Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers

Mark Goresky, *Associate Member, IEEE,* and Andrew M. Klapper, *Associate Member, IEEE*

***Abstract*—A feedback-with-carry shift register (FCSR) with "Fibonacci" architecture is a shift register provided with a small amount of memory which is used in the feedback algorithm. Like the linear feedback shift register (LFSR), the FCSR provides a simple and predictable method for the fast generation of pseudorandom sequences with good statistical properties and large periods. In this paper, we describe and analyze an alternative architecture for the FCSR which is similar to the "Galois" architecture for the LFSR. The Galois architecture is more efficient than the Fibonacci architecture because the feedback computations are performed in parallel. We also describe the output sequences generated by the d-FCSR, a slight modification of the (Fibonacci) FCSR architecture in which the feedback bit is delayed for d clock cycles before being returned to the first cell of the shift register. We explain how these devices may be configured so as to generate sequences with large periods. We show that the d-FCSR also admits a more efficient "Galois" architecture.**

***Index Terms*—d-FCSR, feedback with carry, feedback-with-carry shift register (FCSR), Fibonacci, Galois, linear feedback shift register (LFSR).**

I. 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 pseudorandom sequences. During the last few years, the feedback-with-carry shift register (FCSR) architectures and a simple modification, the d-FCSR architectures have been investigated as alternative methods for the efficient generation of long pseudorandom binary sequences [1]–[3], [12], [14], [25]. 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 [7], [12], [13], [15], [16]). The FCSR circuits described in these papers resemble the "Fibonacci" configuration of the LSFR. The current paper has three objectives:

1) to develop and analyze the "Galois" configuration for FCSR and d-FCSR circuitry (cf. [22]);
2) to give a new elementary description for d-FCSR sequences and to characterize the strictly periodic ones; and
3) to formalize the notion of a mathematical "model" for a finite-state machine with output, and to find such models for FCSR and d-FCSR generators, both in their Fibonacci and Galois configurations.

We now describe each of these three points in greater detail.

Galois and Fibonacci Configurations: The Galois and Fibonacci configurations for an LFSR are recalled in Figs. 1 and 2. The FCSR of Fig. 3 somewhat resembles the Fibonacci representation, and one might ask whether there is an analogous Galois representation for the same FCSR sequences. Such a representation was first discussed in [22]. In this paper, we will analyze the Galois representations for FCSR (and d-FCSR) circuitry. It turns out that the initial loading is easier to describe in the Galois representation. Moreover, 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.

d-FCSR Sequences: There is an enormous collection of variations on the basic FCSR architecture which have also been analyzed to varying degrees [12], [11], [14], [17]–[19]. Perhaps the simplest of these variations is the d-FCSR (Fig. 5), in which the feedback bit is computed but is delayed for $d-1$ clock cycles before being fed back. In Theorem 6.5, we explain the surprising new result that the output of a d-FCSR may be described by

$$a_i = b^{-i} \pmod N \pmod 2 \tag{1}$$

where $N \in \boldsymbol{Z}$ is a certain integer. (Compare this to the case of an FCSR, for which the output sequence is always given by (1) with $b = 2$. It often follows that this sequence is a *decimation* of the FCSR sequence with connection integer N.) This new "elementary description" does not involve algebraic number fields. The d-FCSR architecture also has a "Galois" representation which we describe in Fig. 8 and for which we also construct models (see later).

Mathematical Models: Let M be a finite-state machine with output. 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. Define a *model* for M to consist of a ring R together with an element $\beta \in R$, a mapping T: $R \to \{0, 1\}$, and a correspondence between elements $h \in R$ and periodic states of M so that: a) the

Manuscript received November 1, 2000; revised June 20, 2002. The work of M. Goresky was supported in part by the National Science Foundation (NSF) under Grant CCR-0002693. The work of A. M. Klapper was supported in part by the National Science Foundation (NSF) under Grant CCR-9980429.

M. Goresky is with School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540 USA (e-mail: goresky@ias.edu).

A. M. Klapper is with the Department of Computer Science, University of Kentucky, Lexington, KY 40506-0046 USA (e-mail: klapper@cs.uky.edu).

Communicated by N. I. Koblitz, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2002.804048.

state change is given by $h \mapsto \beta h$ and b) the output is given by $T(h)$. Hence, for a given initial state, the output sequence of the machine is

$$a_i = T(\beta^i h) \tag{2}$$

where $h \in R$ corresponds to the initial state. Sometimes it is easier to describe the correspondence above by a mapping S: $R \to \{\text{periodic states of } M\}$. If S is one to one, we say the collection $\{R, S, T\}$ is an *injective* model. In other cases, the correspondence may be more easily described by a mapping E: $\{\text{periodic states of } M\} \to R$. If E is an onto mapping we say the collection $\{R, E, T\}$ is a *projective* model. Ideally, we would like S or E to be one-to-one correspondences, in which case the inverse mapping can usually 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), (6), (10), (14). In this paper, we describe models for FCSRs, and d-FCSRs, both in their Galois and Fibonacci configurations. In each case, we discover the surprising fact that the models for Fibonacci configurations are injective while the models for the Galois configurations are simpler and are projective. For comparison, in the first (purely expository) part of this paper we quickly recall some (well-known) models for LFSRs.

Throughout this paper, $\boldsymbol{Z}$ denotes the integers; $\boldsymbol{Q}$ denotes the rational numbers, and $\boldsymbol{F}_q$ denotes the Galois field with q elements. The multipliers, and the contents of the shift registers in this paper are assumed to be elements of the field $\boldsymbol{F}_2$. However, the same analysis applies to registers with entries in $\boldsymbol{F}_q$ and for this reason we do not automatically convert every -1 to $+1$.

II. LFSR, Fibonacci Architecture

The purpose of this section is to recall some well-known results concerning LFSRs, in a way which will motivate our treatment of FCSRs. In the Fibonacci representation (see Fig. 1), the register is initially loaded with bits $a_0, a_1, \ldots, a_{r-1}$. The output sequence is given by the linear recurrence

$$a_t = \sum_{i=1}^{r} q_i a_{t-i} \tag{3}$$

for $t \geq r$. Assume $q_r \neq 0$. To such an LFSR of length r, associate 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. Any infinite binary sequence $\boldsymbol{a} = (a_0, a_1, a_2, \ldots)$ may be identified with its generating function $A(X) = \sum_{i=0}^{\infty} a_i X^i$ which is an element of the ring $\boldsymbol{F}_2[[X]]$ of formal power series with coefficients in the integers modulo 2. The sequence $\boldsymbol{a}$ is called the coefficient sequence of the function $A(X)$. It is eventually periodic if and only if $A(X)$ is equal to the quotient of two polynomials $A(X) = -h(X)/q(X) \in \boldsymbol{F}_2[[X]]$. It is strictly periodic if and only if $\deg(h(X)) < \deg(q(X))$. Recall the following classical result [5, Sec. 2.5, p. 30], or [20, Theorem 8.40, p. 416].

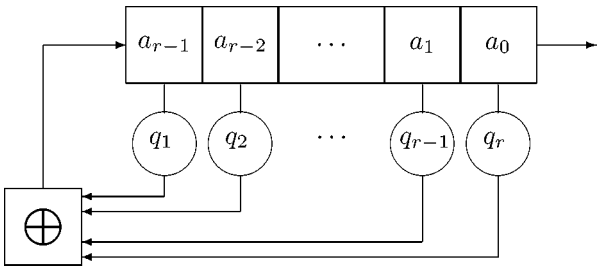

Fig. 1. Fibonacci LFSR.

Theorem 2.1: Suppose an LFSR with connection polynomial q of degree r has initial loading $(a_0, a_1, \ldots, a_{r-1})$. Set

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

where $q_0 = -1$. Then the output sequence is the coefficient sequence of the function $A(X) = -h(X)/q(X)$. Conversely, if $\boldsymbol{b} = b_0, b_1, \ldots$ is any strictly periodic sequence, let $B(X) = -h(X)/q(X)$ be its generating function. Then $q(X)$ is the connection polynomial of an LFSR which generates the sequence, and $h(X)$ determines the initial loading by (4).

Ring-Theoretic Model: Let $\boldsymbol{F}_2[X]$ be the ring of polynomials in X with 0, 1 coefficients. Let us denote the mapping $\boldsymbol{F}_2[X] \to \boldsymbol{F}_2$ which assigns to each polynomial its constant term by $z \mapsto z \pmod X$. It is a homomorphism of rings. The connection polynomial $q(X) = -1 + q_1 X + q_2 X^2 + \cdots + q_r X^r$ generates an ideal (q) in this ring, and we consider the quotient

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

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

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

It follows that any element $h \in R$ may be uniquely represented as a polynomial

$$h(X) = h_0 + h_1 X + \cdots + h_{r-1} X^{r-1}$$

of degree less than r. Define the mapping

$$T\colon R \to \boldsymbol{F}_2 \quad \text{by} \quad T(h) = h(\bmod q)(\bmod X). \tag{5}$$

This means that first the element h is represented by a polynomial of degree less than r, and then $T(h) = h_0$ is taken to be the constant term. (The mapping T is *not* a ring homomorphism, and its definition depends on this particular choice of complete set of representatives in $\boldsymbol{F}_2[X]$ for the elements of R, consisting of polynomials of degree $< r$.) Note that X is invertible in R with $X^{-1} = q_1 + q_2 X + \cdots + q_r X^{r-1}$. Define a mapping $S\colon R \to \{\text{states}\}$ which associates to any $h \in R$ the state $S(h)$ of the shift register which is given by

$$a_i = X^{-i} h(\bmod q)(\bmod X)$$

for $0 \leq i \leq r-1$. The following is a concise statement, in the language of models, of the discussion found in [24, Sec. 7].

Theorem 2.2: The collection $\{R, S, T\}$ is an injective model for the LFSR with connection polynomial $q(X)$. Every state of the LFSR is periodic. The mapping S between elements

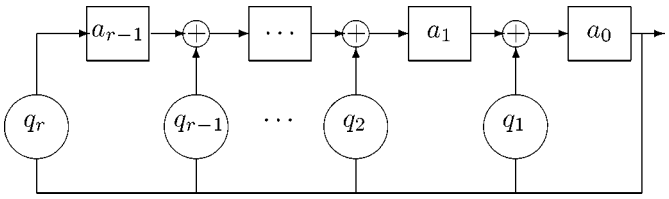

Fig. 2. Galois LFSR.

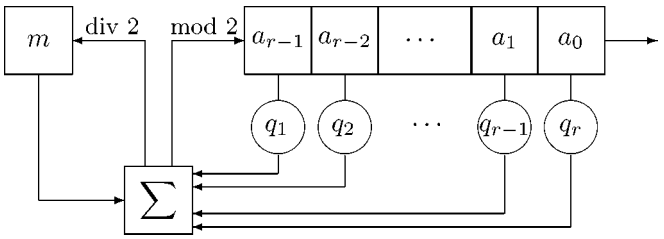

Fig. 3. Fibonacci FCSR.

of R and states of the shift register is a one-to-one correspondence such that the change of state is given by $h \mapsto X^{-1}h$. The output sequence of the LFSR with initial loading $S(h)$ is given by (2), that is, for $i \geq r$,

$$a_i = T(X^{-i}h) = X^{-i}h(\mathrm{mod}\, q)(\mathrm{mod}\, X).$$

Remarks: If q is irreducible and $\alpha \in \boldsymbol{F}_{2^r}$ is a root of q then the mapping Φ: $\boldsymbol{F}_2[X]/(q) \rightarrow \boldsymbol{F}_{2^r}$ given by $X \mapsto \alpha$ is an isomorphism of rings, and there is a unique $\boldsymbol{F}_2$ linear mapping $\hat{T}$: $\boldsymbol{F}_{2^r} \rightarrow \boldsymbol{F}_2$ so that $\hat{T}(\Phi(h)) = T(h)$ for all $h \in \boldsymbol{F}_2[X]/(q)$. Hence, the output sequence is given by the well-known formula $a_i = \hat{T}(\alpha^{-i}z)$ where $z \in \boldsymbol{F}_{2^r}$ is determined by the initial loading. If q is a primitive polynomial then the output sequence has maximal length and it is an m-sequence.

III. LFSR, Galois Architecture

In the Galois representation of Fig. 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. If $q_1, q_2, \ldots, q_r$ are the feedback multipliers then the recurrence equations are as follows:

$$a_i' = a_{i+1} + q_{i+1}a_0, \qquad \text{for } 0 \leq i \leq r-2$$
$$a_{r-1}' = q_r a_0.$$

Define the connection polynomial $q(X) = -1 + \sum_{i=1}^{r} q_i X^i$ and assume $q_r \neq 0$. Let $\boldsymbol{b} = (b_0, b_1, \ldots)$ be the output sequence.

Theorem 3.1: Suppose a (Galois) LFSR with connection polynomial q has initial loading $(a_0, a_1, \ldots, a_{r-1})$. Set

$$h(X) = a_0 + a_1 X + \cdots + a_{r-1}X^{r-1}. \tag{6}$$

Then the output sequence $\boldsymbol{b}$ is the coefficient sequence of the function $\beta(X) = -h(X)/q(X)$. Conversely, if $\boldsymbol{b} = b_0, b_1, \ldots$ is any strictly periodic sequence, let $\beta(X) = -h(X)/q(X)$ be its generating function. Then $q(X)$ is the connection polynomial of a (Galois) LFSR which generates the sequence, and $h(X)$ determines the initial loading by (6).

As in (5), define T: $R \rightarrow \boldsymbol{F}_2$ by $T(h) = h\ (\mathrm{mod}\, q)\ (\mathrm{mod}\, X)$. Assume $\deg(q) = r$. Define the mapping E: $\{\text{states}\} \rightarrow R$ which associates to each state $s = (a_{r-1}, a_{r-2}, \ldots, a_1, a_0)$ of the shift register the following element:

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

Theorem 3.2: The collection $\{R, E, T\}$ forms a projective model for the (Galois) LFSR with connection polynomial $q(X)$. The mapping E: $\{\text{states}\} \rightarrow R$ is a one-to-one correspondence such that the change of state is given by $h \mapsto X^{-1}h$. The output sequence is given by (2), that is,

$$b_i = (X^{-i}h)\,(\mathrm{mod}\, q)\,(\mathrm{mod}\, X). \tag{7}$$

IV. FCSR, Fibonacci Architecture

In the FCSR architecture [12], 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 $\sigma\,(\mathrm{mod}\, 2)$ 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. The output sequence is given by the following *linear recurrence with carry*:

$$2m_t + a_t = m_{t-1} + \sum_{i=0}^{r-1} q_i a_{t-i} \tag{8}$$

which can be solved for m_t and a_t since $a_t \in \{0, 1\}$. (The initial memory is $m = m_{r-1}$.) It was shown in [12] (and is easy to see from the preceding equations) that, for any initial nonnegative memory value m, the memory will decrease exponentially until it lies within the range $0 \leq m \leq \mathrm{wt}\,(q+1)$ 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 $1 + \lfloor \log_2(\mathrm{wt}\,(q+1)) \rfloor$ memory bits (see Fig. 3). Assume $q_r \neq 0$ and define the *connection integer*

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

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

$$\alpha = \sum_{i=0}^{\infty} a_i 2^i. \tag{9}$$

The set of all such power series forms a ring under the obvious operations of addition and multiplication; this is the ring $\boldsymbol{Z}_2$ of 2-adic integers (an elementary review of which is provided in [12]). The ring $\boldsymbol{Z}_2$ contains all fractions $\alpha = m/n$ with $m, n \in \boldsymbol{Z}$, provided that n is odd. The sequence $\boldsymbol{a}$ 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 $\alpha = -h/q$ with q odd and with $0 \leq h \leq q$. (cf. [12, Theorems 2.1 and 6.1], [17], [24, Theorem 15.5, p. 458]). In [12], we proved the following analog of Theorem 2.1, which describes the output of an FCSR.

Theorem 4.1: Suppose an FCSR with connection integer q of degree r has initial loading $(a_0, a_1, \ldots, a_{r-1})$ and initial memory m. Set

$$h = m2^r - \sum_{k=0}^{r-1} \sum_{i=0}^{k} q_i a_{k-i} 2^k \in \boldsymbol{Z} \tag{10}$$

where $q_0 = -1$. Then the output sequence is the coefficient sequence of the 2-adic number $\alpha = -h/q$. Conversely, if $\boldsymbol{a} = a_0, a_1, \ldots$ is any strictly periodic sequence, let $\alpha = -h/q$ be the corresponding 2-adic number. Then, q is the connection number of an FCSR which generates the sequence, and h determines the initial loading by (10).

Besides the all-zero state (the *bottom* state) there is another fixed state (the *top* state): take $a_i = 1$ $(0 \le i \le r-1)$ and $m = \mathrm{wt}\,(q+1) - 1$ where $\mathrm{wt}\,(q+1)$ is the Hamming weight of the binary expansion of $q+1$. The output is the sequence of all 1's. The associated 2-adic number is $\alpha = -1$.

Ring-Theoretic Model: Take $R = \boldsymbol{Z}/(q)$ with distinguished element $\beta = 2^{-1}$. Define

$$T\colon R \to \boldsymbol{Z}/(2) \quad \text{by} \quad T(h) = h(\mathrm{mod}\, q)\,(\mathrm{mod} 2). \tag{11}$$

This means that first the element h is represented by a number between 0 and $q-1$ and then this number is reduced modulo 2. (The mapping T is not a ring homomorphism and its definition depends on this particular choice of complete set of representatives in $\boldsymbol{Z}$ for the elements in R, consisting of the integers between 0 and $q-1$. This set of representatives is chosen because the 2-adic expansion of the resulting numbers $-h/q$ have strictly periodic coefficient sequences.)

Define $S\colon R \to \{\text{states}\}$ by assigning to any $h \in \boldsymbol{Z}/(q)$ the initial state with $a_i = 2^{-i}h(\mathrm{mod}\, q)\,(\mathrm{mod}\, 2)$ (for $0 \le i \le r-1$) and with initial memory

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

Theorem 4.2: Let q be an odd positive integer. The collection $\{R, S, T\}$ is an injective model for the FCSR with connection integer q. The mapping S is a one-to-one correspondence between the elements of $\boldsymbol{Z}/(q)$ and the strictly periodic states (except for the top state) such that the state change is given by $h \mapsto 2^{-1}h$. The output sequence is given by (2)

$$a_j = 2^{-j}h(\mathrm{mod}\, q)\,(\mathrm{mod}\, 2).$$

Remarks: The fact that S is a one-to-one correspondence follows from Theorem 4.1. If q is prime then $\boldsymbol{Z}/(q)$ is a field and its multiplicative group $(\boldsymbol{Z}/(q))^*$ is cyclic. In this case, 2^{-1} is a generator of $(\boldsymbol{Z}/(q))^*$ 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, which are in many ways analogous to the m-sequences generated by an LFSR [12].

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 $B = (2^{\phi(q)} - 1)/q$. Then $Bq \equiv -1 (\mathrm{mod}\, 2^{\phi(q)})$. But $r < \phi(q)$ so $Bq \equiv -1 (\mathrm{mod}\, 2^r)$ which gives

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

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.

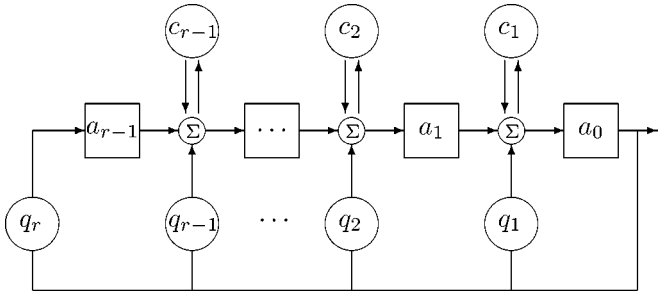

Fig. 4. Galois FCSR.

V. FCSR, Galois Architecture

The Galois representation [22] for an FCSR is illustrated in the Fig. 4.

Here, the bits $q_1, q_2, \ldots, q_r$ are multipliers. (We assume $q_r \neq 0$.) 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 jth adder, the following input bits are received: 1) a_j from the preceding cell, 2) $a_0 q_j$ from the feedback line, and 3) c_j from the memory cell. These are added to form a sum σ_j (with $1 \le j \le r-1$). At the next clock cycle, this sum modulo 2 is passed on to the next cell in the register, and the higher order bit is used to replace the memory

$$a'_{j-1} = \sigma_j \bmod 2 \quad \text{and} \quad c'_j = \sigma_j \operatorname{div} 2.$$

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

$$\begin{aligned} 2c'_j + a'_{j-1} &= a_0 q_j + a_j + c_j, \qquad \text{for } 1 \le j \le r-1 \\ a'_{r-1} &= q_r a_0. \end{aligned} \tag{12}$$

To analyze the behavior of this circuit, define the *connection integer*

$$q = -1 + q_1 2 + q_2 2^2 + \cdots + q_r 2^r. \tag{13}$$

The following result is an analog of Theorem 2.1.

Theorem 5.1: Suppose an r-stage (Galois)-FCSR with connection integer q has initial loading with register and

memory contents $(a_0, a_1, \ldots, a_{r-1})$ and $(c_1, c_2, \ldots, c_{r-1})$, respectively. Set

$$h = a_0 + (a_1 + c_1)2 + \cdots + (a_{r-1} + c_{r-1})2^{r-1}. \quad (14)$$

Then the output sequence $b_0, b_1, b_2 \cdots$ of the FCSR is the coefficient sequence for the 2-adic expansion of the rational number $\beta = -h/q$. Conversely, if $\boldsymbol{b} = b_0, b_1, \ldots$ is any strictly periodic sequence let $\beta = -h/q$ be the corresponding 2-adic number. Then q is the connection integer of a (Galois) FCSR which generates the sequence, and h determines the initial loading by (14).

Proof: 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 $qB + h \in \boldsymbol{Z}_2$ is divisible by 2 (meaning that it has no constant term). In fact

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

The constant term in $qB + h$ is $-b_0 + a_0$. 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 (12). 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 preceding 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. □

There are two stable states: the all-zero state (or *bottom* state), and the *top* state where $a_i = 1$ for $0 \le i \le r-1$ and $c_i = q_i$ for $1 \le i \le r-1$. The output of the top state is the all-one sequence. For any periodic state other than the top state, if $q_j = 0$ then the memory cell c_j will eventually drop to 0 and will remain 0 forever after. So the periodic states must satisfy $c_j = 0$ whenever $q_j = 0$. Let us say that a state satisfying this condition $(c_j \le q_j)$ is an "admissible" state. The admissible states may be thought of as the set of all states of a Galois-FCSR in which memory cells c_j are provided only when the corresponding feedback tap q_j is nonzero.

Now we wish to describe a model for the (Galois)-FCSR. Define $R = \boldsymbol{Z}/(q)$ and $T: R \to \boldsymbol{Z}/(2)$ as in (11). Define E: {states} $\to \boldsymbol{Z}/(q)$ 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 $h (\mathrm{mod}\, q)$, where h is defined in (14).

Theorem 5.2: The collection $\{R, E, T\}$ is a projective model for the Galois-FCSR with connection integer q. For any admissible initial loading, the output of the Galois-FCSR is strictly periodic. The mapping E defines an onto mapping from the set of admissible states (except for the top state) of the FCSR to the elements of $\boldsymbol{Z}/(q)$, such that the change of state is given by $h \mapsto 2^{-1}h$. Hence, the output sequence is given by (2), that is,

$$b_j = 2^{-j} h (\mathrm{mod}\, q) (\mathrm{mod}\, 2).$$

Proof: The greatest possible value for h is when all $a_i = 1$ and all the admissible $c_j = 1$ in which case $c_j = q_j$ for all j, so

$$\begin{aligned} h &= 1 + (1 + q_1)2 + \cdots + (1 + q_{r-1})2^{r-1} \\ &= 2^r - 1 + q + 1 - q_r 2^r = q. \end{aligned}$$

So, for any admissible state s, we have: $0 \le h = E(s) \le q$. It is easy to see that any such h may be realized by an admissible state, hence, the mapping E is onto. If $0 \le h \le q$, the 2-adic expansion for $-h/q$ (which is the output sequence of the shift register initialized at any admissible state) is strictly periodic. Reducing (13) modulo q and multiplying by 2^{-1} gives

$$2^{-1} = q_1 + q_2 2 + q_3 2^2 + \cdots + q_r 2^{r-1} \ (\mathrm{mod}\, q) \quad (15)$$

so

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

which describes the change of state. □

Corollary 5.3: There is an onto function from the set of periodic (admissible) 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: We do not know a simple formula describing the contents of the kth cell as a function of time. Despite Theorem 5.2, 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 (admissible) 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.

VI. d-FCSR, Fibonacci Architecture

The d-FCSR architecture was introduced in [12] and [14], where its basic properties are listed (see also [17]). d-FCSR sequences are important because they exhibit approximately uniform distribution of k-tuples for all $k \le k_0$ (where k_0 is easily

determined from the parameters of the register) [8]. In this section, we recall the operation of these shift registers and summarize the results from [6] which explain how to design them so as to give predictable outputs. 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.

This is best understood using the ring $\boldsymbol{Z}[\pi]$ which consists of polynomials in π (with integer coefficients), subject to the formal relation $\pi^d = 2$. The ring $\boldsymbol{Z}[\pi]$ contains the integers $\boldsymbol{Z}$ and it can be embedded as a subring of the real numbers $\boldsymbol{R}$ by mapping π to the positive $\sqrt[d]{2}$. However, there are also other embeddings into the complex numbers. Any $z \in \boldsymbol{Z}[\pi]$ may be uniquely expressed as a polynomial

$$z = z_0 + z_1\pi + \cdots + z_{d-1}\pi^{d-1}$$

with $z_i \in \boldsymbol{Z}$ 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 $z \in \boldsymbol{Z}[\pi]$ 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 $\boldsymbol{F}_2$. The operations $(\bmod \pi)$ and $(\operatorname{div} \pi)$ make sense in this ring. If $z = z_0 + z_1\pi + \cdots + z_{d-1}\pi^{d-1}$ then

$$z \,(\bmod \pi) = z_0 \,(\bmod 2) \in \boldsymbol{F}_2$$

and we will say that z is *odd* if $z \,(\bmod \pi) = 1$. (For example, $-1 = 1 - \pi^d$ so $-1 \,(\bmod \pi) = 1$.) 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

$$m = m_0 + m_1\pi + \cdots + m_s\pi^s \in \boldsymbol{Z}[\pi].$$

Associated to the feedback connections we define the connection "number"

$$q = -1 + q_1\pi + q_2\pi^2 + \cdots + q_r\pi^r. \tag{16}$$

Then $q \in \boldsymbol{Z}[\pi]$ is odd, and $q+1$ is nonnegative. The output sequence is given by the *linear recurrence with delayed carry*

$$\pi m_t + a_t = m_{t-1} + \sum_{i=0}^{r-1} q_i a_{t-i} \tag{17}$$

with initial memory $m = m_{r-1}$. This equation can be solved for m_t and a_t since $a_t \in \{0, 1\}$.

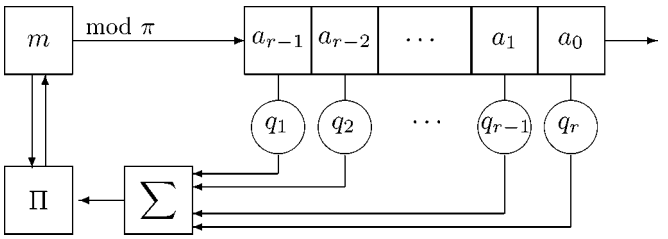

Fig. 5. Fibonacci d-FCSR.

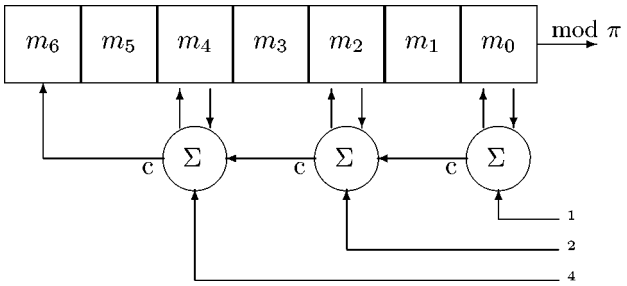

Fig. 6. A $\boldsymbol{Z}[\pi]$ adder for $d = 2$.

To be explicit, 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 $\boldsymbol{Z}[\pi]$, that is, as a polynomial with $0, 1$ coefficients in π, using $2 = \pi^d$. (It is this fact which gives rise to the delay by d steps in the carry operation.) Using addition in $\boldsymbol{Z}[\pi]$ form the (nonnegative) sum $\sigma = m + \sigma'$. Shift the contents of the register cells to the right by one step. Place the bit $a_r = \sigma \,(\bmod \pi)$ 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 $a_i' = a_{i+1}$ for $0 \leq i \leq r-1$ and

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

which shows that the output is given by (17).

Implementation: The block diagram for a d-FCSR is the same as that of an FCSR, but since addition in $\boldsymbol{Z}[\pi]$ is needed, it is slightly more convenient to break the addition into two parts as in Fig. 5. 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 $\boldsymbol{Z}[\pi]$.

For $d = 2$, the $\boldsymbol{Z}[\pi]$ adder Π, together with the memory m may be described as follows. Each symbol Σ represents a full adder with three 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 $\sigma \,(\bmod \pi)$ 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 $\operatorname{wt}(q+1)$ denote the number of nonzero q's involved in the feedback. It is easy to see from Fig. 6 (or from the change of state equations above) that the memory will decrease until $m_i = 0$ for all $i > d\log_2(\operatorname{wt}(q+1)) + d$, so no memory overflow will occur provided the shift register is provided with memory

cells $m_0, m_1, \ldots, m_s$ where $s \geq d\log_2(\mathrm{wt}\,(q+1)) + d$. The deeper analysis of a d-FCSR is completely parallel to that of an FCSR, however, some less familiar mathematics is needed.

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

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i \tag{18}$$

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

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

we see that $\boldsymbol{Z}_\pi$ also contains $\boldsymbol{Z}[\pi]$. In fact, $\boldsymbol{Z}_\pi$ contains all fractions $\alpha = a/b$ with $a, b \in \boldsymbol{Z}[\pi]$ provided that b is odd (meaning that $b\,(\mathrm{mod}\,\pi) = 1$), in which case we shall refer to (18) as "the" π-adic expansion of a/b. Such fractions are precisely the elements of $\boldsymbol{Z}_\pi$ whose π-adic expansions are eventually periodic. The following result was proven in [14].

Theorem 6.1: Suppose a 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 $\boldsymbol{a} = (a_0, a_1, \ldots)$ is a strictly 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. □

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 entries q_i, m_i are permitted to take values in $\{\pm 1, 0\}$. It is easy to see that no "overflow" will ever occur and that *any* $q \in \boldsymbol{Z}[\pi]$ may be realized as the connection number of such a polarized d-FCSR.

Strictly Periodic π-adic Expansions: One of the main results in [6] is a characterization of the strictly periodic sequences. Let $\boldsymbol{Q}[\pi]$ be the d-dimensional vectorspace (over $\boldsymbol{Q}$) with basis $\{1, \pi, \pi^2, \ldots, \pi^{d-1}\}$. In fact, it is the fraction field of $\boldsymbol{Z}[\pi]$ and it is a totally ramified degree d extension of the rational numbers $\boldsymbol{Q}$ [9, Ch. 12]. However, we will not need these facts in this paper. Let $\tau\colon \boldsymbol{Q}[\pi] \to \boldsymbol{Q}^d$ be the vector-space 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 $\tau(\boldsymbol{Z}[\pi])$ consists of all points in $\boldsymbol{Q}^d$ with integer coordinates, so we will refer to $\boldsymbol{Z}[\pi]$ as the set of *lattice points* in $\boldsymbol{Q}[\pi]$.

Fix $q \in \boldsymbol{Z}[\pi]$. Recall that the *norm* $N(q)$ of q is the determinant of the action given by multiplication by q on the vector space $\boldsymbol{Q}[\pi]$. 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 $q \in \boldsymbol{Z}[\pi]$ is odd if and only if its norm $N(q) \in \boldsymbol{Z}$ is odd. Let (q) denote the ideal in $\boldsymbol{Z}[\pi]$ generated by $q \in \boldsymbol{Z}[\pi]$ and let $R = \boldsymbol{Z}[\pi]/(q)$ denote the quotient ring. The number of elements in the ring R is $|N(q)|$. If $z \in \boldsymbol{Z}[\pi]$, we denote by $z\,(\mathrm{mod}\,q)$ 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 $\boldsymbol{Q}^d$, let us denote the (half-open) *parallelepiped spanned by* E to be the set

$$P(E) = \left\{ \sum_{i=1}^{k} a_i e_i \,\middle|\, 0 \leq a_i < 1 \right\}. \tag{19}$$

Let

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

be the set of lattice points in the parallelepiped (in $\boldsymbol{Q}[\pi]$) which is spanned by the set of vectors $\{q, q\pi, q\pi^2, \ldots, q\pi^{d-1}\}$. In [6], we proved the following result.

Theorem 6.2: Suppose that $h, q \in \boldsymbol{Z}[\pi]$ and that q is odd. Then the π-adic expansion of the fraction $\alpha = -h/q$ is strictly periodic if and only if $h \in \Delta$. Moreover, the mapping $\boldsymbol{Z}[\pi] \to \boldsymbol{Z}[\pi]/(q)$ induces a one-to-one correspondence

$$\Delta \leftrightarrow \boldsymbol{Z}[\pi]/(q). \tag{20}$$

Remarks: Theorem 6.2 says that the set Δ is a complete set of representatives for the elements of $\boldsymbol{Z}[\pi]/(q)$. A *face* $F \subset P$ of the parallelepiped (19) is the set of points obtained by setting some of the coefficients $a_j = 0$. The set of lattice points $\Delta \cap F$ in any face corresponds under (20) to an additive subgroup of $\boldsymbol{Z}[\pi]/(q)$. If $\boldsymbol{Z}[\pi]/(q)$ is a prime field then there are no additive subgroups other than $\{0\}$, in which case all the nonzero elements of Δ lie in the interior of the parallelepiped.

Ring-Theoretic Model: Take $R = \boldsymbol{Z}[\pi]/(q)$. Using the set Δ we can define a mapping

$$T\colon R \to \boldsymbol{F}_2 \quad \text{by} \quad T(h) = h\,(\mathrm{mod}\,q)\,(\mathrm{mod}\,\pi). \tag{21}$$

This means that h must first be replaced by the corresponding element in the complete set of representatives Δ, then this element is reduced modulo π to obtain an element of $\boldsymbol{Z}[\pi]/(\pi) = \boldsymbol{Z}/(2)$. Define $S\colon R \to \{\text{states}\}$ to be the mapping which associates to $h \in R$ the initial loading $a_i = \pi^{-i} h\,(\mathrm{mod}\,q)\,(\mathrm{mod}\,\pi)$ for $0 \leq i \leq r-1$ and the initial memory

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

Theorem 6.3: Let $q \in \boldsymbol{Z}[\pi]$ and suppose $q+1$ is nonnegative. Then the collection $\{R, S, T\}$ is an injective model for the

d-FCSR with connection number q. The state change is given by $h \mapsto \pi^{-1}h$ and the output sequence is

$$a_i = \pi^{-i}h \,(\mathrm{mod}\, q)\,(\mathrm{mod}\, \pi). \tag{22}$$

This result (whose proof may be found in [6] or [14]) has the disadvantage that computations in the somewhat mysterious ring $\boldsymbol{Z}[\pi]/(q)$ may be rather messy. However, in certain cases it is possible to identify this ring with the much simpler object $\boldsymbol{Z}/(N)$. In [6] we proved the following lemma.

Lemma 6.4: Suppose $q \in \boldsymbol{Z}[\pi]$ is odd and that $N = |N(q)|$ is prime. Then the natural composition $\boldsymbol{Z} \to \boldsymbol{Z}[\pi] \to \boldsymbol{Z}[\pi]/(q)$ induces an isomorphism of rings

$$\boldsymbol{Z}/N \cong \boldsymbol{Z}[\pi]/(q). \tag{23}$$

It follows that the output sequence (22) can be described as $a_i = b^{-i} \,(\mathrm{mod}\, N)\,(\mathrm{mod}\, 2)$ (up to a shift) for some $b \in \boldsymbol{Z}/(N)$, not necessarily equal to 2. In the next paragraph, we determine this "base" b and the shift.

Let ψ: $\boldsymbol{Z}[\pi]/(q) \to \boldsymbol{Z}/(N)$ denote the inverse to the isomorphism (23). It is completely determined by the single integer $b = \psi(\pi)$ because for any integers c_i (with $0 \le i \le d-1$), the mapping ψ satisfies

$$\psi\left(\sum_{i=0}^{d-1} c_i \pi^i\right) = \sum_{i=0}^{d-1} c_i b^i.$$

The prime number N may be considered as an element of $\boldsymbol{Z}[\pi]$ and as such, it turns out to be divisible by π (see [6]). Define $s_i \in \boldsymbol{Z}$ by expanding

$$\delta = N(q)/q = \sum_{i=0}^{d-1} s_i \pi^i. \tag{24}$$

The following result is proven in [6].

Theorem 6.5: Let $h, q \in \boldsymbol{Z}[\pi]$. Suppose that $N = |N(q)|$ is an odd prime number and that $h \in \Delta$ lies in the strictly periodic region described in Theorem 6.2. Let $b = \psi(\pi)$. Let $A = s_0\psi(h) \in \boldsymbol{Z}/(N)$ where s_0 is defined by (24). Then, for all j, the following equation holds:

$$\pi^{-j}h \,(\mathrm{mod}\, q)\,(\mathrm{mod}\, \pi) = b^{-j}A \,(\mathrm{mod}\, N)\,(\mathrm{mod}\, 2).$$

Thus, the output sequence (22) may be simply described as $Ab^{-j} \,(\mathrm{mod}\, N)\,(\mathrm{mod}\, 2)$. If $b \equiv 2^k \,(\mathrm{mod}\, N)$ then we arrive at the surprising conclusion that the d-FCSR sequence $\boldsymbol{b}$ is the k-fold decimation of the (ordinary) FCSR sequence with connection integer N. The numbers b and s_0 can be computed directly from knowledge of q. For $d = 2$ and $d = 3$ these computations give Table I

TABLE I
PARAMETERS OF $\boldsymbol{Z}[\pi]$

	$d=2$	$d=3$
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	$q_0 - q_1\pi$	$(q_0^2 - q_1q_2) + (2q_2^2 - q_0q_1)\pi$ $+(q_1^2 - q_0q_2)\pi^2$
b	$-2q_1/q_0$	$2(q_1^2 - q_0q_2)/(q_0^2 - q_1q_2)$
s_0	q_0	$q_0^2 - q_1q_2$

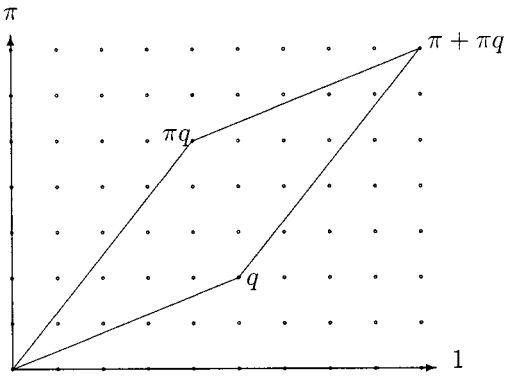

Fig. 7. Parallelogram for $q = 5 + 2\pi$.

An Example: Consider the d-FCSR with $d = 2$ and $q = 5+2\pi$. The shift register is four-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 Fig. 7.

The isomorphism ψ: $\boldsymbol{Z}[\pi]/(q) \to \boldsymbol{Z}/(17)$ maps π to $b = 6$, which is primitive modulo 17, so we obtain a maximal length output sequence. Each element in $\boldsymbol{Z}[\pi]/(q)$ has a unique representative h in the above parallelogram; these representatives are listed in the second column of Table II. Note that the second column modulo π coincides with the third column modulo 2 as predicted by the theorem.

TABLE II
MODEL STATES FOR $q = 5 + 2\pi$

i	$\pi^{-i} \,(\mathrm{mod}\,(q))$	$5 \cdot 6^{-i} (\mathrm{mod}\ 17)$	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

VII. d-FCSR, GALOIS ARCHITECTURE

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.)

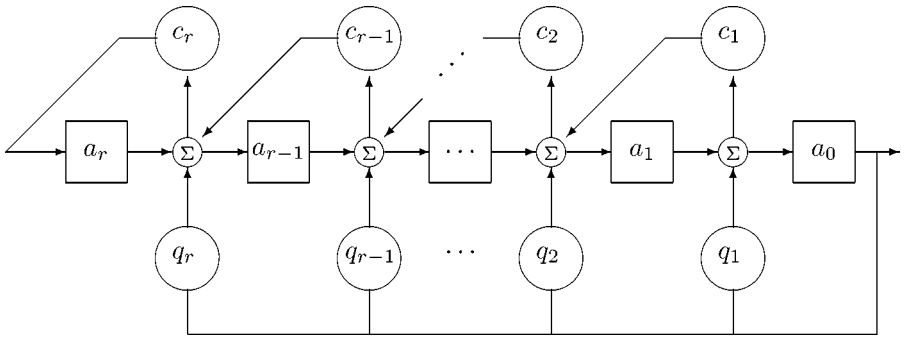

Fig. 8. Galois 2-FCSR.

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 $a_0, \ldots, a_{r+d-2}$ are evidently needed since c_r will feed into a_{r+d-2}. This is illustrated in Fig. 8 for $d = 2$. If $d \geq 3$, the situation is more complicated and an indeterminate number t of "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 "Memory Considerations" subsection in the following text), 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 general (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,

$$2c'_j + a'_{j-1} = a_0 q_j + a_j + c_{j-d+1}, \qquad \text{for } 1 \leq j \leq r+t+d-1. \quad (25)$$

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

Assume $q_r \neq 0$ and define the connection number

$$q = -1 + \sum_{i=1}^{r} q_i \pi^i \in \boldsymbol{Z}[\pi]. \quad (26)$$

Theorem 7.1: Suppose a Galois d-FCSR with connection number $q \in \boldsymbol{Z}[\pi]$ has initial loading $(a_0, \ldots, a_{r+t+d-2}; c_1, c_2, \ldots, c_{r+t})$. Set

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

If t is sufficiently large (as described in "Memory Considerations" below) then no memory overflow will occur, and the output sequence $\boldsymbol{b} = (b_0, b_1, \ldots)$ coincides with the π-adic expansion of the fraction $-h/q \in \boldsymbol{Z}_\pi$. Conversely, if $\boldsymbol{b} = (b_0, b_1, \ldots)$ is a periodic sequence with corresponding π-adic number $\beta = -h/q$ and if $q+1$ is nonnegative, then q is the connection number of a Galois d-FCSR which generates the sequence $\boldsymbol{b}$.

Proof: 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 (25), and hence a new h'. Compute that $\pi B' = (B - b_0) \in \boldsymbol{Z}[\pi]$ and $\pi h' = (h + a_0 q) \in \boldsymbol{Z}[\pi]$ hence

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

By the same argument as above, the constant term of $qB' + h'$ vanishes as well, 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, $qB + h = 0$. This proves the first statement. The converse is similar. The bound on the memory is proven below under "memory considerations." □

Ring-Theoretic Model: Consider a Galois d-FCSR with connection number $q \in \boldsymbol{Z}[\pi]$. Let $R = \boldsymbol{Z}[\pi]/(q)$ and define $T: R \to \boldsymbol{Z}/(2)$ as in (21). Define E: $\{\text{states}\} \to R$ to be the mapping which assigns to any state s the element $h \,(\mathrm{mod}\, q) \in \boldsymbol{Z}[\pi]/(q)$ of (27). The proof of the following theorem is identical to that of Theorem 5.2.

Theorem 7.2: The collection $\{R, E, T\}$ is a projective model for the Galois d-FCSR with connection number q. The change of state is given by $h \mapsto \pi^{-1} h$. Hence, the output sequence is

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

Corollary 7.3: There is a mapping from the set of periodic states of the Fibonacci d-FCSR with connection number q to the set of periodic states of the Galois d-FCSR with connection number q so that corresponding states produce the same output.

Of course, Theorem 6.5 also applies in the Galois case.

Corollary 7.4: Suppose a Galois d-FCSR with connection number

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

is chosen such that $N = |N(q)| \in \boldsymbol{Z}$ is a prime number. Suppose the initial loading is chosen so that (27) $h \in \Delta$ lies in the set of strictly periodic elements (Theorem 6.2). Then the output sequence $\{b_0, b_1, b_2, \ldots\}$ of the d-FCSR is given by

$$b_i = b^{-i} A \pmod N \pmod 2$$

where $b = \psi(\pi)$ and $A = s_0\psi(h) \in \boldsymbol{Z}/(N)$.

Memory Considerations: In this subsection, we make use of some ideas from [17]. Consider a (Galois) d-FCSR as described at the beginning of this section, with feedback multipliers $q_1, \ldots, q_r$, memory cells $c_1, \ldots, \ldots c_{r+t}$, and register cells $a_0, \ldots, a_{r+t+d-2}$. Let $\pi^d = 2$ and define $q \in \boldsymbol{Z}[\pi]$ by (26).

Let us denote the standard embedding $\boldsymbol{Z}[\pi] \to \boldsymbol{R}$ (which maps π to the positive $\sqrt[d]{2}$) by $x \mapsto |x|$. Recall that an element $x = \sum_{i=o}^{m} x_i \pi^i \in \boldsymbol{Z}[\pi]$ is *positive* if each of the coefficients $x_i \geq 0$. This implies (but is not implied by) that $|x| \geq 0$. For a given positive-real number R, there may be infinitely many elements $x \in \boldsymbol{Z}[\pi]$ such that $|x| \leq R$, however, there are only finitely many *positive* such elements x. In this subsection we show that 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 [17], the fact that $|\pi| > 1$ is crucial.)

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. Let $(a'_0, \ldots, a'_{r+t+d-2}; c'_1, \ldots, c'_{r+t})$ denote the next state of the shift register with corresponding value $h' \in \boldsymbol{Z}[\pi]$. 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 $|h| > \frac{|q|}{|\pi|-1}$ then $|h'| < |h|$, meaning that 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 accommodate all such values of h. (The following estimates can be easily 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. □

A deeper result of Klapper and Xu [17] states that even if negative coefficients are permitted in the register contents, the memory will nevertheless remain bounded.

Our understanding of the Galois d-FCSR architecture still leaves much to be desired. We do not know how to intrinsically characterize the strictly periodic states. We do not even 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 contents of each cell as a function of time.

VIII. Conclusion

We have found a "Galois" representation for FCSR and d-FCSR pseudorandom sequence generators. We have constructed "models" for the behavior of 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, 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 $a_i = Ab^{-i} \pmod N \pmod 2$.

Acknowledgment

The authors would like to thank the Institute for Advanced Study in Princeton, NJ for its hospitality and support while this paper was being prepared.

References

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

[2] ——, "Distribution properties of multiply-with-carry random number generators," *Math. Comp.*, vol. 66, pp. 591–607, 1997.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: Elsevier/North-Holland, 1998.

[4] L. E. Dickson, *History of the Theory of Numbers*. Washington, DC: Carnegie Inst., 1919, vol. 1. Reprinted by Chelsea and published by American Mathematical Society, 1966.

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

[6] M. Goresky and A. Klapper, "Periodicity and arithmetic correlations of algebraic feedback shift register sequences over ramified extensions of the rationals," preprint.

[7] M. Goresky, A. M. Klapper, and L. Washington, "Fourier transforms and the 2-adic span of periodic binary sequences," *IEEE Trans. Inform. Theory*, vol. 46, pp. 687–691, Mar. 2000.

[8] M. Goresky and A. Klapper, "Distributional properties of d-FCSR sequences," manuscript, to be published.

[9] K. Ireland and M. Rosen, "A classical introduction to modern number theory," in *Graduate Texts in Mathematics*. New York: Springer-Verlag, 1990, vol. 84.

[10] E. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 732–736, Nov. 1976.

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

[12] A. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," *J. Cryptogr.*, vol. 10, pp. 111–147, 1997.

[13] M. Goresky and A. M. Klapper, "Arithmetic crosscorrelation of feedback with carry shift regiseter sequences," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1342–1346, July 1997.

[14] ——, "Feedback registers based on ramified extensions of the 2-adic numbers," in *Advances in Cryptology—Eurocrypt 1994 (Lecture Notes in Computer Science)*. New York: Springer Verlag, 1994, vol. 718, pp. 215–222.

[15] ——, "Large period nearly de Bruijn sequences," in *Advances in Cryptology—Eurocrypt 1996 (Lecture Notes in Computer Science)*. New York: Springer Verlag, 1995, vol. 921, pp. 263–273.

[16] ——, "Cryptanalysis based on 2-adic rational approximation," in *Advances in Cryptology—Crypto '95 (Lecture Notes in Computer Science)*. New York: Springer Verlag, 1995, vol. 963, pp. 262–273.

[17] A. Klapper and J. Xu, "Algebraic feedback shift registers," *Theor. Comp. Sci.*, vol. 226, pp. 61–93, 1999.

[18] ——, "Feedback with carry shift registers over $\boldsymbol{Z}/(N)$," in *Proc. Int. Conf. Sequences and Their Applications, Singapore, Dec. 1998*. New York: Springer-Verlag, to be published.

[19] ——, "Register synthesis for algebraic feedback shift registers based on nonprimes," manuscript, submitted for publication.

[20] R. Lidl and H. Niederreiter, *Finite Fields Encyclopedia of Mathematics*. Cambridge, U.K.: Cambridge Univ. Press, 1983, vol. 20.

[21] R. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer Academic, 1987.

[22] J. Noras, "Fast pseudorandom sequence generators: Linear feedback shift registers, cellular automata, and carry feedback shift registers," Univ. Bradford Elec. Eng. Dept., Bradford, U.K., Rep. 94, 1997.

[23] W. W. Peterson, "Encoding and error-correction procedure for the Bose–Chaudhuri codes," *IRE Trans. Inform. Theory*, vol. IT-6, pp. 459–470, Sept. 1960.

[24] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[25] B. Schneier, *Applied Cryptography*, 2nd ed. New York: Wiley, 1996.

[26] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*, 2nd ed. New York: McGraw-Hill, 1994.