Study on Generalized Prefer-Opposite (GPO) Algorithm for Constructing the De Bruijn Binary Sequence

A N Setiawan*, M Astuti and Z M Mayasari
Department of Mathematics, Faculty of Mathematics and Natural Science, University of Bengkulu, Indonesia.

*Corresponding author: aisyahnsetiawan@gmail.com

Abstract De Bruijn binary sequence $S_n$ of order $n$ is a string of bits $s_i \in \{0,1\} = \{s_1, \ldots, s_{2^n}\}$, so that each string with length $n$, $\{a_1, \ldots, a_n\} \in \{0,1\}^n$ appears exactly once. De Bruijn binary sequence can be built using the Generalized Prefer-Opposite (GPO) algorithm. The GPO algorithm is based on the Feedback Shift Register (FSR), which is a clock-regulated circuit with $n$ sequential storage units. In running the algorithm, we need input consisting of the feedback function $f(x_0, x_1, \ldots, x_{n-1})$ and initial state $b = b_0, b_1, \ldots, b_{n-1}$. There are many combinations of feedback functions and initial states that can be used, then grouped into three families namely family one, family two and family three. The purpose of this research is studying the GPO algorithm which use the feedback function from family two $f(x_0, \ldots, x_{n-1}) = 1 + \prod_{t=2}^{n-1} x_t$, $0 < t < n$, $t = 2$, $n = 4$ and initial state $b = 1100$ in constructing the de Bruijn binary sequence. The result of this study indicate that the GPO algorithm with the feedback function and the initial state from the family two construct a de Bruijn binary sequence.

1. Introduction

In an era full of technological sophistication, many people are given the convenience of carrying out activities. One of them is the ease of obtaining information. This convenience, of course, requires security over the assets that are input and accessed, especially those concerning the secrets of a country, an institution or something that is private. This is the starting point for the development of a data security system.

Cryptography is the study of protecting information by encrypting the inputted data into a complex code, the code can be converted back into the original data through the description process by the recipient [1]-[2]. In the field of cryptography there is a sequence, called the de Bruijn binary sequence, which can be used to produce information that has a security quantity. This sequence combines the alphabet zero and one.

De Bruijn binary sequence $S_n$ of order $n$ is a string of bits $s_i \in \{0,1\} = \{s_1, \ldots, s_{2^n}\}$, so that each string with length $n$, $\{a_1, \ldots, a_n\} \in \{0,1\}^n$ appears exactly once. The de Bruijn binary sequence was introduced by De Bruijn in 1946 where each element used a binary alphabet of zeros and ones. Based on the article
entitled "A Combinatorial Problem", De Bruijn stated that there are $2^{2^n-1-n}$ kinds of De Bruijn binary Sequences of order $n$. De Bruijn binary sequences can be constructed using the Generalized Prefer-Opposite (GPO) algorithm [3]-[4].

There are many combinations of feedback functions and initial states that can be formed which are grouped into three families, namely family one, family two and family three. However, it is difficult to confirm which functions are actually valid for the GPO algorithm. Therefore, this paper will discuss about the GPO algorithm using a feedback function and the initial state from the family two.

$$f(x_0, \ldots, x_{n-1}) = 1 + \prod_{i=t}^{n-1} x_i,$$

with $0 < t < n$, $t = 2$ and $n = 4$ and initial state $b = 1100$ in constructing the De Bruijn binary sequence. The purpose of paper is to study the feedback function and initial state of family two in building de Bruijn binary sequences.

2. Literature Review

2.1. Graph

A graph $G(V,E)$ is a discrete structure consisting of vertices and edges. According to Bondy and Murty in 1976, A graph $G$ is an ordered triple $(V(G), E(G), \psi_G)$ consisting of a nonempty set $V(G)$ of vertices, a set $E(G)$, disjoint from $V(G)$, of edges, and an incidence function $\psi_G$ that associates with each edge of $G$ an unordered pair of (not necessarily distinct) vertices of $G$ [5]. If $e$ is an edge and $u$ and $v$ are vertices such that $\psi_G(e) = uv$, then $e$ is said to join $u$ and $v$; the vertices $u$ and $v$ are called the end of $e$.

2.2. Tree

Tree is a connected graph that does not contain circuits. In a tree, there is always a path that connects the two nodes in the tree.

2.3. De Bruijn Binary Sequence

De Bruijn binary sequence $S_n$ of order $n$ is a string of bits $s_i \in \{0, 1\} = \{s_1, \ldots, s_{2^n}\}$, so that each string with length $n$, $\{a_1, \ldots, a_n\} \in \{0, 1\}^n$ appears exactly once. De Bruijn (1946) stated that there are $2^{2^n-1-n}$ kinds of De Bruijn binary Sequences of order $n$ [6].

2.4. Feedback Shift Register (FSR)

The feedback shift registers are most useful in designing and generating such pseudorandom or pseudonoise (PN) sequences [7]-[8]. This is due to their simplicity of defining rules and their capability of generating sequences with much longer period. An $n$-stage shift register is a clock-regulated circuit with $n$ consecutive storage units. Each of the units holds a bit and, as the clock pulses, the bit is shifted to the next stage in line. The output is a new bit $s_n$ based on the $n$ bits $S_0 = s_0, \ldots, s_{n-1}$ called the initial state. The corresponding feedback function $f(x_0, \ldots, x_{n-1})$ is the Boolean function that, on input $s_0$, outputs $s_n$.

2.5. State Graph

The state graph of the FSR with feedback function $f(x_0, x_1, \ldots, x_{n-1})$ is a directed graph $G_f$ whose vertices are all of the $n$-stage states. There is a directed edge from a state $u := u_0, u_1, \ldots, u_{n-1}$ to a state $v := u_1, u_2, \ldots, u_{n-1} f(u_0, u_1, \ldots, u_{n-1})$. We call $u$ a child of $v$ and $v$ the parent of $u$. We allow $u = v$, in
which case $G_f$ contains a loop. A leaf in $G_f$ is a vertex with no child, i.e., a leaf has outdegree 1 and indegree 0 [9]-[10].

2.6. Generalized Prefer-Opposite (GPO) Algorithm

The following theorem and lemma will be used in the construction of the De Bruijn sequence:

Lemma 1
Given the state graph $G_f$ of the FSR with feedback function $f$, let the state $s$ be a vertex with two children. Let the GPO Algorithm starts with an initial state $b \neq s$. By the time the algorithm visits $s$ it must have visited both children of $s$ [3].

Theorem 2
The GPO Algorithm, on input a function $f(x_0, x_1, ..., x_{n-1})$ and an initial state $b = b_0, b_1, ..., b_{n-1}$, generates De Bruijn binary sequence of order $n$ if the state graph $G_f$ of the FSR satisfies the following two conditions [3]:
1) all of the states, except for the leaves, have exactly two children;
2) there is a unique directed path from any state $v$ to $b$.

Table 1. Generalized Prefer-Opposite Algorithm [3]

| Algorithm 1. Generalized Prefer-Opposite |
|-----------------------------------------|
| **Input**: Feedback function $f(x_0, x_1, ..., x_{n-1})$ dan initial state $b = b_0, b_1, ..., b_{n-1}$ |
| **Output**: Barisan biner |
| 1. $c = c_0, c_1, ..., c_{n-1} \leftarrow b$ |
| 2. do |
| 3. Print ($c_0$) |
| 4. $y \leftarrow f(c_0, c_1, ..., c_{n-1})$ |
| 5. if $c_1, c_2, ..., c_{n-1}, y$ belum muncul then |
| 6. $c \rightarrow c_1, c_2, ..., c_{n-1}, y$ |
| 7. else |
| 8. $c \rightarrow c_1, c_2, ..., c_{n-1}, y$ |
| 9. while $c \neq b$ |

2.7. Family Two

To construct De Bruijn's sequence using Algorithm 1, it is enough to find a feedback function and initial state that satisfies Theorem 2. There are many combinations of feedback functions and initial state which are grouped into three families, one of which will be discussed, namely the family two that have been obtained [3].
Teorema 3

Given \( n \) and an integer \( 0 < t < n \), let the feedback function be [3]

\[
f(x_0 x_1, \ldots, x_{n-1}) := 1 + \prod_{i=t}^{n-1} x_i
\]

and the initial state \( b \) be any \( n \)-stage state of the sequence \((0, 1^{n-t})\). Then the GPO Algorithm generates the \( f_2(n) \) family of de Bruijn sequences of order \( n \).

3. Result and Discussion

In this paper, De Bruijn binary sequences with order 4. Based on the definition, the de Bruijn sequence \( S_4 \) is a string of bits \( s_i \in \{0,1\} = \{s_1, \ldots, s_{2^4}\} \), \( i = 1, 2, \ldots, 2^4 \), such that each string with \( n = 4 \), \( \{a_1, \ldots, a_4\} \in \{0,1\}^4 \), occurs consecutively once. By using the Generalized Prefer- Opposite algorithm, the output of the De Bruijn binary sequence order 4 with a feedback function of the family two \( f(x_0, \ldots, x_3) = 1 + x_2 \cdot x_3 \) and the initial state \( b = 1100 \) are as follows:

\[
S_4 := (1100 \ 0010 \ 0111 \ 1010)
\]

The following sequence of states

\[
b = 1100 \rightarrow 1000 \rightarrow 0000 \rightarrow 0010 \rightarrow 0100 \rightarrow 1001 \rightarrow 0011 \rightarrow 0111 \rightarrow 1111 \rightarrow 1110 \rightarrow 1010 \rightarrow 0101 \rightarrow 1011 \rightarrow 0110 \rightarrow 1100.
\]

Proof:

The \( x_0 \) coefficient in \( f \) is 0, for any non-leaf state \( G_{f_2(4)} \) in figure 1 has exactly two children. The graph state \( G_{f_2(4)} \) contains a directed cycle, namely \( g_{f_2(4)} \) in figure 2 where each vertex is the \( n \)-stage state of \( S_4 \). All states outside the cycle are vertices in the tree where each root is the state that is above the cycle. Because there is a unique path leading from any state \( u \) to state \( v \) in the cycle, as a result there is a unique path leading to any state in \( G_{f_2(4)} \) to the initial state \( b \). Both conditions in Theorem 2 are met. ■
Furthermore, it is verified that the sequence obtained satisfies Lemma 1. For each non-leaf state $u$ has two children $v$ and $w$ in $G_{2(4)}$, it will be proven that the children of $u$, namely state $v$ and $w$, are first passed by the GPO algorithm. Suppose that any non-leaf state $u = 1110$ is chosen with the two children, $v = 0111$ and $w = 1111$. The GPO algorithm is run from the initial state $b \neq u$ onwards until it arrives at state $u$. It can be seen in sequence of states that state $v$ and $w$ are passed before state $u$. So, Lemma 1 is fulfilled.

4. Conclusion

Based on the results of the discussion of this journal, it can be concluded that the Generalized Prefer-Opposite (GPO) Algorithm with input feedback function and initial state of family two for $(x_0, \ldots, x_{n-1}) = 1 + \prod_{t=1}^{n-1} x_t$, $0 < t < n$, $t = 2$ and $n = 4$ construct a de Bruijn binary sequence, namely $S_4 := (1100 0010 0111 1010)$. Each string with $n = 4$, $\{a_1, \ldots, a_4\} \in \{0,1\}^4$ in $S_4$ appears exactly one time.

Acknowledgments

We would like to say thanks to the Mathematics Department, Faculty of Mathematics and Natural Science, University of Bengkulu for the support of this paper.

References

[1] Sambas A, Vaidyanathan S, Tlelo-Cuautle E, Abd-El-Atty B, Abd El-Latif A A, Guillén-Fernández, O, Hidayat Y, Gundara G 2020 A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption IEEE Access 8 137116-137132
[2] Vaidyanathan S, Azar A T, Rajagopal K, Sambas A, Kacar S and Cavusoglu U 2018 A new hyperchaotic temperature fluctuations model, its circuit simulation, FPGA implementation and an application to image encryption International Journal of Simulation and Process Modelling 13 (3) 281-296
[3] Chang Z, Ezerman M F and Fahreza A A 2020 On greedy algorithms for binary de Bruijn sequences Applicable Algebra in Engineering, Communication and Computing 1-28
[4] Kang Y, Li J, Yuan Q and Sun S 2020 Adjacent vertex sum reducible edge coloring algorithm based on graph cryptography 2020 IEEE 9th Joint International Information Technology and
[5] Bondy J A and Murty U S R 1976 *Graph theory with applications* London: Macmillan

[6] De Bruijn N G 1946 A combinatorial problem *Koninklijke Nederlandse Academie van Wetenschappen* 49 758-764

[7] Woo K S, Wang Y, Kim Y, Kim J, Kim W and Hwang C S 2020 Hardware-Based Security: A Combination of a Volatile-Memristor-Based True Random-Number Generator and a Nonlinear-Feedback Shift Register for High-Speed Encryption *Advanced Electronic Materials* 6 (5) 2070022

[8] Zhong J and Lin D 2018 On minimum period of nonlinear feedback shift registers in grain-like structure *IEEE Transactions on Information Theory* 64 (9) 6429-6442

[9] Bonifati A, Holubová I, Prat-Pérez A and Sakr S 2020 Graph Generators: State of the art and open challenges *ACM Computing Surveys* 53 (2) 1-30

[10] Bi S and Zhang Y J A 2017 Graph-based cyber security analysis of state estimation in smart power grid *IEEE Communications Magazine* 55 (4) 176-183