Fibonacci and Galois Representations of Feedback with Carry Shift Registers

Mark Goresky* Andrew Klapper †

October 27, 2000

Abstract

Feedback with carry shift registers (FCSRs) are a class of finite state devices that are similar to linear feedback shift registers (LFSRs) in their simplicity and statistical randomness, and in that they have algebraic tools for the analysis of their output. In this paper we describe and analyze an alternative architecture for FCSRs that is similar to the Galois architecture for LFSRs. We also explore architectural considerations for d-FCSRs, a natural generalization of FCSRs. Finally, we describe a general framework for algebraically modeling LFSRs, FCSRs, and d-FCSRs in both their Fibonacci and Galois architectures.

1 Introduction

Pseudorandom binary sequences with various statistical properties (such as high linear span, low cross-correlation values, high pairwise Hamming distance) are important in many areas of communications and computing, such as cryptography, spread spectrum communications, error correcting codes, and Monte Carlo integration. Linear feedback shift registers (LFSRs) provide an economical, fast, and efficient method for generating a wide variety of pseudo-random sequences. During the last few years, the feedback-with-carry shift register (FCSR)

*School of Mathematics, Inst. for Adv. Study, Princeton N.J. www.math.ias.edu/~goresky. Research partially supported by N.S.F. grant # 0002693.

†Dept. of Computer Science, University of Kentucky, Lexington, KY, 40506-0046 klapper@cs.uky.edu. Research partially supported by N.S.F. grant # 9980429.

architectures and a simple modification, the d-FCSR architectures, have been investigated as alternative methods for the efficient generation of long pseudorandom binary sequences ([8, 10, 21, 1]). The analysis of FCSR sequences has quite a different flavor from that of LFSR sequences, although they share an incredible list of parallel properties (see [8, 9, 11, 12, 5]). The FCSR circuits described in these papers resemble the "Fibonacci" configuration of the linear feedback shift register. The current paper has three objectives:

1. to develop and analyze the "Galois" configuration architecture for FCSRs and d-FCSRs (cf.[18]);

2. to analyze the output sequences of d-FCSR generators and to give a relatively simple procedure for choosing feedback parameters for a d-FCSR; and

3. following [13], to formalize the notion of a mathematical "model" for a finite state machine with output, and to find such models for LFSR, FCSR, and d-FCSR generators, both in their Fibonacci and Galois configurations.

Even in the case of LFSR's, some of these results appear to be new. We now describe these three points in greater detail.

Galois and Fibonacci configurations. (See Section 2.) Recall that a LFSR in the Fibonacci (Figure 1) configuration has several tapped cells. With each clock cycle, the contents of the tapped cells are added and the sum (modulo 2) is returned to the first cell of the shift register. It is well known that if the corresponding *connection polynomial* is irreducible with degree r and if $\alpha \in \mathbf{F}_{2^r}$ is a root, then the output sequence may be described by

$$a_i = \mathrm{Tr}(\alpha^{-i}) \in \mathbf{F}_2, \tag{1}$$

where Tr is the trace function from $\mathbf{F}2^r$ to $\mathbf{F}_2$. In the Galois representation (Figure 2), with each clock pulse, the output of the last cell is introduced into each of the tapped cells simultaneously, where it is added (modulo 2) to the contents of the preceding cell. Appropriately configured, the same output may be obtained. In Section 2.1 and 2.2 we review the standard facts about these two configurations, including the "power series" method of analysis and the determination of the initial loading of the registers.

In its simplest form (Figure 3), an FCSR consists of a shift register with a small amount of auxiliary memory containing a nonnegative integer. The contents (0 or 1) of the tapped cells are added *as integers* to the current contents of the memory to form a sum σ. The parity bit, σ mod 2 is fed back into the first cell while the higher order bits $\lfloor \sigma/2 \rfloor$ are retained for the new value of the memory. The output is taken from the last cell and (for appropriate choice of feedback connections) the output sequence is given by

$$a_i = 2^{-i} (\bmod\, q) (\bmod\, 2). \tag{2}$$

In Section 2.3 we review the power series analysis of the FCSR in this "Fibonacci" configuration. One might ask whether there is an analogous "Galois" representation for the same FCSR sequences. Such a representation was first discussed in [18]. In Section 2.4 we carry out the power series analysis of the Galois architecture for FCSR sequences. It turns out that the Galois representation is more efficient than the Fibonacci representation since the additions occur simultaneously ("in parallel") and each individual sum involves no more than 3 bits. Moreover the analysis of the initial state is also simpler.

Algebraic Models. (See section 3.) Equations (1) and (2) amount to representations of the actions of certain LFSRs and FCSRs in their Fibonacci configurations by the action of multiplication by a fixed element in a ring. In Section 3 of this paper we formalize this notion as an algebraic model for a finite state automaton, and describe models for general LFSR's and FCSR's, both in their Galois and Fibonacci configurations. (We also describe models for d-FCSR's in Section 4.) In each case we discover the surprising fact that the natural model for the Fibonacci configuration involves a map from the ring to the set of states (that is, an *injective* model), while the model for the Galois configuration is simpler and involves a map from the set of states to the ring (that is, they a *projective* model). Even for the case of LFSR's, the model may be fairly subtle if the connection polynomial is reducible.

d-FCSR sequences. (See Section 4.) There is an enormous collection of variations on the basic FCSR architecture which have also been analyzed to varying degrees ([7, 8, 10, 13, 14, 15]). Perhaps the simplest of these variations is the d-FCSR (Figure 5), in which the feedback bit is computed but is delayed for $d-1$ clock cycles before being fed back. This architecture also has a "Galois" representation which we describe (Figure 10) and for which we also construct models (see below). In this paper we show how to configure these circuits so as to output pseudorandom sequences of the form $k^i (\bmod q) (\bmod 2)$ with choices for k other than $k = 2^{-1}$. It is surprising that such complex feedback mechanisms can be analyzed at all, especially considering the tremendous but largely unsuccessful effort which has been directed toward the analysis of "nonlinear" feedback shift registers over the last thirty years.

Throughout this paper, $\mathbf{Z}$ denotes the integers; $\mathbf{Q}$ denotes the rational numbers, and $\mathbf{F}_q$ denotes the Galois field with q elements.

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

2 Architectures

In this section we describe the architecture of LFSRs and FCSRs. In each case we describe both Fibonacci and Galois architectures. Although this material on linear feedback shift registers is classical [3] and well known [22], it is repeated here so as to motivate the analysis of the FCSR and d-FCSR architectures. For the purposes of this article, the contents a_i of each cell is a *bit* ($a_i \in \mathbf{F}_2$), as are the multipliers q_i, although exactly the same analysis holds when a_i, q_j are considered to be elements of some finite field. (For this reason, we do not automatically convert all -1's to $+1$'s.)

2.1 LFSRs: Fibonacci Architecture

Let us recall some standard facts concerning the Fibonacci representation LFSRs [3].

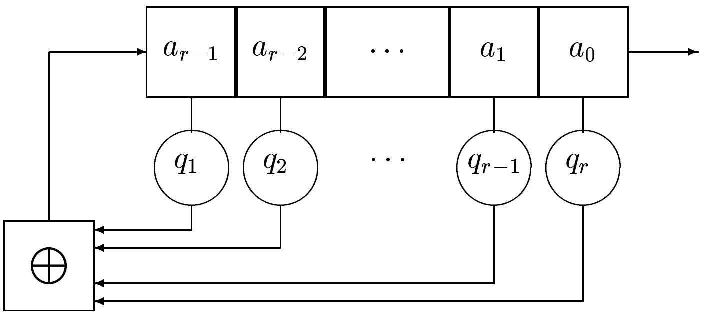

Figure 1: Fibonacci LFSR.

The register is initially loaded with bits $a_0, a_1, \ldots, a_{r-1}$. With each clock cycle these bits are added (modulo 2) with weights given by the multipliers q_i and the resulting bit

$$a_r = \sum_{i=0}^{r-1} q_{r-i} a_i \pmod 2 \tag{3}$$

is fed back into the first cell. This equation is evidently a *linear recurrence* over the field $\mathbf{F}_2$. (See [16] §7 p. 454. The "Fibonacci" designation refers to the fact that the famous Fibonacci series $1, 1, 2, 3, 5, 8, \ldots$ is generated by a similar linear recurrence $a_r = a_{r-1} + a_{r-2}$ over the integers.)

To each LFSR of length r, one associates the *connection polynomial*

$$q(X) = q_r X^r + q_{r-1} X^{r-1} + \cdots + q_1 X - 1$$

where $q_1, q_2, \ldots, q_r$ correspond to the r taps on its cells. Some authors consider instead the polynomial

$$b(X) = -X^r q(\frac{1}{X}) = X^r - q_1 X^{r-1} - \cdots - q_{r-1}X - q_r$$

Then α is a root of $q(X)$ if and only if α^{-1} is a root of $b(X)$.

There are (at least) three different approaches to the analysis of the output sequence: the power series method, which is described in the next paragraph, and the Galois field and the ring-theoretic models, described in Section 3.1.

Power series method. Any infinite binary sequence $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ may be identified with its generating function $A(X) = \sum_{i=0}^{\infty} a_i X^i$ which is an element of the ring $\mathbf{F}_2[[X]]$ of formal power series with coefficients in the integers modulo 2. It is well known (and follows directly from the formula for the sum of a geometric series) that the sequence $\mathbf{a}$ is eventually periodic if and only if its generating function is equal to the quotient of two polynomials,

$$A(X) = \frac{h(X)}{q(X)} \in \mathbf{F}_2[[X]]$$

and it is strictly periodic if and only if $\deg(h(X)) < \deg(q(X))$. In this case, the denominator $q(X)$ is the connection polynomial for a LFSR which generates the sequence $\mathbf{a}$. The numerator $h(X)$ corresponds to the initial loading; they are related by

$$h(X) = \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} X^k \tag{4}$$

where $q_0 = 1$ and where $a_0, a_1, \ldots, a_{r-1}$ denotes the initial contents of the cells (cf. [3] §2.5 p.30, or [16] thm. 8.40, p. 416).

2.2 LFSRs: Galois Architecture

In the Galois representation (Figure 2), with each clock cycle the output of the last cell is introduced into each of the tapped cells simultaneously, where it is added (modulo 2) to the contents of the preceding cell.

Let $q_1, q_2, \ldots, q_r$ denote the feedback multipliers. The recurrence equations are then given by

$$\begin{aligned} a'_i &= a_{i+1} + q_{i+1} a_0 \quad \text{for} \quad 0 \le i \le r-2 \\ a'_{r-1} &= q_r a_0. \end{aligned}$$

As above, form the connection polynomial $q(X) = -1 + \sum_{i=1}^{r} q_i X^i$.

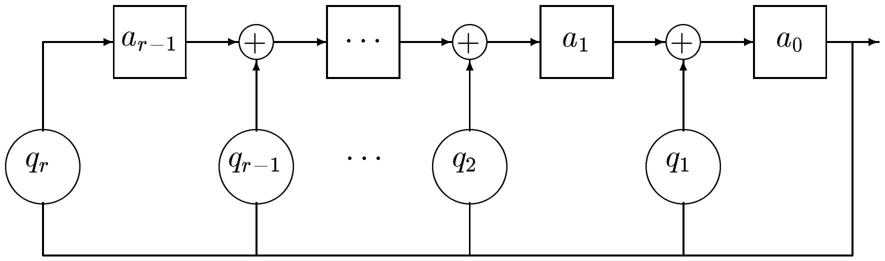

Figure 2: Galois LFSR.

The same three methods may be used to analyze the Galois configuration: the power series method (described in the next paragraph), the Galois field model, and the ring theoretic model (described in Section 3.2. However, there is a difference: in the Fibonacci representation the model is injective (cf §1) while in the Galois representation the model is projective. (See Theorems 3.1 and 3.2 of Section 3). Moreover, Formula (5) for the initial loading is considerably simpler than is formula (4) for the Fibonacci configuration.

Power series method. Suppose $\mathbf{b} = (b_0, b_1, b_2, \ldots)$ is a strictly periodic (infinite) binary sequence, so its generating function $B(X) = \sum b_i X^i$ is the quotient of two polynomials, $B(X) = -h(X)/q(X)$ with $\deg(h) < \deg(q)$.

Theorem 2.1 *The denominator $q(X)$ is the connection polynomial for a (Galois)-LFSR which generates the sequence $\mathbf{b}$. The numerator $-h(X)$ determines (and is determined by) the initial loading $a_0, a_1, \ldots, a_{r-1}$; they are related by*

$$h(X) = a_0 + a_1 X + \cdots + a_{r-1} X^{r-1} \tag{5}$$

Proof: We briefly indicate how to prove this well-known result because a similar method will be needed when we consider the Galois FCSR and the Galois d-FCSR architectures. First observe that for *any* loading $(a_0, a_1, \ldots, a_{r-1})$ of the shift register, the first output bit b_0 equals the first coefficient a_0 in the power series expansion of $-h(X)/q(X)$ (where $h(X) = \sum_{i=0}^{r-1} a_i X^i$). In particular $qB + h$ has no constant term so it is divisible by X. Now run the shift register by one cycle to obtain a new loading $a_0', a_1', \ldots, a_{r-1}'$ (5), a new function $h'(X) = \sum_{i=0}^{r-1} a_i' X^i$ and a new generating function $B'(X) = \sum_{i=0}^{\infty} b_i' X^i$ for the output sequence. (So $b_i' = b_{i+1}$.) By direct computation, $XB' = (B - b_0)$ and $Xh' = (h + a_0 q)$. Hence $X(qB' + h') = qB + h$. By the above observation, the constant term of $qB' + h'$ vanishes as well, which is to say, $qB + h$ is divisible by X^2. By induction we find that $X^n(qB^{(n)} + h^{(n)}) = qB + h$, and so $qB + h$ is divisible by X^n for all n, which is to say, it equals 0. Hence $B(X) = -h(X)/q(X)$. $\square$

2.3 FCSRs: Fibonacci Architecture

In the FCSR architecture (Figure 3), introduced in [8], the basic shift register is provided with a small amount of auxiliary memory m which is a nonnegative integer. The contents (0 or 1) of the tapped cells are added *as integers* to the current contents of the memory to form an integer sum σ. The parity bit $\sigma \mod 2$ is fed back into the first cell of the shift register while the higher order bits $\lfloor \sigma/2 \rfloor$ are retained for the new value of the memory. So the new values $(a'_0, a'_1, \ldots, a'_{r-1}; m')$ are related to the old values $(a_0, a_1, \ldots, a_{r-1}; m)$ by

$$\begin{aligned} a'_i &= a_{i+1} \text{ for } 0 \le i \le r-2 \\ 2m' + a'_r &= m + \sum_{i=1}^{r} q_i a_{r-i}. \end{aligned}$$

It was shown in [8] (and can be seen from the above equations) that, for any initial non-negative memory value m, the memory will decrease exponentially until it lies within the range $0 \le m \le \mathrm{wt}(q+1)$ and will remain in that range forever after. (Here, $\mathrm{wt}(x)$ denotes the number of 1's in the binary expansion of the nonnegative integer x.) Therefore memory overflow will never occur provided the FCSR is equipped with at least $1 + \lfloor \log_2(wt(q+1)) \rfloor$ memory bits.

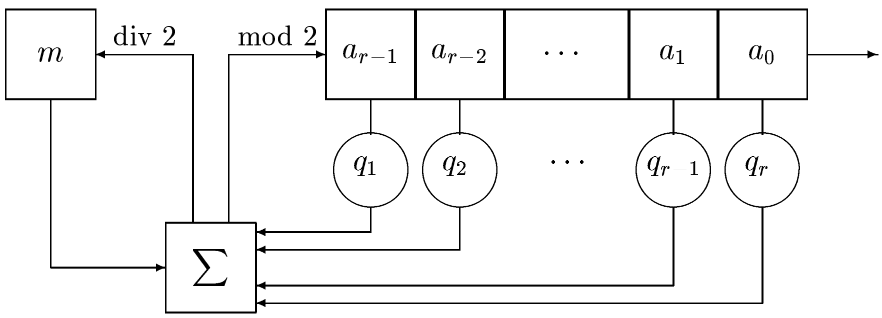

Figure 3: Fibonacci FCSR.

To each FCSR one can associate a *connection integer*

$$q = q_r 2^r + q_{r-1} 2^{r-1} + \cdots + q_1 2 - 1 \in \mathbf{Z}.$$

To any infinite binary sequence $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ one may associate the formal power series

$$\alpha = \sum_{i=0}^{\infty} a_i 2^i. \tag{6}$$

The set of all such power series forms a ring under the obvious operations of addition and multiplication; this is the ring $\mathbf{Z}_2$ of *2-adic integers* (an elementary review of which is provided in [8]). The ring $\mathbf{Z}_2$ contains all fractions $\alpha = m/n$ with $m, n \in \mathbf{Z}$, provided that n is odd. The following (number-theoretic) lemma characterizes those 2-adic numbers which are rational numbers. Although it is elementary and well-known, it is basic to the study of FCSR's so we provide a short proof (cf. [8] thm 2.1, thm. 6.1, [13], [20] thm. 15.5 p. 458).

Lemma 2.2 *The sequence* $\mathbf{a}$ *is eventually periodic if and only if its 2-adic integer* α *is a rational number, in which case it can be expressed as such with an odd denominator. The sequence is strictly periodic if and only if there exist nonnegative integers* h *and* q*, with* q *odd and* $0 \le h \le q-1$ *such that* $\alpha = -h/q$*. In this case the period of the sequence* $\mathbf{a}$ *divides* $\phi(q)$ *(the number of positive integers between 1 and* q *which are relatively prime to* q*) and its i-th term is*

$$a_i = 2^{-i}h \pmod{q} \pmod{2} \tag{7}$$

The reverse of this sequence is the binary expansion of the fraction h/q*.*

Here, 2^{-i} denotes the inverse of 2 in $\mathbf{Z}/(q)$, and $x \pmod{q} \pmod{2}$ means that first the number $x \in \mathbf{Z}/(q)$ is represented by an integer between 0 and $q-1$, then this integer is reduced modulo 2.

Proof. The statement about eventually periodic sequences follows from the statements about strictly periodic sequences, so suppose $\mathbf{a}$ is strictly periodic of some period, T. Let $b = \sum_{i=0}^{T-1} a_i$ be the sum of the first T terms. Then

$$\alpha = b + 2^T b + 2^{2T} b + \cdots = \frac{-b}{2^T - 1}$$

which is a rational number with $0 \le \alpha < 1$. Every factor of $2^T - 1$ is odd, so if this fraction is reduced to its lowest terms we find $\alpha = -h/q$ with q odd and $0 \le h \le q-1$. Conversely suppose that $\alpha = -h/q$ with $0 \le h \le q-1$. Euler's function $\phi(q)$ is the number of integers x relatively prime to q with $1 \le x \le q-1$. Recall that q divides $2^{\phi(q)} - 1$ by Euler's theorem. (The multiplicative group of invertible elements in $\mathbf{Z}/(q)$ has order $\phi(q)$, so any invertible element raised to this power is equal to $1 \pmod{q}$.) Set $B = (2^{\phi(q)} - 1)/q$ so that

$$\alpha = \frac{-h}{q} = -\frac{Bh}{2^{\phi(q)} - 1} = Bh + Bh2^{\phi(q)} + Bh2^{2\phi(q)} + \cdots. \tag{8}$$

But $0 \le h < q$ so $0 \le Bh < 2^{\phi(q)} - 1$ hence the binary expansion of Bh has no more than $\phi(q) - 1$ bits, so these binary expansions do not mix in the above expression. This shows that $-h/q$ has a 2-adic expansion whose coefficient sequence $\mathbf{a}$ is strictly periodic of period $\phi(q)$, although this is not necessarily the minimal period. It follows that the minimal period of the sequence **a** divides $\phi(q)$. Now we verify equation (7). Let $\alpha' = \sum_{i=0}^{\infty} a_{i+1}2^i$ be the 2-adic number which corresponds to the strictly periodic sequence obtained from **a** by throwing away the first term. Then $\alpha' = (\alpha - a_0)/2$ or $-h - qa_0 = 2q\alpha'$, a statement which holds in $\mathbf{Z_2}$ but for which the left hand side is an integer. Hence $h + qa_0$ is even, or, since q is odd,

$$a_0 = h \pmod 2.$$

Therefore

$$\alpha' = -\frac{(h + qa_0)/2}{q} = -h'/q$$

is a rational number with the same denominator q and with numerator $h' = 2^{-1}(h + qa_0)$. Reading this equation modulo q gives $h' = 2^{-1}h \pmod q$. This shows that the sequence of numerators is given by $h, 2^{-1}h, 2^{-2}h, \ldots \pmod q$ and the output sequence is obtained by first realizing these numerators as integers between 0 and q, then reducing modulo 2, which verifies equation (7). The last statement can be verified by direct computation using (8). This completes the proof of Lemma 2.2. □

Caution: The mapping $\mathbf{Z}/(q) \to \mathbf{Z}/(2)$ (given by $z \mapsto z \pmod 2$) is *not* a ring homomorphism, and depends on the particular choice of a complete set M of representatives $\{0, 1, 2, \ldots, p-1\} \subset \mathbf{Z}$ for the elements of $\mathbf{Z}/(p)$. These representatives were chosen because they have the property that for each $h \in M$, the 2-adic expansion of the fraction $-h/q$ is strictly periodic.

The first statement in the following analog of the "power series method" follows immediately from Lemma 2.2. The identification of the numerator h is proven in [8].

Theorem 2.3 *Let* $\mathbf{a} = a_0, a_1, \ldots$ *be a strictly period binary sequence. Let* $\alpha = \sum a_i 2^i$ *be the corresponding 2-adic number, say,* $\alpha = -h/q$ *with* $h, q \in \mathbf{Z}$ *and* $0 \le h \le q-1$. *Write* $q = \sum_{i=0}^{r} q_i 2^i$ *with* $q_i \in \{0,1\}$ *for* $i > 0$ *and* $q_0 = -1$. *Then* q *is the connection integer for a (Fibonacci) FCSR which generates this sequence. The numerator* h *corresponds to the initial loading* $(a_0, a_1, \ldots, a_r)$ *of the register contents and initial memory* m *according to the following equation:*

$$h = m2^r - \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} 2^k \in \mathbf{Z}. \tag{9}$$

(It follows that the full sequence may then be described by $a_j = 2^{-j} \pmod q \pmod 2$.)

2.4 FCSRs: Galois Architecture

The Galois representation [18] for an FCSR is illustrated in the Figure 4.

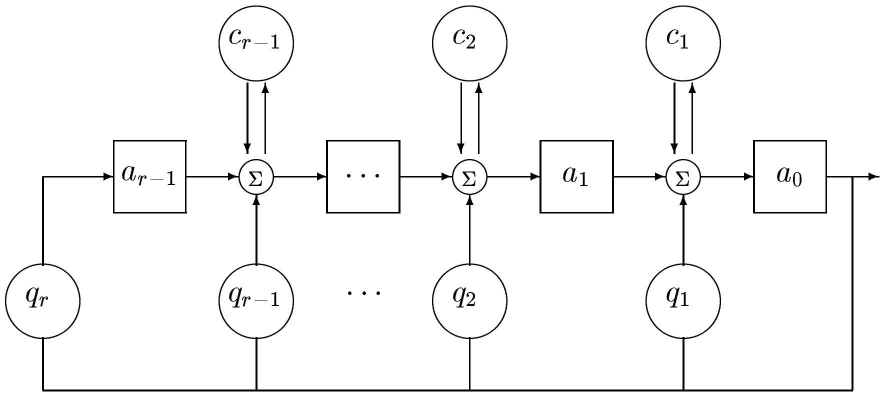

Figure 4: Galois FCSR.

Here, the bits $q_1, q_2, \ldots, q_r$ are multipliers. The cells denoted $c_1, c_2, \ldots, c_{r-1}$ are the memory (or "carry") bits. The Σ sign represents a full adder. At the j-th adder, the following input bits are received :

- a_j from the preceding cell
- $a_0 q_j$ from the feedback line
- c_j from the memory cell,

which are added to form a sum σ_j (with $1 \leq j \leq r-1$). At the next clock cycle, this sum modulo 2 is passed on to the next cell in the register,

$$a'_{j-1} = \sigma_j \bmod 2,$$

and the higher order bit is used to replace the memory,

$$c'_j = \sigma_j \text{ div } 2.$$

In other words, the new values a'_{j-1} and c'_j are given by

$$\begin{aligned} 2c'_j + a'_{j-1} &= a_0 q_j + a_j + c_j \quad \text{for} \quad 1 \leq j \leq r-1 \\ a'_{r-1} &= q_r a_0. \end{aligned} \tag{10}$$

To analyze the behavior of this circuit as before we define the *connection integer*

$$q = -1 + q_1 2 + q_2 2^2 + \cdots + q_r 2^r. \tag{11}$$

The following result is an analog of the power series method.

Theorem 2.4 *Suppose an r-stage (Galois)-FCSR with connection integer q is initially loaded with register and memory contents $(a_0, a_1, \ldots, a_{r-1})$ and $(c_1, c_2, \ldots, c_{r-1})$ respectively. Set*

$$h = a_0 + (a_1 + c_1)2 + \cdots + (a_{r-1} + c_{r-1})2^{r-1}. \tag{12}$$

Then the output sequence $b_0, b_1, b_2 \ldots$ of the FCSR is the coefficient sequence for the 2-adic expansion of the rational number $\alpha = -h/q$.

Proof: The proof is similar to that in the Galois-LFSR case. Given h and q as above, let $B = \sum_{i=0}^{\infty} b_i 2^i$ denote the 2-adic integer which is represented by the output sequence. First we claim that $qB + h \in \mathbf{Z}_2$ is divisible by 2 (meaning that it has no constant term). In fact,

$$\begin{aligned} qB &= (-1 + q_1 2 + q_2 2^2 + \cdots)(b_0 + b_1 2 + b_2 2^2 + \cdots) \\ &= -b_0 + 2(-b_1 + q_1 b_0) + \cdots \end{aligned}$$

The constant term in $qB + h$ is $-b_0 + a_0 (\bmod 2)$. However a_0 is also the first output bit, that is, $a_0 = b_0$, which verifies the claim.

Now run the shift register one step obtaining a new loading $(a'_0, \ldots, a'_{r-1}; c'_1, \ldots, c'_{r-1})$ given by (10). Let $B' = \sum_{i=0}^{\infty} b'_i 2^i$ denote the new 2-adic number represented by the output sequence of this new state; so $b'_i = b_{i+1}$. Define $h' = \sum_{i=0}^{r-1} (a'_i + c'_i) 2^i$ (writing $c'_0 = 0$ for convenience) and calculate that $2B' = B - b_0$ and $2h' = h + a_0 q$. Hence

$$2(qB' + h') = qB + h.$$

By the above claim, the constant term of $qB' + h'$ vanishes as well, which is to say that $qB + h$ is divisible by 2^2. By induction we find that $2^n(qB^{(n)} + h^{(n)}) = qB + h$, and so $qB + h$ is divisible by 2^n for all n, which is to say that it equals 0. □

3 Algebraic Models

Let M be a finite state machine with output whose state change function is denoted F. For simplicity we assume the possible output values are 0 and 1. We say that a state of M is *periodic* if the machine eventually returns to this state after finitely many iterations. This implies that the output from M starting from this state is strictly periodic. Following [13] we define a *model* for M to be a representation of M by an algebraic ring R. In such a representation, states correspond to elements of R and the state change operation corresponds to multiplication by a fixed element of R. Sometimes R represents only a subset of the states, and sometimes several states correspond to the same element of R. More specifically, we say a set of periodic states L is *closed* if it is closed under state change. It is *complete* if it consists of all the periodic states. A model consists of

1. a ring R together with an element $\beta \in R$ and a mapping $T : R \to \{0, 1\}$,

2. a function between R and a closed set L of periodic states of M so that

3. the state change on L is given by $x \mapsto \beta x$ and

4. the output is given by $T(x)$.

Hence, for a given initial state, the output sequence of the machine is given by

$$a_i = T(\beta^i x).$$

Sometimes the function in (2) above is a mapping $S : R \to L \subseteq \{\text{periodic states of } M\}$. Condition (3) then says that for all $x \in R$ we have $S(\beta x) = F(S(x))$. If this is the case and S is one to one, we say the model is an *injective* model. If moreover L is complete and S is onto, then we say the model is a *complete injective model.*

In other cases the function is a mapping $E : L \to R$. Condition (3) then says that for all $x \in L$ we have $E(F(x)) = \beta E(x)$. If this is the case and E is onto, we say the model is a *projective* model. If moreover L is complete and E is one to one, then we say the model is a *complete projective model.*

For complete models, an inverse mapping can be described. However, it may require a nontrivial amount of computation to do so, particularly when attempting to describe the initial state of the machine, cf. (4), (5), (9), (12).

The notion of models can be used to connect what are intuitively different architectures for the "same" type of register. We construct a projective model for one architecture and an injective model for a second architecture, using the same ring R and the same state change element β. The composition of the models then connects the operation of the two architectures and makes precise the relationship between the two.

3.1 LFSRs: Fibonacci Architecture

The Fibonacci architecture for LFSRs has traditionally been analyzed using representations of sequences by powers of elements in Galois fields. This works very well when the connection polynomial is irreducible and moderately well when it is a product of distinct irreducible polyomials. In general, however, such representations become quite complicated. In this subsection we first see that in the first two cases such representations fit into our notion of model. We then see that, using injective models based on more general rings, we obtain very simple representations of arbitrary LFSR sequences by powers of elements.

Galois field model. Suppose for the moment that the connection polynomial $q(X)$ has degree r (that is, $q_r \neq 0$), and is irreducible. Then its roots all lie in the Galois field $\mathbf{F}_{2^r}$. Fix any surjective $\mathbf{F}_2$-linear mapping $T : \mathbf{F}_{2^r} \to \mathbf{F}_2$. (The usual choice is the trace, $Tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{r-1}}$, but any linear mapping will do.) Choose a single root $\alpha \in \mathbf{F}_{2^r}$ of the connection polynomial $q(X)$. To each $z \in \mathbf{F}_{2^r}$ associate the following state $S(z)$ of the LFSR:

$T(\alpha^{1-r}z)$	$T(\alpha^{2-r}z)$	$\cdots$	$T(\alpha^{-1}z)$	$T(z)$

Theorem 3.1 *Every state of the LFSR is periodic. The ring $R = \mathbf{F}_{2^r}$, the function $T : \mathbf{F}_{2^r} \to \mathbf{Z}/(2)$, and the mapping $S : \mathbf{F}_{2^r} \to \{$periodic states$\}$ constitute a complete injective model for the operation of the LFSR. The state change is given by $z \mapsto \alpha^{-1}z$. The output sequence is given by $a_j = T(\alpha^{-j}z)$.*

Proof: The proof is standard (and elementary): α^{-1} is a root of $b(X)$ so $\alpha^{-r} = \sum_{i=1}^{r} q_i \alpha^{i-r}$. The injectivity and completeness follows from the fact that $\{1, \alpha^{-1}, \cdots, \alpha^{1-r}\}$ is a basis for $\mathbf{F}_{2^r}$ over $\mathbf{F}_2$. □

It is also possible to construct a projective model for the LFSR, namely $E = S^{-1} : \{\text{states}\} \to \mathbf{F}_{2^r}$. This mapping associates to each state of the LFSR an element $z \in \mathbf{F}_{2^r}$ of the finite field and the change of state is given by $z \mapsto \alpha^{-1}z$. This may be accomplished under our assumption that $q(X)$ is irreducible because the elements $\{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\}$ are linearly independent over $\mathbf{F}_2$, so the equations $T(z\alpha^i) = a_i$ $(0 \le i \le r-1)$ may be solved uniquely for $z \in \mathbf{F}_{2^r}$. However, solving for z involves some nontrivial computation which is equivalent to inverting a matrix or finding a dual basis for $\mathbf{F}_{2^r}$.

Next, suppose that $q(X) = g_1(X)g_2(X)\cdots g_m(X)$ is a product of irreducible factors $g_i(X)$ of degree d_i, with no factor repeated, and that $q(x)$ has degree r. The mapping S is no longer a one to one correspondence: it becomes necessary to change the definition of the ring R. The roots of $g_i(X)$ lie in the Galois field $\mathbf{F}_{2^{d_i}}$. Let $R = \mathbf{F}_{2^{d_1}} \times \mathbf{F}_{2^{d_2}} \times \cdots \times \mathbf{F}_{2^{d_m}}$ be the product ring with addition and multiplication defined coordinate-wise. (It is *not* a field.) A choice $\alpha_i \in \mathbf{F}_{2^{d_i}}$ of root of each $g_i(X)$ determines an element $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in R$. This element is invertible and its inverse is $\alpha^{-1} = (\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_m^{-1})$. A choice of surjective linear mapping $T_i : \mathbf{F}_{2^{d_i}} \to \mathbf{F}_2$ determines a linear mapping $T : R \to \mathbf{F}_2$ by $T(a_1, a_2, \ldots, a_m) = \sum T_i(a_i)$. To each element $z = (z_1, z_2, \ldots, z_m) \in R$ we may associate a state $S(z)$ of the shift register,

$T(\alpha^{1-r}z)$	$T(\alpha^{2-r}z)$	$\cdots$	$T(\alpha^{-1}z)$	$T(z)$

Then, as in Theorem 3.1 above, every state is periodic and this mapping $S : R \to \{\text{states}\}$ is a complete injective model. The change of state is given by the mapping $z \mapsto \alpha^{-1}z$. In summary, each output sequence of the shift register may be expressed as the well-known linear combination (cf. [16] thm. 8.21 p. 404),

$$a_i = T(\alpha^{-i}z) = \sum_{j=1}^{m} T_j(\alpha_j^{-i}z_j). \tag{13}$$

If the connection polynomial $q(X)$ has repeated factors, then the situation is more complicated (see [6], [16] §8.23 p. 405, or [22] §5.3.3, §5.5.3). In the next subsection we follow [13] and display a model for the action of the shift register which holds for any connection polynomial $q(X)$. This model is implicit in [20] §7.3 and in [19].

Ring-theoretic model. Let $\mathbf{F}_2[X]$ be the ring of polynomials in X with $0, 1$ coefficients. Let us denote the mapping $\mathbf{F}_2[X] \to \mathbf{F}_2$ which assigns to each polynomial its constant term by $z \mapsto z \pmod X$. It is a homomorphism of rings. The connection polynomial $q(X) = -1 + q_1X + q_2X^2 + \cdots + q_rX^r$ generates an ideal (q) in this ring, and we consider the quotient,

$$R = \mathbf{F}_2[X]/(q).$$

We assume $q_r \neq 0$ so that, in this ring,

$$X^r = \frac{1}{q_r}(1 - q_1X - \cdots - q_{r-1}X^{r-1}) = 1 + q_1X + \cdots + q_{r-1}X^{r-1}.$$

It follows that any element $z \in R$ in this quotient may be uniquely represented as a polynomial $z(X) = z_0 + z_1X + \cdots + z_{r-1}X^{r-1}$ of degree less than r, and for any such $z \in R$ we will denote its constant term by $z_0 = z \pmod X \in \mathbf{F}_2$. We define the mapping $T : R \to \mathbf{F}_2$ by $T(z) = z_0$ ($T(z) = z \pmod X$).

Caution: As in Section 2.3, the mapping T is *not* a ring homomorphism. For example, $T(x \cdot x^{r-1}) = T(x^r) = 1$, whereras $T(x)T(x^{r-1}) = 0 \cdot 0 = 0$. Its definition depends on the fact that we have first chosen a complete set of representatives in $\mathbf{F}_2[X]$ for the elements of R, consisting of polynomials of degree $< r$. There are many other possible choices for a complete set of representatives, which may give different mappings $R \to \mathbf{F}_2$.

Since $1 = q_1X + \cdots + q_rX^r \pmod q$ we see that X is invertible in R with

$$X^{-1} = q_1 + q_2X + \cdots + q_rX^{r-1} \tag{14}$$

and that

$$X^{-r} = q_1X^{-(r-1)} + q_2X^{-(r-2)} + \cdots + q_rX^0$$

For any $z \in R$ we may associate the following state $S(z)$ of the shift register,

$X^{-r+1}z\ (q)(X)$	$\cdots$	$X^{-1}z\ (q)(X)$	$z\ (q)(X)$

where $(q)(X)$ denotes $(\bmod q)(\bmod X)$. The following is a special case of results in [13].

Theorem 3.2 *Every state of the LFSR is periodic. The association S between elements of R and states of the shift register is a one-to-one correspondence (whether or not $q(X)$ is irreducible). The change of state is given by $z \mapsto X^{-1}z$. The collection $\{R, S, T\}$ is a complete injective model for the LFSR. The output sequences of the LFSR may be described by the sequence $a_i = T(X^{-i}z(X)) = X^{-i}z(X) \pmod q \pmod X$.*

Proof. The association $S : R \to \{\text{States}\}$ may be regarded as a map $R \to \mathbf{F}_2^r$, in which case it is linear (over $\mathbf{F}_2$). We show this mapping is one-to-one. Suppose $z = z_0 + z_1X + \cdots + z_{r-1}X^{r-1}$ maps to the zero state. Then $z_0 = z \pmod X = 0$ so the constant term is zero. Therefore z is divisible by X, and $X^{-1}z = z_1 + z_2X + \cdots + z_{r-1}X^{r-2}$ and this is therefore the representation of $X^{-1}z \pmod q$. But $X^{-1}z \pmod q \pmod X = 0$ so $z_1 = 0$. Continuing in this way we conclude that $z = 0$. Since R is a vector space of dimension r (over $\mathbf{F}_2$), this shows that the above association is a one-to-one correspondence.

Next, consider the change of state. Fix $z \in R$ and consider the associated state of the shift register, as described above. Then the element $X^{-1}z$ is associated to the state with all cell contents shifted to the right by one step, except for the leftmost cell which contains $X^{-r}z = q_1X^{-(r-1)}z + q_2X^{-(r-2)}z + \cdots + q_rX^0z$. But this is the appropriate linear combination of the old contents of the cells.

The completeness is immediate from the fact that S is one-to-one. $\square$

If q is irreducible then the ring $R = \mathbf{F}_2[X]/(q)$ is a field, isomorphic to $\mathbf{F}_{2^r}$, from which one may recover Theorem 3.1. If q is reducible, say $q(X) = g_1(X)^{e_1}g_2(X)^{e_2}\cdots g_m(X)^{e_m}$ is its decomposition into irreducible factors, then R is isomorphic to the product $R_1R_2\cdots R_m$ with $R_i = \mathbf{F}_2[X]/(g_i^{e_i})$. If all the $e_i = 1$ then each $R_i \cong \mathbf{F}_{2^{\deg(g_i)}}$, from which one may recover equation (13).

3.2 LFSRs: Galois Architecture

In this subsection we construct models for the Galois architecture for LFSRs. As with the Fibonacci architecture, the classical analysis can be seen as based on models where R is a Galois field, but we obtain a simple model in the general case by using more general rings. In the Galois architecture case the models are projective.

Galois field model. Let us suppose that $q(X)$ has degree r and is irreducible. Let α be a root of $q(X)$ in the Galois field $\mathbf{F}_{2^r}$. Define a mapping $E : \{\text{states}\} \to \mathbf{F}_{2^r}$ which associates to any state

a_{r-1}	a_{r-2}	$\cdots$	a_1	a_0

the following element

$$z = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{r-1}\alpha^{r-1} \in \mathbf{F}_{2^m}. \tag{15}$$

Define the linear mapping $T : \mathbf{F}_{2^r} \to \mathbf{F}_2$ by $T(\sum_{i=0}^{r-1} b_i\alpha^i) = b_0$. Then we have the following analogue of Theorem 3.1.

Theorem 3.3 *Every state of the shift register is periodic. The collection* $\{R = \mathbf{F}_{2^r}, E, T\}$ *is a complete projective model for the LFSR in its Galois configuration. The state change is given by* $z \mapsto \alpha^{-1}z$.

Proof: The completeness follows from the facts that E is $\mathbf{F}_2$-linear and that the minimal polynomial of α has degree r. □

Combining this with Theorem 3.2, we have the following.

Corollary 3.4 *There is a one to one correspondence between periodic states of the Galois LFSR with connection polynomial* $q(x)$ *and periodic states of the Fibonacci LFSR with connection polynomial* $q(x)$ *so that corresponding states produce the same output.*

This particular model was chosen to make the mapping E as simple as possible. One could just as easily construct a model in which the mapping T is simple. In fact, given any surjective linear mapping $T' : \mathbf{F}_{2^r} \to \mathbf{F}_2$ define $E' : \{\text{states}\} \to \mathbf{F}_{2^r}$ by

$$E'(s) = CE(s) = C(\sum_{i=0}^{r-1} s_i\alpha^i)$$

where $s = (a_{r-1}, \ldots, a_1, a_0)$ denotes the above state and where $C \in \mathbf{F}_{2^r}$ is the unique element such that $T(x) = T'(Cx)$ for all $x \in \mathbf{F}_{2^r}$. Then the collection $\{R = \mathbf{F}_{2^r}, E', T'\}$ constitutes a projective model for the Galois-LFSR.

If $q(X)$ is reducible, one may still choose a root α and construct the mapping (15) however it will fail to be one to one. In particular, the contents a_0 of the output cell may not be uniquely determined by z. If $q(X) = h_1(X)h_2(X)\cdots h_m(X)$ is a product of irreducible factors with no repeated factors then, as in §3.1 define $R = \mathbf{F}_{2^{d_1}} \times \cdots \times \mathbf{F}_{2^{d_m}}$ where $d_j = \deg(h_j)$. Choose roots $\alpha_j \in \mathbf{F}_{2^{d_j}}$ of $h_j(X)$. Define $T : R \to \mathbf{F}_{2^r}$ by $T(z_1, z_2, \ldots, z_m) = \sum_{i=1}^{m} T_i(z_i)$ where

$$T_i(\sum_{j=0}^{d_i} b_{ij}\alpha_i^j) = b_{i0}.$$

Corresponding to the state $(a_{r-1}, a_{r-2}, \ldots, a_1, a_0)$ of the shift register, we may associate the element $z = (z_1, z_2, \ldots, z_m) \in R$ given by

$$z_j = \sum_{i=o}^{r-1} a_i \alpha_j^i$$

that is, $z = \sum_{j=1}^{r-1} a_j \alpha^j$ where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in R$. Then, as in the Theorem 3.3, the mapping $E : \{\text{states}\} \to R$ is a one to one correspondence, the change of state is given by $z \mapsto \alpha^{-1} z$, and the collection $\{R, E, T\}$ is a projective model for the Galois-LFSR.

Ring-theoretic model. As in Theorem 3.2, let $R = \mathbf{F}_2[X]/(q)$, and define $T : R \to \mathbf{F}_2$ by $T(z) = z \pmod X$. Assume $\deg(q) = r$ but do not necessarily assume that q is irreducible. Associate to each state $s = (a_{r-1}, a_{r-2}, \ldots, a_1, a_0)$ of the shift register the following element

$$z = E(s) = a_0 + a_1 X + a_2 X^2 + \cdots + a_{r-1} X^{r-1}.$$

As in Theorem 3.2, every state of the shift register is periodic. The mapping E gives a one to one correspondence between the states of the shift register and elements $z \in R$; the change of state is given by $z \mapsto X^{-1} z$; the output sequence is given by

$$a_i = (X^{-i} z) \pmod q \pmod X; \tag{16}$$

and the collection $\{R, E, T\}$ forms a complete projective model of the LFSR.

3.3 FCSRs: Fibonacci Architecture

For FCSR sequences, the Galois field model and the Ring-theoretic models merge into a single model. Take $R = \mathbf{Z}/(q)$ with distinguished element $\beta = 2^{-1}$. Define $T : R \to \mathbf{Z}/(2)$ by $T(z) = z \pmod 2$ and define $S : R \to \{\text{states}\}$ by assigning to any $h \in \mathbf{Z}/(q)$ the initial state with $a_i = 2^{-i} h \pmod q \pmod 2$ (for $0 \le i \le r-1$) and with initial memory

$$m = \frac{1}{2^r}(h + \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} 2^k).$$

Let $\Gamma_q = \{$strictly periodic states of the FCSR with connection integer $q\}$. Note that the state $(1, 1, \cdots, 1; \mathrm{wt}(q+1) - 1)$, where $\mathrm{wt}(q+1)$ is the Hamming weight of $q+1$, is a periodic state with output equal to the all 1s sequence. Its associated 2-adic number is -1.

Theorem 3.5 *Let q be an odd positive integer. Then S is a one to one function from $\mathbf{Z}/(q)$ onto $L = \Gamma_q - \{(1, 1, \cdots, 1; \mathrm{wt}(q + 1) - 1)\}$. The state change is given by $h \mapsto 2^{-1}h$ and the output sequence is $a_j = 2^{-j}h \pmod q \pmod 2$. The collection $\{R, S, T\}$ constitute an injective model for the FCSR.*

Proof: That $\{R, S, T\}$ is a model follows from Section 6 and Theorem 11.1 of [8]. To see that S is injective, suppose to the contrary that $(a_0, \cdots, a_{r-1}; m) = S(g) = S(h) = (b_0, \cdots, b_{r-1}; n)$. Then

$$\frac{1}{2^r}(g + \sum_{k=0}^{r-1}\sum_{i=0}^{k} q_i a_{k-i} 2^k) = m = n = \frac{1}{2^r}(h + \sum_{k=0}^{r-1}\sum_{i=0}^{k} q_i b_{k-i} 2^k).$$

But $a_i = b_i$ for every i, so $g/2^r = h/2^r$ and thus $g = h$.

It is known that the 2-adic numbers associated with the periodic outputs from the FCSR with connection integer q are precisely the rational numbers $-p/q$ with $0 \le p \le q$ [8]. Thus there are precisely $q + 1$ periodic states. It follows that in order to see that S maps onto L, it suffices to show that the state $(1, 1, \cdots, 1; \mathrm{wt}(q + 1) - 1)$ is not in the image of S.

Suppose to the contrary that there is an integer h such that $1 = 2^{-j}h \pmod q \pmod 2$ for every j. Since $h \pmod q$ is odd if and only if $-h \pmod q$ is even, this is equivalent to saying there is an h such that all $2^{-j}h \pmod q$ are even. Since 2 is invertible mod q, we can let $m = 2^{\mathrm{ord}_q(2)}h$ and conclude that there is some m such that all $2^j m \pmod q$ are even. Let j be maximal so that $2^j m < q$. Then $q < 2^{j+1}m < 2q$, so $2^{j+1}m \pmod q = 2^{j+1}m - q$, which is odd. This contradiction proves the theorem. $\Box$

Remark 1. Although the mapping S always gives a strictly periodic state of the FCSR, we do not know a simple characterization of these states. The initial loading of the register portion is simply the lower order r bits in the binary expansion of the number

$$W = h\left(\frac{2^{\phi(q)} - 1}{q}\right)$$

(however we do not know a similar simple formula for the initial value of the memory). To see this, let $B = (2^{\phi(q)} - 1)/q$ as in the proof of lemma 2.2. Then $Bq \equiv -1 \pmod{2^{\phi(q)}}$. But $r < \phi(q)$ so $Bq \equiv -1 \pmod{2^r}$ which gives

$$W = h\left(\frac{2^{\phi(q)} - 1}{q}\right) \equiv -h/q \pmod{2^r}.$$

So the lower order r bits in the binary expansion of W coincides with the first r bits in the 2-adic expansion of $-h/q$, which is also the first r bits to be output by the FCSR. However these first r bits also coincide with the initial loading of the register portion of the FCSR.

Remark 2. If q is prime then $\mathbf{Z}/(q)$ is a field and its multiplicative group $(\mathbf{Z}/(q))^*$ is cyclic. In this case, 2^{-1} is a generator of $(\mathbf{Z}/(q))^*$ if and only if 2 is a primitive root modulo q. (Such a choice of q gives rise to maximal length sequences, or ℓ-sequences.) If q is composite, say $q = g_1^{e_1} g_2^{e_2} \cdots g_m^{e_m}$ is its prime decomposition, then the ring $R = \mathbf{Z}/(q)$ decomposes as a product $R = R_1 R_2 \cdots R_m$ with $R_j = \mathbf{Z}/(g_j^{e_j})$, in complete analogy with the LFSR case.

Remark 3. This model is not complete. As seen in the proof of Theorem 3.5, the state $(1, 1, \cdots, 1; \mathrm{wt}(q + 1) - 1)$ is not in the image of S. One can construct a different model that contains this state in its image by using $\{1, 2, \cdots, q\}$ as a set of representatives for the residue classes modulo q in the definition of $z(\mathrm{mod}\, q)(\mathrm{mod}\, 2)$ however the image of S will omit the zero state.

3.4 FCSRs: Galois Architecture

Now we wish to describe a model for the (Galois)-FCSR. Define $R = \mathbf{Z}/(q)$ and $T : R \to \mathbf{Z}/(2)$ as in Theorem 3.5. Define $E : \{\text{states}\} \to \mathbf{Z}/(q)$ to be the mapping which assigns to any state $(a_0, a_1, \ldots, a_{r-1}; c_1, \ldots, c_{r-1})$ the element $h \pmod q$, where h is defined in (12).

Notice that if $q_j = 0$ then the memory cell c_j will eventually drop to 0 and will remain 0 forever after. So for every periodic state there is a periodic state that produces the same output and satisfies $c_j = 0$ whenever $q_j = 0$. Let us say that a state satisfying this condition is an "admissible" state. (So the admissible states may be thought of as representing a Galois-FCSR in which memory cells c_j are provided only when the corresponding feedback tap q_j is nonzero.) Let Γ_q be the set of admissible states. Note that the state $(1, \ldots, 1; q_1, \ldots, q_{r-1})$ is always admissible and produces the all 1 sequence as output.

Theorem 3.6 *The collection $\{R, E, T\}$ is a projective model for the Galois-FCSR. For any admissible initial loading, the output of the Galois FCSR is strictly periodic. The mapping E is a surjection from $\Gamma_q - \{(1, \ldots, 1; q_1, \ldots, q_{r-1})\}$ to $\mathbf{Z}/(q)$ such that the change of state is given by $h \mapsto 2^{-1}h$. Hence the output sequence is $b_j = h2^{-j} \pmod q \pmod 2$.*

Proof: The greatest possible value for h is when all $a_i = 1$ and all the admissible $c_j = 1$. In this case $c_j = q_j$ for all j, so $h = 1 + (1 + q_1)2 + \cdots + (1 + q_{r-1})2^{r-1} = 2^r - 1 + q + 1 - q_r 2^r = q$. So for any admissible state s, we have: $0 \le h = E(s) \le q$ and hence the 2-adic expansion for $-h/q$ (which is the output sequence of the shift register) is strictly periodic. Reducing equation (11) modulo q and multiplying by 2^{-1} gives

$$2^{-1} = q_1 + q_2 2 + q_3 2^2 + \cdots + q_r 2^{r-1} \pmod{q}, \tag{17}$$

so

$$
\begin{aligned}
2^{-1}h &= a_0 2^{-1} + (a_1 + c_1)2^0 + (a_2 + c_2)2^1 + \cdots + (a_{r-1} + c_{r-1})2^{r-2} \\
&= (a_0 q_1 + a_1 + c_1)2^0 + (a_0 q_2 + a_2 + c_2)2^1 + \cdots \\
&\quad + (a_0 q_{r-1} + a_{r-1} + c_{r-1})2^{r-2} + a_0 q_r 2^{r-1} \\
&= (2c'_1 + a'_0)2^0 + (2c'_2 + a'_1)2^1 + \cdots + (2c'_{r-1} + a'_{r-2})2^{r-2} + a'_{r-1}2^{r-1} \\
&= a'_0 + (a'_1 + c'_1)2 + (a'_2 + c'_2)2^2 + \cdots + (a'_{r-1} + c'_{r-1})2^{r-1},
\end{aligned}
$$

which describes the change of state.

Finally, to show that the output function is correct, we must show that for any admissible state $(a_0, \ldots, a_{r-1}; c_1, \ldots, c_{r-1})$ other than $(1, \ldots, 1; q_1, \ldots, q_{r-1})$, we have $x \stackrel{def}{=} a_0 + (a_1 + c_1)2 + \cdots + (a_{r-1} + c_{r-1})2^{r-1} (\bmod q) = a_0$. We have $x = \sum_{i=0}^{r-1} a_i 2^i + \sum_{i=1}^{r-1} c_i 2^i \leq (2^r - 1) + (q + 1 - 2^r) = q$, with equality only if $(a_0, \ldots, a_{r-1}; c_1, \ldots, c_{r-1}) = (1, \ldots, 1; q_1, \ldots, q_{r-1})$. The theorem follows. $\square$

Combining this with Theorem 3.5 we have the following.

Corollary 3.7 *There is an onto function from the set of admissible periodic states of the Galois FCSR with connection integer q to the set of periodic states of the Fibonacci FCSR with connection integer q such that corresponding states produce the same output.*

Remark 1. We do not know a simple formula describing the contents of the kth cell as a function of time. Despite Theorem 3.6, we do not know how to intrinsically characterize the periodic states of the Galois-FCSR, (other than to say that they must be admissible states) because there may be several different states corresponding to the same number h. However, there is only one way to obtain $h = 1$ (namely, by $a_0 = 1$ and all other $a's$ and $c's$ are 0), so this state is necessarily a periodic state. If 2 is primitive modulo q, then all the other periodic states are obtained from this one by running the shift register.

Remark 2. This is not a complete model. Any state for which $a_i = 1$ and $c_i = 0$ has the same image under E as the state that is identical, except that $a_i = 0$ and $c_i = 1$.

4 d-FCSR Architectures

The d-FCSR architecture was introduced in [8] and [10], where its basic properties are listed. (See also [13].) In this section we first recall the operation of these shift registers and summarize the results from [4] which explain how to design them so as to give predictable outputs. We then describe a Galois architecture for d-FCSRs. We also describe models for both architectures.

4.1 Fibonacci Architecture for d-FCSR

The operation of a d-FCSR is similar to that of the FCSR except that each "carried" bit is delayed $d-1$ steps before being added (see Figures 5 and 6).

This is best understood using the ring $\mathbf{Z}[\pi]$ which consists of polynomials in π (with integer coefficients), subject to the formal relation $\pi^d = 2$. The ring $\mathbf{Z}[\pi]$ contains the integers $\mathbf{Z}$ and it can be embedded as a subring of the real numbers $\mathbf{R}$ by mapping π to the positive $\sqrt[d]{2}$. However there are other embeddings into the complex numbers. Any $z \in \mathbf{Z}[\pi]$ may be uniquely expressed as a polynomial $z = z_0 + z_1\pi + \cdots + z_{d-1}\pi^{d-1}$ with $z_i \in \mathbf{Z}$ by making use of the equation $\pi^d = 2 \cdot \pi^0$ whenever higher powers of π are encountered. Let us say that such an element z is *nonnegative* if each $z_i \geq 0$. (This is stronger than saying that the associated real number is nonnegative.) Using the binary expansion of each z_i, we see that a nonnegative element $z \in \mathbf{Z}[\pi]$ can be uniquely expressed as a polynomial

$$z = \sum_{i=0}^{m} z_i' \pi^i$$

with 0,1 coefficients. Addition and multiplication preserve nonnegative elements, and are performed in the obvious way, except that carried bits are advanced d steps because

$$1 + 1 = 2 = 0 + 0\pi + 0\pi^2 + \cdots + 0\pi^{d-1} + \pi^d,$$

so it is best not to think of these coefficients as lying in the field $\mathbf{F}_2$. The operations $(\operatorname{mod} \pi)$ and $(\operatorname{div} \pi)$ make sense in this ring. If $z = z_0 + z_1\pi + \cdots + z_{d-1}\pi^{d-1}$ then $z \pmod{\pi} = z_0 \pmod{2} \in \mathbf{F}_2$, and we say that z is *odd* if $z \pmod{\pi} = 1$. (For example, $-1 = 1 - \pi^d$ so $-1 \pmod{\pi} = 1$.) Similarly $z\ (\operatorname{div} \pi) = z_1 + z_2\pi + \cdots + z_{d-1}\pi^{d-2}$.

A d-FCSR consists of a shift register with cell contents $a_0, a_1, \ldots, a_{r-1}$, feedback connections $q_r, q_{r-1}, \ldots, q_1$, and memory cells $m_0, m_1, \ldots, m_s$, each of which is a 0 or 1. We represent the memory by the nonnegative element $m = m_0 + m_1\pi + \cdots + m_s\pi^s \in \mathbf{Z}[\pi]$. Associated to the feedback connections we define the connection "number"

$$q = -1 + q_1\pi + q_2\pi^2 + \cdots + q_r\pi^r. \tag{18}$$

Then $q \in \mathbf{Z}[\pi]$ is odd, and $q+1$ is nonnegative. The operation of the d-FCSR may be described as follows: Form the integer sum $\sigma' = \sum_{i=0}^{r-1} a_i q_{r-i}$. Write σ' as a nonnegative element of $\mathbf{Z}[\pi]$, that is, as a polynomial with $0,1$ coefficients in π, using $2 = \pi^d$. Using addition in $\mathbf{Z}[\pi]$ form the (nonnegative) sum $\sigma = m + \sigma'$. Shift the contents of the register cells to the right by one step. Place the bit $a_r = \sigma \pmod{\pi}$ in the leftmost register cell. Replace the memory by $m' = \sigma\ (\operatorname{div} \pi) = (\sigma - a_r)/\pi$. Thus the new values $(a_0', a_1', \ldots, a_{r-1}'; m')$ are related to the old values $(a_0, a_1, \ldots, a_{r-1}; m)$ by

$$a_i' = a_{i+1} \quad \text{for} \quad 0 \leq i \leq r-1$$

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

Implementation. The block diagram for a d-FCSR is the same as that of an FCSR, but since addition in $\mathbf{Z}[\pi]$ is needed, it is slightly more convenient to break the addition into two parts. The part labeled Σ adds the 0,1 inputs as integers and outputs the result σ' according to its binary expansion. The part labeled Π is an adder in $\mathbf{Z}[\pi]$.

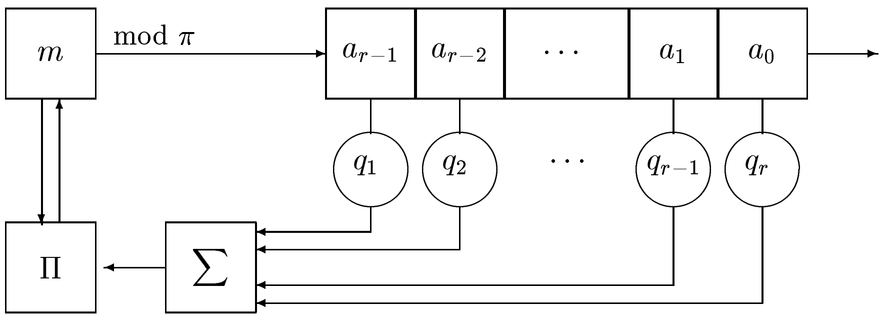

Figure 5: Fibonacci d-FCSR

For $d = 2$ the $\mathbf{Z}[\pi]$ adder Π, together with the memory m may be described as follows (Figure 6). Each symbol Σ represents a full adder with 3 inputs, cascaded so as to form a ripple counter. With each clock cycle the current contents m of the memory is added to the integer σ' which is presented at the input to the adder according to its binary expansion. The result σ is returned to the memory (which involves modifying only the even numbered memory cells). Then the contents of the memory are shifted one step to the right, thus outputting the lowest order bit $\sigma \pmod{\pi}$ and retaining the higher order bits, $\sigma \operatorname{div} \pi$ (with the highest order bit, m_6 in the following example, set to 0).

Let $wt(q+1)$ denote the number of nonzero q's involved in the feedback. It can be seen from Figure 6 (or from the change of state equations above) that the memory will decrease until $m_i = 0$ for all $i > d\log_2(wt(q+1)) + d$, so no memory overflow will occur provided the shift register is provided with memory cells $m_0, m_1, \ldots, m_s$ where $s \geq d\log_2(wt(q+1)) + d$. The deeper analysis of a d-FCSR is completely parallel to that of an FCSR however some less familiar mathematics is needed.

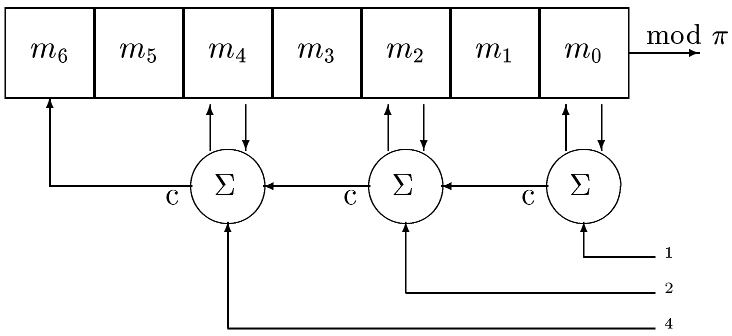

Figure 6: A $\mathbf{Z}[\pi]$-adder for $d = 2$.

Power series method. Let $\mathbf{Z}_\pi$ be the ring of "π-adic integers" consisting of all formal power series in π

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i \tag{19}$$

with $a_i = 0, 1$. Addition and multiplication are performed in the obvious way, using the relation $\pi^d = 2$ whenever necessary; in particular $\mathbf{Z}_\pi$ contains the 2-adic integers $\mathbf{Z}_2$. Since

$$-1 = 1 + \pi^d + \pi^{2d} + \pi^{3d} + \cdots$$

we see that $\mathbf{Z}_\pi$ also contains $\mathbf{Z}[\pi]$. In fact, $\mathbf{Z}_\pi$ contains all fractions $\alpha = a/b$ with $a, b \in \mathbf{Z}[\pi]$ provided that b is odd, (meaning that $b \pmod{\pi} = 1$) in which case we shall refer to (19) as "the" π-adic expansion of a/b. Such fractions are precisely the elements of $\mathbf{Z}_\pi$ whose π-adic expansions are eventually periodic. The following result was proven in [10].

Theorem 4.1 *Suppose an r-stage (Fibonacci) d-FCSR with connection integer q is initially loaded with register contents $(a_0, a_1, \ldots, a_{r-1})$ and memory m. Set $q_0 = -1$ and*

$$h = m\pi^r - \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} \pi^k$$

Then the output sequence of the d-FCSR is the coefficient sequence for the π-adic expansion of the fraction $\alpha = -h/q$. Conversely, if $\mathbf{a} = a_0, a_1, \ldots$ is an eventually periodic binary sequence with corresponding π-adic integer $\alpha = \sum_{i=0}^{\infty} a_i \pi^i = -h/q$ and if $q+1$ is nonnegative, then q is the connection number of a d-FCSR which generates this sequence. $\square$

A surprising consequence is that not every periodic binary sequence may be realized as the output sequence of a d-FCSR: only those for which $q + 1$ is nonnegative. This deficiency (if indeed it is such) can be rectified by considering a "polarized" d-FCSR in which the cells q_i, m_i are permitted to take values in $\{\pm 1, 0\}$. It can be seen that no "overflow" will ever occur and that *any* $q \in \mathbf{Z}[\pi]$ may be realized as the connection number of such a polarized d-FCSR.

Strictly periodic π-adic expansions. One of the main results in [4] is a characterization of the strictly periodic d-FCSR sequences. Let $\mathbf{Q}[\pi]$ be the d-dimensional vectorspace (over $\mathbf{Q}$) with basis $\{1, \pi, \pi^2, \ldots, \pi^{d-1}\}$. (In fact it is the fraction field of $\mathbf{Z}[\pi]$ and it is a totally ramified degree d extension of the rational numbers $\mathbf{Q}$, however we will not need these facts in this paper.) Let $\tau : \mathbf{Q}[\pi] \to \mathbf{Q}^d$ be the vectorspace isomorphism given by $\tau(a_0 + a_1\pi + \cdots + a_{d-1}\pi^{d-1}) = (a_0, a_1, \ldots, a_{d-1})$. Then $\tau(\mathbf{Z}[\pi])$ consists of all points in $\mathbf{Q}^d$ with integer coordinates, so we will refer to $\mathbf{Z}[\pi]$ as the set of *lattice points* in $\mathbf{Q}[\pi]$.

Fix $q \in \mathbf{Z}[\pi]$. Recall that the *norm* $N(q)$ of q is the determinant of the action given by multiplication by q on the vector space $\mathbf{Q}[\pi]$. With respect to the above basis, the matrix for multiplication by q may be easily calculated. For $d = 2$ and $q = q_0 + q_1\pi$, and for $d = 3$ and $q = q_0 + q_1\pi + q_2\pi^2$, these matrices are, respectively

$$\begin{pmatrix} q_0 & 2q_1 \\ q_1 & q_0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} q_0 & 2q_2 & 2q_1 \\ q_1 & q_0 & 2q_2 \\ q_2 & q_1 & q_0 \end{pmatrix}.$$

The matrix for arbitrary d is similar. It follows (by reducing this matrix modulo 2) that $q \in \mathbf{Z}[\pi]$ is odd if and only if its norm $N(q) \in \mathbf{Z}$ is odd. Let (q) denote the ideal in $\mathbf{Z}[\pi]$ generated by $q \in \mathbf{Z}[\pi]$ and let $R = \mathbf{Z}[\pi]/(q)$ denote the quotient ring. The number of elements in the ring R is $|N(q)|$. If $z \in \mathbf{Z}[\pi]$, we denote by $z \pmod{q}$ its image in R. If q is odd then π is invertible in R.

If $E = \{e_1, e_2, \ldots, e_k\}$ is a finite collection of linearly independent vectors in Euclidean space $\mathbf{Q}^d$, let us denote the half-open *parallelepiped spanned by* E to be the set

$$P(E) = \left\{ \sum_{i=1}^{k} a_i e_i |\ 0 \le a_i < 1 \right\}. \tag{20}$$

Let

$$\Delta_q = \mathbf{Z}[\pi] \cap P(q, q\pi, q\pi^2, \ldots, q\pi^{d-1})$$

be the set of lattice points in the parallelepiped (in $\mathbf{Q}[\pi]$) which is spanned by the set of vectors $\{q, q\pi, q\pi^2, \ldots, q\pi^{d-1}\}$. Also let us denote the closed *parallelepiped spanned by* E to be the set

$$\bar{P}(E) = \left\{ \sum_{i=1}^{k} a_i e_i |\ 0 \le a_i \le 1 \right\} \tag{21}$$

and

$$\bar{\Delta}_q = \mathbf{Z}[\pi] \cap \bar{P}(q, q\pi, q\pi^2, \ldots, q\pi^{d-1}).$$

In [4] we prove the following result.

Theorem 4.2 *Suppose that $h, q \in \mathbf{Z}[\pi]$ and that q is odd. Then the π-adic expansion of the fraction $\alpha = -h/q$ is strictly periodic if and only if $h \in \bar{\Delta}_q$. Moreover, the mapping $\mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ induces a one to one correspondence*

$$\Delta_q \leftrightarrow \mathbf{Z}[\pi]/(q). \tag{22}$$

(In other words, the set Δ_q is a complete set of representatives for the elements of $\mathbf{Z}[\pi]/(q)$.) For such an $h \in \Delta_q$ the π-adic expansion of $\alpha = -h/q = \sum_{i=0}^{\infty} b_i \pi^i$ is given by

$$b_i = h\pi^{-i} \pmod{q} \pmod{\pi}. \tag{23}$$

Here, (as in Theorem 3.1 and Lemma 2.2), for any $z \in \mathbf{Z}[\pi]/(q)$ the symbol $z \pmod{\pi}$ means that z must first be replaced by the corresponding element in the complete set of representatives Δ_q, then this element is reduced modulo π to obtain an element of $\mathbf{Z}[\pi]/(\pi) = \mathbf{Z}/(2)$. (The resulting mapping $\mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(2)$ is not a ring homomorphism.) Since the image $\pi \pmod{q} \in \mathbf{Z}[\pi]/(q)$ of π is invertible, the quantity $h\pi^{-i} \pmod{q}$ makes sense in $\mathbf{Z}[\pi]/(q)$.

Remark. A *face* $F \subset P$ of the parallelepiped (20) is the set of points obtained by setting some of the coefficients $a_j = 0$. The set of lattice points $\Delta_q \cap F$ in any face correspond under equation (22) to an additive subgroup of $\mathbf{Z}[\pi]/(q)$. If $\mathbf{Z}[\pi]/(q)$ is a prime field then there are no additive subgroups other than $\{0\}$, in which case all the nonzero elements of Δ_q lie in the interior of the parallelepiped.

Model for Fibonacci d-FCSR. As in the FCSR case, one can construct a ring-theoretic model with $R = \mathbf{Z}[\pi]/(q)$, $T : R \to \{0, 1\}$ given by $T(z) = z \pmod{\pi}$ as above, and with $S : R \to \{\text{states}\}$ defined to be the mapping which associates to $z \in R$ the initial loading $a_i = \pi^{-i} z \pmod{q} \pmod{\pi}$ for $0 \le i \le r-1$ and with initial memory

$$m = \frac{1}{\pi^r}\left(z + \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} \pi^k\right).$$

Then Theorems 4.1 and 4.2 may be restated as follows:

Theorem 4.3 *Let $q \in \mathbf{Z}[\pi]$ and suppose $q+1$ is nonnegative. Then the collection $\{R, S, T\}$ forms an injective model for the d-FCSR with connection number q. The state change is given by $z \mapsto \pi^{-1}z$ and the output sequence is $a_i = \pi^{-i}z \pmod{q} \pmod{\pi}$. The image of S is the set of states whose output is a π-adic number h/q with h in the open parallelipiped Δ_q.*

It is possible to give a much more down-to-earth description of these sequences when the norm $N = |N(q)|$ is an odd prime, which we henceforth assume. In [4] we prove the following:

Lemma 4.4 *Suppose $q \in \mathbf{Z}[\pi]$ is odd and that $N = |N(q)|$ is prime. Then the natural composition $\mathbf{Z} \to \mathbf{Z}[\pi] \to \mathbf{Z}[\pi]/(q)$ induces an isomorphism of rings,*

$$\mathbf{Z}/N \cong \mathbf{Z}[\pi]/(q) \tag{24}$$

which is therefore a field.

Let $\psi : \mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(N)$ denote the inverse to this isomorphism. It is completely determined by the single integer $m = \psi(\pi)$ because for any integers c_i (with $0 \le i \le d-1$), the mapping ψ satisfies $\psi(\sum_{i=0}^{d-1} c_i \pi^i) = \sum_{i=0}^{d-1} c_i m^i$. The prime number N may be considered as an element of $\mathbf{Z}[\pi]$ and as such, it turns out to be divisible by π (see [4]). Define $s_i \in \mathbf{Z}$ by expanding

$$\delta = N(q)/q = \sum_{i=0}^{d-1} s_i \pi^i. \tag{25}$$

The following result is proven in [4].

Theorem 4.5 *Let $h, q \in \mathbf{Z}[\pi]$. Suppose that $N = |N(q)|$ is an odd prime number and that $h \in \Delta_q$ lies in the strictly periodic region described in Theorem 4.2. Let $m = \psi(\pi)$ and let s_0 be defined by equation (25). Then, for all j, the following equation holds,*

$$\pi^{-j}h \pmod{q} \pmod{\pi} = m^{-j}\psi(h)s_0 \pmod{N} \pmod{2}$$

In other words, the output sequence (23) may be simply described as $Ab^j \pmod{N} \pmod{2}$ for appropriately chosen $A = \psi(h)s_0 \in \mathbf{Z}/(N)$ and $b = m^{-1} \in \mathbf{Z}/(N)$. The numbers m and s_0 can be computed directly from knowledge of q, although sometimes just knowing that $m^d \equiv 2 \pmod{N}$ nearly determines m. For $d = 2$ and $d = 3$ these computations are tabulated in Figure 7.

	$d=2$	$d=3$
q	$q_0 + q_1\pi$	$q_0 + q_1\pi + q_2\pi^2$
$N(q)$	$q_0^2 - 2q_1^2$	$q_0^3 + 2q_1^3$ $+4q_2^3 - 6q_0q_1q_2$
δ	$q_0 - q_1\pi$	$(q_0^2 - q_1q_2) + (2q_2^2 - q_0q_1)\pi$ $+(q_1^2 - q_0q_2)\pi^2$
m	$-2q_1/q_0$	$2(q_1^2 - q_0q_2)/(q_0^2 - q_1q_2)$
s_0	q_0	$q_0^2 - q_1q_2$

Figure 7: Parameters of $\mathbf{Z}[\pi]$

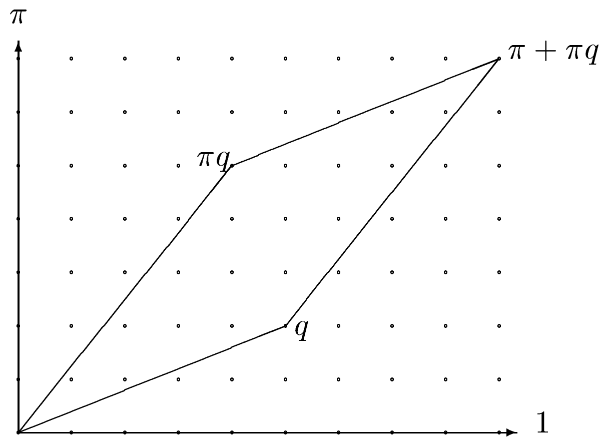

Figure 8: Parallelogram for $q = 5 + 2\pi$.

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

Figure 9: Model states for $q = 5 + 2\pi$.

An Example Consider the d-FCSR with $d = 2$ and $q = 5+2\pi$. The shift register is 4-stage with feedback coefficients $q_1 = 0$, $q_2 = q_3 = q_4 = 1$ (so that $q+1 = 6+2\pi$). Then $N(q) = 17$ which is prime, so the parallelogram contains 16 elements in its interior, see Figure 8.

The isomorphism $\psi : \mathbf{Z}[\pi]/(q) \to \mathbf{Z}/(17)$ maps π to $m = 6$, which is primitive modulo 17, so we obtain a maximal length output sequence. The constant $s_0 = 5$ and computations for the table (Figure 9) may be simplified by observing that $6^{-1} \equiv 3 \pmod{17}$. Each element in $\mathbf{Z}[\pi]/(q)$ has a unique representative h in the above parallelogram; these representatives are listed in the second column of the following table. The corresponding element in $\mathbf{Z}/(17)$ is listed in the third column. The fourth column (which is the d-FCSR sequence under consideration) is the third column modulo 2, and it concides with the second column modulo π as predicted by Theorem 4.5.

4.2 Galois architecture for d-FCSRs

In the Galois architecture for a d-FCSR, the carried bits are delayed $d-1$ steps before being fed back, so the output of the memory or "carry" cell c_i is fed into the register cell a_{i+d-2}. (Recall that the register cells are numbered starting from a_0.) If there are r feedback multipliers $q_1, \ldots, q_r$ and r carry cells $c_1, \ldots, c_r$ then $r + d - 1$ register cells $a_0, \ldots, a_{r+d-2}$

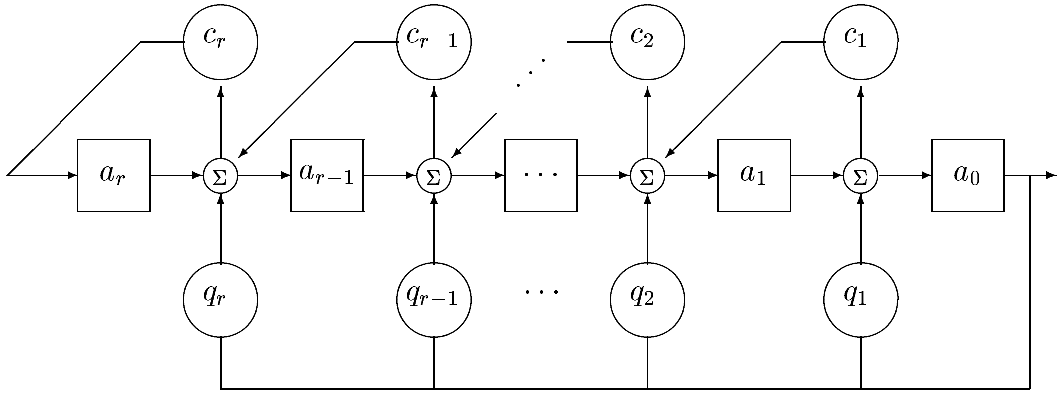

Figure 10: Galois 2-FCSR.

are evidently needed since c_r will feed into a_{r+d-1}. This is illustrated in Figure 10 for $d = 2$. If $d \geq 3$ the situation is more complicated and t "additional" memory cells $c_{r+1}, \ldots, c_{r+t}$ are needed, which feed into t "additional" register cells $a_{r+d-1}, \ldots, a_{r+t+d-2}$. It is not at all obvious at first glance whether the amount t of extra memory can be chosen to be finite without incurring a memory overflow during the operation of the shift register. However (see Theorem 4.8 below) we show that this is indeed the case and henceforth we suppose that t has been chosen as described there, to be sufficiently large so as to avoid any memory overflow. Suppose a Galois d-FCSR is initially loaded with given values (a_0, a_1, $\ldots$, $a_{r+t+d-2}$; c_1, c_2, $\ldots$, c_{r+t}). The register operates as follows. (To simplify notation, set $q_j = 0$ for $j \geq r+1$, set $c_j = 0$ for $j \leq 0$ and also for $j \geq r+t+1$, and set $a_j = 0$ for $j \geq r+t+d-1$.) For each j (with $1 \leq j \leq r+t+d-1$) form the *integer* sum $\sigma_j = a_0 q_j + a_j + c_{j-d+1}$; it is between 0 and 3. The new values are given by $a'_{j-1} = \sigma_j \pmod 2$ and $c'_j = \sigma_j \ (\mathrm{div}\, 2)$, that is,

$$2c'_j + a'_{j-1} = a_0 q_j + a_j + c_{j-d+1} \quad \text{for} \quad 1 \leq j \leq r+t+d-1 \tag{26}$$

(Note, for example, that these equations say $a'_{r+t+d-2} = c_{r+t}$.)

For such a Galois d-FCSR define the connection integer

$$q = -1 + \sum_{i=1}^{r} q_i \pi^i \in \mathbf{Z}[\pi].$$

For a given initial loading $(a_0, \ldots, a_{r+t+d-2}; c_1, c_2, \ldots, c_{r+t})$ using the same conventions as above, define

$$h = \sum_{i=0}^{r+t+d-2} (a_i + c_{i-d+1}) \pi^i \in \mathbf{Z}[\pi]. \tag{27}$$

Theorem 4.6 *If t is large enough that no memory overflow occurs (as described in Theorem 4.8 below), then the output sequence $\{b_1, b_1, \ldots\}$ of the d-FCSR coincides with the π-adic expansion of the fraction $\alpha = -h/q \in \mathbf{Z}_\pi$. Thus if the Galois FCSR is in a purely periodic state,*

$$b_i = \pi^{-i} h (\operatorname{mod} q)(\operatorname{mod} \pi).$$

Proof: The proof is similar to that of Theorem 2.4. Given h and q as above, let $B = \sum_{i=0}^{\infty} b_i \pi^i$ denote the π-adic number which is represented by the output sequence. Compute $qB + h = (-b_0 + a_0) + (-b_1 + q_1 b_0 + a_1)\pi + \cdots$. But $a_0 = b_0$ since this is the first bit to be output from the shift register. Hence the quantity $qB + h$ has no constant term.

Now run the shift register one step, obtaining a shifted output sequence $b'_0, b'_1, \ldots$, a corresponding π-adic number B', a new loading $(a'_0, a_1, \ldots, a'_{r+d-2}; c'_1, \ldots, c'_r)$ given by (26), and hence a new h'. Compute that $\pi B' = (B - b_0) \in \mathbf{Z}[\pi]$ and $\pi h' = (h + a_0 q) \in \mathbf{Z}[\pi]$ hence

$$\pi(qB' + h') = (qB + h).$$

By the same argument as above, the constant term of $qB' + h'$ vanishes. Hence $qB + h$ is divisible by π^2. By induction we find that $qB + h$ is divisible by π^n for all n, which is to say, $qB + h = 0$. $\square$

Using Theorem 4.5 we have the following corollary.

Corollary 4.7 *Suppose a Galois d-FCSR with connection number $q = -1 + \sum_{i=1}^{r} q_i \pi^i \in \mathbf{Z}[\pi]$ is chosen such that $N = |N(q)| \in \mathbf{Z}$ is a prime number. Suppose the initial loading is chosen so that (27) $h \in \Delta_q$ lies in the set of strictly periodic elements (Theorem 4.2). Then the output sequence $\{b_0, b_1, b_2, \ldots\}$ of the d-FCSR is given by*

$$b_i = s_0 m^{-i} \psi(h) \pmod{N} \pmod{2}.$$

Memory considerations In the following analysis we make use of some ideas from [13]. Let us denote the standard embedding $\mathbf{Z}[\pi] \to \mathbf{R}$ (which maps π to the positive $\sqrt[d]{2}$) by $x \mapsto |x|$. Recall that an element $x = \sum_{i=o}^{m} x_i \pi^i \in \mathbf{Z}[\pi]$ is *positive* if each of the coefficients $x_i \geq 0$. This implies (but is not implied by): $|x| \geq 0$. For a given positive real number R there may be infinitely many elements $x \in \mathbf{Z}[\pi]$ such that $|x| \leq R$. However there are only finitely many *positive* such elements x.

Theorem 4.8 *If t is chosen so that*

$$|\pi|^{r+t-2}(|\pi| - 1) \geq \frac{1}{2}|q| \tag{28}$$

then no memory overflow will occur and in fact, for any initial loading of the shift register the memory will decrease until the value (27) of h satisfies

$$|h| \leq \frac{|q|}{|\pi| - 1} \tag{29}$$

and it will remain within this range thereafter.

Here, as in [13], the fact that $|\pi| > 1$ is crucial.

Proof: First suppose the initial loading $(a_0, \ldots, a_{r+t+d-2}; c_1, \ldots, c_{r+t})$ satisfies (29). Then the same will be true for every subsequent state of the shift register. For let $(a'_0, \ldots, a'_{r+t+d-2};$ $c'_1, \ldots, c'_{r+t})$ denote the next state of the shift regsiter with corresponding value $h' \in \mathbf{Z}[\pi]$. Then $\pi h' = h + a_0 q$ (as in the proof above) so

$$|h'| \leq \frac{|h| + |q|}{|\pi|} \leq \frac{1}{|\pi|}\left(\frac{|q|}{|\pi| - 1} + |q|\right) = \frac{|q|}{|\pi| - 1}$$

as claimed. The same calculation shows that if $|h| > |q|/(|\pi| - 1)$ then

$$|h'| - \frac{|q|}{|\pi| - 1} \leq \frac{1}{|\pi|}\left(|h| - \frac{|q|}{|\pi| - 1}\right).$$

Thus the value of h will drop until it enters the range (29). Now let us estimate the maximum number of memory cells which are needed in order to accomodate all such values of h. (The following estimates can be improved.) The worst possible case occurs when all $c_i = a_i = 0$ except for the last possible term ($a_{r+t+d-2} = 1$ or $c_{r+t} = 1$) in which case

$$h = \pi^{r+t+d-2} = 2\pi^{r+t-2}.$$

Then (29) gives

$$|\pi|^{r+t-2}(|\pi| - 1) \leq \frac{1}{2}|q|.$$

Consequently, if t is chosen so that (28) holds then no memory overflow will occur. $\square$

A deeper result of Klapper and Xu [13] states that even if negative coefficients are permitted in the register contents, the memory will nevertheless remain bounded.

Model for Galois d-FCSR Now we wish to describe a model for the Galois d-FCSR. Define $R = \mathbf{Z}[\pi]/(q)$ and $T : R \to \mathbf{Z}/(2)$ as in Theorem 4.3. Define $E : \{\text{states}\} \to \mathbf{Z}/(q)$ to be the mapping which assigns to any state $(a_0, a_1, \ldots, a_{r+t+d-2}; c_1, \ldots, c_{r+t})$ the element $h \pmod{q}$, where h is defined in (27).

Unfortunately, we do not have a clear notion of "admissible states" for the Galois d-FCSR architecture when $d \geq 2$. The best we can do is to let L denote the set of states for which h is in the open parallelipiped $P(q, q\pi, \cdots, q\pi^{d-1})$. Then Theorem 4.6 gives us the following result.

Theorem 4.9 *The collection $\{R, E, T\}$ is a projective model for the Galois-FCSR. For any initial loading in L, the output of the Galois FCSR is strictly periodic. The mapping E is a surjection from L to $\mathbf{Z}[\pi]/(q)$ such that the change of state is given by $h \mapsto \pi^{-1}h$. Hence the output sequence is $b_j = h\pi^{-j} \pmod{q} \pmod{\pi}$.*

Corollary 4.10 *Suppose a Galois d-FCSR with connection number $q = -1 + \sum_{i=1}^{r} q_i\pi^i \in \mathbf{Z}[\pi]$ is chosen such that $N = |N(q)| \in \mathbf{Z}$ is a prime number. Suppose the initial loading is chosen so that (27) $h \in \Delta_q$ lies in the set of strictly periodic elements (Theorem 4.2). Then the output sequence $\{b_0, b_1, b_2, \ldots\}$ of the d-FCSR is given by*

$$b_i = s_0 m^{-i}\psi(h) \pmod{N} \pmod{2}.$$

This association induces a one to one correspondence between the strictly periodic states of the d-FCSR and the elements $h \in \mathbf{Z}/N(q)$.

By choosing different complete sets of representatives for $\mathbf{Z}[\pi]/(q)$ in $\bar{\Delta}_q$ we obtain different models with the same ring R. Every periodic state is accounted for by at least one such model. Thus we have the following corollary to Theorems 4.9 and 4.3.

Corollary 4.11 *If $q+1$ is nonnegative, then there is an onto function from the set of periodic states of the Galois d-FCSR with connection integer q to the set of periodic states of the Fibonacci d-FCSR with connection integer q such that corresponding states produce the same output.*

Unfortunately our understanding of the Galois d-FCSR architecture still leaves much to be desired. We do not know how to find a class of "admissible" states for which the output is strictly periodic (as we did in the case of the FCSR). We do not know an optimal estimate on the amount of memory needed for the d-FCSR (except in the case $d = 2$). We do not know how to describe the output of the kth cell.

5 Conclusions

We have found a "Galois" representation for FCSR and d-FCSR pseudorandom sequence generators. We have constructed "models" for the behavior of LFSR, FCSR, and d-FCSR generators, both in their Fibonacci and Galois representations. In each case, we find the Galois representation to be simpler, especially with regard to the computation of the initial loading of the register. Moreover, in the FCSR and d-FCSR cases, the Galois circuitry is faster since the arithmetic operations occur in parallel. We have analyzed the operation of the d-FCSR circuit using some rather sophisticated number theory, and have shown how it can be configured so as to give output sequences of the form $a_i = Ab^i \pmod{N} \pmod{2}$.

References

[1] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier (North-Holland), Amsterdam, 1998.

[2] L. E. Dickson, History of the Theory of Numbers, vol. 1, Carnegie Inst., Washington D.C., 1919 (reprinted by Chelsea and published by American Mathematical Society).

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

[4] M. Goresky and A. Klapper, Periodicity and arithmetic correlations of algebraic feedback shift register sequences over ramified extensions of the rationals. In preparation.

[5] M. Goresky, A. Klapper and L. Washington, Fourier Transforms and the 2-adic Span of Periodic Binary Sequences, IEEE Trans. Info. Theory **46** (2000) pp. 687-691.

[6] E. Key, An analysis of the structure and complexity of nonlinear binary sequence generators. I.E.E.E. Trans. Info. Theory **IT-22** (1976) pp. 732-736.

[7] A. Klapper, Feedback with carry shift registers over finite fields, *Proceedings of Leuven Algorithms Workshop.* Lecture Notes in Computer Science **1008** Springer Verlag, New York, 1994, pp. 170-178.

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

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

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

[11] A. Klapper and M. Goresky, Large period nearly de Bruijn sequences, *Advances in Cryptology - Eurocrypt 1996.* Lecture Notes in Computer Science **921**, Springer Verlag, New York, 1995, pp. 263-273.

[12] A. Klapper and M. Goresky, Cryptanalysis based on 2-adic rational approximation, *Advances in Cryptology - Crypto '95.* Lecture Notes in Computer Science **963**, Springer Verlag, New York, 1995, pp. 262-273.

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

[14] A. Klapper and J. Ju, Feedback with carry shift registers over $\mathbf{Z}/(N)$, *Proceedings of International Conference on Sequences and their Applications, Singapore, December 1998.* Springer Verlag, New York, to appear.

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

[16] R. Lidl and H. Niederreiter, *Finite Fields* (*Encyclopedia of Mathematics vol. 20*), Cambridge University Press, Cambridge, 1983.

[17] R. McEliece, *Finite Fields for Computer Scientists and Engineers,* Kluwer Academic Publishers, Boston, 1987.

[18] J. Noras, Fast pseudorandom sequence generators: linear feedback shift registers, cellular automata, and carry feedback shift registers. Univ. of Bradford Electrical Engineering department report **594** (1997).

[19] W. W. Peterson, Encoding and error-correction procedure for the Bose-Chaudhuri codes. IRE Trans. Info. Theory **IT-6** (1960) pp. 459-470.

[20] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes* second edition, MIT Press, Cambridge MA, 1972.

[21] B. Schneier, *Applied Cryptography* (second edition), John Wiley and Sons, New York, 1996.

[22] M. Simon, J. Omura, R. Scholtz, B. Levitt, *Spread Spectrum Communications Handbook* (second edition), McGraw-Hill, N.Y., 1994.