드부루인 수열을 이용한 주파수 도약수열
(Frequency Hopping Sequences Using de Bruijn Sequences)

은 유 창*, 박성복**, 이광억**, 송홍엽*

* 연세대학교

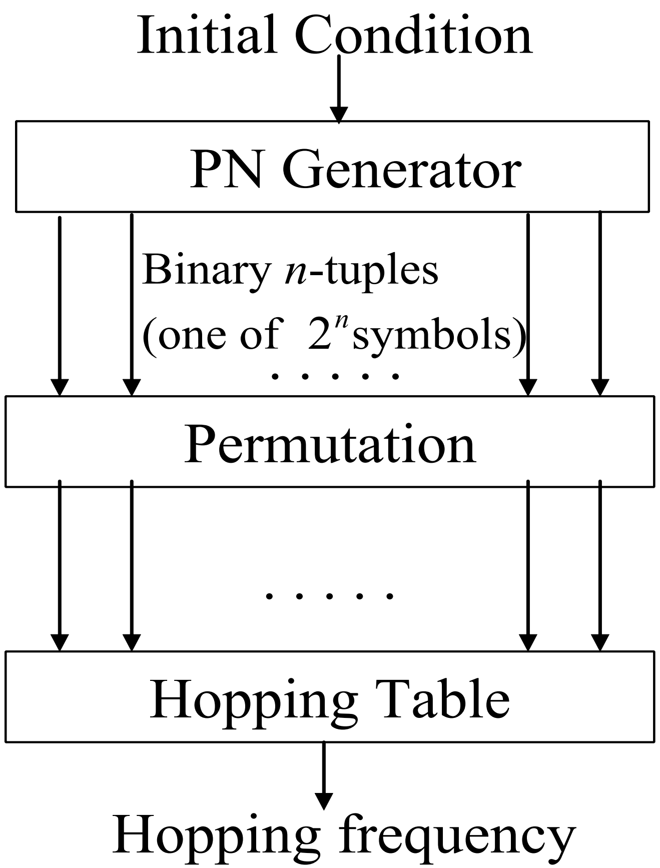
** 국방과학 연구소

YONSEI
UNIVERSITY

AGENCY for DEFENSE
DEVELOPEMENT

Contents

Introduction (I)



< Requirements >

- Binary PN generator for the minimal hardware complexity
- Symbols should appear as equally often as possible.
- Large linear complexity
- Better Hamming correlation is desirable.
- When the number of the hopping slots (the sequence's symbols) is not a power of 2

Introduction (II)

1) Easy to generate and higher linear complexity

$\Rightarrow$ Binary non-linear Feedback Shift Register is a choice

2) All of the 2^n frequency slots must be used in one period as equally often as possible

$\Rightarrow$ A de Bruijn sequence is a solution.

Example 1) n-degree de Bruijn sequence of period = 2^n

$$\ldots, a_i, a_{i+1}, a_{i+2}, \ldots\ldots, a_{i+n-1}, a_{i+n}, a_{i+n+1}, \ldots$$

Introduction (III)

Example) a de Bruijn sequence of period = 16

7

1

0 0 0 0 1 1 1 1 0 1 1 0 0 1 0 1 . . .

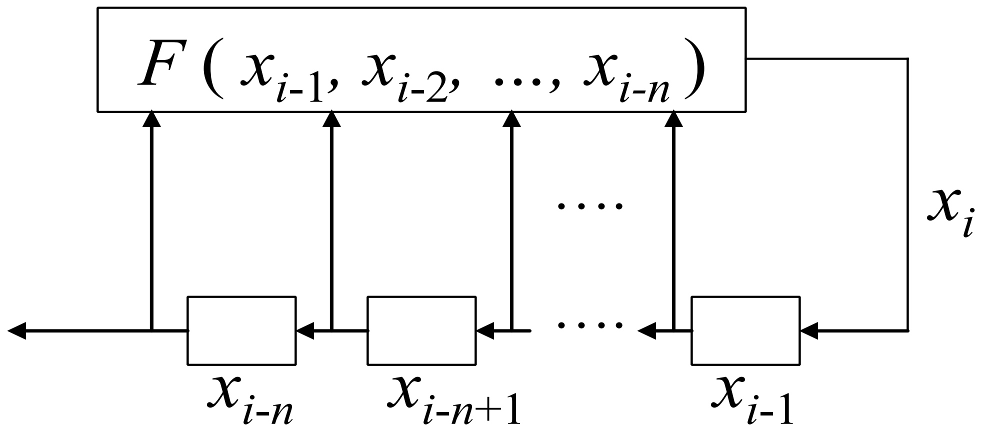
0

3

➔ 0 1 3 7 15 14 13 11 6 12 9 2 5 10 4 8 . . .

de Bruijn squence (I)

< generic FSR configuration >



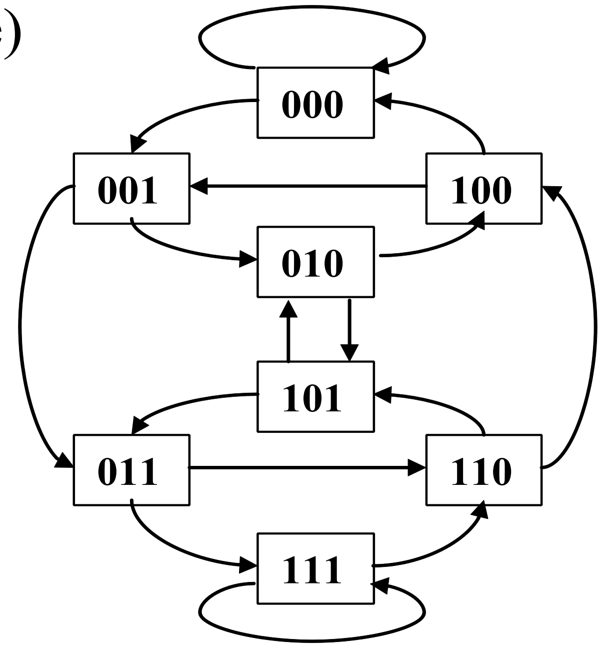
- Initial Condition : $x_0, x_1, x_2, \ldots\ldots, x_{n-1}$
- For $i = n, n+1, \ldots\ldots$ $x_i = F(x_{i-1}, x_{i-2}, \ldots\ldots, x_{i-n})$

de Bruijn squence (II)

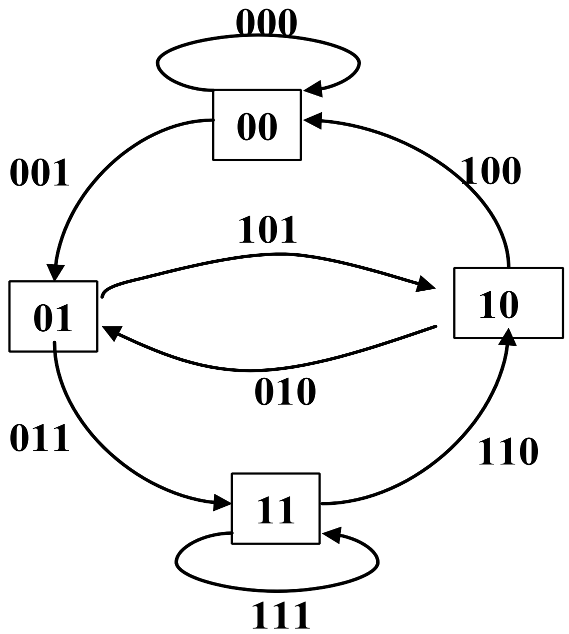
- A state transition is a mapping from binary n-space Ω_n to itself

$$\Omega_n \to \Omega_n \quad \text{i.e.,} \quad (x_1, x_2, \ldots, x_n) \to (x_2, x_3, \ldots, x_n, F(x_1, x_2, \ldots x_n))$$

Example)



a) The nodes of Good's diagram n=3



b) The edges of Good's diagram n*=n-1=2

- *Full cycle search => a) Hamiltonian path b) Eulerian path*

=> $2^{2^{n-1}-n}$ *complete paths (de Bruijn sequence)*

de Bruijn squence (III)

(2) The linear complexity distribution of de Bruijn sequences for n=4

Linear complexity	# of sequences	Sequence indices	Connection Polynomial (increasing order)
12	4	2, 3, 6, 10	1 0 0 0 1 0 0 0 1 0 0 0 1
13	0	*	*
14	4	7, 8, 9, 11	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
15	8	0, 1, 4, 5, 12, 13, 14, 15	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

- L = linear complexity of a de Bruijn sequence of period 2^n

$$\Rightarrow \quad \boxed{2^{n-1} + n \le L \le 2^n - 1}$$

- The reason for using de Bruijn sequences as frequency hopping patterns

1) span n property 2) large linear span

de Bruijn squence (IV)

(1) An example for de Bruijn sequences (n=4)

index	binary sequences	16-ary sequences	8-ary sequences
0	0 0 0 0 1 1 1 1 0 1 1 0 0 1 0 1	0 1 3 7 15 14 13 11 6 12 9 2 5 10 4 8	0 0 1 3 7 7 6 5 3 6 4 1 2 5 2 4
1	0 0 0 0 1 1 1 1 0 1 0 1 1 0 0 1	0 1 3 7 15 14 13 10 5 11 6 12 9 2 4 8	0 0 1 3 7 7 6 5 2 5 3 6 4 1 2 4
2	0 0 0 0 1 1 1 1 0 1 0 0 1 0 1 1	0 1 3 7 15 14 13 10 4 9 2 5 11 6 12 8	0 0 1 3 7 7 6 5 2 4 1 2 5 3 6 4
3	0 0 0 0 1 1 1 1 0 0 1 0 1 1 0 1	0 1 3 7 15 14 12 9 2 5 11 6 13 10 4 8	0 0 1 3 7 7 6 4 1 2 5 3 6 5 2 4
4	0 0 0 0 1 1 0 1 1 1 1 0 0 1 0 1	0 1 3 6 13 11 7 15 14 12 9 2 5 10 4 8	0 0 1 3 6 5 3 7 7 6 4 1 2 5 2 4
5	0 0 0 0 1 1 0 1 0 1 1 1 1 0 0 1	0 1 3 6 13 10 5 11 7 15 14 12 9 2 4 8	0 0 1 3 6 5 2 5 3 7 7 6 4 1 2 4
6	0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 1	0 1 3 6 13 10 4 9 2 5 11 7 15 14 12 8	0 0 1 3 6 5 2 4 1 2 5 3 7 7 6 4
7	0 0 0 0 1 1 0 0 1 0 1 1 1 1 0 1	0 1 3 6 12 9 2 5 11 7 15 14 13 10 4 8	0 0 1 3 6 4 1 2 5 3 7 7 6 5 2 4
8	0 0 0 0 1 0 1 1 1 1 0 1 0 0 1 1	0 1 2 5 11 7 15 14 13 10 4 9 3 6 12 8	0 0 1 2 5 3 7 7 6 5 2 4 1 3 6 4
9	0 0 0 0 1 0 1 1 1 1 0 0 1 1 0 1	0 1 2 5 11 7 15 14 12 9 3 6 13 10 4 8	0 0 1 2 5 3 7 7 6 4 1 3 6 5 2 4
10	0 0 0 0 1 0 1 1 0 1 0 0 1 1 1 1	0 1 2 5 11 6 13 10 4 9 3 7 15 14 12 8	0 0 1 2 5 3 6 5 2 4 1 3 7 7 6 4
11	0 0 0 0 1 0 1 1 0 0 1 1 1 1 0 1	0 1 2 5 11 6 12 9 3 7 15 14 13 10 4 8	0 0 1 2 5 3 6 4 1 3 7 7 6 5 2 4
12	0 0 0 0 1 0 1 0 0 1 1 1 1 0 1 1	0 1 2 5 10 4 9 3 7 15 14 13 11 6 12 8	0 0 1 2 5 2 4 1 3 7 7 6 5 3 6 4
13	0 0 0 0 1 0 1 0 0 1 1 0 1 1 1 1	0 1 2 5 10 4 9 3 6 13 11 7 15 14 12 8	0 0 1 2 5 2 4 1 3 6 5 3 7 7 6 4
14	0 0 0 0 1 0 0 1 1 1 1 0 1 0 1 1	0 1 2 4 9 3 7 15 14 13 10 5 11 6 12 8	0 0 1 2 4 1 3 7 7 6 5 2 5 3 6 4
15	0 0 0 0 1 0 0 1 1 0 1 0 1 1 1 1	0 1 2 4 9 3 6 13 10 5 11 7 15 14 12 8	0 0 1 2 4 1 3 6 5 2 5 3 7 7 6 4

Note) 1st and 15th sequences are the extended m-sequences.

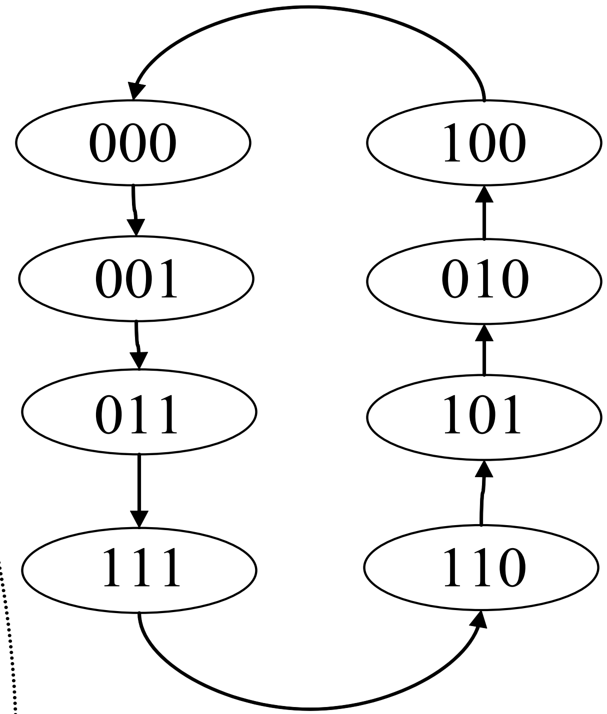
Truth Table Approach (I)

< Theorem 1 > (branchless condition)

Feedback function values of the top half is the complement of the bottom half iff, the cycles generated by the function have no branch points.

Ex1)

Input			Output
a_1	a_2	a_3	a_4
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0



$$a_k = F(a_{k-1}, \ldots, a_{k-n}) = a_{k-1} \oplus f(a_{k-2}, \ldots, a_{k-n})$$

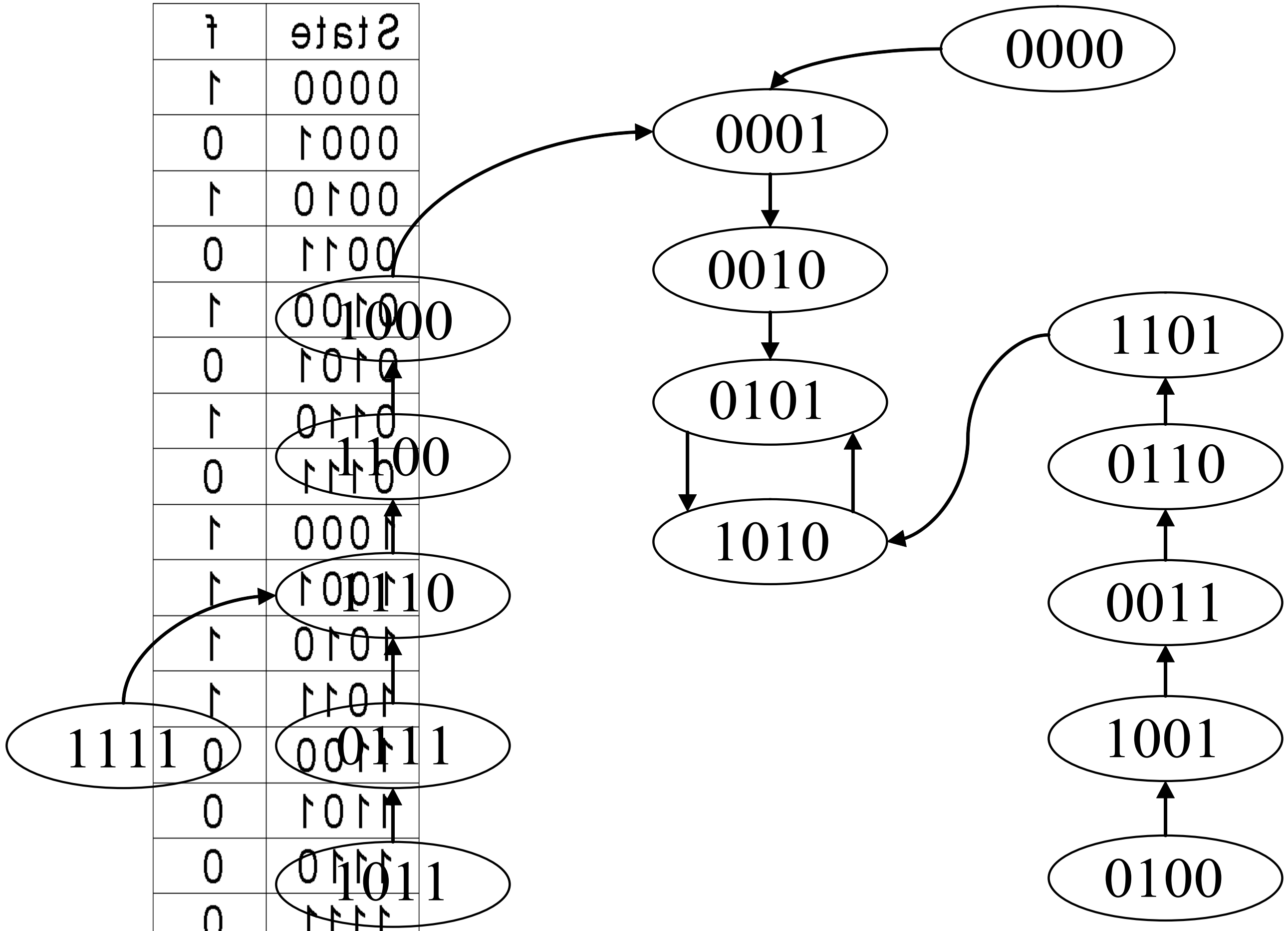
Truth Table Approach (II)

Ex2)

(1) Truth table

State	f
0000	1
0001	0
0010	1
0011	0
0100	1
0101	0
0110	1
0111	0
1000	1
1001	1
1010	1
1011	1
1100	0
1101	0
1110	0
1111	0

(2) State diagram



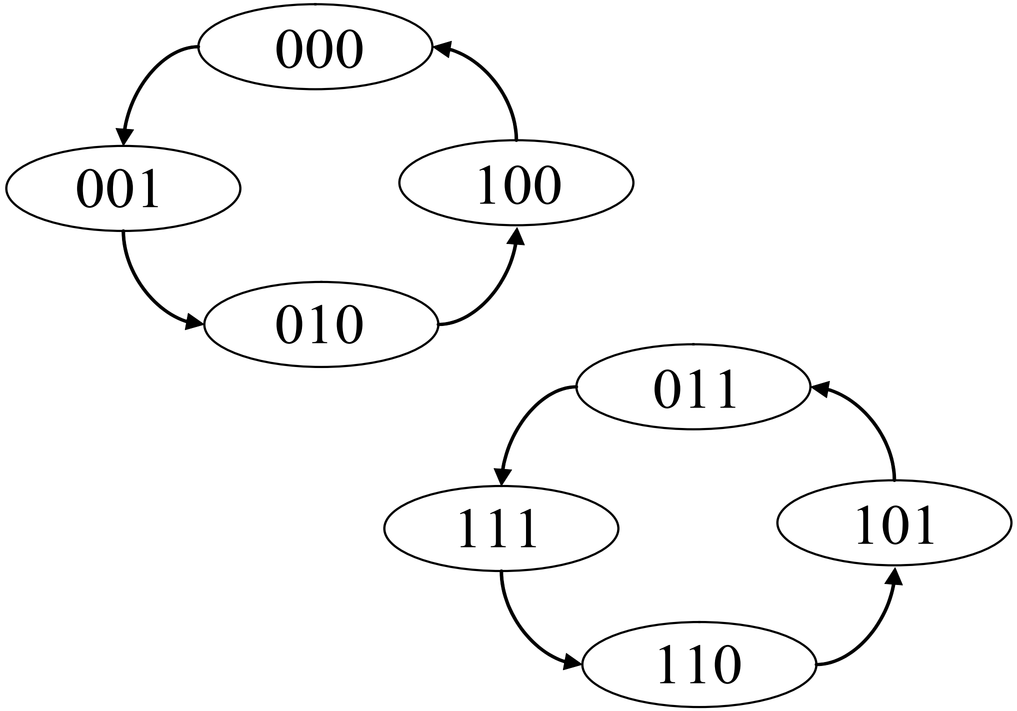
Truth Table Approach (III)

< Theorem 2 > (cycle parity condition)

For n>2, the parity of the number of cycles satisfying theorem 1 is even or odd according to whether the number of 1's in the truth table of $f(a_{k-2},\ldots,a_{k-n})$ is even or odd.

Ex2)

Input			Output
a_1	a_2	a_3	a_4
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0



Truth Table Approach (IV)

< Theorem 3 >

The cycle all 0's occurs iff $f(0,\ldots,0)=0$

The cycle all 1's occurs iff $f(1,\ldots,1)=0$

=> $f(0,\ldots,0)=1$ iff The cycle all 0's never occurs

$f(1,\ldots,1)=1$ iff The cycle all 1's never occurs

- The number of all possible degree n sequence by f is $2^{2^{n-1}}$
- The number of all degree n de Bruijn sequence is $2^{2^{n-1}-n}$ $(=2^{2^{n-1}}/2^n)$

- Using theorem 1, 2, 3,

  For n= 1, 2, 3, the de Bruijn sequences are characterized by the following conditions

  1. $f(0,\ldots,0)=1$
  2. $f(1,\ldots,1)=1$
  3. $\sum_v f(v)=1$

- Generally, The above three condition reduce the number of the sequence to $2^{2^{n-1}}/2^3$
- For n>4, there is no general condition except the above three conditions.

Truth Table Approach (V)

- The weight range of a feedback function *f* 's output

$$Z_n - 1 \le w \le 2^{n-1} - Z_n^* + 1 \quad (w \text{ is odd by theorem 2})$$

Where

$$Z_n = \frac{1}{n} \sum_{d|n} \phi(d) 2^{n/d}$$

$$Z_n^* = \frac{Z_n}{2} - \frac{1}{2n} \sum_{2d|n} \phi(2d) 2^{n/2d}$$

Arbitrary Number of symbols (I)
(Example1: Symbol Addition)

- S1 sequence: period=$L1$, symbol=$q1$
  S2 sequence: period=$L2$, symbol=$q2$

$$S3(i) = S1(i) + S2(i)$$

$\Rightarrow$ S3 sequence : period L = L.C.M($L1$,$L2$)
symbol $q = q1+q2-1$

- Ex) S1 ($L1$=16, $q1$=8) , S2 ($L1$=3, $q1$=3)
  => S3 (L=48, q=10)

S1: 0 0 1 3 7 7 6 5 3 6 4 1 2 5 2 4 0 0 1 3 . . .
\+ S2: 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 . . .

S3: 0 1 3 3 8 9 6 6 5 6 5 3 2 6 4 4 1 2 1 4 . . .

Arbitrary Number of symbols (II)
(Example1: Symbol Addition)

❖ S1 sequence (0 0 1 3 7 7 6 5 3 6 4 1 2 5 2 4 0 0 1 3) : period=16, symbol=8
S2 sequence (0 1 2 … … *q2-1*) : period=*q2*, symbol=*q2*

=> S3 sequence : L =L.C.M(16,$q2$), q=8+$q2$-1 (slots)

(W:symbol weight, F:weight frequency)

9 slots (16)		10 slots (48)		11 slots (16)		12 slots (80)		13 slots (48)		14 slots (112)		15 slots (16)	
W	F	W	F	W	F	W	F	W	F	W	F	W	F
1	4	2	2	1	3	2	2	1	2	2	2	1	6
2	3	4	2	2	2	4	2	2	2	4	2	2	2
3	2	6	6	3	3	6	2	3	2	6	2	3	2
						8	2	4	4	8	2		
						10	4	6	2	10	2		
								8	1	12	2		
										14	2		

Arbitrary Number of symbols (III) (Example 2: Symbol Insertion)

❖ S1 de Bruijn sequence: period = 2^{n_1}
symbol = 2^{k_1} $(n_1 > k_1)$

S2 de Bruijn sequence: period = 2^{n_2} $(n_1 \ge n_2 \ge k_1)$
symbol = 2^{k_1}

$\Rightarrow$ $2^{k_2} (< 2^{k_1})$ symbols are selected among 2^{k_1} symbols in S2

$\Rightarrow$ The selected symbols from S2 are inserted to S1 to make the new sequence S.

$\Rightarrow$ # of symbols of S = $2^{k_1} + 2^{k_2}$

Period of S = $(2^{k_1} + 2^{k_2}) \times 2^{n_1 - k_1}$

- S1 de Bruijn sequence: period = 2^3, symbol = 2^3

  S2 de Bruijn sequence: period = 2^3, symbol = 2^3

➔ S: symbol= $2^3 + 2^2$, Period = $(2^3 + 2^2) \times 2$

S_1	0		0		1		3		6		5		2		5	
S_2		1		3		6		5		3		7		7		6
S	0	X	0	X	1	10	3	9	6	X	5	11	2	11	5	10

S_1	3		7		7		6		4		1		2		4	
S_2		4		0		0		1		2		5		2		4
S	3	8	7	X	7	X	6	X	4	X	1	9	2	X	4	8

➔ S : 0 0 1 10 3 9 6 5 11 2 11 5 10 3 8 7 7 6 4 1 9 2 4 8 … …

6. Concluding Remark

• de Bruijn sequences have good properties as frequency hopping sequences.
  => Span *n* property
  => Large linear complexity

• The truth table properties of de Bruijn Sequences can be used to reduce the their searching range.

• Symbol insertion method can be expanded to any sequence where the number of symbols is the form of $2^{k_1} + 2^{k_2} + \cdots + 2^{k_n}$
  i.e. even number.