Aperiodic Perfect Maps from de Bruijn Sequences[1]

SANG-MOK KIM,
DIVISION OF GENERAL EDUCATION - MATHEMATICS
KWANGWOON UNIVERSITY
SEOUL 139-701, KOREA

e-mail: smkim@kw.ac.kr

Revised July 13, 2007

Abstract. An aperiodic perfect map(APM) is an array with the property that each possible array of a given size, called a window, arises exactly once as a contiguous subarray in the array. In this paper, we give a construction method of an APM being a proper concatenation of some fragments of a given de Bruijn sequence. Firstly, we give a criterion to determine whether a designed sequence T with entries from the index set of a de Bruijn sequence can generate an APM. This implies a sufficient condition for being an APM. Secondly, two infinite families of APMs are given by constructions of corresponding sequences T, respectively, satisfying the criterion.

Footnotes:
2000 Mathematics Subject Classification : 94A55, 05B30.
Key words and phrases : de Bruijn Sequence, Aperiodic Perfect Map, Window property

1 Introduction

The perfect window property is defined as follows; for a given c-ary $m \times n$ array and fixed integers u and v with $u \leq m$ and $v \leq n$, every possible c-ary $u \times v$ array occurs exactly once as a contiguous subarray, called a *window*. A c-ary *aperiodic perfect map*(APM) is a c-ary $m \times n$ array satisfying the *perfect window property*. Analogously, a periodic array is called a c-ary *periodic perfect map*(PM) if it satisfies the perfect window property in a single period. A de Bruijn sequence is the simplest PM, which is a periodic sequence with the perfect window property.

The perfect window property has been studied for 60 years because of useful and possible applications to information theory. For example, in the theory of cryptography, it is well-known that a de Bruijn sequence plays an important role as a key of a stream cipher(see [8]). APMs can be applicable to encoding schemes for sending a two-dimensional position. The idea is that if such an APM is written onto a rectangular surface and there is a device which can examine a certain size of subarray, then examining a subarray can determine its position in the array. On the other hand, the same idea can be applied to the situation

[1]This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD)(KRF-2005- 003-C0006).

that a PM is written onto a torus and a device can examine a certain size of subarray (see J. Burns and C. Mitchell [2]).

The perfect window property was firstly studied for periodic sequences, in particular, de Bruijn sequences. Many construction methods for de Bruijn sequences have been devised ([4]), and the existence of de Bruijn sequences has been established ([1], [3], [11]) for each set of admissible parameters.

For the case of arrays, it is shown by K. Paterson ([9], [10]) that a c-ary PM exists for every possible parameter set when the alphabet size c is a prime power. A PM can be simply transformed into an APM of a slightly larger size by simple extension (seen in S. Kanetkar and M. Wage [6]). However, there are APMs which are not extensions of any PM(See [7]). Furthermore, since the existence of a c-ary PM is known only when the alphabet size c is a prime power (see [9], [10]), the general question about the existence for a c-ary APM for all alphabet size c can not be achieved from the known constructions of c-ary PMs. Not many results on the existence of APM have been known in general. For instance, C. Mitchell [8] (1995) shows that the binary(2-ary) APM always exists, and S.-M. Kim [7] (2002) shows the existence of c-ary APM for 2 by 2 windows for all alphabet sizes c.

In this paper, we deal with a construction of APMs generated from a concatenation of fixed size windows of a given de Bruijn sequence. First, we give a construction method of an array, namely a $(T, [B]_m)$-array for a given de Bruijn sequence B, a fixed row size of the array m and a sequence T with entries from the index set of B. Next, we give a criterion which determines whether the sequence T generates a $(T, [B]_m)$-array that is an APM. Finally, two families of APMs are given, as examples, by constructing such sequences T satisfying the criterion which is a sufficient condition for the generated arrays to be APMs. Note that the existence of $(c^u + 1, c^u + u - 1; 2, u)$APM for any alphabet size c follows directly from the first construction in the examples.

2 Definitions and basic properties

We now begin with formal definitions together with known results on the subject of APMs and PMs, respectively. Most terminologies follow C. Mitchell [8] and S.-M. Kim [7].

We first formalize the definition of arrays and windows. For a positive integer m, from now on, we denote $\{0, \ldots, m-1\}$ by $\mathbb{N}_m$ and $\{1, \ldots, m\}$ by $[m]$. Now, we represent a c-ary $m \times n$ array as

$$A = (a_{i\,j})$$

where $a_{i\,j} \in \mathbb{N}_c$ for each $i \in \mathbb{N}_m$ and $j \in \mathbb{N}_n$. For given integers $s \in \mathbb{N}_m$ and $t \in \mathbb{N}_n$, define the (s,t)-th $u \times v$ *window* of A to be a $u \times v$ subarray

$$A_{s\,t} = (\alpha_{i\,j})$$

such that, for each $i \in \mathbb{N}_s$ and $j \in \mathbb{N}_t$,

$$\alpha_{i\,j} = a_{i+s\;j+t}$$

where $i+s$ is computed modulo m and $j+t$ is computed modulo n. For integers $m_0 \in [m]$ and $n_0 \in [n]$, we denote by $[A_{m_0 \times n_0}]_{u \times v}$ the set of $u \times v$ windows $A_{s\,t}$ for $s \in \mathbb{N}_{m_0}$ and $t \in \mathbb{N}_{n_0}$. Note that the following bounds

$$1 \leq \left|[A_{m_0 \times n_0}]_{u \times v}\right| \leq m_0 n_0$$

are immediate since the lower bound holds only if all windows are identical and the upper bound holds if they are all distinct.

A $1 \times n$ array $A = (a_{0\,0}\ a_{0\,1}\ \ldots\ a_{0\,n-1})$ may be considered as a sequence of length n and so it is simply denoted by

$$A = (a_0\, a_1 \ldots a_{n-1}) = (a_i)$$

for $i \in \mathbb{N}_n$, in which the set of integers $\{0, 1, \ldots, n-1\} (= \mathbb{N}_n)$ is called the index set of A. For integers $n_0 \in [n]$ and $t \in \mathbb{N}_{n_0}$, we also simplify a $1 \times v$ window $A_{1\,t}$ as a v-window A_t, and $[A_{m_0 \times n_0}]_{1 \times v}$ as $[A_{n_0}]_v$.

We now observe the perfect window property applied to the periodic arrays.

Definition 1 A c-ary span v de Bruijn sequence $B = (b_i)$ is defined as a periodic sequence of length $n = c^v$ with entries from $\{0, 1, \ldots, c-1\}$ in which every distinct c-ary v-tuple occurs exactly once as a v-window B_t for some integer t with $0 \leq t \leq c^v - 1$.

Definition 2 Let c, m, n, u and v be integers satisfying $c \geq 2$, $m \geq u \geq 1$, and $n \geq v \geq 1$. A c-ary $m \times n$ array $A = (a_{i\,j})$ is called a c-ary $(m, n; u, v)$ Perfect Map (or simply PM) if each possible c-ary $u \times v$ array occurs exactly once as a $u \times v$ window $A_{s\,t}$ of A for some $s \in \mathbb{N}_m$ and $t \in \mathbb{N}_n$.

As has been observed, a c-ary span v de Bruijn sequence is a c-ary $(1, c^v; 1, v)$PM. The following necessary conditions for the existence of a PM are immediate.

Lemma 3 ([8]) If A is a c-ary $(m, n; u, v)$PM, then the parameters satisfy the following.

(i) $m > u$ or $m = u = 1$,

(ii) $n > v$ or $n = v = 1$, and

(iii) $mn = c^{uv}$.

If the positive integers c, m, n, u and v satisfy the necessary conditions for the existence of a PM in Lemma 3, the set of ordered integers $(c; m, n; u, v)$ is called an *admissible parameter set* for PM.

We next define an aperiodic perfect map as follows.

Definition 4 Let c, m, n, u and v be integers with $c \geq 2$, $1 \leq u \leq m$, and $1 \leq v \leq n$. A c-ary $m \times n$ *array* $A = (a_{i\,j})$ is called a c-ary $(m, n; u, v)$ *aperiodic perfect map* (or simply APM) if each possible c-ary $u \times v$ array occurs exactly once as a window $A_{s\,t}$ of A for some $s \in \mathbb{N}_{m-u+1}$ and $t \in \mathbb{N}_{n-v+1}$.

We also call $(c; m, n; u, v)$ an admissible parameter set for APM if it satisfies the conditions given in the following lemma.

Lemma 5 ([8]) If A is a c-ary $(m, n; u, v)$APM, then the parameters satisfy the following.

(i) $m \geq u$,

(ii) $n \geq v$ and

(iii) $(m - u + 1)(n - v + 1) = c^{uv}$.

According to S. Kanetkar and M. Wage [6], a PM can be transformed into an APM of a slightly larger size by simple extension, as follows. For a given c-ary $(m, n; u, v)$PM $A = (a_{i\,j})$, define an $(m + u - 1) \times (n + v - 1)$ array $\bar{A} = (\bar{a}_{i\,j})$ as

$$\bar{a}_{i\,j} = a_{s\,t}$$

where $s \equiv i \,(mod\, m)$ and $t \equiv j \,(mod\, n)$ for each $i \in \mathbb{N}_{m+u-1}$ and $j \in \mathbb{N}_{n+v-1}$. Then, from the definition, we can immediately show that $\bar{A}$ is a c-ary $(m + u - 1, n + v - 1; u, v)$APM. We call $\bar{A}$ the *closure* of a given PM A. Conversely, a c-ary (m, n, u, v)APM arises, by the construction of Kanetkar and Wage, from a c-ary $(m-u+1, n-v+1, u, v)$PM whose parameters must satisfy the conditions $u = m - u + 1 = 1$ or $m - u + 1 > u$, and $v = n - v + 1 = 1$ or $n - v + 1 > v$ i.e. the parameters of the APM that arises satisfy $m = u = 1$ or $m \geq 2u$, and $n = v = 1$ or $n \geq 2v$.

We finally note the following remark on some possible restrictions of the parameters of PMs and APMs (see [7]).

Remark 6 For a c-ary $m \times n$ array $A = (a_{i\,j})$, the transpose of A is written as $A' = (a'_{i\,j})$ which is the c-ary $n \times m$ array with $a'_{i\,j} = a_{j\,i}$. If A is a PM (or an APM) then A' is also a PM (or an APM, respectively). Hence, without loss of generality, we need only consider those c-ary (m, n, u, v)PM (or APM) with $n \geq m$ and so we restrict our definition of admissible parameter set for PM (or APM) to those with $n \geq m$.

3 A sufficient condition to be APM derived from de Bruijn sequence

For a given c-ary span u de Bruijn sequence B, we first suppose an admissible parameter set $(c; m, n; u, v)$ for APM such that $u \leq m \leq c^u + u - 1$. We establish a criterion to determine a sequence T with entries from index set of B which gives the shifting process of m-windows of a given de Bruijn sequence so that the concatenation of the shifted windows becomes an APM.

Let $B = (b_i)$ be a c-ary span u de Bruijn sequence with index set $\mathbb{N}_{c^u}$ and let $\bar{B} = (\bar{b}_i)$ be the closure of B. Let m be an integer with $u \leq m \leq c^u + u - 1$. Note that the definition of the de Bruijn sequence implies that

$$|[B_{c^u}]_u| = |[B_{c^u}]_m| = c^u \tag{1}$$

since all u-windows B_i, $i = 0, 1, ..., c^u - 1$ are distinct and therefore all m-windows B_i, $i = 0, 1, ..., c^u - 1$, are distinct.
Let $T = (t_i)$ be a finite sequence of length n with the entries $t_i \in \mathbb{N}_{c^u}$ for $0 \leq i \leq n-1$. Since there is a natural one to one correspondence ϕ between $\mathbb{N}_{c^u}$ and $[B_{c^u}]_m$ given by $\phi(t_i) = B_{t_i}$, the sequence $T = (t_i)$ produces an associated $m \times n$ *array* A

$$\begin{aligned} A &= (\phi(t_0)'\ \phi(t_1)'\ \ldots\ \phi(t_{n-1})') \\ &= (B_{t_0}'\ B_{t_1}'\ldots.\ B_{t_{n-1}}') \end{aligned}$$

where B_{t_i}' is the transpose of B_{t_i}. This means that A is the concatenation of the transposes of the m-windows of B corresponding to the entries $t_i \in T$. We say that A is the $(T, [B_{c^u}]_m)$-array. If we denote the array $A = (a_{i\,j})$, then we have

$$a_{i\,j} = b_{i+t_j}.$$

Let $A_{k\,l} = (\alpha_{i\,j})$ be a $u \times v$ window of A for $k \in \mathbb{N}_{m-u+1}$ and $l \in \mathbb{N}_{n-v+1}$. Then, for each $i \in \mathbb{N}_u$ and $j \in \mathbb{N}_v$ the entry $\alpha_{i\,j}$ of $A_{k\,l}$ is expressed as

$$\alpha_{i\,j} = a_{i+k\,j+l} = b_{i+k+t_{j+l}}. \tag{2}$$

in terms of (b_i).

Lemma 7 Let u, v, m, n be positive integers with $u \leq m \leq n$ and $v \leq n$. For a given c-ary span u de Bruijn sequence B and a finite sequence $T = (t_i)$ for $i \in \mathbb{N}_n$ with entries t_i from $\mathbb{N}_{c^u}$(the index set of B), suppose that A is the $(T, [B_{c^u}]_m)$-array. If $A_{k\,l}$ and $A_{k'\,l'}$ are $u \times v$ windows of A for k, $k' \in \mathbb{N}_{m-u+1}$ and l, $l' \in \mathbb{N}_{n-v+1}$, then we have

(i) $u - m \leq k - k' \leq m - u$,

(ii) $A_{k\,l} = A_{k'\,l'}$ if and only if $k - k' \equiv t_{j+l'} - t_{j+l} \pmod{c^u}$ for all $j \in \mathbb{N}_v$.

Proof.

(i) Since $0 \leq k,\ k' \leq m - u$, we have $u - m \leq -k' \leq k - k' \leq k \leq m - u$.

(ii) Let $A_{k\,l} = (\alpha_{ij})$ and $A_{k'\,l'} = (\beta_{ij})$. Then $A_{k\,l} = A_{k'\,l'}$ if and only if $\alpha_{i\,j} = \beta_{i\,j}$ for all $i \in \mathbb{N}_u$ and $j \in \mathbb{N}_v$, i.e. $b_{i+k+t_{j+l}} = b_{i+k'+t_{j+l'}}$. This holds if and only if $B_{k+t_{j+l}} = B_{k'+t_{j+l}}$ for all $j \in \mathbb{N}_v$. This holds if and only if $k + t_{j+l} \equiv k' + t_{j+l'} \pmod{c^u}$ for all $j \in \mathbb{N}_v$, since B is a c-ary span u de Bruijn sequence, i.e. $k - k' \equiv t_{j+l'} - t_{j+l} \pmod{c^u}$ for all $j \in \mathbb{N}_v$.

■

We use the notation $[t_i]_v$ to denote T_i (a v-window $(t_i,\ t_{i+1}\ \ldots\ t_{i+v-1})$ of T), and $[t_i+\alpha]_v$ to denote $(t_i+\alpha\ t_{i+1}+\alpha\ \ldots\ t_{i+v-1}+\alpha)$ for $\alpha \in \mathbb{N}_{c^u}$. Then, (ii) in Lemma 7 can be written as

$$A_{k\,l} = A_{k'\,l'} \text{ if and only if } [t_{l'}]_v = [t_l+\alpha]_v$$

where $\alpha = k - k'$. Now we state a theorem to be a criterion for a type of APMs.

Theorem 8 Let $(c; m, n; u, v)$ be an admissible parameter set for APM. Let $B = (b_i)$ be a c-ary span u de Bruijn sequence and let $T = (t_i)$ be a finite sequence of length n $(0 \le i \le n-1)$ with the entries $t_i \in \mathbb{N}_{c^u}$. Suppose that T satisfies the following conditions.

(i) $[t_i]_v \neq [t_j]_v$ for all $i, j \in \mathbb{N}_{n-v+1}$ with $i \neq j$.

(ii) $[t_j]_v \neq [t_i+\alpha]_v$ for all $i, j \in \mathbb{N}_{n-v+1}$ and all non-zero integer α with $u-m \le \alpha \le m-u$. i.e. $[t_i+\alpha]_v \notin [T_{n-v+1}]_v$ for $i, j \in \mathbb{N}_{n-v+1}$ and all non-zero integer α with $u-m \le \alpha \le m-u$.

Then, the $(T, [B_{c^u}]_m) - array\ A$ is a c-ary $(m, n; u, v)$APM.

Proof. The result follows immediately by Lemma 7. If T satisfies (i) and (ii), it follows that all the $u \times v$ windows $A_{s\,t}$ for $s \in \mathbb{N}_{m-u+1}$ and $t \in \mathbb{N}_{n-v+1}$ are distinct. Moreover, the parameters m, n, u and v satisfy the necessary conditions for the existence of a c-ary APM. So every c-ary $u \times v$ window appears exactly once in $[A_{(m-u+1)\times(n-m+1)}]_{u\times v}$. ■

Referring to Theorem 8, it can be seen that, for given parameters satisfying the necessary conditions for existence of an APM (Lemma 5), whether the $(T, [B_{c^u}]_m)$-array constructed from a c-ary span u de Bruijn sequence and a finite sequence T with entries $t_i \in \mathbb{N}_{c^u}$ is an APM depends on the choice of the sequence T to satisfy the conditions in Theorem 8. In fact, one possibility for the sequence T in the theorem is a contiguous subsequence of a c^u-ary span v de Bruijn sequence which satisfies the condition (ii) in Theorem 8.

4 Constructions of APMs

In this section, two types of APMs are given by constructions of corresponding sequences T satisfying Theorem 8 for given de Bruijn sequences. First, a family of c-ary $(c^u+u-1, c^u+1; u, 2)$APMs is provided as an example in which c is not a prime power. We remark that these APMs must be referred to as the APMs with parameters c-ary $(c^u+1, c^u+u-1; 2, u)$ because of our supposition in Remark 6 that the low size of our APM is not longer that the column size. Note that these APMs form square arrays if $u = 2$. Second, a family of 2^h-ary $(m, n; u, 2)$APMs are given. Note that the sequence T for the construction is formed by an amalgamation of two periodic sequences.

4.1 A construction of c-ary $(c^u+1, c^u+u-1; 2, u)$APM

Let c be any given positive integer. For any given c-ary span u de Bruijn sequence, a class of c-ary $(c^u+u-1, c^u+1; u, 2)$APMs can be given by the designed sequence T satisfying Theorem 8 as follows.

Construction 9 c-ary $(c^u+u-1, c^2+1; u, 2)$APMs
Let $B = (b_i)$ be a c-ary span u de Bruijn sequence of period c^u. Define a sequence $T = (t_i)$ of length c^u+1 as follows;

$$t_{i+1} \equiv t_i + i \pmod{c^u}, \quad t_0 = 0$$

where $t_i \in \mathbb{N}_{c^u}$ for all $i = 1, ..., c^u$. Define a $(c^u+u-1) \times (c^u+1)$ array A as

$$A = ([b_{t_0}]' [b_{t_1}]' \cdots [b_{t_{c^u}}]') ,$$

which is a $(T, [B_{c^u}]_{c^u+u-1})$-array determined by such T and B.

Theorem 10 Let B be a c-ary span u de Bruijn sequence. Let $T = (t_k)$ be the sequence defined in Construction 9 and let A be the $(T, [B_{c^u}]_{c^u+u-1})$-array of size $(c^u+u-1) \times (c^2+1)$. Then the transpose of A is a c-ary $(c^u+1, c^u+u-1; 2, u)$APM.

Proof. We claim that the sequence T defined in Construction 9 satisfies (i) and (ii) in Theorem 8.

(i) Suppose that $(t_i\ t_{i+1}) = [t_i]_2 = [t_j]_2 = (t_j\ t_{j+1})$ for some $i, j \in \mathbb{N}_{c^u}$. Then

$$t_i + i \equiv t_{i+1} = t_{j+1} \equiv t_j + j \pmod{c^u}$$

Since $t_i = t_j$ and $i, j \in \mathbb{N}_{c^u}$, we have $i \equiv j \pmod{c^u}$ and so $i = j$.

(ii) Suppose that $(t_i\ t_{i+1}) \in [T_{c^u}]_2$ and $(t_i+\alpha\ t_{i+1}+\alpha) \in [T_{c^u}]_2$ for some integer α with $\alpha \le |c^u-1|$. Let $(t_i+\alpha\ t_{i+1}+\alpha) = (t_j\ t_{j+1})$ for some $j \in \mathbb{N}_{c^2}$. Since $t_j \equiv t_i + \alpha$ and $t_{j+1} = t_{i+1} + \alpha$ we have

$$t_i + \alpha + j \equiv t_j + j \equiv t_{j+1} \equiv t_{i+1} + \alpha \equiv t_i + i + \alpha \pmod{c^u}$$

which implies that $i \equiv j \pmod{c^u}$ Since $i, j \in \mathbb{N}_{c^u}$ and $\alpha \le |c^u-1|$, we have $i = j$ and $\alpha = 0$.

Hence, the $(T, [B_{c^u}]_{c^u+u-1})$-array A is a c-ary $(c^u+u-1, c^u+1; u, 2)$APM from Theorem 8. Therefore, the transpose of A is a c-ary $(c^u+1, c^u+u-1; 2, u)$APM from Remark 6. ■

We have the following corollary on the existence of the given type of APM directly from Theorem 10.

Corollary 11 For c and u with $c \ge 2$ and $u \ge 1$, there always exists c-ary $(c^u+1, c^u+u-1; 2, u)$APM.

Example 12 Note that the following sequence $B = (b_i)$ $(i = 0, ..., 35)$ is a 6-ary span 2 de Bruijn sequence of period 6^2:

$$B = (005544332211040302015141312524235345).$$

From Construction 9, a 6-ary $(37, 37; 2, 2)$APM can be obtained as follows.

1. $T = (t_i)$ of length $6^2 + 1$ as $t_{i+1} \equiv t_i + i \pmod{6^2}$, $t_0 = 0$ where $t_i \in \mathbb{N}_{6^2}$, i.e.

$$T = (0\ 0\ 1\ 3\ 6\ 10\ 15\ 21\ 28\ 0\ 9\ 19\ 30\ 6\ 19\ 33\ 12\ 28\ 9\ 27\\ 10\ 30\ 15\ 1\ 24\ 12\ 1\ 27\ 18\ 10\ 3\ 33\ 28\ 24\ 21\ 19\ 18).$$

2. Define a 37×37 array A as $(T, [B_{6^2}]_{6^2+1})$-array, i.e.

$$A = ([b_{t_0}]'\ [b_{t_1}]' \ldots [b_{t_{6^2}}]') = ([b_0]'\ [b_0]'\ [b_1]' \ldots [b_{18}]')$$

which gives a 6-ary $(37, 37; 2, 2)$APM (see Figure 1).

0	0	0	5	3	1	3	1	2	0	2	1	2	3	1	3	0	2	2	5	1	2	3	0	3	0	0	5	0	1	5	3	2	3	4	5	0
0	0	5	4	3	1	0	4	4	0	1	5	3	3	5	4	4	4	1	2	1	3	0	5	1	4	5	2	1	1	4	4	4	1	5	0	1
5	5	5	4	2	0	2	1	2	5	1	1	5	2	1	5	0	2	1	4	0	5	2	5	2	0	5	4	5	0	4	5	2	2	0	0	5
5	5	4	3	2	4	0	3	3	5	0	4	3	2	4	0	3	3	0	2	4	3	0	4	5	3	4	2	1	4	3	0	3	5	0	5	1
4	4	4	3	1	0	1	1	5	4	4	1	4	1	1	0	0	5	4	3	0	4	1	4	2	0	4	3	4	0	3	0	5	2	5	5	4
4	4	3	2	1	3	5	2	3	4	0	3	5	1	3	5	2	3	0	5	3	5	5	3	4	2	3	5	1	3	2	5	3	4	5	4	1
3	3	3	2	0	0	1	5	4	3	3	1	0	0	1	5	0	4	3	3	0	0	1	3	2	0	3	3	3	0	2	5	4	2	4	4	3
3	3	2	1	4	2	4	2	5	3	0	2	0	4	2	4	1	5	0	4	2	0	4	2	3	1	2	4	1	2	1	4	5	3	4	3	1
2	2	2	1	0	0	1	4	0	2	2	5	5	0	5	4	5	0	2	5	0	5	1	2	5	5	2	5	2	0	1	4	0	5	3	3	2
2	2	1	0	3	1	3	2	0	2	0	2	5	3	2	3	1	0	0	0	1	5	3	1	3	1	1	0	5	1	0	3	0	3	3	2	5
1	1	1	4	0	5	1	3	5	1	1	4	4	0	4	3	4	5	1	0	5	4	1	1	4	4	1	0	2	5	4	3	5	4	2	2	2
1	1	0	0	2	1	2	5	5	1	5	2	4	2	2	2	2	1	5	5	5	1	4	2	0	5	1	0	5	4	1	0	2	5	5	2	1	4
0	0	4	3	0	4	5	3	4	0	1	3	3	0	3	2	3	4	1	5	4	3	5	4	0	3	4	5	2	4	3	2	4	0	1	1	2
4	4	0	0	1	1	2	4	4	4	4	5	3	1	5	1	1	4	4	4	1	3	2	0	0	1	0	4	3	1	0	1	4	0	1	0	3
0	0	3	2	5	3	4	5	3	0	1	3	2	5	3	1	2	3	1	4	3	2	4	3	5	2	3	4	5	3	2	1	3	5	0	4	5
3	3	0	0	1	1	2	0	3	3	3	4	2	1	4	0	5	3	3	3	1	2	2	0	5	5	0	3	3	1	0	0	3	5	4	0	3
0	0	2	1	4	2	3	0	2	0	1	5	1	4	5	4	2	2	1	3	2	1	3	2	4	2	2	3	4	2	1	4	2	4	0	3	4
2	2	0	5	1	5	5	5	2	2	2	0	1	1	0	0	4	2	2	2	5	1	5	0	4	4	0	2	5	5	5	0	2	4	3	0	5
0	0	1	1	3	2	3	5	1	0	5	0	0	3	0	3	2	1	5	2	2	0	3	1	3	2	1	2	0	2	1	3	1	3	0	2	0
1	1	5	4	1	4	4	4	1	1	2	5	4	1	5	0	3	1	2	1	4	4	4	5	3	3	5	1	0	4	4	0	1	3	2	0	0
5	5	1	1	2	2	5	4	0	5	4	5	0	2	5	2	5	0	4	1	2	0	5	1	2	5	1	1	5	2	1	2	0	2	0	1	5
1	1	4	3	5	3	0	3	4	1	2	4	3	5	4	0	3	4	2	0	3	3	0	4	2	3	4	0	5	3	3	0	4	2	1	5	5
4	4	1	1	2	5	0	3	0	4	3	4	0	2	4	1	4	0	3	4	5	0	0	1	1	4	1	4	4	5	1	1	0	1	5	1	4
1	1	3	2	4	3	5	2	3	1	5	3	2	4	3	5	5	3	5	0	3	2	5	3	1	5	3	0	4	3	2	5	3	1	1	4	4
3	3	1	5	2	4	5	2	0	3	3	3	0	2	3	1	0	0	3	3	4	0	5	1	0	0	1	3	3	4	5	1	0	0	4	1	3
1	1	2	2	3	5	4	1	2	1	4	2	1	3	2	4	0	2	4	0	5	1	4	2	4	0	2	0	3	5	2	4	2	4	1	3	3
2	2	5	4	5	0	4	1	0	2	5	2	5	5	5	2	1	5	0	5	2	0	5	4	5	0	5	5	2	2	0	4	1	0	0	3	1	2
5	5	2	2	3	0	3	0	1	5	0	1	1	3	1	3	5	1	0	0	0	1	3	2	3	5	2	0	2	0	2	3	1	3	1	2	2
2	2	4	3	4	5	3	4	5	2	0	1	4	4	1	1	4	5	0	1	5	4	3	4	0	4	4	1	1	5	3	1	5	0	2	5	1
4	4	2	5	5	5	2	0	1	4	5	0	1	5	0	2	4	1	5	5	5	1	2	2	2	4	2	5	1	5	5	2	1	2	5	2	1
2	2	3	3	0	4	2	3	4	2	5	4	3	0	4	5	3	4	5	1	4	3	2	3	0	3	3	1	0	4	3	5	4	0	2	4	0
3	3	5	4	0	4	1	0	1	3	4	0	1	0	0	2	3	1	4	4	4	1	1	5	1	3	5	4	4	4	4	2	1	1	4	2	4
5	5	3	5	5	3	1	2	3	5	4	3	2	5	3	4	2	3	4	1	3	2	1	3	5	2	3	1	0	3	5	4	3	5	2	3	0
3	3	4	0	5	3	0	0	1	3	3	0	5	5	0	2	2	1	3	3	3	5	0	4	1	2	4	3	3	3	0	2	1	1	3	5	3
4	4	5	0	4	2	4	1	2	4	3	2	2	4	2	3	1	2	3	1	2	2	4	5	4	1	5	1	0	2	0	3	2	4	5	3	0
5	5	0	5	4	2	0	5	5	5	2	0	4	4	0	5	1	5	2	2	2	4	0	0	1	1	0	2	2	2	5	5	5	1	3	4	2
0	0	0	5	3	1	3	1	2	0	2	1	2	3	1	3	0	2	2	5	1	2	3	0	3	0	0	5	0	1	5	3	2	3	4	5	0

Figure 1: 6-ary $(6^2 + 1, 6^2 + 1; 2, 2)$APM

4.2 A Construction of 2^h-ary $(m, n; u, 2)$APM

The following type of APM is constructed by the devised sequence T satisfying Theorem 8 which consists of two amalgamated periodic sequences with entries in the index set of a given de Bruijn sequence.

Construction 13 A class of 2^h-ary $(m, n; u, 2)$APM.

Let $c = 2^h$ and $v = 2$. Then the parameters of a c-ary $(m, n; u, v)$APM satisfy $(m - u + 1)(n - 1) = 2^{2hu}$ so that $(m - u + 1) \mid 2^{2hu}$. Since $m - u + 1 \leq n - 1$ from Remark 6, we can put $m - u + 1 = 2^t$ where $0 \leq t \leq hu$. Suppose $hu \geq 3$ and $t = hu - 2$. Then for arbitrary u, the parameters m and n are given as

$$m = 2^t + u - 1 = 2^{hu-2} + u - 1,$$
$$n = 2^{2hu-t} + 1 = 2^{hu+2} + 1.$$

1. Let B be a 2^h-ary span u de Bruijn sequence, say

$$B = (c_0, c_1, \ldots\ldots, c_{2^{hu}-1}).$$

2. Consider the following set of m-windows of B,

$$[B_{2^{hu}}]_m = \{[c_i]_m \mid 0 \leq i \leq 2^{hu} - 1\}.$$

3. Now we define two sequences (a_i) and (b_i) with entries in $\mathbb{N}_{2^{hu}}$ by the following recurrence relations.

$a_0 = 0$,

$$a_{i+1} \equiv \begin{cases} -a_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 0 \ (\text{mod } 4) \\ 2^{hu-1} - 1 - a_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 1 \ (\text{mod } 4) \\ 2^{hu-1} - a_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 2 \ (\text{mod } 4) \\ -1 - a_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 3 \ (\text{mod } 4) \end{cases}$$

and

$b_0 = 0$,

$$b_{i+1} \equiv \begin{cases} 2^{hu-1} - b_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 0 \ (\text{mod } 4) \\ -1 - b_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 1 \ (\text{mod } 4) \\ -b_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 2 \ (\text{mod } 4) \\ 2^{hu-1} - 1 - b_i & (\text{mod } 2^{hu}) \quad if \quad i \equiv 3 \ (\text{mod } 4). \end{cases}$$

Note that from the recurrence relations, $a_{4i+4} = -2 + a_{4i}$ and $b_{4i+4} = -2 + b_{4i}$, we have $a_{4k} = -2k$ and $b_{4k} = -2k$ which imply

$$a_i = a_{4k+r} \equiv \begin{cases} -2k & (\text{mod } 2^{hu}) \quad if \quad r = 0 \\ 2k & (\text{mod } 2^{hu}) \quad if \quad r = 1 \\ 2^{hu-1} - 1 - 2k & (\text{mod } 2^{hu}) \quad if \quad r = 2 \\ 1 + 2k & (\text{mod } 2^{hu}) \quad if \quad r = 3 \end{cases} \tag{3}$$

$$b_i = b_{4k+r} \equiv \begin{cases} -2k & (\mathrm{mod}\ 2^{hu}) \quad if \quad r=0 \\ 2^{hu-1}+2k & (\mathrm{mod}\ 2^{hu}) \quad if \quad r=1 \\ -2^{hu-1}-1-2k & (\mathrm{mod}\ 2^{hu}) \quad if \quad r=2 \\ 2^{hu-1}+1+2k & (\mathrm{mod}\ 2^{hu}) \quad if \quad r=3 \end{cases} \tag{4}$$

for $k = 0, 1, 2, \ldots$. Here, (a_i) and (b_i) are 2^{hu+1}-periodic sequences since (a_{4k}) and (b_{4k}) are of period 2^{hu-1}.

4. We define a sequence $T = (t_k)$ with entries in $\mathbb{N}_{2^{hu}}$ of length $2^{hu+2}+1$ such that

$$t_k = \begin{cases} a_k & if \quad 0 \le k \le 2^{hu+1} \\ b_k & if \quad 2^{hu+1} \le k \le 2^{hu+2}. \end{cases}$$

Note that $a_{2^{hu+1}} = b_{2^{hu+1}} = 0$ so that $t_{2^{hu+1}}$ is well defined.

5. Define a $(2^{hu-2}+u-1) \times (2^{hu+2}+1)$ array A as

$$A = \left([c_{t_0}]'\,[c_{t_1}]' \cdots [c_{t_{2^{hu+2}}}]'\right) ,$$

which is a $(T, [B_{2^{hu}}]_m)$-array determined by such T and B.

We observe the properties of the sequences (a_i), (b_i) and (t_i) in Construction 13 before we prove the constructed sequence T satisfies (i) and (ii) in Theorem 8.

Lemma 14 Let (a_i), (b_i) and (t_i) be the sequences defined in Construction 13. Then, we have

(i) (a_{4k}) and (b_{4k}) are of period 2^{hu-1}.

(ii) (a_i) and (b_i) are of period 2^{hu+1}.

(iii) for $r = 0, 1, 2, 3$, whenever $0 \le k,\ k' < 2^{hu-1}$ and $k \ne k'$, then

$$a_{4k+r} \ne a_{4k'+r} and \text{ and } b_{4k+r} \ne b_{4k'+r},$$

i.e. the 2^{hu-1} entries in each cycle of (a_{4k}) and (b_{4k}), respectively, are distinct.

Proof. Note that $2k \equiv 2k' (\mathrm{mod}\, 2^{hu})$ if and only if $k \equiv k' (\mathrm{mod}\, 2^{hu-1})$. So, for $r = 0, 1, 2, 3$, $a_{4k+r} = a_{4k'+r}$ if and only if $k \equiv k' \left(\mathrm{mod}\, 2^{hu-1}\right)$. Thus, (i) and (ii) hold. Now, $a_{4k+r} - a_{4k'+r} = 2(k-k')$ and $2(k'-k) \ne 0 \pmod{2^{hu}}$ since $k \ne k' \pmod{2^{hu-1}}$, which implies (iii). ■

Proposition 15 Let $B = (c_i)$ be a 2^h-ary span u de Bruijn sequence and $T = (t_k)$ be the sequence defined in Construction 13. Then, T satisfies the condition (i) in Theorem 8 for $m = 2^{hu-2}+u-1$, $n = 2^{hu+2}+1$ and $v = 2$.

Proof. We show that if $[t_i]_2 = [t_j]_2$ for $i, j \in \mathbb{N}_{2^{hu+2}}$, then $i = j$. Note that T consists of the concatenation of two finite subsequences of (a_i) and (b_i). Note that $t_{2^{hu+1}} = a_{2^{hu+1}} = a_0 = b_0 = b_{2^{hu+1}}$. Thus, for $0 \le i \le 2^{hu+1} - 1$, $[t_i]_2 = [a_i]_2$ and for $2^{hu+1} \le i \le 2^{hu+2}$, $[t_i]_2 = [b_i]_2$. The following table lists the elements $[a_i]_2$ and $[b_i]_2$ where $i = 4k + r$ for $r = 0, 1, 2, 3$ and the entries represent residues modulo 2^{hu}.

r	$[a_i]_2$	$[b_i]_2$
0	$(-2k,\ 2k)$	$(-2k,\ 2^{hu-1} + 2k)$
1	$(\ 2k,\ -2k + 2^{hu-1} - 1)$	$(2^{hu-1} + 2k,\ -2^{hu-1} - 1 - 2k)$
2	$(-2k + 2^{hu-1} - 1,\ 2k + 1)$	$(-2^{hu-1} - 1 - 2k,\ 2^{hu-1} + 1 + 2k)$
3	$(2k + 1,\ -2k - 2)$	$(2^{hu-1} + 1 + 2k,\ -2k - 2)$

(5)

Suppose that $[t_i]_2 = [t_j]_2$ for some $0 \le i, j \le 2^{hu+2} - 1$. There are three cases to be considered.

1. $0 \le i, j \le 2^{hu+1} - 1$; then $(a_i, a_{i+1}) = [t_i]_2 = [t_j]_2 = (a_j, a_{j+1})$.
   Let $i = 4k + r$ and $j = 4k' + r'$ where $0 \le r, r' \le 3$.

   (a) Suppose $r = r'$. Then $2k \equiv 2k' \pmod{2^{hu}}$ and hence $k \equiv k' \pmod{2^{hu-1}}$ which implies that $k = k'$ by Lemma 14 (iii). Thus $i = j$.

   (b) Suppose $r \neq r'$. Without loss of generality, we may assume that $r < r'$. Then, for possible values of r and r', we have the following six congruences derived from (5) and the hypothesis $(a_i\ a_{i+1}) = (a_j\ a_{j+1})$.

r	r'	Congruence derived from (5)		reason
0	1	$2k \equiv -2k' + 2^{hu-1} - 1$	$(\mathrm{mod}\ 2^{hu})$	$a_{i+1} = a_{j+1}$
0	2	$2k \equiv 2k' + 1$	$(\mathrm{mod}\ 2^{hu})$	$a_{i+1} = a_{j+1}$
0	3	$-2k \equiv 2k' + 1$	$(\mathrm{mod}\ 2^{hu})$	$a_i = a_j$
1	2	$2k \equiv -2k' + 2^{hu-1} - 1$	$(\mathrm{mod}\ 2^{hu})$	$a_i = a_j$
1	3	$2k \equiv 2k' + 1$	$(\mathrm{mod}\ 2^{hu})$	$a_i = a_j$
2	3	$2k + 1 \equiv -2k' - 2$	$(\mathrm{mod}\ 2^{hu})$	$a_{i+1} = a_{j+1}$

   Since $hu > 1$, each of these congruencies leads to the contradiction that $0 \equiv 1 \pmod 2$. Thus the case $r \neq r'$ does not occur.

   Hence, in this case, we have $i = j$.

2. $2^{hu+1} \le i, j \le 2^{hu+2} - 1$; then $(b_i, b_{i+1}) = [t_i]_2 = [t_j]_2 = (b_j, b_{j+1})$.
   Let $i = 4k + r$ and $j = 4k' + r'$ where $0 \le r, r' \le 3$. The same argument as stated in case 1 can be applied to this case. Referring (5), for each r and r' with $0 \le r, r' \le 3$, we have a similar congruence to the one in case 1 which implies a contradiction that $0 \equiv 1 \pmod 2$. Hence we have $i = j$.

3. $0 \le i \le 2^{hu+1} - 1$ and $2^{hu+1} \le j \le 2^{hu+2} - 1$; then $(a_i, a_{i+1}) = [t_i]_2 = [t_j]_2 = (b_j, b_{j+1})$.
   Let $i = 4k + r$ and $j = 4k' + r'$ where $0 \le r, r' \le 3$.

(a) Suppose $r = r'$. Then, we have four cases as follows.

(i) $r = 0 = r'$; then, we have $-2k \equiv -2k' (\mathrm{mod}\, 2^{hu})$ and $2k \equiv 2^{hu-1} + 2k' (\mathrm{mod}\, 2^{hu})$.

(ii) $r = 1 = r'$; then, we have $2k \equiv 2^{hu-1} + 2k' (\mathrm{mod}\, 2^{hu})$ and $-2k + 2^{hu-1} - 1 \equiv -2^{hu-1} - 1 - 2k' (\mathrm{mod}\, 2^{hu})$.

(iii) $r = 2 = r'$; then, we have $-2k + 2^{hu-1} - 1 \equiv -2^{hu-1} - 1 - 2k' (\mathrm{mod}\, 2^{hu})$ and $2k + 1 \equiv 2^{hu-1} + 1 + 2k' (\mathrm{mod}\, 2^{hu})$.

(iv) $r = 3 = r'$; then, we have $2k + 1 \equiv 2^{hu-1} + 1 + 2k' (\mathrm{mod}\, 2^{hu})$ and $-2k - 2 \equiv -2k' - 2 (\mathrm{mod}\, 2^{hu})$.

In each case we have $k \equiv k' (\mathrm{mod}\, 2^{hu-1})$ and $k \equiv k' + 2^{hu-2} (\mathrm{mod}\, 2^{hu-1})$. i.e. $2^{hu-2} \equiv 0 (\mathrm{mod}\ 2^{hu-1})$. This contradiction implies that this case does not occur.

(b) Suppose $r \neq r'$. From $(a_i\ a_{i+1}) = (b_j\ b_{j+1})$, we have 12 cases as follows.

r	r'	congruences derived from (5)	reason
0	1	$2k \equiv -2^{hu-1} - 1 - 2k' (\mathrm{mod}\ 2^{hu})$	$a_{i+1} = b_{j+1}$
0	2	$-2k \equiv -2^{hu-1} - 1 - 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
0	3	$-2k \equiv 2^{hu-1} + 1 + 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
1	0	$-2k + 2^{hu-1} - 1 \equiv 2^{hu-1} + 2k' (\mathrm{mod}\ 2^{hu})$	$a_{i+1} = b_{j+1}$
1	2	$2k \equiv -2^{hu-1} - 1 - 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
1	3	$2k \equiv 2^{hu-1} + 1 + 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
2	0	$-2k + 2^{hu-1} - 1 \equiv -2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
2	1	$-2k + 2^{hu-1} - 1 \equiv 2^{hu-1} + 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
2	2	$2k + 1 \equiv -2k' - 2 (\mathrm{mod}\ 2^{hu})$	$a_{i+1} = b_{j+1}$
3	0	$2k + 1 \equiv -2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
3	1	$2k + 1 = 2^{hu-1} + 2k' (\mathrm{mod}\ 2^{hu})$	$a_i = b_j$
3	2	$-2k - 2 \equiv 2^{hu-1} + 1 + 2k' (\mathrm{mod}\ 2^{hu})$	$a_{i+1} = b_{j+1}$

Since $hu > 1$, each of these congruences leads to the contradiction that $0 \equiv 1 \pmod 2$. Thus the case $r \neq r'$ does not occur.

Hence, in this case, we have $i = j$.

In all cases, we have $i = j$. Hence we conclude that $[t_i]_2 \neq [t_j]_2$ if $i \neq j$ and T satisfies condition (i) in Theorem 8. ■

Proposition 16 Let $B = (c_i)$ be a 2^h-ary span u de Bruijn sequence with $hu \geq 3$ and let $T = (t_k)$ be the sequence defined in Construction 13 by B. Then, T satisfies the condition (ii) in Theorem 8 for $m = 2^{hu-2} + u - 1$, $n = 2^{hu+2} + 1$ and $v = 2$.

Proof. Suppose that $[t_i]_2 = [t_j + \alpha]_2$ for some i, j with $0 \leq i, j \leq 2^{hu+2}$ and non-zero integer α with $u - m \leq \alpha \leq m - u$. Then, $t_i \equiv t_j + \alpha \pmod{2^{hu}}$ and $t_{i+1} = t_{j+1} + \alpha \pmod{2^{hu}}$ so that

$$t_{i+1} - t_i \equiv t_{j+1} - t_j (\mathrm{mod}\, 2^{hu}). \tag{6}$$

The following table lists the values $a_{4k+r+1} - a_{4k+r}$ and $b_{4k+r+1} - b_{4k+r}$ for $r = 0, 1, 2, 3$ and the entries represent residues modulo 2^{hu}.

r	$a_{4k+r+1} - a_{4k+r}$	$b_{4k+r+1} - b_{4k+r}$
0	$4k$	$4k + 2^{hu-1}$
1	$-4k - 1 + 2^{hu-1}$	$-4k - 1$
2	$4k - 2^{hu-1} + 2$	$4k + 2$
3	$-4k - 3$	$-4k - 3 - 2^{hu-1}$

(7)

Now let $i = 4k + r$ and $j = 4k' + r'$ where $0 \le r,\ r' \le 3$. In the same manner as the previous lemma, we divide the problem into three cases.

1. $0 \le i,\ j \le 2^{hu+1} - 1$, i.e. $0 \le k, k' \le 2^{hu-1} - 1$; then,

$$a_{4k+r+1} - a_{4k+r} = t_{i+1} - t_i = t_{j+1} - t_j = a_{4k'+r'+1} - a_{4k'+r'}.$$

(a) Suppose $r = r'$. From (7), we have $4k \equiv 4k' \pmod{2^{hu}}$ so that

$$k \equiv k' \pmod{2^{hu-2}}.$$

From the condition that $0 \le k,\ k' \le 2^{hu-1} - 1$, we have $k = k'$ or $k' = k + 2^{hu-2}$. If $k = k'$, then $i = j$ so that $\alpha = t_i - t_j \equiv 0 (\mathrm{mod}\, 2^{hu})$. But $-2^{hu-2}+1 = u-m \le \alpha \le m-u = 2^{hu-2}-1$. Hence $\alpha = 0$. If $k' = k+2^{hu-2}$, then $\alpha = t_i - t_j = a_{4k+r} - a_{4(k+2^{hu-2})+r} \equiv 2^{hu-1} (\mathrm{mod}\, 2^{hu})$ by (3). But $-2^{hu-2} + 1 = u - m \le \alpha \le m - u = 2^{hu-2} - 1$. So this case does not occur.

Thus $\alpha = 0$ and condition (ii) of Theorem 8 holds.

(b) Suppose $r \ne r'$ and, without loss of generality, $r < r'$. Then we have six cases as follows.

	r	r'	Congruences derived from (7)	
(i)	0	1	$4k \equiv -4k' - 1 + 2^{hu-1}$	$(\mathrm{mod}\, 2^{hu})$
(ii)	0	2	$4k \equiv 4k' - 2^{hu-1} + 2$	$(\mathrm{mod}\, 2^{hu})$
(iii)	0	3	$4k \equiv -4k' - 3$	$(\mathrm{mod}\, 2^{hu})$
(iv)	1	2	$-4k - 1 + 2^{hu-1} \equiv 4k' - 2^{hu-1} + 2$	$(\mathrm{mod}\, 2^{hu})$
(v)	1	3	$-4k - 1 + 2^{hu-1} \equiv -4k' - 3$	$(\mathrm{mod}\, 2^{hu})$
(vi)	2	3	$4k - 2^{hu-1} + 2 \equiv -4k' - 3$	$(\mathrm{mod}\, 2^{hu})$

Since $hu > 1$, each of congruences from (i), (iii), (iv) and (vi) leads to the contradiction that $0 \equiv 1 \pmod 2$. From (ii) and (v), we have $2k \equiv 2k' - 2^{hu-2} + 1 (\mathrm{mod}\, 2^{hu-1})$ and $-2k + 2^{hu-2} \equiv -2k' - 1 (\mathrm{mod}\, 2^{hu-1})$, respectively. Since $hu \ge 3$, these congruences lead to the contradictions that $0 \equiv 1 \pmod 2$.

2. $2^{hu+1} \le i,\ j \le 2^{hu+2} - 1$ i.e. $2^{hu-1} \le k \le 2^{hu} - 1$; then, $b_{4k+r+1} - b_{4k+r} = t_{i+1} - t_i = t_{j+1} - t_j = b_{4k'+r'+1} - b_{4k'+r'}$.

Almost same argument stated in case 1 can be applied to the subcase that $r = r'$ and $r \ne r'$, respectively. Thus, if $r = r'$ then $\alpha = 0$ so that condition (ii) of Theorem 8 holds, and if $r \ne r'$, then six congruences occur from (7) all of which imply that $0 \equiv 1 \pmod 2$.

3. $0 \le i < 2^{hu+1}$ and $2^{hu+1} \le j < 2^{hu+2}$ i.e. $0 \le k \le 2^{hu-1}-1$ and $2^{hu-1} \le k' \le 2^{hu}$; then $a_{4k+r+1} - a_{4k+r} = t_{i+1} - t_i = t_{j+1} - t_j = b_{4k'+r'+1} - b_{4k'+r'}$.

   (a) Suppose $r = r'$. Then, from (7), we have $4k - 4k' \equiv 2^{hu-1} \pmod{2^{hu}}$ so that

$$k - k' \equiv 2^{hu-3} \pmod{2^{hu-2}}. \tag{8}$$

   Then the integers k' satisfying (8) may be expressed in terms of k as follows.

k	k'
$0 \le k < 2^{hu-3}$	$k' = 2^{hu-1} + 2^{hu-3} + k$ or $k' = 2^{hu-1} + 2^{hu-2} + 2^{hu-3} + k$
$2^{hu-3} \le k < 2^{hu-2} + 2^{hu-3}$	$k' = 2^{hu-1} + 2^{hu-3} + k$ or $k' = 2^{hu-1} - 2^{hu-3} + k$
$2^{hu-2} + 2^{hu-3} \le k < 2^{hu-1}$	$k' = 2^{hu-1} - 2^{hu-2} - 2^{hu-3} + k$ or $k' = 2^{hu-1} - 2^{hu-3} + k$

(9)

   For each case $r = r' = 0, 1, 2, 3$ and for each range of k in (9), it follows from (3), (4) and (9) that

$$\alpha = t_i - t_j = a_{4k+r} - b_{4k'+r'} \equiv \begin{cases} 2^{hu-2} & \pmod{2^{hu}} \text{ or} \\ 2^{hu-1} + 2^{hu-2} & \pmod{2^{hu}}. \end{cases}$$

   But $-2^{hu-2} + 1 \le u - m \le \alpha \le m - u \le 2^{hu-2} - 1$; so, this case does not occur.

   (b) Suppose $r \ne r'$. From (7), We have 12 cases as follows.

r	r'	congruences derived from (7)	
0	1	$4k \equiv -4k' - 1$	$\pmod{2^{hu}}$
0	2	$4k \equiv -4k' - 3 - 2^{hu-1}$	$\pmod{2^{hu}}$
0	3	$4k \equiv -4k' - 3 - 2^{hu-1}$	$\pmod{2^{hu}}$
1	0	$-4k - 1 + 2^{hu-1} \equiv 4k' + 2^{hu-1}$	$\pmod{2^{hu}}$
1	2	$-4k - 1 + 2^{hu-1} \equiv 4k' + 2$	$\pmod{2^{hu}}$
1	3	$-2k + 2^{hu-2} \equiv -2k' - 1 - 2^{hu-2}$	$\pmod{2^{hu-1}}$
2	0	$2k - 2^{hu-2} + 1 \equiv 2k' + 2^{hu-2}$	$\pmod{2^{hu-1}}$
2	1	$4k - 2^{hu-1} + 2 \equiv -4k' - 1$	$\pmod{2^{hu}}$
2	2	$4k - 2^{hu-1} + 2 \equiv -4k' - 3 - 2^{hu-1}$	$\pmod{2^{hu}}$
3	0	$-4k - 3 \equiv 4k' + 2^{hu-1}$	$\pmod{2^{hu}}$
3	1	$-2k - 1 \equiv -2k'$	$\pmod{2^{hu-1}}$
3	2	$-4k - 3 \equiv 4k' + 2$	$\pmod{2^{hu}}$

   Each of congruences leads to the contradiction that $1 \equiv 0 (\text{mod } 2)$ since $hu > 2$. So this case does not occur.

Therefore, for all integers i and α with $0 \le i \le 2^{hu+2}-1$ and $0 < |\alpha| \le 2^{hu-1}-1$, we conclude that $[t_i + \alpha]_v \notin [T_{n-v+1}]_v$ and so T satisfies (ii) in Theorem 8 for $n = 2^{hu+2} + 1$, $m = 2^{hu-2} + u - 1$ and $v = 2$. ■

From Proposition 15 and Proposition 16, the following result is immediate.

Theorem 17 Let B be a 2^h-ary span u de Bruijn sequence. Put $m = 2^{hu-2} + u - 1$ and $n = 2^{hu+2} + 1$. Let $T = (t_k)$ be the sequence defined in Construction 13. Then, A, the $(T, [B_{2^{hu}}]_m)$-array of size $m \times n$ is a 2^h-ary $(2^{hu-2} + u - 1, 2^{hu+2} + 1; u, 2)$APM.

Proof. Note that the parameters satisfy the necessary condition for existence of APMs stated in Lemma 5. Proposition 15 and Proposition 16 imply that the array A satisfies condition (i) and (ii), respectively, in Theorem 8. Therefore, A is a 2^h-ary $(2^{hu-2} + u - 1, 2^{hu+2} + 1; u, 2)$APM. ■

The following example is the simplest case of Construction 13.

Example 18 A construction of a 2-ary $(4, 33; 3, 2)$APM.

1. Take a 2-ary span 3 de Bruijn Sequence $B = (c_i)$ as

$$B = (00111010)$$

and consider $[B_{2^3}]_4$.

2. Now we define two cyclic sequences (a_i) and (b_i) with entries in $\mathbb{N}_8$ of period 2^4. Let i be a non-negative integer and suppose $i = 4k + r$ for non-negative integers k, r with $0 \le r \le 3$.

$$a_i = a_{4k+r} \equiv \begin{cases} -2k & (\text{mod } 8) \quad if \quad r = 0 \\ 2k & (\text{mod } 8) \quad if \quad r = 1 \\ 3 - 2k & (\text{mod } 8) \quad if \quad r = 2 \\ 1 + 2k & (\text{mod } 8) \quad if \quad r = 3 \end{cases}$$

and

$$b_i = b_{4k+r} \equiv \begin{cases} -2k & (\text{mod } 8) \quad if \quad r = 0 \\ 4 + 2k & (\text{mod } 8) \quad if \quad r = 1 \\ 3 - 2k & (\text{mod } 8) \quad if \quad r = 2 \\ -3 + 2k & (\text{mod } 8) \quad if \quad r = 3. \end{cases}$$

3. Define a finite sequence $T = (t_k)$ in $\mathbb{N}_8$ of length $2^5 + 1$ as

$$t_k = \begin{cases} a_k & if \quad 0 \le k \le 2^4 \\ b_k & if \quad 2^4 \le k \le 2^5. \end{cases}$$

4. Then we have

$$(t_k) = (0\,0\,3\,1\,6\,2\,1\,3\,4\,4\,7\,5\,2\,6\,5\,7\,0\,4\,3\,5\,6\,6\,1\,7\,4\,0\,7\,1\,2\,2\,5\,3\,0).$$

Now we can obtain the $2^2 \times (2^5 + 1)$ $(T, [B_8]_4)$-array A by Construction 13 as follows.

$$\begin{aligned} A &= ([c_{t_0}]'\,[c_{t_1}]'\,[c_{t_2}]'\,[c_{t_3}]'\,\ldots\,[c_{t_{32}}]'\,[c_{t_{33}}]') \\ &= ([c_0]'\,[c_0]'\,[c_3]'\,[c_1]'\,\ldots\,[c_3]'\,[c_0]') \\ &\begin{pmatrix} 0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0 \\ 1\,1\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,1 \\ 1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1 \end{pmatrix} \end{aligned}$$

where $[c_{t_k}]_4 \in [B_8]_4$ for $t_k \in T$. Then, the array is a 2-ary $(4, 33; 3, 2)$APM by Theorem 17.

Acknowledgement

A part of the work is from my Ph.D thesis in Royal Holloway, University of London. I would like to thank both my supervisors Professor Fred Piper and Professor Peter Wild. I also thank anonymous referees for meticulous and valuable comments.

References

[1] N. de Bruijn, A combinatorial problem, Proc. Nederlandse Akademie van Wetenschappen, vol. 49, pp.758-764, 1946.

[2] J. Burns, C. Mitchell, Coding Schemes for two-dimensional position sending, Cryptography and Coding III, M.Ganley Ed. London, UK: Oxford Univ. Press, pp.31-61, 1993.

[3] I.J. Good, Normally recurring decimals, J. London Math. Soc., vol. 21, pp.167-169, 1946.

[4] H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, SIAM J. Algebraic and Discrete Methods, vol. 1, pp.107-113, 1980.

[5] G. Hurlbert, C.J. Mitchell, and K.G. Paterson, On the existence of de Bruijn tori with two by two windows, Journal of Combinatorial Theory (Series A) 76, pp.213-230, 1996.

[6] S. Kanetkar and M. Wage, On Construction of Matrices with distict submatrices, SIAM J. Algebraic and Discrete Method, vol. 1, pp.107-113, 1980.

[7] S.-M. Kim, On the existence of aperiodic perfect maps for 2×2 windows, Ars Combinatoria vol. 65, pp.111-120, 2002.

[8] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[8] C.J. Mitchell, Aperiodic and semi-periodic perfect maps, IEEE transactions on Information Theory 41, pp.88-95, 1995.

[9] K.G. Paterson, New Classes of Perfect Maps I, Journal of Combinatorial Theory (Series A) 73, pp.302-334, 1996.

[10] K.G. Paterson, New Classes of Perfect Maps II, Journal of Combinatorial Theory (Series A) 73, pp.335-345, 1996.

[11] D. Rees, Note on a paper by I. J. Good, J. London Math. Soc., vol. 21, pp.169-172, 1946.