Distributional Properties of d-FCSR Sequences

Andrew Klapper*

Abstract

In this paper we study the distribution properties of d-FCSR sequences. These sequences have efficient generators and have several good statistical properties. We show that for $d = 2$ the number of occurrences of an fixed size subsequence differs from the average number of occurrences by at most a small constant times the square root of the average.

Keywords: FCSR sequence, pseudonoise sequence, pseudorandom sequence, distribution property.

1 Introduction

Pseudorandom sequences play a crucial role in a wide range of applications in areas as diverse as cryptography, radar ranging, Monte Carlo simulation, and probabilistic algorithms. In many cases it is desirable to use sequence for which the distribution of occurrences within a single period of any given s-element pattern is highly uniform, as well as having other statistical properties.

An m-sequence is a maximal period sequence generated by a linear feedback shift register (LFSR). Such a sequence has many excellent properties for these sorts of application (see, for example, [11, Part I, §5.4]). It is easy to generate in hardware. It can be analyzed using standard mathematical techniques. Its autocorrelation function is 2-valued (and hence optimal). It is a pseudo-noise sequence, meaning that if T is the period of the sequence, then the number of occurrences within a single period of any given s-element pattern differs from $T/2^s$ by less than 1. In some cases particular m-sequences have been shown to have additional desirable properties [10].

*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. Research partially supported by NSF grant #9980429.

An ℓ-sequence is a maximal length sequence generated by a feedback-with-carry shift register (FCSR) [7], and it shares many of these advantages: it is easy to generate in hardware and it can be analyzed using standard mathematical techniques. Its *arithmetic* autocorrelation function [8] is 2-valued and optimal, and it is a pseudo-noise sequence in the above sense.

In this paper we consider generalized ℓ-sequences. These are the maximal length sequences which are obtained from the output of a d-FCSR [6], in which each feedback element is delayed for $d-1$ clock cycles before being fed back. Previously we showed that the *d-arithmetic autocorrelation function* of such a sequence is two-valued and optimal [4]. In this paper we consider the pseudo-noise properties of these sequences. Suppose the alphabet has $p = f^2 r$ elements with r square free. In Theorem 4.4 we show that if r is congruent to 2 or 3 modulo 4, $d = 2$, and s is an even number, then the number of occurrences within a single period of any s-element pattern differs from $(T+1)/2^s$ by no more than $c\sqrt{(T+1)/2^s} + 2$. Here c is a constant depending on p. For $p = 2$ we have $c = 3$. For $d \geq 3$ we obtain a weaker estimate on the distribution of s-element patterns. The problem of finding sharp estimates on the distributions of patterns in a generalized ℓ-sequence seems quite intriguing.

Computer search has shown that, within these constraints, different ℓ-sequences have widely varying distribution properties. In some cases the maximum variation from $(T+1)/2^s$ is close to our bound. But in some cases the maximum variation from $(T+1)/2^s$ is less than 2 (in fact in some cases the numbers of occurrences of any two s-element patterns differs by at most 2). Finding conditions on ℓ-sequences that ensures such near optimal behaivour is an open problem.

2 Generalized ℓ-Sequences

In this section we review some results of [4] to which we refer the reader for further explanations, generalizations, and proofs. Throughout this paper we let p denote an integer, fix $d \geq 1$ so that $x^d - p$ is an irreducible polynomial over the rational numbers (this occurs if and only if for every prime number $t|d$, p is not a tth power in $\mathbf{Q}$ and, if $4|d$, p is not -4 times a 4th power in $\mathbf{Q}$ [9, Chap. VIII, §9]), and let $\pi \in \mathbf{R}$ be the positive real solution to $\pi^d = p$. The ring $\mathbf{Z}[\pi]$ consists of all real numbers of the form

$$u_0 + u_1\pi + \cdots + u_{d-1}\pi^{d-1} \tag{1}$$

with $u_i \in \mathbf{Z}$. The field $\mathbf{Q}[\pi]$ consists of the real numbers (1) with $u_i \in \mathbf{Q}$. It is the fraction field of $\mathbf{Z}[\pi]$. That is, every element of $\mathbf{Q}[\pi]$ may be expressed as a fraction u/v with $u, v \in \mathbf{Z}[\pi]$. It is also a vector space over $\mathbf{Q}$ of dimension d, and a basis is given by the collection of vectors $\left\{1, \pi, \pi^2, \ldots, \pi^{d-1}\right\}$. We refer to $\mathbf{Z}[\pi]$ as the set of *lattice points* in $\mathbf{Q}[\pi]$.

The ring $\mathbf{Z}_\pi$ consists of all infinite formal expressions

$$\alpha = a_0 + a_1\pi + a_2\pi^2 + \cdots \tag{2}$$

where $a_i \in T = \{0, 1, \cdots, p-1\}$, with the obvious operations of addition and multiplication (using $\pi^d = p$). If $d = 1$, then $\mathbf{Z}[\pi] = \mathbf{Z}$, $\mathbf{Q}[\pi] = \mathbf{Q}$ and $\mathbf{Z}_\pi = \mathbf{Z}_p$ is the p-adic numbers. In general, the ring $\mathbf{Z}_\pi$ contains both $\mathbf{Z}_p$ and $\mathbf{Z}[\pi]$ as well as many elements of $\mathbf{Q}[\pi]$. In fact, if $u, q \in \mathbf{Z}[\pi]$ then the fraction $u/q \in \mathbf{Q}[\pi]$ is in $\mathbf{Z}_\pi$ if and only if the denominator $q = \sum_{i=0}^{d-1} q_i \pi^i$ is invertible modulo π, which is equivalent to q_0 being relatively prime to p. The π-adic expansion

$$\frac{u}{q} = \sum_{i=0}^{\infty} a_i \pi^i \in \mathbf{Z}_\pi \tag{3}$$

(with $a_i \in T$) is then unique and we refer to the sequence $a_0, a_1, \cdots$ as the *coefficient sequence* of u/q.

Definition 2.1 *The d-FCSR sequence $\mathbf{S}(d, u, q)$ is the coefficient sequence of the π-adic expansion* (3) *of the fraction u/q where $u, q \in \mathbf{Z}[\pi]$ and where q is invertible modulo π.*

The element $q \in \mathbf{Z}[\pi]$ is called the *connection number* of the sequence. The sequence $\mathbf{S}(d, u, q)$ is eventually periodic. Conversely, for any eventually periodic p-ary sequence $\mathbf{a}$ there exists $u, q \in \mathbf{Z}[\pi]$ so that $\mathbf{a} = \mathbf{S}(d, u, q)$. (In Theorem 2.3 we recall how to choose u so that the resulting sequence is strictly periodic.) Such sequences may be generated using a simple shift register circuit whose feedback connections are determined by the choice of q and whose initial state is determined by the choice of u [6, 4].

The *norm* $N(q) \in \mathbf{Q}$ of an element $q \in \mathbf{Q}[\pi]$ is the determinant of the linear transformation given by multiplication by q on the d-dimensional vector space $\mathbf{Q}[\pi]$. If $u \in \mathbf{Z}[\pi]$, then $N(u) \in \mathbf{Z}$. With respect to the basis $1, \pi, \pi^2, \ldots, \pi^{d-1}$ the matrix of multiplication by $q = \sum_{i=0}^{d-1} q_i \pi^i$ is

$$\begin{pmatrix} q_0 & pq_{d-1} & pq_{d-2} & \cdots & pq_2 & pq_1 \\ q_1 & q_0 & pq_{d-1} & \cdots & pq_3 & pq_2 \\ & & \vdots & & & \\ q_{d-2} & q_{d-3} & q_{d-4} & \cdots & q_0 & pq_{d-1} \\ q_{d-1} & q_{d-2} & q_{d-3} & \cdots & q_1 & q_0 \end{pmatrix} \tag{4}$$

from which the norm may be computed. The norm of q is relatively prime to p if and only if q is invertible modulo π. Let $N = |N(q)|$. The composition $\mathbf{Z} \to \mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ passes to a well defined homomorphism of rings

$$\psi : \mathbf{Z}/(N) \to \mathbf{Z}[\pi]/(q) \tag{5}$$

which is an isomorphism if N is prime. In this case, we say that π is *primitive* modulo q if, in $\mathbf{Z}[\pi]/(q)$ the collection of elements $\{1, \pi, \pi^2, \ldots, \pi^{N-2}\}$ exactly accounts for all the nonzero elements in $\mathbf{Z}[\pi]/(q)$ (or equivalently, if the element $\psi^{-1}(\pi)$ is primitive in $\mathbf{Z}/(N)$).

Definition 2.2 *Let $u, q \in \mathbf{Z}[\pi]$. Suppose that $N = |N(q)|$ is prime and that π is primitive modulo q. Suppose the d-FCSR sequence $\mathbf{S}(d, u, q)$ is strictly periodic. Then the sequence $\mathbf{S}(d, u, q)$ is called a generalized ℓ-sequence.*

Such a generalized ℓ-sequence has period $N - 1$. In the case $d = 1$ (so $\pi = p$ and $N = q$) it is an ℓ-sequence in our earlier sense [7]. That is, it is the reverse of the base p expansion of the fraction u/q (cf. [1]). Such sequences have been studied for 200 years (cf. [3]).

We previously characterized those numerators u so that the sequence $\mathbf{S}(d, u, q)$ is strictly periodic [4]. Consider the parallelepiped in $\mathbf{Z}[\pi]$ which is spanned by the d linearly independent vectors $-q, -q\pi, \ldots, -q\pi^{d-1}$,

$$P = \left\{ \sum_{i=0}^{d-1} v_i q \pi^i | \ v_i \in \mathbf{Q} \text{ and } -1 \leq v_i \leq 0 \right\} \subset \mathbf{Q}[\pi] \tag{6}$$

and its interior

$$P_0 = \left\{ \sum_{i=0}^{d-1} v_i q \pi^i | \ v_i \in \mathbf{Q} \text{ and } -1 < v_i < 0 \right\} \subset \mathbf{Q}[\pi]. \tag{7}$$

Let Δ (respectively, Δ_0) be the set of lattice points in P (respectively, P_0):

$$\Delta = P \cap \mathbf{Z}[\pi] \text{ and } \Delta_0 = P_0 \cap \mathbf{Z}[\pi].$$

Theorem 2.3 *Suppose $q \in \mathbf{Z}[\pi]$ is odd, $N = |N(q)|$ is prime, and π is primitive modulo q. Let $\delta = |N(q)|/q \in \mathbf{Z}[\pi]$. Choose $u \in \mathbf{Z}[\pi]$ to be nonzero. Then the following statements are equivalent.*

1. *The d-FCSR sequence $\mathbf{S}(d, u, q)$ is strictly periodic*
2. *$u \in \Delta$*

If $u \in \Delta_0$ then the sequence $\mathbf{S}(d, u, q)$ is a generalized ℓ-sequence. The projection $\phi : \mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ determines a one to one correspondence between Δ_0 and the nonzero elements in $\mathbf{Z}[\pi]/(q)$. The generalized ℓ-sequences with given connection number q are cyclic shifts of one another.

Hence, as v varies within Δ_0, the resulting $N - 1$ generalized ℓ-sequences $\mathbf{S}(d, v, q)$ account precisely for set of all cyclic shifts of any one particular generalized ℓ-sequence $\mathbf{S}(d, u, q)$.

3 Distributions and Lattice Points

As in the previous section, we fix $d \geq 1$, and fix $q \in \mathbf{Z}[\pi]$ so that q is invertible modulo π, $N = |N(q)|$ is prime, and π is primitive modulo q. Let $\mathbf{a} = \mathbf{S}(d, u, q) = a_0, a_1, \cdots$ be a generalized ℓ-sequence with connection number q (and thus with period $N-1$), corresponding to some fixed $u \in \Delta_0$. If $\mathbf{b} = (b_0, b_1, \cdots, b_s) \in T^s$ is an s-element pattern, then an *occurrence of* $\mathbf{b}$ *in a period of* $\mathbf{a}$ is an index i such that $0 \leq i \leq N-2$ and $a_{i+j} = b_j$ for $j = 0, \cdots, s-1$. In this section we show that the number of occurrences of an s-element pattern within a single period of the ℓ-sequence $\mathbf{a}$ is equal to the number of points of a certain integer lattice which lie in a certain hypercube.

The number of occurrences of the pattern $\mathbf{b}$ in a single period of $\mathbf{a}$ is equal to the number of cyclic shifts of $\mathbf{a}$ for which the pattern $\mathbf{b}$ occurs as the first s elements. So we need to count the number of $v \in \Delta_0$ so that the pattern $\mathbf{b}$ occurs as the first s elements in the generalized ℓ-sequence $\mathbf{S}(d, v, q)$.

If $x, y \in \mathbf{Z}_\pi$ with $x = \sum_{i\geq 0} x_i \pi^i$ and $y = \sum_{i \geq 0} y_i \pi^i$ we write $x \equiv y \pmod{\pi^s}$ if $x_i = y_i$ for $0 \leq i \leq s-1$. This is the same as saying that the images $\bar{x}, \bar{y} \in \mathbf{Z}_\pi/(\pi^s)$ of x and y are equal. Then a given s element pattern $(b_0, b_1, \ldots, b_{s-1})$ occurs as the first s elements of the ℓ-sequence $\mathbf{S}(d, v, q)$ if and only if

$$b \equiv \frac{v}{q} \pmod{\pi^s}, \tag{8}$$

where $b = \sum_{i=0}^{d-1} b_i \pi^i$. The element q is invertible modulo π^s, so equation (8) is equivalent to the statement that $qb \equiv v \pmod{\pi^s}$. Multiplication by q acts as a permutation on $\mathbf{Z}_\pi/(\pi^s)$, a ring which we may think of as consisting of the collection of all s element patterns. Since our goal is to determine the distribution of the number of occurrences of each s element pattern in $\mathbf{a} = \mathbf{S}(d, u, q)$ it suffices to determine, for each s element pattern b', the number of $v \in \Delta_0$ such that $b' \equiv v \pmod{\pi^s}$. (Now we drop the prime on the b.) So for each fixed b we need to find the number of $w \in \mathbf{Z}[\pi]$ such that

$$b + w\pi^s \in \Delta_0. \tag{9}$$

Suppose s is a multiple of d, say $s = md$. Let $\delta = N/q$. We previously proved that $\delta \in \mathbf{Z}[\pi]$ [4], so equation (9) becomes

$$\delta w p^m \in \delta\Delta_0 - \delta b,$$

where $\delta\Delta_0 - \delta b = \{\delta u - \delta b | u \in \Delta_0\}$. We claim that the set $\delta\Delta_0$ is the set of lattice points in the interior of a hypercube of side N (and so the same is true of $\delta\Delta_0 - \delta b$). For if $v = \sum_{i=0}^{d-1} v_i \pi^i q \in \Delta_0$ with $-1 < v_i < 0$ then $\delta v = \sum_{i=0}^{d-1} v_i N \pi^i \in \mathbf{Z}[\pi]$ from which it follows that $z_i = v_i N$ is an integer and that $-N < z_i < 0$.

Lemma 3.1 *For any $w \in \mathbf{Z}[\pi]$ there is a unique $k \in \mathbf{Z}$ with $0 \leq k < N$ and a unique $a \in \mathbf{Z}[\pi]$ such that $w\delta = k\delta + aN$.*

Proof: By equation (5), given $v \in \mathbf{Z}[\pi]$ there is a unique $k \in \mathbf{Z}$ with $0 \leq k < N$ so that $v \equiv k \pmod{(q)}$. So there is a unique $a \in \mathbf{Z}[\pi]$ with $v = k + aq$. Multiplying by δ gives $v\delta = k\delta + aN$. □

It follows that it suffices for us to count the number of pairs $k \in \mathbf{Z}, a \in \mathbf{Z}[\pi]$ such that

$$k\delta + aN \in \frac{1}{p^m}\left(\delta\Delta_0 - \delta b\right). \tag{10}$$

This is the number of lattice points of the form $k\delta + aN$ which lie in a real hypercube, each of whose edges has length N/p^m.

4 The Case $d = 2$

In this section we apply the results of Section 3 to the case when $d = 2$. We show that the number of occurrences of each s-tuple, s even, differs from the average number of occurrences by at most a small constant times the square root of the average number of occurrences.

Note that since $d = 2$ we have $\delta = \pm(q_0 - q_1\pi)$. Let s be even and let $t = N/p^{s/2}$. Let B be a t by t square with sides parallel to the axes. We want to bound the cardinality of the set S of points of the form $k(q_0, -q_1) + (Nw_0, Nw_1)$, with $k, w_0, w_1 \in \mathbf{Z}$. Let us assume that $q_1 < 0$. The case when $q_1 > 0$ is similar and is omitted. For fixed $w = (w_0, w_1) \in \mathbf{Z}^2$, let L_w be the real line $L_w = \{k(q_0, -q_1) + Nw : k \in \mathbf{R}\}$. Then S is the union over all w of the set of points $k(q_0, -q_1) + (Nw_0, Nw_1) \in L_w \cap B$. That is, the points in S are in a union of line segments. The number of lattice points on each such segment is approximately the length of the segment divided by the (constant) distance between consecutive lattice points. Alternatively, it is approximately the variation in the second coordinate along the segment divided by the variation in the second coordinate between two consecutive lattice points. The error in this estimate is at most one per line segment. Thus we can bound the size of S by the following steps:

1. Find numbers m_0 and m_1 so that the sum of the variations in the second coordinates along the segments is between m_0 and m_1.

2. The variation in the second coordinate between consecutive lattice points is $|q_1|$.

3. Bound the error: the actual number of lattice points on a segment whose second coordinate varies by r is greater than $(r/|q_1|) - 1$ and at most $(r/|q_1|) + 1$. Let ℓ be the number of segments.

4. Thus the total number of lattice points is at least $(m_0/|q_1|) - \ell$ and at most $(m_1/|q_1|) + \ell$.

The slope of the segments is positive, so there are three types of lines: (a) those that start on the left hand vertical side of B and end on the upper horizontal side; (b) those that start on the lower horizontal side and end on the upper horizontal side; and (c) those that start on the lower horizontal side and end on the right hand vertical side. We can count the number ℓ of segments by counting the x-intercepts and y-intercepts. The x-intercept of a line L_w, $w = (w_0, w_1)$, is a point $k(q_0, -q_1) + N(w_0, w_1)$ such that $Nw_1 - kq_1 = 0$. That is, $k = Nw_1/q_1$. The intercept is the x coordinate, $N(q_0w_1 + q_1w_0)/q_1$. But q_0 and q_1 are relatively prime, so as we let w vary all possible numbers of the form $Na/|q_1|$ occur as intercepts.

Suppose that the first x-intercept in B occurs at distance z from the left hand vertical edge. Then the first y-intercept occurs at distance

$$\frac{|q_1|}{q_0}\left(\frac{N}{|q_1|} - z\right)$$

from the bottom horizontal edge. Thus the number of intercepts is at most

$$\begin{aligned} \left\lceil \frac{t-z}{N/|q_1|} \right\rceil + \left\lceil \frac{t - (|q_1|/q_0)(N/|q_1| - z)}{N/q_0} \right\rceil &\leq \frac{t-z}{N/|q_1|} + \frac{t - (|q_1|/q_0)(N/|q_1| - z)}{N/q_0} + 2 \\ &= \frac{t(q_0 + |q_1|)}{N} + 1. \end{aligned}$$

Similarly, the number of intercepts is at least

$$\frac{t(q_0 + |q_1|)}{N} - 1.$$

Next we want to bound the sum of the variations in the second coordinates along the segments. For a lower bound, let $t' = \lfloor t|q_1|/N \rfloor (N/|q_1|)$ be the largest integral multiple of $N/|q_1|$ that is less than or equal to t. We can shrink B slightly to obtain a t' by t rectangle B' and just measure the parts of the segments in B'. Every segment of type (1) in B' matches up with a segment of type (3) in B' so that the sum of the differences in the second coordinate along the two segments is exactly t. If we call these combined segments and the segments of type (2) *super segments*, then the number of super segments in B' is the number of x-intercepts in B' and each super segment varies in its second coordinate by t. Thus the number of super segments is at least

$$\left\lfloor \frac{t'}{N/|q_1|} \right\rfloor = \left\lfloor \frac{t|q_1|}{N} \right\rfloor \geq \frac{t|q_1|}{N} - 1 = \frac{|q_1|}{p^{s/2}} - 1,$$

and the sum of the variation in the second coordinates is at least

$$m_0 = \frac{t|q_1|}{p^{s/2}} - t = \frac{N|q_1|}{p^s} - \frac{N}{p^{s/2}}.$$

It follows that the number of lattice points in B is at least

$$\begin{aligned} \frac{m_0}{|q_1|} - \ell &\geq \frac{N}{p^s} - \frac{N}{p^{s/2}|q_1|} - \frac{t(|q_0|+|q_1|)}{N} - 1 \\ &= \frac{N}{p^s} - \frac{N}{p^{s/2}|q_1|} - \frac{|q_0|+|q_1|}{p^{s/2}} - 1. \end{aligned}$$

By reversing the roles of q_0 and q_1 we can replace the $|q_1|$ in the first error term by $|q_0|$, and thus by $\max|q_1|, |q_2|$. A similar derivation of an upper bound gives the following theorem.

Theorem 4.1 *Let* **a** *be an ℓ-sequence defined over $\mathbf{Z}[\pi]$, $\pi^2 = p$, whose connection element q has absolute norm N. If s is even, then the number K of occurrences of any s-tuple in one period of* **a** *satisfies*

$$\frac{N}{p^s} - \frac{N}{p^{s/2}\max(|q_0|,|q_1|)} - \frac{|q_0|+|q_1|}{p^{s/2}} - 1 \leq K \leq \frac{N}{p^s} + \frac{N}{p^{s/2}\max(|q_0|,|q_1|)} + \frac{|q_0|+|q_1|}{p^{s/2}} + 1.$$

Next we show that in some cases we can choose the connection number q so the error term is bounded. Suppose that u is a unit in R. Then $uv/uq = v/q$, so the π-adic expansion of v/q equals the π-adic expansion of uv/uq. Also, if u is a unit then $R/(q) = R/(uq)$, so our analysis works equally well with q replaced by uq. Thus we can bound the error term if we can find a unit u so that $uq = q_0' + q_1'\pi$ with $N/|q_1'|$ and $|q_0'| + |q_1'|$ bounded.

The groups of units in quadratic extensions of the rationals have been well studied. We refer the reader to Borevic and Shafarevic's book for details [2]. In general a number field F has some number r_1 of embeddings in the real numbers, and some number $2r_2$ of embeddings in the complex numbers but not strictly in the real numbers. Every such field contains a subring A_F consisting of the set of elements of F that are roots of polynomials with integer coefficients (the ring of allgebraic integers in F). The group of units in A_F (also called the unit group of F) is isomorphic to a group of the form

$$\mathcal{U} \times \mathbf{Z}^{r_1+r_2-1},$$

where $\mathcal{U}$ is finite. Every quadratic (degree 2) extension of the rationals is of the form $\mathbf{Q}[\sqrt{d}]$ for some integer d, which can be assumed to be square-free. Such an extension is *real* if $d > 0$, in which case $r_1 = 2$ and $r_2 = 0$, and is *imaginary* otherwise, in which case $r_1 = 0$ and $r_2 = 1$. Thus the unit group of a real quadratic number field contains an infinite cyclic subgroup. In this case the finite subgroup $\mathcal{U}$ consists only of plus and minus one. The unit group contains an element u such that every unit is of the form $\pm u^i$ with $i \in \mathbf{Z}$, and u can be replaced by $1/u$, $-u$, or $-1/u$. Exactly one of these is greater than 1, so we may assume $1 < u = a + b\sqrt{d}$. In fact it can be shown that then $a > 0$ and $b > 0$. The element u is called *the fundamental unit.*

In our case we can assume that π is the positive square root of p. Let $p = f^2 r$ where $f, r \in \mathbf{Z}$ and r is square free (i.e., there is no prime number whose square divides r). Thus $F = \mathbf{Q}[\sqrt{p}] = \mathbf{Q}[\sqrt{r}]$. We have $R = \mathbf{Z}[\sqrt{p}] \subseteq A_F$, with equality if and only if $f = 1$ and $r \equiv 2, 3 \pmod 4$. The ring R is called an *order* in the field F. Every unit in R is a unit in A_F. If $r \equiv 1 \pmod 4$, then all powers of the fundamental unit are in $A_F - R$, so the unit group of R is just $\{1, -1\}$ and we are unable to modify q. Thus we assume from here on that $r \equiv 2$ or $3 \pmod 4$. For example, if $p = 2$ then $u = 1 + \pi$. If $p = 3$ then $u = 2 + \pi$. If $p = 7$, then $u = 8 + 3\pi$. There is no known simple general expression for the fundamental unit in terms of r, but there are efficient methods for finding it and there are computable bounds on a and b so that $u = a + b\sqrt{r}$ (cf. [2, §7.3]). Suppose that $u = a + b\pi$ is the fundamental unit in A_F. Then the image w of u in $A_F/(f)$ is also a unit. But $A_F/(f)$ is a finite ring, so some power w^n of w equals 1. This implies that $u^n = c + df\sqrt{r} = c + d\sqrt{p} \in R$. That is, R contains a unit with infinite multiplicative order. Moreover, n is positive so both c and d are positive. We refer to the smallest unit of R whose coefficients are positive as the fundamental unit of R. When r is prime and f is a power of r we can say precisely what power of the fundamental unit of F is the fundamental unit of R.

Lemma 4.2 *Suppose that r is prime and $\mu = \sqrt{r}$. Let $a + b\mu$ be the fundamental unit in $\mathbf{Q}[\mu]$. Let ℓ be the largest power of r that divides b. For any k and m with $\gcd(m, r) = 1$, if $(a + b\mu)^{r^k m} = c + d\mu$, then $k + \ell$ is the largest power of r that divides d.*

Proof: We must have $\gcd(a, r) = 1$ or $a + b\mu$ would not be a unit. For any $t > 0$ we have

$$(a + b\mu)^t = \sum_{i \text{ even}} \binom{t}{i} b^i a^{t-i} r^{i/2} + \left(\sum_{i \text{ odd}} \binom{t}{i} b^i a^{t-i} r^{(i-1)/2} \right) \mu. \qquad (11)$$

The first sum is congruent to a^t modulo r, so $\gcd(c, r) = 1$.

We prove the lemma by induction on $r^k m$. For $r^k m = 1$ the lemma is true by definition. If $\gcd(t, r) = 1$, then the second sum in equation (11) is congruent to ba^{t-1} modulo $r^{\ell+1}$, so the lemma is true if $k = 0$.

Suppose it is true for some m and k, with $(a + b\mu)^{r^k m} = c + d\mu$. Let a be replaced by c, let b be replaced by d, and let $t = r$ in equation (11). Then the second sum is congruent to rcd^{r-1} modulo $r^{k+\ell+2}$, so the lemma also holds in this case. □

It follows that if r is prime, $u = a + b\sqrt{r}$ is the fundamental unit of $\mathbf{Q}[\sqrt{r}]$, and ℓ is the largest power of r that divides b, then the fundamental unit of $R = \mathbf{Z}[r^k\sqrt{r}]$ is u if $k \leq \ell$ and is $u^{r^{k-\ell}}$ otherwise. For example, if $r = 2$ then $u = 1 + \sqrt{2}$ and u^{2^k} is the fundamental unit in R. We can use the fundamental unit of R to modify q to obtain reasonable bounds.

Proposition 4.3 *Suppose that $p = f^2 r$ with r square free and $r \equiv 2, 3 \pmod 4$. Let u be the fundamental unit of R. Let $q = q_0 + q_1\pi \in R$. Let $N = |q_0^2 - 2q_1^2|$ be the absolute norm of q. Then there is a unit w in R such that $wq = r_0 + r_1\pi$ with $|r_0| + |r_1| < uN^{1/2}$ and $N^{1/2}/(1+\pi) < \max(|r_0|, |r_1|)$.*

Proof: By repeated multiplication or division by u, we can find a unit w with $N^{1/2} < wq = r_0 + r_1\pi < uN^{1/2}$. Since π, N, and u are positive, it is impossible that both q_0 and q_1 are negative. We claim that they are in fact both positive.

Suppose that $r_0 > 0$ and $r_1 < 0$. Then $r_0 > N^{1/2} + |r_1|\pi$, so $r_0^2 > (N^{1/2} + |r_1|\pi)^2 = N + 2|r_1|\pi + pr_1^2$. Therefore $r_0^2 - pr_1^2 > N + 2|r_1|\pi > N$. But $N = |r_0^2 - pr_1^2|$ is positive, so $N = r_0^2 - pr_1^2 > N$, a contradiction.

Suppose that $r_0 < 0$ and $r_1 > 0$. Then $r_1\pi > N^{1/2} + |r_0|$, so $pr_1^2 > (N^{1/2} + |r_0|)^2 = N + 2|r_0| + r_0^2$. Therefore $pr_1^2 - q_0^2 > N + 2|r_0| > N$. But $N = |r_0^2 - pr_1^2|$ is positive, so $N = pr_1^2 - r_0^2 > N$, a contradiction.

Therefore $r_0, r_1 > 0$. Since $\pi > 1$, the maximum of $r_0 + r_1$ with the constraint $r_0 + r_1\pi \leq uN^{1/2}$ occurs when $r_0 = uN^{1/2}$ and $r_1 = 0$. Since $r_1 \neq 0$, $|r_0| + |r_1| < uN^{1/2}$. If both r_0 and r_1 are less than or equal to $N^{1/2}/(1+\pi)$, then $r_0 + r_1\pi \leq N^{1/2}$, a contradiction. Thus $N^{1/2}/(1+\pi) < \max(|r_0|, |r_1|)$, which proves the proposition. □

Thus we have the following theorem.

Theorem 4.4 *Suppose that $p = f^2 r$ with r square free and $r \equiv 2, 3 \pmod 4$. Let **a** be an ℓ-sequence defined over $\mathbf{Z}[\pi]$, $\pi^2 = p$, whose connection element q has absolute norm N. If s is even, then the number K of occurrences of any s-tuple in one period of **a** satisfies*

$$\frac{N}{p^s} - \left(\frac{(1+\pi+u)N}{p^s}\right)^{1/2} - 1 \leq K \leq \frac{N}{p^s} + \left(\frac{(1+\pi+u)N}{p^s}\right)^{1/2} + 1.$$

In specific cases the error can be reduced by more careful analysis of the specific values of the fundamental unit. For example, for $p = 2$ we have $u = 1 + \pi$, so $1 + \pi + u \sim 4.828$, but his constant can be replaced by 3. In fact, it is likely that in general the error is much smaller than this since our analysis assumes the maximal error along every line segment. Moreover, it is clear from experimental evidence that there is considerable variation in the distributions for different connection numbers q. For example, for $p = 2$ Table 1 gives the connection numbers $q = q_0 + q_1\pi$, $0 < q_0, q_1 \leq 1000$, that satisfy the conclusion of Proposition 4.3 and such that for every $s < \log_2(N)$, the numbers of occurrences of any two s-element patterns differ by at most 2.

q	$\|N(q)\|$	q	$\|N(q)\|$
$1+6\pi$	71	$23+43\pi$	3169
$3+10\pi$	191	$25+31\pi$	1297
$3+17\pi$	569	$27+49\pi$	4073
$3+37\pi$	2729	$31+10\pi$	761
$3+262\pi$	137279	$49+51\pi$	2801
$5+9\pi$	137	$55+17\pi$	2447
$5+13\pi$	313	$55+87\pi$	12113
$7+11\pi$	193	$111+127\pi$	19937
$7+15\pi$	401	$127+13\pi$	15791
$7+79\pi$	12433	$127+32\pi$	14081
$9+134\pi$	35831	$223+263\pi$	88609
$11+21\pi$	761	$249+259\pi$	72161
$11+129\pi$	33161	$255+44\pi$	61153
$13+6\pi$	97	$449+197\pi$	123983
$15+31\pi$	1697	$479+507\pi$	284657
$17+26\pi$	1063	$511+17\pi$	260543
$17+35\pi$	2161		

Table 1: Connection numbers with nearly perfect distributions

5 Larger d

In this section we give a heuristic argument that for $d \geq 3$ the errors will be significantly larger than for $d = 2$. Let $d \geq 3$ and as usual let $q = \sum_{i=0}^{d-1} q_i\pi^i - 1$ be the connection element of an ℓ-sequence $\mathbf{a}$ defined over $\mathbf{Z}[\pi]$ with $\pi^d = p$. Let N be the absolute value of the norm of q, let s be divisible by d, and let $t = N/p^{s/d}$. Note that the number of possible s-tuples is p^s and the number of s-tuples in one period of $\mathbf{a}$ is $N-1$, so each s-tuple occurs $(N-1)/p^s$ times on average, or about t^d/N^{d-1} times. A geometric argument yields the same result: there are N points in the hypercube $[0,N]^d$. We expect about $(t/N)^d$ of them to be in a subhypercube $\bar{b}+[0,t]^d$.

Let $\delta = |N|/q = \sum_{i=0}^{d-1} r_i\pi^i - 1$. Recall that by equation (10), the number of occurrences of any s-tuple in one period of $\mathbf{a}$ equals the cardinality of

$$\begin{aligned}\Gamma(r_0,\cdots,r_{d-1};N,t;\bar{b}) \quad &\stackrel{def}{=} \quad \{k(r_0,\cdots,r_{d-1}) + N(w_0,\cdots,w_{d-1}) : k, w_0,\cdots,w_{d-1} \in \mathbf{Z} \\ &\qquad \text{and } b_i \leq kr_i + Nw_i \leq b_i + t\}\end{aligned}$$

for some vector $\bar{b} = (b_0,\cdots,b_{d-1})$. For any such $\bar{b}$, let $B = \bar{b}+[0,t]^d$ be the hypercube with corner $\bar{b}$ and faces parallel to the coordinate hyperplanes. For any $\bar{w} = (w_0,\cdots,w_{d-1}) \in \mathbf{Z}^d$, we let

$$\Gamma_{\bar{w}}(r_0, \cdots, r_{d-1}; N, t; \bar{b}) \stackrel{def}{=} \{k(r_0, \cdots, r_{d-1}) + N(w_0, \cdots, w_{d-1}) \in B : k \in \mathbf{Z}\},$$

so that

$$\Gamma(r_0, \cdots, r_{d-1}; N, t; \bar{b}) = \cup_{\bar{w} \in \mathbf{Z}^d} \Gamma_{\bar{w}}(r_0, \cdots, r_{d-1}; N, t; \bar{b}).$$

We simply write Γ and $\Gamma_{\bar{w}}$ when the parameters are understood.

As in the case $d = 2$, we can estimate Γ by estimating the sum of the variations in the last coordinate along each $\Gamma_{\bar{w}}$, dividing by $|r_{d-1}|$, and adding an error term equal to the number of nonempty $\Gamma_{\bar{w}}$. If $L_{\bar{w}}$ is the line we obtain by allowing k to be an arbitrary real number in the definition of $\Gamma_{\bar{w}}$, then each $L_{\bar{w}}$ intersects the boundary of B twice, so the size of the number of nonempty $\Gamma_{\bar{w}}$ is bounded by one half the number of points of the form $k(r_0, \cdots, r_{d-1}) + N(w_0, \cdots, w_{d-1})$ on the boundary of B, with k real.

By symmetry it suffices to consider a single face of B, say determined by setting the first coordinate to b_0. This implies that $kr_0 + Nw_0 = b_0$, so $k = b_0 - (N/r_0)w_0$, and the intersection point is

$$\left(b_0, \left(b_0 - \frac{N}{r_0} w_0\right) r_1 + Nw_1, \cdots, \left(b_0 - \frac{N}{r_0} w_0\right) r_{d-1} + Nw_{d-1}\right).$$

But the number of such points is exactly

$$\Gamma\left(r_1, \cdots, r_{d-1}; |r_0|, \frac{t|r_0|}{N}; \frac{|r_0|}{N}(b_1 - b_0 r_1, \cdots, b_{d-1} - r_0 r_{d-1})\right). \tag{12}$$

This is an instance of the same problem, but with dimension one lower, so we can hope to bound it inductively.

Now suppose that we have shown inductively that for dimension $k < d$, $\Gamma(r_0, \cdots, r_{k-1}; N, t; \bar{b})$ is close to t^k/N^{k-1}, its expected value. Then the quantity in equation (12) is close to

$$\frac{(t|r_0|/N)^{d-1}}{|r_0|^{d-2}} = \frac{|r_0| t^{d-1}}{N^{d-1}} = \frac{|r_0|}{p^{s\frac{d-1}{d}}}.$$

For the remaining faces the error terms are the same, with r_0 replaced by other r_i. Thus the total ℓ of this error estimate is about

$$\ell \sim \frac{\sum_{i=0}^{d-1} |r_i|}{p^{s\frac{d-1}{d}}}.$$

However, the absolute norm of δ is N^{d-1}. Thus if ζ is a complex dth root of one, then

$$N^{d-1} = |\prod_{j=0}^{d-1} \sum_{i=0}^{d-1} r_i \zeta^{ji} \pi^i|$$

$$
\begin{aligned}
&\leq \prod_{j=0}^{d-1}\sum_{i=0}^{d-1}|r_i|\pi^i \\
&\leq \max\{|r_i|^d\}(\sum_{i=0}^{d-1}\pi^i)^d \\
&= \frac{\max\{|r_i|^d\}}{(\pi-1)^d}.
\end{aligned}
$$

Thus the error term we obtain is at least

$$
(\pi-1)\left(\frac{N}{p^s}\right)^{(d-1)/d},
$$

which is larger for $d > 2$ than for $d = 2$.

Acknowledgements

The author thanks Mark Goresky for several valuable conversations that helped lead to this result.

References

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

[2] Z. Borevich and I. Shafarevich, *Number Theory.* Academic Press, New York, 1966.

[3] C. F. Gauss, Disquisitiones Arithmeticae, 1801. Reprinted in English translation by Yale University Press, New Haven, CT, 1996.

[4] M. Goresky and A. Klapper, Periodicity, correlation, and distribution properties of d-FCSR sequences, to appear in *SIAM J. Comp.*

[5] M. Goresky and A. Klapper, Fibonacci and Galois representations of feedback with carry shift registers, to appear in *IEEE Trans. Info. Theory.*

[6] A. Klapper and M. Goresky, Feedback registers based on ramified extensions of the 2-adic numbers, *Advances in Cryptology - Eurocrypt 1994.* Lecture Notes in Computer Science **718**, Springer Verlag, New York, 1994, pp. 215–222.

[7] A. Klapper and M. Goresky, Feedback shift registers, 2-adic span, and combiners with memory, *J. Crypt.* **10** (1997), pp. 111–147.

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

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

[10] M. Matsumoto and T. Nishimura, Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator, *ACM Trans. Model. Comput. Simul.* **8** (1998) pp. 2–30.

[11] M. Simon, K. Omura, R. Scholtz, and B. Levitt, Spread Spectrum Communications Handbook. McGraw-Hill, 1994.