Algebraic Feedback Shift Registers Based on Function Fields

Andrew Klapper[1]

University of Kentucky
Department of Computer Science, 779 A Anderson Hall
Lexington, KY 40506-0046, USA
klapper@cs.uky.edu
http://www.cs.uky.edu/∼klapper/

Abstract. We study algebraic feedback shift registers (AFSRs) based on quotients of polynomial rings in several variables over a finite field. These registers are natural generalizations of linear feedback shift registers. We describe conditions under which such AFSRs produce sequences with various ideal randomness properties. We also show that there is an efficient algorithm which, given a prefix of a sequence, synthesizes a minimal such AFSR that outputs the sequence.

1 Introduction

Linear feedback shift registers (LFSRs) are useful for many applications, including cryptography, coding theory, CDMA, radar ranging, and pseudo-Monte Carlo simulation. There is a large body of literature on these simple devices for generating pseudorandom sequences. Naturally, many variations and generalizations of LFSRs have been studied. Algebraic feedback shift registers (AFSRs) are a very general class of sequence generators that include LFSRs as a special case [8]. Each class of AFSRs is based on a choice of an algebraic ring R and a parameter $r \in R$. In the case of LFSRs R is $F[x]$, the ring of polynomials in one variable x over a finite field F, and $r = x$. In previous work we have studied AFSRs over the integers [7] and certain finite extensions of the integers [3, 5, 9]. More recently [4] we have studied AFSRs over $F[x]$ when $r \neq x$. In this paper we generalize this last work further and study AFSRs over polynomial rings of transcendence degree one over finite fields. We call this the function field case since, in the language of algebraic geometry, the field of fractions of such a ring is the function field of an algebraic curve. We describe the basic properties (such as periodicity) of the resulting sequences.

Two aspects of LFSRs that make them especially interesting are the statistical randomness of maximum period LFSR sequences (*m-sequences*) and the existence of the Berlekamp-Massey algorithm. This algorithm efficiently solves the register synthesis problem: given a prefix of a sequence, find a smallest LFSR that outputs the sequence. This algorithm plays a role in both cryptanalysis and error correction. It has been generalized to the setting of codes defined over algebraic curves, or *algebraic geometry codes*, where it is used to solve the so called

"key equation" [12–14], and it has been generalized to the setting of FCSRs and some more general AFSRs [9]. There is, however, no known generalization of the Berlekamp-Massey algorithm that works for all classes of AFSRs, although there is a general approach that works if there is a reasonable analog of degree [9]. We show here that there is such an analog in the function field case, resulting in a solution to the register synthesis problem for AFSRs based on function fields. We characterize the maximal period sequences for a given length of AFSR and show that they have certain good statistical properties — uniform distribution of small subsequences, the run property, and ideal autocorrelations. We also compare them to Blackburn's classification of sequences [1] with the shift and add (SAA) property and show that all sequences with the SAA property and uniform distributions are maximal period sequences over function fields.

A class of AFSRs depends on a choice of ring R, $r \in R$, and $S \subseteq R$, a complete set of representatives modulo r. An AFSR is determined by $q_0, q_1, \cdots, q_k \in R$, q_0 invertible modulo r. States are tuples $(a_0, a_1, \cdots, a_{k-1}; m)$ with $a_i \in S$ and $m \in R$. The element m is called the *extra memory*. The AFSR changes states as follows. There are unique $a_k \in S$ and $m' \in R$ so that

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

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, $r = x$, $S = F$, all $q_i \in S$, and $q_0 = 1$. AFSRs are analyzed in terms of coefficient sequences of r-adic numbers $\sum_{i=0}^{\infty} a_i r^i$, $a_i \in S$. The set of r-adic numbers is denoted by R_r. R_r is a ring, and such an r-adic number is invertible in R_r if and only if a_0 is invertible modulo r. The r-adic number $\alpha(A, r) = \sum_{i=0}^{\infty} a_i r^i$ associated with the output sequence $A = a_0, a_1, \cdots$ is in fact a rational element u/q where $u \in R$ and $q = \sum_{i=1}^{k} q_i r^i - q_0$. In some cases maximal period AFSR sequences, or ℓ-sequences, share many desirable properties with m-sequences [8]. We have shown, for example, that when R is $\mathbf{Z}$ or $\mathbf{Z}[\sqrt{N}]$ for some integer N, then ℓ-sequences have excellent randomness properties, similar to those of m-sequences [4, 5, 7].

One can also consider rings R with nonzero characteristic. Previously we showed that if $R = F[x]$ and $R/(r)$ is not a prime field, ℓ-sequences are distinct from m-sequences but have similar statistical properties: the distributions of subsequences in these ℓ-sequences are as uniform as possible, their distributions of lengths of runs matches the expectation and they have the shift and add property [4]. Thus, with an appropriate definition, they have ideal autocorrelations. In this paper we describe conditions under which the same randomness properties hold in the higher genus case.

It has been shown by Blackburn that every sequence of period $p^{hk} - 1$ over an extension F_{p^h} of F_p with the shift and add property is the F_p-linear image of successive powers of a primitive element in $F_{p^{hk}}$ [1]. Moreover, the sequences that also have uniform distributions can be identified within this classification. The advantage of the approach described here is that it leads to more efficient implementations of generators of the sequences than Blackburn's description.

2 Setting and Hypotheses

In this section we describe the general setting for the sequences we are studying and various conditions that may need to hold to obtain sequences with good properties.

Let $p \in \mathbf{Z}$ be prime, $h > 0 \in \mathbf{Z}$, and I and r be an ideal and an element in $\mathbf{F}_{p^h}[x_1, \cdots, x_n]$. Assume that $R = \mathbf{F}_{p^h}[x_1, \cdots, x_n]/I$ has transcendence degree 1 over $\mathbf{F}_{p^h}$ and that $K = R/(r)$ is finite. Then $R/(r)$ is a vector space over $\mathbf{F}_{p^h}$ so its cardinality is a power of p^h, say p^{he}. If $n = 1$, $r = x_1$, and $I = (0)$, then the AFSRs we obtain are exactly the LFSRs.

One goal is to obtain conditions under which the output from an AFSR based on these ingredients is statistically random. In order to construct AFSRs with good statistical properties we need a "well structured" complete set of representatives S for R modulo r.

Hypothesis H1: S is closed under addition and contains F_{p^h}.

It is straightforward to see that such sets S exist in abundance (the F_{p^h}-span of a lift of a basis containing 1 from $R/(r)$ to R with 1 lifted to 1). Any S that satisfies H1 is closed under multiplication by F_p, but possibly not under multiplication by any larger field. In general we can represent any element of R as an r-adic element with coefficients in S, but in order that we get good randomness properties we need to be able to represent the elements of R finitely.

Hypothesis H2: If $v \in R$ then for some $\ell \in \mathbf{Z}$ and $v_0, \cdots, v_\ell \in S$,

$$v = \sum_{i=0}^{\ell} v_i r^i. \tag{2}$$

Since r is not a zero divisor, the representation in equation (2) is unique if $v_\ell \neq 0$. Indeed, suppose that

$$\sum_{i=0}^{m} u_i r^i = \sum_{i=0}^{\ell} v_i r^i$$

for some $u_i, v_i \in S$ with $u_m \neq 0 \neq v_\ell$ and $(u_0, u_1, \cdots) \neq (v_0, v_1, \cdots)$ and let ℓ be the minimal integer so that such a pair of representations exists. Reading this equation modulo r we see that $u_0 = v_0$, so by subtraction we may assume that $u_0 = v_0 = 0$. But the fact that r is not a zero divisor then implies that

$$\sum_{i=0}^{m-1} u_{i+1} r^i = \sum_{i=0}^{\ell-1} v_{i+1} r^i$$

and $(u_1, u_2, \cdots) \neq (v_1, v_2, \cdots)$. This contradicts the minimality of ℓ.

We say that the ℓ in Hypothesis H2 is the *r-degree of* v, $\ell = \deg_r(v)$.

Lemma 1. *If Hypotheses H1 and H2 hold, then for all* $u, v \in R$, $\deg_r(u+v) \leq \max(\deg_r(u), \deg_r(v))$. *Let* $a = \max\{\deg(st : s, t \in S\}$. *Then for all* $u, v \in R$,

$$\deg_r(uv) \leq \deg_r(u) + \deg_r(v) + a.$$

To prove randomness properties we need an additional hypothesis. Let V_q denote the set of elements u of R such that v/q has a periodic r-adic expansion.

Hypothesis H3: The elements of V_q are distinct modulo r^k.

3 Periodicity

Let $A = a_0, a_1, \cdots$ be the output from an AFSR based on R, r, S with connection element

$$q = \sum_{i=1}^{k} q_i r^i - q_0, q_i \in S,$$

with q_0 invertible modulo r. It follows that

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

for some $u \in R$. We call this a rational representation of A. Any left shift of A can be generated by the same AFSR (with a different initial state), so also has a rational representation with denominator q. Our first task is to analyze the period of A. We need one fact from the general theory of AFSRs (which was misstated in the original paper and is correctly stated here).

Theorem 1. *([8]) Let* A *be periodic. Let* U *denote the set of elements* $v \in R$ *such that* v/q *is a rational representation of a shift of* A. *Suppose no two elements of* U *are congruent modulo* q *and let* V *be a complete set of representatives modulo* q *containing* U. *Then*

$$a_i = q_0^{-1}(wr^{-i} \pmod q) \pmod r, \tag{3}$$

for some $w \in R/(q)$.

By equation (3) we mean first find the multiplicative inverse δ of the image of r in $R/(q)$. Raise δ to the ith power and multiply by w. Then lift the result to an element of V. Reduce the result modulo r to an element of $R/(r)$. Finally, multiply that element by the inverse of the image of q_0 in $R/(r)$.

Let V_q denote the set of elements u of R such that v/q has a periodic r-adic expansion.

Corollary 1. *If* A *is periodic and no two elements of* V_q *are congruent modulo* q, *then*

$$a_i = q_0^{-1}(wr^{-i} \pmod q) \pmod r$$

for some $w \in R/(q)$.

In our case the stronger condition in the corollary holds.

Theorem 2. *A is eventually periodic. If S satisfies Hypotheses H1 and H2, then A's eventual period is a divisor of the multiplicative order of r modulo q. If $R/(q)$ is an integral domain, then the period equals the multiplicative order of r modulo q. In general, for a given q there is at least one periodic sequence with connection element q whose period is the multiplicative order of r modulo q.*

Proof: To see that A is periodic, it suffices to show that the r-degree of the extra memory of the AFSR is bounded, for then there are finitely many distinct states of the AFSR. Eventually the state repeats and from then on the output is periodic.

Suppose that at some point the AFSR is in state

$$(a_j, a_{j+1}, \cdots, a_{j+k-1}; m)$$

with $m = \sum_{i=0}^{\ell} m_i r^i$ and $m_0, \cdots, m_\ell \in S$. Also, suppose that the maximal r-degree of the product of two elements of S is d. Then the carry m' of the next state satisfies

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

The right hand side is divisible by r and its r-degree is at most $\max\{\ell, d\}$, so the r-degree of m' is at most $\max\{\ell - 1, d - 1\}$. Thus the r-degree of the carry decreases monotonically until it is less than d, and then remains less than d forever.

To describe the eventual period, it suffices to consider strictly periodic sequences since q is also a connection element of every shift of A. We claim that no two elements of V_q are congruent modulo q. One consequence of Hypothesis H1 is that the r-adic sum of two periodic sequences is the term-wise sum, so is also periodic. Thus to prove our claim it suffices to show that no nonzero element of V_q is divisible by q. Suppose to the contrary that $uq \in V_q$. Then $u = uq/q$ has a periodic r-ary expansion. But this contradicts the fact that any element of R has a unique r-adic expansion.

Now consider the series of numerators $u_0, u_1, \cdots$ of the rational representations of the r-adic elements associated with the shifts of A. The period is the least t such that $u_t = u_0$. By the argument in the preceding paragraph, this is equivalent to $u_t \equiv u_0 \pmod{q}$. For every i,

$$\frac{u_{i-1}}{q} = a_{i-1} + r\frac{u_i}{q},$$

and so $u_{i-1} = qa_{i-1} + ru_i$. Therefore $u_i \equiv r^{-1}u_{i-1} \equiv r^{-i}u_0 \pmod{q}$ by induction. Thus $u_t \equiv u_0 \pmod{q}$ if and only if $r^t u_0 \equiv u_0 \pmod{q}$, which is equivalent to $(r^t - 1)u_0 \equiv 0 \pmod{q}$.

If $R/(q)$ is an integral domain, then this says that i is the multiplicative order of r modulo q. If $R/(q)$ is not an integral domain, then it implies that i is a divisor of the multiplicative order of r modulo q.

Finally, consider the coefficient sequence of the r-adic expansion of $1/q$. This sequence may not be periodic, but it is eventually periodic, for some j the its shift by j positions is periodic. This shift has a rational representation u/q, and by the above argument, $u \equiv r^{-j} \pmod{q}$. In particular, u is invertible modulo q, so $(r^i - 1)u \equiv 0 \pmod{q}$ if and only if $r^i \equiv 1 \pmod{q}$. Thus in this case the period equals the multiplicative order of r modulo q. □

Corollary 2. (To the proof.) *A has an exponential representation.*

4 ℓ-Sequences and Randomness

Let A be an AFSR of sequence of the type described in Section 2. The period A is largest if $R/(q)$ is a field and r is primitive. Then A has period $p^{hg} - 1$ for some g. A is a *punctured de Bruijn sequence of span k* if each nonzero sequence B of length k in a period of A occurs once and the all-zero sequence of length k does not occur. To produce punctured de Bruijn sequences over $\mathbf{F}_{p^{he}}$ we want the period to be of the form $p^{hek} - 1$. Thus $hg = hek$, so $g = ek$.

Definition 1. *Let $r, q \in R$, $q = \sum_{i=1}^{k} q_i r^i - q_0$ with $q_k \neq 0$, $|R/(r)| = p^{he}$, $S \subseteq R$, and suppose Hypotheses H1 and H2 hold. Let $|R/(q)| = p^{hg}$, and let $R/(q)$ be a field. Let $A = (a_0, a_1, \cdots)$ be the coefficient sequence of the r-adic expansion of a rational function u/q such that $u \neq 0 \in R$ (or equivalently, that is the nonzero periodic output sequence from an AFSR with connection element q). Then A is an* (r, q)-adic ℓ-sequence *if A is periodic with period $p^{hg} - 1$. That is, if r is primitive modulo q.*

Theorem 3. *Suppose A is an (r, q)-adic ℓ-sequence, Hypotheses H1, H2, and H3 hold, and $q_k \in \mathbf{F}_{p^h}$. Then the following hold.*

1. *A is a punctured de Bruijn sequence. Thus the number of occurrences of a sequence B of length $m \leq k$ in a period of A is $p^{he(k-m)}$ if $B \neq (0, \cdots, 0)$ and is $p^{he(k-m)} - 1$ otherwise.*
2. *A has the shift and add property*
3. *A is balanced.*
4. *A has the run property.*
5. *A has ideal autocorrelations. (Care is needed in defining autocorrelations over non-prime fields.)*

Detailed definitions of these properties may be found in Golomb's book [2].
Proof: Properties (3), (4) and (5) follow from properties (1) and (2).

Since $q_k = F_{p^{he}}$ and Hypothesis H2 holds, we have

$$|R/(q)| = |S|^k = p^{hek}.$$

Thus A has period $p^{hek} - 1$. The various shifts of A plus the all-zero sequence give p^{hek} periodic sequences corresponding to elements u/q. Thus,

$$|V_q| \geq p^{hek}.$$

We have seen that the elements of V_q are distinct modulo q, so

$$|V_q| \le p^{hek}.$$

Thus,

$$|V_q| = p^{hek} = |R/(r^k)|.$$

By Hypothesis H3, the elements of V_q are distinct modulo r^k, so V_q is a complete set of representatives modulo r^k.

The set of occurrences in A of a block B of k elements corresponds to the set of shifts of A that begin with B. By the above, every nonzero u/q with $u \in V_q$ occurs as a shift of A, so the set of occurrences in A of B corresponds to the set of nonzero u/q, $u \in V_q$, that begin with B. We claim that the u/q are distinct modulo r^k, so that each nonzero B occurs once. Suppose not, so that $u/q \equiv v/q \pmod{r^k}$ for some $u \ne v \in V_q$. Then $u \equiv v \pmod{r^k}$ since q is invertible modulo r, and hence also modulo r^k. But by Hypothesis H3 the elements of V_q are distinct modulo r^k. It follows that A is a punctured de Bruijn sequence.

Furthermore, if $u, v \in V_q$, then $u+v \in V_q$. The shifts of A account for all the u/q with $u \ne 0 \in V_q$ so the SAA property follows. □

5 ℓ-Sequences and Blackburn Sequences

Blackburn [1] showed that a sequence $A = a_0, a_1, \cdots$ of period $p^{ek}-1$ over F_{p^e} has the shift and add (SAA) property if and only if there is a primitive element $\alpha \in F_{p^{ek}}$ and a surjective F_p-linear function $T : F_{p^{ek}} \to F_{p^e}$ such that $a_i = T(\alpha^i)$ for all $i \ge 0$. We call sequences realized this way *Blackburn sequences.*

Theorem 4. *Let A be a Blackburn sequence that is a punctured de Bruijn sequence. Then A is an (r,q)-adic ℓ-sequence over F_p.*

This section is devoted to a proof of this theorem.

Corollary 3. *Every punctured de Bruijn sequence with the SAA property is an (r,q)-adic ℓ-sequence over F_p.*

Let $A = a_0, a_1, \cdots$ be a sequence with $a_i = T(\alpha^i)$ with T an F_p-linear function from $F_{p^{ek}}$ to F_{p^e} and α primitive in $F_{p^{ek}}$. We first find necessary and sufficient conditions for A to be a punctured de Bruijn sequence. If $\beta_0, \cdots, \beta_{e-1}$ is a basis of F_{p^e} over F_p, then there are F_p-linear functions $T_i : F_{p^{ek}} \to F_p$, $i = 0, \cdots, e-1$, such that $T = \sum_{i=0}^{e-1} \beta_i T_i$.

Lemma 2. *([10, p. 56]) If $f : F_{p^n} \to F_p$ is F_p-linear, then there is a constant $u \in F_{p^n}$ such that*

$$f(x) = Tr_p^{p^n}(ux).$$

Thus we have

$$T_j(x) = Tr_p^{p^{ek}}(u_j x) \text{ with } u_j \in F_{p^{ek}}, i = 0, \cdots, e-1.$$

As was pointed out by a referee of an earlier paper [4], this makes it possible to characterize the sequences that have the SAA property and uniform distributions. We include a proof since, to our knowledge, this fact has not been described in the literature.

Theorem 5. *Let A have the SAA property. Then A is a punctured de Bruijn sequence if and only if*

$$V = \{u_j \alpha^i : 0 \le j < k, 0 \le i < e\}$$

is a basis for $F_{p^{ek}}$ over F_p.

Proof: The sequence A is a punctured de Bruijn sequence if and only if each nonzero k-tuple of elements of F_{p^e} occurs exactly once in each period of A, and the zero k-tuple does not occur. Since the period of A is $p^{ek} - 1$, this is equivalent to each such k-tuple occurring at most once in A, and the zero k-tuple not occurring. Since A has the SAA property, it is equivalent simply to the zero k-tuple not occurring. Indeed, if any k-tuple occurs twice, then we can shift A by the distance between the two occurrences, then subtract A (the same as adding A $p-1$ times) from this shift to obtain an occurrence of the all zero k-tuple.

The all-zero k-tuple occurs if and only if for some n we have $a_n = a_{n+1} = \cdots = a_{n+k-1} = 0$. That is,

$$Tr_p^{p^{ek}}(u_j \alpha^{i+n}) = 0$$

for $0 \le j < k$ and $0 \le i < e$. The set

$$\alpha^n V = \{u_j \alpha^{i+n} : 0 \le j < k, 0 \le i < e\}$$

is a basis for $F_{p^{ek}}$ over F_p if and only if V is. A linear function is zero on a basis if and only if it is identically zero. But the trace function is not identically zero. Thus, if V is a basis, then A is a punctured de Bruijn sequence.

Conversely, if

$$\sum_{i=0}^{e-1} \sum_{j=0}^{k-1} c_{ij} u_j \alpha^i = 0$$

with each c_{ij} in F_p and not all zero, then for any n,

$$\sum_{i=0}^{e-1} \sum_{j=0}^{k-1} c_{ij} Tr_p^{p^{ek}}(u_j \alpha^{i+n}) = 0.$$

That is, the F_p-coordinates of all k-tuples satisfy a common linear relation. Hence not all nonzero values of k-tuples can occur and A is not a punctured de Bruijn sequence. □

Our goal now is to realize a shift of A as a maximum period AFSR sequence over a function field, i.e., an ℓ-sequence. That is, we want to find a ring $R = F_p[z_1, \cdots, z_n]/I$ with I an ideal, an element $r \in R$, a subset $S \subseteq R$, and an element $q \in R$ so that A is the output from an AFSR based on R, r, S with connection element q. That is,

$$a_i = q_0^{-1}(br^i \pmod q) \pmod r,$$

and equivalently, $\sum_{i=0}^{\infty} a_i r^i = u/q$ in the ring R_r of r-adic elements over R, for some $u \in R$.

We achieve this as follows. For any F_p-linear function f, let K_f denote the kernel of f. We construct an appropriate R together with functions $\Gamma : R \to F_{p^{ek}}$ and $\Delta : R \to F_{p^e}$ so that $K_\Gamma = (q), K_\Delta = (r),$ and $\Delta(s) = qT(c\Gamma(s))$ for $s \in S$ and some constant $c \neq 0 \in F_{p^{ek}}$.

Let $f(x)$ be the minimal polynomial of $r = \alpha^{-1}$ over F_{p^e} so that

$$f(x) = \sum_{i=0}^{k} f_i x^i, f_i \in F_{p^e}.$$

We have $f_k = 1 \in F_p$ and

$$f_0 = r^{(p^{ek}-1)/(p^e-1)},$$

since f_0 is the product of the Galois conjugates r^{p^j}, $j = 0, \cdots, k-1$. Let $\beta = f_0$. Then β is primitive in F_{p^e} and $1, \beta, \cdots, \beta^{e-1}$ is a basis of F_{p^e} over F_p.

We have

$$f_i = \sum_{j=0}^{e-1} f_{ij}\beta^j, f_{ij} \in F_p.$$

Thus we can write

$$f(x) = \sum_{j=0}^{e-1}(\sum_{i=0}^{k} f_{ij}x^i)\beta^j = \sum_{j=0}^{e-1} z_j(x)\beta^j.$$

The polynomial $z_j(x) \in F_p[x]$ has degree at most k. In particular, if $e \geq 2$, then $z_j(x)$ does not have r as a root unless $z_j(x)$ is identically zero.

Note that $f_k = 1$, which implies that $z_0(x)$ has degree k and is nonzero. All other $z_i(x)$ have degree at most $k-1$. Since $f_0 = \beta$, $z_1(x)$ has constant term 1, so is nonzero, and all other $z_i(x)$ have constant term 0.

Lemma 3. *There exist $c, \gamma_0, \cdots, \gamma_{e-1} \in F_{p^{ek}}$ so that*

a. $\sum_{j=0}^{e-1} z_j(r)\gamma_j = 0$;
b. $\gamma_0 = 1$;
c. $T(c\gamma_1) = 1$; *and*
d. $T(c\gamma_0), \cdots, T(c\gamma_{e-1})$ *are linearly independent over* F_p.

Proof: See Appendix A. □

Suppose conditions (a), (b), (c), and (d) hold. By conditions (b) and (d) we have $T(c) = T(c\gamma_0) \neq 0$. We define $\Gamma(y_i) = \gamma_i$ and $\Gamma(x) = r$. We also define $\Delta(y_i) = \delta_i = T(c)^{-1}T(c\gamma_i)$ for $i = 0, \cdots e-1$, and $\Delta(x) = 0$. We then extend these to ring homomorphisms. Let I be the intersections of the kernels of Γ and Δ. The functions Γ and Δ induce functions on $R = F_p[x, y_0, \cdots, y_{e-1}]/I$ for which we shall use the same names. It follows from condition (a) that

$$\sum_{i=0}^{k}\sum_{j=0}^{e-1} f_{ij}\gamma_j r^i = 0.$$

Let

$$S = \{\sum_{i=0}^{e-1} s_i y_i : s_i \in F_p\}.$$

Let

$$q_i = \sum_{j=0}^{e-1} f_{ij} y_j \in S,$$

so that

$$\Gamma(q_i) = \sum_{j=0}^{e-1} f_{ij}\gamma_j.$$

Let $q = \sum_{i=0}^{k} q_i x^i$. Then $\Gamma(q) = 0$. We have $\Gamma(y_1) = f_0$ so $q_0 = y_1$ and $\Delta(q) = \Delta(q_0) = T(c)^{-1}T(c\gamma_1) = T(c)^{-1}$ by condition (c). Also, $f_k = 1$ so $\sum_{j=0}^{e-1} f_{ij}\gamma_j = 1$ and $q_k = 1$.

Lemma 4. *Let $c, \gamma_0, \cdots, \gamma_{e-1}$ satisfy the conditions of Lemma 3. If R, S, and q are as above, then Hypotheses H1, H2, and H3 hold.*

Proof: See Appendix B. □

The sequence generated by an AFSR based on R, x, and S with connection element q is given by $b_i = q_0^{-1}(x^{-i} \pmod q) \pmod x$ which really means

$$\begin{aligned} b_i &= \Delta(q_0)^{-1} \cdot \Delta(\Gamma_S^{-1}(\Gamma(x)^{-i}))) \\ &= \Delta(q_0)^{-1} \cdot \Delta(\Gamma_S^{-1}(r^{-i})) \\ &= T(c) \cdot \Delta(\Gamma_S^{-1}(\alpha^i)), \end{aligned}$$

where Γ_S is the restriction of Γ to S. On the other hand $a_i = T(c\alpha^i)$ so we want to see that

$$T(c\alpha^i) = T(c) \cdot \Delta(\Gamma_S^{-1}(\alpha^i))$$

for every i. The powers of α are precisely the images of the nonzero elements of S under Γ, so it suffices to show that for every $y \in S$ we have

$$T(c\Gamma(y)) = T(c) \cdot \Delta(y). \tag{4}$$

Since T, Γ, and Δ are F_p-linear, it suffices to see that equation (4) holds for y in an F_p-basis for S, such as $\{y_0, y_1, \cdots, y_{e-1}\}$. That is, it suffices to see that $T(c\gamma_i) = T(c)\delta_i$. This holds by the definition of δ_i. This completes the proof of Theorem 4.

6 Rational Approximation

In this section we consider the problem of finding an AFSR over R, r, S that generates a sequence A. This is equivalent [8] to finding $u, q \in R$ such that the $\alpha(A, r) = u/q$, so we define the Rational Approximation Problem for AFSRs over R, r, and S as:

Rational Approximation over R, r, and S
Instance: A prefix of sequence A of elements of S.
Problem: Find elements u and $q \in R$ so that $\alpha(A, r) = u/q$.

We may approach problem with successive *rational approximations*: For each i, find $u_i, q_i \in R$ with $\alpha(A, r) \equiv u_i/q_i \pmod{r^i}$. Such an algorithm *converges* after T steps if $\alpha(A, r) = u_T/q_T$. We measure the quality of the algorithm in terms of the smallest T after which it converges, with the smallest such T expressed as a function of the size of the smallest AFSR that outputs A and we measure the quality in terms of the time complexity expressed as a function of T. In the Berlekamp-Massey algorithm (rational approximation for LFSRs), when the previous approximation fails at the next stage, a new approximation is formed by adding a multiple of a (carefully chosen) earlier approximation. If λ is the size of the smallest LFSR that outputs A, then the algorithm converges in 2λ steps with time complexity $O(T^2)$ [11].

One might try the same approach with AFSRs over more general rings. But if there are carries when approximations are added, then the proof of convergence breaks down. Xu and the author overcame this in a general setting [9]. The key idea is to produce a new approximation that works for several new terms. To make this work, we need an *index function* $\phi : R \to \mathbf{Z} \cup \{-\infty\}$ so that the following holds.:

Property 1. There are non-negative integers $a, b \in \mathbf{Z}$ such that

1. $\phi(0) = -\infty$ and $\phi(z) \geq 0$ if $z \neq 0$;
2. for all $z, y \in R$ we have $\phi(zy) \leq \phi(z) + \phi(y) + a$;
3. for all $z, y \in R$, we have $\phi(z \pm y) \leq \max\{\phi(z), \phi(y)\} + b$; and
4. for all $z \in R$ and $n \geq 0 \in Z$, we have $\phi(r^n z) = n + \phi(z)$.

We define $-\infty + c = -\infty$ for every integer c. Let $n_\phi = \max\{\phi(z) : z \in S\} \cup \{\phi(1)\}$. For a pair $x, y \in R$ we define $\Phi(x, y) = \max(\phi(x), \phi(y))$.

If an AFSR over R and r has connection number $q = \sum_{i=0}^{k} q_i r^i$ with $q_i \in T$ and produces output sequence A with $\alpha = \alpha(A, r) = u/q$, then $\phi(q)$ and $\phi(u)$ are bounded by affine functions of k and $\phi(m)$, where m is the initial memory.

Generally $\phi(m)$ measures the storage needed for m. From this and an expression for u in terms of q and the initial state, we show that $\lambda = \max(\phi(u), \phi(q))$ is at most linear in the size of the AFSR. If we bound the execution time of a rational approximation algorithm in terms of λ, then we will have bounded the execution time in terms of the size of the AFSR. If A is an infinite sequence

of elements of S and λ is the minimal value of $\Phi(u,q)$ over all pairs u,q with $\alpha(A,r)=u/q$, then we say λ is the *r-adic complexity of A.*

We also need a subset P of R so that the following holds.

Property 2. There are $c>d\geq 0\in\mathbf{Z}$ such that

1. if $s\in P$, then r^c does not divide s;
2. if $z,y\in R$, then there exist $s,t\in P$ such that $r^c|sz+ty$; and
3. if $z,y\in R$ and $s,t\in P$, then $\phi(sz+ty)\leq\max\{\phi(z),\phi(y)\}+d$.

We call P an *interpolation set.* Let M_P be the cost of finding s,t in Property 2.2.

Theorem 6. *[9] Let ϕ be an index function and let P be an interpolation set for R and r. Then there is a register synthesis algorithm for AFSRs over R,r,S with time complexity $O(M_PT^2)$ such that if λ is the r-adic complexity of a sequence A, then given a prefix of*

$$T>\frac{2c}{c-d}\lambda+\frac{c(2(a+b)+c+b\lceil\log(c)\rceil+n_\phi)}{c-d}+1\in O(\lambda)$$

symbols of A, the algorithm produces an AFSR that outputs A.

Suppose

$$R=F_{p^h}[x_1,\cdots,x_n]/I=F_{p^h}[\overline{x}]/I$$

and $r\in R$, so that $R/(r)$ is finite. Thus $|R/(r)|=r=p^{hg}$ for some $g\in\mathbf{Z}$. Let S be a set of representatives for R modulo r. We want to construct an index function and interpolation set. Define $\phi(v)=\deg_r(v)$ and $\phi(0)=-\infty$. Then Property 1 holds with $a=\max\{\deg_r(uv):u,v\in S\}$ and $b=0$.

If $a=0$, then our AFSRs are LFSRs, so we assume that $a\geq 1$. Let

$$P=\{\sum_{i=0}^{a}s_ir^i:s_i\in S,s_a\in F_{p^h},(s_0,\cdots,s_a)\neq(0,0)\},$$

$c=2a$, and $d=2a-1$ so $0\leq d<c$. Part 1 of Property 2 is immediate.

If

$$s=\sum_{i=0}^{a}s_ir^i\in P\text{ and }z=\sum_{i=0}^{n}z_ir^i$$

with $z_i\in S$, then $\phi(s_jz_i)\leq a$ and $\phi(s_az_i)\leq 0$, so that $\phi(sz)\leq n+2a-1$. Thus if $s,t\in P$ and $z,y\in R$, then $\phi(sz+ty)\leq\Phi(sz,ty)\leq\Phi(z,y)+2a-1=d.$. Thus part 3 of Property 2 holds.

Next let $z,y\in R$. Let

$$\mu:(P\cup\{(0,0)\})^2\to R/(r^c)$$

be defined by $\mu(s,t)=sz+ty\pmod{r^c}$. Then μ is an F_{p^h}-linear map from a set of cardinality

$$(|P|+1)^2=|S|^{2a}|F_{p^h}|^2=p^{2h(ea+1)}$$

to a set of cardinality

$$|S|^c = p^{2hea}.$$

The former set is larger, so μ has a nontrivial kernel. That is, there exist $s, t \in P$, not both zero, such that r^c divides $sz + ty$. This proves part 2 of Property 2. It follows that we have a rational approximation algorithm in this setting.

Theorem 7. *Let S be a complete set of representatives modulo r satisfying Hypotheses H1 and H2. Let $a = \max\{\deg_r(uv) : u, v \in S\}$. Then there is a register synthesis algorithm for AFSRs over R, r, S with time complexity $O(M_P T^2)$, such that if λ is the r-adic complexity of a sequence A, then the algorithm produces an AFSR that generates the sequence if it is given a prefix of $T > 4a\lambda + 8a^2 + 1 \in O(\lambda)$ symbols of the sequence.*

For cryptography this gives us another security test that stream ciphers must pass. For coding theory this may give us new classes of algebraic geometry codes with efficient decoding algorithms, but this is a subject for future research.

References

1. S. Blackburn: A Note on Sequences with the Shift and Add Property. Designs, Codes, and Crypt. **9** (1996) pp. 251-256.
2. S. Golomb: Shift Register Sequences. Aegean Park Press, Laguna Hills CA (1982).
3. M. Goresky and A. Klapper: Periodicity and Correlations of of d-FCSR Sequences. Designs, Codes, and Crypt. **33** (2004) 123-148.
4. M. Goresky and A. Klapper: Polynomial pseudo-noise sequences based on algebraic feedback shift registers, under review.
5. A. Klapper: Distributional properties of d-FCSR sequences. J. Complexity **20** (2004) 305-317.
6. A. Klapper, Pseudonoise Sequences Based on Algebraic Function Fields, presented at ISIT 2004, Chicago, USA.
7. A. Klapper and M. Goresky: Feedback Shift Registers, Combiners with Memory, and 2-Adic Span. J. Cryptology **10** (1997) 111-147.
8. A. Klapper and J. Xu: Algebraic feedback shift registers, Theoretical Comp. Sci. **226** (1999) 61-93.
9. A. Klapper and J. Xu: Register synthesis for algebraic feedback shift registers based on non-primes. Designs, Codes, and Crypt. **31** (2004) 227-25.
10. R. Lidl and H. Niederreiter: Finite Fields, Encycl. Math. Appl. **20**. Addision Wesley, Reading, MA (1983).
11. J. Massey: Shift-register synthesis and BCH decoding. IEEE Trans. Info. Thy. **IT-15** (1969) 122-127.
12. M. O'Sullivan: Decoding of codes defined by a single point on a curve. IEEE Trans. Info. Thy. **41** (1995) 1709-1719.
13. S. Porter, B.-Z. Shen, and R. Pellikaan: Decoding geometric Goppa codes using an extra place. IEEE Trans. Info. Thy. **38** (1992) 1663-1676.
14. S. Sakata, H. Jensen, and T. Hoholdt: Generalized Berlekamp-Massey decoding of algebraic geometry codes up to half the Feng-Rao bound. IEEE Trans. Info. Thy. **41** (1995) 1762-1768.

A Proof of Lemma 3

Suppose that

$$\frac{z_1(r)}{z_0(r)} \cdot K_T \subseteq K_T + F_p T^{-1}(1).$$

The right hand side equals $K_T + F_p v$ for any element v with $T(v) = 1$. Let $u \in F_{p^e} - F_p$ and define $T'(y) = uT(y)$. Then T' is also F_p-linear and $K_{T'} = K_T$. However

$$\frac{z_1(r)}{z_0(r)} \cdot K_{T'} \not\subseteq K_{T'} + F_p T'^{-1}(1).$$

Now suppose we can show that any sequence $A = a_0, a_1, \cdots$ generated by Blackburn's method using primitive element r^{-1} and linear function T' in fact is an ℓ-sequence, say based on ring R, $x \in R$, and set of representatives S, with connection element $q \in R$, and satisfying Hypotheses H1, H2, and H3. That is, $\sum_{i=0}^{\infty} a_i x^i = z/q$ for some $z \in R$.

Lemma 5. *The sequence $A' = u^{-1}a_0, u^{-1}a_1, \cdots$ is an ℓ-sequence based on R, $x \in R$, S, and connection integer q satisfying Hypotheses H1, H2, and H3.*

Proof: Let $\hat{u} \in S$ reduce to u modulo x. Let $S' = \hat{u}^{-1}S$. Then S' is an F_p-vector space and contains F_p. Thus Hypothesis H1 holds. Hypothesis H2 holds, since any $v \in R$ can be written $v = \hat{u}^{-1}v'$ for some $v \in R$. If moreover $w \in R$, then we can write

$$\hat{u}w = \sum_{i=0}^{t} w_i x^i,$$

with $w_i \in S$ so

$$w = \sum_{i=0}^{t} \hat{u}^{-1} w_i x^i.$$

Since $\sum_{i=0}^{\infty} a_i x^i = z/q$, we also have

$$\sum_{i=0}^{\infty} \hat{u}^{-1} a_i x^i = \frac{\hat{u}^{-1} z}{q}.$$

It follows that A' is an ℓ-sequence. Hypothesis H3 holds by similar reasoning. □

Thus we may assume from here on that

$$\frac{z_1(r)}{z_0(r)} \cdot K_T \not\subseteq K_T + F_p T^{-1}(1). \tag{5}$$

We claim that we can pick $\gamma_1, \gamma_2, \cdots, \gamma_{e-1}$ so that $T(\gamma_1) = 1$, $T(\gamma_1), \cdots, T(\gamma_{e-1})$ are linearly independent over F_p, and

$$\frac{z_1(r)}{z_0(r)} K_T \not\subseteq K_T + \sum_{j=1}^{e-1} F_p \gamma_j. \tag{6}$$

This is possible: To see this, first pick γ_1 arbitrarily so that $T(\gamma_1) = 1$. Then by equation (5) there exists $\kappa \in K_T$ so that $(z_1(r)/z_0(r))\kappa \notin K_T + F_p T^{-1}(1)$. Finally, we can pick $\gamma_2, \cdots, \gamma_{e-1}$ so that

$$T(\frac{z_1(r)}{z_0(r)}\kappa), 1, T(\gamma_2), \cdots, T(\gamma_{e-1})$$

are F_p-linearly independent.

In particular, we have $\kappa \in K_T$ with

$$\frac{z_1(r)}{z_0(r)}\kappa \notin K_T + \sum_{j=1}^{e-1} F_p \gamma_j.$$

Let

$$\gamma_0 = -\sum_{j=1}^{e-1} \frac{z_j(r)}{z_0(r)}\gamma_j.$$

Thus $\sum_{j=0}^{e-1} z_j(r)\gamma_j = 0$.

Suppose that $T(\gamma_0), \cdots, T(\gamma_{e-1})$ are linearly dependent over F_p. Then we have $T(\gamma_0) = \sum_{j=1}^{e-1} b_j T(\gamma_j)$ for some $b_j \in F_p$. Let

$$\gamma'_j = \begin{cases} \gamma_j + \frac{z_j(r)}{z_0(r)}\kappa & \text{if } j = 0 \\ \gamma_j - \kappa & \text{if } j = i \\ \gamma_j & \text{otherwise.} \end{cases}$$

Then $T(\gamma'_1) = 1$, $T(\gamma'_1), \cdots, T(\gamma'_{e-1})$ are linearly independent over F_p, and $\sum_{j=0}^{e-1} z_j(r)\gamma'_j = 0$. Suppose that $T(\gamma'_0), \cdots, T(\gamma'_{e-1})$ are linearly dependent over F_p. Then we have $T(\gamma'_0) = \sum_{j=1}^{e-1} c_j \gamma'_j$ for some $c_j \in F_p$. Since $T(\gamma'_j) = T(\gamma_j)$ for $j \geq 1$, it follows that

$$T(\frac{z_j(r)}{z_0(r)}\kappa) = \sum_{j=1}^{e-1}(c_j - b_j)T(\gamma_j).$$

This contradicts equation (6) and proves the following lemma.

Lemma 6. *There exist $\gamma_0, \gamma_1, \cdots, \gamma_{e-1} \in R$ so that $T(\gamma_1) = 1$, $\sum_{j=0}^{e-1} z_j(r)\gamma_j = 0$, and the images $T(\gamma_0), T(\gamma_1), \cdots, T(\gamma_{e-1})$ are linearly independent over F_p.*

Now let $c = \gamma_0$. For $j = 0, \cdots, e-1$, let $\gamma'_j = c^{-1}\gamma_j$. Then

1. $\sum_{j=0}^{e-1} z_j(r)\gamma'_j = 0$;
2. $\gamma'_0 = 1$;
3. $T(c\gamma'_1) = 1$; and
4. $T(c\gamma'_0), T(c\gamma'_1), \cdots, T(c\gamma'_{e-1})$ are linearly independent over F_p.

This completes the proof of Lemma 3.

B Proof of Lemma 4

That $F_p \subseteq S$ follows from (2), and the closure under addition is immediate from the definition. Thus Hypothesis H1 holds.

We have $\Delta(y_0) = 1$ and $\Gamma(y_0) = 1$, so $y_0 - 1 \in I$. We know from (4) that the set of δ_j spans F_{p^e} over F_p, so every product $\delta_i \delta_j$ can be written uniquely as

$$\delta_i \delta_j = \sum_{\ell=0}^{e-1} v_{ij\ell} \delta_\ell.$$

Therefore

$$y_i y_j - \sum_{\ell=0}^{e-1} v_{ij\ell} y_\ell \in K_\Delta.$$

If

$$y_i y_j - \sum_{\ell=0}^{e-1} v_{ij\ell} y_\ell \in K_\Gamma,$$

then it is in I. Otherwise we have

$$\Gamma(y_i y_j - \sum_{\ell=0}^{e-1} v_{ij\ell} y_\ell) = \alpha^t$$

for some t. Thus

$$y_i y_j - \sum_{\ell=0}^{e-1} v_{ij\ell} y_\ell - x^t \in I.$$

In particular, every element of R can be written as a finite sum $\sum_{i=0}^{s} u_i x^i$ with $u_i \in S$. This implies that every element of $R/(q)$ can be written in this form with $s < k$. Thus $|R/(q)| \leq p^{ek}$. But the image of R in $F_{p^{ek}}$ is all of $F_{p^{ek}}$ and is a quotient of $R/(q)$. Hence $|R/(q)| = p^{ek}$ and $(q) = K_\Gamma$ in R. Thus Hypothesis H2 holds.

Suppose that Hypothesis H3 is false. Then there are distinct elements $u, v \in R$ such that u/q and v/q have periodic x-adic expansions and $u \equiv v \pmod{q}$. Since the termwise difference of two periodic sequences is periodic and corresponds to the difference of the corresponding x-adic elements, we can assume that $u \in R$ with $u = wx^k$. But then the x-adic expansion of u/q is x^k times the x-adic expansion of w/q, hence has k consecutive zeros. But this is false for a punctured de Bruijn sequence. Thus Hypothesis H3 holds.