On the existence of Aperiodic Perfect Maps for 2×2 Windows

SANG-MOK KIM

DEPARTMENT OF MATHEMATICS SOGANG UNIVERSITY SEOUL 121-742, KOREA

e-mail: smkim@math.sogang.ac.kr

June 11, 2002

Abstract. An aperiodic perfect map(APM) is an array with the property that each possible array of certain size, called a window, arises exactly once as a subarray in the array. In this article, we give some constructions which imply a complete answer for the existence of APMs with 2×2 windows for any alphabet size.

Footnotes:

2000 Mathematics Subject Classification: 94A55, 05B30.

Key words and phrases: de Bruijn Sequence, Aperiodic Perfect Map, Window property

This work was supported by the Brain Korea 21 Project.

ARS COMBINATORIA 65(2002), pp. 111-120

1 Introduction

An Aperiodic Perfect Map(APM) is a c-ary $m \times n$ array such that for some $u \leq m$ and $v \leq n$ every c-ary $u \times v$ array occurs exactly once as a contiguous subarray or a window. This is called the perfect window property. An analogous perfect window property is also applicable to a periodic array: in a Periodic Perfect Map(PM), each window of a certain size occurs exactly once in a single period of the array.

The perfect window property was first studied mainly in the periodic case. De Bruijn considered periodic sequences [1] - a sequence of period n is called a de Bruijn sequence if for some $v \leq n$ every possible v-tuple array occurs exactly once in a period. Many construction methods for de Bruijn sequences have been devised [4], and whenever the parameters satisfy certain necessary conditions, the existence of de Bruijn sequences has been established ([1], [3], [10]). It is also shown by K.Paterson ([8], [9]) that a PM exists for every possible parameter set when the alphabet size c is a prime power.

According to S.Kanetkar and M.Wagh [6], a PM can be transformed into an APM of a slightly larger size by simple extension (this APM is called the *closure* of the PM). However, if the window size of APM is small enough or the alphabet size is not a prime power, there are still sets of parameters satisfying necessary conditions for existence of APM for which there does not exist a closure of any PM. This means that the general existence question for APM is still unsolved.

In this article, we give a complete answer for the question of the existence of APM with 2×2 windows for any alphabet size. We begin with some formal definitions and go on to give a brief introduction to the subject of aperiodic perfect maps and periodic perfect maps. Most of terminologies follow C. Mitchell [7].

Let C be a finite set with |C|=c. Conventionally, we represent a c-ary $m\times n$ array as

$$A = (a_{ij}) \qquad (0 \le i \le m-1, \ 0 \le j \le n-1),$$

where each entry a_{ij} satisfies $0 \le a_{ij} \le c - 1$. For given integers s and t with $0 \le s \le m - 1$, $0 \le t \le n - 1$, we define the (s, t)-th $u \times v$ window of A to be the $u \times v$ subarray

$$A_{s,t} = (\alpha_{i,j})$$
 $(0 \le i \le u - 1, 0 \le j \le v - 1)$

defined by

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

where i+s is computed modulo m and j+t is computed modulo n. For integers m_0 and n_0 with $1 \le m_0 \le m$, $1 \le n_0 \le n$, we denote by $[A_{m_0 \times n_0}]_{u \times v}$

the set of $u \times v$ windows $A_{s,t}$ for $0 \le s \le m_0 - 1$, $0 \le t \le n_0 - 1$, i.e.

$$[A_{m_0 \times n_0}]_{u \times v} = \{A_{s \ t} \mid 0 \le s \le m_0 - 1, \ 0 \le t \le n_0 - 1\}.$$

Note that following bounds

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

are immediate since the lower bound holds only if all windows $A_{s\,t}$, $0 \le s \le m_0 - 1$, $0 \le t \le n_0 - 1$, are identical and the upper bound holds if they are all distinct.

In the case of a finite sequence A of length n, A may be denoted by

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

where $0 \le i \le n-1$. For integers n_0 and t with $1 \le n_0 \le n$, $0 \le t \le n_0-1$, we also simplify $A_{1\,t}$ as A_t and $[A_{m_0 \times n_0}]_{1 \times v}$ as $[A_{n_0}]_v$.

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 $\{0, 1, ..., c-1\}$ in which every distinct c-ary v-tuple occurs exactly once as a window B_t for some integer t with $0 \le t \le c^v - 1$. The well-known result on the existence of de Bruijn sequence is as follows.

Result 1 ([1], [3] and [10]) For any given $c \ge 2$ and $v \ge 1$, there exists a c-ary span v de Bruijn sequence.

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 $A = (a_{ij})$ 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_{st} of A with $0 \leq s \leq m-1$ and $0 \leq t \leq n-1$. As has been observed, a c-ary span v de Bruijn sequence is a c-ary $(1, c^v; 1, v)$ PM.

Now we immediately have the following necessary conditions for the existence of PM.

Result 2 ([7]) 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 2, the set of ordered integers (c; m, n; u, v) is called an *admissible parameter set* for PM.

When the window of size is 2×2 , the complete answer for the existence of PM is given by G.Hurlbert, C.J.Mitchell, and K.G.Paterson [5], as follows.

Result 3 The necessary conditions of Result 2 are sufficient for the existence of a c - ary(m, n; 2, 2) PM, i.e. for all m > 2, n > 2 and c with $mn = c^4$, there exists a c - ary(m, n; 2, 2) PM.

We define an APM as follows. 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 $c-ary \ m \times n \ array \ A = (a_{ij})$ 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_{st} of A with $0 \leq s \leq m-u$ and $0 \leq t \leq n-v$. We also define (c;m,n;u,v) as an admissible parameter set for APM if it satisfies the conditions given in the following lemma.

Result 4 ([7]) 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) $(m-u+1)(n-v+1)=c^{uv}$.

In 1995, C.Mitchell [7] proved the existence theorem of 2-ary(binary) APMs as follows.

Result 5 A 2-ary (m,n;u,v)APM exists for every admissible parameter set (c;m,n;u,v) for APM, i.e. the necessary condition for PM in Result 4 is sufficient when the alphabet size c is 2.

Now we describe a construction of an APM from the simple extension of a PM. Note that the construction was suggested by S.Kanetkar and M.Wagh [6], and the notation follows C.Mitchell [7].

Definition 6 Suppose m, n, u, v are positive integers satisfying $1 \le u \le m$ and $1 \le v \le n$. Suppose that $A = (a_{i \ j})$ $(0 \le i \le m-1, 0 \le j \le n-1)$ is an $m \times n$ array. Let $E_{u \ v}(A) = (b_{i \ j})$ $(0 \le i \le m+u-2, 0 \le j \le n+v-2)$ be the $(m+u-1) \times (n+v-1)$ array defined by

$$b_{ij} = a_{st}$$

where $s \equiv i \pmod{m}$ and $t \equiv j \pmod{n}$.

Then we can state the following lemma which follows immediately from the definitions.

Lemma 7 If A is a c-ary (m,n;u,v)PM then $E_{uv}(A)$ is a c-ary (m+u-1,n+v-1;u,v)APM.

Let $A=(a_{i\,j})$ be a given c-ary (m,n;u,v)PM. Then we denote $E_{u\,v}(A)=(b_{i\,j})$ by $\bar{A}=(\bar{a}_{i\,j})$ where $b_{i\,j}=\bar{a}_{i\,j}$, and \bar{A} is called the *closure* of a periodic perfect map A.

Remark 8 Let $A=(a_{i\,j})$ be a c-ary $m\times n$ array. The transpose A^T of A is the c-ary $n\times m$ array $A^T=(a_{i\,j}^T)$ where $a^T=a_{j\,i}$. If A is a PM (or an APM) then A^T 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 we restrict our definition of admissible parameter set for PM (or APM) to those with $n\geq m$.

Remark 9 Note that a c-ary (m,n,u,v)APM arises, by Result 7, from a c-ary (m-u+1,n-v+1,u,v)PM. The latter 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 $n\geq 2v$.

2 Existence of APMs for 2×2 Windows

We give two constructions of APMs to show that they exist for all admissible parameter sets when the window size is 2×2 , which means the necessary conditions in Result 4 are sufficient for the existence of an APM for those parameters. Note that the first construction is also given in [7] for the binary case.

Suppose that u = v = 2 for the admissible parameter set (c; m, n; u, v) for APM. By the necessary condition for an APM in Result 4 (iii), we have

$$(m-1)(n-1) = c^4. (1)$$

We break the problem into three cases for possible values of m when m = 2, m = 3 and $m \ge 4$. Recall that by Remark 8 we need only consider n > m.

Consider the case $m \ge 4$. Since $n-1 \ge m-1 > 2 = u$, Result $\overline{3}$, [7] implies that c-ary (m-1, n-1; 2, 2)PM always exists if (c; m-1, n-1; 2, 2) is an admissible set for PM. Hence, whenever m > 3 and n > 3, this PM gives rise to its closure which is a c-ary (m, n; 2, 2)APM as described in Definition 6 (see Remark 9). In order to complete our analysis of the existence of APM, therefore, it is sufficient to consider the other two cases, m=2 and m=3.

In the following two subsections, we deal with two general constructions which cover the cases m=2 and m=3, respectively. From these results, we conclude that there exists an APM for 2×2 windows if and only if the parameters form an admissible parameter set for APM. (i.e. the necessary conditions for APM (Result 4) are sufficient for the existence of c-ary (m,n;2,2)APM.

2.1 The existence of c-ary (m, n; 2, 2)APM when m = 2

Before we deal with the case m=2, we consider a more general construction that implies the existence of c-ary (2,n;2,2)APM. The following construction is obtained directly from the existence of a c^u -ary span v de Bruijn sequence. Notice that for the binary case it was suggested by J.Burns and C.J.Mitchell [7]. From now on, we use the notation that $\mathbb{N}_l = \{0,1,\ldots,l-1\}$ and $\mathbb{N}_l^n = \mathbb{N}_l \times \mathbb{N}_l^{n-1}$ for given positive integers l and n.

Construction 10 (c-ary(u, n; u, v)APM)

Suppose that (c; m = u, n; u, v) is an admissible parameter set for APM (i.e. $n - v + 1 = c^{uv}$ from Result 4). We construct a c-ary (u, n; u, v) APM. Let $B = (b_k)$ be a c^u -ary span v de Bruijn sequence. Then, by Lemma 7, $\bar{B} = (\bar{b}_j)$ (the closure of B) is a c^u -ary $(1, c^{uv} + v - 1; 1, v)$ APM where $\bar{b}_j = b_k$ if $k \equiv j \pmod{c^{uv}}$. Since $\bar{b}_j \in \mathbb{N}_{c^u}$, each \bar{b}_j can be written as an integer representation in base c, i.e. let $\bar{b}_j = \sum_{i=0}^{u-1} b_{ij} c^i$ $(0 \le b_{ij} \le c - 1)$. Using the one-to-one correspondence ϕ between \mathbb{N}_{c^u} and \mathbb{N}_c^u , we can write \bar{b}_j as a u-bit c-ary tuple $(b_{0j}, \dots b_{u-1j})$, i.e.

$$\phi(\bar{b_j}) = \phi\left(\sum_{i=0}^{u-1} b_{i\,j}c^i\right) = (b_{0\,j}\ b_{1\,j}\ \dots\ b_{u-1\,j}) \in \mathbb{N}_c^u.$$

We define $a \ u \times (c^{uv} + v - 1)$ array $A = (a_{ij})$ by $a_{ij} = b_{ij}$ where $0 \le i \le u - 1$, $0 \le j \le c^{uv} + v - 2$, and $\bar{b}_j = b_k$ with $j = k \pmod{c^{uv}}$, i.e.

$$A = \left(\phi\left(\bar{b}_{0}\right)^{T} \mid \phi\left(\bar{b}_{1}\right)^{T} \mid \cdot \cdot \cdot \cdot \mid \phi\left(\bar{b}_{c^{uv}+v-3}\right)^{T} \mid \phi\left(\bar{b}_{c^{uv}+v-2}\right)^{T}\right)$$

where $(\cdot \mid \cdot)$ denotes the concatenation of column vectors.

Theorem 11 Let (c; m = u, n; u, v) be an admissible parameter for APM. Let B be a c^u -ary span v de Bruijn sequence. Then the $u \times (c^{uv} + v - 1)$ array constructed from B by Construction 10 is a c-ary (u, n; u, v)APM.

Proof. Note that by Result 1 there always exists a c^u -ary span v de Bruijn sequence $B=(b_k)$. We prove that $A=(a_{i\,j})$ in Construction 10 is a c-ary (u,n;u,v)APM. Note that since we suppose m=u and $n-v+1=c^{uv}$, any $u\times v$ window $A_{s\,t}$ in $[A_{1\times(n-v+1)}]_{u\times v}$ has s=0 and $0\le t\le c^{uv}-1$. Let $A_{0\,t}=(\alpha_{i\,j})$ and $A_{0\,t'}=(\beta_{i\,j})$ be any two $u\times v$ windows in $[A_{1\times c^{uv}}]_{u\times v}$ where $0\le t,t'\le c^{uv}-1$. Suppose that $A_{0\,t}=A_{0\,t'}$. Then, for $i=0,1,...,u-1,\ j=0,1,...,v-1$, we have $\alpha_{i\,j}=a_{i\,j+t}=a_{i\,j+t'}=\beta_{i\,j}$ so that $b_{i\,j+t}=b_{i\,j+t'}$.

The one-to-one correspondence ϕ implies that $\bar{b}_{j+t} = \bar{b}_{j+t'}$ for $0 \le j \le v-1$. Hence, $B_t = B_{t'}$ in $[B_{c^{uv}}]_v$. From the definition of a de

Bruijn sequence, it follows that t=t'. Therefore, all windows $A_{0\,t}$ in $[A_{1\times(n-v+1)}]_{u\times v}$ are distinct so that $|[A_{1\times(n-v+1)}]_{u\times v}|=n-v+1$. Since $n-v+1=c^{uv}$, it follows that each c-ary $u\times v$ array occurs exactly once in $[A_{1\times(n-v+1)}]_{u\times v}$ and so A is a c-ary (u,n;u,v)APM.

We have a simple example as follows.

Example 12 For a given 2^2 – ary span 2 de Bruijn sequence

$$B = (0\ 0\ 1\ 1\ 2\ 2\ 3\ 3\ 2\ 1\ 0\ 3\ 1\ 3\ 0\ 2)$$

Construction 10 gives rise to a 2-ary (2, 17, 2, 2) APM which is

$$A = \begin{pmatrix} 00001111100101010 \\ 00110011010111000 \end{pmatrix}$$

where the j-th column is $\phi(\bar{b}_j) = \begin{pmatrix} a_{0\ j} \\ a_{1\ j} \end{pmatrix}$ where $\bar{b}_j = a_{0\ j} + 2a_{1\ j}$ with $a_{0\ j},\ a_{1\ j} \in \mathbb{N}_2$ is the j-th entry of \bar{B} .

Now we return to the main interest on the existence of APM for all 2×2 window size when m=2. From Construction 10 and Theorem 11, we obtain the following corollary which shows the existence of a c-ary (2, n; 2, 2)APM for arbitrary c.

Corollary 13 For any given admissible parameter set (c; m = 2, n; u = 2, v = 2) for APM, there exists a c-ary (2, n; 2, 2)APM.

This establishes the case m = 2 of APM for 2×2 windows.

2.2 The existence of c-ary (m, n; 2, 2)APM when m = 3

Let (c; m = 2u - 1, n; u, v) be an admissible parameter set. We first deal with a new construction of c-ary (2u - 1, n; u, v)APM which covers the case m = 3.

Construction 14 (c-ary (2u-1, n; u, v)APM)

We construct an array with entries from N_c where $c \geq 2$. Let (c; 2u-1, n; u, v) be an admissible set of parameters for APM, i.e. $n = c^{uv}/u + v - 1$. Let $B = (b_l)$ be a c-ary span uv de Bruijn sequence and let $\bar{B} = (\bar{b}_k)$ be the closure of B which is a $1 \times (c^{uv} + uv - 1)$ array. Define a $(2u-1) \times (\frac{c^{uv}}{u} + v - 1)$ array $A = (a_{ij})$ by

$$a_{i\,j} = \bar{b}_{i+uj}$$

for $0 \le i \le 2u - 2$ and $0 \le j \le \frac{c^{uv}}{u} + v - 2$. Thus,

$$A = (a_{ij}) = \begin{pmatrix} \bar{b}_0 & \bar{b}_u & \dots & \bar{b}_{c^{uv}+uv-2u} \\ \bar{b}_1 & \bar{b}_{u+1} & \dots & \dots & \dots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{b}_{2u-2} & \bar{b}_{3u-2} & \dots & \bar{b}_{c^{uv}+uv-2} \end{pmatrix}$$

Note that $\bar{b}_k = b_l$ for $l \equiv k \pmod{c^{uv}}$.

Theorem 15 Let (c; m = 2u - 1, n; u, v) be an admissible parameter for APM. Let B be a c-ary span uv de Bruijn sequence. Then the $u \times (c^{uv} + v - 1)$ array constructed from B by Construction 14 is a c-ary $(2u - 1, \frac{c^{uv}}{u} + v - 1; u, v)$ APM.

Proof. Note that there always exists a c-ary span uv de Bruijn sequence B. Let $A_{s\ t}$ and $A_{s'\ t'}$ be $u\times v$ windows for $0\leq s,s'\leq u-1$ and $0\leq t,t'\leq c^{uv}/u-1$, and let $A_{s\ t}=(\alpha_{i\ j})$ and $A_{s'\ t'}=(\beta_{i\ j})$ where $0\leq i\leq u-1$, $0\leq j\leq v-1$. Suppose that $A_{s\ t}=A_{s'\ t'}$. Then, for all $0\leq i\leq u-1$, $0\leq j\leq v-1$, we have $\alpha_{i\ j}=\beta_{i\ j}$ i.e. $a_{s+i\ t+j}=a_{s'+i\ t'+j}$, and hence $\overline{b}_{(i+uj)+s+tu}=\overline{b}_{(i+uj)+s'+t'u}$. This implies that $\overline{b}_{s+tu+l}=\overline{b}_{s'+t'u+l}$ for all l with $0\leq l\leq uv-1$. This implies that $B_{s+tu}=B_{s'+t'u}$. Since $0\leq s,s'\leq u-1$ and $0\leq t,t'\leq (c^{uv}/u)-1$ so that $0\leq s+tu,\ s'+t'u\leq c^{uv}-1$, it follows from the definition of the given de Bruijn sequence that s+tu=s'+t'u and hence s=s' and t=t'. Therefore, we conclude that $A_{s\ t}$ and $A_{s'\ t'}$ are identical if and only if s=s' and t=t', which implies that

$$u\left(c^{uv} + v - 1\right) = \left| \left[A_{(m-u+1)\times(n-v+1)} \right] \right| = \left| \left[A_{u\times(\frac{c^{uv}}{u})} \right] \right| = c^{uv}.$$

It follows that every c-ary $u \times v$ array occurs exactly once as a window i.e. A is a c-ary $(2u-1, \frac{c^{uv}}{u}+v-1; u, v)$ APM. \blacksquare

The following example is established directly from Construction 14.

Example 16 (A 2-ary (3,9;2,2)APM)

This is the case u = v = 2 in Construction 14. Then uv = 4 and $c^{uv} + uv - 1 = 19$. We take $\bar{B} = (\bar{b}_k)$ the closure of a 2-ary span 4(=uv) de Bruijn sequence $B = (b_l)$ such as

$$\bar{B} = (b_0 \ b_1 \dots b_{15} \ b_0 \ b_1 \ b_2) = (0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1).$$

By Construction 14, we obtain the following 2-ary (3,9;2,2)APM $A = (a_{ij})$ where $a_{ij} = \bar{b}_{i+2j}$.

By Theorem 15, we have the following corollary concerning the existence for an APM when m=3 and u=2, v=2.

Corollary 17 For any given admissible parameter set (c; m = 3, n; u = 2, v = 2) for APM, there exists a c-ary (3, n; 2, 2)APM.

Proof. Clearly, m = 3 = 2u - 1 and the result follows by Theorem 15.

By Corollary 13, Corollary 17 and Result 3, therefore, the following result on the existence of APM for 2×2 window size is immediate.

Theorem 18 For every admissible parameter set (c; m, n; 2, 2) for APM, there exists a c - ary (m, n; 2, 2)APM. (i.e. the necessary condition for APM (Result 4) is sufficient for the existence of a c - ary (m, n; 2, 2)APM)

Acknowledgement

Most of the work is a part of my Ph.D thesis in Royal Holloway, University of London. I would like to thank both my supervisor, Prof. Fred Piper, and my advisor, Prof. Peter Wild.

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. Wagh, On Construction of Matrices with distict submatrices, SIAM J. Algebraic and Discrete Methods, vol. 1, pp.107-113, 1980.

- [7] C.J. Mitchell, Aperiodic and semi-periodic perfect maps, IEEE transactions on Information Theory 41, pp.88-95, 1995.
- [8] K.G. Paterson, New Classes of Perfect Maps I, Journal of Combinatorial Theory (Series A) 73, pp.302-334, 1996.
- [9] K.G. Paterson, New Classes of Perfect Maps II, Journal of Combinatorial Theory (Series A) 73, pp.335-345, 1996.
- [10] D. Rees, Note on a paper by I. J. Good, J. London Math. Soc., vol. 21, pp.169-172, 1946.