A New Class of Pseudonoise Sequences

Mark Goresky[1]
School of Mathematics
Institute for Advanced Study

Andrew Klapper[2]
Department of Computer Science
University of Kentucky

Abstract — **We apply the framework of π-adic algebra and algebraic feedback shift registers to polynomial rings over finite fields. We give a construction of new pseudorandom sequences over a non-prime finite field that satisfy Golomb's randomness criteria.**

Pseudonoise sequences or m-sequences are important in areas including radar, error correction, CDMA, cryptography, and Monte Carlo simulation. Golomb [2] showed that these sequences have several critical randomness properties: the distribution of subsequences is nearly uniform, the distribution of lengths of runs of ones and zeros fits the expectation, and they have ideal autocorrelations.

Recently the authors have studied sequences, called ℓ-sequences, that are analogous to m-sequences and share many of their desirable properties [6, 7, 8, 9]. While m-sequences are analyzed in terms of coefficient sequences of rational functions, ℓ-sequences are analyzed in terms of coefficient sequences of p-adic numbers. While m-sequences are defined in a function field setting, ℓ-sequences are defined in a number field setting. These ℓ-sequences have excellent randomness properties that are nearly as good as those of m-sequences.

The authors have also developed an algebraic setting for analyzing sequences that subsumes the analysis of both m-sequences (by power series) and ℓ-sequences (by p-adic numbers) [9]. In this paper we use these techniques to define and analyze a new class of pseudonoise sequences based on the algebra of power series. These include m-sequences as a special case, but when the entries are not in a prime field $\mathbf{F}_p$, (p prime) the new sequences are distinct from m-sequences. These sequences have many of the same statistical properties as m-sequences: the distribution of fixed size subsequences is nearly uniform, the distribution of lengths of runs matches the expectation and, with an appropriate definition, they have ideal autocorrelations. G. Gong, A. Di Porto, and W. Wolfowicz previously constructed sequences with these randomness properties over a non-prime field F_{p^d} by applying an F_p-linear transformation to each element of an m-sequence over F_{p^d} [3]. However, at least in some cases (and we suspect in all cases) our new sequences are distinct from these.

I. Basics

A *linearly recurrent sequence* or *linear feedback shift register (LFSR) sequence* of span k over a finite field F can be defined in three ways. It is the unique solution to a linear recurrence $a_j = q_1a_{j-1} + q_2a_{j-2} + \cdots + q_ka_{j-k}$, $j \ge k$, with $a_j \in F$ and $q_1, \cdots, q_k, a_0, \cdots, a_{k-1} \in F$ given. It is the output from a LFSR with length k and entries (the a_j) and multipliers (the q_j) in F. Associated with the recurrence or LFSR is the polynomial $q(x) = \sum_{i=1}^{k} q_ix^i - 1$, known as the *connection polynomial.* The sequence is also the sequence of coefficients in the power series representation of a certain rational function $p(x)/q(x)$ with denominator $q(x)$. Moreover, if $q(x)$ is irreducible over F, then $a_j = Tr_{E/F}(a\delta^j)$ where E is the splitting field of q, $Tr_{E/F}$ is the trace function from E to F, δ is a root of q in E, and $a \in E$.

A linearly recurrent sequence is eventually periodic and its period is at most $|F|^k - 1$. A linearly recurrent sequence of span k whose period is $|F|^k - 1$ is called a *maximal length sequence* or *m-sequence.* It is well known that this maximal period is achieved precisely when the connection polynomial $q(x)$ is a primitive polynomial (that is, any root of $q(x)$ is a generator for the multiplicative group of the Galois field with $|F|^k$ elements).

An analogous class of sequences based on addition with carry was invented by the authors of this paper and independently by Couture and L'Ecuyer [1, 6]. With entries in the set $\mathbf{Z}/(M) = \{0, 1, \cdots, M-1\}$ for some integer M, a *multiply with carry sequence* or *feedback with carry shift register (FCSR) sequence* can also be defined in three ways. It is the unique solution to a with-carry linear recurrence $a_j = q_1a_{j-1} + q_2a_{j-2} + \cdots + q_ka_{j-k} + c$, $j \ge k$, with $a_j \in \mathbf{Z}/(M)$ and $q_1, \cdots, q_k, a_0, \cdots, a_{k-1} \in \mathbf{Z}/(M)$ given. The products and sum are to be computed in $\mathbf{Z}$. The value of a_j is the remainder modulo M, but the "carry" – the integer part of the quotient by M – is saved back into c for the next iteration. More precisely, given $q_1, \cdots, q_k, a_0, \cdots, a_{k-1} \in \mathbf{Z}/(M)$ and given $c_{k-1} \in \mathbf{Z}$ we define $a_j \in \mathbf{Z}/(M)$ and $c_j \in \mathbf{Z}$ recursively by the equation $a_j + Mc_j = q_1a_{j-1} + q_2a_{j-2} + \cdots + q_ka_{j-k} + c_{j-1}$, for $j \ge k$.

The sequence A is also the output from very fast generator known as an FCSR that is like an LFSR, but with additional memory for a carry. Associated with the recurrence or FCSR is an integer $q = \sum_{i=1}^{k} q_iM^i - 1$, known as the *connection integer.*

The sequence is also the sequence of coefficients in the M-adic expansion of a certain rational number

$$\frac{u}{q} = \sum_{i=0}^{\infty} a_iM^i$$

with denominator q. Moreover, the sequence is strictly periodic if and only if $-q \le u \le 0$. If $-q < u \le 0$, then we

[1]Research partially supported by NSF grant #0002693.
[2]Research partially supported by NSF grant #9980429.

have $a_j = (a\delta^j \pmod q) \pmod M$ where δ is the inverse of M modulo q and a is an integer. This notation means first find the element in $\{0, 1, \cdots, q-1\}$ that is congruent to $a\delta^j$ modulo q, then reduce this integer modulo M.

An FCSR sequence is eventually periodic and its period is a divisor of the order of M modulo q (and hence a divisor of $\phi(q)$). In particular, the extra memory m remains bounded in absolute value, so the FCSR is indeed a finite state device. An FCSR sequence with period $\phi(q)$ is an *ℓ-sequence.* For there to be an ℓ-sequence based on a given connection integer q it is necessary and sufficient that q be a power of a prime and that M be primitive modulo q.

LFSR sequences and FCSR sequences are special cases of *algebraic feedback shift register (AFSR) sequences* [9]. A class of AFSR sequences is based on a 4-tuple (R, f, S, T), where R is an integral domain (that is, a ring with no zero divisors), $f \in R$, and S, T are subsets of R each of which is a complete set of representatives for $R/(f)$. An AFSR in this class is then determined by a choice of elements $q_0, q_1, \cdots, q_k \in T$ such that q_0 is invertible modulo f. The AFSR is a (not necessarily finite) state device whose states are tuples $(a_0, a_1, \cdots, a_{k-1}; m)$ with each $a_i \in S$ and $m \in R$. It changes states as follows. There are unique elements $a_k \in S$ and $m' \in R$ such that

$$q_0 a_k + f m' = m + \sum_{i=1}^{k} q_i a_{k-i}.$$

Then the new state is $(a_1, a_2, \cdots, a_k; m')$.

An LFSR is an AFSR with $R = F[x]$ for some field F, $f = x$, $S = T = F$, and $q_0 = 1$. An FCSR is an AFSR with $R = \mathbf{Z}$, $f = M \in \mathbf{Z}$, $S = T = \{0, 1, \cdots, M-1\}$, and $q_0 = 1$. We have studied AFSRs based on rings R that are finite extensions of the integers [4, 10]. For R of the form $\mathbf{Z}[M^{1/d}]$, we characterized the periodic AFSR sequences [4]. We showed that the maximal length sequences based on such a ring have ideal *arithmetic (or with-carry) correlations* [4] and that they have highly uniform distributions of fixed size subsequences.

An AFSR sequence is also the solution to a with-carry linear recurrence over R. Associated with the recurrence or AFSR is an element $q = \sum_{i=1}^{k} q_i f^i - q_0 \in R$, known as the *connection element.* There is again a relationship with power series-like objects. The set of formal sums

$$R_f = \{\sum_{i=0}^{\infty} a_i f^i : a_i \in S, i = 0, 1, \cdots\}$$

is a ring whose elements are called *f-adic.* There is a ring homomorphism from R to R_f that is one-to-one if $\cap_{i=1}^{\infty}(f^i) = (0)$ (no nonzero element of R is divisible by every power of f). This homomorphism extends to the set of fractions u/q with $u, q \in R$ and q invertible modulo f. We refer to the representation of an element u/q in R_f as its *f-adic expansion.* An AFSR sequence with connection element q is the sequence of coefficients in the f-adic expansion of such a fraction u/q.

The question of periodicity is, in general, more complicated for AFSRs than for FCSRs and LFSRs. Indeed, there are some R and f for which the output is aperiodic and the memory does not remain bounded

In this paper we study AFSR sequences based on the ring $R = F[x]$ for a finite field F, but with $f \in R$ a polynomial of degree greater than 1.

II. The New Sequences

Let p be a prime integer, s be a positive integer, $R = \mathbf{F}_{p^s}[x]$, $e \geq 2$ be an integer, $n = se$, and $f(x) \in R$ have degree e. Let S be the set of polynomials of degree less than e with coefficients in $\mathbf{F}_{p^s}$. Then S is a complete set of representatives for $\mathbf{F}_{p^s}[x]$ modulo f, and so can be identified with $R/(f)$. From here on we study AFSR sequences based on (R, f, S, S). The set S is closed under addition, but not under multiplication.

Let d be a positive integer and let $q(x) \in R$ have degree d and be relatively prime to f, so that each is invertible modulo the other. Then $q(x) = \sum_{i=1}^{k} q_i f^i - q_0$ for some k, with $q_i \in S$, $i = 0, 1, \cdots, k$, and q_0 invertible modulo f. The output A from an AFSR based on (R, f, S, S) and with coefficients $q_0, q_1, \cdots, q_k$ is the coefficient sequence of the f-adic expansion of a rational function u/q, with $u \in R$. Conversely, every rational function with denominator q can be written as an f-adic number

$$\frac{u}{q} = \sum_{i=0}^{\infty} a_i f^i, \tag{1}$$

with each $a_i(x)$ an element of S. We show below that under suitable conditions the sequence $A = (a_0, a_1, \cdots)$ has excellent statistical properties.

Proposition 1 *The coefficient sequence $A = (a_0, a_1, \cdots)$ of the f-adic expansion of u/q is strictly periodic if and only if the degree of u is less than the degree of q.*

Proof: Suppose first that A is strictly periodic, say with period N. Then

$$\frac{u}{q} = (\sum_{i=0}^{N-1} a_i f^i) \sum_{i=1}^{\infty} f^{Ni} = \frac{\sum_{i=0}^{N-1} a_i f^i}{1 - f^N}.$$

The degree of the numerator in this last expression is strictly less than Ne, the degree of the denominator. Thus the degree of u is less than the degree of q.

Conversely, suppose that $\deg(u) < \deg(q)$. We have assumed that q and f are relatively prime, so that f is in the multiplicative group of the ring $R/(q)$. This is a finite group, so f has finite order modulo q. That is, there is an integer N so that $f^N \equiv 1 \pmod q$. Equivalently, q divides $1 - f^N$, say $1 - f^N = hq$. It follows that $u/q = (hu)/(1 - f^N)$, and $\deg(hu) < Ne$. Thus we can write $hu = \sum_{i=0}^{N-1} b_i f^i$ with $b_i \in S$. It follows that $a_j = b_{j \bmod N}$ for all j, so A is strictly periodic. $\square$

It follows from Theorem 1 and Theorem 10 of [9] that if the sequence is periodic, then

$$a_i = v(hf^{-i} \pmod{q}) \pmod{f} \tag{2}$$

with $h \in R, v \in S$. By the reduction of polynomial b mod polynomial c we mean the unique polynomial b' of degree less than the degree of c such that c divides $b - b'$.

Corollary 2 *The sequence A is eventually periodic. The period of A is the multiplicative order of f modulo q.*

Proof: We have $u/q = b + v/q$ with $\deg(v) < \deg(q)$. Thus v/q has a strictly periodic f-adic expansion by Proposition 1. The addition of b affects finitely many terms since S is closed under addition. Thus A is eventually periodic and its period equals that of v/q.

Now we may assume that A is strictly periodic, given by equation (2). Let T be the set of numerators of the rational representations of the shifts of A. The degrees of the elements of T are less than $\deg(q)$. The second statement then follows from Corollary 11 of [9]. □

We want sequences with large period relative to their generators. By Corollary 2, the period is largest if f has maximal multiplicative order modulo q. If q is irreducible then $R/(q)$ is a field, and its multiplicative group has order $p^{sd} - 1$. If f is primitive in this field (not the same as being a primitive polynomial over $\mathbf{F}_{p^s}$), then A has period $p^{sd} - 1$. In the terminology of [9], this says that A is an ℓ-sequence. To produce modified deBruijn sequences over $\mathbf{F}_{p^n}$ (defined in the next section), we also want the period to be of the form $p^{nk} - 1$ for some k. That is, we want $sd = nk = sek$, so we must have $d = ek$. Thus $\deg(q)$ must be a multiple of $\deg(f)$.

Definition 3 *Let $f, q \in R$ with $\deg(f) = e$ and $\deg(q) = d$. Let $\mathcal{S}_{f,q}$ denote the set of sequences $A = (a_0, a_1, \cdots)$ that are the coefficient sequences of the f-adic expansions of those rational functions u/q such that $u \in R$, $u \neq 0$, and $\deg(u) < \deg(d)$. A sequence $A \in \mathcal{S}_{f,q}$ is an (f,q)-adic ℓ-sequence if A has period $p^{sd} - 1$, that is, if e divides d, if q is irreducible, and if f is primitive modulo q.*

III. Distribution Property

In this section we show that the distribution of substrings is nearly uniform in an (f,q)-adic ℓ-sequence.

Let A be a periodic sequence of period N. An *occurrence of $b = (b_0, \cdots, b_{r-1})$ in A* is an index $i < N - 2$ such that $(a_i, a_{i+1}, \cdots, a_{i+r-1}) = b$. A sequence A is a *deBruijn sequence of span r* if every element of length r occurs exactly once in A. A sequence A is a *modified deBruijn sequence of span r* if it is obtained from a deBruijn sequence of span r by deleting a single element from one occurrence of r identical consecutive elements. In this section we show that an (f,q)-adic ℓ-sequence is a modified deBruijn sequence.

Let e, s, and k be integers, $n = es$, $d = ek$, and $f, q \in \mathbf{F}_{p^s}[x]$ with $\deg(f) = e$, $\deg(q) = d$, q irreducible, and f a primitive element in $R/(q)$. Any (f,q)-adic ℓ-sequence A is periodic with period $p^{nk} - 1$.

Theorem 4 *With the hypotheses as above, the number of occurrences of a sequence b of length $r \leq k$ in A is $p^{n(k-r)}$ if $b \neq (0, \cdots, 0)$ and is $p^{n(k-r)} - 1$ otherwise.*

Proof: First note that i is an occurrence of a sequence b in A if and only if b is the first r elements of the shift of A to the left by i positions. Let

$$\alpha' = \frac{\alpha - a_0}{f} = \sum_{i=0}^{\infty} a_{i+1} f^i.$$

This is a rational function u'/q', with u' and q' relatively prime, whose coefficient sequence is a shift of A. Moreover, f cannot divide q'. We have

$$\frac{u}{q} = a_0 + f\frac{u'}{q'} = \frac{a_0 q' + f u'}{q'},$$

and q' is relatively prime to $a_0 q' + f u'$. It follows that $q' = q$. Repeating this we see that every shift of A is the f-adic coefficient sequence of a rational function with denominator q. Every shift of A is periodic, so the degree of the numerator is less than d. Moreover, the number of shifts of A is $p^{nk} - 1$ and all shifts are distinct (otherwise the period of A would be smaller than $p^{nk} - 1$). But there are exactly $p^{nk} - 1$ nonzero polynomials over $\mathbf{F}_{p^s}$ of degree less than d. Therefore the number of occurrences of b in A is equal to the number of nonzero polynomials u' of degree less than d such that b is the first r coefficients of the f-adic expansion of u'/q.

The sequence b is the first r coefficients of the f-adic expansion of u'/q if and only if $u'/q \equiv \sum_{i=0}^{r-1} b_i f^i \pmod{f^r}$, if and only if

$$u' \equiv q \sum_{i=0}^{r-1} b_i f^i \equiv \sum_{i=0}^{r-1} c_i f^i \pmod{f^r} \tag{3}$$

for some $c = (c_0, \cdots, c_{r-1})$ that depends only on b and q. The sequence c determines the low $re - 1$ degree monomials of u', leaving the remaining $d - 1 - (re - 1) = e(k - r)$ monomials free. Thus there are $p^{se(k-r)} = p^{n(k-r)}$ polynomials u' of degree less than d satisfying equation (3). They are all nonzero if b is nonzero, and all but one is nonzero if b is zero. The theorem follows. □

Golomb's first randomness postulate for a sequence over $\mathbf{F}_{p^n}$ of period $p^{nk} - 1$ says that the sequence is as balanced as possible, in the sense that in each period every element except 0 occurs $p^{n(k-1)}$ times, while 0 occurs $p^{n(k-1)} - 1$ times (see [2] for the binary case).

Corollary 5 *Any (f,q)-adic ℓ-sequence is balanced.*

Corollary 6 *The sequence A is a modified deBruijn sequence. That is, if we insert a single zero in the unique subsequence with $k-1$ zeros, then we obtain a sequence in which every length k sequence occurs exactly once.*

IV. Run Property

The run property is the second of Golomb's randomness postulates [2].

Definition 7 *A* run of length r *in a sequence $A = a_0, a_1, \cdots$ of period N over $\mathbf{F}_{p^n}$ is a sequence of r consecutive identical symbols that is not contained in a longer sequence of identical symbols. That is, it is an index i such that $1 \leq i \leq N$ and $a_{i-1} \neq a_i = a_{i+1} = \cdots = a_{i+r-1} \neq a_{i+r}$.*

Definition 8 *A sequence A over $\mathbf{F}_{p^n}$ with period $p^{nk}-1$ has the* run property *if the number of runs of length $r \leq k-1$ is $p^{n(k-r-1)}(p^n-1)^2$, the number of runs of length k is $p^n - 1$, and there are no runs of length greater than k.*

Theorem 9 *Suppose that e, s, and k are integers, $n = es$, $d = ek$, and $f, q \in R$ are polynomials of degrees e and d respectively. If $A \in \mathcal{S}_{f,q}$ is an (f,q)-adic ℓ-sequence, then A has the run property.*

Proof: A run of length r is of the form $xyy\cdots yz$ where x and z are distinct from y, and the number of ys is r. If $1 \leq r \leq k-2$, then by Theorem 4 there are $p^{n(k-r-2)}$ occurrences of such a subsequence of A for each x, y, z, so there are $p^{n(k-r-1)}(p^n-1)^2$ runs of length r.

Let $r = k-1$. Each sequence $xyy\cdots y$ of length k with $x \neq y$ occurs once. If $y \neq 0$, then there is one choice of x for which the next symbol after the ys is another y, and no such choice of x if $y = 0$. Thus there are $p^n - 2$ runs of length $k-1$ for each nonzero y, p^n-1 runs of length $k-1$ for $y=0$, and $(p^n-1)^2$ runs of length $k-1$ in all.

Let $r = k$. For each $y \neq 0$ there is one sequence of k consecutive ys, so there must be a run of ys of length k and no run of length greater than k. There is no sequence of k consecutive 0s. This proves the theorem. □

V. Shift and Add and Autocorrelations

Golomb's third randomness postulate is that the shifted autocorrelations are at most 1 in absolute value [2]. Such sequences are said to have *ideal autocorrelations*. The notion of autocorrelation is usually defined only for sequences over prime fields, so we must find a sensible generalization for Golomb's third randomness postulate.

Golomb also defined a property called the *shift-and-add property* which can be used to prove that a binary sequence has ideal autocorrelations. We generalize the shift-and-add property as follows. Let $(G, +)$ be a group and let $\mathcal{S}$ be a set of sequences with components in G. A shift of a sequence $A = (a_0, a_1, \cdots) \in \mathcal{S}$ is a sequence $(a_i, a_{i+1}, \cdots)$. For any two sequences $A = (a_0, a_1, \cdots)$ and $B = (b_0, b_1, \cdots)$ with components in G, let $A - B$ denote the componentwise difference of A and B. That is, $A - B = (a_0 - b_0, a_1 - b_1, \cdots)$. The set $\mathcal{S}$ has the *shift-and-subtract property* if $A - B \in \mathcal{S}$ whenever $A \in \mathcal{S}$, B is a shift of an element of $\mathcal{S}$, and $A \neq B$. In our case the group G is the additive group of $R/(f)$.

Below we generalize the notion of autocorrelation to sequences over arbitrary groups and use the shift-and-subtract property to show that every (f,q)-adic ℓ-sequence has ideal autocorrelations.

Theorem 10 *The set of sequences $\mathcal{S}_{f,q}$ has the shift-and-subtract property.*

Proof: A shift of a sequence in $\mathcal{S}_{f,q}$ is in $\mathcal{S}_{f,q}$, and any two sequences A and B in $\mathcal{S}_{f,q}$ are the coefficient sequences of rational functions u/q and u'/q, where u and u' have degrees less than d. The set S of polynomials of degree less than e is closed under addition and subtraction. Thus $A - B$ is the coefficient sequence of the rational function $(u-u')/q$. Since $u - u'$ has degree less than d, it follows that $A - B \in \mathcal{S}_{f,q}$ unless $A = B$. □

To generalize the ideal autocorrelation property to sequences over a finite group G, we must consider all characters of G.

Definition 11 *A* character *of a finite group G is a group homomorphism from G to the multiplicative group of the complex numbers $\mathbf{C}$. That is, it is a function $\chi : G \to \mathbf{C}$ such that $\chi(a+b) = \chi(a)\chi(b)$ for all $a, b \in G$. Such a function is* nontrivial *if $\chi(a) \neq 1$ for some a.*

The image of a character consists of elements of finite order, hence must be in the unit circle. If r is the least common multiple of the orders of the elements of G and ζ is a complex primitive rth root of unity, then the image of a character of G is in the set of powers of ζ.

Definition 12 *Let G be a finite group.*

1. *Let A be a sequence over G with period N and let χ be a character of G. The* autocorrelation function *on A with respect to χ is the function*
$$\mathcal{A}_{A,\chi}(t) = \sum_{i=0}^{N-1} \chi(a_i)\overline{\chi(a_{i+t})} = \sum_{i=0}^{N-1} \chi(a_i + a_{i+t}).$$
2. *A sequence A over G with period N has* ideal autocorrelations *if for every nontrivial character χ of G and every $t \not\equiv 0 \pmod{N}$ we have $|\mathcal{A}_{A,\chi}(t)| \leq 1$.*

Theorem 13 *Suppose that e, s, and k are integers, $n = es$, $d = ek$, and $f, q \in R$ have degrees e and d. Suppose that $A = (a_0, a_1, \cdots)$ is an (f,q)-adic ℓ-sequence. Then A has ideal autocorrelations.*

Proof: Let ζ be a complex primitive pth root of unity. Every nonzero element of $R/(f)$ has additive order p. Thus the image of any nontrivial character χ is in $\{\zeta^i : i = 0, 1, \cdots, p-1\}$. If we let $\sigma(a) = i$ if $\chi(a) = \zeta^i$, $0 \le i \le p-1$, then σ is an $\mathbf{F}_p$-linear vector space homomorphism from $R/(f)$ to $\mathbf{F}_p$. Thus there is a basis $\gamma_1, \cdots, \gamma_n$ of $R/(f)$ over $\mathbf{F}_p$ such that $\chi(\gamma_1) \ne 1$ and $\chi(\gamma_i) = 1$ for $2 \le i \le n$. Therefore by Corollary 5 we have

$$\begin{aligned}
&\sum_{i=0}^{p^{nk}-2} \chi(a_i) = p^{n(k-1)} \sum_{x \in R/(f)} \chi(x) - 1 \\
&= p^{n(k-1)} \sum_{b_1,\cdots,b_n \in \mathbf{F}_p} \chi(\sum_{i=1}^{n} b_i \gamma_i) - 1 \\
&= p^{n(k-1)} \sum_{b_2,\cdots,b_n \in \mathbf{F}_p} \chi(\sum_{i=2}^{n} b_i \gamma_i) \sum_{b_1 \in \mathbf{F}_p} \chi(\gamma_1)^{b_1} - 1 \\
&= -1.
\end{aligned}$$

By Theorem 10, for any $t \not\equiv 0 \pmod{p^{nk}-1}$ there is an integer s so that for all i, $a_i + a_{i+t} = a_{i+s}$. Thus

$$\begin{aligned}
\mathcal{A}_{A,\chi}(t) &= \sum_{i=0}^{p^{nk}-2} \chi(a_i + a_{i+t}) = \sum_{i=0}^{p^{nk}-2} \chi(a_{i+s}) \\
&= \sum_{i=0}^{p^{nk}-2} \chi(a_i) = -1.
\end{aligned}$$

□

VI. Distinctness from m-sequences

Let e, s, and k be integers, $n = es$, $d = ek$, and let $f, q \in R$ have degrees e and d respectively. Let $A \in \mathcal{S}_{f,q}$ be an (f,q)-adic ℓ-sequence. If f is irreducible, then A is a sequence of elements of $\mathbf{F}_{p^n}$. It is well known that m-sequences over a finite field have all the randomness properties that we have discussed (in fact, m-sequences are exactly the case $e = 1$). Furthermore, if $n = 1$ and $p = 2$, then it is conjectured that m-sequences are the only balanced sequences that have the run property and ideal autocorrelations [2]. Thus it is natural to ask whether (f,q)-adic ℓ-sequences are in general simply m-sequences. We must take care to make this question precise. The (f,q)-adic ℓ-sequence A is a sequence with entries in the set S (or $R/(f)$), while any m-sequence we compare it to will have entries in $\mathbf{F}_{p^n}$. When f is irreducible, the field $\mathbf{F}_{p^n}$ is isomorphic to $R/(f)$, so we consider these to be identified.

Let $q = \sum_{i=0}^{k} q_i f^i$ with $q_i \in S$. Since $\deg(q) = ek$, we must have $q_k \in \mathbf{F}_{p^s}$. In fact we may assume that $q_k = 1$ since multiplying q by an element of $\mathbf{F}_{p^m}$ does not change the set of coefficient sequences for rational functions of the form u/q.

Theorem 14 *If $e \ge 2$, f is irreducible, and at least one q_j has degree greater than 0, then A is not an m-sequence.*

Proof: Suppose to the contrary that A is an m-sequence. We know that A can be generated by an AFSR of length k based on $\mathbf{F}_{p^s}$, f, and S with connection element q, and we know that A can be generated by an LFSR with elements in $\mathbf{F}_{p^n}$, and with length k. Associated with this LFSR is a connection polynomial $r(x,y) \in \mathbf{F}_{p^n}[y]$, and we can write $r(x,y) = \sum_{i=0}^{k} q_i' y^i$ with $q_i' \in \mathbf{F}_{p^n}$ and $q_k' = 1$. If $(a_0, \cdots, a_{k-1}; m)$ and $(a_1, \cdots, a_k; m')$ are consecutive periodic states of the AFSR, then $(a_0, \cdots, a_{k-1})$ and $(a_1, \cdots, a_k)$ are consecutive periodic states of the LFSR

The output from an AFSR with connection element q is the coefficient sequence of a rational function α with denominator q [9]. If the initial state is $(a_0, \cdots, a_{k-1}; m)$, then

$$\alpha = \frac{\sum_{t=0}^{k-1} \sum_{i=0}^{t} q_i a_{t-i} f^t - m f^k}{q}.$$

Consider the state with $m = 0$, some $a_\ell = 1$, and all other $a_i = 0$. Then the numerator of $\alpha = (\sum_{t=j}^{k-1} q_{t-j} f^t)/q$ has degree less than $d = ke$, so the coefficient sequence of α is strictly periodic. If γ is the inverse of q_0 modulo f (with $\deg(\gamma) < e$), then the next state of the AFSR is $(a_1, a_2, \cdots, a_{k-1}, \gamma q_j; m')$ for some m'. Thus if we take $(a_0, a_1, \cdots, a_{k-1})$ as the initial state of the LFSR with connection polynomial $r(x,y)$, then the next state of the LFSR is $(a_1, a_2, \cdots, a_{k-1}, \gamma q_j)$. However, from the state $(a_0, a_1, \cdots, a_{k-1})$ of an LFSR the next state is also $(a_1, a_2, \cdots, a_{k-1}, q_j')$, and it follows that $q_j' \equiv \gamma q_j \pmod{f}$.

Now suppose that $\deg(q_j) > 0$ for some j. Let $g_j \equiv -q_j^{-1} \pmod{f}$, $1 \le \deg(g_j) < e$, so there is an $m \ne 0$ so that $q_j g_j = -1 + mf$. Note that $1 \le \deg(m) \le e - 2$. Consider the state of the AFSR with $a_i = 0$ for $i \ne k-1-j$, $a_{k-1-j} = g_j$, and memory m. Then $\sum_{t=0}^{k-1} \sum_{i=0}^{t} q_i a_{t-i} f^t - m f^k$ has degree less than d, so once again we have a state that generates a periodic sequence. In the AFSR the next state $(a_1, \cdots, a_k; m')$ satisfies $m' f + q_0 a_k = m + q_j g_j$. In the LFSR, the next state $(a_1, \cdots, a_k)$ satisfies $a_k \equiv q_j' g_j \equiv \gamma q_j g_j \equiv -\gamma \pmod{f}$. It follows that $m \equiv 0 \pmod{f}$. But the degree of m is at most $e-2$, so m is not divisible by f unless $m = 0$, a contradiction. □

Questions remain concerning uniqueness and distinctness. First, it may be that A is an m-sequence with the symbols of the underlying alphabet permuted.

Conjecture 15 *If A is an (f,q)-adic ℓ-sequence with $\deg(f) \ge 2$ then there is no set theoretic isomorphism $\sigma : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ such that the sequence $(\sigma(a_0), \sigma(a_1), \cdots)$ is an m-sequence.*

Next, suppose we have a second pair of polynomials $f', q' \in R$ of degrees e and d such that f' is primitive modulo q'. The resulting (f',q')-adic ℓ-sequence may or may not be distinct from A. In fact, it is apparent from the examples below that the reversal of A and certain sequences obtained from A by permuting the set S are again (f',q')-adic ℓ-sequences for some f' and q'. It would be interesting to determine just how many new sequences arise by our construction for a given e,d.

More generally, suppose we take another set of integers s',e',k' with $s'e' = se$ and $e'k' = ek$, but $s \neq s'$; and polynomials $f',q' \in \mathbf{F}_{p^{s'}}[x] = R'$ of degrees e' and $e'k'$ such that f' is primitive modulo q'. In this case we conjecture that the the resulting (f',q')-adic ℓ-sequence is distinct from A.

VII. Existence

It is not immediately apparent that (f,q)-adic ℓ-sequences that are not m-sequences are abundant. In order to find such sequences we must find a pair of polynomials f and q with $e = \deg(f) \geq 2$, $d = \deg(q)$ divisible by e, $q = \sum_{i=0}^{k} q_i f^i$ with at least one q_i of degree greater than 0, and q irreducible.

Let $q(x) \in R$ be a primitive polynomial of degree d. Then x is a primitive element in $\mathbf{F}_{p^s}[x]/(f) = \mathbf{F}_{p^{se}}$. Let $f(x) = x^t$ where $t > 1$ divides d. Then f is primitive modulo q if and only if $\gcd(t, p^d - 1) = 1$. In particular, t can be any divisor of d if $\gcd(d, p^d - 1) = 1$. Thus in these cases we obtain (f,q)-adic ℓ-sequences. For example if $p = 2$, then we can take $f = x^2$ and q any primitive polynomial of even degree, or $f = x^3$ and q any primitive polynomial whose degree is an odd multiple of 3.

We can ask whether for any polynomial f of degree e over $\mathbf{F}_{p^s}$ and multiple d of e there is a polynomial q of degree d over $\mathbf{F}_{p^s}$ such that f is primitive mod q. A pair (f,d) is *acceptable* if at least one such q exists. There are certain "degenerate" pairs (f,d) that are not acceptable. Suppose $t \neq 1$ is a divisor of d, and $f = g^t$ for some $g \in R$. Suppose also that $\gcd(t, p^{sd} - 1) > 1$. If q is irreducible, then $R/(q)$ is isomorphic to $\mathbf{F}_{p^{sd}}$. Thus $(R/(q))^*$ is a cyclic group of order $p^{sd} - 1$. Thus

$$f^{(p^{sd}-1)/\gcd(t,p^{sd}-1)} \equiv 1 \pmod{q},$$

so f is not primitive modulo q. We have done a computer search to test whether any nondegenerate pairs are not acceptable, even ignoring the condition that e divide d. Curiously, for $p = 2$ and $d \leq 22$ the only nondegenerate pair that is not acceptable is $(x^4 + x, 6)$.

Conjecture 16 *If (f,d) is a nondegenerate pair with $f \in \mathbf{F}_{p^s}[x]$ and d a multiple of the degree of e, then there is a polynomial $q \in \mathbf{F}_{p^s}[x]$ of degree d such that f is primitive modulo q.*

VIII. Examples

In this section we let $p = 2$ and $s = 1$. If $\deg(f) = 1$, then we obtain m-sequences. The case $f(x) = x$ is the standard analysis of m-sequences by power series. The case $f(x) = x + 1$ is equivalent by a change of basis.

Suppose that f has degree 2. Then for any choice of q we obtain sequences with elements in $U = \mathbf{F}_2[x]/(f) = \{0, 1, x, x+1\}$. If $f(x) = x^2 + x + 1$, which is irreducible over $\mathbf{F}_2$, we have $U = \mathbf{F}_4$, but for all other fs of degree two the ring U is not a field. If we let $f(x) = x^2 + x + 1$ and use the connection element $q(x) = x^4 + x^3 + 1 = f^2 + xf + x$, then it can be shown that f is primitive modulo q and one period of the (f,q)-adic ℓ-sequence we obtain is (possibly a cyclic shift of)

$$1, 1, x, 0, 1, 0, x, x, x+1, x+1, 1, x+1, 0, x+1, x. \quad (4)$$

All other (f,q)-adic ℓ-sequences obtained by different choices of f of degree 2 and q of degree 4 with f primitive modulo q are obtained from the sequence (4) by some combination of shifts, reversals, and permutations of the alphabet $\{0, 1, x, x+1\}$.

However, the sequence with one period equal to

$$1, 1, x, 1, 0, x+1, x+1, 1, x+1, 0, x, x, x+1, x, 0$$

is an m-sequence over $\mathbf{F}_4$, and all other m-sequences of span 2 over $\mathbf{F}_4$ are obtained from this sequence by some combination of shifts, reversals, and switching x and $x+1$. This illustrates the fact that the new set of sequences is disjoint from the set of m-sequences.

References

[1] R. Couture and P. L'Ecuyer, On the lattice structure of certain linear congruential sequences related to AWC/SWB generators. Math. Comp. **62** (1994), p. 799–808.

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

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

[4] M. Goresky and A. Klapper, Periodicity and arithmetic correlations of algebraic feedback shift register sequences over ramified extensions of the rationals, to appear, *Designs, Codes, and Cryptography.*

[5] A. Klapper, Distributional properties of d-FCSR sequences, in preparation.

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

[7] A. Klapper and M. Goresky, Large period nearly de Bruijn FCSR sequences, *Advances in Cryptology - Eurocrypt 1996.* LNCS **921**, Springer Verlag, New York, 1995, pp. 263-273.

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

[9] A. Klapper and J. Xu, Algebraic feedback shift registers, *Theoretical Comp. Sci.* **226** (1999) pp. 61-93.

[10] A. Klapper and J. Xu, Register synthesis for algebraic feedback shift registers based on non-primes, to appear.

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

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