Expected π-Adic Security Measures of Sequences

Andrew Klapper, *Senior Member, IEEE*

***Abstract*—Various measures of security of stream ciphers have been studied that are based on the problem of finding a minimum size generator for the keystream in some special class of generators. These include linear and p-adic spans, as well as π-adic span, which is based on a choice of an element π in a finite extension of the integers. The corresponding sequence generators are known as linear feedback shift registers, feedback with carry shift registers, and the more general algebraic feedback shift registers, respectively. In this paper the average behavior of such security measures when $\pi^d = p > 0$ or $\pi^2 = -p < 0$ is studied. In these cases, if $\mathbb{Z}[\pi]$ is the ring of integers in its fraction field and is a UFD, it is shown that the average π-adic span is $n - O(\log(n))$ for sequences with period n.**

Keywords: algebraic feedback shift register, applied abstract algebra, security measure, stream cipher.

I. Introduction

A variety of measures, such as linear span and 2-adic span, have been proposed for deciding the cryptographic security of stream ciphers. Recently there has been interest in understanding the average behavior of such measures. Several variations have been studied, both for linear and 2-adic span [13], [14], [15], [16]. In this paper we extend this work to more general π-adic span, where π is an element of a general algebraic ring.

Many of these measures arise as follows: We are given a class $\mathcal{F}$ of sequence generators. There is a notion of *size* of a generator with a particular initial state. This integer should be approximately the number of elements of the output alphabet needed to represent all states in the execution of the generator starting at that initial state. That is, the size should be approximately the ceiling of the log with base equal to the size of the output alphabet of the cardinality of the state space. But for practical reasons it is usually the number of alphabet symbols in some natural encoding of the state space as strings. For example, if the state were a monic polynomial of degree d over a field, then it might be encoded as the d-tuple of its coefficients. Thus the size would be d, even if not all monic polynomials of degree d actually occurred as states.

The *$\mathcal{F}$-span* of a (finite or infinite) sequence is the smallest size of a generator in the given class that outputs the sequence. It is infinite if there is no such generator. Often there is another closely related measure that is defined algebraically and is easier to work with. We typically call this related measure the *$\mathcal{F}$-complexity*. It may be based on a function defined on some related algebraic structure that satisfies properties such as

$$f(ab) = f(a) + f(b)$$

or

$$f(a+b) \leq \max(f(a), f(b)) + c$$

for some constant c. In the case when $\mathcal{F}$ is the set of *linear feedback shift registers* (LFSRs) the $\mathcal{F}$-span is called the *linear span*. The size of an LFSR with connection polynomial $q(x)$ is simply the number of cells it contains. If the generating function of the output sequence is $u(x)/q(x)$, then the *linear complexity* is

$$\max(\deg(q), \deg(u) + 1)$$

and equals the linear span. In the case of *feedback with carry shift registers* (FCSRs) with output alphabet $\{0, 1, \cdots, N-1\}$, $N \in \mathbb{Z}$ [7], the $\mathcal{F}$-span is called the *N-adic span*. The integer values of the carry are encoded by their base N expansions. Thus the size of an FCSR with connection integer q is the number of cells in the basic register plus the ceiling of the log base N of the maximum absolute value of the carry over its infinite execution. If the output sequence has associated N-adic number $\alpha = u/q$, then the related *N-adic complexity* is

$$\log_N(\max(|u|, |q|)).$$

It is different from the N-adic span (it may not even be an integer) but the difference is in $O(\log(\text{the } N\text{-adic span}))$ [7].

More generally we may consider *algebraic feedback shift registers* (AFSRs) with respect to some particular algebraic ring R and parameter π. AFSRs include both LFSRs ($R = F[x]$ with F a field, $\pi = x$) and FCSRs ($R = \mathbb{Z}$, $\pi \geq 2$) [8]. The $\mathcal{F}$-span associated with the class $\mathcal{F}$ of AFSRs based on R and π is called the *π-adic span*. However, we know of no algebraic definition of a "π-adic complexity" that makes sense for all (or even many) classes of AFSRs.

Now we describe AFSRs in more detail. Let R be a commutative ring and $\pi \in R$. Assume that $R/(q)$ is finite for every nonzero $q \in R$. We consider sequences over the ring $R/(\pi)$, whose cardinality we denote by p. We also let $S \subseteq R$ be a fixed complete set of representatives for $R/(\pi)$. We identify sequences over $R/(\pi)$ with sequences over S. An AFSR based on R, π, and S is a stated device D with output. It is determined by constants $q_0, \cdots, q_r \in R$, $r \geq 1$, with the image of q_0 in $R/(\pi)$ invertible. Its state is an $(r+1)$-tuple

$$\sigma = (a_0, a_1, \cdots, a_{r-1}; m)$$

where $a_i \in S$, $i = 0, \cdots, r-1$, and $m \in R$. From this state the AFSR outputs a_0 and changes state to $(a_1, \cdots, a_r; m')$

Dept. of Computer Science, 779A Anderson Hall, University of Kentucky, Lexington, KY, 40506-0046. www.cs.uky.edu/∼klapper. Parts of this work were carried out while the author was visiting the Fields Institute at the University of Toronto; The Institute for Advanced Study; and Princeton University. This material is based upon work supported by the National Science Foundation under Grant Nos. CCF-0514660 and CCF-0914828. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

where $a_r \in S$ and

$$q_0 a_r + \pi m' = m + \sum_{i=1}^{r} q_i a_{r-i}.$$

By repeating the state change operation, the AFSR generates an infinite sequence, denoted by $D(\sigma)$. We refer to $D(\sigma)$ as the sequence generated by D with initial state σ. Note that in general an AFSR is not a finite state device (due to the carry m). However, it can be shown that in many important cases every AFSR goes through only finitely many distinct states in any infinite execution (equivalently, m is constrained to a finite set in any infinite execution and, equivalently, the state sequence is eventually periodic). In this paper we are concerned with average behavior of the $\mathcal{F}$-span where $\mathcal{F}$ is the class of AFSRs based on R, π, S. The $\mathcal{F}$-span is commonly referred to as the π-adic span. See [8] for more details on AFSRs and their analysis by π-adic numbers.

The element

$$q^D = q = \sum_{i=1}^{r} q_i \pi^i - q_0 \qquad (1)$$

is known as the *connection element* of the AFSR. If we start with q, we denote by D_q the AFSR with q the connection element.[1] We may also refer to it as a connection element for any sequence $\mathbf{a}$ generated by D_q. Any given sequence has many connection elements. The connection element plays a critical role in the analysis of AFSR sequences. We can associate a *π-adic integer*

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i$$

to the sequence $\mathbf{a} = a_0, a_1, \cdots$, $a_i \in S$. The set of all π-adic integers is a ring in a natural way. But note that this is not simply a power series ring – the sum or product of two elements of S may not be in S, so expressing sums and products of π-adic integers as π-adic integers in general involves complicated carries to higher degree terms, perhaps even carries to infinitely many terms. Again, we refer to [8] for more details on π-adic integers.

If q is as in equation (1) with q_0 invertible modulo π, then any rational element $u/q \in R[1/q]$, $u \in R$, can also be expressed as such a π-adic integer[2] and it can be shown that $\mathbf{a}$ is the output from an AFSR with connection element q if and only if there exists $u \in R$ so that $u/q = \alpha$. In fact u can be expressed in terms of the initial state $(a_0, \cdots, a_{r-1}; m)$ by

$$\begin{aligned} \alpha &= \frac{\sum_{n=0}^{r-1}\sum_{i=1}^{n} q_i a_{n-i}\pi^n - q_0 \sum_{n=0}^{r-1} a_n \pi^n - m\pi^r}{q} \\ &= \frac{u}{q}. \qquad (2) \end{aligned}$$

The question of what values to allow as the coefficients q_i is a delicate one. In theory one may allow arbitrary elements of R to be q_is (as long as q_0 is invertible modulo π). But this would make implementation of AFSRs potentially problematic and complicate defining the size of an AFSR. At the other extreme, we might restrict the q_i to be in the complete set S of representatives modulo π. But this would lead to situations where not all q that are invertible modulo π can be realized as connection elements of AFSRs. For example, if $R = \mathbb{Z}$, π is a positive integer, and $S = \{0, 1, \cdots, \pi - 1\}$, then most negative integers q cannot be written in the form in equation (1). We settle for an intermediate solution: we assume there is a finite *coefficient set* $T \subset R$ such that every element of R can be expressed as a finite linear combination of powers of π with coefficients in T (perhaps not uniquely). This will be an assumption throughout the paper. In the example above, we might take $T = \{-\pi+1, -\pi+2, \cdots, \pi-2, \pi-1\}$. Note that varying T only affects our estimates of the average span by an additive constant.

More discussion of AFSRs, π-adic numbers, and π-adic size measures can be found in a paper by Xu and Klapper [17]. We emphasize that the π-adic span of an AFSR depends both on the structure of the AFSR (that is, on the connection element q) and on a particular initial state. It also depends on T and the specific class $\mathcal{F}$. For example, if we replaced Fibonacci mode AFSRs by Galois mode AFSRs, the span would also change in general.

The π-adic span of a sequence is important as a security measure if there is an *AFSR synthesis algorithm* for R, π, S, and T. This is an algorithm which takes a prefix of a sequence as input and outputs a minimal AFSR over R, π, and S that outputs the prefix. If the prefix is sufficiently large (typically a constant times the π-adic span of the sequence), then the AFSR in fact generates the entire sequence. Thus if such an algorithm is known (register synthesis algorithms are only known for certain types of AFSRs [17]), any sequence used as a key in a stream cipher should have large π-adic span. $\mathcal{F}$-synthesis algorithms are known in a number of cases, notably for LFSRs (the Berlekamp-Massey algorithm [12]), for FCSRs (the 2-adic Rational Approximation algorithm [7] and the Euclidean algorithm [1]), and AFSRs over various extensions of the integers, including the cases where we estimate the average $\mathcal{F}$-span in this paper (Xu's algorithm [17]). In all these cases the length of the required prefix of the sequence is linear in the $\mathcal{F}$-span and the time complexity of the algorithm is quadratic in the number of symbols used. It is important, then, to understand the average behavior of π-adic span, as has been done for linear span and 2-adic span [13], [14], [15], [16].

The π-adic span of an infinite sequence is not always defined. As is the case with linear feedback shift registers and feedback with carry shift registers, some sequences are not generated by any AFSR over R, π, and S at all. For example, the sequences generated by LFSRs are exactly the eventually periodic sequences. Thus they make up a countable subset of the uncountable set of all sequences over S. The same is true of the sequences generated by FCSRs. However, some AFSRs generate sequences that are not eventually periodic. This implies that the memory is unbounded over an infinite execution of the AFSR, so the π-adic span is infinite. However,

[1] We are being a little sloppy here since a given q may have several representations in the form in equation (1), but this causes no problems in what follows.

[2] Actually, for this statement to be true we need a *separability condition* on R, that $\cap_{i=1}^{\infty}(\pi)^i = (0)$. This condition always holds when $R = \mathbb{Z}[\pi]$ and π is integral over $\mathbb{Q}$.

it is known that if R is an integral domain whose field of fractions is a number field, and for every embedding of R in the complex numbers, the complex norm of π is greater than 1, then the memory of every AFSR is bounded over every infinite execution [8]. When this happens, the sequences for which π-adic span is defined are exactly the eventually periodic sequences. This is the case for all rings studied here.

Our goal in this paper is to find the average π-adic span of periodic sequences with fixed period n. All such sequences have $\pi^n - 1$ as a connection element. Thus we can generalize to finding (or estimating) the average π-adic span of sequences with a fixed q as a connection element. We work initially as generally as possible, then specialize to particular rings.

In Section II we study notions of the span of sequences associated with a class of AFSRs. In Section III we lower bound the expected span in terms of minimal connection elements of sequences. In Section IV we relate the algebraic norm and sizes of AFSRs and introduce two classes of algebraic number fields whose associated AFSRs we focus on in the remainder of the paper: $R = \mathbb{Z}[\pi]$ where either $\pi^2 = -p < 0$ with $p \in \mathbb{Z}$, or $\pi^d = p > 0$ with $p \in \mathbb{Z}$ and $x^d - p$ irreducible over $\mathbb{Z}$. in Section V we lower bound the number of n-periodic sequences with a given minimal connection element. In Section VI we put the results of the previous sections to prove our main result that in the cases of R just mentioned, if R is a unique factorization domain, then the expected π-adic span is at least $n - O(\log(n))$ (see Theorem 4). Finally, in Section VII we discuss the extension of these results to rings $\mathbb{Z}[\pi]$ whose integral closure is a unique factorization domain.

Some of the results in this paper have appeared previously in the SETA 2008 conference [10]. That paper was restricted to the case where $\pi^2 = 2$, and many of the proofs were omitted.

II. Definitions: Size, Span, and Complexity

In this section we give formal definitions of and basic results on the span and complexity of sequences based on a notion of the size of an element of the ring R.

Definition 1: Let R be a ring. A *size function on R relative to π* is a function

$$\lambda : R \to \mathbb{R}^{\geq 0}$$

satisfying the following axioms.

S1: The size of a sum is at most the maximum of the sizes of the addends plus a constant. That is, there is a constant c_1 so that for all $a, b \in R$,

$$\lambda(a \pm b) \leq \max(\lambda(a), \lambda(b)) + c_1;$$

S2: The size of a product is at most the sum of the sizes of the multiplicands plus a constant. That is, there is a constant c_2 so that for all $a, b \in R$,

$$\lambda(ab) \leq \lambda(a) + \lambda(b) + c_2;$$

S3: Multiplying by π increases the size by one. That is, for all $a \in R$,

$$\lambda(\pi a) = 1 + \lambda(a);$$

S4: There is a constant c_4 so that for all $a_0, \cdots, a_{r-1} \in S$ with $a_{r-1} \neq 0$,

$$\left| \lambda \left(\sum_{i=0}^{r-1} a_i \pi^i \right) - r \right| \leq c_4.$$

S5: For any real number x, there are finitely many elements $a \in R$ with $\lambda(a) \leq x$.

For example, if $R = F[x]$ is a polynomial ring over a finite field F, $\pi = x$, and $S = F$, then these axioms hold with $\lambda(a)$ equal to the degree of a and $c_1 = c_2 = 0$ and $c_4 = 1$. If $R = \mathbb{Z}$, $\pi \geq 2$, and $S = \{0, 1, \cdots, \pi - 1\}$, then the axioms hold with

$$\lambda(a) = \log_\pi(|a|), \quad c_1 = \log_\pi(2), \quad c_2 = 0, \text{ and } c_4 = 1.$$

They also hold with

$$\lambda(a) = r \text{ if } |a| = \sum_{i=0}^{r-1} a_i \pi^i$$

with all $a_i \in S$ and $a_{r-1} \neq 0$. That is, $\lambda(a) = \lceil \log_\pi(|a| + 1) \rceil$. In this case $c_1 = 1$, $c_2 = 1$, and $c_4 = 0$. More examples appear later in the paper.

Lemma 1: If axiom S1 holds, then for any $a_1, \cdots, a_n \in R$ we have

$$\lambda(a_1 \pm \cdots \pm a_n) \leq \max\{\lambda(a_i), i = 1, \cdots, n\} + c_1 \lceil \log_2(n) \rceil .$$

Proof: By axiom S1 we have

$$\begin{aligned} \lambda(a_1 \pm \cdots \pm a_n) \quad \leq \quad & \max(\lambda(a_1 \pm \cdots \pm a_{\lfloor n/2 \rfloor}), \\ & \lambda(a_{\lfloor n/2 \rfloor + 1} \pm \cdots \pm a_n)) + c_1. \end{aligned}$$

The lemma then follows by induction on n. □

Such a size function λ is extended to states of an AFSR and to sequences generated by AFSRs.

Definition 2: Let λ be a size function on R relative to π.

1) If $(a_0, \cdots, a_{r-1}; m)$ is a state, then

$$\lambda(a_0, \cdots, a_{r-1}; m) = r + \lambda(m).$$

2) If D is an AFSR and λ is a state of D, then $\lambda(D, \sigma)$ is the maximum of $\lambda(\tau)$ over all states τ that occur in the infinite execution of the AFSR starting with initial state σ.

3) Let $\mathbf{a}$ be a sequence over S. Then $\lambda(\mathbf{a})$ is the minimum of $\lambda(D, \sigma)$ over all AFSRs D and states σ so that $D(\sigma) = \mathbf{a}$, if there are any. If not, then $\lambda(\mathbf{a}) = \infty$.

We refer to $\lambda(\mathbf{a})$ as the *π-adic span* of $\mathbf{a}$.

Note that the π-adic span of $\mathbf{a}$ depends on the choice of $\lambda : R \to \mathbb{R}$, as well as the choice of R, π, S, and T.

As discussed in Section I, it is sometimes desirable to find a more algebraically defined measure, π-adic complexity, that approximates π-adic span.

Definition 3: For any pair of elements $a, b \in R$, let

$$\phi(a,b) = \max(\lambda(a), \lambda(b)).$$

Let $\mathbf{a} = a_0, a_1, \cdots$ be a sequence over S with associated π-adic number

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i.$$

If α has a rational representation, $\alpha = u/q$, then let

$$\phi(\mathbf{a}) = \min\{\phi(u,q) : \alpha = u/q\}.$$

Otherwise $\phi(\mathbf{a}) = \infty$. We refer to $\phi(\mathbf{a})$ as the *π-adic complexity of* $\mathbf{a}$.

If $\mathbf{a}$ is a periodic sequence over S, say with period n, then the associated π-adic element is $v/(1-\pi^n)$ where

$$v = \sum_{i=0}^{n-1} a_i \pi^i.$$

Thus

$$\phi(\mathbf{a}) \le n + O(\log(n)).$$

Note that if R is a unique factorization domain (see Section III), then there is a minimal connection element of $\mathbf{a}$, in the sense that it divides all other connection elements. In particular, it divides $\pi^n - 1$.

Let Γ_n denote the set of pairs (D, σ) such that D is an AFSR, σ is a state of D, and $D(\sigma)$ has period n.

Now suppose that $\mathbf{a} = a_0, a_1, \cdots$ is a sequence over S. Suppose that $D_q(\sigma) = \mathbf{a}$ for some initial state σ, and $\lambda(\mathbf{a}) = \lambda(D_q, \sigma)$. We say that the pair (q, σ) is a *witness* to $\lambda(\mathbf{a})$.

We want to show that the carry m of the AFSRs makes a negligible contribution to the expected π-adic span of a periodic sequence.

Lemma 2: Let $\sigma = (a_0, \cdots, a_{r-1}; m)$ be a state of an AFSR D_q with

$$q = \sum_{i=1}^{r} q_i \pi^i - q_0, \quad q_i \in T.$$

Suppose the π-adic number associated with $D_q(\sigma)$ is u/q. Then

$$\begin{aligned}
\lambda(\sigma) &\le \max(\lambda(u), r + O(\log(\lambda(q)))) + c_1 \\
&\le \max(\lambda(u), r + O(\log(r))) + c_1.
\end{aligned}$$

Proof: By equation (2) we have

$$m\pi^r = \sum_{n=1}^{r-1} \sum_{i=1}^{n} q_i a_{n-i} \pi^n - q_0 \sum_{n=0}^{r-1} a_n \pi^n - u.$$

Thus

$$\begin{aligned}
\lambda(\sigma) &= r + \lambda(m) \\
&= \lambda(\pi^r m) \\
&\le \max\left(\lambda(u), \lambda\left(\sum_{n=1}^{r-1}\sum_{i=1}^{n} q_i a_{n-i}\pi^n \right.\right. \\
&\qquad\qquad \left.\left. -q_0 \sum_{n=0}^{r-1} a_n \pi^n\right)\right) + c_1 \\
&\le \max(\lambda(u), \max\{\lambda(st\pi^r) : s \in S, t \in T\} \\
&\qquad + \left\lceil \log_2\left(r^2 + \frac{r}{2}\right)\right\rceil c_1) + c_1 \\
&\le \max(\lambda(u), r + 2\log(r) + e) + c_1 \\
&\le \max(\lambda(u), r + 2\log(\lambda(q) + f) + e) + c_1 \\
&\le \max(\lambda(u), r + 2\log(\lambda(q)) + g) + c_1 \\
&\le \max(\lambda(u), r + O(\log(\lambda(q)))) + c_1,
\end{aligned}$$

where e, f, and g are constants. This proves the first inequality. The second inequality follows from Lemma 1. □

It follows that the size of the AFSR in its initial state is at most

$$\max(\lambda(u), \lambda(q) + O(\log(\lambda(q)))) + c_1.$$

We want to bound the size of the carry throughout the execution of D_q. Let the memory after j state changes be denoted by m_j. If we take the state after j state changes as a new initial state, then the output is $a_j, a_{j+1}, \cdots$ and the associated π-adic number is u_j/q for some u_j. Thus the size of the AFSR after j state changes is bounded by

$$\max(\lambda(u_j), \lambda(q) + O(\log(\lambda(q)))) + c_1.$$

Lemma 3: Suppose that $\mathbf{a}$ is strictly periodic with period n. Then

$$\lambda(\mathbf{a}) \in \lambda(q) + O(\log(\lambda(q))) = r + O(\log(r)).$$

Proof: Since by axiom S5 there are only finitely many elements z in R with $\lambda(z) \le \lambda(u)$, if we take n sufficiently large we may assume that

$$\lambda(u) < \lambda(u(\pi^n - 1)).$$

We have

$$\frac{u}{q} = \frac{v}{\pi^n - 1},$$

where

$$v = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}.$$

Thus

$$u(\pi^n - 1) = vq.$$

Then

$$\begin{aligned}
n+\lambda(u) &= \lambda(u\pi^n) \\
&= \lambda(u(\pi^n-1)+u) \\
&\le \max(\lambda(u(\pi^n-1)),\lambda(u))+c_1 \\
&= \lambda(u(\pi^n-1))+c_1 \\
&= \lambda(vq)+c_1 \\
&\le \lambda(v)+\lambda(q)+c_2+c_1.
\end{aligned}$$

Therefore

$$\begin{aligned}
\lambda(u) &\le \lambda(q)+\lambda(v)-n+c_2+c_1 \\
&\le \lambda(q)+c_4+c_2+c_1.
\end{aligned}$$

Since the output of the AFSR is periodic if it is begun from any state $(a_j,\cdots,a_{j+r-1};m_j)$, the same bound applies to every $\lambda(u_j)$. Combining this with Lemma 2 proves the current lemma. □

Corollary 1: For any sequence $\mathbf{a}$ over S we have

$$\lambda(\mathbf{a}) \le \phi(\mathbf{a})+O(\log(\phi(\mathbf{a}))).$$

III. Expected π-Adic Span

Our goal is to approximate the expected π-adic span of sequences with fixed period n. This expected value is upper bounded by $n+O(1)$, so we focus on finding lower bounds, hopefully of the form $n-O(\text{small})$. Let R, π, S, and T be as before.

Let λ be a size function for R. Let Γ_n^* denote the set of pairs $(D,\sigma)\in\Gamma_n$ such that (q^D,σ) is a witness to $\lambda(D(\sigma))$, i.e., such that $\lambda(D(\sigma))=\lambda(D,\sigma)$. Suppose $(D,\sigma)\in\Gamma_n^*$ and

$$q^D=\sum_{i=1}^r q_i\pi^i-q_0.$$

If there is more than one such minimal (D,σ), we choose one arbitrarily. Then

$$\lambda(D(\sigma))\ge r\ge\lambda\left(\sum_{i=1}^r q_i\pi^i\right)-c_4$$

by axiom S4. Furthermore,

$$\begin{aligned}
\lambda(q^D) &= \lambda\left(\sum_{i=1}^r q_i\pi^i-q_0\right) \\
&\le \max(\lambda\left(\sum_{i=1}^r q_i\pi^i\right),\lambda(q_0))+c_1 \\
&\le \lambda\left(\sum_{i=1}^r q_i\pi^i\right)+\max(\lambda(t):t\in T)+c_1.
\end{aligned}$$

It follows that

$$\lambda(D(\sigma))\ge\lambda(q^D)-c$$

for some constant c.

There are two notions of minimality that we can consider for connection elements of a sequence $\mathbf{a}$. We denote by $q_{\mathbf{a}}\in R$ a connection element that is a witness to $\lambda(\mathbf{a})$ and say that $q_{\mathbf{a}}$ is λ-*minimal* for $\mathbf{a}$ (if there is not a unique witness we simply choose one to call $q_{\mathbf{a}}$). A connection element q is R-*minimal* if it divides every other connection element of $\mathbf{a}$. The two notions are not equivalent, since we might have $\lambda(zq)<\lambda(q)$ for some z. Nor is a minimal element necessarily unique. For example, if q is R-minimal for $\mathbf{a}$ and z is a unit, then zq is also R-minimal for $\mathbf{a}$. In fact, there may be no R-minimal connection element for $\mathbf{a}$ at all.

Let E_n^λ be the expected π-adic span of the set of sequences with period n over an alphabet with p elements. Thus

$$\begin{aligned}
E_n^\lambda &= \frac{1}{p^n}\sum_{\mathbf{a}}\lambda(\mathbf{a}) \\
&= \frac{1}{p^n}\sum_{\mathbf{a}}\lambda(D_{\mathbf{a}}(\sigma_{\mathbf{a}})) \\
&\ge \frac{1}{p^n}\sum_{\mathbf{a}}(\lambda(q_{\mathbf{a}})-c) \\
&= \left(\frac{1}{p^n}\sum_{\mathbf{a}}\lambda(q_{\mathbf{a}})\right)-c, \qquad (3)
\end{aligned}$$

where the sums are over all periodic sequences over $R/(\pi)$ with period n.

IV. Norms and Examples

From this point on in the paper we focus on AFSRs whose underlying ring is of the form $R=\mathbb{Z}[\pi]$, where π is an algebraic number and is not a unit. We do not know whether for every such ring R there is a finite set T such that every element of R can be expressed as a finite linear combination of powers of π with coefficients in T, so we must check this in the specific cases we consider later.

In this section we review some basic properties of the algebraic norm that are useful later. Let F be a finite extension of the rational numbers $\mathbb{Q}$. Then there is a *norm function* $N:F\to\mathbb{Z}$. If $a\in F$, then $N(a)$ can be defined as the norm of the matrix representation of the linear function "multiply by a". This is a multiplicative function (meaning that $N(ab)=N(a)N(b)$ for all $a,b\in F$) whose properties can be found in any good book on abstract algebra or algebraic number theory. If F is a Galois extension of $\mathbb{Q}$ and G is the Galois group of F over $\mathbb{Q}$, then also

$$N(a)=\prod_{g\in G}g(a).$$

If R is the ring of integers in F (i.e., the roots of monic polynomials with integer coefficients), then N maps R into $\mathbb{Z}$. An element in R is a unit if and only if its norm is 1 or -1.

Lemma 4: If $R=\mathbb{Z}[\pi]$ with π integral, F is the fraction field of R and $z\in R$, then $|R/(z)|=|N(z)|$.

This follows from basic results in number theory [2, Lemma 1, p. 125].

We will also need to know about the density of primes.

Theorem 1: (Landau's Theorem [3, p. 448]) If F is a number field and R is the ring of integers in F, then the number of prime ideals with norm at most n is asymptotically $n/\ln(n)$.

If R is a principal ideal domain, then there is a one to one correspondence between the set of prime ideals and the set of irreducible elements, where we identify elements that are associates[3].

Corollary 2: If F is a number field, R is the ring of integers in F, and R is a principal ideal domain, then the number of irreducible elements in R with norm at most n is asymptotically $n/\ln(n)$ (where we identify elements that are associates).

A. $\pi^2 = -p < 0$

Suppose that $p \geq 2$ is an integer, so that x^2+p is irreducible, and $F = \mathbb{Q}[\pi]$ with $\pi^2 = -p$. We let $R = \mathbb{Z}[\pi]$ and $S = \{0, 1, \cdots, p-1\}$. The only units in R are 1 and -1. If p is square-free, then the ring of integers in F is $\mathbb{Z}[(1+\pi)/2]$ if $p \equiv 3 \mod 4$ and is $\mathbb{Z}[\pi]$ otherwise. The only units in the ring of integers are 1 and -1, unless $p = 3u^2$ for some integer u, when the elements $(\pm 1 \pm \sqrt{3})/2$ are also units.

We can parametrize R by $R = \{b = b_0 + b_1\pi : b_i \in \mathbb{Z}\}$. If we write

$$b_i = \pm \sum_{j=0}^{k} b_{i,j} p^j = \sum_{j=0}^{k} \pm b_{i,j} \pi^{2j}$$

with $b_{i,j} \in S$, then we have

$$b = b_0 + b_1\pi = \sum_{i=0}^{1} \sum_{j=0}^{k} \pm b_{i,j} \pi^{2j} = \sum_{\ell=0}^{2k+1} c_\ell \pi^\ell,$$

with

$$c_\ell \in \{-(p-1), -(p-2), \cdots, p-1\} = S \cup -S.$$

Thus we let T be this set.

We have

$$N(b_0 + b_1\pi) = b_0^2 + pb_1^2 \geq 0$$

and so

$$|R/(\pi)| = |\mathbb{Z}/(p)| = p = |N(\pi)|.$$

Define

$$\lambda(z) = \log_p(N(z)). \qquad (4)$$

This is the same size function that was used to establish the existence of a rational approximation algorithm for AFSRs over quadratic imaginary fields [17].

Theorem 2: If λ is defined as above, then axioms S1, S2, S3, S4, and S5 are satisfied with $c_1 = \log_p(8)$, $c_2 = 0$, and $c_4 = \log_p(2)$.

Proof: Let

$$\alpha = a_0 + a_1\pi \text{ and } \beta = b_0 + b_1\pi$$

with $a_0, a_1, b_0, b_1 \in \mathbb{Z}$. we have

$$\begin{aligned} (a_0 + b_0)^2 &\leq (2\max(a_0, b_0))^2 \\ &\leq 4\max(N(\alpha), N(\beta)), \end{aligned}$$

and similarly

$$p(a_1 + b_0)^2 \leq 4\max(N(\alpha), N(\beta)).$$

Thus

$$N(\alpha + \beta) \leq 8\max(N(\alpha), N(\beta))$$

and so

$$\lambda(\alpha + \beta) \leq \max(\lambda(\alpha), \lambda(\beta)) + \log_p(8).$$

This gives axiom S1.

The norm function is multiplicative, so axioms S2 and S3 are immediate.

For axiom S4, we have

$$\begin{aligned} \lambda(a + b\pi) &= \log_p(a^2 + pb^2) \\ &\leq \log_p(2\max(a^2, pb^2)) \\ &= \max(2\log_p|a|, 2\log_p|b| + 1) + \log_p(2). \end{aligned}$$

Also,

$$\begin{aligned} \lambda(a + b\pi) &= \log_p(a^2 + pb^2) \\ &\geq \log_p(\max(a^2, pb^2)) \\ &= \max(2\log_p|a|, 2\log_p|b| + 1). \end{aligned}$$

Thus

$$|\lambda(\alpha) - \max(2\log_p|a|, 2\log_p|b| + 1)| \leq \log_p(2).$$

For axiom S5, we have

$$|a_0| \leq N(\alpha)^{1/2} \text{ and } |a_1| \leq p^{-1}N(\alpha)^{1/2},$$

so the set of elements with bounded norm is finite. □

In order to analyze sequences of period n, we need to know the norm of $\pi^n - 1$.

Lemma 5: We have

$$N(\pi^n - 1) = \begin{cases} p^n - 2p^{n/2} + 1 & \text{if } 4|n \\ p^n + 2p^{n/2} + 1 & \text{if } n \equiv 2 \mod 4 \\ p^n - 1 & \text{if } n \text{ is odd.} \end{cases}$$

Thus $\log_p|N(\pi^n - 1)| \in n + o(1)$.

Proof: The proof is straightforward. □

[3] Recall that elements $x, y \in R$ are *associates* if there is a unit $u \in R$ with $x = uy$.

B. $\pi^d = p > 0$

Suppose that $p, d \geq 2$ are integers, that $F = \mathbb{Q}[\pi]$ with $\pi^d = p$, and that $x^d - p$ an irreducible polynomial. Then

$$N\left(\sum_{i=0}^{d-1} b_i \pi^i\right) = \prod_{j=0}^{d-1}\left(\sum_{i=0}^{d-1} b_i \zeta^{ij}\pi^i\right),$$

where ζ is a complex primitive dth root of 1.

Let $R = \mathbb{Z}[\pi]$ and $S = \{0, 1, \cdots, p-1\}$. Then

$$R = \left\{\sum_{i=0}^{d-1} b_i \pi^i : b_i \in \mathbb{Z}\right\}.$$

Note that $|R/(\pi)| = p$. AFSRs over such a ring are called d-FCSRs, and many of their properties have been studied [4], [5], [6], [9]. By an argument similar to the one in Section IV-A, we can take $T = \{-(p-1), -(p-2), \cdots, p-1\}$.

We define

$$\lambda\left(\sum_{i=0}^{d-1} b_i \pi^i\right) = \max(d \log_p |b_i| + i).$$

This is the same size function that was used to establish the existence of a rational approximation algorithm for d-FCSRs [17].

Theorem 3: If λ is defined as above, then axioms S1, S2, S3, S4, and S5 are satisfied with $c_1 = d\log_p(2)$, $c_2 = d\log_p(d)$, and $c_4 = d$.

Proof: Let

$$\alpha = \sum_{i=0}^{d-1} a_i \pi^i \text{ and } \beta = \sum_{i=0}^{d-1} b_i \pi^i.$$

For axiom S1 we have

$$\begin{aligned}
\lambda(\alpha \pm \beta) &= \max\{d \log_p |a_i \pm b_i| + i\} \\
&\leq \max\{d \log_p(2\max(|a_i|, |b_i|)) + i : \\
&\quad i = 0, \cdots, d-1\} \\
&= \max\{d \log_p |a_i| + i, d\log_p |b_i| + i : \\
&\quad i = 0, \cdots, d-1\} + d\log_p(2) \\
&= \max(\lambda(\alpha), \lambda(\beta)) + d\log_p(2).
\end{aligned}$$

For axiom S2 first observe that

$$\alpha\beta = \sum_{i=0}^{d-1} e_i \pi^i$$

where

$$e_i = \sum_{j=0}^{i} a_j b_{i-j} + p\sum_{j=i+1}^{d-1} a_j b_{i+d-j}.$$

Then we have

$$\begin{aligned}
\lambda(\alpha\beta) &= \max\{d\log_p(e_i) + i : i = 0, \cdots, d-1\} \\
&\leq \max\{d\log_p(d\max\{|a_j b_{i-j}|, p|a_j b_{i+d-j}| : \\
&\quad j = 0, \cdots, d-1\}) + i : i = 0, \cdots, d-1\} \\
&= \max\{d\log_p |a_j b_{i-j}| + i, d\log_p |a_j b_{i+d-j}| + i \\
&\quad + d : j = 0, \cdots, d-1, i = 0, \cdots, d-1\} \\
&\quad + d\log_p(d) \\
&= \max\{d\log_p |a_i b_j| + i + j : i, j = 0, \cdots, d-1\} \\
&\quad + d\log_p(d) \\
&\leq \max\{d\log_p |a_i| + i : i = 0, \cdots, d-1\} \\
&\quad + \max\{d\log_p |b_j| + j : j = 0, \cdots, d-1\} \\
&\quad + d\log_p(d) \\
&= \lambda(\alpha) + \lambda(\beta) + d\log_p(d).
\end{aligned}$$

For axiom S3, we have

$$\begin{aligned}
\lambda(\pi\alpha) &= \lambda(pa_{d-1} + \sum_{i=1}^{d-1} a_{i-1}\pi^i) \\
&= \max(d\log_p(pa_{d-1}), d\log_p(a_0) + 1, \cdots, \\
&\quad d\log_p(a_{d-1}) + d) \\
&= 1 + \lambda(\alpha).
\end{aligned}$$

For axiom S4, suppose $a_i \in S = \{0, \cdots, p-1\}$, $i = 0, \cdots, r$, and $a_r \neq 0$. Let

$$\begin{aligned}
\gamma &= \sum_{i=0}^{r} a_i \pi^i \\
&= \sum_{j=0}^{d-1} (a_j + pa_{j+d} + \cdots + p^{\lfloor (r-j)/d \rfloor} a_{j+\lfloor (r-j)/d \rfloor d})\pi^j.
\end{aligned}$$

Then

$$\begin{aligned}
\lambda(\gamma) &= \max\left\{d\log_p\left(\sum_{i=0}^{\lfloor (r-j)/d \rfloor} a_{j+id} p^i\right) + j : \right. \\
&\quad \left. j = 0, \cdots, d-1\right\} \\
&\leq \max\left\{d\left(\left\lfloor \frac{r-j}{d} \right\rfloor + 1\right) + j : \right. \\
&\quad \left. j = 0, \cdots, d-1\right\} \\
&\leq r + d.
\end{aligned}$$

Also,

$$a_r \pi^r = a_r p^{\lfloor r/d \rfloor} \pi^{r - d\lfloor r/d \rfloor}$$

is nonzero, so the log of the coefficient of

$$\pi^{r - d\lfloor r/d \rfloor}$$

is at least $\lfloor r/d \rfloor$. Thus $\lambda(\gamma) \geq r$.

Finally, axiom S5 holds because there are finitely many integers a with $\log_p |a|$ less than any given bound. This completes the proof. □

Lemma 6: Suppose that $F = \mathbb{Q}[\pi]$ with $\pi^d = p$ and $x^d - p$ an irreducible polynomial. Let $R = \mathbb{Z}[\pi]$ and let $z \in R$. Then

1) $\log_p |N(z)| \leq d \log_p(d) + \lambda(z)$.
2) If $d = 2$, then $\log_p |N(z)| \leq \lambda(z)$.
3) If $d = 2$ and R is the full ring of integers in its fraction field, then there is a unit $u \in R$ and a constant $c_p \in \mathbb{R}^+$ so that $\lambda(uz) \leq 2\log_p(|N(z)| + c_p) - \log_p(4)$.
4) If $d = 2$ and $p = 2$, then there is a unit $u \in R$ so that $\lambda(uz) \leq \log_2 |N(z)| + 1$.

Proof: To prove the first statement, observe that if

$$z = \sum_{i=0}^{d-1} b_i \pi^i \text{ with } b_i \in \mathbb{Z},$$

and ζ is a complex primitive dth root of unity, then

$$\begin{aligned} |N(z)| &= \left| \prod_{j=0}^{d-1} \left(\sum_{i=0}^{d-1} b_i \zeta^{ij} \pi^i \right) \right| \\ &\leq \prod_{j=0}^{d-1} \left(\sum_{i=0}^{d-1} |b_i \zeta^{ij} \pi^i| \right) \\ &\leq \prod_{j=0}^{d-1} (d \max |b_i| p^{i/d}) \\ &= d^d \max |b_i|^d p^i. \end{aligned}$$

Thus

$$\log_p |N(z)| \leq d \log_p(d) + \lambda(z)$$

as claimed.

When $d = 2$,

$$N(b_0 + b_1 \pi) = b_0^2 - p b_1^2,$$

so

$$|N(z)| \leq \max(b_0^2, p b_1^2).$$

Thus

$$\log_p |N(z)| \leq \max(2 \log_p |b_0|, 1 + 2 \log_p |b_1|) = \lambda(z)$$

as claimed in the second statement.

To prove the third statement, suppose that $d = 2$ and R is the full ring of integers in its fraction field. We can consider R to be a subset of the real numbers. The group of units in R is isomorphic to $\{1, -1\} \times \mathbb{Z}$ [2]. This isomorphism can be arranged so that there is a generator v of the infinite part that is a real number greater than 1. This is the so-called *fundamental unit*. So it suffices to see that the lemma is true when u or $-u$ is a power of v or v^{-1}.

Let $z = a + b\pi$. If z is a unit, we can take $u = z^{-1}$. If $z = 0$, the result is trivial. So assume that z is neither 0 nor a unit. Both $N(z)$ and $\lambda(z)$ are unchanged by multiplying z by -1 and by replacing z by its Galois conjugate $a - b\pi$. Also, the conjugate of the product uz is the product of the conjugates of u and z, and u is a unit if and only if its conjugate is a unit. Thus we can multiply z by -1 or replace z by its conjugate. Therefore we may assume that a and b are positive, so that $z > 1$. It follows that for some k we have

$$v^k < z < v^{k+1}.$$

Take $u = v^{-k}$ so that $1 < uz < v$. We can replace z by uz and assume that

$$1 < z < v. \tag{5}$$

Suppose that $N(z) > 0$. We have

$$a - b\pi = \frac{N(z)}{z},$$

so also

$$\frac{N(z)}{v} < a - b\pi < N(z). \tag{6}$$

Adding equations (5) and (6) and dividing by 2 gives

$$\frac{N(z) + v}{2v} < a < \frac{N(z) + v}{2}.$$

Subtracting the equations and dividing by 2 gives

$$\frac{1 - N(z)}{2\pi} < b < \frac{v^2 - N(z)}{2\pi v}.$$

Thus

$$\lambda(a + b\pi) \leq 2 \log_p(N(z) + v) - \log_p(4).$$

Now suppose that $N(z) < 0$. We have

$$N(z) < a - b\pi < \frac{N(z)}{v}. \tag{7}$$

Adding equations (5) and (7) and dividing by 2 gives

$$\frac{N(z) + 1}{2} < a < \frac{N(z) + v^2}{2v}.$$

Subtracting the equations and dividing by 2 gives

$$\frac{1 - N(z)}{2\pi} < b < \frac{v^2 - N(z)}{2\pi v}.$$

Thus

$$\lambda(a + b\pi) \leq 2 \log_p(|N(z)| + v) - \log_p(4).$$

This proves the third assertion with $c_p = v$.

Finally, consider the fourth statement. As before, we may assume that $a, b \geq 0$. Suppose that $b \geq a$. Then

$$b^2 \leq 2b^2 - a^2 = |N(z)|,$$

so

$$a \leq b \leq |N(z)|^{1/2}.$$

Thus

$$\lambda(z) = \max(2 \log_2(a), 1 + 2 \log_2(b)) \leq \log_2 |N(z)| + 1,$$

as claimed. Similarly, if $b = 0$, then

$$a = |N(z)|^{1/2},$$

and the same bound holds.

Now suppose $a > b > 0$. Multiplying z by $w = -1 + \pi$ (the negative of the conjugate of the fundamental unit) gives

$$wz = 2b - a + (a - b)\pi.$$

We have $0 < |a-b| < a$. If $b < a \le 2b$, then also

$$0 \le 2b - a = b - (a-b) < \max(b, a-b) < a.$$

If $2b < a$, then $0 \le a - 2b < a$. By induction there is a unit u such that

$$\lambda(uwz) \le \log_2 |N(wz)| + 1 = \log_2 |N(z)| + 1.$$

This proves the lemma. □

Again, in order to analyze sequences of period n, we need to know the norm of $\pi^n - 1$.

Lemma 7: Let $n > 0$ and let $e = \gcd(n, d)$. Then

$$N(\pi^n - 1) = (p^{n/e} - 1)^e.$$

Moreover

$$\log_p |N(\pi^n - 1)| \in n + o(1).$$

Proof: For any $k > 0$, if γ is a complex primitive kth root of one, then

$$\prod_{i=0}^{k-1} (x - \gamma^i) = x^k - 1.$$

Let ζ be a complex primitive dth root of one. Then ζ^n is a primitive (d/e)th root of one. We have

$$\begin{aligned} N(\pi^n - 1) &= \prod_{i=0}^{d-1} (\zeta^{ni}\pi^n - 1) \\ &= p^n (-1)^d \prod_{i=0}^{d-1} (\pi^{-n} - \zeta^{ni}) \\ &= p^n (-1)^d \left(\prod_{i=0}^{d/e-1} (\pi^{-n} - \zeta^{ni}) \right)^e \\ &= p^n (-1)^d (\pi^{-nd/e} - 1)^e \\ &= p^n (-1)^d (p^{-n/e} - 1)^e \\ &= (-1)^{d+e} (p^{n/e} - 1)^e. \end{aligned}$$

This proves the first statement. The second statement follows by taking log base p of the absolute value of the penultimate line. □

C. Expectation in Terms of the Norm

Now we suppose we are in either of the cases considered in Sections IV-A and IV-B. Let

$$e = \begin{cases} d \log_p(d) & \text{if } \pi^d = p > 0 \\ 0 & \text{if } \pi^2 = -p < 0. \end{cases}$$

Then in both cases for every $q \in R$ we have

$$\lambda(q) \ge \log_p |N(q)| - e.$$

If $\mathbf{a}$ is a periodic sequence over S with period n, let $\hat{q}_{\mathbf{a}}$ be a connection element of an AFSR that outputs $\mathbf{a}$ so that $|N(\hat{q}_{\mathbf{a}})|$ is minimal. For any $q \in R$, let $\Delta_n(q)$ denote the number of period n sequences with q as a connection element, and let $\Delta_n^*(q)$ denote the number of period n sequences $\mathbf{a}$ such that q is an associate of $\hat{q}_{\mathbf{a}}$.

Then by equation (3) we have

$$\begin{aligned} E_n^\lambda &\ge \left(\frac{1}{p^n} \sum_{\mathbf{a}} \lambda(q_{\mathbf{a}}) \right) - c \\ &\ge \frac{1}{p^n} \sum_{\mathbf{a}} (\log_p |N(q_{\mathbf{a}})| - e) - c \\ &= \frac{1}{p^n} \sum_{\mathbf{a}} \log_p |N(q_{\mathbf{a}})| - e - c \\ &\ge \frac{1}{p^n} \sum_{\mathbf{a}} \log_p |N(\hat{q}_{\mathbf{a}})| - e - c. \qquad (8) \end{aligned}$$

Recall that R is a unique factorization domain (UFD) if every element $q \in R$ can be written as a product

$$z = u \prod z_i^{e_i},$$

where u is a unit, the z_i are irreducible, each e_i is positive, and z_i and z_j are not associates if $i \neq j$. This representation of q is unique up to permutation of the z_i and up to replacing a z_i by an associate and changing the unit u. If R is a UFD then every sequence has an R-minimal connection element. Any two R-minimal connection elements for a given sequence are associates. Also, in a UFD, if a is irreducible and divides uv then a divides u or a divides b.

Suppose that R is a UFD. If $\mathbf{a}$ is a sequence with period n, then it is the sequence of coefficients in the π-adic expansion of some

$$\frac{u}{\pi^n - 1} = \frac{v}{\hat{q}_{\mathbf{a}}}.$$

Thus

$$u\hat{q}_{\mathbf{a}} = v(\pi^n - 1).$$

If v and $\hat{q}_{\mathbf{a}}$ had a common divisor z and z were not a unit, then $\hat{q}_{\mathbf{a}}/z$ would be the connection element of an AFSR that outputs $\mathbf{a}$, and its norm would be smaller than that of $\hat{q}_{\mathbf{a}}$. Thus v and $\hat{q}_{\mathbf{a}}$ are relatively prime. By the fact that R is a UFD, $\hat{q}_{\mathbf{a}}$ divides $\pi^n - 1$. Thus equation (8) implies

$$E_n^\lambda \ge \frac{1}{p^n} \sum_{q |^* \pi^n - 1} \log_p |N(q)| \Delta_n^*(q) - e - c, \qquad (9)$$

where the notation $q|^*\pi^n - 1$ means we take one associate from each set of associate divisors of $\pi^n - 1$.

V. Δ_n^* in Certain UFDs

Throughout this section p is a positive integer. We analyze $\Delta_n^*(z)$ when $R = \mathbb{Z}[\pi]$ with

$$\pi^2 = -p < 0 \text{ or } \pi^d = p > 0.$$

In the former case we always assume that $x^2 + p$ is irreducible over $\mathbb{Z}$ and in the latter case we always assume that $x^d - p$ is irreducible over $\mathbb{Z}$. In the former case we also let $d = 2$.

To proceed we need a better understanding of when the coefficient sequence of the π-adic expansion of a rational u/z

is periodic, and when it has a given period. First, we do this for $R = \mathbb{Z}$.

Lemma 8: Let p and q be integers greater than 1 with $\gcd(p, q) = 1$.

1) A rational element u/q, with $u, q \in \mathbb{Z}$, $q > 0$, and $\gcd(q, p) = 1$, has a strictly periodic p-adic expansion if and only if $-q \leq u \leq 0$. If q divides $p^n - 1$, then in any case the eventual period of the p-adic expansion divides n.
2) A rational element u/q, with $u, q \in \mathbb{Z}$, $q > 0$, and $\gcd(q, p) = 1$, has a strictly periodic $(-p)$-adic expansion if and only if
$$-q/(p+1) \leq u \leq pq/(p+1). \tag{10}$$
If q divides $p^n - 1$ and
$$\frac{u}{q} \notin \left\{ -\frac{1}{p+1}, \frac{p}{p+1} \right\},$$
then in any case the eventual period of the p-adic expansion divides n.

Proof: The first claim is well known [7]. Suppose that u/q has a periodic $(-p)$-adic expansion. We may assume the period, n, is even. Then
$$\frac{u}{q} = \frac{v}{1 - p^n}$$
with
$$v = \sum_{i=0}^{n-1} v_i (-p)^i$$
and $0 \leq v_i < p$. It follows that
$$\begin{aligned} &-(p-1)p - (p-1)p^3 + \cdots - (p-1)p^{n-1} \\ &\quad \leq v \leq (p-1) + (p-1)p^2 + \cdots + (p-1)p^{n-2}. \end{aligned}$$
That is,
$$-\frac{p(p^n - 1)}{p+1} \leq v \leq \frac{p^n - 1}{p+1}. \tag{11}$$
We have $u = vq/(1 - p^n)$ and $q/(1 - p^n) < 0$ so equation (10) holds.

Conversely, we want to see that if equation (10) holds, then the $(-p)$-adic expansion of u/q is periodic. Since p and q are relatively prime, there is an integer n so that
$$q | (-p)^n - 1.$$
First suppose that n is even. Let $p^n - 1 = qz$, so $z > 0$. Multiplying equation (10) by z gives equation (11). The number of v satisfying equation (11) is exactly p^n, the number of sequences with period n, so the $(-p)$-adic expansion of every u/q with u satisfying equation (10) is periodic. This also proves the last statement for periodic expansions with even period.

When n is odd, the equation analogous to equation (11) is
$$-\frac{p^n + 1}{p+1} \leq v \leq \frac{p(p^n + 1}{p+1}.$$
There are $p^n + 2$ solutions v to this equation, so there are two $(v/((-p)^n - 1)$s with periodic expansion whose period divides $2n$ but not n. It is straightforward to check that the $(-p)$-adic expansions of
$$\frac{-1}{p+1} = \frac{1 - p + p^2 - + \cdots - p^{n-1}}{(-p)^n - 1}$$
and
$$\frac{p}{p+1} = \frac{-p + p^3 - + \cdots + p^n}{(-p)^n - 1}$$
are $(p - 1, 0, p - 1, 0, \cdots)$ and $(0, p - 1, 0, p - 1, \cdots)$, respectively. Both sequences have period 2, which divides $2n$ but not n.

If the expansion of u/q is only eventually periodic, it nonetheless has the same periodic part as some v/q with a periodic expansion. This element's expansion has period n. □

Now we consider the periodic π-adic sequences. We use the fact that these are either interleavings of d p-adic or $(-p)$-adic sequences.

Lemma 9: Let $\pi^d = p > 0$, let $n \geq 1$ be an integer, and let
$$\begin{aligned} U \quad = \quad &\{u : u/(1 - \pi^n) \text{ has a strictly periodic} \\ &\pi\text{-adic expansion with period } n\}. \end{aligned}$$
Then U contains a complete set of representatives for R modulo $\pi^n - 1$.

Proof: First note that $u \in U$ if and only if u can be written
$$u = \sum_{i=0}^{n-1} u_i \pi^i,$$
where $0 \leq u_i < p$ for $0 \leq i < n$. Let $v \neq u$ be another element of U with
$$v = \sum_{i=0}^{n-1} v_i \pi^i,$$
where $0 \leq v_i < p$ for $0 \leq i < n$. We want to determine when $u \equiv v \mod \pi^n - 1$.

Let $e = \gcd(n, d)$ and
$$\delta = 1 + \pi^n + \cdots + \pi^{n(d/e - 1)}.$$
Then
$$(\pi^n - 1)\delta = \pi^{nd/e} - 1 = p^{n/e} - 1 \in \mathbb{Z}.$$
Let
$$u\delta = \sum_{j=0}^{d-1} a_j \pi^j \quad \text{and} \quad v\delta = \sum_{j=0}^{d-1} b_j \pi^j,$$
where $a_j, b_j \in \mathbb{Z}$, $0 \leq j < d$. Since the coefficient sequence of the π-adic expansion of
$$\frac{u}{1 - \pi^n} = \frac{u\delta}{1 - p^{n/e}}$$
is the interleaving of the coefficient sequences of the p-adic expansions of the
$$\frac{a_j}{1 - p^{n/e}}$$

and the former sequence is periodic, the latter sequences are periodic as well. Thus

$$0 \leq a_j \leq p^{n/e} - 1.$$

Similarly,

$$0 \leq b_j \leq p^{n/e} - 1.$$

Moreover

$$u \equiv v \mod \pi^n - 1$$

if and only if $p^{n/e} - 1$ divides $u\delta - v\delta$. This holds if and only if

$$(p^{n/e} - 1) | (a_j - b_j)$$

for every $0 \leq j < d$. The only possibility is that for every j, $a_j = b_j$ or

$$\{a_j, b_j\} = \{0, p^{n/e} - 1\}.$$

Let V be the set of $u \in U$ such that, if

$$u\delta = \sum_{j=0}^{d-1} a_j \pi^j$$

with $a_i \in \mathbb{Z}$, then every $a_j \neq 0$. Then by the preceding paragraph, no two elements in V are congruent modulo $\pi^n - 1$. Since by Lemma 7 we have

$$|R/(\pi^n - 1)| = (p^{n/e} - 1)^e,$$

we will have proved the lemma if we prove that

$$|V| = (p^{n/e} - 1)^e$$

as well.

Let

$$u = \sum_{i=0}^{n-1} u_i \pi^i \text{ with } 0 \leq u_i < p,$$

and

$$u\delta = \sum_{j=0}^{d-1} a_j \pi^j \text{ with } a_j \in \mathbb{Z}.$$

Then

$$a_j = \sum u_i p^{(i+nk-j)/d},$$

where the sum is over all $0 \leq i < n$ and $0 \leq k < d/e$ with $i + nk \equiv j \mod d$. For any $0 \leq j < d$, let W_j be the set of $0 \leq i < n$ such that there exists a (necessarily unique) $0 \leq k < d/e$ so that $i + nk \equiv j \mod d$. Since all u_i are nonnegative, $a_j = 0$ if and only if $u_i = 0$ for every $i \in W_j$. Moreover, if $0 \leq \ell < d$, then $W_\ell = W_j$ if and only if $\ell \equiv j - nt \mod d$ for some t. Equivalently, if and only if $\ell \equiv j \mod e$ for some t. Otherwise W_j and W_ℓ are disjoint.

This gives us a partition of $\{0, 1, \cdots, n-1\}$ into e subsets $W_0, \cdots, W_{e-1}$. An element u is in V if and only if, for each $0 \leq j < e$, at least one $i \in W_j$ is nonzero. Each W_j has n/e elements. Thus for each such j there are $p^{n/e} - 1$ allowable values for the set of u_i with $i \in W_j$. This gives

$$(p^{n/e} - 1)^e$$

allowable values of $u_0, \cdots, u_{n-1}$ with $u \in V$, and completes the proof of the lemma. □

Lemma 10: Let $\pi^d = p$ with $p > 0$ and $x^d - p$ irreducible. If $z \in R$ divides $\pi^n - 1$ and is not a unit, then

$$\Delta_n(z) \geq |(R/(z))|.$$

If also R is a UFD, then

$$\Delta_n^*(z) \geq |(R/(z))^*|.$$

Proof: The first inequality follows from Lemma 9 since every complete set of representatives modulo $\pi^n - 1$ contains a complete set of representatives modulo z.

Now suppose R is a UFD. Suppose that $\mathbf{a} = a_0, a_1, \cdots$ is a periodic sequence with period n. Then

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

is rational and by our choice of T, the denominator in any rational representation is the connection element of an AFSR. Thus $a = u_{\mathbf{a}}/\hat{q}_{\mathbf{a}}$ for some $u_{\mathbf{a}}$. We have $\gcd(u_{\mathbf{a}}, \hat{q}_{\mathbf{a}}) = 1$ since otherwise $\hat{q}_{\mathbf{a}}/\gcd(u_{\mathbf{a}}, \hat{q}_{\mathbf{a}})$ would be a connection element of $\mathbf{a}$ with a smaller norm than that of $\hat{q}_{\mathbf{a}}$.

Let $V \subseteq \Delta_n(z)$ be a complete set of representatives for R modulo z. Let $v \in V$ be a unit modulo z. Let $\mathbf{a}$ be the coefficient sequence of the π-adic expansion of v/z. Then $v/z = u_{\mathbf{a}}/\hat{q}_{\mathbf{a}}$, so $v\hat{q}_{\mathbf{a}} = u_{\mathbf{a}} z$. But $\hat{q}_{\mathbf{a}}$ is relatively prime to $u_{\mathbf{a}}$, so $\hat{q}_{\mathbf{a}}$ divides z. Since v is a unit modulo z, z divides $\hat{q}_{\mathbf{a}}$, so z and $\hat{q}_{\mathbf{a}}$ are associates. Thus $v \in \Delta_n^*(z)$. This proves the second inequality. □

Lemma 11: Let $\pi^2 = -p$ with $p > 0$ and $x^2 + p$ irreducible. Let $4|n$. If z divides $\pi^n - 1 = p^{n/2} - 1$, then

$$\Delta_n(z) \geq |(R/(z))| \text{ and } \Delta_n^*(z) \geq |(R/(z))^*|.$$

Proof: Let $u \in R$. Then u/z has an eventually periodic π-adic expansion [8], so there is an element $a \in R$ so that

$$\frac{y}{z} = a + \frac{u}{z}$$

has a strictly periodic π-adic expansion. Then

$$u \equiv y \mod z,$$

so the set of y such that y/z has a strictly periodic π-adic expansion contains a complete set of representatives for $R/(z)$. Thus it suffices to show that if u/z is strictly periodic, then its period divides n. To show this it suffices to prove the lemma in the case when $z = \pi^n - 1$.

Since $4|n$,

$$\pi^n - 1 = (-p)^{n/2} - 1 \in \mathbb{Z}$$

is positive. Let $u = u_0 + u_1\pi$ with $u_0, u_1 \in \mathbb{Z}$. The π-adic expansion of

$$\frac{u}{p^{n/2} - 1}$$

is the interlacing of the p-adic expansions of

$$\frac{u_0}{p^{n/2} - 1} \text{ and } \frac{u_1}{p^{n/2} - 1}.$$

Thus by Lemma 8, $u/(p^{n/2}-1)$ is periodic if and only if

$$\frac{-(p^{n/2}-1)}{p+1} \leq u_i \leq \frac{p(p^{n/2}-1)}{p+1},$$

for $i=0,1$. If v is a second element of R such that the π-adic expansion of $v/(p^{n/2}-1)$ is periodic, and

$$v \equiv u \mod p^{n/2}-1,$$

then $u_i = v_i$ or

$$u_i, v_i \in \left\{\frac{-(p^{n/2}-1)}{p+1}, \frac{p(p^{n/2}-1)}{p+1}\right\}$$

for $i=0,1$. Thus the elements $u = u_0 + u_1\pi$ with

$$\frac{-(p^{n/2}-1)}{p+1} \leq u_i < \frac{p(p^{n/2}-1)}{p+1},$$

for $i=0,1$ are all distinct modulo $p^{n/2}-1$. There are

$$(p^{n/2}-1)^2$$

such elements, and this is also the cardinality of $R/(p^{n/2}-1)$. Thus the set of such u is a complete set of representatives for R modulo $p^{n/2}-1$. Thus for every $w \in (R/(z))^*$, there is such a u with

$$u \equiv w \mod p^{n/2}-1.$$

The lemma follows from this. □

Note that Lemma 11 is false if n is not a multiple of 4.

Having lower bounded $\Delta_n^*(z)$ by $|(R/(z))^*|$, we proceed to analyze $|(R/(z))^*|$ in terms of its irreducible factorization.

Lemma 12: Let $R = \mathbb{Z}[\pi]$, where $\pi^d = p$ or $\pi^2 = -p$, be a UFD If $z_1, \cdots, z_t \in R$ are not units and are pairwise relatively prime, then

$$\left|R/\left(\prod_{i=1}^{t} z_i\right)\right| = \prod_{i=1}^{t} |R/(z_i)|$$

and

$$\left|\left(R/(\prod_{i=1}^{t} z_i)\right)^*\right| = \prod_{i=1}^{t} |(R/(z_i))^*|.$$

Proof: By induction it suffices to prove the result when $t=2$. The ring $R/(z_1)$ is finite since $z_1 | N(z_1) \in \mathbb{Z}$. Thus the sequence

$$1, z_2, z_2^2, \cdots \in R/(z_1)$$

eventually repeats. That is, there are $\ell < k$ with

$$z_2^\ell \equiv z_2^k \mod z_1.$$

Hence

$$z_1 | (z_2^k - z_2^\ell) = z_2^\ell (z_2^{k-\ell} - 1).$$

Since z_1 and z_2 are relatively prime,

$$z_1 | z_2^{k-\ell} - 1.$$

Thus there are elements $a, b \in R$ with $az_1 + bz_2 = 1$.

Consider the function

$$\Psi : R/(z_1 z_2) \rightarrow (R/(z_1)) \times (R/(z_2))$$

defined by reduction modulo z_1 and z_2. If $x \in R/(z_1)$ and $y \in R/(z_2)$, then

$$\Psi(bz_2x + az_1y) = (x, y),$$

so Ψ is onto. Conversely, Ψ is one to one since $\psi(x) = (0,0)$ implies that both z_1 and z_2 divide x, hence z_1z_2 divides x. Thus Ψ is a ring isomorphism. This gives the first identity[4]. Ψ also induces an isomorphism of unit groups, which gives the second identity. □

Lemma 13: Let $R = \mathbb{Z}[\pi]$, where $\pi^d = p$ or $\pi^2 = -p$, be a UFD. If $z \in R$ is irreducible and $t \geq 1$, then

$$|R/(z^t)^*| = |R/(z)|^{t-1}(|R/(z)| - 1).$$

Proof: We prove this by induction on t. Suppose $t = 1$. Then for any nonzero $u \in R/(z)$, the map $v \mapsto vu$ is a one to one map from $R/(z)$ to itself. Since this quotient is finite, this map is also onto, so v is invertible. This proves the claim in this case.

Now suppose $t \geq 2$. Let

$$f : R/(z^t) \rightarrow R/(z^{t-1})$$

be the function given by reduction modulo z^{t-1}. Then f maps units to units. Moreover, if x is a unit in $R/(z^{t-1})$, then there are $y, u \in R$ with

$$xy = 1 + uz^{t-1}.$$

Then

$$xy(1 - uz^{t-1}) = 1 - u^2 z^{2(t-1)} \equiv 1 \mod z^t,$$

so x is a unit in $R/(z^t)$. Thus f induces a surjective multiplicative group homomorphism

$$f^* : (R/(z^t))^* \rightarrow (R/(z^{t-1}))^*.$$

The kernel of f^* is

$$1 + z^{t-1}(R/(z^t)).$$

which has cardinality $|R/(z)|$. The lemma follows from this. □

Corollary 3: Let $R = \mathbb{Z}[\pi]$, where $\pi^d = p$ or $\pi^2 = -p$, be a UFD. If $z \in R$ is irreducible and $t \geq 1$, then

$$\sum_{i=1}^{t} \Delta_n^*(z^i) \geq \sum_{i=1}^{t} |R/(z^i)^*| = |R/(z)|^t - 1 = |N(z)|^t - 1.$$

[4] We have shown that the Chinese Remainder Theorem holds in a UFD when all the quotient rings are finite.

VI. A Lower Bound on the Expected Span

Throughout this section we assume that $R = \mathbb{Z}[\pi]$ is a UFD, where $\pi^d = p$ (with $x^d - p$ irreducible) or $\pi^2 = -p$ (with $x^2 + p$ irreducible) with $p > 0$. Let $n \in \mathbb{Z}$ be arbitrary in the former case and let $4|n$ in the latter. We have seen that it is possible to obtain lower bounds on $\Delta_n^*(z)$ as long as R is a UFD. In this section we use these bounds to obtain lower bounds on the expected π-adic span of sequences with period n.

The question of when a ring $R = \mathbb{Z}[\pi]$ is a UFD is a delicate one, not fully understood. First, it is generally necessary to use the integral closure of R rather than R to obtain a UFD. For example, the full ring of integers of $R = \mathbb{Z}[\sqrt{5}]$ is $R' = \mathbb{Z}[(1+\sqrt{5})/2]$. In R we have the distinct factorizations

$$2 \cdot 2 = 4 = (1+\sqrt{5}) \cdot (-1+\sqrt{5}).$$

These factorizations are equivalent in R' because

$$1+\sqrt{5} = \frac{1+\sqrt{5}}{2} \cdot 2,$$

and $(1+\sqrt{5})/2$ is a unit in R'. Similarly for the other factor.

The $p > 0$ for which the integral closure of $\mathbb{Z}[\sqrt{-p}]$ is a UFD are known: they are

$$p \in \{163, 67, 43, 19, 11, 7, 3, 2, 1\}.$$

However the $p > 0$ for which the integral closure of $\mathbb{Z}[\sqrt{p}]$ is a UFD are only partly known: the known ones are

$$\begin{aligned} p \in \{&2,3,5,6,7,11,13,14,17,19,21,22,23,29,\\ &33,37,41,53,57,61,69,73,77,89,93,97\}. \end{aligned}$$

Since R is a UFD we can write

$$\pi^n - 1 = u \prod_{i=1}^{t} z_i^{e_i},$$

where u is a unit and each z_i is irreducible.

Theorem 4: If $R = \mathbb{Z}[\pi]$ is a UFD with $\pi^2 = -p < 0$ or $\pi^d = p > 0$, and n is a multiple of 4 in the former case and is arbitrary in the latter case, then

$$E_n^\lambda \in n - O(\log(n)).$$

Proof: Suppose that

$$\pi^n - 1 = \prod_{i=1}^{k} z_i^{t_i}$$

where $z_i \in R$ is irreducible, z_i and z_j not associates if $i \neq j$, $t_i \geq 1$, $i,j = 1,\cdots,k$. Let

$$\mathcal{J} = \{(j_1,\cdots,j_t) : 0 \leq j_i \leq t_i, i = 1,\cdots,k\} \subseteq \mathbb{Z}^k.$$

Then by equation (9)

$$\begin{aligned} E_n^\lambda &= \frac{1}{p^n} \sum_{J\in\mathcal{J}} \log_p \left| N\left(\prod_{i=1}^{k} z_i^{j_i}\right)\right| \Delta_n^*\left(\prod_{i=1}^{k} z_i^{j_i}\right) \\ &\quad -e-c. \end{aligned} \tag{12}$$

Let

$$\Delta_{0,n}^*(x) = \begin{cases} 1 & \text{if } x \text{ is a unit} \\ \Delta_n^*(x) & \text{otherwise.} \end{cases}$$

Thus by Corollary 3

$$\sum_{i=0}^{t} \Delta_{0,n}^*(z^t) \geq |N(z)|^t. \tag{13}$$

Then note that the right hand side of equation (12) is unchanged if we replace Δ_n^* by $\Delta_{0,n}^*$. Thus, using equation (13) to obtain the third line, we have

$$\begin{aligned} E_n^\lambda &\geq \frac{1}{p^n} \sum_{J\in\mathcal{J}} \sum_{i=1}^{k} j_i \log_p |N(z_i)| \prod_{i=1}^{k} \Delta_{0,n}^*(z_i^{j_i}) - e - c \\ &= \frac{1}{p^n} \sum_{\ell=1}^{k} \sum_{j_\ell=0}^{t_\ell} j_\ell \log_p |N(z_\ell)| \Delta_{0,n}^*(z_\ell^{j_\ell}) \\ &\quad \cdot \prod_{\substack{i=1\\ i\neq\ell}}^{k} \sum_{j_i=0}^{t_i} \Delta_{0,n}^*(z_i^{j_i}) - e - c \\ &\geq \frac{1}{p^n} \sum_{\ell=1}^{k} \sum_{j_\ell=0}^{t_\ell} j_\ell \log_p |N(z_\ell)| \Delta_{0,n}^*(z_\ell^{j_\ell}) \\ &\quad \cdot \prod_{\substack{i=1\\ i\neq\ell}}^{k} |N(z_i)|^{t_i} - e - c \\ &= \frac{1}{p^n} \sum_{\ell=1}^{k} \sum_{j_\ell=0}^{t_\ell} j_\ell \log_p |N(z_\ell)| \Delta_{0,n}^*(z_\ell^{j_\ell}) \frac{|N(\pi^n - 1)|}{|N(z_\ell)|^{t_\ell}} \\ &\quad -e-c \\ &\geq \frac{|N(\pi^n-1)|}{p^n} \sum_{\ell=1}^{k} \frac{\log_p |N(z_\ell)|}{|N(z_\ell)|^{t_\ell}} \\ &\quad \cdot \sum_{j_\ell=1}^{t_\ell} j_\ell (|N(z_\ell)|^{j_\ell} - |N(z_\ell)|^{j_\ell - 1}) - e - c \\ &= \frac{|N(\pi^n-1)|}{p^n} \sum_{\ell=1}^{k} \frac{\log_p |N(z_\ell)|}{|N(z_\ell)|^{t_\ell}} \\ &\quad \cdot \left(t_\ell |N(z_\ell)|^{t_\ell} - \sum_{j_\ell=0}^{t_\ell - 1} |N(z_\ell)|^{j_\ell} \right) - e - c \end{aligned}$$

$$\begin{aligned}
&= \frac{|N(\pi^n-1)}{p^n}\sum_{\ell=1}^{k}\frac{\log_p|N(z_\ell)|}{|N(z_\ell)|^{t_\ell}} \\
&\quad\cdot\left(t_\ell|N(z_\ell)|^{t_\ell}-\frac{|N(z_\ell)|^{t_\ell}-1}{|N(z_\ell)|-1}\right)-e-c \\
&= \frac{|N(\pi^n-1)}{p^n}\sum_{\ell=1}^{k}\log_p|N(z_\ell)| \\
&\quad\cdot\left(t_\ell-\frac{1-|N(z_\ell)|^{-t_\ell}}{|N(z_\ell)|-1}\right)-e-c \\
&= \frac{|N(\pi^n-1)}{p^n}\log_p|N(\pi^n-1)| \\
&\quad-\frac{|N(\pi^n-1)|}{p^n}\sum_{\ell=1}^{k}\log_p|N(z_\ell)|\left(\frac{1-|N(z_\ell)|^{-t_\ell}}{|N(z_\ell)|-1}\right) \\
&\quad-e-c \\
&\geq \frac{|N(\pi^n-1)|}{p^n}\log_p|N(\pi^n-1)| \\
&\quad-\frac{|N(\pi^n-1)|}{p^n}\sum_{\ell=1}^{k}\frac{\log_p|N(z_\ell)|}{|N(z_\ell)|-1}-e-c.
\end{aligned}$$

Now we want to bound the summation in the last line. For any $f \geq 2$ we have

$$\frac{\log_p(f)}{f-1} \leq \frac{2\log_p(f)}{f} \leq \frac{2\log_2(f)}{f},$$

and if $t \geq 1$ then $1 - f^{-t} < 1$. Thus it suffices to bound

$$A \overset{def}{=} \sum_{\ell=1}^{k}\frac{\log_2(|N(z_\ell)|)}{|N(z_\ell)|}$$

in terms of $N(\pi^n - 1)$. In bounding A, if we replace $\pi^n - 1$ by a divisor q of $\pi^n - 1$ with the same distinct prime factors, while leaving A unchanged, or replace A by a larger number while leaving q unchanged, this can only weaken our bound. That is, if

$$|N(q)| < |N(\pi^n-1)|, A < A', \text{ and } A' \in O(\log|N(q)|),$$

then

$$A \in O(\log|N(\pi^n-1)|).$$

So first we replace $\pi^n - 1$ by

$$q = \prod_{\ell=1}^{k} z_\ell.$$

That is, we assume that each $t_\ell = 1$. The function $\log_2(x)/x$ is decreasing for integers $x \geq 3$. Thus decreasing an $N(z_\ell)$ will increase A while decreasing $N(q)$. Thus we may assume that the set of z_ℓs consists of the k irreducible and pairwise relatively prime elements of R with the k smallest norms.

Let m be a positive integer and consider the irreducible elements with norms between 2^m and 2^{m-1}. By Landau's prime ideal theorem, Corollary 2, there are asymptotically

$$\frac{2^m}{\ln(2^m)} = \frac{2^m}{m\ln(2)}$$

such elements. Each contributes at most $m/2^m$ to A, so the total contribution to A is at most $1/\ln(2)$. It also follows from Landau's prime ideal theorem that the largest 2^m we must consider is asymptotically $k\ln(k)$. It follows that $A \in O(\log(k))$.

Now consider $|N(q)|$. The contribution to $|N(q)|$ from the irreducible elements with norms between 2^m and 2^{m+1} is asymptotically at least

$$(2^m)^{2^m/(m\ln(2))} = 2^{2^m/\ln(2)}.$$

The largest m we need is at most $\log(k\ln(k)) < 2\log(k)$. Thus

$$\begin{aligned}
|N(q)| &\in \Omega\left(\prod_{m=1}^{2\log(k)} 2^{2^m/\ln(2)}\right) \\
&= \Omega(2^{(\sum_{m=1}^{2\log(k)} 2^m/\ln(2))}) \\
&= \Omega(2^{(2^{2\log(k)+1}/\ln(2))}) \\
&= \Omega(2^{2k^2/\ln(2)}).
\end{aligned}$$

Therefore, by Lemmas 5 and 7,

$$\begin{aligned}
A &\in O(\log\log|N(q)|) \\
&\subseteq O(\log\log|N(\pi^n-1)|) \\
&\subseteq O(\log(n)).
\end{aligned}$$

This proves the theorem. □

VII. When $\mathbb{Z}[\pi]$ is Not the Full Ring of Integers

If $\mathbb{Z}[\pi]$ is not the full ring of integers, then it is not a UFD and the arguments we have used apparently do not work. However, we can instead consider AFSRs based on the full ring of integers R. In switching from $\mathbb{Z}[\pi]$ to R as the ring on which our AFSRs are based, we must see that $R/(\pi) = \mathbb{Z}[\pi]/(\pi)$; that there is a size function on R relative to π; and that the remainder of the derivation of the average span goes through essentially unchanged.

It is well known from algebraic number theory that if π is an integral element with $F = \mathbb{Q}(\pi)$ and $[\mathbb{Q} : F] = d$, then both $\mathbb{Z}[\pi]$ and the ring of integers R in F are free Abelian groups of rank d [2, p. 86]. Let $\omega_1, \cdots, \omega_d$ be a $\mathbb{Z}$-basis of R and let $\eta_1, \cdots, \nu_d$ be a $\mathbb{Z}$-basis of $\mathbb{Z}[\pi]$. Then there are integers $a_{i,j}$, $1 \leq i, j \leq d$, so that

$$\eta_i = \sum_{j=i}^{d} a_{ij}\omega_j.$$

It follows that the ideal πR in R is an Abelian group and has a basis $\pi\omega_1, \cdots, \pi\omega_d$ and that the ideal $\pi\mathbb{Z}[\pi]$ in $\mathbb{Z}[\pi]$ is an Abelian group and has a basis $\pi\omega_1, \cdots, \pi\omega_d$. These bases are related by equations

$$\pi\omega_i = \sum_{j=i}^{d} b_{ij}\omega_j$$

and

$$\pi\eta_i = \sum_{j=i}^{d} c_{ij}\eta_j = \sum_{j=i}^{d} c_{ij}\sum_{k=i}^{d} a_{jk}\omega_k,$$

where $b_{ij}, c_{ij} \in \mathbb{Z}$. We also have

$$\pi\eta_i = \sum_{j=i}^{d} a_{ij}\pi\omega_j = \sum_{j=i}^{d} a_{ij} \sum_{k=i}^{d} b_{jk}\omega_k.$$

If we form the matrices $A = [a_{ij}]$, $B = [b_{ij}]$, and $C = [c_{ij}]$, then this says that $AB = CA$. All three matrices have rank d, so $\det(B) = \det(C)$. We also know that $\det(B) = |R/\pi R|$ and $\det(C) = |\mathbb{Z}[\pi]/\pi\mathbb{Z}[\pi]|$, so these two quotients have the same cardinality. But $\mathbb{Z}[\pi]/\pi\mathbb{Z}[\pi]$ injects into $R/\pi R$, so the two quotients are equal and the complete set of representatives S for $\mathbb{Z}[\pi]$ modulo π is also a the complete set of representatives for R modulo π.

Also, by inverting the matrix A, we obtain an expression for the ω_i as linear combinations of the η_i with rational coefficients with denominator $r = \det(A) \in \mathbb{Z}$. Thus every $z \in R$ can be written in the form

$$z = \sum_{i=0}^{d-1} \frac{z_i}{r}\pi^i, \qquad (14)$$

where $z_i \in \mathbb{Z}$. (But possibly not every element of this form is in R.)

Now let us specialize to the rings we have been studying, namely $R = \mathbb{Z}[\pi]$ with $\pi^2 = -p < 0$ or $\pi^d = p > 0$. If $\pi^2 = -p < 0$, then we can define

$$\lambda(a) = \log_p(N(a))$$

as we did for $\mathbb{Z}[\pi]$. If $\pi^d = p > 0$, then we define

$$\lambda\left(\sum_{i=0}^{d-1} \frac{z_i}{r}\pi^i\right) = \max(d\log_p|z_i| + i : i = 0, \cdots, d-1).$$

It is straightforward to see that axioms S1–S5 hold in both cases. It then follows that all the results in Sections II, III, and IV hold.

However, Lemma 9 and the proof of Lemma 11 do not hold in general. The problem is that elements of the form

$$\frac{u}{z} = \frac{\sum_{i=0}^{d-1} \frac{u_i}{r}\pi^i}{z} = \frac{\sum_{i=0}^{d-1} u_i\pi^i}{rz},$$

with $u_i \in \mathbb{Z}$ may have strictly periodic π-adic expansions that do not have period n. (This happens if z divides $\pi^n - 1$, but rz does not.) Thus we cannot show by exactly this method that

$$\Delta_n(z) \geq |R/(z)| \text{ and } \Delta_n^*(z) \geq |(R/(z))^*|.$$

However, in some cases there are enough elements

$$\frac{\sum_{i=0}^{d-1} u_i\pi^i}{z}$$

with periodic π-adic expansions (which must have period n) that the lower bounds still hold. This happens for the first lower bound in the imaginary quadratic case, $\pi^2 = -p < 0$. Here $r = 2$. There are enough "extra" n-periodic (u/z)s with $u \in \mathbb{Z}[\pi]$ to compensate for the ones whose periods are too large. But this argument does not work for proving the lower bound on $\Delta_n^*(z)$.

However, if we also have $p \equiv 7 \equiv -1 \mod 8$, then

$$\begin{aligned} N(u) &= N\left(\frac{u_0 + u_1\pi}{2}\right) \\ &= \frac{u_0^2 + pu_1^2}{4} \\ &\equiv \frac{u_0^2 - u_1^2}{4} \\ &\equiv 0 \mod 2. \end{aligned}$$

Thus if z is a multiple of 2, then u is not invertible modulo z, so there are no (u/v)s with u invertible modulo z whose π-adic expansions are periodic with period not dividing n. Hence every invertible element v modulo z is congruent to an invertible u so the expansion of u/z is periodic with period n. This gives the desired lower bound. In this case the lower bound in Theorem 4 holds in the integral closure R of $\mathbb{Z}[\pi]$.

In fact the lower bound may be false. If so, it would have serious implications for cryptography. Let $R, \pi \in R, S \subseteq R$ be the setup for a class of AFSRs. Suppose that the average π-adic span of sequences is substantially smaller than n (in some sense of "substantially"). Suppose we also have a register synthesis algorithm for this class of AFSRs with similar time complexity and threshold for success (that is, length of a prefix the algorithm needs in order to output the correct AFSR, usually measured in terms of λ) to those of the Berlekamp-Massey algorithm. Then cryptanalysis using this class of AFSRs is more likely to be effective against random n-periodic sequences, than the Berlekamp-Massey algorithm, and π-adic span is a more important security measure than linear span.

VIII. Conclusions

For a variety of algebraic settings for the construction of algebraic feedback shift registers we have shown that the average π-adic span of n-periodic sequences is asymptotically n. This coincides with what is already known about linear span and p-adic span (p an integer).

There remain many cases we have not yet been able to analyze, including even the case when $\pi^d = \pm p$ and R is not a UFD.

IX. Acknowledgement

Thanks to Hugh Williams for suggesting the proof of part 3 of Lemma 6. Thanks to the referees for making several suggestions that greatly improved the presentation.

References

[1] F. Arnault, B. Berger and A. Necer, "Feedback with carry shift register synthesis with the Euclidean algorithm," *IEEE Trans. Information Theory,* vol. 50, iss. 5, 2004, pp. 910-917

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

[3] W. A. Coppel, "Number Theory, An Introduction to Mathematics, Part B." New York, N.Y.: Springer, 2006.

[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, "Fibonacci and Galois Mode Implementation of Feedback with Carry Shift Registers," *IEEE Trans. Information Theory,* vol. 48, 2002, pp. 2826-2836.

[6] M. Goresky and A. Klapper, "Periodicity and Correlations of d-FCSR Sequences," *Designs, Codes, and Cryptography,* vol. 3, 2004, pp. 123-148.

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

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

[9] A. Klapper, "Distributional properties of d-FCSR sequences," *J. Complexity,* vol. 20, 2004, pp. 305-317.

[10] A. Klapper, "Expected π-Adic Complexity of Sequences," in S. Golomb, M. Parker, A. Pott, and A. Winterhof, eds., *Sequences and Their Applications - SETA 2008, Lecture Notes in Computer Science,* vol. 5203, 2008, pp. 219-229.

[11] R. Lidl and H. Niederreiter, "Finite Fields, 2nd ed." Cambridge, UK: Cambridge University Press, 1997.

[12] J.L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Information Theory,* vol. IT–15, 1969, pp. 122-127.

[13] W. Meidl and H. Niederreiter, "Counting functions and expected values for the k-error linear complexity," *Finite Fields and their Applications,* vol. 8, 2002, pp. 142-154.

[14] W. Meidl and H. Niederreiter, "On the expected value of linear complexity and the k-error linear complexity of periodic sequences," *IEEE Trans. Information Theory,* vol. 48, 2002, pp. 2817-2825.

[15] W. Meidl and H. Niederreiter, "The expected value of joint linear complexity of multisequences," *J. Complexity,* vol. 19, 2003, pp. 61-72.

[16] H. Niederreiter, "A combinatorial approach to probabilistic results on the linear complexity profile of random sequences," *J. Cryptology,* vol. 2, 1990, pp. 105-112.

[17] J. Xu and A. Klapper, "Register synthesis for algebraic feedback shift registers based on non-primes," *Designs, Codes, and Cryptography,* vol. 31, 2004, pp. 227-25.

X. Biography

Andrew M. Klapper was born in White Plains, New York, in 1952. He received the A.B. degree in mathematics from New York University, New York, NY, in 1974, the M.S. degree in applied mathematics from SUNY at Binghamton, Binghamton, NY, in 1975, the M.S. degree in mathematics from Stanford University, Stanford, CA, in 1976, and the Ph.D. degree in mathematics from Brown University, Providence, RI, in 1982. His thesis, in the area of arithmetic geometry, concerned the existence of canonical subgroups in formal grouplaws.

He has been a Postdoc at Clark University, an Assistant Professor in at Northeastern University, iand an Assistant Professor at the University of Manitoba. Currently he is a Professor in the Department of Computer Science at the University of Kentucky. He was awarded a University Research Professorship for 2002-03. His past research has included work on algebraic geometry over p-adic integer rings, computational geometry, modeling distributed systems, structural complexity theory, and cryptography. His current interests include statistical properties of pseudo-random sequences with applications in cryptography and CDMA; covering properties of codes; and morris dancing.

Dr. Klapper is a Senior Member of the IEEE Information Theory Society. He was the general chair of the Crypto 1998 conference. He was the Associate Editor for Sequences for the IEEE Transactions on Information Theory from 1999 to 2002. He was the organizer of SETA 2008 in Lexington, KY. He is an associate editor for Advances in Mathematics of Communications and for Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences.