PN Sequence Generation from 2-D Array of Shift Registers

Hyun Jung Kim, Inkyu Lee, and Woonkyung M. Kim

Toward code division multiple access (CDMA) communications and data protection, we propose and analyze pseudorandom noise (PN) sequences generated from a 2-dimensional array structure of shift-registers. For any positive integers *m* and *n*, we construct PN sequences of period 2^{mn}–1 using an *m*×*n* array of registers and show that we can generate all shifted PN sequences as required by IS-95x with the proper linear combination of available sequences.

Keywords: Pseudorandom noise codes, DS/CDMA system, multimedia communication, encryption/decryption.

I. Introduction

Binary sequences that satisfy recursions over the Galois field with two elements ($GF(2)$) are easy to generate and can have special properties such as balance, correlation, and shift [1],[2] toward their successful applications in acquisition, tracking, and orthogonal modulation/demodulation of digital communications [3],[4].

Binary sequences of maximum period 2^n-1 that are generated by linear recursions over $GF(2)$ of order $n \geq 1$ are called binary maximal-sequences or pseudorandom noise (PN) sequences. A class of generalized PN sequences over $GF(p^m)$ with good correlation properties (with p being an arbitrary prime number and m an arbitrary positive integer) are often constructed and utilized [5]-[6].

Generalizing the conventional 1-dimensional (1-D) simple shift register generator (SSRG) structure for the generation of PN sequences [2], we propose and exclusively analyze the 2-D shift register structure (2DSRS) of Fig. 1, which depicts an $m \times n$ array of registers configured as a series feedback connection. Using the 2DSRS, we can generate PN sequences over $GF(2)$[1] or, alternatively, PN sequences over $GF(2^m)$.[2]

Analyzing the 2DSRS, we can build foundations for many new applications relating to the IS-95x code division multiple access (CDMA) paradigm [7]. In particular, by a state-space analysis of this formulation, we show that 2DSRS's latency, concurrency and synchronicity advantages can be exploited in numerous communications-related applications as typically found in CDMA and other scrambling environments. In this paper, we focus on the cases where the connections are selected to produce

Manuscript received Oct. 17, 2003; revised Apr. 8, 2005.

This project was supported by Grant No. R01-2002-000-00404-0 from the Basic Research Program of the Korea Science and Engineering Foundation.

Hyun Jung Kim (phone: +82 2 3290 3690, email: hjkim@korea.ac.kr), Inkyu Lee (email: inkyu@korea.ac.kr), Woonkyung M. Kim (email: mwkim@korea.ac.kr) are with Department of Radio Sciences and Engineering, Korea University, Seoul, Korea.

1) For example, the 0/1-valued sequences as generated over time in any particular register.

2) For example, the vector-valued representation sequences as generated over time by each $m \times 1$ vertically-aligned registers.

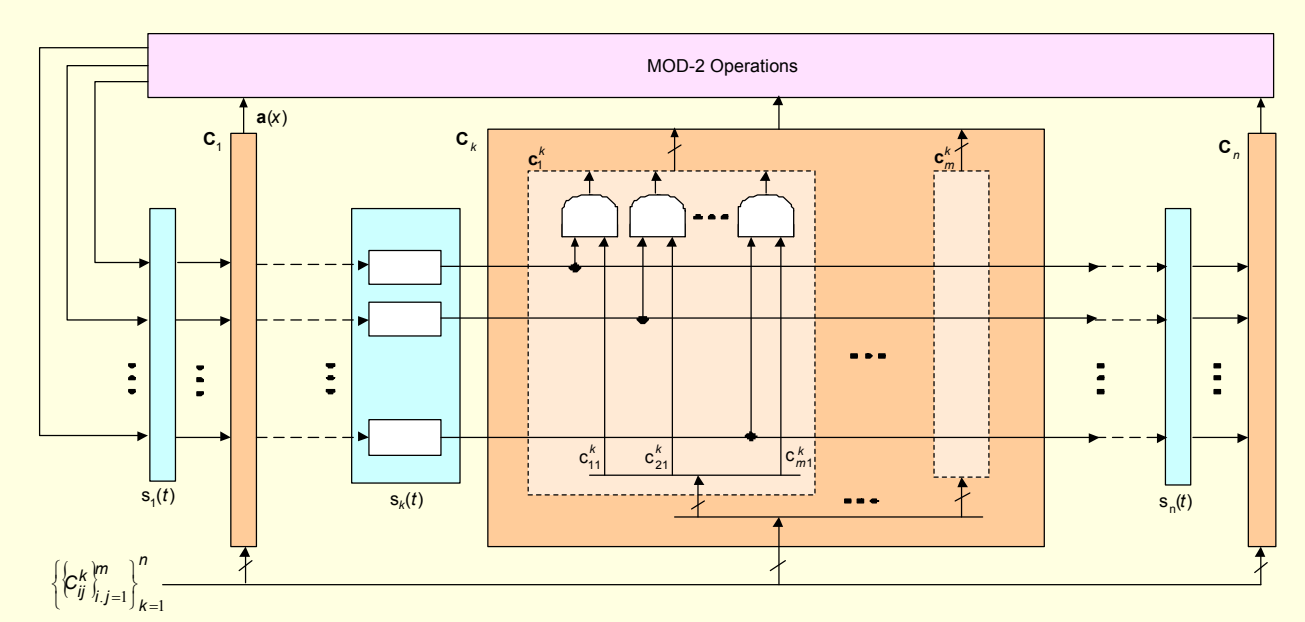

Fig. 1. 2DSRS.

PN sequences which have natural applications for CDMA [7] communications and image and video scrambling [8].

After providing a (matrix) dynamical system problem formulation of the 2DSRS in the context of a more general architecture in section II, we utilize the generation of function-based analyses to derive some fundamental properties of the associated sequences in the shift registers in section III. After providing some design examples in section IV, we conclude the paper with some comments on its significance with respect to theory and applications in section V.

II. Problem Formulation

For arbitrary (henceforth, fixed) positive integers m and n, we first consider an arbitrarily linearly networked connection called a 2-D general register structure (2DGRS) involving an $m \times n$ array of registers.

Utilizing the dynamical system method [9], we denote the overall state at each time $t \in Z^+$ of the 2DSRS by the mn-dimensional column vector, $\mathbf{s}(t)$,

$$\mathbf{s}(t) = [\mathbf{s}_1(t)^T \mathbf{s}_2(t)^T \ldots \mathbf{s}_n(t)^T]^T = [s_1^1(t) \ldots s_m^1(t) \ldots s_1^n(t) \ldots s_m^n(t)]^T \tag{1}$$

consisting of n m-dimensional column subvectors, $\mathbf{s}_i(t)$, each representing the state of the i-th vertically-aligned registers[3] (VARs) at time $t \in Z^+$ lying in (field F-induced) vector space $(F^n, F) = (\{0,1\}^n, \{0,1\})$ with field operations.[4] The feedback dynamics of the 2DGRS—reflecting on the GMW sequence construction [10]—can be modeled by an autonomous dynamical equation, and the output can be assumed to be generated via an mn-dimensional masking[5] column vector consisting of n m-dimensional masking column subvectors $\{\mathbf{d}_j\}_{j=1}^n$:

$$\mathbf{d} = [\mathbf{d}_1^T \mathbf{d}_2^T \ldots \mathbf{d}_n^T]^T = [d_1^1 \ldots d_m^1 \ldots d_1^n \ldots d_m^n]^T. \tag{2}$$

We then have the following dynamical system equations with state and output equations, involving the $mn \times mn$ state transition matrix $\mathbf{Q}$ which consists of n^2 $m \times m$ feedback matrices $\{\mathbf{Q}_{ij}\}_{i,j=1}^n$.

With $\mathbf{s}(0)$ given, for all $t \in Z^+$,

$$\mathbf{s}(t+1) = \begin{bmatrix} \mathbf{Q}_{11} & \mathbf{Q}_{12} & \cdots & \cdots & \mathbf{Q}_{1n} \\ \mathbf{Q}_{21} & \mathbf{Q}_{22} & & \cdots & \mathbf{Q}_{2n} \\ \mathbf{Q}_{31} & \mathbf{Q}_{32} & & \cdots & \mathbf{Q}_{3n} \\ \vdots & & \ddots & \ddots & \vdots \\ \mathbf{Q}_{(n-1)1} & & \cdots & & \\ \mathbf{Q}_{n1} & \mathbf{Q}_{n2} & \cdots & & \mathbf{Q}_{nn} \end{bmatrix} \mathbf{s}(t) = \mathbf{Q}\mathbf{s}(t), \tag{3}$$

3) For example, i-th column of the $m \times n$ array of registers.

4) For example, all addition and multiplication field operations in this paper are mod-2 addition and multiplication, respectively.

5) This (linear combination) formulation encompasses most applications pertaining to IS-95x communications and scrambling employment.

$$y(t;\mathbf{d})=\mathbf{d}^T\mathbf{s}(t). \quad (4)$$

It is clear from [9] that the dynamical system equations as defined by (3) and (4) have solutions as determined by state transition matrix **Q** and initial conditions **s**(0).

Recall that the feedback connections of Fig. 1, denoted by the collection of n $m\times m$ connection matrices $\{\mathbf{C}_k\}_{k=1}^n$, may also be enumerated as either a collection $\{\{\mathbf{c}_j^k\}_{j=1}^m\}_{k=1}^n$ of m-dimensional column vectors called connection vectors or a collection of $\{\{c_{ij}^k\}_{i,j=1}^m\}_{k=1}^n$ with connection values 0 or 1, as depicted in detail by the (magnified) gray area in Fig. 1.

Observation 1.

The 2DSRS is a special instance of the 2DGRS.

Proof. The 2DSRS with the connection matrices $\{\mathbf{C}_k\}_{k=1}^n$ is a 2DGRS with

$$\mathbf{Q}_{ij}=\begin{cases}\mathbf{C}_j, & \text{for } i=1,\ j=1,\ldots,n\\ \mathbf{I}, & \text{for } i=2,\ldots,n,\ j=i-1,\\ \mathbf{0}, & \text{otherwise}\end{cases}$$

so that

$$\mathbf{Q}=\begin{bmatrix}\mathbf{C}_1 & \mathbf{C}_2 & \cdots & \cdots & \mathbf{C}_n\\ \mathbf{I} & \mathbf{0} & \cdots & & \mathbf{0}\\ \mathbf{0} & \mathbf{I} & \cdots & & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{0}\end{bmatrix}=\mathbf{Q}_{2DSRS}. \quad (5)\ \square$$

In the next section, we will analyze the 2DSRS using the 2DGRS formulation.

III. Analysis

In this section—as was true in the classical derivation [3] and paralleling our comments following (3) and (4)—we derive the generating functions from the 2DSRS's VARs. We also derive outputs as functions of connection matrices[6] $\{\mathbf{C}_k\}_{k=1}^n$ and initial conditions[7] **s**(0). Then, we verify that all of the involved sequences become PN sequences under appropriate conditions on the connection topology.

With the indeterminate variable x and, as depicted in Fig. 1, the generating function $\mathbf{s}_1(x)$ corresponds to the m-dimensional column vector-valued sequence out of the leftmost VAR and is written as

$$\mathbf{s}_1(x)=\sum_{t=0}^{\infty}\mathbf{s}_1(t)x^t=[s_1^1(x)s_2^1(x)\ldots s_m^1(x)]^T, \quad (6)$$

and the following (matrix) relation pertaining to 2DSRS is still valid[8]:

$$\mathbf{F}(x)\ \mathbf{s}_1(x)=\mathbf{g}(x), \quad (7)$$

where

$$\mathbf{F}(x)\equiv\mathbf{I}+\mathbf{C}_1x+\cdots+\mathbf{C}_nx^n\equiv\begin{bmatrix}f_{11}(x) & \cdots & f_{1m}(x)\\ \vdots & \ddots & \\ f_{m1}(x) & & f_{mm}(x)\end{bmatrix}, \quad (8)$$

$$\mathbf{g}(x)=\sum_{k=1}^{n}[\mathbf{C}_k\sum_{j=1}^{k}(\mathbf{s}_j(0)x^{k-j})]\equiv\begin{bmatrix}g_1(x)\\ \vdots\\ g_n(x)\end{bmatrix}. \quad (9)$$

Under the assumption that **F**(x) is invertible,[9] (7) has the solution

$$\mathbf{s}_1(x)=[s_1^1(x)s_2^1(x)\ldots s_m^1(x)]^T=\mathbf{F}^{-1}(x)\mathbf{g}(x). \quad (10)$$

By Cramer's Rule, $s_j^1(x)$ can be obtained by

$$s_j^1(x)=\frac{|\mathbf{G}_j(x)|}{|\mathbf{F}(x)|},\quad \forall j=1,\ldots,m, \quad (11)$$

where

$$\mathbf{G}_j(x)=\begin{bmatrix}f_{11}(x) & \cdots & g_1(x) & \cdots & f_{1m}(x)\\ \vdots & & \vdots & & \\ f_{m1}(x) & & \underset{\substack{\uparrow\\ j\text{–th column:}\mathbf{g}(x)}}{g_m(x)} & & f_{mm}(x)\end{bmatrix}. \quad (12)$$

and $|\mathbf{G}_j(x)|$ and $|\mathbf{F}(x)|$ are determinants of $\mathbf{G}_j(x)$ and $\mathbf{F}(x)$, respectively.

The following observations pertaining to $|\mathbf{F}(x)|$ of 2DSRS (8) are extensions of and deducible from those for the 1-dimensional structure [1]-[3]:

Observation 2.

For the 2DSRS with any connection matrices, $\{\mathbf{C}_k\}_{k=1}^n$, and any initial state vector, **s**(0), the components of $\mathbf{s}_1(x)$ are rational functions.

Proof. $|\mathbf{F}(x)|$ and $|\mathbf{G}_j(x)|$ of (8) and (12), respectively, are clearly polynomials such that

$$\partial\left[|\mathbf{F}(x)|\right]\le mn \ \text{ and } \ \partial\left[|\mathbf{G}_j(x)|\right]\le mn-1, \forall j=1,\ldots,m,$$

6) Alternatively, hardware topology of the SSRG configuration [3].

7) Alternatively, initial values $\{\mathbf{s}_k(0)\}_{k=1}^n$ in the VARs.

8) Notice that when $m=1$, the relation reduces to the familiar formula corresponding to the 1-D SSRG [1]-[3].

9) We assume (for PN Code design purposes) invertibility of **F**(x) throughout this paper; invertibility refers to matrix invertibility over the field of rational functions (over *GF*(2)).

where $\partial[h(x)]$ denotes the degree of the polynomial $h(x)$. Applying this equation to (11) and (12) proves the observation. □

With a judicious choice of the connection matrices, $\{\mathbf{C}_k\}_{k=1}^n$, it is clear that the polynomial $|\mathbf{F}(x)|$ can be designed to be primitive.[10] In this case, the following observation becomes relevant with respect to our ultimate objective of designing PN generators.

Observation 3.

For the 2DSRS with connection matrices $\{\mathbf{C}_k\}_{k=1}^n$ such that $|\mathbf{F}(x)|$ is a degree *mn* primitive polynomial over *GF*(2) and for any initial state vector **s**(0), the components of $\mathbf{s}_1(x)$ are proper rational functions.

Proof. By the proof of Observation 2, we have

$$\partial\left[\left|\mathbf{G}_j(x)\right|\right] \le mn-1 < mn = \partial\left[\left|\mathbf{F}(x)\right|\right], \forall j = 1,\ldots,m.$$

Applying this equation to (11) and (12) proves the observation. □

By further extending the classical arguments [1]-[3], the generating function becomes

$$y(x;\mathbf{d}) = \sum_{t=0}^{\infty} y(t;\mathbf{d})x^t, \tag{13}$$

which corresponds to the output sequence $y(t;\mathbf{d})=\mathbf{d}^T\mathbf{s}(t)$ of (4) as follows[11]:

$y(x;\mathbf{d})=\mathbf{d}^T\mathbf{s}(x)$

$$= \left[\mathbf{d}_1^T, \mathbf{d}_2^T, \cdots, \mathbf{d}_n^T\right]^T \begin{bmatrix} x\mathbf{F}^{-1}(x)\mathbf{g}(x) + \mathbf{s}_1(0) \\ \vdots \\ x^n\mathbf{F}^{-1}(x)\mathbf{g}(x) + \sum_{j=1}^{n} x^{n-j}\mathbf{s}_j(0) \end{bmatrix}$$

$$= \left(\mathbf{d}_1^T x + \mathbf{d}_2^T x^2 + \cdots + \mathbf{d}_n^T x^n\right)\mathbf{F}^{-1}(x)\mathbf{g}(x) + \left(\sum_{i=1}^{n}\mathbf{d}_i^T\sum_{j=1}^{i}x^{i-j}\mathbf{s}_j(0)\right)$$

$$= \left(\mathbf{d}_1^T x + \mathbf{d}_2^T x^2 + \cdots + \mathbf{d}_n^T x^n\right)\mathbf{s}_1(x) + \left(\sum_{i=1}^{n}\mathbf{d}_i^T\sum_{j=1}^{i}x^{i-j}\mathbf{s}_j(0)\right). \tag{14}$$

Following convention [1]-[3], we identify a one-sided sequence, or generating function, with another one-sided sequence when they differ in at most a finite number of positions; the generating function in (14) is therefore identified with the following generating function:

$$\begin{aligned} a(x,\mathbf{d}) &\equiv \left(\mathbf{d}_1^T x + \mathbf{d}_1^T x^2 + \cdots + \mathbf{d}_n^T x^n\right)\mathbf{F}^{-1}(x)\mathbf{g}(x) \\ &= \left(\mathbf{d}_1^T x + \mathbf{d}_2^T x^2 + \cdots \mathbf{d}_n^T x^n\right)\mathbf{s}_1(x). \end{aligned} \tag{15}$$

In particular, we call a sequence periodic if it is periodic after some finite time, i.e., when the sequence is identifiable with a one-sided periodic sequence.

When we denote the standard basis as

$$\left\{\mathbf{e}_i = \underbrace{[0\ldots010\ldots0]^T}_{\text{only } i\text{-th of } mn \text{ terms equal to } 1}\right\}_{i=1}^{mn} \subseteq \{0,1\}^{mn} \tag{16}$$

we have the Theorem 1.

Theorem 1.

For the 2DSRS with connection matrices $\{\mathbf{C}_k\}_{k=1}^n$ such that $|\mathbf{F}(x)|$ is a degree *mn* primitive polynomial over *GF*(2), we have the following:

1. For any initial state vector **s**(0), the components[12] of $\mathbf{s}_1(t)$ are PN sequences of period 2^{mn}-1.

2. The initial state vector **s**(0) can always be chosen such that $\{y(t;\mathbf{e}_j)\}_{j=1}^{mn}$ becomes a basis for (periodic sequence) subspace $(\{y(t;\mathbf{d})\}_{\mathbf{d}\neq 0}, \{0,1\})$. In this case, $\{y(t;\mathbf{d})\}_{\mathbf{d}\neq 0}$ constitutes all distinctly-shifted periodic PN sequences of period 2^{mn}-1.

Proof.

1. It is clear from the facts that $\mathbf{s}_1(x)$ is a proper rational function by Observation 3 and that a rational function with a primitive polynomial as the denominator necessarily corresponds to a period 2^{mn}-1 PN sequence.

2. By (14) and (15) (with $\mathbf{d}=\mathbf{e}_j$), each $y(t;\mathbf{e}_j)$ or $y(x;\mathbf{e}_j)$ is clearly identified with the *j*-th component of the following vector:

$$\left[x\mathbf{s}_1(x)^T \cdots x^n\mathbf{s}_n(x)^T\right]^T, \tag{17}$$

which can always be designed such that the components of $\mathbf{s}_1(x)$ are non-consecutive. The rest of the proposition can be proved by Theorem 1.1 and the properties of PN sequences generated via the same primitive polynomial [1]-[3]. The fact that the sequences $\{y(t;\mathbf{d})\}_{\mathbf{d}\neq 0}$ are all distinct follows since, for any nonzero masking vector **d**, $y(t;\mathbf{d})$ denotes a nontrivial linear combination of a basis (i.e., the validity follows from uniqueness of representation involving a basis [9]). □

Notice that Theorem 1 states that the sequences in the 2DSRS' *mn* memory elements—as represented by the

10) This process generally leads to many solutions, and there is a certain amount of flexibility in the design of connection matrices.

11) Notice that, up to identification as described in the ensuing paragraph with (15), the component (vector-valued) generating functions in $\mathbf{s}(x)$ in (14) correspond to linear shifts of $\mathbf{s}_1(x)$ which, by (10), is equal to $\mathbf{F}^{-1}(x)\mathbf{g}(x)$.

12) For example, by (1) and (6), $\mathbf{s}_1(t) \equiv \left[s_1^1(t)\ldots s_m^1(t)\right]^T$ or, alternatively by (4), $\{y(t;\mathbf{e}_j)\}_{j=1}^m$.

generally non-consecutive $\{y(t;\mathbf{e}_j)\}_{j=1}^{mn}$ of Theorem 1.2—can be used to generate any offset/shifted PN code of $\{y(t;\mathbf{d})\}_{\mathbf{d}\neq 0}$ of Theorem 1.2 via suitable linear combination masking, which is a necessary feature in the current IS-95x implementations of CDMA [2]; alternatively, the mn sequences in the memory elements can be used directly in parallel towards multimedia (e.g., real-time video) scrambling applications [7].

In vector space-theoretic terms, the importance of Theorem 1 is that the span of the sequences directly produced in the individual registers is the complete mn-dimensional subspace consisting of all 2^{mn} sequences (the complete set of 2^{mn}-1 offset PN sequences plus the zero sequence).

IV. Illustrative Design Examples

Designing the 2DSRS corresponds to specifying the connection architecture/configuration and the initial conditions which, in turn, correspond to the selection of

$$(m,\ n,\ \mathbf{C}_1,...,\mathbf{C}_n,\mathbf{d}) \text{ and } \mathbf{s}(0), \tag{18}$$

respectively. The 2DSRS design can be made under different design criteria (e.g., specifying particular PN sequences in the registers).

If we confine the design to a simple 2×2 (m=2, n=2) 2DSRS in this section (see Fig. 2), by Observation 1 and (1) through (5),

$$\mathbf{Q}_{2DSRS}=\begin{bmatrix}\mathbf{C}_1 & \mathbf{C}_2\\ 1\ 0\ 0\ 0\\ 0\ 1\ 0\ 0\end{bmatrix}=\begin{bmatrix}c_{11}^1 & c_{12}^1 & c_{11}^2 & c_{12}^2\\ c_{21}^1 & c_{22}^1 & c_{21}^2 & c_{22}^2\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}, \quad \text{and}$$

$$\mathbf{s}(0)\equiv\left[\mathbf{s}_1(0)^T\,\mathbf{s}_2(0)^T\right]^T=\left[s_1^1(0)s_2^1(0)s_1^2(0)s_2^2(0)\right]^T. \tag{19}$$

In all of our designs below, the 4-dimensional masking vector can be chosen arbitrarily [1]-[3], of course, to obtain any offset of the underlying length (2^{mn}-1=2^4-1=15) PN code as follows.

$$\mathbf{d}=\left[\mathbf{d}_1^T\mathbf{d}_2^T\right]^T=\left[d_1^1d_2^1d_1^2d_2^2\right]^T \tag{20}$$

However, we initially choose $\mathbf{d}$ implicitly to be the standard basis of (16) to determine the hardware connection configuration via considering the sequences as generated in the individual registers.

For the 2DSRS to generate PN sequences of period 2^{mn}-1=2^4-1=15 in each of the mn=4 registers, by Theorems 1.1 and 1.2, it suffices to choose $|\mathbf{F}(x)|$ to be a primitive polynomial of degree mn=4. This means that

$$\begin{aligned}|\mathbf{F}(x)| &= 1+(c_{11}^1+c_{22}^1)x\\ &\quad+(c_{11}^2+c_{11}^1c_{22}^1+c_{22}^2+c_{21}^1c_{12}^1)x^2\\ &\quad+(c_{11}^1c_{22}^2+c_{11}^2c_{22}^1+c_{21}^1c_{12}^2+c_{21}^2c_{12}^1)x^3\\ &\quad+(c_{11}^2c_{22}^2+c_{21}^2c_{12}^2)x^4\end{aligned} \tag{21}$$

has to be either $1+x+x^4$ or $1+x^3+x^4$; this constraint can be used to determine[13] $\mathbf{C}_1$ and $\mathbf{C}_2$ of (18), which quantify the 2DSRS connection architecture.

By Theorem 1, the generating function of PN sequences in the leftmost VAR of (6), $\mathbf{s}_1(x)$, can be obtained as a solution to (7) with the following:

1. $\mathbf{F}(x)$ of (8) as determined from above and
2. $\mathbf{g}(x)$ of (9) as determined[14] via suitable nonzero initial values in the registers as represented by $\mathbf{s}(0)$ of (19); for demonstrative purposes (for our examples), it suffices to let $\mathbf{s}(0)=[1\ \ 0\ \ 0\ \ 0]^T$.

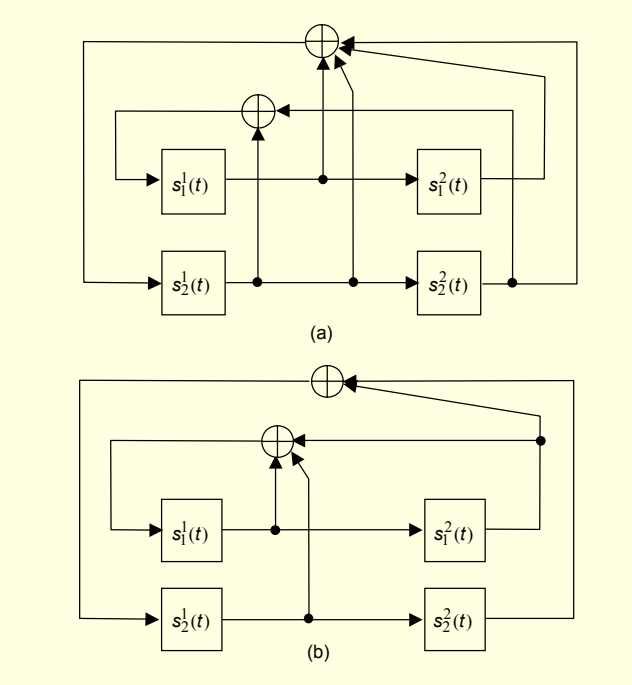

Fig. 2. 2DSRS for $m=n=2$ with primitive polynomials (a) $1+x+x^4$ and (b) $1+x^3+x^4$.

13) Equation (21) has many solutions and there is a certain amount of flexibility in the design of connection matrices, $\mathbf{C}_1$ and $\mathbf{C}_2$.

14) Once the connection matrices $\mathbf{C}_1$ and $\mathbf{C}_2$ are determined via the constraint on $|\mathbf{F}(x)|$ being a primitive polynomial (as above), $\mathbf{g}(x)$, by (9), can be determined from the choice of $\mathbf{s}(0)$ so as to make the components of $\mathbf{s}_1(x)$ be distinct (proper) rational functions—the choice of $\mathbf{s}(0)$ that fulfills this criterion is generally not unique.

Table 1. Some example generations of PN Codes for a 2DSRS ($m=n=2$).

Figure reference	$\lvert\mathbf{F}(x)\rvert$	$\mathbf{C}_1$	$\mathbf{C}_2$	$\mathbf{s}(0)$
	$\mathbf{F}(x)$		$\mathbf{g}(x)$	$\mathbf{s}_1(x)$
Figure 2(a)	$1+x+x^4$	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&1\end{bmatrix}$	$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$
	$\begin{bmatrix}1 & x+x^2\\ x+x^2 & 1+x+x^2\end{bmatrix}$		$\begin{bmatrix}0\\1+x\end{bmatrix}$	$\begin{bmatrix}\frac{x+x^3}{1+x+x^4}\\ \frac{1+x}{1+x+x^4}\end{bmatrix}$
	$s_1^1(t):011001000111101$ $s_2^1(t):100011110101100$ $s_1^2(t):101100100011110$ $s_2^2(t):010001111010110$ e.g., $s_1^1(t)$ is 5 times right circular shift of $s_2^1(t)$			
Figure 2(b)	$1+x+x^4$	$\begin{bmatrix}1&1\\0&0\end{bmatrix}$	$\begin{bmatrix}1&0\\1&1\end{bmatrix}$	$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}$
	$\begin{bmatrix}1+x+x^2 & x\\ x^2 & 1+x^2\end{bmatrix}$		$\begin{bmatrix}1+x\\ x\end{bmatrix}$	$\begin{bmatrix}\frac{1+x+x^3}{1+x+x^4}\\ \frac{x}{1+x+x^4}\end{bmatrix}$
	$s_1^1(t):100100011110101$ $s_2^1(t):011110101100100$ $s_1^2(t):110010001111010$ $s_2^2(t):001111010110010$ e.g., $s_1^1(t)$ is 6 times right circular shift of $s_2^1(t)$			

Having determined $\mathbf{s}_1(x)$ as above—by Theorem 1.2—with a suitable choice of the masking connection as represented by $\mathbf{d}$ of (20), the generating function $y(x;\mathbf{d})$ of (14) and (15) for the output PN sequence $y(t;\mathbf{d})=\mathbf{d}^T\mathbf{s}(t)$ can be designed to be any arbitrary offset of the underlying PN code.

The solutions and the approaches to solutions, as exemplified in this section—summarized in Table 1 and illustrated in Figs. 2(a) and 2(b)—attest to the possible flexibility in the selection of *mn* PN codes.

V. Conclusion

In this paper, we have introduced and analyzed a new compact 2-D structure for directly generating non-consecutive PN codes of lengths 2^{mn}-1; with the 2-D architecture, it was shown in Theorem 1 that once properly designed[15] as dictated by IS-95x and scrambling applications, we can get all shifted PN sequences as with the 1-D structured shift registers.

The 2DSRS scheme provides for alternative VLSI/firmware implementations of PN generators. With respect to the number of memory elements and connections needed, the implementation costs between the proposed 2-D scheme and the conventional 1-D scheme are similar, but the former is superior because of its versatility and richness: Whereas the traditional SSRG structure [1]-[3] is capable of generating a PN basis consisting of a single collection of consecutively-shifted PN sequences, the 2DSRS is capable of generating a PN basis consisting of multiple collections of consecutively-shifted PN sequences; the 2DSRS, because it normally offers multiple solutions for a given specification, allows for more flexible designs as compared to the 1-D linear feedback shift register [1]-[3] designs, which mostly allows for flexibility in the choice of the initial values in the registers.

Acknowledgement

The authors gratefully acknowledge the generous support of Samyang Corporation and its Vice President Won Kim for the donation of LMDS equipment, which provided a further motivation for this research.

References

[1] S.W. Golomb, *Shift Register Sequences*, Holden- Day, Inc., 1967.

[2] J.S. Lee and L.E. Miller, *CDMA Systems Engineering Handbook*, Artech House, 1998.

[3] Andrew J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*, Addison-Wesley Publishing Company, 1995.

[4] K. Simon, J. Omura, R. Scholz, and K. Levitt, *Spread Spectrum Communication*, vol. 3, Rockville, MD, Computer Science Press, 1985.

[5] William J. Park, John J. Komo, "Relationships between m-Sequences over GF(q) and GF(q^m)," *IEEE Trans. Information Theory*, vol. 35, no. 1, Jan. 1989.

[6] Xu-duan Lin and Chang-nian Cai, "Generalized m-Sequences and their Crosscorrelation Properties," *IEEE Region 10 Conf. on Computer and Commun. Systems*, Sept. 1990.

[7] IS-95-A, *Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, 1995.

[8] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996.

15) This includes determining the hardware configuration (i.e., (m, n, $\mathbf{C}_1$,…,$\mathbf{C}_n$, $\mathbf{d}$) or (m, n, $\mathbf{Q}_{2DSRS}$, $\mathbf{d}$)) and loading the registers with appropriate initial values (i.e., $\mathbf{s}(0)$).

[9] C.T. Chen, *Linear System Theory & Design*, Saunders College Publishing, 1984.
[10] R.A. Scholtz and L.R. Welch, " GMW Sequences," *IEEE Trans. Information Theory*, vol. IT-30, no. 3, May 1984.

Hyun Jung Kim received the BS and MS degrees in radio sciences and engineering from Korea University, Seoul, Korea, in 1996 and 1998. Since 2001, she has been working toward the PhD degree at Korea University. From 1998 to 2001, she worked for LG Electronics, Anyang, Korea, and since 2003, she has been with Samsung Electronics, Suwon, Korea. Her research interests include channel coding (Turbo, LDPC codes, etc.), iterative decoding algorithms for linear codes, and FPGA implementations.

Inkyu Lee was born in Seoul, Korea, in 1967. He received the BS degree (with honors) in control and instrumentation engineering from Seoul National University, Seoul, in 1990 and the MS and PhD degrees in electrical engineering from Stanford University, Stanford, CA, in 1992 and 1995, respectively. From 1991 to 1995, he was a Research Assistant at the Information Systems Laboratory, Stanford University. From 1995 to 2001, he was a Member of Technical Staff at Bell Laboratories, Lucent Technologies, where he studied wireless communication system design. He later worked for Agere Systems (formerly Microelectronics Group of Lucent Technologies), Murray Hill, NJ, as a Distinguished Member of Technical Staff from 2001 to 2002. In September 2002, he joined the Faculty of the Department of Radio Communications Engineering, Korea University, Seoul, Korea. He received the Young Scientist Award from the Ministry of Science and Technology, Korea, in 2003. He is an Editor for the IEEE Transactions on Communications and is also a Chief Editor for "4G wireless systems" special issue in the IEEE Journal on Selected Areas in Communications.

Woonkyung M. Kim received SB degrees in Electrical Engineering and Mathematics from Massachusetts Institute of Technology, SB degree in Computer Science from Boston University, MS degree in Engineering Sciences(Electrical Engineering) from Harvard University, and PhD degree in Engineering Sciences (Electrical Engineering) from Harvard University. His work towards an MS degree in Computer Science from Boston University was halted in 1994 when he joined the Artificial Intelligence Lab (Department of Cognitive Sciences) at Massachusetts Institute of Technology as a Postdoctoral Fellow. He has briefly interned at Electronic Telecommunications Research Institute (ETRI) in 1977. He now holds a Full Professorship at the School of Electrical Engineering at Korea University where his current theoretical interests include Communications (CDMA and PN Codes), Multimedia (MPEG-X), Morphological Signal Processing, Virtual Reality and Intelligent Systems. He heads three laboratories–Communications Signal Processing Lab, Multimedia Information Communication Lab, and Intelligent System Lab–on campus at Korea University. He also serves as a CTO at Multimedia Wiz, an Internet Video Infrastructure company in Irvine, California, that he helped found.