Periodicity, correlation, and distribution properties of d-FCSR sequences

Mark Goresky* Andrew Klapper†

October 27, 2000

Abstract

Statistical properties are studied for certain sequences based on the arithmetic of totally ramified extensions of the rational numbers. A simplified exponential representation is found. The arithmetic cross-correlations are shown in some cases to vanish identically. Bounds on the distribution of subsequences are found.

Key Words – Cross-correlations, 2-Adic Numbers, Binary Sequences, Number Field.

1 Introduction

Pseudorandom sequences have a wide array of uses in computer science and engineering including appications to spread spectrum communication systems, radar systems, signal synchronization, simulation, and cryptography. The pseudorandom sequences in a good family should (a) be easy to generate (possibly with hardware or software), (b) have good distribution properties which make them appear (statistically) to be "random", (c) have low crosscorrelation values so that each sequence may be separated from the others in the family, and (d) arise from some underlying algebraic structure so they can be analyzed using standard mathematical tools. (Of course other properties are desired as well, depending upon the application.) In this paper we continue the study begun in 1993 by the authors of a class of sequences based on the arithmetic of the p-adic numbers and their finite extensions [6] which enjoy all four of the above properties.

The simplest sequences of this type were described in terms of a class of efficient hardware generators called feedback with carry shift registers (or FCSRs). An FCSR is structurally similar to a linear feedback shift register (or LFSR), but whereas the analysis of LFSR sequences

*The Institute for Advanced Study, School of Mathematics, (www.math.ias.edu/~goresky/). Research partially supported by N.S.F. grant # 0002693.

†Dept. of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046 and the Institute for Advanced Study, School of Mathematics. E-mail: klapper@cs.uky.edu. Project sponsored by the National Science Foundation under grant # 9980429.

involves the algebra of power series with coefficients in $GF(2)$, the analysis of FCSR sequences involves the algebra of the p-adic numbers [9] (an elementary review of which is provided in [6]). The analysis of FCSR sequences led to the cryptanalysis of the stream cipher known as the summation combiner [14]. It was further shown that various desirable statistical properties hold for FCSR sequences (see below), in most cases paralleling properties of LFSR sequences. FCSR sequences were discovered independently in a slightly different context by [12], [13] who showed they were useful as (pseudo-) random number generators for simulations. The simplest p-ary FCSR sequences may be described by

$$a_i = Ap^{-i} \pmod{N} \pmod{p} \in \mathbf{Z}/(p) \tag{1}$$

where p and N are prime numbers for which p is a primitive root (cf §9) modulo N, where $A \in \mathbf{Z}/(N)$ and where $\pmod{N} \pmod{p}$ means that first the number $Ap^{-i} \in \mathbf{Z}/(N)$ is represented by an integer between 0 and $N-1$; then this integer is reduced modulo p. (For most applications, p will be 2.)

A wide variety of generalizations of FCSRs has been described. The case of interest in this paper, the d-FCSR, was described briefly in our papers [4] and [6]. It is the purpose of this paper to analyze these sequences. First we describe (Theorem 4.2) the output of a d-FCSR generator in terms of certain objects arising in algebraic number theory (namely, ramified extensions of the p-adic numbers). Then in Corollary 5.2 we show how these sequences can often (but not always) be described in terms of simple integer arithmetic:

$$a_i = Ab^i \pmod{N} \pmod{p} \tag{2}$$

for values of $b \in \mathbf{Z}/(N)$ other than $b = p^{-1}$.

A much more general class of pseudorandom generators which includes LFSRs, FCSRs, and d-FCSRs all as special cases, was described by Klapper and Xu [8]. These generators are called *algebraic feedback shift registers* or AFSRs. Many of the results in this paper are special cases of phenomena which occur for any AFSR, and some of these results were already described in [8]. The AFSR setting is the mathematically most natural setting in which to study shift register sequences. It also "explains" the many apparent similarities between the theory of LFSRs and the theory of FCSRs (and d-FCSRs). However in this paper we restrict our attention to the d-FCSRs. This paper is self-contained and does not rely on any results from [8].

In [5] we show how to build shift register hardware which will generate these d-FCSR sequences with given design parameters. However, in this paper we maintain a purely algebraic point of view and we will only tangentially refer to the relevant shift register hardware. The constructions in [5] depend heavily on this paper.

In the remaining sections our attention is restricted to the binary case, $p = 2$. The usual notion of cross-correlation (with shift τ) of two binary sequences $\mathbf{S}$ and $\mathbf{T}$ is the sum $\sum_i (-1)^{S_i + T_{i+\tau}}$. The addition in the exponent may be replaced by addition modulo 2. Hence the cross-correlation with shift τ may be thought of as the number of ones minus the number of zeros in one period of the sequence formed by adding $\mathbf{S}$ to the τ-shift of $\mathbf{T}$, bit by bit modulo 2. Recently [7] the authors considered a slightly different notion of cross-correlation between sequences: the *arithmetic cross-correlation* (with shift τ) of $\mathbf{S}$ and $\mathbf{T}$ is the number of ones minus the number of zeroes in one period of (the periodic part of) the sequence formed by adding $\mathbf{S}$ to the τ-shift of $\mathbf{T}$ *with carry*. When $\mathbf{S} = \mathbf{T}$ the arithmetic cross-correlation is called the *arithmetic autocorrelation*. It was (to the best of our knowledge) first considered by Mandelbaum [11] who showed that certain binary sequences (the codewords of the Barrows-Mandelbaum arithmetic code) have "ideal" arithmetic autocorrelations: they are zero for every nontrivial shift τ. The authors then showed [7] that certain families of FCSR sequences even have ideal arithmetic cross-correlations. That is, all the nontrivial arithmetic cross-correlations are identically zero. The sizes of these families are conjectured to be huge, on the basis of experimental evidence. In Section 9 we further extend these results to d-FCSR sequences: we consider the *d-arithmetic cross-correlation* of two binary sequences and show that certain families of d-FCSR sequences have ideal d-arithmetic cross-correlations. Results of this type contrast with the case of ordinary cross-correlations, where there are well known lower bounds on the minimal cross-correlations in families of a given size. For example, the maximum shifted cross-correlation in a family of M sequences of period N is at least $M^2\sqrt{(M-1)/(MN-1)}$ [16].

The FCSR (and d-FCSR) sequences include the codewords of the Barrows-Mandelbaum arithmetic codes as a special case. (We have previously referred to these as ℓ-sequences, in order to stress the analogy with m-sequences.) Like the Barrows-Mandelbaum codes, since they have ideal arithmetic autocorrelations (respectively, d-arithmetic autocorrelations), they may be used for synchronization [11]. However since they also have ideal (d-) arithmetic cross-correlations, our sequences may be used for simultaneous synchronization and identification in a multi-user environment.

To give a simple example, suppose a central dispatch (D) wishes to send individual messages to one of a number of possible clients $(R_1, R_2, \ldots, R_k)$. Choose a family of (FCSR or d-FCSR) sequences with at least k members; let N denote the period of each sequence in this family. Each client R_i is assigned a signature sequence $\mathbf{S_i}$ from the family. She monitors a common synchronization and identification channel on which D broadcasts a bitstream $\mathbf{T}$. At the n^{th} clock tick, the client R_i computes the (d-) arithmetic cross-correlation $\Theta_{\mathbf{S_i},\mathbf{T}}(n)$ between her signature sequence $\mathbf{S_i}$ and the current window of size N in the bitstream $\mathbf{T}$.

If the dispatcher D sends the i-th signature sequence $\mathbf{T} = \mathbf{S_i}$ on the common channel, the receiver R_i will compute a single large correlation value Θ exactly N clock ticks later, while the other clients will compute $\Theta_{\mathbf{S_j},\mathbf{T}}(m) = 0$ for all $j \neq i$ and for all shifts m. So the client R_i has been identified as the intended recipient and her receiver has been synchronized to the message.

Finally, it was shown in [6] that if the period of an FCSR sequence is maximal in a certain sense, then the distribution of subsequences of fixed length is nearly uniform (the numbers of occurrences of any two patterns of consecutive bits of fixed length differ by at most two). In Section 10 we obtain bounds in the d-FCSR case on the difference between the numbers of occurrences of any two such patterns.

Acknowledgements. The authors would like to thank the Institue for Advanced Study in Princeton N.J. for its hospitality and support while this paper was being written

2 Preliminaries

Let $p \geq 2$ and $d \geq 1$ be integers such that the polynomial $X^d - p$ is irreducible over the rational numbers $\mathbf{Q}$. This occurs precisely when p is not a kth power, for any prime number k dividing d [10, p. 221]. (In particular, it holds when p is prime, which will be the main case of interest.) Let $\pi \in \mathbf{C}$ be a root of this polynomial. The set of all linear combinations $\sum_{i=0}^{d-1} a_i \pi^i$ with $a_i \in \mathbf{Q}$ is denoted $\mathbf{Q}[\pi]$. It is a field under the obvious operations of addition and multiplication (using $\pi^d = p$), and every nonzero element has an inverse (note that $\pi^{-1} = \frac{1}{p}\pi^{d-1}$). It is a degree d (totally ramified) extension of the rational numbers $\mathbf{Q}$ and it is the smallest field extension of $\mathbf{Q}$ containing π. Having fixed $\pi \in \mathbf{C}$, we obtain an embedding $\mathbf{Q}[\pi] \subset \mathbf{C}$. However $\mathbf{Q}[\pi]$ actually admits d different embeddings into the complex numbers, $\sigma_i : \mathbf{Q}[\pi] \to \mathbf{C}$ which are determined by setting $\sigma_i(\pi) = \zeta^i \pi$ (for $0 \leq i \leq d-1$) where $\zeta \in \mathbf{C}$ is a primitive d-th root of unity.

Similarly define $\mathbf{Z}[\pi]$ to be the ring consisting of all expressions

$$u = \sum_{i=0}^{p-1} u_i \pi^i \tag{3}$$

with $u_i \in \mathbf{Z}$. It is an entire ring in which every prime ideal is maximal. Every element of $\mathbf{Q}[\pi]$ may be expressed as a fraction u/v with $u, v \in \mathbf{Z}[\pi]$. In other words, $\mathbf{Q}[\pi]$ is the fraction field of $\mathbf{Z}[\pi]$, and $\mathbf{Z}[\pi]$ is an "order" in $\mathbf{Q}[\pi]$ (although it does not necessarily coincide with the full ring of integers in $\mathbf{Q}[\pi]$, cf. [2]).

Let $(\pi) \subset \mathbf{Z}[\pi]$ denote the ideal generated by π. The inclusion $\mathbf{Z} \to \mathbf{Z}[\pi]$ induces an isomorphism of rings $\mathbf{Z}/(p) \cong \mathbf{Z}[\pi]/(\pi)$. If $u \in \mathbf{Z}[\pi]$ is given by (3) then we denote by $\bar{u}$ its image in $\mathbf{Z}[\pi]/(\pi)$; it becomes identified with the number $u_0 \pmod{p} \in \mathbf{Z}/(p)$ under this isomorphism. We shall often make (implicit) use of the vectorspace isomorphism

$$\tau : \mathbf{Q}[\pi] \to \mathbf{Q}^d \tag{4}$$

which is given by $\tau(\sum_{i=0}^{d-1} u_i \pi^i) = (u_0, u_1, \ldots, u_{d-1})$. Then $\tau(\mathbf{Z}[\pi]) = \mathbf{Z}^d$ which is a lattice in $\mathbf{Q}^d$.

The ring $\mathbf{Z}_\pi$ of π-adic integers consists of all (infinite) formal expressions $\alpha = a_0 + a_1\pi + a_2\pi^2 + \cdots$ with $0 \leq a_i \leq p-1$, with the obvious operations of addition and multiplication (also using $\pi^d = 2$). It is equal to the completion of the ring $\mathbf{Z}[\pi]$ at the ideal (π) generated by π. If $d = 1$ then $\pi = p$, $\mathbf{Z}[\pi] = \mathbf{Z}$, $\mathbf{Q}[\pi] = \mathbf{Q}$, and the π-adic integers are just the p-adic integers $\mathbf{Z}_p$. (See also §8.)

The π-adic integers $\mathbf{Z}_\pi$ contains both $\mathbf{Z}_p$ (the p-adic integers) and $\mathbf{Z}[\pi]$ as well as many elements of $\mathbf{Q}[\pi]$. More, precisely, we have the following proposition, whose proof is just the same as that of Theorem 2.1 in [6].

Proposition 2.1 *The π-adic integer $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$ (with $0 \le a_i \le p-1$) is in $\mathbf{Q}[\pi]$ if and only if its coefficient sequence $(a_0, a_1, a_2, \ldots)$ is eventually periodic. For any $u, q \in \mathbf{Z}[\pi]$, the fraction $u/q \in \mathbf{Q}[\pi]$ lies in $\mathbf{Z}_\pi$ if and only if the denominator $q = \sum_{i=0}^{d-1} q_i \pi^i$ (with $q_i \in \mathbf{Z}$) satisfies either of the following three equivalent conditions,*

- *q is invertible in $\mathbf{Z}_\pi$,*
- *the image of q in $\mathbf{Z}[\pi]/(\pi)$ is invertible, or*
- *q_0 is relatively prime to p.* □

In this case, we say that q is invertible mod π. The π-adic expansion

$$\frac{u}{q} = \sum_{i=0}^{\infty} a_i \pi^i \in \mathbf{Z}_\pi \tag{5}$$

(with $0 \le a_i \le p-1$) is then unique, and we refer to the (eventually periodic) sequence $a_0, a_1, \ldots$ as the *coefficient sequence* of u/q.

Definition 2.2 *A d-FCSR sequence is the (eventually periodic) coefficient sequence of the π-adic expansion (5) of any fraction u/q, where $u, q \in \mathbf{Z}[\pi]$ and where q is invertible mod π.*

The denominator $q \in \mathbf{Z}[\pi]$ is called the *connection number* of the sequence. The purpose of this paper is to describe the (pseudorandom) sequences which are obtained this way (Theorem 4.2 and Corollary 5.2), and to investigate their distribution (Theorem 10.2) and correlation (Theorem 9.2) properties. It is a remarkable fact that (when $p = 2$) such sequences may be generated using a simple shift register circuit whose feedback connections are determined by the choice of q and whose initial loading is determined by the choice of u. These circuits were first described in [4, 6] and are analyzed in [5] using the results of this paper. The reader is referred to these other papers for applications and implementations of d-FCSR sequences.

3 The Norm

As in §2 suppose that $X^d - p$ is irreducible over $\mathbf{Q}$ and that $\pi \in \mathbf{C}$ is a root of this polynomial. In our analysis a central role is played by the algebraic norm of the connection number. The norm $N(x) \in \mathbf{Q}$ of an element $x = \sum_{i=0}^{d-1} x_i \pi^i \in \mathbf{Q}[\pi]$ is defined to be the determinant of the linear transformation $f_x(y) = xy$ on the field $\mathbf{Q}[\pi]$ (when it is considered as a d-dimensional vectorspace over $\mathbf{Q}$). With respect to the basis $\{1, \pi, \pi^2, \ldots, \pi^{d-1}\}$ the matrix of f_x is given by

$$\begin{pmatrix} x_0 & px_{d-1} & \ldots & px_2 & px_1 \\ x_1 & x_0 & \ldots & px_3 & px_2 \\ & & \ldots & & \\ x_{d-1} & x_{d-2} & \ldots & x_1 & x_0 \end{pmatrix} \tag{6}$$

The norm can also be computed as follows. Let ζ be a primitive dth root of unity in the complex numbers and let $\sigma_i : \mathbf{Z}[\pi] \to \mathbf{C}$ be the above embedding defined by $\sigma_i(\pi) = \zeta^i \pi$. Then the norm of an element $x \in \mathbf{Q}[\pi]$ is the rational number

$$N(x) = \prod_{i=0}^{d-1} \sigma_i(x). \tag{7}$$

If $x \in \mathbf{Z}[\pi]$, then $N(x) \in \mathbf{Z}$ is an integer.

Lemma 3.1 *Let $q \in \mathbf{Z}[\pi]$ and let (q) denote the ideal in $\mathbf{Z}[\pi]$ generated by q. Then the absolute value $|N(q)|$ is equal to the number of elements in the quotient ring $\mathbf{Z}[\pi]/(q)$. The element $\delta = |N(q)|/q$ is in $\mathbf{Z}[\pi]$.*

Proof: The proof of the first statement is standard and follows from [2] Lemma 1, p. 125: If $N \subset M$ are torsion free abelian groups of rank n then the quotient M/N is finite and has cardinality equal to the absolute value of the determinant of any transition matrix from a basis of M to a basis of N. Take $M = \mathbf{Z}[\pi]$ with basis $\{1, \pi, \ldots, \pi^{d-1}\}$ and $N = (q)$ with basis $\{q, q\pi, \ldots, q\pi^{d-1}\}$. The transition matrix is that of the linear transformation $f_q(y) = qy$ whose determinant is also equal to the norm $N(q)$.

The second statement takes a bit more work. Let $q = \sum_{i=0}^{d-1} a_i \pi^i$ with $a_i \in \mathbf{Z}$. As in Section 2, let ζ be a primitive dth root of unity, so that by equation (7), we can write

$$\delta = \pm \prod_{j=1}^{d-1} \sigma_j(q) = \pm \prod_{j=1}^{d-1} \sum_{i=0}^{d-1} a_i \zeta^{ij} \pi^i.$$

For any multi-index $I = (i_1, i_2, \ldots, i_{d-1})$ (where $0 \le i_j \le d-1$), let $\mu(I) = E = (e_0, e_1, \ldots, e_{d-1})$ if for each j, the number of occurences of j in the components of I is exactly e_j. It follows that

$$\delta = \pm \sum_E \left(\sum_{I:\mu(I)=E} \zeta^{\sum_{j=1}^{d-1} j i_j} \right) \prod_{i=0}^{d-1} a_i^{e_i} \pi^{i e_i}$$

where the first sum is over all multi-indices $E = (e_0, e_1, \ldots, e_{d-1})$ such that $0 \le e_j \le d-1$ and $\sum e_j = d-1$. For each such multi-index E let

$$c_E(x) = \sum_{I:\mu(I)=E} x^{\sum_{j=1}^{d-1} j i_j}.$$

Since the a_i are integers, to prove the lemma it suffices to show that $c_E(\zeta)$ is an integer for each E. Note that q has now left the picture.

The element $c_E(\zeta)$ lies in the field $\mathbf{Q}[\zeta]$, which is a Galois extension of the rational numbers. For an integer k, let τ_k be the homomorphism on $\mathbf{Q}[\zeta]$ induced by $\tau_k(\zeta) = \zeta^k$. The Galois group $\mathrm{Gal}(\mathbf{Q}[\zeta]/\mathbf{Q})$ consists of all τ_k such that k is relatively prime to d [15, p. 195].

We claim that $c_E(\zeta)$ is a rational number. By Galois theory, to show this it suffices to show that $c_E(\tau_k(\zeta)) = c_E(\zeta)$ for every τ_k in the Galois group of $\mathbf{Q}[\zeta]$ over $\mathbf{Q}$. Let $k\ell \equiv 1 \pmod d$. For any multi-index $I = (i_1, \ldots, i_{d-1})$, let $i'_j = i_{\ell j}$, and $I' = (i'_1, \ldots, i'_{d-1})$ (here the index ℓj in $i_{\ell j}$ is taken modulo d). The mapping from I to I' is a permutation of the multi-indices I with $\mu(I) = E$. Thus

$$\begin{aligned} c_E(\zeta^k) &= \sum_{I:\mu(I)=E} \zeta^{\sum_{j=1}^{d-1} kji_j} \\ &= \sum_{I:\mu(I)=E} \zeta^{\sum_{j=1}^{d-1} ji_{\ell j}} \\ &= \sum_{I:\mu(I')=E} \zeta^{\sum_{j=1}^{d-1} ji'_j} \\ &= c_E(\zeta). \end{aligned}$$

This proves the claim.

Furthermore, $c_E(\zeta)$ is integral over $\mathbf{Z}$ (ζ is integral over $\mathbf{Z}$ since it is a root of the integral polynomial $x^d - 1$. The sum and product of integral elements are integral.) But the only elements of $\mathbf{Q}$ that are integral over $\mathbf{Z}$ are the integers. Thus $c_E(\zeta) \in \mathbf{Z}$, proving the lemma. $\square$

The second statement in Lemma 3.1 says that for any $q \in \mathbf{Z}[\pi]$ the norm $N(q)$ is divisible (in $\mathbf{Z}[\pi]$) by q. It follows that the composition $\mathbf{Z} \to \mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ induces a well-defined ring homomorphism

$$\psi : \mathbf{Z}/(N(q)) \to \mathbf{Z}[\pi]/(q).$$

Proposition 3.2 *Suppose that $(q) = (r)^t$ for some $r \in \mathbf{Z}[\pi]$ and $t \in \mathbf{Z}^+$, and that $N(r)$ is (an ordinary, or "rational") prime. Then $(r) \subset \mathbf{Z}[\pi]$ is a prime ideal, $N(q) = N(r)^t$, and the mapping $\psi : \mathbf{Z}/(N(q)) \to \mathbf{Z}[\pi]/(q)$ is an isomorphism.*

Proof: First consider the case $t = 1$. The ring homomorphism ψ is nontrivial since it takes 1 to 1. So its image is a sub-ring of $\mathbf{Z}/(N(q))$ which is a field, so ψ is surjective. Moreover the cardinality of $\mathbf{Z}[\pi]/(q)$ is $|N(q)|$ so ψ is an isomorphism.

Now we proceed by induction on t. For any s let us write $\psi = \psi_s : \mathbf{Z}/(N(r^s)) \to \mathbf{Z}[\pi]/(r^s)$. This induces a mapping between short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{Z}[\pi]/(r^{k-1}) & \xrightarrow{\cdot r} & \mathbf{Z}[\pi]/(r^k) & \longrightarrow & \mathbf{Z}[\pi]/(r) & \longrightarrow & 0 \\ & & \Big\uparrow \psi_{k-1} & & \Big\uparrow \psi_k & & \Big\uparrow \psi_1 & & \\ 0 & \longrightarrow & \mathbf{Z}/(N(r^{k-1})) & \xrightarrow{\cdot r} & \mathbf{Z}/(N(r^k)) & \longrightarrow & \mathbf{Z}/(N(r)) & \longrightarrow & 0 \end{array}$$

The horizontal maps are additive group homomorphisms giving short exact sequences. The vertical maps are ring homomorphisms. Since the vertical homomorphisms on the ends are isomorphisms by induction, the homomorphism in the middle must be a group isomorphism as well. But since it is also a ring homomorphism, it must be a ring isomorphism as well. Finally, the norm mapping is multiplicative so $N(r^t) = (N(r))^t$. This proves the proposition. $\square$

Proposition 3.2 says two things:

- If $u \in \mathbf{Z}[\pi]$ then there exists an integer $m \in \mathbf{Z}$ such that $m \equiv u \pmod{q}$. Moreover m may be chosen so that $0 \leq m < |N(q)|$.
- If $a, b \in \mathbf{Z}$ are integers, then $a \equiv b \pmod{N(q)}$ (as integers) if and only if $a \equiv b \pmod{q}$ (as elements of $\mathbf{Z}[\pi]$).

4 Periodicity

As in §2 assume that $X^d - p$ is irreducible over $\mathbf{Q}$ and that $\pi \in \mathbf{C}$ is a root. In this section we identify the fractions $u/q \in \mathbf{Q}[\pi]$ whose π-adic expansions exist and are strictly periodic. Fix $q = \sum_{i=0}^{d-1} q_i \pi^i \in \mathbf{Z}[\pi]$ which is invertible in $\mathbf{Z}_\pi$. (By Proposition 2.1 this means that $q_0 \pmod{p}$ is invertible in $\mathbf{Z}/(p)$.) Let $\delta = |N(q)|/q \in \mathbf{Z}[\pi]$.

Lemma 4.1 *Let $u \in \mathbf{Z}[\pi]$ and set $\delta u = \sum_{i=0}^{d-1} z_i \pi^i$ with $z_i \in \mathbf{Z}$. Then the π-adic expansion of u/q is strictly periodic if and only if $-|N(q)| \leq z_i \leq 0$.*

Proof: We can uniquely write $\delta u = \sum_{i=0}^{d-1} z_i \pi^i$ with $z_i \in \mathbf{Z}$. Then in $\mathbf{Q}[\pi]$,

$$\begin{aligned} \frac{u}{q} &= \frac{\delta u}{|N(q)|} \\ &= \sum_{i=0}^{d-1} \frac{z_i}{|N(q)|} \pi^i. \end{aligned}$$

It follows that the π-adic expansion of u/q is the interleaving of the p-adic expansions of the $z_i/|N(q)|$. Thus the former is strictly periodic if and only if each of the latter is strictly periodic. But the p-adic expansion of $z_i/|N(q)|$ is strictly periodic if and only if

$$-|N(q)| \leq z_i \leq 0.$$

(This fact is proven, for example, in [6] for the case $p = 2$ however the same proof works for general p.) The proposition follows. $\square$

Suppose that $q \in \mathbf{Z}[\pi]$ is invertible mod π (cf. Proposition 2.1). Define the (half open) parallelpiped for q to be

$$P = \left\{ \sum_{i=0}^{d-1} a_i q \pi^i \mid a_i \in \mathbf{Q} \text{ and } -1 < a_i \leq 0 \right\} \subset \mathbf{Q}[\pi]. \tag{8}$$

(The terminology refers to the fact that in equation (4) the image $\tau(P) \subset \mathbf{Q}^d$ is the parallepiped spanned by the vectors $-q,\ -q\pi,\ -q\pi^2,\ \ldots,\ -q\pi^{d-1}$). Define

$$\Delta = P \cap \mathbf{Z}[\pi]$$

to be the set of lattice points in this parallelepiped. Applying the projection to $\mathbf{Z}[\pi]/(q)$ gives a mapping

$$\phi : \Delta \to \mathbf{Z}[\pi]/(q). \tag{9}$$

As in [6, 4, 8] we have the following result.

Theorem 4.2 *If $q \in \mathbf{Z}[\pi]$ is invertible mod π then the mapping ϕ is a one to one correspondence. For any element $u \in \Delta$, the π-adic expansion*

$$\frac{u}{q} = \sum_{i=0}^{\infty} a_i \pi^i \tag{10}$$

of the fraction u/q is strictly periodic with

$$a_i = \bar{q}^{-1}\left(\pi^{-i}u \pmod{q}\right) \pmod{\pi}. \tag{11}$$

This last equation needs a bit of explanation. Using the fact that ϕ is a one to one correspondence, for any element $x \in \mathbf{Z}[\pi]/(q)$ define

$$x \pmod{\pi} = \phi^{-1}(x) \pmod{\pi} \in \mathbf{Z}[\pi]/(\pi) = \mathbf{Z}/(p), \tag{12}$$

meaning that we first lift x up to Δ and then reduce modulo π. The image of π in $\mathbf{Z}[\pi]/(q)$ is invertible, so the product $x = \pi^{-i}u$ is defined in $\mathbf{Z}[\pi]/(q)$. Hence

$$\pi^{-i}u \pmod{\pi} = \phi^{-1}(\pi^{-i}u \pmod{q}) \pmod{\pi}$$

is defined in $\mathbf{Z}/(p)$. Moreover, the element

$$\bar{q} = q \pmod{\pi} \in \mathbf{Z}[\pi]/(\pi) = \mathbf{Z}/(p)$$

is also invertible; by (6) it coincides with $q_0 \pmod{p}$. So the product (11) makes sense in $\mathbf{Z}/(p)$. We remark that the mapping (12), $\mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(p)$ is not a ring homomorphism and in fact it depends on the choice $\Delta \subset \mathbf{Z}[\pi]$ of a complete set of representatives for the elements of $\mathbf{Z}[\pi]/(q)$.

Proof: We need to show that the composition $\Delta \subset \mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ is one to one and surjective. The idea is that existence and uniqueness of representatives $\pmod{q}$ in P corresponds to existence and uniqueness $\pmod{|N(q)|}$ in the (half-open) hypercube

$$\delta P = \left\{ \sum_{i=0}^{d-1} a_i \pi^i \,|\, a_i \in \mathbf{Q} \text{ and } -|N(q)| < a_i \leq 0 \right\}$$

(the image of P under the linear map $\mathbf{Q}[\pi] \to \mathbf{Q}[\pi]$ which is given by multiplication by δ). First we verify surjectivity. For any $z \in \mathbf{Q}$ define $\hat{z} \in \mathbf{Q}$ to be the unique rational number such that $-|N(q)| < \hat{z} \leq 0$ and such that $z - \hat{z} = m|N(q)|$ for some integer m. If z is an integer then so is $\hat{z}$.

Now let $x \in \mathbf{Z}[\pi]$ be arbitrary, and write $\delta x = \sum_{i=0}^{d-1} x_i \pi^i$ for some integers x_i. Set $y = \sum_{i=0}^{d-1} \hat{x}_i \pi^i$. We claim that $\delta^{-1} y \in \Delta$ and that it is congruent to x modulo q. In fact,

$$\begin{aligned} x - \delta^{-1} y &= \delta^{-1}(\delta x - y) \\ &= \delta^{-1} \sum_{i=0}^{d-1} (x_i - \hat{x}_i)\pi^i \\ &= \delta^{-1} \sum_{i=0}^{d-1} m_i |N(q)| \pi^i \\ &= q \sum_{i=0}^{d-1} m_i \pi^i \end{aligned}$$

(for some integers m_i). This last expression is in $\mathbf{Z}[\pi]$, hence $\delta^{-1} y \in \mathbf{Z}[\pi]$. But $\delta^{-1} y$ is also in P, so $\delta^{-1} y \in \Delta$ and (again by the last expression) it is congruent to x modulo (q). To prove injectivity, suppose that $x, x' \in \Delta$ are congruent modulo (q). Then $x - x' = cq$ for some $c \in \mathbf{Z}[\pi]$, so $\delta x - \delta x' = c\delta q = c|N(q)|$. But both δx and $\delta x'$ lie in the half-open hypercube δP whose sides all have length $|N(q)|$. So no coordinate can differ by as much as $|N(q)|$, hence $c = 0$. The statement about strictly periodic π-adic expansions follows immediately from Lemma 4.1.

Now let us verify (11). The sequence $\{a_1, a_2, \ldots\}$ is also strictly periodic and corresponds to a π-adic integer $u'/q = \sum_{i=0}^{\infty} a_{i+1}\pi^i$ with the same denominator q (and with some numerator $u' \in \Delta$). Then

$$\frac{u'}{q}\pi = \frac{u}{q} - a_0 \quad \text{or} \quad u'\pi = u - a_0 q \in \mathbf{Z}[\pi]. \tag{13}$$

Reducing this equation mod π gives the first case of (11), $a_0 \equiv \bar{q}^{-1} u \pmod{\pi}$. (Since the element u is already in Δ it is not necessary to "lift" it.) Similarly,

$$a_1 \equiv \bar{q}^{-1} u' \pmod{\pi}. \tag{14}$$

Reducing (13) modulo q gives $u' \equiv \pi^{-1} u \pmod{q} \in \mathbf{Z}[\pi]/(q)$. Since $\phi : \Delta \to \mathbf{Z}[\pi]/(q)$ is a bijection, this element u' is the unique "lift" of the quantity $\pi^{-1} u \pmod{q} \in \mathbf{Z}[\pi]/(q)$. Substituting into (14) gives

$$a_1 = \bar{q}^{-1}(\pi^{-1} u) \pmod{q} \pmod{\pi}$$

where the operation $z \mapsto z \pmod{q} \pmod{\pi}$ means that first $z \in \mathbf{Z}[\pi]/(q)$ is lifted to $\Delta \subset \mathbf{Z}[\pi]$ then reduced modulo π. Now equation (11) follows by induction. $\square$

Remark. A *face* $F \subset P$ of the parallelepiped (8) is the set of points obtained by setting some of the coefficients $a_j = 0$. The set of lattice points $\Delta \cap F$ in any face correspond under equation

(9) to an additive subgroup of $\mathbf{Z}[\pi]/(q)$. If $N(q)$ is prime then there are no additive subgroups other than $\{0\}$. Hence, if $N(q)$ is prime, all the nonzero elements of Δ lie in the interior of the parallelepiped.

In order to reconcile the notation with that of [5] we briefly consider the special case $p = 2$. Then $\mathbf{Z}[\pi]/(\pi) = \mathbf{Z}/(2)$. If $q \in \mathbf{Z}[\pi]$ is invertible mod π (meaning that q_0 is odd) then $\bar{q}^{-1} = 1$. Let

$$P' = \left\{ \sum a_i q \pi^i \in \mathbf{Z}[\pi] \mid a_i \in \mathbf{Q} \text{ and } \mathbf{0 \le a_i < 1} \right\}$$

and set $\Delta' = P' \cap \mathbf{Z}[\pi]$. Then Δ' is the "negative" of Δ and, like Δ it is a complete set of representatives for the elements of $\mathbf{Z}[\pi]/(q)$, that is, the mapping

$$\phi' : \Delta' \to \mathbf{Z}[\pi]/(q)$$

(which is given by reduction modulo q) is a one-to-one correspondence. Fix $u \in \Delta$ and set $h = -u \in \Delta'$. Then Theorem 4.2 becomes:

Corollary 4.3 *Suppose that $d = 2$, that q is invertible mod π, and that $h \in \Delta'$. Then the π-adic expansion*

$$-h/q = \sum_{i=0}^{\infty} b_i \pi^i$$

of the fraction $-h/q$ is strictly periodic with

$$b_i = \pi^{-i} h \pmod{q} \pmod{\pi}$$

where the operation $z \pmod{q} \pmod{\pi}$ means that first the element $z \in \mathbf{Z}[\pi]/(q)$ is lifted to the complete set of representatives Δ', and then reduced modulo q. □

We now return to the general case. The following lemma will be used in the proof of Proposition 9.3 to analyze arithmetic correlations.

Lemma 4.4 *Suppose $x \in \Delta$. Then the representative of $-x$ modulo q in Δ is*

$$y = -q \frac{\pi^d - 1}{\pi - 1} - x.$$

Proof: The element x is in Δ if and only if each π-adic coordinate z_i of δx is between $-|N(q)|$ and 0. If this holds, then

$$-|N(q)| < -|N(q)| - z_i < 0.$$

But $-|N(q)| - z_i$ is the ith π-adic coordinate of $-|N(q)|(1 + \pi + \pi^2 + \cdots + \pi^{d-1}) - \delta x = \delta y$. Thus y is in Δ and is congruent to $-x$ modulo q. □

5 Elementary description of d-FCSR sequences

In most cases it is possible to describe the d-FCSR sequences in elementary terms (without reference to algebraic number fields). This is the first main result of the paper.

As in §2 and §3, suppose that $\pi^d = p$ and that $X^d - p$ is irreducible over $\mathbf{Q}$. Let $q \in \mathbf{Z}[\pi]$ and suppose that

- q is invertible in $\mathbf{Z}_\pi$,
- d is relatively prime to $N(q)$,
- $(q) = (r^t)$ for some $r \in \mathbf{Z}[\pi]$, and
- $N(r)$ is (a "rational", or ordinary) prime.

Recall that all these conditions are satisfied if p is prime and $N(q)$ is prime.

Let N denote $|N(q)|$. By Proposition 3.2 we have a natural isomorphism of rings, $\psi : \mathbf{Z}/(N) \to \mathbf{Z}[\pi]/(q)$. Each of these rings has a canonical set of representatives: let

$$S = \{0, -1, -2, \ldots, -(N-1)\} \subset \mathbf{Z}$$

and let $\Delta \subset \mathbf{Z}[\pi]$ be the parallelepiped as defined as in §4. Then S is a complete set of representatives for the elements of $\mathbf{Z}/(N)$ and Δ is a complete set of representatives for the elements of $\mathbf{Z}[\pi]/(q)$. By abuse of notation we shall also write $\psi : S \to \Delta$ for the resulting one-to-one correspondence. Set $\delta = \sum_{i=0}^{d-1} s_i \pi^i$.

Theorem 5.1 *Let $u \in \Delta$. Then in $\mathbf{Z}/(p)$,*

$$(\bar{q}^{-1}u) \pmod{\pi} = \overline{N(q)}^{-1}(s_0\psi^{-1}(u) \pmod{N}) \pmod{p}.$$

The left side of this equation makes sense since the image $\bar{q} \in \mathbf{Z}[\pi]/(\pi)$ of $q \in \mathbf{Z}[\pi]$ is invertible. On the right side of the equation, the element $\psi^{-1}(u) \in \mathbf{Z}/(N)$ is multiplied by $s_0 \pmod{N}$ then lifted to the set S of representatives. Then the result is reduced modulo p. The image $\overline{N(q)} \in \mathbf{Z}/(p)$ of $N(q) \in \mathbf{Z}$ is invertible, so the product on the right hand side makes sense. This result may be best explained in terms of the following two diagrams. Both the upper and lower squares in the first diagram commute. Although the upper square in the second diagram commutes, the lower square does not. Theorem 5.1 supplies "correction factors" which are needed in order to make it commute.

$$\begin{tikzcd}
\mathbf{Z}/(N) \arrow[r, "\psi"] & \mathbf{Z}[\pi]/(q) \\
\mathbf{Z} \arrow[u, "\text{mod N}"] \arrow[r] \arrow[d, "\text{mod p}"'] & \mathbf{Z}[\pi] \arrow[u, "\text{mod q}"'] \arrow[d, "\text{mod } \pi"] \\
\mathbf{Z}/(p) \arrow[r, "\cong"] & \mathbf{Z}[\pi]/(\pi)
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbf{Z}/(N) \arrow[r, "\psi"] & \mathbf{Z}[\pi]/(q) \\
S \arrow[u] \arrow[r, "\psi"] \arrow[d] & \Delta \arrow[u] \arrow[d] \\
\mathbf{Z}/(p) \arrow[r, "\cong"] & \mathbf{Z}[\pi]/(\pi)
\end{tikzcd}$$

Replacing u with $\bar{\pi}^{-i}u$ in Theorem 5.1 gives the following corollary which describes the d-FCSR sequence completely in terms of operations on ordinary integers.

Corollary 5.2 *Let $u \in \Delta$ and let $m = \psi^{-1}(\pi) \in \mathbf{Z}/(N)$. Write $u/q = \sum_{j=0}^{\infty} a_j \pi^j$ for the π-adic expansion of the fraction u/q. Then the coefficient sequence $a_0, a_1, \ldots$ is strictly periodic and moreover*

$$a_j = \bar{N}(q)^{-1}(Ab^i \pmod{N}) \pmod{p}$$

where $b = m^{-1}$ and $A = s_0\psi^{-1}(u) \in \mathbf{Z}/(N)$.

The proof of theorem 5.1 will occupy the next section.

6 Proof of theorem 5.1

Continue with the same notation as in §4, that is, $\pi^d = p$, $q \in \mathbf{Z}[\pi]$, $N = |N(q)|$, $\delta = N(q)/q = \sum_{i=0}^{d-1} s_i \pi^i$, and $m = \psi^{-1}(\pi) \in \mathbf{Z}/(N)$. Let $\zeta \in \mathbf{C}$ be a primitive d-th root of unity and let R denote any one of the following rings: $\mathbf{Z}, \mathbf{Z}[\pi], \mathbf{Z}[\zeta], \mathbf{Z}[\pi, \zeta]$. The integer $N \in \mathbf{Z}$ generates an ideal $(N)_R$ in the ring R. If $a, b \in \mathbf{Z}$ we write

$$a \equiv b \pmod{N} \text{ in } R$$

to mean that $a - b \in (N)_R$.

Lemma 6.1 *For any $a, b \in \mathbf{Z}$ we have*

$$a \equiv b \pmod{N} \textit{ in } R \iff a \equiv b \pmod{N} \textit{ in } \mathbf{Z}.$$

Proof: Both π and ζ are integral over $\mathbf{Z}$ so each $x \in R$ is integral over $\mathbf{Z}$. If $a \equiv b \pmod{N}$ in R, then $a - b = xN$ for some $x \in R$. Then $x = (a-b)/N$ is a rational number which is integral over $\mathbf{Z}$, hence $x \in \mathbf{Z}$. $\square$

Lemma 6.2 *The inclusion $\mathbf{Z}[\zeta] \to \mathbf{Z}[\pi, \zeta]$ induces a ring isomorphism*

$$\Psi : \mathbf{Z}[\zeta]/(N) \cong \mathbf{Z}[\pi, \zeta]/(q).$$

Proof: The proof is similar to that of Proposition 3.2. Since $q|N$ in $\mathbf{Z}[\pi, \zeta]$ the mapping Ψ is well defined. To see it is surjective it suffices to show that π is in the image of ϕ. But $\pi \equiv m \pmod{q}$ in $\mathbf{Z}[\pi]$, hence also in $\mathbf{Z}[\pi, \zeta]$, that is, $\Psi(m) = \pi$. Finally, the cardinality of both rings is $|N|^{\phi(d)}$ (where ϕ is the Euler totient function), hence Ψ is also injective. $\square$

Lemma 6.3 *Let $u \in \mathbf{Z}[\pi]$ and set $\delta u = \sum_{i=0}^{d} z_i \pi^i$. Then $z_k \pi^k \equiv z_0 \pmod{q}$ (in $\mathbf{Z}[\pi]$) and $z_k m^k \equiv z_0 \pmod{N}$ (in $\mathbf{Z}$) for all $k = 0, 1, \ldots, d$.*

Proof: Let $\hat{z}_j$ denote the j-th Fourier coefficient of the finite sequence of complex numbers

$$(z_0, z_1\pi, z_2\pi^2, \ldots z_{d-1}\pi^{d-1}),$$

which may be considered to be a function $f : \mathbf{Z}/(d) \to \mathbf{C}$. In other words, if $\zeta \in \mathbf{C}$ denotes a primitive d-th root of unity, then

$$\hat{z}_j = \sum_{i=0}^{d-1} z_i \pi^i \zeta^{ij}.$$

Evidently, the Fourier coefficient $\hat{z}_j$ lies in the ring $\mathbf{Z}[\pi, \zeta]$. The homomorphism $\sigma_j : \mathbf{Z}[\pi] \to \mathbf{C}$ may be extended to this ring by setting $\sigma_j(\zeta) = \zeta$. Then

$$\sigma_j(\delta) = \prod_{i \neq j} \sigma_i(q)$$

which implies that, in the ring $\mathbf{Z}[\pi, \zeta]$, the element $\sigma_j(\delta)$ is divisible by q, for $j = 1, 2, \ldots, d-1$. Hence

$$\begin{aligned} \hat{z}_j &= \sum_{i=0}^{d-1} z_i \pi^i \zeta^{ij} \\ &= \sigma_j(\delta u) \\ &= \sigma_j(\delta)\sigma_j(u) \\ &\equiv 0 \pmod{q}. \end{aligned}$$

The Fourier inversion formula gives

$$\begin{aligned} d z_k \pi^k &= \textstyle\sum_{j=0}^{d-1} \hat{z}_j \zeta^{-kj} \\ &\equiv \hat{z}_0 \pmod{q}, \end{aligned}$$

which is independent of k. Since d is invertible mod $N(q)$ it is also invertible in $\mathbf{Z}[\pi]/(q)$, meaning that $dx = 1 + yq$ for some $x, y \in \mathbf{Z}[\pi]$. Hence d is also invertible in $\mathbf{Z}[\pi, \zeta]/(q)$, which shows that

$$z_k \pi^k \equiv z_0 \pi^0 \pmod{q} \text{ in } \mathbf{Z}[\pi, \zeta]$$

for all k. We need to show the same holds in $\mathbf{Z}[\pi]$. However,

$$\begin{aligned} & z_k \pi^k \equiv z_0 \pmod{q} \text{ in } \mathbf{Z}[\pi, \zeta] \\ \Rightarrow\ & z_k m^k \equiv z_0 \pmod{q} \text{ in } \mathbf{Z}[\pi, \zeta] \\ \Rightarrow\ & z_k m^k \equiv z_0 \pmod{N} \text{ in } \mathbf{Z}[\zeta] \\ \Rightarrow\ & z_k m^k \equiv z_0 \pmod{N} \text{ in } \mathbf{Z} \\ \Rightarrow\ & z_k m^k \equiv z_0 \pmod{q} \text{ in } \mathbf{Z}[\pi] \\ \Rightarrow\ & z_k \pi^k \equiv z_0 \pmod{q} \text{ in } \mathbf{Z}[\pi] \end{aligned}$$

by Lemma (6.2), Lemma (6.1), and Proposition (3.2). □

6.1 Proof of theorem 5.1

As in the previous section set $\delta u = \sum_{k=0}^{d-1} z_k \pi^k$ and set $\delta = \sum_{k=0}^{d-1} s_k \pi^k$. Lemma 6.3 gives $\delta u \equiv dz_0 \pmod{q}$ and $\delta \equiv ds_0 \pmod{q}$, hence $dz_0 \equiv ds_0 u \pmod{q}$. Since d is invertible $\pmod{q}$, this implies $z_0 \equiv s_o u \pmod{q}$. The isomorphism $\psi^{-1} : \mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(N)$ is the identity on integers, so we obtain

$$z_0 = s_0 \psi^{-1}(u) \text{ in } \mathbf{Z}/(N).$$

Now lift these elements to the set $S \subset \mathbf{Z}$ of representatives of $\mathbf{Z}/(N)$ and reduce modulo p to obtain

$$z_0 \pmod{p} = (s_0 \psi^{-1}(u) \pmod{N}) \pmod{p}.$$

But $z_0 \pmod{p} = \delta u \pmod{\pi} \in \mathbf{Z}/(p)$. That is,

$$(\delta u) \pmod{\pi} = (s_0 \psi^{-1}(u) \pmod{N}) \pmod{p}.$$

Multiplying by $\bar{N(q)}^{-1} \in \mathbf{Z}/(p)$ gives

$$(\bar{q}^{-1} u) \pmod{\pi} = \bar{N(q)}^{-1} (s_0 \psi^{-1}(u) \pmod{N}) \pmod{p}$$

where $\bar{q} \in \mathbf{Z}[\pi]/(\pi)$ is the image of q, and where the right hand side is interpreted as follows: first compute $s_0\psi^{-1}(u) \in \mathbf{Z}/(N)$, then lift this to the set S of representatives, then reduce modulo p, then multiply by $\bar{N(q)}^{-1}$. This completes the proof of theorem 5.1. $\square$

7 Example

Consider a binary d-FCSR (meaning that $p = 2$) with $\pi^2 = 2$ (so $d = 2$) and with connection number $q \in \mathbf{Z}[\pi]$ which is invertible in $\mathbf{Z}_\pi$. Let $N = |N(q)|$. Then $\bar{N(q)}^{-1} = 1$ and Corollary 5.2 says that the strictly periodic portions of the d-FCSR sequence will be described by

$$a_j = Ab^j \pmod{N} \pmod{2}$$

for certain $A, b \in \mathbf{Z}/(N)$. Let us take $q = 5 + 2\pi$. Then $N(q) = 17$ which is prime, so the parallelogram contains 16 elements in its interior. It is illustrated in Figure 1.

The isomorphism $\psi : \mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(17)$ maps π to $m = 6$. Hence $m^{-1} = 3 \in \mathbf{Z}/(17)$ which is primitive, so we obtain a maximal length output sequence. The element $\delta = 5 - 2\pi$ hence $s_0 = 5$. Each element in $\mathbf{Z}[\pi]/(q)$ has a unique representative u in the parallelogram; these representatives are listed in the second column of the table in Figure 2. Each element in $\mathbf{Z}/(17)$ has a unique representative in the set $S = \{-1, -2, \ldots, -16\}$; these representatives h are listed in the third column. The correspondence between the second and third column is given by Theorem 5.1, that is, $h = s_0\psi^{-1}(u)$ (since $\bar{q} \equiv \bar{N}(q) \equiv 1 \pmod{2}$). The fourth column (which is the d-FCSR sequence under consideration) is the third column modulo 2, and it concides with the second column modulo π.

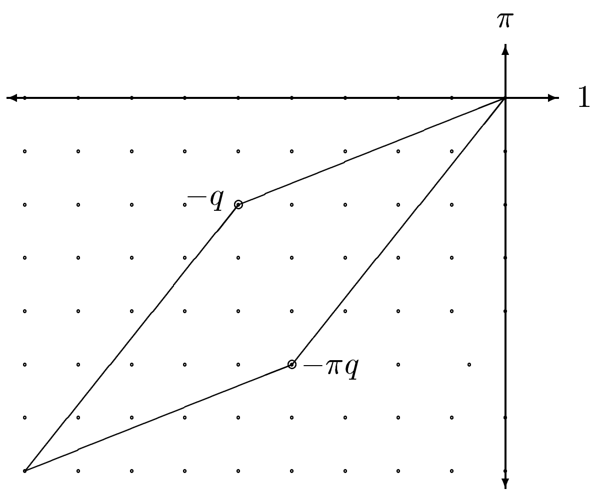

Figure 1. Parallelogram for $q = 5 + 2\pi$.

i	$\pi^{-i} \pmod q$	$5 \cdot 6^{-i} \pmod{17}$	output
0	$-4 - 2\pi$	-12	0
1	$-2 - 2\pi$	-2	0
2	$-2 - \pi$	-6	0
3	$-1 - \pi$	-1	1
4	$-3 - 3\pi$	-3	1
5	$-5 - 4\pi$	-9	1
6	$-6 - 5\pi$	-10	0
7	$-5 - 3\pi$	-13	1
8	$-5 - 5\pi$	-5	1
9	$-7 - 5\pi$	-15	1
10	$-7 - 6\pi$	-11	1
11	$-8 - 6\pi$	-16	0
12	$-6 - 4\pi$	-14	0
13	$-4 - 3\pi$	-8	0
14	$-3 - 2\pi$	-7	1
15	$-4 - 4\pi$	-4	0

Figure 2. Model states for $q = 5 + 2\pi$.

8 Arithmetic in $\mathbf{Z}_\pi$

The comments in this section will be needed for §9. As in §2, let $\pi^d = p$. A *p-ary sequence* $\mathbf{a} = a_0, a_1, \ldots$ is an infinite sequence of symbols with $0 \le a_i \le p - 1$. Such a sequence is the coefficient sequence of a unique π-adic integer

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i \in \mathbf{Z}_\pi.$$

Addition of π-adic integers $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$ and $\beta = \sum_{i=0}^{\infty} b_i \pi^i$ is accomplished by adding their coefficients symbol by symbol, using a "carry" operation which delays each carried bit d steps before adding it back in. In other words, if $\alpha + \beta = \sum_{i=0}^{\infty} e_i \pi^i$ with $0 \le e_i \le p-1$ then

$$a_i + b_i + c_i = e_i + pc_{i+d}$$

where c_i denotes the amount carried to the ith position. Since $c_0 = 0$, it follows immediately that c_i is either 0 or 1. Similarly the difference $\alpha - \beta = \sum_{i=0}^{\infty} f_i \pi^i$ is obtained by subtracting the coefficients symbol by symbol, using a "borrow" operation which is delayed d steps. The "borrow" operation is actually the same as the "carry" operation, but the carried quantity is negative, that is,

$$a_i - b_i + c_i = e_i + pc_{i+d}$$

from which it also follows immediately that the amount c_i to be carried to the ith place is either 0 or -1.

Even if the coefficient sequences of $\alpha, \beta \in \mathbf{Z}_\pi$ are strictly periodic of the same period, say L, the same is not necessarily true for the coefficient sequences of $\alpha \pm \beta$. Since the carries are delayed for d steps, the periodic part of $\alpha \pm \beta$ might begin only after d symbols have passed.

Lemma 8.1 *Let $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$ and $\beta = \sum_{i=0}^{\infty} b_i \pi^i$ be π-adic integers whose coefficient sequences are eventually periodic with period dividing L. Then the coefficient sequence of $\alpha \pm \beta$ is eventually periodic with period dividing L.*

Proof: (We consider the case of $\alpha - \beta$; the case of the sum is similar.) According to the preceding remarks it suffices to show that the sequence of carries $c_0, c_1, \ldots$ is eventually periodic with period dividing L. Suppose a carry occurs in the ith place, i.e. $c_i = -1$. This occurs if and only if for some positive $k \le i/d$ we have $a_{i-jd} = b_{i-jd}$ for $1 \le j \le k-1$, $a_{i-kd} = 0$, and $b_{i-kd} = 1$. But if this occurs then the same is true with i replaced by $i + rL$ for every positive integer r.

Thus there are two posibilities for any i. Either for all r there is no carry to position $i + rL$, or for r large enough there is a carry to position $i + sL$ for every $s \ge r$. Therefeore the sequence of carries has eventual period dividing L, and the lemma follows. $\square$

9 Arithmetic Correlations

In this section we consider only the binary case, $p = 2$. Recall [6] that a binary ℓ sequence is a periodic sequence of the form

$$a_i = A2^{-i} \pmod{N} \pmod{2}$$

where N is a prime number such that 2 is a primitive root modulo N, where $A \in \mathbf{Z}/(N)$, and where $\pmod N \pmod 2$ means that first $A2^{-i} \in \mathbf{Z}/(N)$ is represented as an integer between 0 and $N-1$, then this integer is reduced modulo 2. The sequence has period $N-1$. Different choices of A give different cyclic shifts of the same sequence.

As in §2 let $\pi^d = 2$, let $q \in \mathbf{Z}[\pi]$ and suppose that $(q) = (r^t)$ for some $r \in \mathbf{Z}[\pi]$ such that $n = N(r)$ is (an ordinary) prime number. (Then $N(q) = n^t$.) By Proposition 3.2, $\mathbf{Z}[\pi]/(q) \cong \mathbf{Z}/(N(q)) \cong \mathbf{Z}/(n^t)$. The group of invertible elements $\mathbf{Z}[\pi]/(q)^*$ in this ring is cyclic and has order $\phi(n^t) = n^{t-1}(n-1)$. In analogy with the simpler situation described in the preceding paragraph, we further assume that π is a primitive element in $\mathbf{Z}[\pi]/(q)$, meaning that the $n^{t-1}(n-1)$ different powers of π exactly account for the elements in $\mathbf{Z}[\pi]/(q)^*$. Fix $u \in \mathbf{Z}[\pi]/(q)^*$. We shall say that the resulting d-FCSR sequence,

$$a_i = u\pi^{-i} \pmod q \pmod \pi \tag{15}$$

is a *generalized ℓ-sequence* with connection number q. The sequence is periodic of period $n^{t-1}(n-1)$. Different choices of u give different cyclic shifts of the same sequence.

If $\mathbf{a} = a_0, a_1, \ldots$ is a binary sequence and $k \neq 0$ is an integer, then the sequence $\mathbf{b} = b_0, b_1, \ldots$ is said to be the *k-fold decimation* of $\mathbf{a}$ if $b_i = a_{di}$ for every i. Let $\mathbf{a}$ be a generalized ℓ-sequence. Let $\mathcal{F}_\mathbf{a}$ be the family of all k-fold decimations of $\mathbf{a}$, where $k \geq 1$ is allowed to vary over all integers which are relatively prime to the period of $\mathbf{a}$.

Let τ be a nonnegative integer. If $\mathbf{b} = b_0, b_1, \ldots$ is an infinite binary sequence, denote by $\mathbf{b}^\tau$ the shift of $\mathbf{b}$ by τ steps, that is, $b_i^\tau = b_{i+\tau}$. If $\beta = \sum_{i=0}^\infty b_i \pi^i$ is the π-adic integer corresponding to $\mathbf{b}$, let β_τ denote the π-adic integer corresponding to $\mathbf{b}^\tau$. That is,

$$\beta_\tau = \frac{1}{\pi^\tau}(b - b_0 - b_1\pi - \ldots - b_{\tau-1}\pi^{\tau-1}) = \sum_{i=0}^\infty b_{i+\tau}\pi^i.$$

Recall that the ordinary cross-correlation with shift τ of two binary sequences $\mathbf{a}$ and $\mathbf{b}$ of period L can be defined either as the sum $\sum_{i=1}^N (-1)^{s_i + t_{i+\tau}}$ or as 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 $\mathbf{b}$ [3]. The arithmetic cross-correlation is the with-carry analogue of the latter definition. The following definition makes sense, because of Lemma 8.1.

Definition 9.1 *Let $\mathbf{a}$ and $\mathbf{b}$ be two periodic binary sequences with period L, with corresponding π-adic integers $\alpha, \beta \in \mathbf{Z}_\pi$. Let $0 \leq \tau < L$. The* d-arithmetic cross-correlation with shift τ, *$\Theta_{\mathbf{a},\mathbf{b}}(\tau)$ of $\mathbf{a}$ and $\mathbf{b}$, is the number of zeros minus the number of ones in any periodic portion of length L of the coefficient sequence for $\alpha - \beta_\tau \in \mathbf{Z}_\pi$. When $\mathbf{a} = \mathbf{b}$, the d-arithmetic cross-correlation is called the* d-arithmetic autocorrelation *of $\mathbf{a}$.*

The sequences $\mathbf{a}, \mathbf{b}$ (of period L) are said to have *ideal d-arithmetic correlations* if,

$$\Theta_{\mathbf{a},\mathbf{b}}(\tau) = \begin{cases} L & \text{if } \mathbf{a} = \mathbf{b}^\tau \\ 0 & \text{otherwise} \end{cases}$$

for each τ with $0 \le \tau < L$. A family of sequences is said to have ideal d-arithmetic correlations if every pair of sequences in the family has ideal d-arithmetic correlations. The second main result in this paper is the following.

Theorem 9.2 *Let $\pi^d = 2$. Let $\mathbf{a}$ be a generalized ℓ-sequence with connection integer $q \in \mathbf{Z}[\pi]$. Suppose that $(q) = (r^t)$ for some $r \in \mathbf{Z}[\pi]$ such that $N(r)$ is prime. Suppose also that $\gcd(d, \phi(N(q))) = 1$. Then the family $\mathcal{F}_{\mathbf{a}}$ has ideal d-arithmetic correlations.*

Remarks. The last two hypotheses are satisfied automatically if $N(q)$ is prime. One would like to find families with ideal d-arithmetic correlations such that whenever $\mathbf{a}, \mathbf{b}$ are distinct elements in the family then $\mathbf{a}$ and $\mathbf{b}^\tau$ are distinct (for all τ), and such that whenever $\tau \ne 1$ then $\mathbf{a}$ and $\mathbf{a}^\tau$ are distinct. There is a certain amount of evidence that this happens quite often, cf. [7].

The remainder of this section consists of a proof of Theorem 9.2. We first need a constraint on the sequences that can occur as generalized ℓ-sequences.

Proposition 9.3 *Under the hypotheses of Theorem 9.2, the second half of one period of $\mathbf{a}$ is the bitwise complement of the first half.*

Proof: Since $\mathbf{Z}[\pi]/(q) \cong \mathbf{Z}/(N(q))$, we have that

$$\pi^{\phi(N(q))} \equiv 1 \pmod{q}.$$

That is,

$$q | \pi^{n^{t-1}(n-1)} - 1 = (\pi^{n^{t-1}(n-1)/2} - 1)(\pi^{n^{t-1}(n-1)/2} + 1).$$

These two factors differ by 2, so r can only divide one of them. Thus q divides exactly one of them. Since π is primitive modulo q, q cannot divide the first factor, hence it divides the second factor. It follows that $\pi^{\phi(N(q))/2} \equiv -1 \pmod{q}$.

By Corollary 5.2 we have

$$\begin{aligned} a_{i+\phi(N(q))/2} &= (zm^{-i-\phi(N(q))/2} \pmod{N(q)}) \pmod{2} \\ &= (-zm^{-i} \pmod{N(q)}) \pmod{2} \end{aligned}$$

for some z. By Lemma 4.4, if x is the element of Δ congruent to $-zm^{-i}$ modulo q, then the element of Δ that is congruent to $-zm^{-i}$ modulo q is

$$-q\frac{\pi^d - 1}{\pi - 1} - x \equiv 1 - x \pmod{2}.$$

That is,

$$a_{i+\phi(N(q))/2} = 1 - a_i,$$

which proves the proposition. □

The above property is extended to decimations of generalized ℓ-sequences by the following lemma.

Lemma 9.4 *Let* $\mathbf{a}$ *be a binary sequence of even period* L *whose second half is the complement of its first half. Let* $k > 0$ *be relatively prime to* L*, and let* $\mathbf{b}$ *be a* k*-fold decimation of* $\mathbf{a}$*. Then the second half of one period of* $\mathbf{b}$ *is the complement of the first half.*

Proof: Note that k must be odd and $a_j = 1 - a_{j+L/2}$. Thus we have

$$\begin{aligned} b_i &= a_{id} \\ &= 1 - a_{id+L/2} \\ &= 1 - a_{(i+L/2)d} \\ &= 1 - b_{i+L/2}, \end{aligned}$$

which proves the proposition. □

Lemma 9.5 *Let* L *be an even integer. Let* $\mathbf{b} = b_0, b_1, \ldots$ *be a strictly periodic sequence with period* L *such that the second half of each period is the bitwise complement of the first half and let*

$$\beta = \sum_{i=0}^{\infty} b_i \pi^i.$$

Then

$$\beta = \frac{v}{\pi^{L/2} + 1}$$

for some $v \in \mathbf{Z}[\pi]$.

Conversely, if $\mathbf{b} = b_0, b_1, \ldots$ *is the* π*-adic expansion of a* π*-adic integer* $w/(\pi^{L/2} + 1)$ *with eventual period dividing* L*,* $\gcd(L, d) = 1$ *and* $w \notin \{0, (\pi^{L/2} + 1)/(\pi - 1)\}$*, then the second half of each* L *bit period of* $\mathbf{b}$ *is the bitwise complement of the first half.*

Proof: If α is a π-adic number, then we let $\bar{\alpha}$ be the complementary π-adic number. That is, we replace each 1 by 0 and each 0 by 1 in the π-adic expansion of α. For the first part, we have

$$\begin{aligned} \beta + \bar{\beta} &= 1 + \pi + \pi^2 + \cdots \\ &= \frac{-1}{\pi - 1} \\ &= -(1 + \pi + \pi^2 + \cdots + \pi^{d-1}) \end{aligned}$$

since $\pi^d = 2$. Therefore

$$\begin{aligned} -(1 + \pi + \pi^2 + \cdots + \pi^{d-1}) - \beta &= \bar{\beta} \\ &= x + \pi^{L/2}\beta \end{aligned}$$

for some $x \in \mathbf{Z}[\pi]$. Solving for β we have

$$\beta = \frac{-x - 1 - \pi - \cdots - \pi^{d-1}}{\pi^{L/2} + 1},$$

as claimed.

Now consider the converse. We first reduce to the case when $\mathbf{b}$ is strictly periodic. We can write

$$\frac{w}{\pi^{L/2}+1} = x + \pi^k \gamma$$

with $x \in \mathbf{Z}[\pi]$, k a positive integer, and γ a π-adic integer with strictly periodic π-adic expansion. Since the π-adic expansion of γ is periodic, we can write $\gamma = y/(\pi^L - 1)$ for some $y \in \mathbf{Z}[\pi]$. Thus

$$(w - x(\pi^{L/2}+1))(\pi^{L/2}-1) = \pi^k y. \tag{16}$$

In particular, π^k divides the left hand side of equation (16). It follows that π divides $w - x(\pi^{L/2} + 1)$, since $\pi^{L/2} - 1$ is congruent to -1 modulo π. Note that we must be careful here since $\mathbf{Z}[\pi]$ may not be a unique factorization domain. By induction, π^k divides $w - x(\pi^{L/2} + 1)$. Thus we can write $w - x(\pi^{L/2} + 1) = \pi^k z$ for some $z \in \mathbf{Z}[\pi]$. Therefore

$$\gamma = \frac{z}{\pi^{L/2}+1}$$

and we may assume $\mathbf{b}$ is strictly periodic.

Let

$$\mu = \pi^{(d-1)L/2} - \pi^{(d-2)L/2} + - \cdots - \pi^{L/2} + 1,$$

so $\mu(\pi^{L/2} + 1) = \pi^{dL/2} + 1 = 2^{L/2} + 1$. Then

$$\begin{aligned} \frac{w}{\pi^{L/2}+1} &= \frac{w\mu}{2^{L/2}+1} \\ &= \frac{v_0}{2^{L/2}+1} + \frac{v_1}{2^{L/2}+1}\pi + \cdots + \frac{v_{d-1}}{2^{L/2}+1}\pi^{d-1} \end{aligned}$$

for some rational integers $v_0, v_1, \ldots, v_{d-1}$. Since $\mathbf{b}$ is strictly periodic, we must have

$$-(2^{L/2}+1) \le v_j \le 0$$

for all j.

We claim that if any of the v_j is zero, then they all are, and that if any of the v_j is $-(2^{L/2}+1)$, then they all are. For any j we have

$$\frac{v_j}{2^{L/2}+1} = \sum_{i=0}^{\infty} b_{di+j} 2^i.$$

Fix a particular j. Since L and d are relatively prime, we can choose $n, m \in \mathbf{Z}$ so that $nL + j = md$, and we can assume that n and m are nonnegative. Then by the fact that $\mathbf{b}$ is periodic with period dividing L, for every i

$$\begin{aligned} b_{di+j} &= b_{di+nL+j} \\ &= b_{d(i+m)}. \end{aligned}$$

It follows that

$$\begin{aligned}
\frac{v_j}{2^{L/2}+1} &= \sum_{i=0}^{\infty} b_{d(i+m)} 2^i \\
&= 2^{-dm} \sum_{i=m}^{\infty} b_{di} 2^i \\
&= 2^{-dm}\left(\frac{v_0}{2^{L/2}+1} - x\right),
\end{aligned}$$

where x is a rational integer between 0 and $2^m - 1$. That is, $2^{dm} v_j = v_0 - (2^{L/2}+1)x$. It follows that if $2^{L/2}+1$ divides one of v_j and v_0, then it divides the other. If $v_0 = 0$ and $v_j = -(2^{L/2}+1)$, then $x = 2^{dm}$, which is impossible. If $v_0 = -(2^{L/2}+1)$ and $v_j = 0$, then $x = -1$, which is also impossible. The claim follows.

Now, by hypothesis the v_j are not all zero and are not all $-(2^{L/2}+1)$. Hence by the above claim, none is zero and none is $-(2^{L/2}+1)$. In particular there is an exponential representation for $v_0/(2^{L/2}+1)$, $b_{di} = (-v_0 2^{-i} \pmod{2}^{L/2}+1) \pmod{2}$. Since d is odd,

$$\begin{aligned}
b_{di+L/2} &= b_{d(i+L/2)} \\
&= (-v_0 2^{-i-L/2} \pmod{2}^{L/2}+1) \pmod{2} \\
&= (v_0 2^{-i} \pmod{2}^{L/2}+1) \pmod{2} \\
&= 1 - b_{di}.
\end{aligned}$$

Now let m be arbitrary and pick i and k so $m = id + kL$ and $i \geq 0$. Then

$$\begin{aligned}
b_{m+L/2} &= b_{id+kL+L/2} \\
&= b_{id+L/2} \\
&= 1 - b_{id} \\
&= 1 - b_{m-kL} \\
&= 1 - b_m,
\end{aligned}$$

which proves the lemma. □

Theorem 9.2 is an immediate consequence of the following computation.

Theorem 9.6 *Let the hypotheses be as in Theorem 9.2. Let k and k' be relatively prime to $\phi(N(q))$ with $1 \leq k, k' < \phi(N(q))$. Let $\mathbf{b}$ and $\mathbf{c}$ be k and k'-fold decimations of $\mathbf{a}$, respectively. Then the d-arithmetic cross-correlation of $\mathbf{c}$ and $\mathbf{d}$ with shift τ is*

$$\Theta_{\mathbf{c},\mathbf{d}}(\tau) = \begin{cases} \phi(N(q)) & \text{if } \mathbf{c} = \mathbf{d}^{\tau} \\ 0 & \text{otherwise} \end{cases}$$

Proof: Let $L = \phi(N(q))$. Let $\mathbf{b}$ and $\mathbf{c}$ have associated π-adic numbers $\alpha' = a'/(\pi^{L/2}+1)$ and $\alpha'' = a''/(\pi^{L/2}+1)$, respectively. This is possible by Lemma 9.5. The shift of $\mathbf{c}$ by τ corresponds to a π-adic integer $\pi^{L-\tau}\alpha'' + x$ for some $x \in \mathbf{Z}[\pi]$. The d-arithmetic cross-correlation of $\mathbf{b}$ and $\mathbf{c}$ with shift τ is the number of zeros minus the number of ones in one length L period of

$$\begin{aligned}\beta &= \alpha' - (\pi^{L-\tau}\alpha'' + x) \\ &= \frac{a' - \pi^{L-\tau}a'' - x(\pi^{L/2}+1)}{\pi^{L/2}+1} \\ &\stackrel{\text{def}}{=} \frac{b}{\pi^{L/2}+1}.\end{aligned}$$

If $\mathbf{c}$ is a shift of $\mathbf{b}$ with shift τ, then $\beta = 0$ and the result follows.

Suppose $\mathbf{c}$ is not a shift of $\mathbf{b}$ with shift τ. Let $\mathbf{d}$ be the sequence associated to β. It suffices to show that any period of $\mathbf{d}$ is balanced. The element b is nonzero and by Lemma 8.1 the coefficient sequence of $b/(\pi^{L/2}+1) \in \mathbf{Z}_\pi$ has eventual period dividing L. The theorem then follows from the second part of Lemma 9.5. □

Remark. It is not in general true that the coefficient sequence of a π-adic integer of the form $w/(\pi^{L/2}+1)$ has eventual period dividing L. For example, if we take $w = -\pi^{L/2} - 1$, then the period is d. However, the π-adic integer $b/(\pi^{L/2}+1)$ (which arises in the preceding proof) is the difference of two π-adic integers whose coefficient sequences have period dividing L.

10 Distribution Properties of Generalized ℓ-Sequences

If $\mathbf{a} = a_0, a_1, \ldots$ is a periodic sequence of symbols $0 \le a_i < p$ of period L and if $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is an n-element pattern of symbols, then by an *occurrence of* $\mathbf{c}$ *in* $\mathbf{a}$ we mean an index i such that $0 \le i \le L-1$, and $\mathbf{c} = (a_i, a_i+1, \ldots, a_{i+n-1})$. That is, we allow the n-element pattern to extend into the second period, as long as it starts in the first period.

In [1] it was shown that if $\mathbf{a}$ is a binary ℓ-sequence based on a prime connection number q then the number of occurrences of any two n-element patterns $\mathbf{c}$ differ at most by one. This result was extended [6] to the slightly more general notion of ℓ-sequence for which the connection number q is a power of a prime. In this section we consider the same question for the generalized ℓ-sequences of (15). As in §2 suppose that $X^d - p$ is irreducible over $\mathbf{Q}$ and that $q \in \mathbf{Z}[\pi]$ is invertible mod π. Assume that $q = r^t$ for some $r \in \mathbf{Z}[\pi]$ such that $N(r)$ is prime. Finally, as in (15) assume that the image of π in $\mathbf{Z}[\pi]/(q)$ is primitive.

By Corollary 5.2, $a_j = (N(q)^{-1}(zm^{-j} \pmod{N(q)}) \pmod{p})$ where $\pi \equiv m \pmod{q}$ and reduction modulo $N(q)$ means reduction to the set $\{-|N(q)|, \ldots, -1\}$. Suppose that p divides m, and let

$$b_j = N(q)^{-1}(zm^{-j} \pmod{N(q)}) \pmod{m}.$$

Thus $b_j \in \{0, \ldots, m-1\}$ and

$$\beta = \sum_{i=0}^{\infty} b_i m^i = \frac{x}{N(q)}$$

is an m-adic number. Since $\mathbf{a}$ is a generalized ℓ-sequence, π is primitive modulo q. Thus m has order $\phi(N(q))$ modulo $N(q)$. It follows that $\mathbf{b}$ is also a generalized ℓ-sequence. We first analyze the distribution properties of $\mathbf{b}$.

Proposition 10.1 *Let m and t be relatively prime rational integers such that t is a power of a prime s. Let m have order $\phi(t)$ modulo t so that the sequence $\mathbf{b}$ with*

$$b_j = |t|^{-1}(zm^{-j} \pmod{t}) \pmod{m}$$

has period $\phi(t)$. If $t = s$, then the number of occurrences of any n-element pattern in $\mathbf{b}$ is $\lceil |t|/m^n \rceil$ or $\lfloor |t|/m^n \rfloor$. In particular, the numbers of occurrences of any two such patterns differ by at most one. If $t \neq s$, then the numbers of occurrences of any two n-element patterns differ by at most two.

Proof: We may assume without loss of generality that t is positive. Let $u_i \in \mathbf{Z}$ be the element such that the sequence of coefficients in the m-adic expansion of $-u_i/t$ is the shift of $\mathbf{b}$ by i positions to the left. Let $\Phi = \{u_i : i = 0, 1, \ldots\}$. Then i is an occurrence of $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \{0, \ldots, m-1\}^n$ in $\mathbf{b}$ if and only if the first n elements of the m-adic expansion of u_i/q are $(c_0, \ldots, c_{n-1})$. That is,

$$\frac{-u_i}{t} \equiv \sum_{j=0}^{n-1} c_j m^j \pmod{m}^n,$$

or equivalently

$$u_i \equiv -t \left(\sum_{j=0}^{n-1} c_j m^j \right) \pmod{m}^n. \tag{17}$$

Thus the number of occurrences of $\mathbf{c}$ is the number of i such that equation (17) holds. Note that t is invertible modulo m, so multiplication by $-t$ just permutes the elements modulo m. Thus if i is an occurrence of $\mathbf{c}$, then the number of occurrences of $\mathbf{c}$ is the number of js with $u_i \equiv u_j \pmod{m}^n$. Therefore to understand the distribution of the $\mathbf{c}$s it suffices to understand the variation in the sizes of the congruence classes of u_is modulo m^n.

We first restrict our attention to the case when t is prime, i.e., $t = s$. Then $\Phi = \{1, \ldots, t-1\}$. If $1 \leq u \leq t-1-m^n \lfloor (t-1)/m^n \rfloor$, then the congruence class of u modulo m^n has $\lfloor (t-1)/m^n \rfloor + 1$ elements in Φ. If $t - m^n \lfloor (t-1)/m^n \rfloor \leq u \leq m^n$, then the congruence class of u modulo m^n has $\lfloor (t-1)/m^n \rfloor$ elements in Φ. This proves the first assertion. Note that if we were to extend Φ to include t, then only the congruence class of $t - m^n \lfloor (t-1)/m^n \rfloor$ would change, and its size would become $\lfloor (t-1)/m^n \rfloor + 1$.

Now let $t \neq s$, so $t = s^k$ for some $k \geq 2$. Then

$$\begin{aligned} \Phi &= \{u : 0 < u < t \text{ and } s \not| u\} \\ &= \{u : 0 < u < t\} - s\{u : 0 < u \leq s^{k-1}\}. \end{aligned}$$

Let $v \in \Phi$. Let $x = \{u : 0 < u < t, u \equiv v \pmod{m}^n\}$ and $y = \{u : 0 < u \leq s^{k-1}, su \equiv v \pmod{m}^n\} = \{u : 0 < u \leq s^{k-1}, u \equiv s^{-1}v \pmod{m}^n\}$. Then the number of elements of Φ that are congruent to u modulo m^n is $x - y$. As above we have

$$\lfloor t/m^n \rfloor \leq x \leq \lfloor t/m^n \rfloor + 1$$

and

$$\left\lfloor s^{k-1}/m^n \right\rfloor \leq y \leq \left\lfloor s^{k-1}/m^n \right\rfloor + 1.$$

Thus

$$\lfloor t/m^n \rfloor - \left\lfloor s^{k-1}/m^n \right\rfloor - 1 \leq x - y \leq \lfloor t/m^n \rfloor - \left\lfloor s^{k-1}/m^n \right\rfloor + 1.$$

This proves the proposition. $\square$

We can then analyze our original generalized ℓ-sequence **a** by reducing **b** modulo p.

Theorem 10.2 *Let* $\mathbf{a} = a_0, a_1, \ldots$ *be a generalized* ℓ*-sequence based on* $\mathbf{Z}[\pi]$*, with* $\pi^d = p$*. Let* $q = r^k$ *be its connection number with* $N(r)$ *prime and relatively prime to* d*. Let* $m \in \mathbf{Z}$ *be congruent to* π *modulo* $N(q)$*. Suppose* p *divides* m*. If* $k = 1$*, then the numbers of occurrences of any two* n*-element patterns in* **a** *differ by at most* $(m/p)^n$*. If* $k > 1$*, then the numbers of occurrences of any two* n*-element patterns in* **a** *differ by at most* $2(m/p)^n$*.*

Proof: This follows from Proposition 10.1 since reduction modulo p is a $(m/p)^n$ to one map from $(\mathbf{Z}/(m))^n$ to $(\mathbf{Z}/(p))^n$. $\square$

Unfortunately these bounds are fairly weak. In fact they say nothing at all if $m^n \geq p^n\phi(N(q))$ since the total number of n-element patterns in **a** is only $\phi(N(q))$. However, a small amount of experimental evidence suggests that the range of numbers of occurrences of n-element patterns in fact is much smaller.

References

[1] L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudorandom number generator, *SIAM J. Comp.* **15** (1986) 364-383.

[2] Z. I. Borevich and I. R. Shefarevich, *Number Theory*, Academic Press: New York, N.Y., 1966.

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

[4] M. Goresky and A. Klapper, Feedback registers based on ramified extensions of the 2-adic numbers, *Advances in Cryptology - Eurocrypt '94* Lecture Notes in Computer Science **950**, Springer Verlag: New York, 1995.

[5] M. Goresky and A. Klapper, Galois and Fibonacci Representations for Feedback with Carry Shift Registers, in preparation.

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

[7] A. Klapper and M. Goresky, Arithmetic Cross-Correlations of FCSR Sequences, *IEEE Transactions on Information Theory* **43** (1997) pp. 1342-1346.

[8] A. Klapper and J. Xu, Algebraic feedback shift registers, *Theoretical Computer Science* **226** (1999) pp. 61-93.

[9] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions,* Springer-Verlag: New York, 1984.

[10] S. Lang, *Algebra,* Addison-Wesley: Reading, MA, 1965.

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

[12] G. Marsaglia, The mathematics of random number generators, *The Unreasonable Effectiveness of Number Theory*, Amer. Math. Soc., Providence R. I., 1992. pp. 73-90.

[13] G. Marsaglia and A. Zaman, A new class of random number generators, *Annals of Applied Probability* **1** (1991) pp. 462-480.

[14] J. Massey and R. Rueppel, Method of, and Apparatus for, Transforming a Digital Data Sequence into an Encoded Form, U.S. Patent No. 4,797,922, 1989.

[15] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer-Verlag: New York, 1990.

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