see that

$$\begin{aligned} Z\left(\frac{(N^{T-\tau}-1)f}{N^T-1} - c_{f,\tau}\right) &= Z\left(\frac{(N^{T-\tau}-1)f}{N^T-1}\right) \\ &= Z\left(N^{T-\tau}\frac{(1-N^{\tau})f}{N^T-1}\right) \\ &= Z\left(-\frac{(N^{\tau}-1)f}{N^T-1}\right) \\ &= -Z\left(\frac{(N^{\tau}-1)f}{N^T-1}\right) \\ &= -Z\left(\frac{(N^{\tau}-1)f}{N^T-1} - c_{f,T-\tau}\right), \end{aligned}$$

as we claimed. □

It follows that in his case for any $\tau \not\equiv 0, T/2 \pmod{T}$, the contribution to S from the τth term plus the contribution from the $(T-\tau)$th term equals zero. The contribution from the $(T/2)$th term equals its own negative, so is zero. The contribution from the 0th term is the period T, so $S = T$. More generally, we have the following.

Theorem 17. *Let* $\mathbf{a}$ *be a sequence with minimal period* T' *dividing* T*. then* $E_{\tau}[\mathcal{A}^A_{\mathbf{a}}(\tau)] = T/T'$*.*

Proof. Let us denote the S obtained by thinking of $\mathbf{a}$ as a period T sequence by S_T and the S obtained by thinking of it as a period T' sequence as $S_{T'}$. By the discussion above, $S_{T'} = T'$.

When we treat $\mathbf{a}$ as a sequence of period T, it consists of T/T' copies of its minimal period. Thus for any shift τ modulo T, the arithmetic autocorrelation with shift τ of $\mathbf{a}$ as a period T sequence is T/T' times the autocorrelation as a period T' sequence with shift τ modulo T'. Moreover, each shift modulo T' corresponds to T/T' shifts modulo T. Thus

$$S_T = \left(\frac{T}{T'}\right)^2 S_{T'} = \frac{T^2}{T'}.$$

It follows that $E_{\tau}[\mathcal{A}^A_{\mathbf{a}}(\tau)] = T/T'$ as claimed. □

7. Conclusions

We have analyzed the autocorrelations of ℓ-sequences, where we saw that all the shifted autocorrelations are small. We have analyzed the expected arithmetic auto- and cross-corellations for fixed shifts which we saw are similar to the expectations in the classical (no carry) case – the expected values are close to zero, and the second moments are close to the period.

We have also considered the expected correlations for a fixed sequence or pair of sequences. We have described the expected arithmetic autocorrelations only for binary sequences. Here we find that the arithmetic case is very different from the classical case. We leave as an open problem the determination of the expected arithmetic cross-correlation of fixed sequences and the expected arithmetic autocorrelation of a fixed non-binary sequence.

References

[1] S. Golomb, *Shift Register Sequences.* Aegean Park Press, Laguna Hills CA, 1982.

[2] M. Goresky and A. Klapper, Arithmetic Cross-Correlations of FCSR Sequences, *IEEE Trans. Info. Theory.* **43** (1997) pp. 1342-1346.

[3] M. Goresky and A. Klapper, Periodicity and Correlations of of d-FCSR Sequences. Designs, Codes, and Crypt. **33** (2004) 123-148.

[4] M. Goresky and A. Klapper, Some Results on the Arithmetic Correlation of Sequences (Extended Abstract), in M. Parker, A. Pott, and A. Winterhof, eds., *Sequences and Their Applications - SETA 2008, Lecture Notes in Computer Science* **5203** (2008) 71-80.

[5] A. Klapper and M. Goresky, Feedback Shift Registers, Combiners with Memory, and 2-Adic Span, *Journal of Cryptology* **10** (1997) pp. 111-147.

[6] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions.* Graduate Texts in Mathematics Vol. 58, Springer Verlag, N. Y. 1984.

[7] S. Lang, *Algebra.* Addison-Wesley, Reading, MA, 1971.

[8] D. Mandelbaum, Arithmetic codes with large distance. *IEEE Trans. Info. Theory,* vol. IT-13, 1967 pp. 237-242.

[9] T. R. N. Rao, *Error Coding For Arithmetic Processors*, Academic Press, New York N. Y., 1974.

[10] L. R. Welch, Lower bounds on the maximum correlation of signals, *IEEE Trans. Info. Theory* **IT–20** (1974), 397–399.