New c-ary Perfect Factors in the de Bruijn Graph

C. J. Mitchell

Computer Science Department, Royal Holloway, University of London, Egham, Surrey TW20 0EX, England

Abstract

A *c-ary Perfect Factor* is a collection 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, [1], who showed that the necessary conditions for their existence are in fact sufficient. This result has recently been extended by Paterson, [2], who has shown that the necessary existence conditions are sufficient whenever c is a prime power. In [3] the existence question for general composite c was studied, and it was conjectured that the necessary existence conditions are also sufficient in this case. However, although construction methods for these Perfect Factors were exhibited in [3], the conjecture remains open. In this paper we provide further evidence for the conjecture by constructing c-ary Perfect Factors for several of the previously undecided cases.

1 Introduction

Perfect factors were introduced, in the binary case, by Etzion, [1], 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 a straightforward generalisation of Etzion's construction to construct non-binary Perfect Maps; for further details see [2]. Perfect Maps, both binary and non-binary, have possible application in the field of automatic position sensing, as discussed in [4].

Secondly, they are of interest in their own right as natural generali-

sations of the classical de Bruijn sequences, about which much has been written. They also have applications in other areas, including the construction of de Bruijn sequences with minimal linear complexity, [2].

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 $\boldsymbol{t} = (t_0, t_1, \ldots, t_{v-1})$ is a c-ary v-tuple (i.e. $t_i \in \{0, 1, \ldots, c-1\}$ for every i, $(0 \leq i < v)$), and $\boldsymbol{s} = [s_0, s_1, \ldots, s_{n-1}]$ is a c-ary cycle of period n $(n \geq v)$, then we say that $\boldsymbol{t}$ *occurs in* $\boldsymbol{s}$ *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 $\boldsymbol{s}$ and $\boldsymbol{s}'$ are two v-tuples, then we write $\boldsymbol{s}+\boldsymbol{s}'$ for the v-tuple obtained by element-wise adding together the two tuples. Similarly, if k is any integer, we write $k\boldsymbol{s}$ for the tuple obtained by element-wise multiplying the tuple $\boldsymbol{s}$ by k. Again, if we write $\boldsymbol{t} = \boldsymbol{s} \bmod k$, then $\boldsymbol{t}$ is the tuple obtained by reducing every element in $\boldsymbol{s}$ modulo k. An exactly analogous interpretation should be used for arithmetic operations on cycles.

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

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

where $i + k$ is calculated modulo n.

Suppose $\boldsymbol{u} = [u_0, u_1, \ldots, u_{n-1}]$ and $\boldsymbol{u}' = [u'_0, u'_1, \ldots, u'_{n'-1}]$ are c-ary cycles of periods n and n' respectively. Then define the *concatenation* of $\boldsymbol{u}$ and $\boldsymbol{u}'$ to be a c-ary cycle of period $n + n'$

$$\boldsymbol{s} = [s_0, s_1, \ldots, s_{n+n'-1}],$$

where

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

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. *Suppose n, c and v are positive integers (where we also assume that $c \geq 2$). An (n, c, v)–*Perfect Factor*, or simply an (n, c, v)–PF, is a collection 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 collection of cycles, which are thus necessarily all distinct. Also observe that a (c^v, c, v)–PF is simply a c-ary span v de Bruijn sequence.

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

$$[\ 0\quad 0\quad 1\ ],\ [\ 1\quad 1\quad 2\ ],\ [\ 2\quad 2\quad 0\ ].$$

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

Lemma 3. *([3]) Suppose A is a (n, c, v)–PF. Then*

1. *$n|c^v$, and*
2. *$v < n$ or $n = v = 1$.*

We also have the following.

Conjecture A. ([3]) The necessary conditions of Lemma 3 are sufficient for the existence of a Perfect Factor.

Etzion, [1], showed that Conjecture A is true in the binary case, i.e. $c = 2$. Paterson, [2], has recently shown that Conjecture A is true whenever $c = p^\alpha$ for p any prime and α a positive integer. The following existence result for general composite c has recently been constructively obtained.

Theorem 4. *([3]) Suppose n, c and v are positive integers satisfying $n|c^v$, $n > v$ and $c > 1$. If $p^\beta > v$ and $p^\beta|n$ for some prime p, then an (n, c, v)–PF can be constructed.*

This leads to the following.

Corollary. ([3]) Suppose n and c are positive integers satisfying $n|c^2$, $n > 2$ and $c > 1$. Then an $(n, c, 2)$–PF can be constructed.

This means that Conjecture A is true for the case $v = 2$. In this paper we construct Perfect Factors for parameter sets not covered by Theorem 4; in particular we show that Conjecture A holds for the cases $v = 3$ and $v = 4$.

1.3 Perfect Multi-factors

We define a related set of combinatorial objects, first introduced in [3].

Definition 5. *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 collection of c^v/m c-ary cycles of period mn with the property that for every c-ary v-tuple $\boldsymbol{t}$ and for every integer j in the range $0 \leq j < n$, $\boldsymbol{t}$ 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 collection of cycles, once in each of the possible position congruency classes (mod n). This also implies that all the cycles are distinct.

It should be clear that an $(m, 1, c, v)$–PMF is precisely equivalent to an (m, c, v)–PF. In addition, observe that a $(1, n, c, v)$–PMF is simply a collection of c^v c-ary cycles of period n with the property that every c-ary v-tuple occurs at every possible position in one of the cycles.

We next give a simple example of a PMF which is not a PF; this PMF can be very easily constructed using the method described in Section 4 of [3].

Example 6. *The following four cycles form a $(2, 3, 2, 3)$–PMF.*

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

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

Lemma 7. *([3]) Suppose A is an (m, n, c, v)–PMF. Then*

1. *$m|c^v$, and*
2. *(a) $m = 1$ and $v \leq mn$, or*
   (b) $m > 1$ and $v < mn$.

This leads to a second existence conjecture, which implies Conjecture A.

Conjecture B. ([3]) The necessary conditions of Lemma 7 for the existence of an (m, n, c, v)–PMF are sufficient.

We have the following result on the construction of PMFs, establishing Conjecture B whenever $n \geq v$.

Theorem 8. *([3]) Suppose n, c, v are positive integers ($c \geq 2$ and $n \geq v$). Then there exists a (m, n, c, v)–PMF for every positive integer m satisfying $m|c^v$.*

This means that, for the special case $m = 1$, Conjecture B has been established, i.e. we have the following.

Theorem 9. *([3]) Suppose n, c, v are positive integers ($c \geq 2$ and $n \geq v$). Then there exists a $(1, n, c, v)$–PMF.*

1.4 Generalised Perfect Factors

We now define yet another set of combinatorial objects, the definition of which is a generalisation of the notion of Perfect Factor (as is the definition of Perfect Multi-factor). We subsequently use these objects to help us construct some new Perfect Factors.

Definition 10. *Suppose m, n, c and v are positive integers satisfying $m|c^v$ and $c \geq 2$. An (m, n, c, v)–*Generalised Perfect Factor*, or simply an (m, n, c, v)–GPF, is a collection of c^v/m c-ary cycles of period mn with the following property. For every c-ary v-tuple $\boldsymbol{t}$, there exists an integer j in the range $0 \leq j < m$ such that for every i $(0 \leq i < n)$ $\boldsymbol{t}$ occurs at position $j + im$ in one of these cycles.*

Note that, because we insist that a GPF 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 position $j + im$ $(0 \leq i < n)$. This immediately implies that all the cycles are distinct.

Remark. It should be clear that

1. an $(m, 1, c, v)$–GPF is precisely equivalent to an (m, c, v)–PF, and
2. a $(1, n, c, v)$–GPF is precisely equivalent to a $(1, n, c, v)$–PMF.

The following result is also straightforward to prove:

Theorem 11. *Suppose A is an (m, n, c, v)–GPF, where $(m, n) = 1$. Then A is also a (m, n, c, v)–PMF.*

Proof. Choose any c-ary v-tuple, $\boldsymbol{t}$ say. Then, by definition, $\boldsymbol{t}$ occurs at position $j + im$ in some cycle of A for every i $(0 \leq i < n)$, for some fixed

j $(0 \leq j < m)$. Now consider the collection of positions at which $\boldsymbol{t}$ occurs modulo n, i.e. consider the multi-set

$$\{j \bmod n, j+m \bmod n, j+2m \bmod n, \ldots, j+(n-1)m \bmod n\}.$$

But since we assumed that $(m,n)=1$ the above is nothing more than

$$\{0,1,2,\ldots,n-1\}$$

and the result follows on examination of the definition of a PMF.

It is important to note that the converse of the above result does not hold. Indeed, as we show below, there exist parameter sets (m,n,c,v) with $(m,n)=1$ for which (m,n,c,v)–GPFs do not exist, but for which there do exist (m,n,c,v)–PMFs.

We next give a simple example of a GPF which is neither a PF or a PMF.

Example 12. *The following two cycles constitute a* $(2,2,2,2)$*–GPF.*

$$\left[\begin{array}{cccc} 1 & 1 & 0 & 0 \end{array}\right], \left[\begin{array}{cccc} 0 & 0 & 1 & 1 \end{array}\right].$$

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

Lemma 13. *Suppose A is an (m,n,c,v)–GPF. Then*

1. $m|c^v$, *and*
2. *(a)* $m=1$ *and* $v \leq mn$, *or*
   (b) $m>1$ *and* $v<mn$.

It is tempting at this point to conjecture that the necessary conditions specified in Lemma 13 for the existence of an (m,n,c,v)–GPF are sufficient. However, this is not true.

To see this consider the parameter set $(2,3,2,4)$. These parameters satisfy the necessary conditions of Lemma 13. Now, if a $(2,3,2,4)$–GPF existed it would consist of a set of 8 binary cycles of length 6 in which every binary 4-tuple occurs exactly three times, either in positions 0, 2 and 4 or at positions 1, 3 and 5. In particular the tuples $(0,0,0,0)$ and $(1,1,1,1)$ must occur, and hence such a GPF must contain the following six cycles (or their shift by one place).

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right], \left[\begin{array}{cccccc} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right].$$

To see why this holds note that a sequence of five consecutive zeros (or ones) in a cycle would give two all-zero (all-one) 4-tuples in adjacent positions, which is not permitted within such a GPF.

Finally note that the above set of cycles contains the 4-tuple $(0, 0, 1, 1)$ six times, and hence these cycles cannot all be contained in a $(2, 3, 2, 4)$–GPF. Hence such a GPF cannot exist. However, as the next example shows, a PMF with these parameters *does* exist.

Example 14. *The following set of eight binary cycles of length 6 constitutes a* $(2, 3, 2, 4)$*–PMF.*

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

This set of cycles was obtained by applying the inverse of Lempel's Homomorphism (see [5]) twice to the cycles of the following $(2, 3, 2, 2)$*–PMF:*

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

We also give the following additional example which will be of use below.

Example 15. *The following four binary cycles of length 12 constitute a* $(4, 3, 2, 4)$*–PMF.*

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

This set of cycles was obtained by concatenating pairs of cycles from the previous example.

2 Constructing Generalised Perfect Factors

We next show how to construct a large class of GPFs.

Construction C. Suppose m, n, c and v are positive integers which satisfy $m|c^v$ and $c \geq 2$. Suppose

$$A = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{t-1}\}$$

is a set of c-ary cycles of lengths

$$\ell_0, \ell_1, \ldots, \ell_{t-1}$$

respectively, with the property that

$$m|\ell_i$$

and

$$\ell_i|mn$$

for every i $(0 \leq i < t)$. Suppose moreover that every c-ary v-tuple occurs precisely once somewhere in this set of cycles, and hence

$$\sum_{i=0}^{t-1} \ell_i = c^v.$$

Then, for every i $(0 \leq i < t)$ let $\boldsymbol{w}_i$ be defined as $\boldsymbol{a}_i$ concatenated with itself mn/ℓ_i times. Next let

$$b_{ij} = \boldsymbol{T}_{jm}(\boldsymbol{w}_i)$$

for every j, $(0 \leq j < \ell_i/m)$. Finally let

$$B = \{\boldsymbol{b}_{ij} \,:\, 0 \leq i < t,\, 0 \leq j < \ell_i/m\},$$

and B will consist of a set of

$$\sum_{i=0}^{t-1} \frac{\ell_i}{m} = \frac{c^v}{m}$$

c-ary cycles of length mn.

Theorem 16. *Suppose m, n, c and v are positive integers satisfying $m|c^v$ and $c \geq 2$, and*

$$A = \{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{t-1}\}$$

is a set of c-ary cycles satisfying the conditions of Construction C. If B is constructed from A using Construction C then B is a (m, n, c, v)–GPF.

Proof. Choose some c-ary v-tuple, $\boldsymbol{t}$ say. Then, by assumption, $\boldsymbol{t}$ occurs at some position, r say, in a cycle of A. Suppose this cycle is $\boldsymbol{a}_s$ of length ℓ_s, and hence $0 \leq r < \ell_s$. Using the notation of Construction C, $\boldsymbol{t}$ will then occur at positions

$$r, r + \ell_s, \ldots, r + (mn/\ell_s - 1)\ell_s$$

in the cycle $\boldsymbol{w}_s$. Hence $\boldsymbol{t}$ will occur at positions

$$jm + r, jm + r + \ell_s, \ldots, jm + r + (mn/\ell_s - 1)\ell_s$$

in cycle $\boldsymbol{b}_{sj}$ of B for every j $(0 \leq j < \ell_s/m)$, since, by definition

$$\boldsymbol{b}_{sj} = \boldsymbol{T}_{jm}(\boldsymbol{w}_i).$$

Note that all these positions should be reduced modulo mn.

Hence $\boldsymbol{t}$ occurs in some cycle of B at all the following positions:

$$r, r + m, r + 2m, \ldots, r + (n-1)m$$

and the result follows from the definition of a GPF.

Example 17. *Consider the following set of 3-ary cycles:*

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 2 & 1 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 0 & 2 \end{array}\right], \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 1 & 0 \end{array}\right],$$
$$\left[\begin{array}{ccc} 0 & 0 & 2 \end{array}\right], \quad \left[\begin{array}{ccc} 1 & 1 & 0 \end{array}\right], \quad \left[\begin{array}{ccc} 2 & 2 & 1 \end{array}\right].$$

It is straightforward to see that the above set of cycles contain every 3-ary 3-tuple exactly once. Moreover if we set $m = 3$, $n = 2$, $c = 3$ and $v = 3$ it should be clear that $m = 3$ divides the length of each cycle and also that the length of every cycle is a factor of $mn = 6$. Hence, using Construction C we obtain the following set of nine cycles which, by Theorem 16, constitute a $(3, 2, 3, 3)$–GPF.

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 2 & 1 \\ 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 2 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 0 & 2 \\ 2 & 0 & 2 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right], \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right].$$

Example 18. *Consider the following set of 3-ary cycles:*

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 2 & 2 & 1 & 1 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 1 & 0 \end{array}\right], \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 2 & 1 \end{array}\right],$$
$$\left[\begin{array}{ccc} 0 & 1 & 2 \end{array}\right].$$

The above set of cycles contain every 3-ary 3-tuple exactly once. Moreover if we set $m = 3$, $n = 2$, $c = 3$ and $v = 3$ it should be clear that $m = 3$ divides the length of each cycle and also that the length of every cycle is a factor of $mn = 6$. Hence, using Construction C we obtain the following set of nine cycles which, by Theorem 16, constitute a $(3, 2, 3, 3)$–GPF.

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 & 1 & 1 \\ 2 & 1 & 1 & 0 & 0 & 2 \end{array}\right], \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 2 & 1 \\ 0 & 2 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 \end{array}\right].$$

Of particular note about this second example is the fact that the sum of the elements of each of the nine cycles is congruent to 0 mod 3. This means that we can apply the inverse of Lempel's Homomorphism (see [5]) to the above set of cycles to obtain a set of 27 cycles of length 6 constituting a $(3, 2, 3, 4)$–GPF, as follows.

$$\left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 2 & 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 2 \\ 0 & 0 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 & 1 & 2 \\ 2 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{cccccc} 1 & 1 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 & 2 \end{array}\right], \left[\begin{array}{cccccc} 2 & 2 & 2 & 2 & 0 & 0 \\ 2 & 0 & 1 & 2 & 1 & 2 \\ 2 & 1 & 0 & 2 & 2 & 1 \\ 2 & 0 & 0 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 & 0 & 1 \\ 2 & 2 & 1 & 2 & 1 & 0 \\ 2 & 2 & 2 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 \end{array}\right].$$

More generally, the above construction enables us to establish the existence of a large class of GPFs from the previously known Perfect Factors, as the following Corollary shows.

Corollary. Suppose p is a prime, $v \geq 2$, $\gamma \geq 1$ and α, β are non-negative integers satisfying

1. $v < p^{\alpha+\beta}$,
2. $\alpha + \beta \leq \gamma v$.

Then there exists a $(p^\alpha, p^\beta, p^\gamma, v)$–GPF.

Proof. Since $1 < v < p^{\alpha+\beta} \leq (p^\gamma)^v$ and $\gamma \geq 1$, there exists a $(p^{\alpha+\beta}, p^\gamma, v)$–PF (from [2]). The result then follows immediately from Theorem 16.

We next present a very simple method of obtaining a 'larger' Generalised Perfect Factor from a 'smaller' one.

Construction D. Suppose that

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

is an (m, n, c, v)–GPF. Now, given $\lambda \geq 1$, let

$$A_\lambda = \{\boldsymbol{s}_i : 0 \leq i < c^v/m\}$$

be a set of cycles of period λmn where $\boldsymbol{s}_i$ is defined to be equal to $\boldsymbol{u}_i$ concatenated with itself λ times.

Theorem 19. *Suppose A_λ (where $\lambda \geq 1$) is obtained from an (m, n, c, v)–GPF A using Construction D. Then A_λ is an $(m, \lambda n, c, v)$–GPF.*

Proof. The result follows immediately from the definition of GPF.

Example 20. *Suppose A is the $(3, 2, 3, 3)$–GPF of Example 17. Using Construction D with $\lambda = 2$ we obtain the following set of nine 3-ary cycles of length 12, constituting a $(3, 4, 3, 3)$–GPF.*

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

We now show how a GPF and a PMF can be combined to produce a GPF on a larger alphabet.

Construction E. Suppose that

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

is an (m, n, c, v)–GPF. Suppose also that

$$A' = \{\boldsymbol{v}_i : 0 \le i < h\}$$

is a set of h d-ary cycles of period mn for some $d \ge 2$. Now let

$$B = \{\boldsymbol{s}_{ij} : 0 \le i < c^v/m,\ \ 0 \le j < h\}$$

be the set of cd-ary cycles of period mn defined by

$$\boldsymbol{s}_{ij} = \boldsymbol{u}_i + c\boldsymbol{v}_j.$$

Theorem 21. *Suppose B is constructed from an (m, n, c, v)–GPF A and a $(1, mn, d, v)$–PMF A' (with $h = d^v$) using Construction E. Then B is an (m, n, cd, v)–GPF.*

Proof. Suppose $\boldsymbol{t}$ is a (cd)-ary v-tuple. Let $\boldsymbol{s} = \boldsymbol{t} \bmod c$, and let $\boldsymbol{w} = (\boldsymbol{t} - \boldsymbol{s})/c$. Then $\boldsymbol{s}$ is a c-ary v-tuple and $\boldsymbol{w}$ is a d-ary v-tuple and we have

$$\boldsymbol{t} = \boldsymbol{s} + c\boldsymbol{w}.$$

Now, since A is a (m, n, c, v)–GPF there exists an integer j $(0 \le j < m)$ such that for every i, $(0 \le i < n)$, $\boldsymbol{s}$ occurs at position $j + im$ in a cycle of A. We now claim that for every i, $(0 \le i < n)$, $\boldsymbol{t}$ occurs at position $j + im$ in a cycle of B.

To show this choose any i satisfying $0 \le i < n$ and suppose $\boldsymbol{s}$ occurs at position $j + im$ in cycle $\boldsymbol{u}_r$ of A. Now, since A' is a $(1, mn, d, v)$–PMF, there exists a cycle in A', $\boldsymbol{v}_q$ say, such that $\boldsymbol{w}$ occurs at position $j + im$ in cycle $\boldsymbol{v}_q$. It should then be clear that $\boldsymbol{t}$ occurs at position $j + im$ in cycle $\boldsymbol{s}_{rq}$ of B and the result follows.

Example 22. *Suppose A is the following $(3, 2, 3, 2)$–GPF (consisting of three 3-ary cycles of length 6):*

$$\boldsymbol{u}_0 = \left[\begin{array}{cccccc} 0 & 0 & 2 & 0 & 0 & 2 \end{array}\right],\ \boldsymbol{u}_1 = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right],\ \boldsymbol{u}_2 = \left[\begin{array}{cccccc} 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right].$$

Suppose also that A' is the following $(1, 6, 2, 2)$–GPF (consisting of four binary cycles of length 6):

$$\begin{array}{ll} \boldsymbol{v}_0 = \left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right], & \boldsymbol{v}_1 = \left[\begin{array}{cccccc} 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right], \\ \boldsymbol{v}_2 = \left[\begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right], & \boldsymbol{v}_3 = \left[\begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right]. \end{array}$$

Then B, derived using Construction E, is a $(3, 2, 6, 2)$–GPF, and consists of the following set of 12 6-ary cycles of length 6

$$\begin{array}{llll}
\boldsymbol{s}_{00} = \left[\begin{array}{cccccc} 0 & 0 & 2 & 0 & 0 & 2 \end{array}\right], & \boldsymbol{s}_{01} = \left[\begin{array}{cccccc} 0 & 3 & 2 & 3 & 0 & 5 \end{array}\right], \\
\boldsymbol{s}_{02} = \left[\begin{array}{cccccc} 3 & 3 & 5 & 3 & 3 & 5 \end{array}\right], & \boldsymbol{s}_{03} = \left[\begin{array}{cccccc} 3 & 0 & 5 & 0 & 3 & 2 \end{array}\right], \\
\boldsymbol{s}_{10} = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right], & \boldsymbol{s}_{11} = \left[\begin{array}{cccccc} 1 & 4 & 0 & 4 & 1 & 3 \end{array}\right], \\
\boldsymbol{s}_{12} = \left[\begin{array}{cccccc} 4 & 4 & 3 & 4 & 4 & 3 \end{array}\right], & \boldsymbol{s}_{13} = \left[\begin{array}{cccccc} 4 & 1 & 3 & 1 & 4 & 0 \end{array}\right], \\
\boldsymbol{s}_{20} = \left[\begin{array}{cccccc} 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right], & \boldsymbol{s}_{21} = \left[\begin{array}{cccccc} 2 & 5 & 1 & 5 & 2 & 4 \end{array}\right], \\
\boldsymbol{s}_{22} = \left[\begin{array}{cccccc} 5 & 5 & 4 & 5 & 5 & 4 \end{array}\right], & \boldsymbol{s}_{23} = \left[\begin{array}{cccccc} 5 & 2 & 4 & 2 & 5 & 1 \end{array}\right].
\end{array}$$

3 Constructing Perfect Factors using GPFs

We now show how Construction E may be used to construct Perfect Factors.

Theorem 23. *Suppose B is constructed from an (ν, μ, c, v)–GPF A and an (μ, ν, d, v)–PMF A' using Construction E. Then B is an $(\mu\nu, cd, v)$–PF.*

Proof. Consider any (cd)-ary v-tuple, x say. Then let

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

Then $\boldsymbol{y}$ is a c-ary v-tuple and hence occurs precisely μ times in cycles of A, at positions $j, j+\nu, \ldots, j+(\mu-1)\nu$ in cycles $\boldsymbol{u}_{k_0}, \boldsymbol{u}_{k_1}, \ldots, \boldsymbol{u}_{k_{\mu-1}}$, say, where $0 \le j < \nu$.

Now let

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

this is simple to do in integers since every element of $\boldsymbol{x} - \boldsymbol{y}$ must be a multiple of c. It should also be clear that $\boldsymbol{z}$ is a d-ary v-tuple, and hence occurs at position $d \equiv j \pmod{\nu}$ (say $d = j + \lambda\nu$) in some cycle in A', say $\boldsymbol{v}_{k'}$. It is now straightforward to check that $\boldsymbol{x}$ appears at position d in the cycle $\boldsymbol{s}_{k_\lambda k'}$ 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 $(cd)^v/\mu\nu$ cycles in B, each of length $\mu\nu$.

Example 24. *Let A be the $(3, 2, 3, 3)$–GPF of Example 17, i.e. A contains the cycles*

$$\begin{array}{lll}
\boldsymbol{u}_0 = \left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 2 & 1 \end{array}\right], & \boldsymbol{u}_1 = \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 0 & 2 \end{array}\right], & \boldsymbol{u}_2 = \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 1 & 0 \end{array}\right], \\
\boldsymbol{u}_3 = \left[\begin{array}{cccccc} 1 & 2 & 1 & 0 & 0 & 0 \end{array}\right], & \boldsymbol{u}_4 = \left[\begin{array}{cccccc} 2 & 0 & 2 & 1 & 1 & 1 \end{array}\right], & \boldsymbol{u}_5 = \left[\begin{array}{cccccc} 0 & 1 & 0 & 2 & 2 & 2 \end{array}\right], \\
\boldsymbol{u}_6 = \left[\begin{array}{cccccc} 0 & 0 & 2 & 0 & 0 & 2 \end{array}\right], & \boldsymbol{u}_7 = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right], & \boldsymbol{u}_8 = \left[\begin{array}{cccccc} 2 & 2 & 1 & 2 & 2 & 1 \end{array}\right].
\end{array}$$

Let A' be the $(2, 3, 2, 3)$–PMF of Example 6, i.e. A' contains the cycles

$$\begin{array}{ll}
\boldsymbol{v}_0 = \left[\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right], & \boldsymbol{v}_1 = \left[\begin{array}{cccccc} 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right], \\
\boldsymbol{v}_2 = \left[\begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right], & \boldsymbol{v}_3 = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 1 \end{array}\right].
\end{array}$$

Then B, derived using Construction E, is a $(6,6,3)$–PF, and is as follows:

$$\begin{array}{llll}
\boldsymbol{s}_{00} = \left[\begin{array}{cccccc} 0 & 0 & 0 & 1 & 2 & 4 \end{array}\right], & \boldsymbol{s}_{01} = \left[\begin{array}{cccccc} 0 & 3 & 0 & 1 & 5 & 4 \end{array}\right], \\
\boldsymbol{s}_{02} = \left[\begin{array}{cccccc} 3 & 0 & 0 & 4 & 2 & 4 \end{array}\right], & \boldsymbol{s}_{03} = \left[\begin{array}{cccccc} 3 & 3 & 0 & 4 & 5 & 4 \end{array}\right], \\
\boldsymbol{s}_{10} = \left[\begin{array}{cccccc} 1 & 1 & 1 & 2 & 0 & 5 \end{array}\right], & \boldsymbol{s}_{11} = \left[\begin{array}{cccccc} 1 & 4 & 1 & 2 & 3 & 5 \end{array}\right], \\
\boldsymbol{s}_{12} = \left[\begin{array}{cccccc} 4 & 1 & 1 & 5 & 0 & 5 \end{array}\right], & \boldsymbol{s}_{13} = \left[\begin{array}{cccccc} 4 & 4 & 1 & 5 & 3 & 5 \end{array}\right], \\
\boldsymbol{s}_{20} = \left[\begin{array}{cccccc} 2 & 2 & 2 & 0 & 1 & 3 \end{array}\right], & \boldsymbol{s}_{21} = \left[\begin{array}{cccccc} 2 & 5 & 2 & 0 & 4 & 3 \end{array}\right], \\
\boldsymbol{s}_{22} = \left[\begin{array}{cccccc} 5 & 2 & 2 & 3 & 1 & 3 \end{array}\right], & \boldsymbol{s}_{23} = \left[\begin{array}{cccccc} 5 & 5 & 2 & 3 & 4 & 3 \end{array}\right], \\
\boldsymbol{s}_{30} = \left[\begin{array}{cccccc} 1 & 2 & 1 & 0 & 0 & 3 \end{array}\right], & \boldsymbol{s}_{31} = \left[\begin{array}{cccccc} 1 & 5 & 1 & 0 & 3 & 3 \end{array}\right], \\
\boldsymbol{s}_{32} = \left[\begin{array}{cccccc} 4 & 2 & 1 & 3 & 0 & 3 \end{array}\right], & \boldsymbol{s}_{33} = \left[\begin{array}{cccccc} 4 & 5 & 1 & 3 & 3 & 3 \end{array}\right], \\
\boldsymbol{s}_{40} = \left[\begin{array}{cccccc} 2 & 0 & 2 & 1 & 1 & 4 \end{array}\right], & \boldsymbol{s}_{41} = \left[\begin{array}{cccccc} 2 & 3 & 2 & 1 & 4 & 4 \end{array}\right], \\
\boldsymbol{s}_{42} = \left[\begin{array}{cccccc} 5 & 0 & 2 & 4 & 1 & 4 \end{array}\right], & \boldsymbol{s}_{43} = \left[\begin{array}{cccccc} 5 & 3 & 2 & 4 & 4 & 4 \end{array}\right], \\
\boldsymbol{s}_{50} = \left[\begin{array}{cccccc} 0 & 1 & 0 & 2 & 2 & 5 \end{array}\right], & \boldsymbol{s}_{51} = \left[\begin{array}{cccccc} 0 & 4 & 0 & 2 & 5 & 5 \end{array}\right], \\
\boldsymbol{s}_{52} = \left[\begin{array}{cccccc} 3 & 1 & 0 & 5 & 2 & 5 \end{array}\right], & \boldsymbol{s}_{53} = \left[\begin{array}{cccccc} 3 & 4 & 0 & 5 & 5 & 5 \end{array}\right], \\
\boldsymbol{s}_{60} = \left[\begin{array}{cccccc} 0 & 0 & 2 & 0 & 0 & 5 \end{array}\right], & \boldsymbol{s}_{61} = \left[\begin{array}{cccccc} 0 & 3 & 2 & 0 & 3 & 5 \end{array}\right], \\
\boldsymbol{s}_{62} = \left[\begin{array}{cccccc} 3 & 0 & 2 & 3 & 0 & 5 \end{array}\right], & \boldsymbol{s}_{63} = \left[\begin{array}{cccccc} 3 & 3 & 2 & 3 & 3 & 5 \end{array}\right], \\
\boldsymbol{s}_{70} = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 3 \end{array}\right], & \boldsymbol{s}_{71} = \left[\begin{array}{cccccc} 1 & 4 & 0 & 1 & 4 & 3 \end{array}\right], \\
\boldsymbol{s}_{72} = \left[\begin{array}{cccccc} 4 & 1 & 0 & 4 & 1 & 3 \end{array}\right], & \boldsymbol{s}_{73} = \left[\begin{array}{cccccc} 4 & 4 & 0 & 4 & 4 & 3 \end{array}\right], \\
\boldsymbol{s}_{80} = \left[\begin{array}{cccccc} 2 & 2 & 1 & 2 & 2 & 4 \end{array}\right], & \boldsymbol{s}_{81} = \left[\begin{array}{cccccc} 2 & 5 & 1 & 2 & 5 & 4 \end{array}\right], \\
\boldsymbol{s}_{82} = \left[\begin{array}{cccccc} 5 & 2 & 1 & 5 & 2 & 4 \end{array}\right], & \boldsymbol{s}_{83} = \left[\begin{array}{cccccc} 5 & 5 & 1 & 5 & 5 & 4 \end{array}\right].
\end{array}$$

Note that the existence of a $(6,6,3)$–PF was the smallest undecided case given in [3].

Example 25. *The $(3,2,3,3)$–GPF of Example 17 can also be used in conjunction with a $(2,3,4,3)$–PMF (which exists by Theorem 8) to obtain a $(6,12,3)$–PF, the second undecided case of [3].*

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

We can now state and prove the following result, establishing the validity of Conjecture A in the cases $v = 3$ and $v = 4$.

Theorem 26. *Suppose n, c and v are positive integers satisfying $n|c^v$, $n > v$, $c > 1$ and $3 \leq v \leq 4$. Then an (n,c,v)–PF can be constructed.*

Proof. First suppose $v = 3$. By Theorem 4 we need only establish the existence of an $(n,c,3)$–PF for values of n satisfying

$$p^\beta \leq 3$$

for every prime factor p of n, where β is the largest power of p dividing n. Hence, since $n > 3$, we need only consider $n = 6$, i.e. we need to show how to construct a $(6,c,3)$–PF for all possible values of c.

Since $n|c^3$ this implies that $2|c$ and $3|c$. Suppose then that $c = 3d$, where $2|d$. Next observe that Example 17 provides us with a $(3, 2, 3, 3)$–GPF, and by Theorem 8 there exists a $(2, 3, d, 3)$–PMF (since $2|d$). Hence, by Theorem 23, there exists a $(6, 3d, 3)$–PF, and the desired result follows.

Now suppose $v = 4$. By identical arguments we need only show how to construct a $(6, c, 4)$–PF and a $(12, c, 4)$–PF for all c satisfying $6|c$. In this case suppose $c = 6d$.

First observe that a $(3, 2, 3, 4)$–GPF exists by Example 18. If $d = 1$ then we already have a $(3, 2, 3d, 4)$–GPF. Otherwise observe that a $(1, 6, d, 4)$–PMF exists by Theorem 9, and hence a $(3, 2, 3d, 4)$–GPF exists by Theorem 21. Next note that a $(2, 3, 2, 4)$–PMF exists (see Example 14). Combining a $(3, 2, 3d, 4)$–GPF and a $(2, 3, 2, 4)$–PMF using Theorem 23 we obtain a $(6, 6d, 4)$–PF, as required.

Now we can transform a $(3, 2, 3d, 4)$–GPF into a $(3, 4, 3d, 4)$–GPF by using Theorem 19 with $\lambda = 2$. In addition a $(4, 3, 2, 4)$–PMF is listed in Example 15, and hence we can obtain a $(12, 6d, 4)$–PF using Theorem 23.

4 Summary and Conclusions

We have defined a class of combinatorial objects called *Generalised Perfect Factors*, of which the previously defined Perfect Factors are a special case, and shown how to construct a large class of such objects. We have then exhibited a method for constructing Perfect Factors using these more general structures. This method enables us to construct Perfect Factors of sizes not previously known. Indeed the existence of Perfect Factors with parameters corresponding to all four of the smallest open cases listed in [3] has been established. In particular, Conjecture A has now been established for $v < 5$.

The next open case is clearly $v = 5$. To prove the necessary conditions are sufficient for the existence of PFs in this case would require the construction of PFs for the following parameter sets: $(6, 6d, 5)$, $(10, 10d, 5)$, $(12, 6d, 5)$, $(15, 15d, 5)$, $(20, 10d, 5)$, $(30, 30d, 5)$ and $(60, 30d, 5)$ (for every $d \geq 1$).

5 References

1. Etzion, T. (1988). Constructions for perfect maps and pseudo-random arrays. *IEEE Transactions on Information Theory*, **34**, 1308–1316.

2. Paterson, K.G. (?). Perfect factors in the de Bruijn graph. *Designs, Codes and Cryptography*, submitted.

3. Mitchell, C.J. (?). Constructing c-ary perfect factors. *Designs, Codes and Cryptography*, submitted.

4. Burns, J. and Mitchell, C.J. (?). Coding schemes for two-dimensional position sensing. In M. Ganley, editor, *Cryptography and Coding III*. Oxford University Press, Oxford (to appear).

5. Lempel, A. (1970). On a homomorphism of the de Bruijn graph and its application to the design of feedback shift registers. *IEEE Transactions on Computers*, **C-19**, 1204–1209.