Analysis of Sequences Generated by 90/150 maximum-length NBCA

Sung-Jin Cho*, Seok-Tae Kim†, Han-Doo Kim**, Un-Sook Choi***,
Seong-Hun Heo*, Yoon-Hee Hwang† and Sung-Ga Lee*
*Pukyong National University, **Inje University, ***Youngsan University

최대길이를 갖는 90/150 NBCA에 의해서 생성되는 수열의 분석†
조성진*, 김석태†, 김한두**, 최언숙***, 허성훈†, 황윤희†, 이상가*
*부경대학교, **인제대학교, ***영산대학교
E-mail : sjcho@pknu.ac.kr

ABSTRACT

In this paper, we analyze Pseudo-Noise (PN) sequences generated by a 90/150 maximum-length Null Boundary Cellular Automata.

요 약

본 논문에서는 90/150 NBCA에 의해서 생성되는 PN 수열을 분석한다.

Keyword

Cellular Automata, Pseudo-Noise sequences, primitive polynomials, ranges, offsets, reciprocal polynomials, characteristic polynomials.

1. Introduction

Cellular Automata (CA) was first introduced by Von Neumann [1] for modeling biological self-reproduction. Wolfram [2] pioneered the investigation of CA as mathematical models for self-organizing statistical systems and suggested the use of a simple two-state, three -neighborhood CA with cells arranged linearly in one dimension. Das et al. [3] developed a matrix algebraic tool capable of characterizing CA. CA have been employed in several applications ([4], [5], [6]). Cho et al. ([7], [8], [9], [10], [11]) analyzed CA to study hash function, data storage, cryptography and so on. In this paper, we analyze PN sequences generated by a 90/150 maximum-length Null Boundary CA(NBCA).

II. Definitions and Preliminaries

Definition 2.1 [10] A CA is called a group CA if det(T) = 1, where T is the characteristic matrix for the CA.

Group CA can be classified into maximum- and minimum-length CA. An n-cell maximum-length CA is characterized by the presence of a cycle of length $(2^n - 1)$ with all nonzero states. Moreover, the characteristic
polynomial of such a CA is primitive. A primitive polynomial \( p(x) \) of degree \( n \) is an irreducible polynomial such that \( \min \{ m : p(x) \mid x^m + 1 \} = 2^n - 1 \).

**Definition 2.2** [13] \( f(x) = 1 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \) be an \( n \)-degree primitive polynomial, where \( c_i \in \{0, 1\} \). Then \( f(x) \) generates a periodic sequence whose period is \( 2^n - 1 \). This sequence is called a Pseudo-Noise (PN) sequence.

**Definition 2.3** Consider an \( n \)-degree primitive polynomial \( f(x) = 1 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \), where \( c_i \in \{0, 1\} \). Let \( f^*(x) = x^n f(\frac{1}{x}) \). Then \( f^*(x) \) is called the reciprocal polynomial of \( f(x) \).

**Definition 2.4** A CA is said to be a Null Boundary CA (NBCA) if the left (right) neighborhood of the leftmost (rightmost) terminal cell is connected to logic 0-state.

### III. Analysis of PN Sequences Generated by a 90/150 NBCA

In this section, a few theoretical results have been developed based on matrices consisting of PN sequences as their columns. And we give the relationship between \( O_1 \) and \( O_2 \), where \( O_1 \) and \( O_2 \) are the minimum offsets for an \( n \)-degree primitive polynomial and its reciprocal polynomial, respectively.

Consider an \( n \)-degree primitive polynomial \( f(x) = 1 + c_1 x + \cdots + c_{n-1} x^{n-1} + x^n \), where \( c_i \in \{0, 1\} \). \( f(x) \) generates a periodic sequence whose period is \( 2^n - 1 \). This sequence is a PN sequence. Since \( f(x) \) is primitive, the reciprocal polynomial \( f^*(x) \) of \( f(x) \) is also an \( n \)-degree primitive polynomial. And thus the period of the sequence generated by \( f^*(x) \) is \( 2^n - 1 \).

**Definition 3.1** In the Galois field \( F_2 = \{0, 1\} \), let the sequence \( \{s_j\} \) satisfy the homogeneous linear recurrence relation

\[
s_{t+n} = c_0 s_t + c_1 s_{t+1} + \cdots + c_{n-1} s_{t+n-1}
\]

\((t = 0, 1, 2, \cdots, )\), \( c_0, c_1, \cdots, c_{n-1} \in F_2 \)

Then \( f(x) \) is said to be the characteristic polynomial of \( \{s_j\} \).

Let \( \mathcal{Q}(f(x)) \) be the set of all sequences \( \{s_j\} \) which have \( f(x) \) as the characteristic polynomial. Thus

\[
\mathcal{Q}(f(x)) = \{ s \mid s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}, \ t = 0, 1, 2, \cdots \}
\]

Given an arbitrary sequence \( s_0, s_1, \cdots \) of elements of \( F_2 \), we associate with it its generating function, which is a purely formal expression of the type

\[
G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{i=0}^{\infty} s_i x^i
\]

with an indeterminate \( x \).

**Lemma 3.2** [12] Let \( \{s_j\} \in \mathcal{Q}(f(x)) \), let \( f^*(x) \) be the reciprocal characteristic polynomial of \( f(x) \) and \( G(x) \) be its generating function in \((*)\). Then the identity

\[
G(x) = \frac{g(x)}{f^*(x)}
\]

holds with

\[
g(x) = -\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} c_i s_{j+k} x^j,
\]

where we set \( c_{n} = -1 \).

The following theorem is very important to study PN sequences.

**Theorem 3.3** Let \( f(x) \) is an \( n \)-degree primitive polynomial. Also let \( \{s_j\} \in \mathcal{Q}(f(x)) \) and \( s(x) = s_0 + s_1 x + \cdots + s_{r-1} x^{r-1} \) where \( r = 2^n - 1 \). Let \( \{u_j\} \) be the cyclic sequence such that \( u(x)(c) = u_0 + u_1 x + \cdots + u_{r-1} x^{r-1} \) = \( s^*(x) \). Then \( \{u_j\} \in \mathcal{Q}(f^*(x)) \).

Consider a \((2^n-1) \times n\) matrix \( A \) consisting of \( n \) independent maximum-length sequences generated by an \( n \)-degree primitive polynomial as its columns. A matrix \( A \) corresponding to \( x^4 + x + 1 \) is shown in Figure 1.(a). Any column of this matrix is a PN sequence generated by the CA \( C \) having \( x^4 + x + 1 \) as its characteristic polynomial. In fact the rule of \( C \) is \( <90, 150, 90, 150> \). Thus the state-transition matrix \( T \) of \( C \) is

\[
T = \begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1
\end{bmatrix}
\]

Now, consider a \((2^n-1) \times (n-1)\) matrix obtained by deleting only one of the columns of
A. Such a reduced matrix is referred to as
matrix $B$ [Figure 1(b),(b')] in the subsequent
discussions. Without loss of generality, let only
the all-zeros $(n-1)$-tuple appear as the first
row of $B$.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>000</td>
<td>0001</td>
<td>000</td>
<td></td>
</tr>
<tr>
<td>0011</td>
<td>001</td>
<td>0011</td>
<td>001</td>
<td></td>
</tr>
<tr>
<td>0110</td>
<td>011</td>
<td>0100</td>
<td>010</td>
<td></td>
</tr>
<tr>
<td>1011</td>
<td>101</td>
<td>1010</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>0010</td>
<td>001</td>
<td>1111</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>0101</td>
<td>010</td>
<td>1110</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>110</td>
<td>1001</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>111</td>
<td>0010</td>
<td>001</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>110</td>
<td>0011</td>
<td>011</td>
<td></td>
</tr>
<tr>
<td>1010</td>
<td>101</td>
<td>1110</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>(a)</td>
<td>(b)</td>
<td>(a')</td>
<td>(b')</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: $A$ matrix (a) (resp. (a')) and $B$
matrix (b) (resp. (b')) corresponding
to $x^4 + x + 1$ (resp. $x^4 + x^3 + 1$)

Definition 3.4 [3] Range: The range of an
$(n - 1)$-tuple vector (say $B_r$, $0 \leq r \leq 2^{n-2}$)
in a $B$ matrix is defined as the minimum span
in $B$ (starting with $B_r$) in which all of the
$(n-1)$-tuple (including the all-zeros tuple)
appear at least once. Offset: The distance $r$
of an $(n-1)$-tuple (say $B_r$) in a $B$ matrix, in
terms of the number of row vectors from the
all-zeros $(n-1)$-tuple, is defined as the offset
of the $(n-1)$-tuple.

The range and the offset of the 3-tuple row vector $<110>$ in row 7 of the $B$ matrix of Figure
1(b) are 11 and 6, respectively.

range of a $B$ matrix is defined as the minimum
of all the ranges associated with vectors in $B$.
Minimum Offset: Minimum offset in a $B$ matrix
is defined as the offset of the particular $(n-1)$-
tuple associated with the minimum range.

Lemma 3.6 [3] The minimum range and
minimum offset remain invariant with respect to
the choice of any $B$ matrix generated out of the
$A$ matrix, corresponding to the same $n$-degree
primitive polynomial.

Since $\text{rank}(B) = n-1$, we can reduce $B$ to
the following $(2^n-1)\times(n-1)$ matrix by
elementary column operation,

$$C = \begin{bmatrix} I_{n-1} \\ 0 \end{bmatrix},$$

where 0 is the all-zero $(n-1)$-tuple, $I_{n-1}$
is the $(n-1)\times(n-1)$ identity matrix and Q
is a $(2^n-n-1)\times(n-1)$ nonzero matrix.

Theorem 3.7 Let $T$ be the characteristic
matrix of an $n$-cell 90/150 NBCA whose
characteristic polynomial is an $n$-degree
primitive polynomial $f(x)$. Then there exists $p$
$(1 \leq p \leq 2^{n-2})$ such that

$$T^n \oplus T^p = I_n$$

Corollary 3.8 Let $T$ be the characteristic
matrix of an $n$-cell 90/150 NBCA whose
characteristic polynomial is an $n$-degree
primitive polynomial. Then there exists $k$
$(1 \leq k \leq 2^{n-2})$ such that

$$T^k \oplus T^{k+1} = I_n$$

Corollary 3.9 Let $T$ be the characteristic
matrix of an $n$-cell 90/150 NBCA whose
characteristic polynomial is an $n$-degree
primitive polynomial. For nonzero states $a, b$
such that $a \oplus b = (0, 0, \cdots, 0, 1)^t$, there exists a
$k$ $(1 \leq k \leq 2^{n-2})$ such that

$$T^k(0,0,\cdots,0,1)^t = a$$

and $T^{k+1}(0,0,\cdots,0,1)^t = b$

Lemma 3.10 Let $T$ be the characteristic matrix
of an $n$-cell 90/150 NBCA whose characteristic
polynomial is an $n$-degree primitive polynomial.
And let $f^*(x)$ be the reciprocal polynomial of
$f(x)$ and $T^*$ be the characteristic matrix of
the $n$-cell 90/150 NBCA obtained from $f^*(x)$
by the method in [14]. For some $k$ $(1 \leq k \leq 2^n-2)$
such that $T^k \oplus T^{k+1} = I_n$, let

$$T^k \oplus T^{k+1} = I_n.$$
polynomial and its reciprocal polynomial, respectively, and $d$ is the minimum range in both case. Let $|OA_1| = a$, $|A_2 \hat{O}| = b$, $|B_1 \hat{O}| = y$. Then the following hold:

$$O_1 + O_2 = 2(2^n - 1) - b - y.$$  

Corollary 3.13 If $O_1$ and $O_2$ are the minimum offsets for an $n$-degree primitive polynomial and its reciprocal polynomial, respectively, and $d$ is the minimum range in both case. Let $|OA_1| (: = a) \neq |A_2 \hat{O}| (: = b)$, $|B_1 \hat{O}| = y$. Then $O_1 + O_2 \neq 2^n - 1 + |A_1 B_1|.$

Corollary 3.14 If $O_1$ and $O_2$ are the minimum offsets for an $n$-degree primitive polynomial and its reciprocal polynomial, respectively, and $d$ is the minimum range in both case. Let $|OA_1| = |A_2 \hat{O}|$. Then $O_2 = 2(2^n - 1) - (O_1 + d) + 1$.

IV. Conclusion

In this paper, we analyzed PN sequences generated by a 90/150 NBCA whose characteristic polynomial is a primitive polynomial, and we give the relationship among offsets $O$ such that the minimum offset $O_1$ is obtained from the $A_1$ matrix whose characteristic polynomial is the primitive polynomial $f(x)$ and $O_2$ is obtained from the $A_2$ matrix whose characteristic polynomial is the reciprocal polynomial of $f(x)$. This analysis is helpful to study for the pattern generation, cryptography and so on.

References


