Some Results on the Arithmetic Correlation of Sequences

Mark Goresky[*] Andrew Klapper[†]

Abstract

In this paper we study various properties of arithmetic correlations of sequences. Arithmetic correlations are the with-carry analogs of classical correlations. Here 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. We study sequences with the arithmetic shift and add property, showing that they are exactly the ℓ-sequences with prime connection element.

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

1 Introduction

Sequences with good correlation properties are essential ingredients in a wide range of applications including CDMA systems and radar ranging. On the plus side, a great deal is known about the design and generation of sequences with good correlation properties. Unfortunately, we also know that there are fundamental limits on the sizes of families of sequences with such properties.

[*] School of Mathematics, Institute for Advanced Study

[†] Dept. of Computer Science, University of Kentucky. Parts of this work were carried out while the author visited the Fields Inst. at the University of Toronto; The Inst. for Advanced Study; and Princeton Universiy. This material is based upon work supported by the National Science Foundation under Grant No. CCF-0514660. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

The purpose of this paper is to study properties of an arithmetic or "with-carry" analog of the classical correlation function. This 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 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 [4, 5, 7, 8]. The arithmetic autocorrelations of these sequences were previously studied in the context of arithmetic coding [10, 11]. 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. Finally, we define a notion of arithmetic shift and add sequence, generalizing the classical notion of shift and add sequence [1, 2, 3, 6], and prove that the arithmetic shift and add sequences are exactly the ℓ-sequences with prime connection integer.

2 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 [8, 9]. 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. 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.*

For any N-ary sequence $\mathbf{b}$, let $\mathbf{b}^\tau$ be the sequence formed by shifting $\mathbf{b}$ by τ positions, $b_i^\tau = b_{i+\tau}$. 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 $\mathbf{b}$ [2]. The arithmetic cross-correlation is the with-carry analog of this [4].

Definition 2 *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*

$$\mathcal{C}^{A}_{\mathbf{a},\mathbf{b}}(\tau) = Z(a - b^{(\tau)}), \tag{1}$$

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.

3 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, $\text{ord}_q(N)$, 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 [7].

Theorem 3 *Suppose the* $\mathbf{a}$ *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 4 *Let* **a** *be an* N*-ary* ℓ*-sequence based on a connection integer* $q = p^e$*,* p *prime,* $e \geq 1$*. Then*

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

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

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

Theorem 5 *Let* **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* $q \equiv 1 \mod N$*, then* $\mathcal{A}^A_{\mathbf{a}}(\tau) = 0$*. This last statement holds when* $N = 2$*.*

Proof: The N-adic number associated with **a** is a fraction $-f/q$ as above. By an argument similar to the one in Section 3.1, the arithmetic autocorrelation of **a** with shift τ is the imbalance of the rational number

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

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 4. □

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.

3.1 Expected Arithmetic Correlations

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 leave the problem of computing second moments and variances of the arithmetic autocorrelations as open problems.

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 **a** of rational numbers of the form

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

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

Lemma 6 *If a and b are distinct N-adic numbers whose coefficient sequences are periodic with period T, and $a - b \in \mathbb{Z}$, then $\{a, b\} = \{0, -1\}$.*

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 $0 \le c_{f,\tau} < N^{T-\tau}$ 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

$$\begin{aligned} \mathcal{C}^A_{\mathbf{a},\mathbf{b}}(\tau) &= Z\left(\frac{-f}{N^T - 1} - \left(c_{g,\tau} + \frac{-N^{T-\tau} g}{N^T - 1}\right)\right) \\ &= Z\left(\frac{N^{T-\tau} g - f}{N^T - 1} - c_{g,\tau}\right). \end{aligned} \tag{2}$$

Theorem 7 *For any τ, the expected arithmetic autocorrelation, averaged over all sequences $\mathbf{a}$ of period T, is*

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

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

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

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 6 $a - b^{(\tau)}$ 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 (2) that the expected arithmetic autocorrelation is $E[\mathcal{A}^A_{\mathbf{a}}(\tau)] = S/N^T$.

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

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

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 $d = \gcd(T, T-\tau) = \gcd(T, \tau)$. Then $\gcd(N^T-1, N^{T-\tau}-1) = N^d-1$. Then the set of elements of the form $(N^{T-\tau}-1)f \mod N^T-1$ is the same as the set of elements of the form $(N^d-1)f \mod N^T-1$. Thus

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

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 $(N^d-1)f \mod N^T-1 = (N^d-1)u \mod N^T-1 = (N^d-1)u - (N^T-1)$. Thus

$$\frac{(N^d-1)f \mod N^T-1}{N^T-1} = \frac{(N^d-1)u}{N^T-1} - 1. \qquad (3)$$

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 (3) modulo N. We have

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

Since $-(1 + N^d + N^{2d} + \cdots + N^{T-d}) \leq -u - 1 \leq -2$, 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

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

The derivation of the expected arithmetic cross-correlation uses similar methods. □

Theorem 8 *For any shift τ, the second moment of the arithmetic cross-correlation, averaged over all pairs of sequences* **a** *and* **b** *is*

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

The variance is

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

Proof: The proof uses methods similar to those used in the proof of Theorem 7. □

4 Computing Arithmetic Cross-correlations

If **b** and **c** are two periodic sequences with associated N-adic numbers b and c, respectively, then the sequence associated with the difference $b - c$ may not be strictly periodic (although it must be eventually periodic). Thus at first glance computing the arithmetic cross-correlation of two sequences is problematic. How many symbols of the difference must be computed before we reach the periodic part? As it turns out, however, the number of symbols needed is well bounded.

Proposition 9 *Let* $\mathbf{b}$ *and* $\mathbf{c}$ *be periodic sequences with period* T. *Let* b *and* c *be the* N*-adic numbers associated with* $\mathbf{b}$ *and* $\mathbf{c}$. *Let* $\mathbf{d} = d_0, d_1, \cdots$ *be the sequence associated with* $b - c$. *Then* $\mathbf{d}$ *is strictly periodic from at least* d_T *on.*

Proof: As noted earlier, the strict periodicity of $\mathbf{b}$ and $\mathbf{c}$ implies that there are integers g and h so that $b = -g/(N^T - 1)$, $c = -h/(N^T - 1)$, $0 \leq g \leq N^T - 1$, and $0 \leq h \leq N^T - 1$. Thus

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

We either have $-(N^T - 1) \leq h - g \leq 0$, in which case $b - c$ is periodic, or $-(N^T - 1) < h - g - 1 \leq 0$. In the latter case we just show that adding 1 to a period T sequence results in a sequence that is periodic from position T on. □

Consequently, the arithmetic cross-correlation of $\mathbf{b}$ and $\mathbf{c}$ can be computed by computing the first $2T$ bits of the difference $b - c$, and finding the imbalance of the last T of these $2T$ bits. This is a linear time computation in T (although not easily parallelizable as is the case with standard cross-correlations).

5 Arithmetic Shift and Add Sequences

It is natural to consider an arithmetic analog of the shift and add property. In this section we give some basic definitions and characterize the sequences satisfying the arithmetic shift and add property.

Let $N \geq 2$ be a natural number and let $\mathbf{a} = a_0, a_1, \cdots$ be an infinite N-ary sequence. Let

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

be the N-adic number associated with $\mathbf{a}$. As above, for any integer τ let $\mathbf{a}_\tau = a_\tau, a_{\tau+1}, \cdots$ be the left shift of $\mathbf{a}$ by τ positions and let $a^{(\tau)}$ be the N-adic number associated with $\mathbf{a}_\tau$. We shall sometimes refer to the left shift of an N-adic number a, meaning the N-adic number associated with the left shift of the coefficient sequence of $\mathbf{a}$

A first attempt would be to ask that the set of shifts of $\mathbf{a}$ be closed under N-adic addition. This is impossible for eventually periodic sequences — multiples of an N-adic number by distinct positive integers are distinct, so there are infinitely many such multiples. If the set of shifts were closed under addition, all these multiples of **a** would be shifts of **a**. But there are only finitely many distinct shifts of an eventually periodic sequence.

The solution is to concern ourselves only with the periodic part of the sum of two sequences, as we have done in defining arithmetic correlations.

Definition 10 *The sequence* **a** *is said to have the* arithmetic shift and add property *if for any shift $\tau \geq 0$, either (1) some left shift of $a + a^{(\tau)}$ is zero or (2) some left shift of $a + a^{(\tau)}$ equals* **a**. *That is, there is a τ' so that $(a + a^{(\tau)})^{(\tau')} = a$.*

We may similarly define the shift and subtract property.

It is helpful here to use rational representations of sequences. If **a** is periodic with minimal period T then for some q and f we have $a = f/q$ with $-q \leq f \leq 0$ and $\gcd(q, f) = 1$. Then a shift $\mathbf{a}_\tau$ of **a** also corresponds to a rational number of this form, say $a^{(\tau)} = f_\tau/q$. Moreover, there is an integer c_τ so that

$$a^{(\tau)} = c_\tau + N^{T-\tau}a.$$

Thus $f_\tau = c_\tau q + N^{T-\tau}f$. It follows that

$$f_\tau \equiv N^{T-\tau}f \mod q.$$

The set of integers

$$C_f = \{f, Nf \mod q, N^2 f \mod q, \cdots\}$$

is called the *fth cyclotomic coset modulo q relative to N* (the terms "modulo q" and "relative to N" may be omitted if q and/or N are understood). It follows that the set of numerators f_τ of the N-adic numbers associated with the cyclic shifts of **a** is the fth cyclotomic coset modulo q relative to N.

Now suppose that $(\mathbf{a}+\mathbf{a}_\tau)_{\tau'} = \mathbf{a}$. Let g/r be the rational representation of the N-adic number associated with $\mathbf{a} + \mathbf{a}_\tau$. Then

$$\frac{g}{r} = d + N^{\tau'}\frac{f}{q}$$

for some integer d. In particular, we can take $r = q$. Then $g = qd + N^{\tau'}f$. Thus $g \equiv N^{\tau'}f \mod q$, so that $-g$ is in the cyclotomic coset of f.

Theorem 11 *The periodic N-ary sequence* **a** *with associated N-adic number f/q with* $\gcd(q, f) = 1$ *has the arithmetic shift and add property if and only if $G = C_f \cup \{0\}$ is an additive subgroup of $\mathbb{Z}/(q)$.*

Proof Sketch: The proof amounts to showing that addition in G corresponds mod q to addition of the associated numerators of fractions, and that the integer multiple of q difference does not affect the periodic part. □

Corollary 12 *A sequence has the arithmetic shift and add property if and only if it has the arithmetic shift and subtract property.*

How can it be that $C_f \cup \{0\}$ is a subgroup of $\mathbb{Z}/(q)$? It implies, in particular, that $C_f \cup \{0\}$ is closed under multiplication by integers modulo q. If we take q and f so that $\gcd(f, q) = 1$, then for any integer g, $C_f \cup \{0\}$ is closed under multiplication by gf^{-1} modulo q, so that $g \in C_f \cup \{0\}$. That is, $C_f \cup \{0\} = \mathbb{Z}/(q)$, and so $C_f = \mathbb{Z}/(q) - \{0\}$. In particular, every nonzero element of $\mathbf{Z}/(q)$ is of the form $N^i f$, hence is a unit. Thus q is prime. Moreover, $1 \in C_f$, so that $(\mathbb{Z}/(q))^* = C_1 = \{N^i \mod q, i = 0, 1, \cdots, q-2\}$. That is, N is a primitive element modulo q.

Theorem 13 *A non-zero N-ary sequence has the arithmetic shift and add property if and only if it is an ℓ-sequence.*

6 Conclusions

We have analyzed the autocorrelations of ℓ-sequences and the expected arithmetic auto- and cross-corellations for fixed shift, and we have characterized arithmetic shift and add sequences. In all these cases the answers are similar to the answers in the classical (no carry) case.

Two problems are left open here. First, we have not computed the arithmetic cross-correlations of non-binary sequences. In the binary case, this is one instance where the answer in the arithmetic realm is radically different from the answer in the classical realm.

Second, we have not computed the second moment and variance of the arithmetic autocorrelation. This appears to be a much harder problem than computing the expected arithmetic auto- and cross-correlations or the second moment of the arithmetic cross-correlation.

References

[1] S. Blackburn, A Note on Sequences with the Shift and Add Property. Designs, Codes, and Crypt. **9** (1996) pp. 251-256.

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

[3] G. Gong, A. Di Porto, and W. Wolfowicz, Galois linear group sequences, *La Comm., Note Rec. Not.* **XLII**(1993), 83-89.

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

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

[6] M. Goresky and A. Klapper, Polynomial pseudo-noise sequences based on algebraic shift register sequences. *IEEE Trans. Info. Theory* **53** (2006) 1649-1662.

[7] A. Klapper and M. Goresky, Arithmetic cross-correlation of FCSR sequences, *IEEE Trans. Info. Theory,* **43** (1997) 1342-1346.

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

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

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

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