Aperiodic and Semi-Periodic Perfect Maps

Chris J. Mitchell

Abstract— **Paterson [1] has recently shown that the trivial necessary conditions are sufficient for the existence of a (binary) perfect map. These periodic structures can be transformed very simply into corresponding aperiodic and semi-periodic perfect maps. However, aperiodic and semi-periodic perfect maps can exist for parameter sets for which the corresponding periodic perfect maps cannot. In this paper it is shown, by construction, that (binary) aperiodic and semi-periodic perfect maps exist for all possible parameter sets.**

Index Terms— **de Bruijn array, window array, de Bruijn sequence.**

I. Introduction

PERFECT MAPS, namely, two-dimensional arrays in which every possible rectangular sub-array (of fixed size) occurs precisely once, have been studied for some 30 years (see, for example, Reed and Stewart's 1962 paper [2]). A number of construction methods have been devised [3]–[5] and the existence question has recently been completely answered [1].

A number of possible applications exist for such arrays, perhaps the most obvious of which is their use for two-dimensional position location. The basic idea is that, if such a map is written in some way onto a planar surface, then any device capable of examining an appropriately sized rectangular subarray will be able to precisely determine its position on the surface. Brief mention is made of such an application by Reed and Stewart, [2], and a more detailed description of applications of this type can be found in Burns and Mitchell [6]. Before proceeding also note that, in the one-dimensional case, similar position-detection applications have been suggested for de Bruijn and m-sequences by a number of authors (see, for example, Bondy and Murty [7], Petriu *et al.* [8]–[13], and Arazi [14]).

It is worth pointing out that the position-detection application does not require the "extreme" property of Perfect Maps; namely, that each subarray occurs exactly once. The key requirement is that each subarray occurs at most once. This logic has led some authors to apply the term Perfect Map in a rather looser way to a much larger class of arrays (see, for example, Reed and Stewart [2]). Of particular importance in this context are the *pseudorandom arrays* (see, for example, Nomura *et al.* [15], MacWilliams and Sloane [16], and Etzion [3]) which have the property that each subarray, apart from the all-zero subarray, occurs exactly once. Other arrays with the property that each subarray occurs at most once have been constructed by Dénes and Keedwell [17] and Etzion [3].

Historically, the study of Perfect Maps has almost exclusively been concerned with the *periodic* case, i.e., where the array is considered to be wrapped round on itself—in the one-dimensional case this corresponds to writing the sequence on the outside of a cylinder, and in the two-dimensional case to writing the array onto a torus. Subarrays then exist starting at any point in the array, which no longer has any "edges." It is also occasionally worth considering the case where one dimension is regarded periodically and the other aperiodically, as would happen if a two-dimensional array were written onto the outside of a cylinder.

However, for the practical position-location application briefly mentioned above, the *aperiodic* case is far more relevant. Here the array is deemed to be written onto a planar surface and the subarrays are always completely within the borders of the array. For these practical reasons, we are primarily concerned in this paper with this aperiodic case. However, we do consider *semi-periodic* arrays, where the array is considered periodically in one axis and aperiodically in the other. This corresponds to writing the array onto the outside of a cylinder.

We first show that any periodic array can be used in a very simple way to construct slightly larger aperiodic and semi-periodic arrays. We then give some construction methods for c-ary semi-periodic and aperiodic perfect maps which, in the binary case (i.e., $c = 2$), completely answer the existence question for these arrays.

II. Formal Definitions and Notation

In this paper we consider c-ary m by n integer arrays, which we write as

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

where each entry a_{ij} satisfies $0 \leq a_{ij} \leq c-1$.

If A is an m by n c-ary array, we define its u by v subarrays to be the c-ary arrays

$$A_{st} = (a_{ij}^{(st)},\ 0 \leq i \leq u-1,\ 0 \leq j \leq v-1), \qquad 0 \leq s \leq m-1,\ 0 \leq t \leq n-1$$

defined by

$$a_{ij}^{(st)} = a_{i+s,j+t}$$

where $i+s$ is computed modulo m and $j+t$ is computed modulo n. In the case of a sequence of length n, we analogously refer to the set of *subsequences* of length v, where this set will contain n members.

Manuscript received March 8, 1993; revised December 22, 1993.
The author is with the Department of Computer Science, Royal Holloway, University of London, Egham, Surrey TW20 OEX, England.
IEEE Log Number 9406408.

0018–9448/95$04.00

Observe that in the aperiodic case we are only interested in those subarrays. A_{st} for which $0 \le s \le m-u$ and $0 \le t \le n-v$. We call this subset of subarrays the *aperiodic subarrays.*

A. Periodic Perfect Maps and de Bruijn Sequences

Using the notation of Fan *et al.* [4], define a $(m, n; u, v)$-*Periodic Perfect Map*, or simply a $(m, n; u, v)$-PM to be a c-ary m by n array ($c \ge 2$, $m \ge u \ge 1$, $n \ge v \ge 1$) with the property that each possible u by v c-ary array occurs exactly once in the set of u by v subarrays $\{A_{st}: 0 \le s \le m-1,\ 0 \le t \le n-1\}$. Note that $(1, n; 1, v)$-PMs are simply the well-known de Bruijn sequences.

We immediately have the following well-known result relating the parameters of a Periodic Perfect Map.

Lemma 1: If A is a c-ary $(m, n; u, v)$*-PM then*

i) $$m > u \quad \text{or} \quad m = u = 1$$

ii) $$n > v \quad \text{or} \quad n = v = 1$$

and

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

Proof: i) is immediate on observing that if $m = u$ then any $m \times n$ array must contain the all-zero $u \times v$ subarray either not at all or at least u times. ii) is similar and iii) follows directly from the definition of perfect map. ■

It has recently been shown by Paterson [1], that in the binary case, the necessary conditions of Lemma 1 are in fact sufficient for the existence of Periodic Perfect Maps.

We next briefly review the one-dimensional analog of Periodic Perfect Maps. As we have already observed, a $(1, n; 1, v)$-PM is simply a span *v de Bruijn sequence.* For such sequences we have the following well-known result [18]–[20].

Theorem 2 (De Bruijn, Good, Rees): A c-ary span v de Bruijn sequence (i.e., a sequence of length $n = c^v$ with entries from $\{0, 1, \cdots, c-1\}$ in which every distinct c-ary v-tuple occurs exactly once) exists for every c and v ($c \ge 2$ and $v \ge 1$).

Many construction methods have been devised for de Bruijn sequences, see, for example, [21].

The one-dimensional analog of a pseudorandom array is what we call a *span v pseudorandom sequence*, and is a c-ary sequence of length $n = c^v - 1$ with the property that every c-ary v-tuple occurs, with the exception of the all-zero v-tuple. The following result is well-known (see, for example, [6]).

Lemma 3: There exists a $(c-1)$-to-one correspondence between the set of c-ary span v de Bruijn sequences and the set of c-ary span v pseudorandom sequences.

Given a span v de Bruijn sequence, the corresponding pseudorandom sequence is derived be deleting one of the zeros from the unique v-tuple of zeros. Hence pseudorandom sequences exist for every choice of c and v.

Given a finite sequence $C = (c_i)$, $(0 \le i \le n-1)$, and a nonnegative integer k, we define $\boldsymbol{T}_k(C)$ to be the *cyclic shift* of C by k places. If we write $(d_i) = \boldsymbol{T}_k(C)$, then

$$d_{i+k} = c_i \qquad (0 \le i \le n-1)$$

where $i + k$ is calculated modulo n.

We also need to consider the existence of *Perfect Factors*, introduced by Etzion [3]. An (n, c, v)-Perfect Factor ($c \ge 2$, $n \mid c^v$) consists of a collection of c^v/n c-ary sequences (*cycles*) of length n, with the property that every c-ary v-tuple occurs in a unique sequence in the collection. Note that a (c^v, c, v)-Perfect Factor is simply a c-ary, span v de Bruijn sequence. Etzion ([3, Theorem 4]) established the following key result:

Theorem 4 (Etzion): If k and v are positive integers satisfying

$$v < 2^k \le 2^v$$

then there exists a $(2^k, 2, v)$-Perfect Factor.

B. Aperiodic and Semi-Periodic Perfect Maps

Next define a $(m, n; u, v)$-*Aperiodic Perfect Map*, or simply a $(m, n; u, v)$-APM to be a c-ary m by n array ($c \ge 2$, $m \ge u \ge 1$, $n \ge v \ge 1$) with the property that each possible u by v c-ary array occurs exactly once in the set of u by v aperiodic subarrays $\{A_{st}: 0 \le s \le m-u,\ 0 \le t \le n-v\}$. We immediately have the following result relating the parameters of an Aperiodic Perfect Map:

Lemma 5: If A is a c-ary $(m, n; u, v)$-APM then

i) $$m \ge u$$

ii) $$n \ge v$$

and

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

Proof: i) is immediate on observing that if $m < u$ then the array will have no aperiodic subarrays. ii) is similar and iii) follows directly from the definition of aperiodic perfect map. ■

Examples of aperiodic binary perfect maps can be found in [6]. More specifically, [6, figs. 2 and 3] contain a (3, 34, 2, 3)-APM and a (4, 33, 3, 2)-APM, respectively.

In the remainder of this paper we work with a class of arrays which we call *Semi-Periodic Perfect Maps.* These two-dimensional arrays are regarded as periodic in one dimension and aperiodic in the other. More formally given a c-ary m by n array A, with u by v subarrays A_{st}, we call those subarrays A_{st} having $0 \le s \le m-u$ and $0 \le t \le n-1$ the *Semi-Periodic Subarrays* of A. We can then define a $(m, n; u, v)$-*Semi-Periodic Perfect Map*, or simply a $(m, n; u, v)$-SPM to be a c-ary m by n array ($c \ge 2$, $m \ge u \ge 1$, $n \ge v \ge 1$) with the property that each possible u by v c-ary array occurs exactly once in the set of u by v semi-periodic subarrays $\{A_{st}: 0 \le s \le m-u,\ 0 \le t \le n-1\}$. As previously, we immediately have the following result relating the parameters of a Semi-Periodic Perfect Map:

Lemma 6: If A is a c-ary $(m, n; u, v)$-SPM then

i) $$m \ge u$$

ii) $$n > v \quad \text{or} \quad n = v = 1$$

and

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

Before proceeding we make the following existence conjectures for Semi-Periodic and Aperiodic Perfect Maps.

Conjecture 7: The necessary conditions of Lemma 5 on m, n, u, v are sufficient for the existence of a c-ary $(m, n; u, v)$-APM.

Conjecture 8: The necessary conditions of Lemma 6 on m, n, u, v are sufficient for the existence of a c-ary $(m, n; u, v)$-SPM.

As has been observed in [6], Conjecture 7 trivially holds when $m = 1$, i.e., in the sequence case. In the remainder of this paper we show that the above two Conjectures hold in the case when $c = 2$.

III. Constructing APM's from PM's

We next describe how any c-ary periodic perfect map (an $(m, n; u, v)$-PM say) can be trivially transformed into a c-ary aperiodic perfect map of slightly larger dimensions (an $(m+u-1, n+v-1; u, v)$-APM)—this construction is also given in [6]. This construction merely involves adding copies of the first $u-1$ rows of a periodic array at the bottom of the array and adding copies of the first $v-1$ columns of the array after the last column (generating an $(m+u-1)\times(n+v-1)$ array from an $m \times n$ array).

Definition 9: Suppose m, n, u, v are positive integers satisfying $1 \le u \le m$ and $1 \le v \le n$. Suppose also that $A = (a_{ij})$ $(0 \le i \le m-1,\ 0 \le j \le n-1)$ is an m by n array. Then let $\boldsymbol{E}_{uv}(A) = (b_{ij})$ $(0 \le i \le m+u-2$ and $0 \le j \le n+v-2)$ be the $(m+u-1)$ by $(n+v-1)$ array defined by

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

where $s = i \bmod m$ and $t = j \bmod n$.

Observe that $\boldsymbol{E}_{1,1}(A) = A$. Note also that the above elementary construction was previously described by Kanetkar and Wagh [22]. We can now state the following:

Lemma 10: If A is a $(m-u+1, n-v+1; u, v)$-PM $(m \ge u, n \ge v)$, then $\boldsymbol{E}_{uv}(A)$ is an $(m, n; u, v)$-APM.

Proof: It should be clear that the set of u by v subarrays of A is identical to the set of u by v *aperiodic* subarrays of $\boldsymbol{E}_{uv}(A)$. The result follows immediately from the definitions. ∎

We now have:

Corollary 11: Suppose m, n, u, v are positive integers satisfying

i) $m \ge 2u$ or $m = u = 1$
ii) $n \ge 2v$ or $n = v = 1$

and

iii) $(m-u+1)(n-v+1) = 2^{uv}$.

Then there exists a binary $(m, n; u, v)$-APM.

Proof: First observe that Paterson [1] has shown that the necessary conditions of Lemma 1 are sufficient for the existence of Periodic Perfect Maps in the binary case (i.e., for $c = 2$). Hence there exists a binary $(m-u+1, n-v+1; u, v)$-PM. The result follows immediately from Lemma 10. ∎

Observe that, in a similar way, we may obtain an $(m+u-1, n; u, v)$-SPM from an $(m, n; u, v)$-PM and an $(m, n+v-1; u, v)$-APM from an $(m, n; u, v)$-SPM. Indeed, the example of a (3, 34, 2, 3)-APM given in [6] has its first two columns equal to its last two columns, and hence has been derived from a (3, 32, 2, 3)-SPM. Similarly, the (4, 33, 3, 2)-APM in [6] has its first column equal to its last and has therefore been derived from a (4, 32, 3, 2)-SPM. This leads to the following two results.

Corollary 12: Suppose m, n, u, v are positive integers satisfying

i) $m \ge 2u$ or $m = u = 1$
ii) $n > v$ or $n = v = 1$

and

iii) $(m-u+1)n = 2^{uv}$.

Then there exists a binary $(m, n; u, v)$-SPM.

Corollary 13: Suppose there exists a c-ary $(m, n; u, v)$-SPM. Then there also exists a c-ary $(m, n+v-1; u, v)$-APM.

We can now state the following key lemma.

Lemma 14: If Conjecture 8 holds for any c, then Conjecture 7 also holds for that value of c.

Proof: Suppose c is fixed and suppose Conjecture 8 holds for that value of c. Suppose also that (m, n, u, v) satisfy the conditions of Lemma 5.

First observe that if $(m, n-v+1, u, v)$ satisfy the conditions of Lemma 6, then a c-ary $(m, n; u, v)$-APM exists by Corollary 13. But $(m, n-v+1, u, v)$ do satisfy the conditions of Lemma 6 unless $n-v+1 \le v$, i.e., unless $n \le 2v-1$.

Next note that if $(n, m-u+1, v, u)$ satisfy the conditions of Lemma 6, then a c-ary $(n, m; v, u)$-APM exists by Corollary 13, and hence a c-ary $(m, n; u, v)$-APM exists; but $(n, m-u+1, v, u)$ do satisfy the conditions of Lemma 6 unless $m \le 2u-1$. Hence we need only consider the case where $n \le 2v-1$ and $m \le 2u-1$. Since $(m-u+1)(n-v+1) = c^{uv}$, we have $c^{uv} \le uv$. But this can never hold given $uv \ge 1$ and $c \ge 2$. This completes the proof of the lemma. ∎

Remark 15: From Corollary 12 and Lemma 14, in order to prove Conjectures 7 and 8 for the binary case we now need only show how to construct an $(m, n; u, v)$-SPM when $u \le m < 2u$ (and, as always, given $n > v$ or $n = v = 1$ and $2^{uv} = (m+u-1)n$).

IV. The Main Construction Method

We next give a construction method which, in the binary case, leaves only the existence of SPMs satisfying $v \in \{1, 2\}$ unresolved. We show how arrays with these parameters may be constructed in a subsequent part of this paper.

Construction 16: Suppose c, m, u, v are positive integers satisfying

i) $c > 1$
ii) $u \le m$
iii) $(m-u+1) \mid c^u$

(and hence let $d = c^u/(m-u+1)$ and $n = c^{uv}/(m-u+1) + (v-1)$) and

iv) if $(m-u+1)$

is even then $v > 2$, else $v > 1$.

Suppose that B is a c-ary span u de Bruijn sequence (which exists by Theorem 2), and let $\{B_s : 0 \le s < c^u\}$ be the set of subsequences of B of length m.

Let (r_i), $(0 \le i < n)$, be $(m-u+1)^{v-1}$ repetitions of a d-ary span v de Bruijn sequence followed by the first $v-1$ elements of this sequence (such de Bruijn sequences always exist by Theorem 2). Suppose also that (s_i), $(0 \le i < n)$, is d^v repetitions of a $(m-u+1)$-ary span $v-1$ pseudorandom sequence for which the first $v-2$ elements are all zeros, preceded by d^v zeros and followed by $v-1$ zeros (again such sequences always exist by Theorem 2 and Lemma 3). Note that if $m = u$ then (s_i) consists of $c^{uv} + v - 1$ zeros. Finally, define the sequence (w_i), $(0 \le i < n)$ by

$$w_i = \sum_{j=0}^{i-1} s_j \bmod (m-u+1)$$

where $w_0 = 0$. Now define an $m \times n$ array by letting it have column $i (0 \le i < n)$ equal to $B_{(m-u+1)r_i + w_i}$, i.e., the ith column consists of the subsequence $B_{(m-u+1)r_i+w_i}$ of the chosen c-ary span u de Bruijn sequence B.

Theorem 17: Suppose c, m, u, v satisfy the conditions of Construction 16. Then an $m \times n$ array A obtained using Construction 16 is a c-ary $(m, n;\ u, v)$-APM.

Proof: For the purposes of this proof let

$$t = (m-u+1)^{v-1} - 1.$$

First note that

$$w_{i+\mu t} - w_i = 0 \tag{1}$$

for any nonnegative integers i and μ satisfying $d^v \le i$ and $i + \mu t < n$. To show this, observe that, since (s_j) is periodic with period t (for $d^v \le j < n-1$)

$$\begin{aligned} w_{i+\mu t} - w_i &\equiv \sum_{j=0}^{i+\mu t-1} s_j - \sum_{j=0}^{i-1} s_j \pmod{m-u+1} \\ &= \sum_{j=i}^{i+\mu t-1} s_j \\ &= \mu S \end{aligned}$$

where

$$\begin{aligned} S &= \sum_{i=0}^{t-1} s_j \\ &= (m-u+1)^{v-2}(1+2+\cdots+(m-u+1)-1) \\ &= \frac{(m-u+1)^{v-1}(m-u)}{2}. \end{aligned}$$

Since $v > 2$ if $(m-u+1)$ is even and $v > 1$ if $(m-u+1)$ is odd, we have

$$S \equiv 0 \pmod{m-u+1}$$

and the desired result follows.

Next suppose D is a $u \times v$ c-ary array—we need to show that this array occurs somewhere within the $m \times n$ array A. To achieve this we show that it can occur at most once in the array, and by numerical considerations we have completed the proof.

Suppose D has columns $\boldsymbol{d}_0, \boldsymbol{d}_1, \cdots, \boldsymbol{d}_{v-1}$, where

$$\boldsymbol{d}_i = (d_{i,0}, d_{i,1}, \cdots, d_{i,u-1})$$

is a c-ary u-tuple $(0 \le i < u)$. Suppose also that D occurs in A both

- in columns $x, x+1, \cdots, x+v-1$ and in rows $y, y+1, \cdots, y+u-1$, and
- in columns $x', x'+1, \cdots, x'+v-1$ and in rows $y', y'+1, \cdots, y'+u-1$,

where $0 \le x \le n-v$, $0 \le y \le m-u$, $0 \le x' \le n-v$, and $0 \le y' \le m-u$. Hence, by definition of A we have

$$d_{ij} = b_{(m-u+1)r_{x+i} + w_{x+i} + y + j}$$

and also

$$d_{ij} = b_{(m-u+1)r_{x'+i} + w_{x'+i} + y' + j}$$

for every i, j, $(0 \le i < v,\ 0 \le j < u)$. Then

$$b_{(m-u+1)r_{x+i} + w_{x+i} + y + j} = b_{(m-u+1)r_{x'+i} + w_{x'+i} + y' + j}$$

for every i, j, $(0 \le i < v,\ 0 \le j < u)$, and, since $B = (b_i)$ is a c-ary span u de Bruijn sequence

$$\begin{aligned} (m-u+1)r_{x+i} + w_{x+i} + y \equiv (m-u+1)&r_{x'+i} \\ + w_{x'+i} + y' &\pmod{c^u} \end{aligned} \tag{2}$$

for every i, $(0 \le i < v)$. Now we know that $(m-u+1) \mid c^u$ so

$$w_{x+i} + y \equiv w_{x'+i} + y' \pmod{m-u+1} \tag{3}$$

for every i, $(0 \le i < v)$. Now, by definition,

$$w_{x+i} \equiv \sum_{j=0}^{x+i-1} s_j \pmod{m-u+1}$$

and hence

$$s_{x+i} \equiv w_{x+i+1} - w_{x+i} \pmod{m-u+1}$$

for every i, $(0 \le i \le v-2)$. Thus by (3), we have

$$s_{x+i} \equiv s_{x'+i} \pmod{m-u+1}$$

for every i, $(0 \le i \le v-2)$. Now (s_i) consists of d^v repetitions of a $(m-u+1)$-ary span $v-1$ pseudo-random sequence for which the first $v-2$ elements are zeros (and hence the last element is nonzero), preceded by d^v zeros and succeeded by $v-1$ zeros. Since $x+i \le n-2$ and $x'+i \le n-2$, either

i) $$s_{x+i} = s_{x'+i} = 0$$

for every i, $(0 \le i \le v-2)$, in which case $x, x' \in \{0, 1, \cdots, d^v - 1\}$, or

ii) $$x,\, x' \in \{d^v,\, d^v+1, \cdots, n-v\}$$

and $x \equiv x' \pmod{t}$ (since the pseudo-random sequence used to construct (s_i) has period t).

We now claim that we must have

$$w_{x+i} = w_{x'+i} \tag{4}$$

for every i, $(0 \le i < v)$. In case i) this follows immediately from the definition of (w_i), since we must have $w_{x+i} = w_{x'+i} = 0$ for every i, $(0 \le i < v)$. In case ii) the desired result follows immediately from (1). Combining (3) and (4) we immediately obtain

$$y \equiv y' \pmod{m-u+1}$$

and since $y,\, y' \in \{0, 1, \cdots, m-u\}$, we have

$$y = y'. \tag{5}$$

Substituting (4) and (5) into (2) we obtain

$$(m-u+1)r_{x+i} \equiv (m-u+1)r_{x'+i} \pmod{c^u}$$

for every i, $(0 \le i < v)$, and hence

$$r_{x+i} \equiv r_{x'+i} \pmod{d}$$

for every i, $(0 \le i < v)$. However, (r_i) consists of $t+1$ repetitions of a d-ary span v de Bruijn sequence, so

$$x \equiv x' \pmod{d^v}. \tag{6}$$

Recall that either

i) $$x,\, x' \in \{0, 1, \cdots, d^v-1\},$$

or

ii) $$x,\, x' \in \{d^v,\, d^v+1, \cdots, n-v\}$$

and $x \equiv x' \pmod{t}$.

In case i), (6) immediately implies that $x = x'$. In case ii), if we combine (6) and the fact that $x \equiv x' \pmod{t}$ (noting that $(d^v, t) = 1$) we obtain

$$x \equiv x' \pmod{d^v t}. \tag{7}$$

Now $n - v = d^v + (d^v t - 1)$, and, by (7), we must have

$$x = x'.$$

The result now follows. ■

Example 18: As an example of the above construction method, consider the case $c = 2$, $u = 2$, $v = 3$, and $m = 3$ (hence $c^{uv}/(m-u+1) + v - 1 = n = 2^6/2 + 2 = 34$ and so we construct a (3, 34; 2, 3)-APM). We first need a 2-ary span 2 de Bruijn sequence, for example:

$$B = (0\ 0\ 1\ 1).$$

Hence, since $m = 3$ we also have

$$\begin{aligned} B_0 &= (0\ 0\ 1) \\ B_1 &= (0\ 1\ 1) \\ B_2 &= (1\ 1\ 0) \\ B_3 &= (1\ 0\ 0). \end{aligned}$$

Now (r_i) is 4 repetitions (plus the first two elements) of a 2-ary span 3 de Bruijn sequence, an example of which is provided by

$$(0\ 0\ 0\ 1\ 0\ 1\ 1\ 1)$$

and hence (r_i) is

$$(0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1$$
$$1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0).$$

Similarly (s_i) is 8 repetitions (preceded by 8 zeros and succeeded by two zeros) of a 2-ary span 2 pseudo-random sequence starting with one zero, an example of which is provided by

$$(0\ 1\ 1)$$

and hence (s_i) is

$$(0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1$$
$$0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0).$$

Then $(w_i) = (\sum_{j=0}^{i-1} s_j \bmod 2)$ is

$$(0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$$
$$0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0),$$

and $(2r_i + w_i)$ is as follows:

$$(0\ 0\ 0\ 2\ 0\ 2\ 2\ 2\ 0$$
$$0\ 1\ 2\ 0\ 3\ 2\ 2\ 1\ 0\ 0\ 3\ 0\ 2\ 3\ 2\ 0\ 1\ 0\ 2\ 1\ 2\ 2\ 3\ 0\ 0).$$

Using (r_i) and (w_i) as indicated in Construction 16 we obtain the following (3, 34; 2, 3)-APM (see bottom of page):

Remark 19: Construction 16 above is a modified version of [23, Construction 3.2], which is itself both a generalization of a construction of Ma [5], and a special case of a construction of Etzion [3].

$$\begin{pmatrix} 0&0&0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&0&0&1&0&1&1&1&0&0 \\ 0&0&0&1&0&1&1&1&0&0&1&1&0&0&1&1&1&0&0&0&0&1&0&1&0&1&0&1&1&1&1&0&0&0 \\ 1&1&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1&1 \end{pmatrix}.$$

Remark 20: It should be clear that, given that the conditions of Theorem 17 hold, if A is a c-ary $(m,\ c^{uv}/(m-u+1)+(v-1);\ u,\ v)$-APM obtained using Construction 16, A will have its first $v-1$ columns equal to its last $v-1$ columns. Hence if A' is obtained from A by deleting its last $v-1$ columns then A' will be a $(m,\ c^{uv}/(m-u+1);\ u,\ v)$-SPM.

V. A Surgical Construction Method

We next present a construction method which, in conjunction with Construction 16 above and certain other observations, enables us to completely answer the existence question for binary SPM's (and hence also for APM's).

Construction 21: Suppose $m,\ n,\ u,\ v$ are positive integers where i) $m \geq u$, ii) $n > v$ or $v = 1$, and iii) $(m-u+1)$ is even. Let A be a c-ary $(m,\ n;\ u,\ v)$-SPM, and put $m' = (m-u+1)/2 + (u-1)$. Suppose also that, for some $i,\ j \in \{0,\ 1, \cdots, n-1\}$, the $m' \times (v-1)$ submatrix D_i of A consisting of the entries in columns $i,\ i+1, \cdots, i+v-2$ (working modulo n) and rows $0,\ 1, \cdots, m'-1$, is equal to the $m' \times (v-1)$ submatrix E_j of A consisting of the entries in columns $j,\ j+1, \cdots, j+v-2$ (working modulo n) and rows $m-m',\ m-m'+1, \cdots, m-1$. Equivalently, if A_{st}, $(0 \leq s \leq m-u,\ 0 \leq t \leq n-1)$ are the $m' \times (v-1)$ semiperiodic subarrays of A, then suppose that A_{0i} is equal to $A_{m-m',j}$ for some $i,\ j$. Then construct an $m' \times 2n$ matrix A' as follows:

- Let columns $0,\ 1, \cdots, i-1$ be equal to the first m' entries in columns $0,\ 1, \cdots, i-1$ of A (i.e., the entries in rows $0,\ 1, \cdots, m'-1$).
- Let columns $i,\ i+1, \cdots, i+n-1$ be equal to the last m' entries in columns $j,\ j+1, \cdots, n-1,\ 0,\ 1, \cdots, j-1$ of A (i.e., the entries in rows $m-m',\ m-m'+1, \cdots, m-1$).
- Let columns $i+n,\ i+n+1, \cdots, 2n-1$ be equal to the first m' entries in columns $i,\ i+1, \cdots, n-1$ of A (i.e., the entries in rows $0,\ 1, \cdots, m'-1$).

Theorem 22: Let A be a c-ary $(m,\ n;\ u,\ v)$-SPM satisfying the conditions of Construction 21. Then A' (constructed from A using Construction 21) is a c-ary $(m',\ 2n;\ u,\ v)$-SPM.

Proof: Suppose D is any c-ary u by v array. We need to show that D is equal to one of the u by v semiperiodic subarrays of A'. First note that, by the assumption of the theorem, D must be equal to a u by v semiperiodic subarray of A. Suppose D is equal to the semiperiodic subarray A_{ij} of A, where $i,\ j$ satisfy $0 \leq i \leq m-u$, $0 \leq j \leq n-1$. We need to consider two cases:

i) $$0 \leq i \leq m'-u$$

and

ii) $$m'-u < i \leq m-u.$$

In case i), D will be completely contained in rows $0,\ 1, \cdots, m'-1$ of A. Hence, by definition, D will appear in A'. Similarly, in case ii), D will be completely contained in rows $m-m',\ m-m'+1, \cdots, m-1$ of A, and hence must again appear in A'. ■

In the remainder of this section we show how to apply Construction 21 to SPM's satisfying $c = v = 2$ (i.e., binary arrays with subarrays having two columns). Observe that if A is a binary $(m,\ n;\ u,\ 2)$-SPM then, by Lemma 6 iii), we have

$$(m-u+1)n = 2^{2u}$$

so there exists an integer $k (0 \leq k < 2n-1)$ such that

$$m = 2^k + (u-1)$$

and

$$n = 2^{2u-k}.$$

We next give necessary conditions for the repeated application of Construction 21 in this special case. We first need the following definition. Suppose A is a binary $(2^k + (u-1),\ 2^{2u-k};\ u,\ 2)$-SPM for some integer k, $(0 \leq k < 2u-1)$. Suppose also that A contains pairs of columns (not necessarily disjoint)

$$(\boldsymbol{x}_0,\ \boldsymbol{y}_0),\ (\boldsymbol{x}_1,\ \boldsymbol{y}_1), \cdots, (\boldsymbol{x}_{k-1},\ \boldsymbol{y}_{k-1})$$

with the property that entries $0,\ 1, \cdots, 2^i + (u-1)$ of $\boldsymbol{x}_i$ are identical to entries $2^i,\ 2^i+1, \cdots, 2^{i+1} + (u-1)$ of $\boldsymbol{y}_i$ for every i, $(0 \leq i < k)$. Then A is said to satisfy *Condition R*.

Lemma 23: Suppose A_k is a binary $(2^k + (u-1),\ 2^{2u-k};\ u,\ 2)$-SPM for some integer k, $(0 \leq k < 2u-1)$. Suppose also that A_k satisfies Condition R. Then Construction 21 can be recursively applied a total of u times to A_k to produce a sequence of arrays $A_{k-1},\ A_{k-2}, \cdots, A_0$, where A_i is a $(2^i + (u-1),\ 2^{2u-i};\ u,\ 2)$-SPM for every i, $(0 \leq i < k)$.

Proof: First observe that the existence of the pair of columns $(\boldsymbol{x}_{k-1},\ \boldsymbol{y}_{k-1})$ in A_k are sufficient to enable us to apply Construction 21 to A_k to obtain a $(2^{k-1} + (u-1),\ 2^{2u-k+1};\ u,\ 2)$-SPM which we call A_{k-1}. We now show that A_{k-1} satisfies Condition R and the result then follows by induction.

In constructing A_{k-1} from A_k, every column of A_k, $\boldsymbol{x}$ say, is used to produce two columns of A_{k-1}. Label these columns $\boldsymbol{x}^u$ and $\boldsymbol{x}'$, where $\boldsymbol{x}^u$ contains the first $2^{k-1} + (u-1)$ elements of $\boldsymbol{x}$ and $\boldsymbol{x}'$ contains the last $2^{k-1} + (u-1)$ elements of $\boldsymbol{x}$. It should then be clear that the following pairs of columns of A_{k-1} have the properties required for Condition R to hold:

$$(\boldsymbol{x}_0^u,\ \boldsymbol{y}_0^u),\ (\boldsymbol{x}_1^u,\ \boldsymbol{y}_1^u), \cdots, (\boldsymbol{x}_{k-2}^u,\ \boldsymbol{y}_{k-2}^u).$$

The result now follows. ■

We next show how to construct SPM's suitable for use in Construction 21, i.e., satisfying Condition R. To do this we need the following construction method given in [23], which we repeat below for the special case $v = 2$.

Construction 24: Suppose u and k are positive integers satisfying

$$u + 1 \leq 2^k < 2^n.$$

Suppose $C_0,\ C_1, \cdots C_{2^{n-k}-1}$ are the 2^{n-k} cycles of length 2^k of a $(2^k,\ 2,\ u)$-Perfect Factor (such a Perfect Factor exists by Theorem 4). Let (r_i), $(0 \leq i < 2^{2u-k})$, be 2^k repetitions of a 2^{u-k}-ary span 2 de Bruijn sequence. Suppose also that (s_i), $(0 \leq i < 2^{2u-k})$, is $2^{2(u-k)}$ repetitions of a 2^k-ary span 1 pseudorandom sequence, preceded by $2^{2(u-k)}$ zeros. Finally, define the sequence (w_i), $(0 \le i < 2^{2u-k})$ by

$$w_i = \sum_{j=0}^{i-1} s_j \bmod 2^k$$

where $w_0 = 0$.

Now define a $2^k \times 2^{2u-k}$ array by letting it have column i, $(0 \le i \le 2^{2u-k} - 1)$ be equal to $\boldsymbol{T}_{w_i}(C_{r_i})$, i.e., the ith column consists of the cycle C_{r_i} of the chosen Perfect Factor cyclically shifted by w_i places.

The following result is also taken from [23].

Theorem 25: Suppose u and k are positive integers satisfying

$$u + 1 \le 2^k < 2^u.$$

Then a $2^k \times 2^{2u-k}$ array A obtained using Construction 24 is a $(2^k, 2^{2u-k}; u, 2)$-PM.

We can now state the following.

Lemma 26: Suppose $u \ge 3$ and let K be the unique integer satisfying

$$2^{K-1} \le u < 2^K.$$

Then Construction 24 can be used to obtain a $(2^K + (u-1), 2^{2u-K}; u, 2)$-SPM satisfying Condition R.

Proof: First note that, since $u \ge 3$, we must have $u > K$, and hence u and K satisfy the conditions of Theorem 25. Hence we can use Construction 24 to obtain a $(2^K, 2^{2u-K}; u, 2)$-PM, A say. By using the technique of Section III we can derive the desired $(2^K + (u-1), 2^{2u-K}; u, 2)$-SPM, A' say. It remains to show that A' satisfies Condition R.

The following statement can be deduced from the proof of Theorem 25 contained in [23].

> Every pair of cycles from the Perfect Factor used to construct A occur as consecutive columns at every possible relative shift somewhere in A.

Hence, for every i, $(0 \le i \le K-1)$, there exists a j_i, $(0 \le j_i \le 2^K - 1)$ such that $\boldsymbol{T}_{j_i}(C_0)$ and $\boldsymbol{T}_{j_i+2^i}(C_0)$ occur as consecutive columns in A, where $j_i + 2^i$ is computed modulo 2^K. It should be clear that the entries in positions $0, 1, \cdots, 2^i + u - 1$ of $\boldsymbol{T}_{j_i}(C_0)$ are the same as the entries in positions $2^i, 2^i + 1, \cdots, 2^{i+1} + u - 1$ of $\boldsymbol{T}_{j_i+2^i}(C_0)$, given that the entry positions are calculated modulo 2^K where necessary.

If $\boldsymbol{x}$ is a vector of length m, let $\boldsymbol{E}_u(\boldsymbol{x})$ denote the vector of length $m + u - 1$ obtained by adjoining to the end of $\boldsymbol{x}$ its first $u - 1$ elements (given $m \ge u$). Then it should be clear that if A has columns

$$\boldsymbol{z}_0, \boldsymbol{z}_1, \cdots, \boldsymbol{z}_{2^{2u-K}-1}$$

then A' has columns

$$\boldsymbol{E}_u(\boldsymbol{z}_0), \boldsymbol{E}_u(\boldsymbol{z}_1), \cdots, \boldsymbol{E}_u(\boldsymbol{z}_{2^{2u-K}-1}).$$

Thus if

$$\boldsymbol{z}_{l_i} = \boldsymbol{T}_{j_i}(C_0)$$

and

$$\boldsymbol{z}_{l_i+1} = \boldsymbol{T}_{j_i+2^i}(C_0)$$

then the entries in positions $0, 1, \cdots, 2^i + u - 1$ of $\boldsymbol{E}_u(\boldsymbol{z}_{l_i})$ are the same as the entries in positions $2^i, 2^i + 1, \cdots, 2^{i+1} + u - 1$ of $\boldsymbol{E}_u(\boldsymbol{z}_{l_i+1})$. Hence if we set

$$\boldsymbol{x}_i = \boldsymbol{E}_u(\boldsymbol{z}_{l_i})$$

and

$$\boldsymbol{y}_i = \boldsymbol{E}_u(\boldsymbol{z}_{l_i+1})$$

then the pairs

$$(\boldsymbol{x}_0, \boldsymbol{y}_0), (\boldsymbol{x}_1, \boldsymbol{y}_1), \cdots, (\boldsymbol{x}_{K-1}, \boldsymbol{y}_{K-1})$$

have the properties required to ensure that A' satisfies Condition R. The result now follows. ■

The following result is immediate from Lemmas 23 and 26.

Corollary 27: For every pair u, k satisfying

$$0 \le k < u, \; u \ge 3$$

Constructions 21 and 24 can be used to construct a $(2^k + u - 1, 2^{2u-k}; u, 2)$-SPM.

VI. Completing the Binary Case

We now consider for which parameter sets we can construct SPM's using the techniques described above, with the objective of proving Conjecture 8 for the binary case.

First note that, by Remark 15, we need only show how to construct a binary $(2^k + u - 1, 2^{uv-k}; u, v)$-SPM for k satisfying $1 \le 2^k \le u$. Now observe that, if $2^k \le u$ then, since $u \ge 1$, we must have $k < u$. But by Theorem 17 and Remark 20 we can construct a $(2^k + u - 1, 2^{uv-k}; u, v)$-SPM for every u, v, k given that

$$v \ge 3, \quad 2^k \ge 1, \quad k \le u.$$

Hence, given $v \ge 3$, we have shown that Conjecture 8 holds in the binary case.

In addition, by Corollary 27, if $u \ge 3$ we can construct a $(2^k + u - 1, 2^{2u-k}; u, 2)$-SPM for every u, k given that $0 \le k < u$. To complete the main objective of this paper, i.e., to show Conjecture 8 holds in the binary case, we need only consider the following three cases:

i) $$v = 1$$

ii) $$v = 2 \quad \text{and} \quad u = 1$$

and

iii) $$v = u = 2.$$

Case i) is covered by [6, Construction A and Theorem 10(i)], observing that when $v = 1$ the definition of an SPM coincides with the definition of an APM. In case ii) there is only one possible parameter set for an SPM, namely (1, 4; 1, 2), since we must have $n > v = 2$. Such an array clearly exists (it is nothing more than a span 2 de Bruijn sequence).

$$\begin{pmatrix} 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&1&1&0&1&1&0&1&1&0&1&1 \end{pmatrix}$$

Fig. 1. A (2, 16; 2, 2)-Semiperiodic Perfect Map.

$$\begin{pmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&0&1&0&0&1&0 \\ 0&0&1&1&1&1&0&0 \end{pmatrix}$$

Fig. 2. A (3, 8; 2, 2)-Semiperiodic Perfect Map.

In case iii) there are only three possible parameter sets for an SPM, namely

$$(2, 16;\ 2, 2),\ (3, 8;\ 2, 2),\ (5, 4;\ 2, 2).$$

A (5, 4; 2, 2)-SPM can be derived from a (4, 4; 2, 2)-PM as in Section III above. Examples of a (2, 16; 2, 2)-SPM and a (3, 8; 2, 2)-SPM are given in Figs. 1 and 2.

VII. The Decoding Problem

As discussed in [6] and [23], the application of Perfect Maps in position location applications requires a method for decoding. By decoding we mean a method for computing the position of a given subarray within a Perfect Map.

For those APM's and SPM's derived from Periodic Perfect Maps using the techniques of Section III, the decoding problem will be precisely the same as the decoding problem for the Periodic Perfect Map from which they are derived. This will, in turn, depend on the method used to construct the Periodic Map. Hence we do not discuss it further here.

The SPMs constructed using Construction 16 can almost certainly be decoded efficiently using a similar method to that described in detail in [23]. This is because the method of construction is very similar to that described in [23].

Finally, we consider those SPM's constructed using Construction 21 from other SPM's. It is straightforward to see that any decoding method for an SPM input to this method of construction can be modified to provide a decoding method for an output SPM. This modified decoding method need only incorporate information as to where "surgery" was performed on the original SPM.

VIII. Conclusions

In this paper we have shown that binary Semiperiodic and Aperiodic Perfect Maps exist for all possible parameter sets, i.e., Conjectures 7 and 8 hold when $c = 2$. More generally, we may also draw conclusions about the validity of these conjectures for $c > 2$. Suppose, as one might conjecture, that the necessary conditions of Lemma 1 are also sufficient for the existence of a Periodic Perfect Map. As we have already observed, Paterson [1] has shown this to be true for the binary case. Then the construction methods presented in this paper are sufficient to almost completely resolve Conjectures 7 and 8 for general c. It seems probable that the only case which would present any problems is when $v = 2$, and some variation on the theme of Section V can possibly be used to construct the desired SPM's in this case.

Finally note that the construction methods described here can possibly be generalized both to the multidimensional case of Perfect Maps and to a multidimensional generalization of Perfect Factors. Indeed, it would appear plausible that the obvious necessary conditions are sufficient for all these multidimensional de Bruijn-like structures, although proving this will probably require some new construction techniques.

Acknowledgment

The author wishes to thank K. Paterson for many valuable discussions and suggestions.

References

[1] K. Paterson, "Perfect maps," *IEEE Trans. on Inform. Theory*, vol. 40, pp. 743–753, 1994..

[2] I. S. Reed and R. Stewart, "Note on the existence of perfect maps," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 10–12, 1962.

[3] T. Etzion, "Constructions for perfect maps and pseudo-random arrays," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1308–1316, 1988.

[4] C. Fan, S. Fan, S. Ma, and M. Siu, "On de Bruijn arrays," *Ars Combinatoria*, vol. 19A, pp. 205–213, 1985.

[5] S. Ma, "A note on binary arrays with a certain window property," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 774–775, 1984.

[6] J. Burns and C. Mitchell, "Coding schemes for two-dimensional position sensing," in *Cryptography and Coding III*, M. Ganley, Ed. London, UK: Oxford Univ. Press, 1993, pp. 31–66.

[7] J. Bondy and U. Murty, *Graph Theory with Applications*. Amsterdam, The Netherlands: Elsevier, 1976.

[8] E. Petriu, "Absolute-type pseudorandom shaft encoder with any desired resolution," *Electron. Lett.*, vol. 21, pp. 215–216, 1985.

[9] ——, "Absolute-type position transducers using a pseudorandom encoding," *IEEE Trans. Instrum. Meas.*, vol. IM-36, pp. 950–955, 1987.

[10] ——, "New pseudorandom/natural code conversion method," *Electron. Lett.*, vol. 24, pp. 1358–1359, 1988.

[11] ——, "Scanning method for absolute pseudorandom position encoders," *Electron. Lett.*, vol. 24, pp. 1236–1237, 1988.

[12] E. Petriu and J. Basran, "On the position measurement of automated guided vehicles using pseudorandom encoding," *IEEE Trans. Instrum. Meas.*, vol. 38, pp. 799–803, 1989.

[13] E. Petriu, J. Basran, and F. Groen, "Automated guided vehicle position recovery," *IEEE Trans. Instrum. Meas.*, vol. 39, pp. 254–258, 1990.

[14] B. Arazi, "Position recovery using binary sequences," *Electron. Lett.*, vol. 20, pp. 61–62, 1984.

[15] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A theory of two-dimensional linear recurring arrays," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 775–785, 1972.

[16] F. J. MacWilliams and N. J. A. Sloane, "Pseudo-random sequences and arrays," *Proc. IEEE*, vol. 64, pp. 1715–1729, 1976.

[17] J. Dénes and A. Keedwell, "A new construction of two-dimensional arrays with the window property," *IEEE Trans. Inform. Theory*, vol. 36, pp. 873–876, 1990.

[18] N. de Bruijn, "A combinatorial problem," *Proc. Nederlandse Akademie van Wetenschappen*, vol. 49, pp. 758–764, 1946.

[19] I. J. Good, "Normally recurring decimals," *J. London Math. Soc.*, vol. 21, pp. 167–169, 1946.

[20] D. Rees, "Note on a paper by I. J. Good," *J. London Math. Soc.*, vol. 21, pp. 169–172, 1946.

[21] H. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," *SIAM Rev.*, vol. 24, pp. 195–221, 1982.

[22] S. Kanetkar and M. Wagh, "On construction of matrices with distinct submatrices," *SIAM J. Algebraic and Discrete Methods*, vol. 1, pp. 107–113, 1980.

[23] C. Mitchell and K. Paterson, "Decoding perfect maps," *Des., Codes Cryptog.*, vol. 4, pp. 11–30, 1994.