Constructing c-ary Perfect Factors

Chris J. Mitchell
Computer Science Department,
Royal Holloway, University of London,
Egham Hill,
Egham,
Surrey TW20 0EX,
England.

Tel.: +44–784–443423
Fax: +44–784–443420
Email: cjm@dcs.rhbnc.ac.uk

20th March 1993

Abstract

A *c-ary Perfect Factor* is a set of uniformly long cycles whose elements are drawn from a set of size c, in which every possible v-tuple of elements occurs exactly once. In the binary case, i.e. where $c = 2$, these perfect factors have previously been studied by Etzion, [2], who showed that the obvious necessary conditions for their existence are in fact sufficient. This result has recently been extended by Paterson, [4], who has shown that the necessary existence conditions are sufficient whenever c is a prime power. In this paper we conjecture that the same is true for arbitrary values of c, and exhibit a number of constructions. We also construct a family of related combinatorial objects, which we call *Perfect Multi-factors*.

Index Terms: de Bruijn graph, de Bruijn sequence, window sequence.

1 Introduction

Perfect factors were introduced, in the binary case, by Etzion, [2], who used them to construct a certain class of (binary) Perfect Maps. In doing so Etzion succeeded in showing that all the possible binary Perfect Factors exist. In this paper we are concerned with Perfect Factors over arbitrary finite alphabets. The motive for constructing these objects is two-fold.

Firstly, they can be used in an obvious generalisation of Etzion's construction to construct non-binary Perfect Maps; for further details see [4]. Perfect Maps, both binary and non-binary, have possible application in the field of automatic position sensing, see, for example, [1].

Secondly, they are of interest in their own right as natural generalisations of the classical de Bruijn sequences, about which much has been written. As described in [4], they also have applications in other areas, including the construction of de Bruijn sequences with minimal linear complexity.

1.1 Preliminary remarks and notation

We are concerned here with c-ary periodic sequences, where by the term c-ary we mean sequences whose elements are drawn from the set $\{0, 1, \ldots, c-1\}$. We refer throughout to c-ary cycles of period n, by which we mean cyclic sequences $(s_0, s_1, \ldots, s_{n-1})$ where $s_i \in \{0, 1, \ldots, c-1\}$ for every i, $(0 \leq i < n)$.

If $\mathbf{t} = (t_0, t_1, \ldots, t_{v-1})$ is a c-ary v-tuple (i.e. $t_i \in \{0, 1, \ldots, c-1\}$ for every i, $(0 \leq i < v)$), and $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})$ is a c-ary cycle of period n $(n \geq v)$,

then we say that $\mathbf{t}$ *occurs in* $\mathbf{s}$ *at position* j if and only if

$$t_i = s_{i+j}$$

for every i, $(0 \leq i < v)$, where $i + j$ is computed modulo n.

If $\mathbf{s}$ and $\mathbf{s}'$ are two v-tuples, then we write $\mathbf{s} + \mathbf{s}'$ for the v-tuple obtained by element-wise adding together the two tuples. Similarly, if k is any integer, we write $k\mathbf{s}$ for the tuple obtained by element-wise multiplying the tuple $\mathbf{s}$ by k. Again, if we write $\mathbf{t} = \mathbf{s} \bmod k$, then $\mathbf{t}$ is the tuple obtained by reducing every element in $\mathbf{s}$ modulo k. An exactly analogous interpretation should be used for arithmetic operations on cycles.

Given a cycle $\mathbf{s} = (s_i)$, $(0 \leq i < n)$, and any integer k, we define $\mathbf{T}_k(\mathbf{s})$ to be the *cyclic shift* of $\mathbf{s}$ by k places. I.e. if we write $\mathbf{s}' = (s'_i) = \mathbf{T}_k(\mathbf{s})$ then

$$s'_{i+k} = s_i, \quad (0 \leq i < n)$$

where $i + k$ is calculated modulo n.

Suppose $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\mathbf{u}' = (u'_0, u'_1, \ldots, u'_{n'-1})$ are c-ary cycles of periods n and n' respectively. Then define the *concatenation* of $\mathbf{u}$ and $\mathbf{u}'$, written

$$\mathbf{u}||\mathbf{u}'$$

to be a c-ary cycle of period $n + n'$

$$\mathbf{s} = (s_0, s_1, \ldots, s_{n+n'-1}) = \mathbf{u}||\mathbf{u}',$$

where

$$s_i = \begin{cases} u_i & \text{if } 0 \leq i < n \\ u'_{i-n} & \text{if } n \leq i < n + n' \end{cases}$$

We also need some notation linking sets of c-ary cycles with matrices. Suppose that $A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v-1}\}$ is a set of c^v c-ary cycles of period n. Then let $\mathcal{X}^A$ be the $c^v \times n$ matrix with row i equal to $\mathbf{a}_i$, $(0 \leq$

$i \leq c^v - 1$). Conversely, suppose that $\mathcal{X}$ is a $c^v \times n$ matrix. Then let $A^{\mathcal{X}} = \{\mathbf{a}_0^{\mathcal{X}}, \mathbf{a}_1^{\mathcal{X}}, \ldots, \mathbf{a}_{c^v-1}^{\mathcal{X}}\}$ be the set of c-ary cycles (of length n) defined so that $\mathbf{a}_i^{\mathcal{X}}$ is equal to row i of $\mathcal{X}$ ($0 \leq i \leq c^v - 1$).

We use the following matrix notation. Suppose $\mathcal{X}$ and $\mathcal{Y}$ are matrices of dimensions $s \times t$ and $s \times u$ respectively. Then $\mathcal{Z} = (\mathcal{X}|\mathcal{Y})$ denotes the $s \times t + u$ matrix whose first t columns are the columns of $\mathcal{X}$ and whose last u columns are the columns of $\mathcal{Y}$. For any matrix $\mathcal{X}$, the transpose of $\mathcal{X}$ is denoted by $\mathcal{X}^T$.

Finally note that, throughout this paper, the notation (m, n) represents the *Greatest Common Divisor* of m and n (given that m, n are a pair of positive integers).

1.2 Fundamentals

We can now define the combinatorial objects which are the main focus of this paper.

Definition 1.1 *Suppose n, c and v are positive integers (where we also assume that $c \geq 2$). An (n, c, v)–Perfect Factor, or simply a (n, c, v)–PF, is then a set of c^v/n c-ary cycles of period n with the property that every c-ary v-tuple occurs in one of these cycles.*

Note that, because we insist that a Perfect Factor contains exactly c^v/n cycles, and because there are clearly c^v different c-ary v-tuples, each v-tuple will actually occur exactly once somewhere in the set of cycles. Also observe that a (c^v, c, v)–PF is simply a c-ary span v de Bruijn sequence.

Example 1.2 *The following three cycles form a $(3, 3, 2)$–PF.*

$$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 0 \end{pmatrix}.$$

The following necessary conditions for the existence of a Perfect Factor are trivial to establish.

Lemma 1.3 *Suppose A is a (n, c, v)–PF. Then*

1. *$n|c^v$, and*
2. *$v < n \leq c^v$.*

We now state our main conjecture regarding the existence of Perfect Factors.

Conjecture 1.4 *The necessary conditions specified in Lemma 1.3 are sufficient for the existence of a Perfect Factor.*

Etzion, [2], showed that Conjecture 1.4 is true in the binary case, i.e. $c = 2$. Paterson, [4], has recently shown that Conjecture 1.4 is true whenever $c = p^\alpha$ for p any prime and α a positive integer. In this paper, as an effort towards establishing this conjecture, we demonstrate some constructions for c-ary Perfect Factors for general c.

2 Perfect Multi-factors

Before giving our first method of construction for Perfect Factors, we define a related set of combinatorial objects which will be of some use in their construction.

Definition 2.1 *Suppose m, n, c and v are positive integers satisfying $m|c^v$ and $c \geq 2$. An (m, n, c, v)–Perfect Multi-factor, or simply a (m, n, c, v)–PMF, is a set of c^v/m c-ary cycles of period mn with the property that for every c-ary v-tuple $\mathbf{t}$ and for every integer j in the range $0 \leq j < n$, $\mathbf{t}$ occurs at a position $p \equiv j \pmod{n}$ in one of these cycles.*

Note that, because we insist that a PMF contains exactly c^v/m cycles (each of length mn and hence 'containing' mn v-tuples), and because there are clearly c^v different c-ary v-tuples, each v-tuple will actually occur exactly n times in the set of cycles, once in each of the possible position congruency classes (mod n).

Remark 2.2 *It should be clear that an $(m, 1, c, v)$–PMF is precisely equivalent to an (m, c, v)–PF.*

We next give a simple example of a PMF which is not a PF.

Example 2.3 *The following two cycles form a $(2, 3, 2, 2)$–PMF.*

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

The following necessary conditions for the existence of a Perfect Multi-factor are trivial to establish.

Lemma 2.4 *Suppose A is an (m, n, c, v)–PMF. Then*

(i) $m | c^v$, *and*

(ii) *(a)* $m = 1$ *and* $v \leq mn$, *or*

(b) $m > 1$ *and* $v < mn$.

This leads to our second existence conjecture.

Conjecture 2.5 *The necessary conditions specified in Lemma 2.4 for the existence of an (m, n, c, v)–PMF are sufficient.*

Remark 2.6 *By Remark 2.2 above, it should be clear that Conjecture 2.5 implies Conjecture 1.4.*

3 Constructing Perfect Multi-factors with $m = 1$

In this section we consider the construction of Perfect Multi-factors for the special case $m = 1$. Because of the importance of this special case we repeat some of the above discussion in a simpler form.

Definition 3.1 *Suppose n, c and v are positive integers (where we also assume that $c \geq 2$). A $(1, n, c, v)$–Perfect Multi-factor, or simply a $(1, n, c, v)$–PMF, is a set of c^v c-ary cycles of period n with the property that for every c-ary v-tuple $\mathbf{t}$ and for every integer j in the range $0 \leq j < n$, $\mathbf{t}$ occurs at position j in one of these cycles.*

Note that, because we insist that a Perfect Multi-factor with $m = 1$ contains exactly c^v cycles, and because there are clearly c^v different c-ary v-tuples, each v-tuple will actually occur exactly n times in the set of cycles, once in each of the possible positions.

Example 3.2 *The following four cycles form a $(1, 3, 2, 2)$–PMF.*

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

Example 3.3 *The following nine cycles form a $(1, 3, 3, 2)$–PMF.*

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 1 \\ 0 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 1 \\ 2 & 0 & 2 \end{pmatrix},$$

The following necessary condition for the existence of a Perfect Multi-factor in the case $m = 1$ is a trivial consequence of Lemma 2.4.

Lemma 3.4 *Suppose A is a $(1, n, c, v)$–PMF. Then*

$$v \leq n.$$

As we show below, this necessary condition is also sufficient for the existence of a PMF with $m = 1$. We first give an elementary construction for Perfect Multi-factors. In essence, it consists of taking as cycles every possible v-tuple.

Construction 3.5 *Suppose c and v are positive integers satisfying $c \geq 2$. Suppose also that $T = \{\mathbf{t}_i : 0 \leq i < c^v\}$ is the set of all c-ary v-tuples. Then let $B = \{\mathbf{s}_i : 0 \leq i < c^v\}$ be the set of c-ary cycles of period v with the property that $\mathbf{t}_i$ occurs in $\mathbf{s}_i$ at position 0 for every i, $(0 \leq i < c^v)$.*

Theorem 3.6 *Suppose B is a set of c^v cycles constructed using Construction 3.5. Then B is an $(1, v, c, v)$–PMF.*

Proof Consider any c-ary v-tuple $\mathbf{u} = (u_0, u_1, \ldots, u_{v-1})$, and any position j $(0 \leq j < v)$. Let $\mathbf{u}' = T_{-j}(\mathbf{u})$. Then $\mathbf{u}'$ is a c-ary v-tuple and hence must 'equal' one cycle in B, $\mathbf{s}_k$ say. If we let $\mathbf{s}_k = (a_0, a_1, \ldots, a_{v-1})$ then

$$a_i = u_{i-j}$$

for every i $(0 \leq i < v)$, where $i - j$ is calculated modulo v. Hence

$$a_{i+j} = u_i$$

for every i $(0 \leq i < v)$, where $i + j$ is calculated modulo v, i.e. $\mathbf{u}$ occurs at position j in $\mathbf{s}_k$, and the result follows. □

Example 3.7 *The following set of cycles B, constructed using Construction 3.5, is a $(1, 2, 3, 2)$–PMF.*

$$\begin{pmatrix} 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \end{pmatrix}.$$

We now give the main results of this section.

Lemma 3.8 *Suppose B is an $(1, v, c, v)$–PMF for some positive integers v, c (where $c \geq 2$). Let*

$$\mathbf{x}_0^T, \mathbf{x}_1^T, \ldots, \mathbf{x}_{v-1}^T$$

be the column vectors of $\mathcal{X}^B$. Suppose also that $t \geq 1$, and let $\mathcal{Y}$ be a c-ary matrix of dimensions $c^v \times t$ having column vectors $\mathbf{x}_{v+j}^T$, $(0 \leq j \leq t-1)$. Hence $\mathbf{x}_i$ is a c-ary vector of length c^v for every i, $(0 \leq i \leq v+t-1)$).

Then, if for every j and s, $(0 \leq j \leq v-1, 0 \leq s \leq v+t-1)$, there exist integers $e_{ij}^{(s)}$, $(0 \leq i \leq v-1)$, such that

$$\mathbf{x}_j = \sum_{i=0}^{v-1} e_{ij}^{(s)} \mathbf{x}_{s+i} \bmod c$$

where the subscript $s+i$ is computed modulo $v+t$, then $A^{(\mathcal{X}^B|\mathcal{Y})}$ is a $(1, v+t, c, v)$–PMF.

Proof Let

$$\mathbf{x}_i = (x_{i,0}, x_{i,1}, \ldots, x_{i,c^v-1})$$

for every i, $(0 \leq i \leq v+t-1)$.

Now choose any s, $(0 \leq s \leq v+t-1)$, and suppose that

$$(x_{s,p}, x_{s+1,p}, \ldots, x_{s+v-1,p}) = (x_{s,q}, x_{s+1,q}, \ldots, x_{s+v-1,q})$$

for some $p, q \in \{0, 1, \ldots, c^v - 1\}$, and where the subscripts $s+i$ are computed modulo $v+t$. We need to show that $p = q$, and hence that at any position s, no two of the c-ary v-tuples in $A^{(\mathcal{X}^B|\mathcal{Y})}$ are the same—the result will then follow from Definition 3.1.

By the assumption, if j satisfies $0 \leq j \leq v-1$, then there exist $e_{ij}^{(s)}$ such that

$$\mathbf{x}_j = \sum_{i=0}^{v-1} e_{ij}^{(s)} \mathbf{x}_{s+i}.$$

Hence

$$x_{j,p} = \sum_{i=0}^{v-1} e_{ij}^{(s)} x_{s+i,p} = \sum_{i=0}^{v-1} e_{ij}^{(s)} x_{s+i,q} = x_{j,q}.$$

Hence

$$(x_{0,p}, x_{1,p}, \ldots, x_{v-1,p}) = (x_{0,q}, x_{1,q}, \ldots, x_{v-1,q}).$$

But, since B is an $(1, v, c, v)$–PMF, we must have $p = q$, and the result follows. □

Lemma 3.9 *Suppose v, c, t are positive integers ($c \geq 2$). Further suppose that $\mathcal{X}$ is a c-ary matrix of dimensions $c^v \times v$ having column vectors*

$$\mathbf{x}_0^T, \mathbf{x}_1^T, \ldots, \mathbf{x}_{v-1}^T$$

whose first v rows are equal to I_v, and that $\mathcal{Y}$ is a c-ary matrix of dimensions $c^v \times t$ having column vectors

$$\mathbf{x}_v^T, \mathbf{x}_{v+1}^T, \ldots, \mathbf{x}_{v+t-1}^T$$

where

$$\mathcal{Y} = \mathcal{X}\mathcal{D} \bmod c \tag{1}$$

and $\mathcal{D} = (d_{ij})$ $(0 \leq i \leq v-1, 0 \leq j \leq t-1)$, is a c-ary matrix of dimensions $v \times t$.

Then, for every j and s, $(0 \leq j \leq v-1, 0 \leq s \leq v+t-1)$, there exist integers $e_{ij}^{(s)}$, $(0 \leq i \leq v-1)$, such that

$$\mathbf{x}_j = \sum_{i=0}^{v-1} e_{ij}^{(s)} \mathbf{x}_{s+i} \bmod c$$

where the subscript $s+i$ is computed modulo $v+t$, if and only if every $v \times v$ sub-matrix of $(\mathcal{I}_v|\mathcal{D}|\mathcal{I}_v)$ is invertible over the ring of $v \times v$ matrices modulo c (where $\mathcal{I}_v$ is the $v \times v$ identity matrix).

Proof If s satisfies $0 \leq s \leq v+t-1$, then let $\mathcal{X}_s$ be the $v \times v$ matrix consisting of columns $s, s+1, \ldots, s+v-1$ of the matrix $(\mathcal{X}|\mathcal{Y}|\mathcal{X})$, where the columns of this latter matrix are numbered from 0 up to $2v+t-1$ inclusive.

It is immediate to see that, for any s satisfying $0 \leq s \leq v+t-1$, there exists integers $e_{ij}^{(s)}$, $(0 \leq i \leq v-1)$, such that

$$\mathbf{x}_j = \sum_{i=0}^{v-1} e_{ij}^{(s)} \mathbf{x}_{s+i} \bmod c$$

where the subscript $s+i$ is computed modulo $v+t$, if and only if there exists a c-ary $v \times v$ matrix $\mathcal{E}_s = (e_{ij}^{(s)})$ such that

$$\mathcal{X} = \mathcal{X}_s \mathcal{E}_s \bmod c.$$

Now, if s satisfies $0 \leq s \leq v+t$, then let $\mathcal{F}_s$ be the $v \times v$ matrix consisting of columns $s, s+1, \ldots, s+v-1$ of $(\mathcal{I}_v|\mathcal{D}|\mathcal{I}_v)$, where the columns of this latter matrix are numbered from 0 up to $2v+t-1$ inclusive. Then it is straightforward to see that

$$\{\mathcal{F}_s : 0 \leq s \leq v+t\}$$

is the set of all $v \times v$ sub-matrices of $(\mathcal{I}_v|\mathcal{D}|\mathcal{I}_v)$.

It should be clear that, by equation (1),

$$\mathcal{X}(\mathcal{I}_v|\mathcal{D}|\mathcal{I}_v) = (\mathcal{X}|\mathcal{Y}|\mathcal{X}) \bmod c$$

and hence

$$\mathcal{X}\mathcal{F}_s = \mathcal{X}_s \bmod c \tag{2}$$

for every s satisfying $0 \leq s \leq v+t-1$.

Next observe that $\mathcal{F}_{v+t} = \mathcal{I}_v$ and hence is trivially invertible. We now show that, if s is any integer satisfying $0 \leq s \leq v+t-1$, then $\mathcal{F}_s$ is invertible if and only if there exists a c-ary $v \times v$ matrix $\mathcal{E}_s$ such that

$$\mathcal{X} = \mathcal{X}_s \mathcal{E}_s \bmod c,$$

and the desired result follows.

Choose s such that $0 \leq s \leq v+t-1$.

First suppose $\mathcal{F}_s$ is invertible, i.e. suppose that there exists a c-ary $v \times v$ matrix $\mathcal{G}_s$ such that

$$\mathcal{F}_s \mathcal{G}_s = \mathcal{I}_v \bmod c.$$

Hence, by equation (2),

$$\mathcal{X} = \mathcal{X}_s \mathcal{G}_s \bmod c$$

as required.

Second suppose that there exists a c-ary $v \times v$ matrix $\mathcal{E}_s$ such that

$$\mathcal{X} = \mathcal{X}_s \mathcal{E}_s \bmod c.$$

Then, by equation (2)

$$\mathcal{X} = \mathcal{X} \mathcal{F}_s \mathcal{E}_s \bmod c.$$

But, by assumption, the first v rows of X are equal to $\mathcal{I}_v$ and hence we have

$$\mathcal{I}_v = \mathcal{F}_s \mathcal{E}_s \bmod c$$

and hence $\mathcal{F}_s$ is invertible.

The result follows. □

Lemma 3.10 *Suppose $c \geq 2$, v and t are positive integers, and suppose $\mathcal{X}$ is a c-ary $v \times t$ matrix. Then every $v \times v$ sub-matrix of $(\mathcal{I}_v | \mathcal{X} | \mathcal{I}_v)$ is invertible in the ring of $v \times v$ matrices modulo c if and only if every $t \times t$ sub-matrix of $(\mathcal{I}_t | \mathcal{X}^T | \mathcal{I}_t)$ is invertible in the ring of $t \times t$ matrices modulo c.*

Proof We assume every $t \times t$ sub-matrix of $(\mathcal{I}_t | \mathcal{X}^T | \mathcal{I}_t)$ is invertible.

If s satisfies $0 \leq s \leq v + t$, let $\mathcal{C}_s$ be the $v \times v$ matrix consisting of columns $s, s+1, \ldots, s+v-1$ of the matrix $(\mathcal{I}_v | \mathcal{X} | \mathcal{I}_v)$, where the columns of this latter matrix are numbered from 0 up to $2v + t - 1$ inclusive. It is straightforward to see that

$$\{\mathcal{C}_s : 0 \leq s \leq v + t\}$$

is the set of all $v \times v$ sub-matrices of $(\mathcal{I}_v|\mathcal{X}|\mathcal{I}_v)$. We need to show that $\mathcal{A}_s$ is invertible for every s $(0 \leq s \leq v+t)$, and the result will follow.

Without loss of generality suppose that s satisfies $0 \leq s \leq v$. We need to consider two cases.

- $s \leq t$. By our assumption, the $t \times t$ matrix consisting of columns $s, s+1, \ldots, s+t-1$ of $(\mathcal{I}_t|\mathcal{X}^T|\mathcal{I}_t)$ is invertible. This matrix contains the last $t-s$ columns of $\mathcal{I}_t$ and the first s columns of $\mathcal{X}^T$. Hence the $s \times s$ matrix consisting of the first s rows and columns of $\mathcal{X}^T$ is invertible, and thus the $s \times s$ matrix consisting of the first s rows and columns of $\mathcal{X}$ is invertible. Since $\mathcal{A}_s$ is nothing more than the last $v-s$ columns of $\mathcal{I}_v$ and the first s columns of $\mathcal{X}$ it follows that $\mathcal{A}_s$ is invertible.

- $s > t$. Again by our assumption, the $t \times t$ matrix consisting of columns $s, s+1, \ldots, s+t-1$ of $(\mathcal{I}_t|\mathcal{X}^T|\mathcal{I}_t)$ is invertible. Since $t < s \leq v$, this consists of columns $s-t, s-t+1, \ldots, s-1$ of $\mathcal{X}^T$, and hence this $t \times t$ sub-matrix of $\mathcal{X}^T$ is invertible. This implies that the $t \times t$ matrix containing rows $s-t, s-t+1, \ldots, s-1$ of $\mathcal{X}$ is invertible. Now $\mathcal{A}_s$ is the concatenation of the last $v-s$ columns of $\mathcal{I}_v$, all t columns of $\mathcal{X}$ and the first $s-t$ columns of $\mathcal{I}_v$, and hence $\mathcal{A}_s$ is invertible.

The result follows by substituting v for t (and vice versa) in the above argument. □

Definition 3.11 *If the $v \times t$ matrix $\mathcal{X}$ has the property that every $v \times v$ sub-matrix of $(\mathcal{I}_v|\mathcal{X}|\mathcal{I}_v)$ is invertible in the ring of $v \times v$ matrices modulo c, we say that $\mathcal{X}$ has* Property X.

Lemma 3.12 *Suppose $c \geq 2$, v and t are positive integers. Then there exists a c-ary $v \times t$ matrix $\mathcal{D}$ with Property* X.

Proof We prove this by induction on $\max\{v,t\}$. If $v = t = 1$ then $D = (1)$ trivially has Property X. Now suppose a matrix with Property X exists for every v, t satisfying $\max\{v,t\} < L$ for some positive integer $L > 1$. We now show that a matrix with Property X exists if $L = \max\{v,t\}$.

First note that if $L = v = t$ then $\mathcal{D} = \mathcal{I}_L$ clearly has Property X.

Next suppose $L = t > v$. Let $t = cv + d$, where $c > 0$ and $0 \leq d < v$. There are two cases to consider.

- If $d = 0$ let $\mathcal{D}$ equal $\mathcal{I}_v$ concatenated with itself c times, i.e.

  $$\mathcal{D} = (\mathcal{I}_v|\mathcal{I}_v|\cdots|\mathcal{I}_v)$$

  and $\mathcal{D}$ has Property X.

- If $d > 0$ then, by the inductive hypothesis, there exists a c-ary $v \times d$ matrix $\mathcal{Y}$ such that every $v \times v$ sub-matrix of $(\mathcal{I}_v|\mathcal{Y}|\mathcal{I}_v)$ is invertible. Let $\mathcal{D}$ equal $\mathcal{I}_v$ concatenated with itself c times, concatenated with $\mathcal{Y}$, i.e.

  $$\mathcal{D} = (\mathcal{I}_v|\mathcal{I}_v|\cdots|\mathcal{I}_v|\mathcal{Y})$$

  and $\mathcal{D}$ has Property X.

Finally suppose $t < v = L$. By the above argument there exists an $t \times v$ matrix $\mathcal{E}$ with Property X. But, by Lemma 3.10 this means that the $v \times t$ matrix $\mathcal{D} = \mathcal{E}^T$ also has Property X and the result follows. □

We can now state the main result of this section, showing that the necessary conditions of Lemma 3.4 are sufficient for the existence of a Perfect Multi-factor in the special case $m = 1$.

Theorem 3.13 *Suppose n, c, v are positive integers ($c \geq 2$ and $n \geq v$). Then there exists a $(1, n, c, v)$–PMF.*

Proof First let $n = v + t$. If $t = 0$ (i.e. if $n = v$) then the theorem follows immediately from Theorem 3.6. Hence suppose that $t \geq 1$.

By Lemma 3.12 there exists a c-ary $v \times t$ matrix, $\mathcal{D}$ say, with Property X. By Theorem 3.6 there exists an $(1, v, c, v)$–PMF, B say. By appropriate re-ordering of the elements of B (if necessary), we can ensure that the first v rows of $\mathcal{X}^B$ are equal to I_v. Now let

$$\mathcal{Y} = \mathcal{X}^B.\mathcal{D} \bmod c,$$

and by Lemma 3.9 there exist integers $e_{ij}^{(s)}$, $(0 \leq i \leq v-1)$, such that

$$\mathbf{x}_j = \sum_{i=0}^{v-1} e_{ij}^{(s)} \mathbf{x}_{s+i} \bmod c$$

where the subscript $s + i$ is computed modulo $v + t$. Hence, by Lemma 3.8, $A^{(\mathcal{X}^B|\mathcal{Y})}$ is an $(1, v + t, c, v)$–PMF, as required. □

Remark 3.14 *It should be clear that the above proof is actually constructive, i.e. it provides a simple recipe for the construction of a PMF with any desired parameters (given $m = 1$).*

Example 3.15 *Consider the case $v = 3$, $t = 2$ and $c = 2$. Following the proof of Theorem 3.13, we first need a 2-ary 3×2 matrix $\mathcal{D}$ with property X. Using the proof of Lemma 3.12 we obtain:*

$$\mathcal{D} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Using Construction 3.5 we obtain the following set of 8 cycles constituting a $(1, 3, 2, 3)$–PMF, $\mathcal{B}$ say:

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

Hence

$$\mathcal{X}^B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

and

$$\mathcal{Y} = \mathcal{X}^B\mathcal{D} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} \bmod 2.$$

Thus

$$(\mathcal{X}^B|\mathcal{Y}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

and the following eight binary cycles form a $(1, 5, 2, 3)$*–PMF:*

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

4 Constructing Perfect Multi-factors for every m

We now demonstrate some constructions for Perfect Multi-factors for general m.

4.1 Some elementary constructions

We start by giving two elementary construction techniques.

Construction 4.1 *Suppose $A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v/n-1}\}$ is an (n, c, v)–PF, and let m be any positive integer satisfying $m|n$. Then define B to be the following set containing c^v/m cycles:*

$$B = \{\mathbf{T}_k(\mathbf{a}_i) \mid 0 \leq k < n/m,\ 0 \leq i < c^v/n\}.$$

Theorem 4.2 *Suppose B is a set of cycles constructed from A (an (n, c, v)–PF) using Construction 4.1. Then B is an $(m, n/m, c, v)$–PMF.*

Proof Consider any c-ary v-tuple $\mathbf{t} = (t_0, t_1, \ldots, t_{v-1})$, and any integer j $(0 \leq j < n/m)$. Now, since A is a Perfect Factor, $\mathbf{t}$ must occur in a cycle of A; without loss of generality suppose $\mathbf{t}$ occurs at position h in cycle $\mathbf{a}_k$. If we let $\mathbf{a}_k = (a_0, a_1, \ldots, a_{n-1})$, then, by definition,

$$t_i = a_{i+h}, \quad (0 \leq i < v)$$

where $i + h$ is calculated modulo n.

Now let $q = j - h \bmod (n/m)$ (i.e. $0 \leq q < n/m$) and also let $p = q + h$. Consider $\mathbf{T}_q(\mathbf{a}_k)$, which, by definition, is a member of B. By definition, if we let $\mathbf{T}_q(\mathbf{a}_k) = (a'_0, a'_1, \ldots, a'_{n-1})$, then

$$a'_{i+q} = a_i$$

for every i $(0 \leq i < n)$, where $i + q$ is calculated modulo n. Hence, since $q = p - h$,

$$a'_{i+p} = a_{i+h} = t_i$$

for every i $(0 \leq i < v)$, where $i + p$ and $i + h$ are calculated modulo n. Hence, by definition, $\mathbf{t}$ occurs at position p of $\mathbf{T}_q(\mathbf{a}_k)$. But

$$p = q + h \equiv (j - h) + h = j \pmod{n/m},$$

and the result follows. □

Example 4.3 *Suppose A is the following $(4, 2, 3)$–PF.*

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 1 \end{array} \right), \left(\begin{array}{cccc} 1 & 1 & 1 & 0 \end{array} \right).$$

Let $m = 2$. Then B, constructed using Construction 4.1, is a $(2, 2, 2, 3)$–PMF and is as follows.

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 1 \end{array} \right), \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \end{array} \right), \left(\begin{array}{cccc} 1 & 1 & 1 & 0 \end{array} \right), \left(\begin{array}{cccc} 0 & 1 & 1 & 1 \end{array} \right).$$

We next have:

Construction 4.4 *Suppose that*

$$A = \{\mathbf{u}_i : 0 \leq i < c^v/m\}$$

is an (m, n, c, v)–PMF and that β is a positive integer satisfying $(\beta, m) = 1$, i.e. β is co-prime to m. Then let

$$B = \{\mathbf{s}_i : 0 \leq i < c^v/m\}$$

be a set of c-ary cycles of period $m\beta n$ defined so that $\mathbf{s}_i$ is equal to $\mathbf{u}_i$ concatenated with itself β times.

Theorem 4.5 *Suppose B is constructed from an (m, n, c, v)–PMF A using Construction 4.4 (with some value of β co-prime to m). Then B is an $(m, \beta n, c, v)$–PMF.*

Proof Consider any c-ary v-tuple $\mathbf{t} = (t_0, t_1, \ldots, t_{v-1})$, and any integer j $(0 \leq j < \beta n)$. Suppose $j' = j \bmod n$.

Now, by definition of PMF, $\mathbf{t}$ occurs at some position $p \equiv j' \bmod n$ in one cycle, $\mathbf{u}_k$ say, of A. Hence, by definition, $\mathbf{t}$ will occur at every position in the set

$$P = \{p, p + mn, p + 2mn, \ldots, p + (\beta - 1)mn\}$$

in cycle $\mathbf{s}_k$ of B. We next observe that the elements of P are all distinct modulo βn. This follows since suppose

$$p + \mu mn \equiv p + \mu' mn \pmod{\beta n}$$

where $0 \leq \mu, \mu' < \beta$. Hence $\beta n | (\mu' - \mu)mn$, i.e. $\beta | (\mu' - \mu)m$. But we assumed that $(\beta, m) = 1$ and hence $\beta | (\mu' - \mu)$. Finally note that $|\mu' - \mu| < \beta$ and hence $\mu = \mu'$.

It is also straightforward to verify that the elements of P are all congruent to j modulo n. Hence, since $|P| = \beta$, it follows that exactly one element of P is congruent to j modulo βn, and the result follows. □

Example 4.6 *Let A be the $(2, 2, 2, 3)$–PMF of Example 4.3, i.e. A contains the four cycles:*

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

Then B, derived using Construction 4.4 with $\beta = 3$, is a $(2, 6, 2, 3)$–PMF, and is as follows:

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

4.2 The main result

We now present a method for constructing a Perfect Multi-factor with $m > 1$ from a Perfect Multi-factor with $m = 1$. This construction method can be divided into two main parts:

- Partitioning the cycles of the perfect multi-factor with $m = 1$ into (equally-sized) subsets, and
- Joining together the cycles within each subset of the partition to form the cycles of a new Perfect Multi-factor.

4.2.1 Notation and definitions

We now define some connectedness relationships between sets of cycles. First we have:

Definition 4.7 *Suppose that* $X = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}\}$ *is some set of c-ary cycles with the property that each cycle* $\mathbf{a}_i$ *has length a positive integer multiple of* n*, (*$r_i n$ *say), for some* $n \geq v \geq 1$ *(where* $c \geq 2$*). In addition let*

$$\mathbf{a}_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,r_i n-1})$$

for every i*,* $(0 \leq i < s)$*. Then, for any* i, j*,* $(i, j \in \{0, 1, \ldots, s-1\})$*, say that* $\mathbf{a}_i$ *and* $\mathbf{a}_j$ *are* (n, v)*–adjacent, or simply write*

$$\mathbf{a}_i \overset{n,v}{\sim} \mathbf{a}_j$$

if and only if there exists some t *and* α*,* $(0 \leq t < n, 0 \leq \alpha < r_j)$*, such that*

$$(a_{i,t}, a_{i,t+1,}, \ldots, a_{i,t+v-2}) = (a_{j,t-\alpha n}, a_{j,t-\alpha n+1,}, \ldots, a_{j,t-\alpha n+v-2}),$$

i.e. if and only if $\mathbf{a}_i$ *and* $\mathbf{a}_j$ *agree in some consecutive* $v-1$ *positions, given* $\mathbf{a}_j$ *is cyclically shifted by some multiple of* n *positions.*

This then leads naturally to the following.

Definition 4.8 *Suppose that* $X = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_s - 1\}$ *is some set of c-ary cycles with lengths a multiple of* $n \geq v \geq 1$ *(where* $c \geq 2$*). Then, for any* i, j*,*

$(i, j \in \{0, 1, \ldots, s-1\})$, *say that* $\mathbf{a}_i$ *and* $\mathbf{a}_j$ *are* (n, v)*–connected, or simply write*

$$\mathbf{a}_i \overset{n,v}{\approx} \mathbf{a}_j$$

if and only if there exist some $\mathbf{a}_{i_0}, \mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_z} \in X$, $(z \geq 0))$, *such that*

(i) $i_0 = i$,

(ii) $i_z = j$, *and*

(iii) $\mathbf{a}_{i_k} \overset{n,v}{\sim} \mathbf{a}_{i_{k+1}}$ *for every* k, $(0 \leq k < z)$.

This then enables us to state the following.

Definition 4.9 *Suppose that* $X = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_s - 1\}$ *is some set of c-ary cycles with lengths a multiple of* $n \geq v \geq 1$ *(where* $c \geq 2$*). The* X *is said to be* (n, v)–connected *if and only if* $\mathbf{a}_i \overset{n,v}{\approx} \mathbf{a}_j$ *for every pair* $\mathbf{a}_i, \mathbf{a}_j \in X$.

4.2.2 Preliminaries

Suppose $c \geq 2$, $n \geq 1$ and $v \geq 1$.

First suppose that $A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v-1}\}$ is an $(1, n, c, v)$–PMF. Suppose moreover that

$$\mathbf{a}_i = (a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})$$

for every i, $(0 \leq i < c^v)$.

We next create a set of v different partitions of A into equally sized subsets by considering the $(v-1)$-tuples occurring at certain positions within the cycles of A. More formally, suppose j satisfies

$$0 \leq j < v,$$

and partition the cycles $\{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v-1}\}$ into c^{v-1} subsets

$$B_0^{(j)}, B_1^{(j)}, \ldots, B_{c^{v-1}-1}^{(j)}$$

in such a way that if $\mathbf{a}_i \in B_s^{(j)}$ and $\mathbf{a}_{i'} \in B_{s'}^{(j)}$ then

$$(a_{i,j}, a_{i,j+1}, \ldots, a_{i,j+v-2}) = (a_{i',j}, a_{i',j+1}, \ldots, a_{i',j+v-2})$$

if and only if $s = s'$. Since A is a Perfect Multi-factor, it is immediate to see that

$$|B_i^{(j)}| = c$$

for every i, j $(0 \leq i < c^{v-1}, 0 \leq j < v)$.

Next suppose $m|c^v$, and let $m_0, m_1, \ldots, m_{v-1}$ be defined so that

(i) $m_i|c$ for every i $(0 \leq i < v)$, and

(ii) $\prod_{i=0}^{v-1} m_i = m$.

In addition, if $1 \leq i < v$, let $r_i = \prod_{j=0}^{i-1} m_j$, and put $r_0 = 1$. Correspondingly, if $0 \leq i < v$, let $q_i = c^v/r_i$. Note that we immediately have $r_v = m$ and $q_v = c^v/m$.

Finally, for every i $(0 \leq i < v)$, let

$$E_0^{(i)}, E_1^{(i)}, \ldots, E_{c^v/m_i-1}^{(i)}$$

be an arbitrary sub-partition of

$$B_0^{(i)}, B_1^{(i)}, \ldots, B_{c^{v-1}-1}^{(i)}$$

into $c/m_i(c^{v-1}) = c^v/m_i$ subsets, each of size m_i. Hence, for every j, $(0 \leq j < c^v/m_i)$, there exists a k, $(0 \leq k < c^{v-1})$, such that

$$E_j^{(i)} \subseteq B_k^{(i)}.$$

We can now proceed with the description of an algorithm which uses an $(1, n, c, v)$–PMF to construct an (m, n, c, v)–PMF. We use the notation and definitions given above throughout the discussion of this derivation method.

4.2.3 Partitioning a Perfect Multi-factor

We first describe an (iterative) algorithm for partitioning the cycles of A into c^v/m subsets with m cycles in each. The algorithm is iterated a total of v times, with i (the iterative index) ranging from 0 up to $v-1$, and at each stage a partition $\mathcal{A}_i$ of the cycles of A is transformed into a partition $\mathcal{A}_{i+1}$, where each member of $\mathcal{A}_{i+1}$ is obtained by taking a union of members of $\mathcal{A}_i$.

We describe below a single step of this algorithm, i.e. how the partition $\mathcal{A}_{i+1}$ is derived from $\mathcal{A}_i$. We first need the following.

Definition 4.10 *If $0 \leq i < v$ and $\mathcal{A}_i = \{A_{i,0}, A_{i,1}, \ldots, A_{i,q_i-1}\}$ is a partition of the cycles of A, then it is said to be a (i, r_i, v)–*Partition *if and only if for every s, $(0 \leq s < q_i)$:*

(i) $A_{i,s}$ is (n, v)–connected,

(ii) $|A_{i,s}| = r_i$, and

(iii) If $\mathbf{a}_t, \mathbf{a}_{t'} \in A_{i,s}$ then

$$(a_{t,i-1}, a_{t,i}, \ldots, a_{t,v-2}) = (a_{t',i-1}, a_{t',i}, \ldots, a_{t',v-2}).$$

I.e. all cycles in $A_{i,s}$ agree in positions $\{i-1, i, \ldots, v-2\}$.

Algorithm 4.11 *Suppose i satisfies $0 \leq i < v$ and suppose also that*

$$\mathcal{A}_i = \{A_{i,0}, A_{i,1}, \ldots, A_{i,q_i-1}\}$$

is an (i, r_i, v)–Partition of the cycles of A. Then

let $\mathcal{Z}_{i,0} = \emptyset$;
for $j = 0$ to $q_{i+1} - 1$ do

choose some element, A_{i,f_j} say, from $\mathcal{A}_i - \mathcal{Z}_{i,j}$ (where $0 \leq f_j < q_i$);

choose some cycle, $\mathbf{a}_{g_j} \in A_{i,f_j}$, and suppose $\mathbf{a}_{g_j} \in E^{(i)}_{h_j}$;

let

$$A_{i+1,j} = \bigcup_s^* A_{i,s}$$

where $\bigcup_s^*$ denotes the union over all s, $(0 \leq s < q_i)$, such that

$$A_{i,s} \cap E^{(i)}_{h_j} \neq \emptyset; \tag{3}$$

let

$$\mathcal{Z}_{i,j+1} = \mathcal{Z}_{i,j} \cup \{A_{i,s} : 0 \leq s < q_i, A_{i,s} \cap E^{(i)}_{h_j} \neq \emptyset\};$$

Lemma 4.12 *Suppose $\mathcal{A}_{i+1}$ has been obtained from an (i, r_i, v)–Partition $\mathcal{A}_i$ using Algorithm 4.11 (where $0 \leq i < v$). Then $\mathcal{A}_{i+1}$ is a $(i+1, r_{i+1}, v)$–Partition of the cycles of A.*

Proof We start by observing that, by definition, the subsets $A_{i+1,j}$, $(0 \leq j < q_{i+1})$, are disjoint.

We next claim that

$$|A_{i,s} \cap E^{(i)}_t| \leq 1$$

for every s, t, $(0 \leq s < q_i, 0 \leq t < c^v/m_i)$. To establish this, suppose $\mathbf{a}_x, \mathbf{a}_y \in A_{i,s} \cap E^{(i)}_t$ for some s, t. Then $\mathbf{a}_x, \mathbf{a}_y \in A_{i,s}$, and hence $\mathbf{a}_x$ and $\mathbf{a}_y$ agree in positions $\{i-1, i, \ldots, v-2\}$. But we also have $\mathbf{a}_x, \mathbf{a}_y \in E^{(i)}_t \subseteq B^{(i)}_k$ for some k, $(0 \leq k < c^{v-1})$, and hence $\mathbf{a}_x$ and $\mathbf{a}_y$ agree in positions $\{i, i+1, \ldots, i+v-2\}$. Hence, since $0 \leq i < v$, $\mathbf{a}_x$ and $\mathbf{a}_y$ agree in positions $\{i-1, i, \ldots, i+v-2\}$, and so, since A is an $(1, n, c, v)$–PMF, we must have $x = y$, and the desired result follows.

Next observe that, by Algorithm 4.11

$$A_{i+1,j} = \bigcup_s^* A_{i,s}$$

where $\bigcup_s^*$ denotes the union over all s, $(0 \leq s < q_i)$, satisfying (3). Now, since

$$|A_{i,s} \cap E_{h_j}^{(i)}| \leq 1$$

for every s, $(0 \leq s < q_i)$, there must be precisely $|E_{h_j}^{(i)}|$ terms in the union defining $A_{i+1,j}$, and hence

$$|A_{i+1,j}| = |E_{h_j}^{(i)}|.|A_{i,s}| = m_i r_i = r_{i+1}$$

as required for Definition 4.10(ii).

In addition, since we have already observed that the subsets $A_{i+1,j}$, $(0 \leq j < q_{i+1})$, are disjoint, it immediately follows that $\mathcal{A}_{i+1}$ is a partition of the cycles of A (since $q_{i+1}r_{i+1} = c^v$).

We next consider any two cycles in $A_{i+1,j}$ (for some j satisfying $0 \leq j < q_{i+1}$). We need to show that they agree in positions $\{i, i+1, \ldots, v-2\}$ in order to satisfy Definition 4.10(iii). As before, by definition,

$$A_{i+1,j} = \bigcup_s^* A_{i,s}$$

where $\bigcup_s^*$ denotes the union over all s, $(0 \leq s < q_i)$, satisfying (3). Now the elements of $E_{h_j}^{(i)}$ all agree in positions $\{i, i+1, \ldots, i+v-2\}$ (since $E_{h_j}^{(i)} \subseteq B_k^{(i)}$ for some k, $(0 \leq k < c^{v-1})$). Moreover, by the assumption that $\mathcal{A}_i$ is an (i, r_i, v)–Partition, the elements of $A_{i,s}$ all agree in positions $\{i-1, i, \ldots, v-2\}$ for any s, $(0 \leq s < q_i)$. Hence the elements of $A_{i+1,j}$ all agree in positions

$$\{i, i+1, \ldots, i+v-2\} \cap \{i-1, i, \ldots, v-2\} = \{i, i+1, \ldots, v-2\}$$

as required.

It remains for us to show that $A_{i+1,s}$ is (n, v)–connected (and hence satisfies Definition 4.10(i)). As before, by definition,

$$A_{i+1,j} = \bigcup_s^* A_{i,s}$$

where $\bigcup_s^*$ denotes the union over all s, $(0 \leq s < q_i)$, satisfying (3). Let $\mathbf{a}_{x_s} \in A_{i,s} \cap E_{h_j}^{(i)}$ for every s satisfying (3). Now since $\mathbf{a}_{x_s} \in E_{h_j}^{(i)}$ for every s satisfying (3) (and since $E_{h_j}^{(i)} \subseteq B_k^{(i)}$ for some k $(0 \leq k < c^{v-1})$) we must have

$$\mathbf{a}_{x_s} \overset{n,v}{\sim} \mathbf{a}_{x_{s'}}$$

for every pair s, s' satisfying (3). Since, by assumption, $A_{i,s}$ is (n, v)–connected for every s, it follows immediately that $A_{i+1,j}$ is (n, v)–connected. The Lemma now follows. □

4.2.4 Merging the cycles

We can now state our main result.

Theorem 4.13 *Suppose n, c, v, t are positive integers ($c \geq 2$, $n \geq v$ and $t|c^v$). Suppose also that $A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v-1}\}$ is an $(1, n, c, v)$–PMF. Let $\mathcal{X} = \{X_0, X_1, \ldots, X_{c^v/t-1}\}$ be a partition of the cycles of A into c^v/t subsets of t cycles each, and suppose finally that X_i is (n, v)–connected for all i, $(0 \leq i < c^v/t)$. Then there exists a (t, n, c, v)–PMF.*

Before giving a proof of this result we need the following definition.

Definition 4.14 *Suppose*

$$\mathbf{a}_0 = (a_{0,0}, a_{0,1}, \ldots, a_{0,r_0 n-1}) \quad \textit{and} \quad \mathbf{a}_1 = (a_{1,0}, a_{1,1}, \ldots, a_{1,r_1 n-1})$$

are c-ary cycles of lengths $r_0 n$ and $r_1 n$ respectively (where $c \geq 2$, n, r_0 and r_1 are positive integers). Suppose, moreover, that $\mathbf{a}_0$ and $\mathbf{a}_1$ are (n, v)–adjacent. Hence there exist integers p and α, $(0 \leq p < n, 0 \leq \alpha < r_1)$, such that

$$(a_{0,p}, a_{0,p+1}, \ldots, a_{0,p+v-2}) = (a_{1,p-\alpha n}, a_{1,p-\alpha n+1}, \ldots, a_{1,p-\alpha n+v-2}).$$

Then define $(\mathbf{a}_0|\mathbf{a}_1)_p^{\alpha n}$ *to be the following c-ary cycle of length* $(r_0+r_1)n$*. Let* $(\mathbf{a}_0|\mathbf{a}_1)_p^{\alpha n} = (c_0, c_1, \ldots, c_{(r_0+r_1)n-1})$ *where, if* $p - \alpha n \geq 0$*:*

$$c_i = \begin{cases} a_{0,i} & \text{if } 0 \leq i < p \\ a_{1,i-\alpha n} & \text{if } p \leq i < (r_1+\alpha)n \\ a_{1,i-(r_1+\alpha)n} & \text{if } (r_1+\alpha)n \leq i < p + r_1 n \\ a_{0,i-r_1 n} & \text{if } p + r_1 n \leq i < (r_0+r_1)n \end{cases}$$

and if $p - \alpha n < 0$*:*

$$c_i = \begin{cases} a_{0,i} & \text{if } 0 \leq i < p \\ a_{1,i+(r_1-\alpha)n} & \text{if } p \leq i < \alpha n \\ a_{1,i-\alpha n} & \text{if } \alpha n \leq i < p + r_1 n \\ a_{0,i-r_1 n} & \text{if } p + r_1 n \leq i < (r_0+r_1)n \end{cases}$$

Proof of Theorem 4.13 For each $X_i \in \mathcal{X}$ we can construct a cycle $\mathbf{b}_i$ of length nt by concatenating the cycles in X_i. More formally, given i, $(0 \leq i < c^v/t)$, perform the following algorithm:

choose $\mathbf{a}_{i,0} \in X_i$;
let $Y_{i,0} = \{\mathbf{a}_{i,0}\}$;
let $\mathbf{b}_{i,0} = \mathbf{a}_{i,0}$;
for $j = 0$ to $t-1$ do

> choose $\mathbf{a}_{i,j+1} \in X_i - Y_{i,j}$ such that $\mathbf{a}_{i,j+1} \overset{n,v}{\sim} \mathbf{b}_{i,j}$;
> let $\mathbf{b}_{i,j+1} = (\mathbf{a}_{i,j+1}|\mathbf{b}_{i,j})_p^{\alpha n}$ for some p, α (which exist since $\mathbf{a}_{i,j+1} \overset{n,v}{\sim} \mathbf{b}_{i,j}$);
> let $Y_{i,j+1} = Y_{i,j} \cup \{\mathbf{a}_{i,j+1}\}$;

The end result of the above algorithm will be a c-ary cycle, $\mathbf{b}_i = \mathbf{b}_{i,t}$, of length nt.

To prove that this algorithm runs to completion we need to show that, for every j, there exists an $\mathbf{a}_{i,j+1} \in X_i - Y_{i,j}$ such that $\mathbf{a}_{i,j+1} \overset{n,v}{\sim} \mathbf{b}_{i,j}$. To

establish this we consider the set

$$Z_j = X_i - Y_{i,j} \cup \{\mathbf{b}_{i,j}\}$$

for every j, $(0 \leq j < t)$, and claim that Z_j is (n, v)–connected for every j. We show this by induction.

First note that

$$Z_0 = X_i - Y_{i,0} \cup \{\mathbf{b}_{i,0}\} = X_0$$

which is (n, v)–connected by assumption. Secondly suppose that Z_j is (n, v)–connected for some j satisfying $0 \leq j < t$. By definition

$$Z_{j+1} = Z_j - \{\mathbf{a}_{i,j+1}, \mathbf{b}_{i,j}\} \cup \{\mathbf{b}_{i,j+1}\}$$

where

$$\mathbf{b}_{i,j+1} = (\mathbf{a}_{i,j+1}|\mathbf{b}_{i,j})_p^{\alpha n}$$

for some p, α. Given any cycle $\mathbf{y}$, it should be clear that

- if $\mathbf{y} \overset{n,v}{\sim} \mathbf{a}_{i,j+1}$ then $\mathbf{y} \overset{n,v}{\sim} (\mathbf{a}_{i,j+1}|\mathbf{b}_{i,j})_p^{\alpha n}$, and
- if $\mathbf{y} \overset{n,v}{\sim} \mathbf{b}_{i,j}$ then $\mathbf{y} \overset{n,v}{\sim} (\mathbf{a}_{i,j+1}|\mathbf{b}_{i,j})_p^{\alpha n}$,

and hence Z_{j+1} is (n, v)–connected, and thus the induction is complete.

Now, since we have established that $X_i - Y_{i,j} \cup \{\mathbf{b}_{i,j}\}$ is (n, v)–connected for every j, it should be clear that, for every j there exists $\mathbf{a}_{i,j+1} \in X_i - Y_{i,j}$ such that $\mathbf{a}_{i,j+1} \overset{n,v}{\sim} \mathbf{b}_{i,j}$, as required.

We have thus established that the above algorithm, when supplied with a partition of the specified type, will produce a set $B = \{\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{c^v/t-1}\}$ of c-ary cycles of length t. We now claim that this set constitutes the desired (t, n, c, v)–PMF.

Choose any c-ary v-tuple, $\mathbf{t}$ say, and any integer j, $(0 \leq j < n)$. We need to find a cycle $\mathbf{b}_i$ such that $\mathbf{t}$ occurs in $\mathbf{b}_i$ at a position $q \equiv j \pmod{n}$. Now,

since A is an $(1, n, c, v)$–PMF, $\mathbf{t}$ occurs in a cycle in A, $\mathbf{a}_i$ say, at position j. Moreover, since $\mathcal{X}$ is a partition of the cycles of A, $\mathbf{a}_i$ occurs in a (unique) element of $\mathcal{X}$, X_s say. Hence, $\mathbf{a}_i$ was used in the construction of $\mathbf{b}_s$.

Now, given any pair of tuples $\mathbf{x}, \mathbf{y}$ of lengths a multiple of n and with the property that $\mathbf{x} \overset{n,v}{\sim} \mathbf{y}$, it is certainly that case that if $\mathbf{t}$ occurs in position q in $\mathbf{x}$, then

- $\mathbf{t}$ occurs at a position $q' \equiv q \pmod{n}$ in $(\mathbf{x}|\mathbf{y})_p^{\alpha n}$, and
- $\mathbf{t}$ occurs at a position $q'' \equiv q \pmod{n}$ in $(\mathbf{y}|\mathbf{x})_p^{\alpha' n}$.

Hence $\mathbf{t}$ occurs at a position $q \equiv j \pmod{n}$ in $\mathbf{b}_s$.

The proof is now complete. □

4.2.5 Examples

Remark 4.15 *It should be clear that Example 2.3 (a $(2, 3, 2, 2)$–PMF) can be derived using the above construction from the $(1, 3, 2, 2)$–PMF of Example 3.2 (with $m = 2$).*

Example 4.16 *As a further example of the above technique we let $c = 2$, $v = 3$ and $m = n = 4$ and show how a $(4, 4, 2, 3)$–PMF can be constructed from a $(1, 4, 2, 3)$–PMF.*

Let $m_0 = 2$, $m_1 = 1$ and $m_2 = 2$, and hence $r_0 = 1$, $r_1 = r_2 = 2$, $q_0 = 8$ and $q_1 = q_2 = 4$. Let A be the following $(4, 2, 3)$–PMF:

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

Then the partitions $(B_i^{(j)})$, $(0 \le i < 3, 0 \le j < 2)$ are as follows:

$$B_0^{(0)} = \{\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}\},$$

$$B_1^{(0)} = \{\begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}\},$$

$$B_2^{(0)} = \{\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}\},$$

$$B_3^{(0)} = \{\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}\},$$

$$B_0^{(1)} = \{\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}\},$$

$$B_1^{(1)} = \{\begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}\},$$

$$B_2^{(1)} = \{\begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}\},$$

$$B_3^{(1)} = \{\begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}\},$$

$$B_0^{(2)} = \{\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}\},$$

$$B_1^{(2)} = \{\begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}\},$$

$$B_2^{(2)} = \{\begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}\},$$

$$B_3^{(2)} = \{\begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}\}.$$

Now since $m_0 = m_2 = 2$ *and* $m_1 = 1$*, we have*

$$(E_i^{(0)}) = (B_i^{(0)}),$$

$$(E_i^{(2)}) = (B_i^{(2)}),$$

and

$$E_0^{(1)} = \{\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}\}, \quad E_1^{(1)} = \{\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}\},$$
$$E_2^{(1)} = \{\begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}\}, \quad E_3^{(1)} = \{\begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}\},$$
$$E_4^{(1)} = \{\begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}\}, \quad E_5^{(1)} = \{\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}\},$$
$$E_6^{(1)} = \{\begin{pmatrix} 0 & 1 & 1 & 0 \end{pmatrix}\}, \quad E_7^{(1)} = \{\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}\}.$$

Following Algorithm 4.11 we have

$$\mathcal{A}_1 = \mathcal{A}_2 = (E_i^{(0)}),$$

and

$$\mathcal{A}_3 = \begin{array}{l} \{\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}\}, \\ \{\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}\}. \end{array}$$

Merging the elements within the two classes of $\mathcal{A}_3$ *we obtain*

$$B = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}, \right\}.$$

4.2.6 Implications

The following summarises what types of PMF can be constructed using the technique described above.

Corollary 4.17 *Suppose* n, c, v *are positive integers* ($c \geq 2$ *and* $n \geq v$). *Then there exists an* (m, n, c, v)*–PMF for every positive integer* m *satisfying* $m|c^v$.

Proof By Theorem 3.13 there exists an $(1, n, c, v)$–PMF, $A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v-1}\}$ say. Let $\mathcal{A}_0 = \{A_{0,0}, A_{0,1}, \ldots, A_{0,c^v-1}\}$ be the 'trivial' partition of the cycles of A defined by

$$A_{0,i} = \{\mathbf{a}_i\}$$

for every i, $(0 \leq i < c^v)$.

First observe that $\mathcal{A}_0$ is a $(0, r_0, v)$–Partition of the cycles of A. To show this we need only check that, for every s, $(0 \leq s < c^v)$:

(i) $A_{0,s}$ is (n, v)–connected (this is trivially true since $|A_{0,s}| = 1$),

(ii) $|A_{0,s}| = 1$ (true by definition), and

(iii) if $\mathbf{a}_t, \mathbf{a}_{t'} \in A_{0,s}$ then $\mathbf{a}_t$ and $\mathbf{a}_{t'}$ must agree in positions $\{-1, 0, \ldots, v-2\}$, i.e. in positions $\{0, 1, \ldots, v-2\}$ and in position $n-1$ (this again holds trivially since $|A_{0,s}| = 1$).

Hence if we apply Algorithm 4.11 v times to $\mathcal{A}_0$ to obtain the partition

$$\mathcal{A}_v = \{A_{v,0}, A_{v,1}, \ldots, A_{v,q_v-1}\},$$

then, by Lemma 4.12, $\mathcal{A}_v$ is an (v, r_v, v)–Partition of the cycles of A. That is $\mathcal{A}_v$ is a partition of the cycles of A into $q_v = c^v/m$ subsets of $r_v = m$ cycles each. Moreover, each $A_{v,i}$ is (n, v)–connected. The result now follows immediately on application of Theorem 4.13. □

Remark 4.18 *Hence Conjecture 2.5 is true for all sufficiently large values of n.*

5 Constructing Perfect Factors from Perfect Multi-factors

We now show how Perfect Multi-factors may be used in conjunction with Perfect Factors to construct other Perfect Factors. We have the following.

Construction 5.1 *Suppose that*

$$A = \{\mathbf{u}_i : 0 \leq i < c^v/n\}$$

is an (n, c, v)–PF. Suppose also that

$$A' = \{\mathbf{v}_i : 0 \leq i < d^v/m\}$$

is an (m, n, d, v)–PMF.

For each cycle $\mathbf{u}_i$ of A, concatenate it with itself m times to obtain the cycle $\mathbf{w}_i$ having period mn. Now let

$$B = \{\mathbf{s}_{ij} : 0 \leq i < c^v/n,\ 0 \leq j < d^v/m\}$$

be the set of cycles of period mn defined by

$$\mathbf{s}_{ij} = \mathbf{w}_i + c\mathbf{v}_j.$$

Theorem 5.2 *Suppose B is constructed from an (n, c, v)–PF and an (m, n, d, v)–PMF using Construction 5.1. Then B is an (mn, cd, v)–PF.*

Proof Consider any (cd)-ary v-tuple, $\mathbf{x}$ say. Then let

$$\mathbf{y} = \mathbf{x} \bmod c.$$

Then $\mathbf{y}$ is a c-ary v-tuple and hence occurs in some cycle of A, say at position j in cycle $\mathbf{u}_k$. Now let

$$\mathbf{z} = (\mathbf{x} - \mathbf{y})/c;$$

this is simple to do in integers since every element of $\mathbf{x} - \mathbf{y}$ must be a multiple of c. It should also be clear that $\mathbf{z}$ is a d-ary v-tuple, and hence occurs at position $d \equiv j \pmod{n}$ in some cycle in A', say $\mathbf{v}_{k'}$. It is now straightforward to check that $\mathbf{x}$ appears at position d in the cycle $\mathbf{s}_{kk'}$ of B.

Hence every (cd)-ary v-tuple occurs in at least one cycle, and the result then follows on observing that there are precisely $(cd)^v/mn$ cycles in B, each of length mn. □

Example 5.3 *Let A be the $(3, 3, 2)$–PF of Example 1.2, i.e. A contains the cycles*

$$u_0 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix},\ u_1 = \begin{pmatrix} 1 & 1 & 2 \end{pmatrix},\ u_2 = \begin{pmatrix} 2 & 2 & 0 \end{pmatrix}.$$

Hence, given $m = 2$, the concatenated cycles w_0, w_1, w_2 are as follows:

$$w_0 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, w_1 = \begin{pmatrix} 1 & 1 & 2 & 1 & 1 & 2 \end{pmatrix}, w_2 = \begin{pmatrix} 2 & 2 & 0 & 2 & 2 & 0 \end{pmatrix}.$$

Let A' be the $(2, 3, 2, 2)$–PMF of Example 2.3, i.e. A' contains the cycles

$$v_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix},\ v_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Then B, derived using Construction 5.1 is a $(6, 6, 2)$–PF, and is as follows:

$$\begin{aligned}
s_{00} &= \begin{pmatrix} 0 & 0 & 1 & 0 & 3 & 4 \end{pmatrix}, \quad s_{01} = \begin{pmatrix} 3 & 0 & 4 & 3 & 3 & 1 \end{pmatrix}, \\
s_{10} &= \begin{pmatrix} 1 & 1 & 2 & 1 & 4 & 5 \end{pmatrix}, \quad s_{11} = \begin{pmatrix} 4 & 1 & 5 & 4 & 4 & 2 \end{pmatrix}, \\
s_{20} &= \begin{pmatrix} 2 & 2 & 0 & 2 & 5 & 3 \end{pmatrix}, \quad s_{21} = \begin{pmatrix} 5 & 2 & 3 & 5 & 5 & 0 \end{pmatrix}.
\end{aligned}$$

Remark 5.4 *Construction 5.1 of [3] can be regarded as a special case of Construction 5.1 above.*

6 Combining two Perfect Factors

We now present a method for combining two Perfect Factors to produce a new Perfect Factor. As we show in the proof of Theorem 6.2 below, this construction can be regarded as the result of combining Constructions 4.1, 4.4 and 5.1.

Construction 6.1 *Suppose that*

$$A = \{\mathbf{u}_i : 0 \leq i < c^v/n\}$$

is an (n, c, v)*–PF. Suppose also that*

$$A' = \{\mathbf{v}_j : 0 \leq j < d^v/n'\}$$

is an (n', d, v)*–PF.*

For each cycle $\mathbf{u}_i$ *of* A*, concatenate it with itself* $n'/(n, n')$ *times, to obtain the cycle* $\mathbf{w}_i$ *having period* $nn'/(n, n')$*,* $(0 \leq i < c^v/n)$*. In a similar way, for each cycle* $\mathbf{v}_j$ *of* A'*, concatenate it with itself* $n/(n, n')$ *times, to obtain the cycle* $\mathbf{x}_j$ *having period* $nn'/(n, n')$*,* $(0 \leq j < d^v/n')$*. Finally let*

$$B = \{\mathbf{s}_{ijh} : 0 \leq i < c^v/n,\ 0 \leq j < d^v/n',\ 0 \leq h < (n, n')\}$$

be the set of cycles of period $nn'/(n, n')$ *defined by*

$$\mathbf{s}_{ijh} = \mathbf{w}_i + c\mathbf{T}_h(\mathbf{x}_j).$$

Theorem 6.2 *Suppose* B *is constructed from* A *(an* (n, c, v)*–PF) and* A' *(an* (n', d, v)*–PF) using Construction 6.1. Then* B *is an* $(nn'/(n, n'), cd, v)$*–PF.*

Proof As in the definition of the construction, suppose

$$A' = \{\mathbf{v}_j : 0 \le j < d^v/n'\}.$$

We first apply Construction 4.1 to A', setting $m = n'/(n, n')$. The resulting set of cycles, which we call C, is defined by

$$C = \{\mathbf{y}_{jh} = \mathbf{T}_h(\mathbf{v}_j) \mid 0 \le h < (n, n'),\ \ 0 \le j < d^v/n'\}.$$

By Theorem 4.2, C is an $(n'/(n, n'), (n, n'), d, v)$–PMF.

Next apply Construction 4.4 to C, setting $\beta = n/(n, n')$ and observing that

$$(n/(n, n'), n'/(n, n')) = 1.$$

The resulting set of cycles, which we call D, is defined by

$$D = \{\mathbf{z}_{jh} \ \ :\ \ 0 \le h < (n, n'),\ \ 0 \le j < d^v/n'\}$$

where $\mathbf{z}_{jh} = \mathbf{y}_{jh}$ concatenated with itself $n/(n, n')$ times. By Theorem 4.5, D is an $(n'/(n, n'), n, d, v)$–PMF.

Finally, apply Construction 5.1 to A and D, to produce the set of cycles

$$B = \{\mathbf{w}_i + c\mathbf{z}_{jh} : 0 \le i < c^v/n,\ \ 0 \le h < (n, n'),\ \ 0 \le j < d^v/n'\},$$

where $\mathbf{w}_i$ is equal to $\mathbf{u}_i$ concatenated with itself $n'/(n, n')$ times. By Theorem 5.2, B is an $(nn'/(n, n'), cd, v)$–PF.

Finally observe that, if $\mathbf{x}_j$ is defined as in Construction 6.1 above, then

$$\mathbf{z}_{jh} = \mathbf{T}_h(\mathbf{x}_j)$$

for every j, h, $(0 \le h < (n, n'),\ \ 0 \le j < d^v/n')$, and the result follows. □

Example 6.3 *Let A be the following $(4, 2, 2)$–PF (a 2-ary span 2 de Bruijn sequence):*

$$u_0 = \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}.$$

Let A' be the $(6,6,2)$–PF constructed in Example 5.3, as follows

$$v_0 = \begin{pmatrix} 0 & 0 & 1 & 0 & 3 & 4 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 3 & 0 & 4 & 3 & 3 & 1 \end{pmatrix},$$
$$v_2 = \begin{pmatrix} 1 & 1 & 2 & 1 & 4 & 5 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 4 & 1 & 5 & 4 & 4 & 2 \end{pmatrix},$$
$$v_4 = \begin{pmatrix} 2 & 2 & 0 & 2 & 5 & 3 \end{pmatrix}, \quad v_5 = \begin{pmatrix} 5 & 2 & 3 & 5 & 5 & 0 \end{pmatrix}.$$

Hence since $n = 4$ and $n' = 6$, we have $nn'/(n,n') = 12$. Thus we have

$$w_0 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

We also have

$$x_0 = \begin{pmatrix} 0 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 1 & 0 & 3 & 4 \end{pmatrix}, \; x_1 = \begin{pmatrix} 3 & 0 & 4 & 3 & 3 & 1 & 3 & 0 & 4 & 3 & 3 & 1 \end{pmatrix},$$
$$x_2 = \begin{pmatrix} 1 & 1 & 2 & 1 & 4 & 5 & 1 & 1 & 2 & 1 & 4 & 5 \end{pmatrix}, \; x_3 = \begin{pmatrix} 4 & 1 & 5 & 4 & 4 & 2 & 4 & 1 & 5 & 4 & 4 & 2 \end{pmatrix},$$
$$x_4 = \begin{pmatrix} 2 & 2 & 0 & 2 & 5 & 3 & 2 & 2 & 0 & 2 & 5 & 3 \end{pmatrix}, \; x_5 = \begin{pmatrix} 5 & 2 & 3 & 5 & 5 & 0 & 5 & 2 & 3 & 5 & 5 & 0 \end{pmatrix}.$$

Hence B, derived using Construction 6.1, is a $(12,12,2)$–PF, and is as follows:

$$s_{000} = \begin{pmatrix} 0 & 0 & 3 & 1 & 6 & 8 & 1 & 1 & 2 & 0 & 7 & 9 \end{pmatrix}, \quad s_{010} = \begin{pmatrix} 6 & 0 & 9 & 7 & 6 & 2 & 7 & 1 & 8 & 6 & 7 & 3 \end{pmatrix},$$
$$s_{020} = \begin{pmatrix} 2 & 2 & 5 & 3 & 8 & 10 & 3 & 3 & 4 & 2 & 9 & 11 \end{pmatrix}, \; s_{030} = \begin{pmatrix} 8 & 2 & 11 & 9 & 8 & 4 & 9 & 3 & 10 & 8 & 9 & 5 \end{pmatrix},$$
$$s_{040} = \begin{pmatrix} 4 & 4 & 1 & 5 & 10 & 6 & 5 & 5 & 0 & 4 & 11 & 7 \end{pmatrix}, \; s_{050} = \begin{pmatrix} 10 & 4 & 7 & 11 & 10 & 0 & 11 & 5 & 6 & 10 & 11 & 1 \end{pmatrix},$$
$$s_{001} = \begin{pmatrix} 8 & 0 & 1 & 3 & 0 & 6 & 9 & 1 & 0 & 2 & 1 & 7 \end{pmatrix}, \quad s_{011} = \begin{pmatrix} 2 & 6 & 1 & 9 & 6 & 6 & 3 & 7 & 0 & 8 & 7 & 7 \end{pmatrix},$$
$$s_{021} = \begin{pmatrix} 10 & 2 & 3 & 5 & 2 & 8 & 11 & 3 & 2 & 4 & 3 & 9 \end{pmatrix}, \; s_{031} = \begin{pmatrix} 4 & 8 & 3 & 11 & 8 & 8 & 5 & 9 & 2 & 10 & 9 & 9 \end{pmatrix},$$
$$s_{041} = \begin{pmatrix} 6 & 4 & 5 & 1 & 4 & 10 & 7 & 5 & 4 & 0 & 5 & 11 \end{pmatrix}, \; s_{051} = \begin{pmatrix} 0 & 10 & 5 & 7 & 10 & 10 & 1 & 11 & 4 & 6 & 11 & 11 \end{pmatrix}.$$

We conclude this section by observing that Paterson, [4], has recently also devised a distinct method of combining two Perfect Factors, with the result that the following theorem is true.

Theorem 6.4 (Paterson (1992), [4]) *If there exists an (n,c,v)–PF and an (n',c',v)–PF, where $(c,c') = 1$, then there also exists an (nn',cc',v)–PF.*

7 Summary and conclusions

We conclude this paper by considering how far we have gone towards establishing Conjecture 1.4, i.e. for which values of n, c and v we can construct an (n, c, v)–PF.

7.1 The existence result

Before giving our main existence result, we need to establish some notation. Suppose n, c and v are positive integers satisfying $n|c^v$, $n > v$ and $c > 1$. Suppose further that

$$c = \prod_{i \in F} p_i^{\alpha_i},$$

and that

$$n = \prod_{i \in G \subseteq F} p_i^{\beta_i},$$

where p_i ($i \in F$) are distinct primes and α_i and β_i are positive integers (hence G contains the indices of those primes occurring with a positive exponent in the prime decomposition of n). Note that it should be clear that, since $n|c^v$, we must have $\beta_i \leq v\alpha_i$ for every $i \in G$. Finally define H to be the following subset of G:

$$H = \{i \in G : (p_i)^{\beta_i} > v\}.$$

Theorem 7.1 *Using the above notation, an (n, c, v)–PF can be constructed for any n, c, v satisfying $n|c^v$, $n > v$ and $c > 1$, as long as $H \neq \emptyset$.*

Proof Choose $i \in H$ and let $\gamma_i = \min\{\beta_i, v\}$. The we immediately have

$$p_i^{\gamma_i} \geq \min\{p_i^{\beta_i}, p_i^v\} > v$$

(since $p_i \geq 2$, $v \geq 1$ and $i \in H$). Hence, by Etzion, [2], and Paterson, [4], there exists a $(p_i^{\gamma_i}, p_i, v)$–PF.

If $c = p_i$ (and hence $n = p_i^{\gamma_i}$) then we are done. Hence suppose that $c > p_i$, and then we have $c/p_i \geq 2$, $p_i^{\gamma_i} \geq v$, and

$$(\frac{n}{p_i^{\gamma_i}}) \mid (\frac{c}{p_i})^v,$$

and hence, by Corollary 4.17, there exists an $(n/p_i^{\gamma_i}, p_i^{\gamma_i}, c/p_i, v)$–PMF.

If this PMF is combined with the above-mentioned $(p_i^{\gamma_i}, p_i, v)$–PF using Construction 5.1, then, by Theorem 5.2 the result will be a (n, c, v)–PF, as required. □

Remark 7.2 *The above result only requires a method for constructing an (n, c, v)–PF for any n satisfying $v < n|c^v$ and for any prime c, not the more powerful result proved by Paterson, [4], that such a PF exists for any c a* prime power.

Corollary 7.3 *Conjecture 1.4 is true for $v = 2$ and any n and c.*

Proof Since $n \geq 3$, it follows that $H \neq \emptyset$ and the result follows. □

7.2 Open cases

We conclude this note by considering the ramifications of Theorem 7.1 for small values of c and v (c not a prime power and $v \geq 3$). For each pair (c, v) that we consider, the existence question for every value of n which satisfies the necessary conditions of Lemma 1.3 is considered.

7.2.1 Example I: $(n, 6, 3)$–PFs

The 13 possible values for n are 4, 6, 8, 9, 12, 18, 24, 27, 36, 54, 72, 108 and 216. Perfect Factors for all but the second value exist by Theorem 7.1. If $n = 6$ then observe that the condition of Theorem 7.1 is not satisfied, since in this case $H = \emptyset$. Hence the existence of a $(6, 6, 3)$–PF remains an open question.

7.2.2 Example II: $(n, 10, 3)$–PFs

The 14 possible values for n are 4, 5, 8, 10, 20, 25, 40, 50, 100, 125, 200, 250, 500 and 1000. Perfect Factors for all values exist by Theorem 7.1.

7.2.3 Example III: $(n, 12, 3)$–PFs

The 25 possible values for n are 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, 64, 72, 96, 108, 144, 192, 216, 288, 432, 576, 864 and 1728. For 24 of these values (namely all but 6) we have $H \neq \emptyset$, i.e. the condition of Theorem 7.1 is satisfied. Hence the existence of a $(6, 12, 3)$–PF is an open question.

7.2.4 Example IV: $(n, 6, 4)$–PFs

The 21 possible values for n are 6, 8, 9, 12, 16, 18, 24, 27, 36, 48, 54, 72, 81, 108, 144, 162, 216, 324, 432, 648 and 1296. For 19 of these values (namely all but 6 and 12) we have $H \neq \emptyset$, i.e. the condition of Theorem 7.1 is satisfied. Hence the existence of a $(6, 6, 4)$–PF and a $(12, 6, 4)$–PF remain an open question.

7.2.5 Example V: $(n, 12, 4)$–PFs

The 41 possible values for n are 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, 48, 54, 64, 72, 81, 96, 108, 128, 144, 162, 192, 216, 256, 288, 324, 384, 432, 576, 648, 768, 864, 1152, 1296, 1728, 2304, 2592, 3456, 5184, 6912, 10368 and 20736. For 39 of these values (namely all but 6 and 12) we have $H \neq \emptyset$, i.e. the condition of Theorem 7.1 is satisfied. Hence the existence of a $(6, 12, 4)$–PF and a $(12, 12, 4)$–PF remain an open question.

Acknowledgements

The author would like to thank Kenny Paterson, Wen-Ai Jackson and Peter Wild for many helpful discussions and suggestions.

References

[1] J. Burns and C.J. Mitchell. Coding schemes for two-dimensional position sensing. In M.J. Ganley, editor, *Cryptography and Coding III*, pages 31–66. Oxford University Press, 1993.

[2] T. Etzion. Constructions for perfect maps and pseudo-random arrays. *IEEE Transactions on Information Theory*, **34**:1308–1316, 1988.

[3] C.J. Mitchell and K.G. Paterson. Decoding perfect maps. *Designs, Codes and Cryptography*, **4**:11–30, 1994.

[4] K.G. Paterson. Perfect factors in the de Bruijn graph. *Designs, Codes and Cryptography*, **5**:115–138, 1995.