PERFECT FACTORS FROM CYCLIC CODES AND INTERLEAVING

CHRIS J. MITCHELL* AND KENNETH G. PATERSON†

Abstract. In this paper we introduce new construction methods for Perfect Factors. These are based on the theory of cyclic codes, interleaving techniques and the Lempel homomorphism. The constructions enable us to settle the existence question for Perfect Factors for window sizes at most six.

Key words. de Bruijn sequence, de Bruijn graph, window sequence, perfect factor, cyclic code, Lempel homomorphism, interleaving

AMS subject classifications. 05C70, 05C38, 94A99, 68R10, 94A55

1. Introduction. In this paper we address the existence question for Perfect Factors. Perfect Factors, i.e. sets of uniformly long cycles whose elements are drawn from an alphabet of size c and in which every possible v-tuple (or 'window') of elements occurs exactly once, are of significance for two main reasons (apart from combinatorial interest in their own right).

- They can be used to construct Perfect Maps (or two-dimensional de Bruijn arrays), see for example, [1, 3, 10, 11], which are of practical importance in certain position-location applications.
- They are special cases of Perfect Maps themselves, and hence their existence is of significance in deciding whether Perfect Maps exist for all parameter sets satisfying certain simple necessary conditions (it has recently been established that these necessary conditions are sufficient for prime power size alphabets, [13, 14]).

It has been conjectured, [7], that the simple necessary conditions for the existence of a Perfect Factor (Lemma 1.3 below) are sufficient for all finite alphabets and for all window sizes. Work towards a proof of this conjecture has progressed along two fronts: firstly, the conjecture has been shown to be true for specific classes of alphabet size c (for every v) and secondly, the conjecture has been shown to be true for small values of v regardless of the alphabet size.

The truth of the conjecture was established by Etzion [1] for $c = 2$ and by Paterson [12] in the case where c is a prime power. Further progress was made by Mitchell, who introduced two auxiliary classes of combinatorial objects: Perfect Multi-Factors (PMFs) [7] and Generalized Perfect Factors (GPFs) [8], which can be combined in various ways to yield Perfect Factors. Powerful constructions for PMFs and GPFs have been given in [7, 8]. An important consequence of this latter work is that the existence question for any particular v can be reduced to an existence question concerning a finite number of 'small' parameter sets (see §7.1 below). In [7, 8] these ideas were used to settle the existence question for $v \leq 4$.

In this paper we continue to attack the existence question for Perfect Factors. We introduce three new construction methods for PMFs and GPFs. The first of these uses cyclic codes to construct sequences (§2), the second is based on interleaving (§3

*Department of Computer Science, Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K. (cjm@dcs.rhbnc.ac.uk).

†Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, U.K. (kp@hplb.hpl.hp.com). This author's research supported by Lloyd's of London Tercentenary Foundation whilst a Research Fellow at the Department of Mathematics, Royal Holloway, University of London.

and 4) and the third uses a generalisation of the Lempel homomorphism (§5). We show how these methods can be combined to efficiently analyse the parameter sets required to settle the existence question for $v \leq 6$ (§7). We also apply our methods to the cases $v = 7$ and $v = 8$, resolving the existence question in all but two cases.

1.1. Notation. We first set up some notation which we will use throughout the paper.

We are concerned here with c-ary periodic sequences, where by c-ary we mean sequences whose elements are drawn from the set $Z_c = \{0, 1, \ldots, c-1\}$. We refer throughout to c-ary cycles of period n, by which we mean periodic sequences $\mathbf{s} = [s_0, s_1, \ldots, s_{n-1}]$ where $s_i \in \{0, 1, \ldots, c-1\}$ for every i, $(0 \leq i < n)$. The least period of such a cycle is defined to be the least positive integer such that $s_i = s_{i+t}$ for all $0 \leq i < n$ (subscripts modulo 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 a is any integer, we write $a\mathbf{s}$ for the tuple obtained by element-wise multiplying the tuple $\mathbf{s}$ by a. 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.

If $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{t-1}$ are t cycles all of period n, and if $\mathbf{s}_i = [s_{i0}, s_{i1}, \ldots, s_{i(n-1)}]$ $(0 \leq i < t)$, then $\mathcal{I}(\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{t-1})$ denotes the t-fold interleaving of these cycles, i.e. $\mathcal{I}(\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{t-1}) = [s_{00}, s_{10}, \ldots, s_{(t-1)0}, s_{01}, s_{11}, \ldots, s_{(t-1)(n-1)}]$, a cycle of period nt.

We define the left shift operator E acting on cycles of period n as follows. The action of E on $\mathbf{s}$, denoted $E\mathbf{s}$, is the cycle whose i-th term is s_{i+1} (subscripts being computed modulo n). For $m \geq 2$, we define the action of E^m on $\mathbf{s}$ by writing $E^m\mathbf{s} = E(E^{m-1}\mathbf{s})$. For any polynomial $f(X) = \sum_{i=0}^{m} a_i X^i$ with coefficients in Z_c, we define the action of the operator $f(E)$ on $\mathbf{s}$ to be the cycle $a_0\mathbf{s} + a_1 E\mathbf{s} + \cdots + a_m E^m\mathbf{s}$.

We define a *truncation operator* operating on cycles. Let $\mathbf{s} = [s_0, s_1, \ldots, s_{nt-1}]$ be a cycle, and t be the least positive integer such that $E^t(\mathbf{s}) = \mathbf{s}$, i.e. t is the least period of $\mathbf{s}$. Then let $\mathcal{T}(\mathbf{s}) = [s_0, s_1, \ldots, s_{t-1}]$. Any cycle $\mathbf{s}$ of period n and least period t is equally well represented by the cycle $\mathcal{T}(\mathbf{s})$.

The weight of a period n cycle is defined to be the sum of its n elements evaluated in Z_c. Notice that

$$\frac{E^n - 1}{E - 1}\mathbf{s} = (E^{n-1} + \cdots + E + 1)s = [\sum_{i=0}^{n-1} s_i, \sum_{i=0}^{n-1} s_i, \ldots, \sum_{i=0}^{n-1} s_i]$$

so that $\frac{E^n-1}{E-1}\mathbf{s}$ is a constant cycle whose terms equal the weight of $\mathbf{s}$. We say that a set of period n cycles over Z_c is a *constant weight set* if each of the cycles in the set has the same weight. We define the *total weight* of the set to be the sum of the weights of the cycles in the set.

In addition, we use the notation (m, n) to represent the *Greatest Common Divisor* of m and n (given that m, n are a pair of positive integers or a pair of polynomials over some field). By convention, $(0, n) = n$.

1.2. Fundamental Definitions and Results.

1.2.1. De Bruijn Sequences. We first have:

DEFINITION 1.1. *A c-ary* de Bruijn sequence of span v *is a c-ary cycle of period c^v which contains c^v distinct v-tuples in a period of the cycle; equivalently every possible c-ary v-tuple occurs precisely once in a period of a de Bruijn sequence.*

It has long been known that c-ary span v de Bruijn sequences exist for all values of $c > 1$ and $v > 0$ (see [2] for a proof of this result and a comprehensive survey of the long and interesting history of de Bruijn sequences).

1.2.2. Perfect Factors. We next define a generalisation of de Bruijn sequences, the construction of which is the main theme of this paper.

DEFINITION 1.2. *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 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 (and hence all the cycles are distinct). Also observe that a (c^v, c, v)–PF is simply a c-ary span v de Bruijn sequence.

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. *$v < n$ (or $n = v = 1$).*

CONJECTURE 1.4. *[7, Conjecture 1.4] The conditions of Lemma 1.3 are sufficient for the existence of an (n, c, v)–PF.*

We next give a simple but useful construction for Perfect Factors.

CONSTRUCTION 1.5. *Suppose n and c are integers greater than 1, where $n | c^{n-1}$. Let A^* be the set of all c-ary cycles of period n with the property that the sum of the elements in each cycle is congruent to 1 modulo c. If $\mathbf{a}, \mathbf{a}' \in A^*$, then define $\mathbf{a} \sim \mathbf{a}'$ if and only if $\mathbf{a} = E^s \mathbf{a}'$ for some s. It is simple to see that $\sim$ is an equivalence relation on the elements of A^*, and hence define A to be a set of $\sim$-representatives from A^*.*

LEMMA 1.6. *If n, c and A are as in Construction 1.5, then A is an $(n, c, n-1)$–PF.*

Proof. Consider any c-ary $(n-1)$-tuple. It clearly occurs at position 0 in a unique cycle in A^*, and can only occur once in any cycle of A^*. Hence it occurs once within a unique cycle in A, and the result follows. □

COROLLARY 1.7. *The conditions of Lemma 1.3 are sufficient for the existence of an (n, c, v)–PF when $v = n - 1$.*

In view of the first condition in Lemma 1.3, we can assume that the prime factorisations of c and n are

$$c = \prod_{i=1}^{t} {p_i}^{r_i} \quad \text{and} \quad n = \prod_{i=1}^{t} {p_i}^{s_i}$$

where $0 \leq s_i \leq r_i v$ for each i.

We discuss next the extent to which Conjecture 1.4 is known to be true. The case where $v = 1$ is clearly trivial, and we have dealt with the case $v = n - 1$ in Corollary 1.7. The conditions of Result 1.3 are known to be sufficient when $c = 2$ [1] and when c is a power of a prime [12]. It was also proved in [12] that the conditions

of Lemma 1.3 are sufficient when $p_i^{s_i} > v$ for *every* index i. In [7] this result has been improved to establish the sufficiency of the conditions of Lemma 1.3 whenever $p_i^{s_i} > v$ for *at least one* index i:

THEOREM 1.8 (Theorem 7.1 of [7]). *An (n, c, v)–PF can be constructed for any n, c and v satisfying $v < n|c^v$ and $c > 1$, as long as $v < p^s$ and $p^s|n$ for some prime p and some positive integer s.*

This immediately implies that Conjecture 1.4 holds for $v = 2$ and that the conjecture remains open only for periods $n = \prod_{i=1}^{t} p_i{}^{s_i}$ for which $p_i^{s_i} \leq v$ for each $1 \leq i \leq t$.

The truth of Conjecture 1.4 has also been established for every c when $v \leq 4$ [8]. Certain other cases for $v = 6$ and larger composite v have recently been dealt with in [9].

1.2.3. Perfect Multi-Factors. We define a related set of combinatorial objects, first introduced in [7].

DEFINITION 1.9. *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 $\mathbf{t}$ 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 a PMF contains c^v/m cycles (each of period 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.

REMARK 1.10. *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.*

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

LEMMA 1.11 ([7]). *Suppose A is an (m, n, c, v)–PMF. Then*

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

(ii) $v < mn$ (or $m = 1$ and $v = n$).

It has been conjectured in [7] that the above necessary conditions are sufficient for the existence of a Perfect Multi-Factor. The following result establishes the existence conjecture whenever $n \geq v$ (and in particular for the special case $m = 1$).

THEOREM 1.12 ([7]). *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 $m|c^v$.*

We next show how an established construction technique can be used to produce Perfect Multi-Factors. A slightly different formulation of the following method was previously given as Construction E in [8].

CONSTRUCTION 1.13. *Suppose c, d, σ, τ, μ are positive integers where $c \geq 2$ and $d \geq 2$, and let*

$$A = \{\mathbf{a}_i : 0 \leq i < \sigma\}$$

be a set of σ c-ary cycles of period μ, and

$$B = \{\mathbf{b}_i : 0 \leq i < \tau\}$$

be a set of τ d-ary cycles also of period μ. Now let

$$C = \{\mathbf{s}_{ij} : 0 \leq i < \sigma,\ 0 \leq j < \tau\}$$

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

$$\mathbf{s}_{ij} = \mathbf{a}_i + c\mathbf{b}_j .$$

THEOREM 1.14. *Suppose c, d, σ, τ, μ, A and B satisfy the conditions of Construction 1.13. Suppose also that, for some $v \geq 1$, A is an (m, n, c, v)–PMF and B is a $(1, mn, d, v)$–PMF. If C is derived from A and B (with $\sigma = c^v/m$, $\tau = d^v$ and $\mu = mn$) using Construction 1.13, then C is an (m, n, cd, v)–PMF.*

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

$$\mathbf{t} = \mathbf{u} + c\mathbf{w}.$$

Now suppose $0 \leq i < n$; then we need to show that $\mathbf{t}$ occurs at a position congruent to i modulo n in some cycle of C. Now, since A is an (m, n, c, v)–PMF, $\mathbf{u}$ occurs at a position congruent to i modulo n in some cycle of A; say $\mathbf{s}$ occurs at position $i + \ell n$ in cycle $\mathbf{a}_j$ for some ℓ and j. In addition, since B is a $(1, mn, d, v)$–PMF, $\mathbf{t}$ occurs at position $i + \ell n$ in some cycle, say $\mathbf{b}_k$, of A'. It is then immediate to see that $\mathbf{t}$ occurs at position $i + \ell n$ in $\mathbf{s}_{jk}$, and the result follows. □

Next observe that, by Theorem 1.12, a $(1, mn, d, v)$–PMF exists whenever $mn \geq v$, and hence by combining Theorem 1.14 with Theorem 6.5 of [7], we have:

THEOREM 1.15. *Suppose there exists an (m, n, c, v)–PMF. Then, for every $\beta \geq 1$ and every $d \geq 1$, there exists an $(m, \beta n, cd, v)$–PMF, given that $(\beta, m) = 1$.*

1.2.4. Generalised Perfect Factors. We now define yet another class of combinatorial objects, the definition of which is a generalisation of the notion of Perfect Factor (as is the definition of PMF). We subsequently use these objects to help construct new Perfect Factors.

DEFINITION 1.16. *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 $\mathbf{t}$, there exists an integer j in the range $0 \leq j < m$ such that for every i $(0 \leq i < n)$ $\mathbf{t}$ occurs at position $j + im$ in one of these cycles.*

Note that, because a GPF contains exactly c^v/m cycles (each '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 1.17. *It should be clear that*

(i) an $(m, 1, c, v)$–GPF is precisely equivalent to an (m, c, v)–PF, and

(ii) 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 1.18 ([8]). *Suppose A is an (m, n, c, v)–GPF, where $(m, n) = 1$. Then A is also an (m, n, c, v)–PMF.*

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

LEMMA 1.19 ([8]). *Suppose A is an (m, n, c, v)–GPF. Then*

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

(ii) $v < mn$ (or $m = 1$ and $v = n$).

It is tempting at this point to conjecture that the necessary conditions specified in Lemma 1.19 for the existence of an (m, n, c, v)–GPF are sufficient. However, as

established in [8], this is not true. Nevertheless we do have the following (constructive) existence results for GPFs.

THEOREM 1.20 ([8], Theorems 19 and 21). *Suppose there exists an (m, n, c, v)–GPF. Then, for every $\lambda \geq 1$ and every $d \geq 1$, there exists an $(m, \lambda n, cd, v)$–GPF.*

This result provides a useful analogue to Theorem 1.15.

We also have the following result, which we use repeatedly below.

THEOREM 1.21 (Theorem 16 of [8]). *Suppose m, n, c and v are positive integers satisfying $m|c^v$ and $c \geq 2$, and*

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

is a set of c-ary cycles of least periods $\ell_0, \ell_1, \ldots, \ell_{t-1}$ respectively, with the property that $m|\ell_i|mn$ for every i, $0 \leq i < t$, and with the property that every c-ary v-tuple occurs precisely once in the set of cycles. Then, for every i $(0 \leq i < t)$ let $\mathbf{w}_i$ be defined as $\mathbf{a}_i$ concatenated with itself mn/ℓ_i times. Next let

$$\mathbf{b}_{ij} = \mathbf{E}^{jm}(\mathbf{w}_i)$$

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

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

Then B is an (m, n, c, v)–GPF.

We next observe that Construction 1.13 can also be used to produce new GPFs:

THEOREM 1.22. *Suppose c, d, σ, τ, μ, A and B satisfy the conditions of Construction 1.13. Suppose also that, for some $v \geq 1$, A is an (m_1, n_1, c, v)–GPF and B is an (m_2, n_2, d, v)–GPF, where $m_1 n_1 = m_2 n_2$ and $(m_1, m_2) = 1$ (and hence $m_2|n_1$). If C is derived from A and B (with $\sigma = c^v/m_1$, $\tau = d^v/m_2$ and $\mu = m_1 n_1 = m_2 n_2$) using Construction 1.13, then C is an $(m_1 m_2, n_1/m_2, cd, v)$–GPF.*

Proof. Suppose $\mathbf{t}$ is a (cd)-ary v-tuple. We need to exhibit an integer j with $0 \leq j < m_1 m_2$ such that for every i $(0 \leq i < n_1/m_2)$, $\mathbf{t}$ occurs at position $j + im_1 m_2$ in one of the cycles $\mathbf{s}_{ij}$ of C. Let $\mathbf{u} = \mathbf{t} \bmod c$, and let $\mathbf{w} = (\mathbf{t} - \mathbf{u})/c$. Then $\mathbf{u}$ is a c-ary v-tuple and $\mathbf{w}$ is a d-ary v-tuple and we have

$$\mathbf{t} = \mathbf{u} + c\mathbf{w}.$$

Now there exists an integer j_1 with $0 \leq j_1 < m_1$ such that for every i $(0 \leq i < n_1)$, $\mathbf{u}$ occurs at position $j_1 + im_1$ in a cycle of A. There also exists an integer j_2 with $0 \leq j_2 < m_2$ such that for every i $(0 \leq i < n_2)$, $\mathbf{w}$ occurs at position $j_2 + im_2$ in a cycle of B. Since $(m_1, m_2) = 1$, by the Chinese Remainder Theorem there is a unique j with $0 \leq j < m_1 m_2$ that satisfies the pair of congruences:

$$\begin{aligned} j &\equiv j_1 \pmod{m_1} \\ j &\equiv j_2 \pmod{m_2}. \end{aligned}$$

Suppose i with $0 \leq i < n_1/m_2$ is fixed. It is certainly true that there is a cycle $\mathbf{a}_i \in A$ and a cycle $\mathbf{b}_j \in B$ such that $\mathbf{u}$ appears in $\mathbf{a}_i$ and $\mathbf{w}$ appears in $\mathbf{b}_j$ at position $j + im_1 m_2$. The v-tuple $\mathbf{t}$ then appears at position $j + im_1 m_2$ in the cycle $\mathbf{s}_{ij}$. It follows that the set of cycles C forms an $(m_1 m_2, n_1/m_2, cd, v)$–GPF. □

REMARK 1.23. *Observe that, in the case $m_2 = n_1$ (and hence $m_1 = n_2$ and the constructed GPF is actually a PF), by Theorem 1.18 the above result coincides with Theorem 23 of [8].*

1.3. Using PMFs and GPFs to construct Perfect Factors. We conclude these introductory remarks by showing how PMFs and GPFs can be used to construct Perfect Factors. We start with an existence result for Perfect Factors from [8] (Theorem 23). This result, which derives from a simple application of Construction 1.13, is central to the work in this paper.

THEOREM 1.24. *Suppose there exists an (ν, μ, c, v)–GPF and a (μ, ν, d, v)–PMF. Then there exists a $(\mu\nu, cd, v)$–PF.*

Now, from Remark 1.17(i) and Theorem 1.20, it should be clear that if there exists an (n, c, v)–PF then we can construct an (n, m, c, v)–GPF for every positive integer m. Combining this observation with Theorem 1.24 we obtain as an immediate corollary the following result, first given as Theorem 5.2 of [7].

THEOREM 1.25. *If there exists an (n, c, v)–PF and an (m, n, d, v)–PMF then there exists an (mn, cd, v)–PF.*

Since, by Theorem 1.12, a $(1, n, d, v)$–PMF exists for every n, d and v ($n \geq v$ and $d > 1$), we immediately have:

COROLLARY 1.26. *If there exists an (n, c, v)–PF then there exists an (n, cd, v)–PF for every $d \geq 1$.*

2. Sequence Sets from Cyclic Codes. In this section we will give constructions for GPFs and PMFs that are based on the theory of cyclic codes. We refer to [6, Chapter 7] for the necessary background information that we assume here.

Throughout, we assume that n is an integer and p is a prime with $n = p^l s$, $(p, s) = 1$. We work with p-ary cycles and codes of length n. We define a cyclic code of length n over Z_p to be an ideal C in the ring $Z_p[X]/(X^n - 1)$. This ring is a principal ideal domain and so C has a generator g. We can associate with g a polynomial $g(X) \in Z_p[X]$ with $\deg g(X) \leq n$ and $g(X) | X^n - 1$. Let $k = \deg g(X)$. We can then write

$$C = \{c(X)g(X) \bmod X^n - 1 : c(X) \in Z_p[X], \deg c(X) < n - k\}.$$

and regard C as a set of polynomials of degree at most $n - 1$. The code C is a linear code with dimension $n - k$. We can associate with each polynomial $a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ the p-ary n-tuple $\mathbf{a} = [a_0, a_1, \ldots, a_{n-1}]$. We call the set of tuples obtained from the elements of C in this way the codewords of C. We can regard the codewords as a set of cycles. Then it is easy to see that the action of E on a cycle is equivalent to that of multiplication of the corresponding polynomial by $X^{n-1} \bmod X^n - 1$. Notice also that the weight of a cycle $\mathbf{a}$ is equal to $a(1)$, the value of $a(X)$ evaluated at 1.

We need to examine the tuples appearing in the cycles obtained from C. Because of the linearity of C, there is a $(n - k) \times n$ matrix G (called the generator matrix of C) such that every codeword of C is a linear combination of the rows of G. We can assume that G is of the form $[I_{n-k} | A]$ where I_{n-k} denotes the $(n-k) \times (n-k)$ identity matrix and A is an $(n - k) \times k$ matrix. Thus if the $n - k$ values $a_0, a_1, \ldots, a_{n-k-1}$ are specified, then there is a unique n-tuple $\mathbf{a} = [a_0, a_1, \ldots, a_{n-k-1}, a_{n-k}, \ldots, a_{n-1}]$ such that $\mathbf{a} \in C$. This shows that every p-ary $(n - k)$-tuple occurs exactly once in position zero of a codeword of C. Since the set C is closed under cyclic shifting, the same is true of any position i with $0 \leq i < n$. This immediately shows that the set of cycles obtained from any cyclic code C form a $(1, n, p, n - k)$–PMF.

2.1. Some Preliminaries. We will use cosets of cyclic codes to obtain GPFs and PMFs. The coset of C defined by polynomial $b(X)$ is defined to be the set $C + b(X)$ (addition modulo $X^n - 1$). We have the following lemmas:

LEMMA 2.1. *Let C be a length n cyclic code with generator polynomial $g(X)$. Then the coset $C + b(X)$ is closed under cyclic shifting by all multiples of t positions if and only if $a(X)g(X) \equiv b(X)(X^t - 1) \pmod{X^n - 1}$ for some $a(X)$.*

Proof. The elements of $C + b(X)$ are the polynomials $c(x)g(X) + b(X)$, where $\deg c(X) < n - k$, and a set S of polynomials is closed under cyclic shifting by all multiples of t positions if and only if $X^t S \equiv S \pmod{X^n - 1}$. Now $X^t(c(X)g(X) + b(X)) = X^t c(X)g(X) + X^t b(X)$ lies in $C + b(X)$ if and only if $X^t b(X) \equiv a(X)g(X) + b(X) \pmod{X^n - 1}$ for some polynomial $a(X)$, which in turn is equivalent to writing $b(X)(X^t - 1) \equiv a(X)g(X) \pmod{X^n - 1}$. □

LEMMA 2.2. *Suppose that $r \leq l$ and that for every t with $t|n$ and $(t, p^l)|p^{r-1}$, we have that the polynomial*

$$\left(g(X), \frac{X^n - 1}{X^t - 1}\right)$$

does not divide $b(X)$. Then every cycle derived from the coset $C + b(X)$ has least period divisible by p^r.

Proof. Suppose that the condition in the statement of the lemma holds. Then for any t with $t|n$ and $(t, p^l)|p^{r-1}$, we have that $(g(X), \frac{X^n-1}{X^t-1})$ does not divide the polynomial $c(X)g(X) + b(X)$ for any $c(X)$. Hence, for every $s(X) \in C + b(X)$, $((X^t - 1)g(X), X^n - 1)$ does not divide $s(X)(X^t - 1)$. Hence

$$s(X)(X^t - 1) \neq 0 \bmod X^n - 1, \quad \text{for every } s(X) \in C + b(X).$$

It follows from this that no cycle from $C + b(X)$ has least period divisible by t. Since every such cycle has least period dividing $n = p^l s$, we deduce that p^r must divide the period of every cycle from $C + b(X)$. □

LEMMA 2.3. *Suppose that, for every t with $t|n$ $(t \neq n)$, the polynomial*

$$\left(g(X), \frac{X^n - 1}{X^t - 1}\right)$$

does not divide $b(X)$. Then every cycle derived from the coset $C + b(X)$ has least period n.

Proof. Using exactly the same argument as in the proof of Lemma 2.2, no cycle from $C + b(X)$ has least period divisible by t for any $t|n$ $(t \neq n)$. But every cycle has least period dividing n and the lemma follows. □

2.2. A Cyclic Code Construction for GPFs. We now have a construction for GPFs:

CONSTRUCTION 2.4. *Let n be an integer and p a prime with $n = p^l s$, $(p, s) = 1$. Suppose $1 \leq r \leq l$. Let $g(X)$ be a polynomial of degree k in $Z_p[X]$ with $g(X)|X^n - 1$ and suppose $X - 1$ divides $g(X)$ exactly λ times, where $1 \leq \lambda \leq p^l - p^{r-1}$. Let C denote the length n p-ary code with generator polynomial $g(X)$. Let $b(X) = g(X)/(X - 1)$ and define $S = C + b(X)$. We regard S as a set of p-ary cycles of period n. Define an equivalence relation $\sim$ on S by writing $\mathbf{x} \sim \mathbf{y}$ if and only if $\mathbf{x} = E^t(\mathbf{y})$ for some t. Let R be a set of $\sim$-class representatives. Finally, let $A = \{\mathcal{T}(\mathbf{a}) : \mathbf{a} \in R\}$.*

THEOREM 2.5. *Let A be constructed as in Construction 2.4. Then A is a collection of cycles such that*

- *every p-ary $(n - k)$-tuple occurs exactly once in a cycle of A,*
- *every cycle of A has a least period t satisfying $p^r|t|n$.*

The result of applying Theorem 1.21 to A is a $(p^r, n/p^r, p, n-k)$–GPF in which each cycle has weight equal to $b(1)$.

Proof. Define $g(X)$ and the sets S and A as in Construction 2.4. Notice that each cycle in S has weight equal to $c(1)g(1) + b(1)$ for some polynomial $c(X)$. But $g(1) = 0$ (because $X - 1 | g(X)$), so S has constant weight equal to $b(1)$.

Suppose $t|n$ and $(t, p^l)|p^{r-1}$. Then in $Z_p[X]$, $X^t - 1$ is divisible by $X - 1$ at most p^{r-1} times, while $X^n - 1$ is divisible by $X - 1$ exactly p^l times. It follows that the polynomial $(g(X), \frac{X^n-1}{X^t-1})$ is divisible by $X-1$ exactly λ times. But $b(X) = g(X)/X-1$ is divisible by $X-1$ exactly $\lambda-1$ times, so $(g(X), \frac{X^n-1}{X^t-1})$ does not divide $b(X)$. From Lemma 2.2, each cycle in S has least period divisible by p^r. Therefore the cycles in A all have periods that are divisible by p^r.

We also know that every $(n-k)$-tuple appears exactly once in position 0 of some cycle derived from the code C, and so the same is true of $S = C + b(X)$. Moreover, because of the choice for $b(X)$, by Lemma 2.1 S is closed under cyclic shifting. It follows that the $(n-k)$-tuples occurring in a cycle $\mathbf{a}$ of R are exactly the $(n-k)$-tuples that occur in position 0 of the cycles in the $\sim$-class containing $\mathbf{a}$. Thus the set A, derived from R by truncation, has the property that every p-ary $(n-k)$-tuple occurs exactly once as a subsequence of a cycle in A.

Theorem 1.21 guarantees that A can be used to produce a $(p^r, n/p^r, p, n-k)$–GPF. Each cycle of this GPF is obtained from a cycle of A by concatenation and shifting, and so in fact is a cycle of S. Since the cycles of S all have weight $b(1)$, so do the cycles of the GPF. □

The parameters of the GPFs that can be obtained from Construction 2.4 depend heavily on the degrees of the factors of $X^n - 1$ in $Z_p[X]$ (since we require a degree k polynomial $g(X)$ with $X - 1 | g(X) | X^n - 1$). The complete factorisation of $X^n - 1$ in $Z_p[X]$ is known [5, Theorems 2.45 and 2.47]: if $n = p^l s$ with $(s, p) = 1$, then $X^n - 1 = (X^s - 1)^{p^l}$ and

$$X^s - 1 = \prod_{d|s} C_d(X)$$

where $C_d(X)$ of degree $\phi(d)$ is the *d-th cyclotomic polynomial over $Z_p[X]$*. The polynomial $C_d(X)$ has $\phi(d)/e$ irreducible factors of degree e, where e is the least positive integer such that $p^e \equiv 1 \bmod d$.

EXAMPLE 2.6. *We aim to construct a $(2,3,2,3)$–GPF and a $(3,2,3,3)$–GPF. By Theorem 1.22, if these are combined using Construction 1.13, then we obtain a $(6,6,3)$–PF.*

We take $n = 6$, $p = 2$ and find that $X^6 - 1 = (X+1)^2(X^2+X+1)^2$ in $Z_2[X]$. We take $r = 1$ and $g(X) = (X+1)(X^2+X+1)$ in Construction 2.4 to obtain a $(2,3,2,3)$–GPF in which each cycle has weight 1.

Similarly, $X^6 - 1 = (X-1)^3(X+1)^3$ in $Z_3[X]$. We take $r = 1$ and $g(X) = (X-1)(X+1)^2$ in Construction 2.4 to obtain a $(3,2,3,3)$–GPF in which each cycle has weight 1.

Combining these two GPFs using Construction 1.13, we obtain a $(6,6,3)$–PF.

We now have the following theorem, whose proof gives a constructive method for obtaining Perfect Factors having prime window size v. This theorem will be useful when we come to analyze parameter sets for small v in §7.

THEOREM 2.7. *Suppose that p is a prime with $p|c$ and p divides n exactly once. Suppose further that the parameters (n, c, p) satisfy the necessary conditions of Lemma*

1.3. Finally suppose that for some prime q with $q|(n/p)$, we have $p \equiv 1 \pmod{q}$. Then there exists an (n, c, p)–PF.

Proof. Let n, c and p be as above. We aim to use Construction 2.4 to obtain a $(p, n/p, p, p)$–GPF.

Consider the factorisation of $X^n - 1$ in $Z_p[X]$. Because q satisfies $p \equiv 1 \pmod{q}$, the q-th cyclotomic polynomial $C_q(X)$ over $Z_p[X]$ has $q - 1 \geq 1$ linear factors. Let $X - \alpha$, $\alpha \neq 1$, be one of these. Since $q \geq 2$ divides n/p, $C_1(X)C_q(X)$ divides $X^{n/p} - 1$. We deduce that $X^n - 1 = (X-1)^p(X-\alpha)^p h(X)$ for some polynomial $h(X)$ where $(X - 1, h(X)) = 1$. We take

$$g(X) = \frac{(X^n - 1)}{(X-1)^{p-1}(X-\alpha)}$$

so that $X - 1$ divides $g(X)$ exactly once and $g(X)$ has degree equal to $n - p$. Taking $\ell = r = 1$ in Construction 2.4, we can obtain a GPF with parameters $(p, n/p, p, p)$.

Now because the parameters (n, c, p) satisfy the necessary conditions of Lemma 1.3 and p divides n exactly once, we have $(n/p)|(c/p)^p$. We can use Theorem 1.12 to deduce that there exists an $(n/p, p, c/p, p)$–PMF. Combining this PMF and the GPF constructed above using Theorem 1.24, we obtain an (n, c, v)–PF. □

2.3. A Cyclic Code Construction for PMFs. We now have a corresponding code construction for PMFs:

CONSTRUCTION 2.8. *Let n, p and r be non-negative integers where p is prime, $n > 0$ and $p^r|n$. Let $b(X), g(X) \in Z_p[X]$ ($g(X)|X^n - 1$ and $g(X)$ of degree k), and suppose:*

(i) $g(X)|b(X)(X^{n/p^r} - 1)$, and

(ii) $(g(X), \frac{X^n-1}{X^t-1})$ does not divide $b(X)$ for any $t|n$ $(t \neq n)$.

Let C denote the length n p-ary code with generator polynomial $g(X)$, and define $S = C + b(X)$. We regard S as a set of p-ary cycles of period n. Finally define an equivalence relation $\sim$ on S by writing $\mathbf{x} \sim \mathbf{y}$ if and only if $\mathbf{x} = E^{un/p^r}(\mathbf{y})$ for some integer u, and let A be a set of $\sim$-class representatives.

THEOREM 2.9. *Let A be constructed as in Construction 2.8. Then A is a $(p^r, n/p^r, p, n-k)$–PMF.*

Proof. Define $g(X)$ and the sets S and A as in Construction 2.8.

By Lemma 2.3, condition (ii) of the construction immediately implies that each cycle in A has least period n.

We also know that, for every i $(1 \leq i < n)$, every $(n-k)$-tuple appears exactly once in position i of some cycle derived from the code C, and so the same is true of $S = C + b(X)$. Moreover, because of the choice for $b(X)$, Lemma 2.1 implies that S is closed under cyclic shifting by multiples of n/p^r positions. Thus, for every i $(1 \leq i < n/p^r)$ every $(n-k)$-tuple appears exactly once at a position congruent to i modulo n/p^r in some cycle from the set A.

The result now follows. □

As previously, the parameters of the PMFs that Construction 2.8 allows us to obtain depend heavily on the degrees of the factors of $X^n - 1$ in $Z_p[X]$ (since we require a degree k polynomial $g(X)$ with $g(X)|X^n - 1$).

EXAMPLE 2.10. *We aim to construct a $(2, 3, 2, 4)$–PMF and a $(3, 2, 3, 4)$–GPF. By Theorem 1.24, these can be combined to obtain a $(6, 6, 4)$–PF.*

Using Construction 2.8, we take $r = 1$, $n = 6$, $p = 2$ and find that $X^6 - 1 = (X+1)^2(X^2+X+1)^2$ in $Z_2[X]$. We take $b(X) = 1$ and $g(X) = (X^2 + X + 1)$ to obtain a $(2, 3, 2, 4)$–PMF.

Now, $X^6 - 1 = (X-1)^3(X+1)^3$ in $Z_3[X]$. We take $r = 1$ and $g(X) = (X-1)(X+1)$ in Construction 2.4 to obtain a $(3,2,3,4)$–GPF.

Applying Theorem 1.24, we obtain a $(6,6,4)$–PF.

3. An Interleaving Construction for Perfect Multi-Factors. We now describe a method for constructing Perfect Multi-Factors by interleaving the cycles of a (smaller) Perfect Factor. We subsequently use this construction method to help construct Perfect Factors with 'new' parameters.

3.1. The Construction Method. CONSTRUCTION 3.1. *Suppose c, n, t and v are positive integers where $c \geq 2$ and $t \geq 2$, and let $A = \{\mathbf{a}_i : 0 \leq i < c^v/n\}$ be an (n,c,v)–PF.*

Now define a set B containing c^{tv}/n c-ary cycles of period nt by

$$B = \{\mathbf{b_{ij}} : \mathbf{i} = (i_0, i_1, \ldots, i_{t-1}),\ (0 \leq i_s < c^v/n);\ \mathbf{j} = (j_0, j_1, \ldots, j_{t-2}),\ (0 \leq j_s < n)\}$$

where

$$\mathbf{b_{ij}} = \mathcal{I}(\mathbf{a}_{i_0}, E^{j_0}\mathbf{a}_{i_1}, \ldots, E^{j_{t-2}}\mathbf{a}_{i_{t-1}}).$$

We then have the following result.

THEOREM 3.2. *Suppose c, n, t, v and A satisfy the conditions of Construction 3.1. If B is constructed from A using Construction 3.1, then B is an (n,t,c,tv)–PMF.*

Proof. Suppose $\mathbf{y}$ is any c-ary tv-tuple, and choose any r with $0 \leq r < t$. We need to show that $\mathbf{y}$ occurs at a position congruent to r modulo t in a cycle of B.

First let

$$\mathbf{y} = \mathcal{I}(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{t-1})$$

where $\mathbf{x}_u$ is a c-ary v-tuple for every u. Now, $\mathbf{y}$ occurs at position $r + st$ in $\mathbf{b_{ij}}$ (for some $s, \mathbf{i}$ and $\mathbf{j}$) if and only if

$$\mathbf{x}_u \text{ occurs at position } \begin{cases} s \\ s+1 \\ s+1 \end{cases} \text{ in } \begin{cases} E^{j_{u+r-1}}\mathbf{a}_{i_{u+r}} & \text{if } 0 \leq u < t-r \\ \mathbf{a}_{i_0} & \text{if } u = t-r \\ E^{j_{u+r-1-t}}\mathbf{a}_{i_{u+r-t}} & \text{if } t-r+1 \leq u < t \end{cases}$$

Now, since A is an (n,c,v)–PF, there exists a unique pair of values (s, i_0) for which $\mathbf{x}_{t-r}$ occurs at position $s+1$ in $\mathbf{a}_{i_0}$. Given this value of s, then there exist unique pairs of values: (j_{u+r-1}, i_{u+r}) for which

$$\mathbf{x}_u \text{ occurs at position } s \text{ in } E^{j_{u+r-1}}\mathbf{a}_{i_{u+r}}, \quad (0 \leq u < t-r),$$

and also there exist unique pairs of values: $(j_{u+r-1-t}, i_{u+r-t})$ for which

$$\mathbf{x}_u \text{ occurs at position } s+1 \text{ in } E^{j_{u+r-1-t}}\mathbf{a}_{i_{u+r-t}}, \quad (t-r+1 \leq u < t).$$

Thus $\mathbf{y}$ occurs at a position congruent to r modulo t in a unique cycle of B, and hence B is a (n,t,c,tv)–PMF. □

EXAMPLE 3.3. *Let A be the following set of five 5-ary cycles of period 5, which constitute a $(5,5,2)$–PF.*

$$\mathbf{a}_0 = [0\,0\,1\,3\,1], \mathbf{a}_1 = [1\,1\,2\,4\,2], \mathbf{a}_2 = [2\,2\,3\,0\,3], \mathbf{a}_3 = [3\,3\,4\,1\,4], \mathbf{a}_4 = [4\,4\,0\,2\,0].$$

Then, by applying Construction 3.1 with $t = 2$ we obtain the following $(5, 2, 5, 4)$–PMF (a set of 125 cycles of period 10 in which every 5-ary 4-tuple occurs at positions congruent to 0 and 1 modulo 2).

$$\mathbf{b}_{(00)(0)} = [0\,0\,0\,0\,1\,1\,3\,3\,1\,1], \mathbf{b}_{(00)(1)} = [0\,0\,0\,1\,1\,3\,3\,1\,1\,0], \mathbf{b}_{(00)(2)} = [0\,1\,0\,3\,1\,1\,3\,0\,1\,0],$$
$$\mathbf{b}_{(00)(3)} = [0\,3\,0\,1\,1\,0\,3\,0\,1\,1], \mathbf{b}_{(00)(4)} = [0\,1\,0\,0\,1\,0\,3\,1\,1\,3],$$
$$\mathbf{b}_{(01)(0)} = [0\,1\,0\,1\,1\,2\,3\,4\,1\,2], \mathbf{b}_{(01)(1)} = [0\,1\,0\,2\,1\,4\,3\,2\,1\,1], \mathbf{b}_{(01)(2)} = [0\,2\,0\,4\,1\,2\,3\,1\,1\,1],$$
$$\mathbf{b}_{(01)(3)} = [0\,4\,0\,2\,1\,1\,3\,1\,1\,2], \mathbf{b}_{(01)(4)} = [0\,2\,0\,1\,1\,1\,3\,2\,1\,4],$$
$$\mathbf{b}_{(02)(0)} = [0\,2\,0\,2\,1\,3\,3\,0\,1\,3], \mathbf{b}_{(02)(1)} = [0\,2\,0\,3\,1\,0\,3\,3\,1\,2], \mathbf{b}_{(02)(2)} = [0\,3\,0\,0\,1\,3\,3\,2\,1\,2],$$
$$\mathbf{b}_{(02)(3)} = [0\,0\,0\,3\,1\,2\,3\,2\,1\,3], \mathbf{b}_{(02)(4)} = [0\,3\,0\,2\,1\,2\,3\,3\,1\,0],$$
$$\mathbf{b}_{(03)(0)} = [0\,3\,0\,3\,1\,4\,3\,1\,1\,4], \mathbf{b}_{(03)(1)} = [0\,3\,0\,4\,1\,1\,3\,4\,1\,3], \mathbf{b}_{(03)(2)} = [0\,4\,0\,1\,1\,4\,3\,3\,1\,3],$$
$$\mathbf{b}_{(03)(3)} = [0\,1\,0\,4\,1\,3\,3\,3\,1\,4], \mathbf{b}_{(03)(4)} = [0\,4\,0\,3\,1\,3\,3\,4\,1\,1],$$
$$\mathbf{b}_{(04)(0)} = [0\,4\,0\,4\,1\,0\,3\,2\,1\,0], \mathbf{b}_{(04)(1)} = [0\,4\,0\,0\,1\,2\,3\,0\,1\,4], \mathbf{b}_{(04)(2)} = [0\,0\,0\,2\,1\,0\,3\,4\,1\,4],$$
$$\mathbf{b}_{(04)(3)} = [0\,2\,0\,0\,1\,4\,3\,4\,1\,0], \mathbf{b}_{(04)(4)} = [0\,0\,0\,4\,1\,4\,3\,0\,1\,2],$$
$$\mathbf{b}_{(10)(0)} = [1\,0\,1\,0\,2\,1\,4\,3\,2\,1], \mathbf{b}_{(10)(1)} = [1\,0\,1\,1\,2\,3\,4\,1\,2\,0], \mathbf{b}_{(10)(2)} = [1\,1\,1\,3\,2\,1\,4\,0\,2\,0],$$
$$\mathbf{b}_{(10)(3)} = [1\,3\,1\,1\,2\,0\,4\,0\,2\,1], \mathbf{b}_{(10)(4)} = [1\,1\,1\,0\,2\,0\,4\,1\,2\,3],$$
$$\mathbf{b}_{(11)(0)} = [1\,1\,1\,1\,2\,2\,4\,4\,2\,2], \mathbf{b}_{(11)(1)} = [1\,1\,1\,2\,2\,4\,4\,2\,2\,1], \mathbf{b}_{(11)(2)} = [1\,2\,1\,4\,2\,2\,4\,1\,2\,1],$$
$$\mathbf{b}_{(11)(3)} = [1\,4\,1\,2\,2\,1\,4\,1\,2\,2], \mathbf{b}_{(11)(4)} = [1\,2\,1\,1\,2\,1\,4\,2\,2\,4],$$
$$\mathbf{b}_{(12)(0)} = [1\,2\,1\,2\,2\,3\,4\,0\,2\,3], \mathbf{b}_{(12)(1)} = [1\,2\,1\,3\,2\,0\,4\,3\,2\,2], \mathbf{b}_{(12)(2)} = [1\,3\,1\,0\,2\,3\,4\,2\,2\,2],$$
$$\mathbf{b}_{(12)(3)} = [1\,0\,1\,3\,2\,2\,4\,2\,2\,3], \mathbf{b}_{(12)(4)} = [1\,3\,1\,2\,2\,2\,4\,3\,2\,0],$$
$$\mathbf{b}_{(13)(0)} = [1\,3\,1\,3\,2\,4\,4\,1\,2\,4], \mathbf{b}_{(13)(1)} = [1\,3\,1\,4\,2\,1\,4\,4\,2\,3], \mathbf{b}_{(13)(2)} = [1\,4\,1\,1\,2\,4\,4\,3\,2\,3],$$
$$\mathbf{b}_{(13)(3)} = [1\,1\,1\,4\,2\,3\,4\,3\,2\,4], \mathbf{b}_{(13)(4)} = [1\,4\,1\,3\,2\,3\,4\,4\,2\,1],$$
$$\mathbf{b}_{(14)(0)} = [1\,4\,1\,4\,2\,0\,4\,2\,2\,0], \mathbf{b}_{(14)(1)} = [1\,4\,1\,0\,2\,2\,4\,0\,2\,4], \mathbf{b}_{(14)(2)} = [1\,0\,1\,2\,2\,0\,4\,4\,2\,4],$$
$$\mathbf{b}_{(14)(3)} = [1\,2\,1\,0\,2\,4\,4\,4\,2\,0], \mathbf{b}_{(14)(4)} = [1\,0\,1\,4\,2\,4\,4\,0\,2\,2],$$
$$\mathbf{b}_{(20)(0)} = [2\,0\,2\,0\,3\,1\,0\,3\,3\,1], \mathbf{b}_{(20)(1)} = [2\,0\,2\,1\,3\,3\,0\,1\,3\,0], \mathbf{b}_{(20)(2)} = [2\,1\,2\,3\,3\,1\,0\,0\,3\,0],$$
$$\mathbf{b}_{(20)(3)} = [2\,3\,2\,1\,3\,0\,0\,0\,3\,1], \mathbf{b}_{(20)(4)} = [2\,1\,2\,0\,3\,0\,0\,1\,3\,3],$$
$$\mathbf{b}_{(21)(0)} = [2\,1\,2\,1\,3\,2\,0\,4\,3\,2], \mathbf{b}_{(21)(1)} = [2\,1\,2\,2\,3\,4\,0\,2\,3\,1], \mathbf{b}_{(21)(2)} = [2\,2\,2\,4\,3\,2\,0\,1\,3\,1],$$
$$\mathbf{b}_{(21)(3)} = [2\,4\,2\,2\,3\,1\,0\,1\,3\,2], \mathbf{b}_{(21)(4)} = [2\,2\,2\,1\,3\,1\,0\,2\,3\,4],$$
$$\mathbf{b}_{(22)(0)} = [2\,2\,2\,2\,3\,3\,0\,0\,3\,3], \mathbf{b}_{(22)(1)} = [2\,2\,2\,3\,3\,0\,0\,3\,3\,2], \mathbf{b}_{(22)(2)} = [2\,3\,2\,0\,3\,3\,0\,2\,3\,2],$$
$$\mathbf{b}_{(22)(3)} = [2\,0\,2\,3\,3\,2\,0\,2\,3\,3], \mathbf{b}_{(22)(4)} = [2\,3\,2\,2\,3\,2\,0\,3\,3\,0],$$
$$\mathbf{b}_{(23)(0)} = [2\,3\,2\,3\,3\,4\,0\,1\,3\,4], \mathbf{b}_{(23)(1)} = [2\,3\,2\,4\,3\,1\,0\,4\,3\,3], \mathbf{b}_{(23)(2)} = [2\,4\,2\,1\,3\,4\,0\,3\,3\,3],$$
$$\mathbf{b}_{(23)(3)} = [2\,1\,2\,4\,3\,3\,0\,3\,3\,4], \mathbf{b}_{(23)(4)} = [2\,4\,2\,3\,3\,3\,0\,4\,3\,1],$$
$$\mathbf{b}_{(24)(0)} = [2\,4\,2\,4\,3\,0\,0\,2\,3\,0], \mathbf{b}_{(24)(1)} = [2\,4\,2\,0\,3\,2\,0\,0\,3\,4], \mathbf{b}_{(24)(2)} = [2\,0\,2\,2\,3\,0\,0\,4\,3\,4],$$
$$\mathbf{b}_{(24)(3)} = [2\,2\,2\,0\,3\,4\,0\,4\,3\,0], \mathbf{b}_{(24)(4)} = [2\,0\,2\,4\,3\,4\,0\,0\,3\,2],$$
$$\mathbf{b}_{(30)(0)} = [3\,0\,3\,0\,4\,1\,1\,3\,4\,1], \mathbf{b}_{(30)(1)} = [3\,0\,3\,1\,4\,3\,1\,1\,4\,0], \mathbf{b}_{(30)(2)} = [3\,1\,3\,3\,4\,1\,1\,0\,4\,0],$$
$$\mathbf{b}_{(30)(3)} = [3\,3\,3\,1\,4\,0\,1\,0\,4\,1], \mathbf{b}_{(30)(4)} = [3\,1\,3\,0\,4\,0\,1\,1\,4\,3],$$
$$\mathbf{b}_{(31)(0)} = [3\,1\,3\,1\,4\,2\,1\,4\,4\,2], \mathbf{b}_{(31)(1)} = [3\,1\,3\,2\,4\,4\,1\,2\,4\,1], \mathbf{b}_{(31)(2)} = [3\,2\,3\,4\,4\,2\,1\,1\,4\,1],$$
$$\mathbf{b}_{(31)(3)} = [3\,4\,3\,2\,4\,1\,1\,1\,4\,2], \mathbf{b}_{(31)(4)} = [3\,2\,3\,1\,4\,1\,1\,2\,4\,4],$$
$$\mathbf{b}_{(32)(0)} = [3\,2\,3\,2\,4\,3\,1\,0\,4\,3], \mathbf{b}_{(32)(1)} = [3\,2\,3\,3\,4\,0\,1\,3\,4\,2], \mathbf{b}_{(32)(2)} = [3\,3\,3\,0\,4\,3\,1\,2\,4\,2],$$
$$\mathbf{b}_{(32)(3)} = [3\,0\,3\,3\,4\,2\,1\,2\,4\,3], \mathbf{b}_{(32)(4)} = [3\,3\,3\,2\,4\,2\,1\,3\,4\,0],$$
$$\mathbf{b}_{(33)(0)} = [3\,3\,3\,3\,4\,4\,1\,1\,4\,4], \mathbf{b}_{(33)(1)} = [3\,3\,3\,4\,4\,1\,1\,4\,4\,3], \mathbf{b}_{(33)(2)} = [3\,4\,3\,1\,4\,4\,1\,3\,4\,3],$$
$$\mathbf{b}_{(33)(3)} = [3\,1\,3\,4\,4\,3\,1\,3\,4\,4], \mathbf{b}_{(33)(4)} = [3\,4\,3\,3\,4\,3\,1\,4\,4\,1],$$
$$\mathbf{b}_{(34)(0)} = [3\,4\,3\,4\,4\,0\,1\,2\,4\,0], \mathbf{b}_{(34)(1)} = [3\,4\,3\,0\,4\,2\,1\,0\,4\,4], \mathbf{b}_{(34)(2)} = [3\,0\,3\,2\,4\,0\,1\,4\,4\,4],$$
$$\mathbf{b}_{(34)(3)} = [3\,2\,3\,0\,4\,4\,1\,4\,4\,0], \mathbf{b}_{(34)(4)} = [3\,0\,3\,4\,4\,4\,1\,0\,4\,2],$$
$$\mathbf{b}_{(40)(0)} = [4\,0\,4\,0\,0\,1\,2\,3\,0\,1], \mathbf{b}_{(40)(1)} = [4\,0\,4\,1\,0\,3\,2\,1\,0\,0], \mathbf{b}_{(40)(2)} = [4\,1\,4\,3\,0\,1\,2\,0\,0\,0],$$
$$\mathbf{b}_{(40)(3)} = [4\,3\,4\,1\,0\,0\,2\,0\,0\,1], \mathbf{b}_{(40)(4)} = [4\,1\,4\,0\,0\,0\,2\,1\,0\,3],$$
$$\mathbf{b}_{(41)(0)} = [4\,1\,4\,1\,0\,2\,2\,4\,0\,2], \mathbf{b}_{(41)(1)} = [4\,1\,4\,2\,0\,4\,2\,2\,0\,1], \mathbf{b}_{(41)(2)} = [4\,2\,4\,4\,0\,2\,2\,1\,0\,1],$$
$$\mathbf{b}_{(41)(3)} = [4\,4\,4\,2\,0\,1\,2\,1\,0\,2], \mathbf{b}_{(41)(4)} = [4\,2\,4\,1\,0\,1\,2\,2\,0\,4],$$
$$\mathbf{b}_{(42)(0)} = [4\,2\,4\,2\,0\,3\,2\,0\,0\,3], \mathbf{b}_{(42)(1)} = [4\,2\,4\,3\,0\,0\,2\,3\,0\,2], \mathbf{b}_{(42)(2)} = [4\,3\,4\,0\,0\,3\,2\,2\,0\,2],$$
$$\mathbf{b}_{(42)(3)} = [4\,0\,4\,3\,0\,2\,2\,2\,0\,3], \mathbf{b}_{(42)(4)} = [4\,3\,4\,2\,0\,2\,2\,3\,0\,0],$$
$$\mathbf{b}_{(43)(0)} = [4\,3\,4\,3\,0\,4\,2\,1\,0\,4], \mathbf{b}_{(43)(1)} = [4\,3\,4\,4\,0\,1\,2\,4\,0\,3], \mathbf{b}_{(43)(2)} = [4\,4\,4\,1\,0\,4\,2\,3\,0\,3],$$
$$\mathbf{b}_{(43)(3)} = [4\,1\,4\,4\,0\,3\,2\,3\,0\,4], \mathbf{b}_{(43)(4)} = [4\,4\,4\,3\,0\,3\,2\,4\,0\,1],$$
$$\mathbf{b}_{(44)(0)} = [4\,4\,4\,4\,0\,0\,2\,2\,0\,0], \mathbf{b}_{(44)(1)} = [4\,4\,4\,0\,0\,2\,2\,0\,0\,4], \mathbf{b}_{(44)(2)} = [4\,0\,4\,2\,0\,0\,2\,4\,0\,4],$$
$$\mathbf{b}_{(44)(3)} = [4\,2\,4\,0\,0\,4\,2\,4\,0\,0], \mathbf{b}_{(44)(4)} = [4\,0\,4\,4\,0\,4\,2\,0\,0\,2],$$

4. An Interleaving Construction for GPFs. We now describe a method which enables us to construct many new GPFs; it is similar to Construction 3.1, and is actually a generalisation of Construction 3.1 of [9].

4.1. The Construction Method. CONSTRUCTION 4.1. *Suppose c, n, t, v are positive integers where $c \geq 2$. Suppose also that*

$$A = \{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{c^v/n-1}\}$$

is an (n, c, v)–PF. Consider the set S of all n-ary cycles $\mathbf{x} = [x_0, x_1, \ldots, x_{t-1}]$ with the property that

$$\sum_{i=0}^{t-1} x_i \equiv 1 \pmod{n}.$$

If $\mathbf{x}, \mathbf{y} \in S$ *then write* $\mathbf{x} \sim \mathbf{y}$ *if and only if* $\mathbf{x} = E^i(\mathbf{y})$ *for some* i. *It is simple to verify that* $\sim$ *is an equivalence relation on* S *which partitions* S *into* q *classes say. Now let*

$$X = \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{q-1}\}$$

be a set of $\sim$*-class representatives. Next let*

$$A^t = \{(\mathbf{a}_{i_0}, \mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_{t-1}}) \ : \ \mathbf{a}_{i_0}, \mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_{t-1}} \in A\}$$

be the set of all t*-tuples of elements of* A. *Now define* B' *to be the collection of all cycles of the form*

$$\mathcal{I}(E^0\mathbf{a}_{i_0}, E^{x_0}\mathbf{a}_{i_1}, E^{x_0+x_1}\mathbf{a}_{i_2}, \ldots, E^{x_0+x_1+\cdots+x_{t-2}}\mathbf{a}_{i_{t-1}}),$$

where $(x_0, x_1, \ldots, x_{t-1}) \in X$ *and* $(\mathbf{a}_{i_0}, \mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_{t-1}}) \in A^t$. *Hence* $|B'| = qc^{tv}/n^t$.

Finally put $B = \{\mathcal{I}(\mathbf{z}) \ : \ \mathbf{z} \in B'\}$. *Note that whilst* B' *may contain duplicate cycles,* B *(defined as a set) will not, i.e. duplicates are discarded.*

We can now state and prove the following result.

THEOREM 4.2. *Suppose* c, n, t, v *and* A *satisfy the conditions of Construction 4.1. If* B *is constructed from* A *using Construction 4.1 then* B *is a collection of cycles with the property that every* c*-ary* (tv)*-tuple occurs exactly once in a cycle of* B. *Every cycle* $\mathbf{b} \in B$ *has least period* $\ell_{\mathbf{b}}n$, *for some positive integer* $\ell_{\mathbf{b}}$ *satisfying* $\ell_{\mathbf{b}}|t$ *and* $(\frac{t}{\ell_{\mathbf{b}}}, n) = 1$.

Proof. Suppose $\mathbf{y}$ is any c-ary (tv)-tuple. We first show that $\mathbf{y}$ occurs in one of the cycles of B'. Suppose

$$\mathbf{y} = \mathcal{I}(\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{t-1})$$

where $\mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_{t-1}$ are c-ary t-tuples. Now suppose that $\mathbf{z}_i$ occurs in cycle $\mathbf{a}_{\ell_i}$ at position k_i, for every i satisfying $0 \le i < t$. In addition we define a further n-ary t-tuple $\mathbf{x} = (x_0, x_1, \ldots, x_{t-1})$ where $x_i \equiv k_{i+1} - k_i \pmod n$, for every i satisfying $0 \le i < t-1$, and $x_{t-1} \equiv k_0 - k_{t-1} + 1 \pmod n$. First observe that $\mathbf{x} \in S$, since

$$\sum_{i=0}^{t-1} x_i \equiv \sum_{i=0}^{t-2}(k_{i+1} - k_i) + (k_0 - k_{t-1} + 1) \equiv 1 \pmod n.$$

Hence there exists some cyclic shift of $\mathbf{x}$, say

$$E^u(\mathbf{x}) = (x_u, x_{u+1}, \ldots, x_{t-1}, x_0, \ldots, x_{u-1}),$$

which is a member of X. Hence if we define the n-ary t-tuple $(v_0, v_1, \ldots, v_{t-1})$ by

$$v_i = \begin{cases} 0 & \text{if } i = 0 \\ \sum_{j=u}^{i+u-1} x_j \bmod n & \text{(subscripts modulo } t\text{) if } 0 < i \le t-1 \end{cases}$$

then the following cycle is a member of B':

$$\mathbf{w} = \mathcal{I}(E^{v_0}\mathbf{a}_{\ell_u}, E^{v_1}\mathbf{a}_{\ell_{u+1}}, \ldots, E^{v_{t-u-1}}\mathbf{a}_{\ell_{t-1}}, E^{v_{t-u}}\mathbf{a}_{\ell_0}, \ldots, E^{v_{t-1}}\mathbf{a}_{\ell_{u-1}}).$$

Now $\mathbf{z}_{u+i}$ occurs in $E^{v_i}(\mathbf{a}_{\ell_{u+i}})$ at position $k_{u+i} - v_i$, $(0 \le i < t-u)$, and z_i occurs in $E^{v_i+t-u}(\mathbf{a}_{\ell_i})$ at position $k_i - v_{t-u+i}$, $(0 \le i \le u-1)$, where positions are calculated modulo n. By definition of $\mathbf{x}$ we also have

$$v_i = \begin{cases} 0 & \text{if } i = 0 \\ k_{u+i} - k_u \bmod n & \text{if } 0 < i < t-u \\ k_{u-t+i} - k_u + 1 \bmod n & \text{if } t-u \le i \le t-1 \end{cases}$$

Thus $\mathbf{z}_{u+i}$ occurs in $E^{v_i}(\mathbf{a}_{\ell_{u+i}})$ at position k_u, $(0 \leq i < t-u)$, and $\mathbf{z}_i$ occurs in $E^{v_i+t-u}(\mathbf{a}_{\ell_i})$ at position k_u+1, $(0 \leq i \leq u-1)$. Hence $\mathbf{y}$ occurs in $\mathbf{w}$ at position $k_u t - u$.

Now since a (tv)-tuple $\mathbf{y}$ occurs in a cycle of B', it follows (from the way in which B was derived from B') that $\mathbf{y}$ must occur in a cycle of B. Next suppose that $\mathbf{y}$ occurs at two different points in the cycles of B'. Now, because A is a PF, $\mathbf{y}$ can only arise from one $(t-1)$-tuple of 'relative shifts' and one t-tuple from A^t. Hence $\mathbf{y}$ can only arise twice if the same $(t-1)$-tuple of relative shifts occurs twice in the same element of X (the same $(t-1)$-tuple of relative shifts cannot arise in different elements of X since X contains a unique element from each equivalence class under $\sim$ and this class is uniquely determined by a $(t-1)$-tuple of relative shifts). That is, the same (tv)-tuple can only occur multiple times in two ways:

- within the same cycle of B', or
- in two distinct cycles of B' generated by the same set of relative shifts $\mathbf{x}$ and by two different cyclic shifts of the same t-tuple of elements of A.

In both cases this can only happen when the t-tuple of relative shifts used to derive the cycle(s) ($\mathbf{x}$ say) satisfies $\mathbf{x} = E^i\mathbf{x}$ for some i $(0 < i < t)$. The second case is rather easier to deal with, since in this case the resulting cycles of B' will be identical to one another (except for a cyclic shift). Hence the duplication will be removed when B is derived from B'. We therefore need only consider the first case. If the same (tv)-tuple occurs twice within the same cycle $\mathbf{b}$ of B', say at positions i and j, then we must have $E^i\mathbf{b} = E^j\mathbf{b}$, and hence the (tv)-tuple will *not* be repeated within $\mathcal{T}(\mathbf{b})$. Hence all the (tv)-tuples in the cycles of B are distinct.

We next consider the possible periods of the cycles in B. Suppose $\mathbf{b} = E^i\mathbf{b}$ for some i $(0 < i \leq nt)$. Note that we must have $i|nt$. Suppose also that $i' = i \bmod t$, and hence if $\mathbf{x} \in X$ is used to produce $\mathbf{b}$, then $\mathbf{x} = E^{i'}\mathbf{x}$ and so $i'|t$. Now, by definition of S, if $\mathbf{x} = [x_0, x_1, \ldots, x_{t-1}]$ then $\sum_{j=0}^{t-1} x_j \equiv 1 \bmod n$, and hence, since $\mathbf{x} = E^{i'}(\mathbf{x})$, we have

$$(\frac{t}{i'}) \sum_{j=0}^{i'-1} x_j \equiv 1 \pmod{n}.$$

Note that this implies that $(t/i', n) = 1$ and also that $(\sum_{j=0}^{i'-1} x_j, n) = 1$.

Now, since $i'|t$ and $i \equiv i' \pmod{t}$, it follows that $i'|i$, say $i = \nu i'$. Hence, since $\mathbf{b} = E^i\mathbf{b}$, we have

$$\nu \sum_{j=0}^{i'-1} x_j \equiv 0 \pmod{n}$$

(this follows since the total relative shift at a displacement of i in $\mathbf{b}$ must be zero). But we have already observed that $(\sum_{j=0}^{i'-1} x_j, n) = 1$, and hence we must have $n|\nu$. Hence $ni'|i$ and $(t/i', n) = 1$. Since we have already observed that $i|nt$, the desired result on the periods of cycles in B follows. □

When we combine the above result with Theorem 1.21, we immediately have:

COROLLARY 4.3. *If an (n, c, v)–PF exists, then there exists a (n, t, c, tv)–GPF for every positive integer t.*

REMARK 4.4. *In fact the cycles of the GPF in this corollary can be derived directly from the cycles in the set B' of Construction 4.1 merely by discarding duplicate cycles from the set (that is, without truncating cycles as in the derivation of B from B').*

This means that each cycle in the GPF is obtained by t-fold interleaving of the cycles of the (n, c, v)–PF.

REMARK 4.5. *It is straightforward to see that $n|t^{n-1}$ if and only if $(t/\ell, n) \neq 1$ for every factor ℓ of t (except for $\ell = t$). Hence if $n|t^{n-1}$, then Construction 4.1 yields a set B of cycles of period exactly nt (in fact $B = B'$), and hence B is an (nt, c, tv)–PF. This corresponds to Construction 3.1 of [9].*

4.2. Examples. EXAMPLE 4.6. *Let A be the $(5, 5, 1)$–PF consisting of the single cycle $[01234]$. Then, to apply Construction 4.1 to this cycle with $t = 3$, we first need to define*

$$X = \{[001], [024], [033], [042], [114], [123], [132], [222], [344]\}.$$

Using this choice for X we then obtain the following set B of nine cycles (of periods 15 and 5) in which every 5-ary 3-tuple occurs exactly once.

$$\begin{array}{lll} [0\,0\,0\,1\,1\,1\,2\,2\,2\,3\,3\,3\,4\,4\,4], & [0\,0\,2\,1\,1\,3\,2\,2\,4\,3\,3\,0\,4\,4\,1], & [0\,0\,3\,1\,1\,4\,2\,2\,0\,3\,3\,1\,4\,4\,2], \\ [0\,0\,4\,1\,1\,0\,2\,2\,1\,3\,3\,2\,4\,4\,3], & [0\,1\,2\,1\,2\,3\,2\,3\,4\,3\,4\,0\,4\,0\,1], & [0\,1\,3\,1\,2\,4\,2\,3\,0\,3\,4\,1\,4\,0\,2], \\ [0\,1\,4\,1\,2\,0\,2\,3\,1\,3\,4\,2\,4\,0\,3], & [0\,2\,4\,1\,3], & [0\,3\,2\,1\,4\,3\,2\,0\,4\,3\,1\,0\,4\,2\,1]. \end{array}$$

Using Theorem 1.21, the set B can be used to produce a $(5, 3, 5, 3)$–GPF.

EXAMPLE 4.7. *Let A be the following set of five 5-ary cycles of period 5, which constitute a $(5, 5, 2)$–PF.*

$$\mathbf{a}_0 = [0\,0\,1\,3\,1], \mathbf{a}_1 = [1\,1\,2\,4\,2], \mathbf{a}_2 = [2\,2\,3\,0\,3], \mathbf{a}_3 = [3\,3\,4\,1\,4], \mathbf{a}_4 = [4\,4\,0\,2\,0].$$

Put $t = 2$ and

$$X = \{[33], [01], [42]\}.$$

In the table below, we give the set of 65 cycles resulting from applying Construction 4.1 to A with $t = 2$. In each row we give the three cycles obtained by applying the three 'shift tuples' of X to a pair of interleaved cycles from A, with indices as marked at the start of the row. Note that the 10 duplicate cycles (which do not count as part of the 65 cycles) are preceded with an asterisk, and arise when the representative from X has cyclic symmetry. Five of the cycles have period 5 and sixty have period 10, and hence we can use these cycles to produce a $(5, 2, 5, 4)$–GPF.

	[33]	[01]	[42]
00	[03011]	[0000113311]	[0100103113]
01	[0402113112],	[0101123412],	[0201113214],
02	[0003123213],	[0202133013],	[0302123310],
03	[0104133314],	[0303143114],	[0403133411],
04	[0200143410],	[0404103210],	[0004143012],
10	*[1311204021],	[1010214321],	[1110204123],
11	[14122],	[1111224022],	[1211214224],
12	[1013224223],	[1212234023],	[1312224320],
13	[1114234324],	[1313244124],	[1413234421],
14	[1210244420],	[1414204220],	[1014244022],
20	*[2321300031],	[2020310331],	[2120300133],
21	*[2422310132],	[2121320032],	[2221310230],
22	[20233],	[2222330033],	[2322320330],
23	[2124330334],	[2323340134],	[2423330431],
24	[2220340430],	[2424300230],	[2024340032],
30	*[3331401041],	[3030411341],	[3130401143],
31	*[3432411142],	[3131421442],	[3231411244],
32	*[3033421243],	[3232431043],	[3332421340],
33	[31344],	[3333441144],	[3433431441],
34	[3230441440],	[3434401240],	[3034441042],
40	*[4341002001],	[4040012301],	[4140002103],
41	*[4442012102],	[4141022402],	[4241012204],
42	*[4043022203],	[4242032003],	[4342022300],
43	*[4144032304],	[4343042104],	[4443032401],
44	[42400],	[4444002200],	[4044042002].

5. The Lempel Homomorphism and the Construction of PMFs and GPFs. The Lempel homomorphism [4] (and its generalisation to arbitrary finite fields), has been very widely applied in the construction of de Bruijn sequences [4], Perfect Factors [1, 12] and Perfect Maps [13]. We now briefly show how it can be applied to the construction of PMFs and GPFs over alphabets Z_c.

5.1. The Lempel Homomorphism. We first define a version of the Lempel homomorphism on c-ary cycles, where the elements of the c-ary alphabet are taken as the integers modulo c.

DEFINITION 5.1. *We define the Lempel homomorphism D acting on c-ary cycles to be the operator $E-1$ (we will usually write $E-1$ for D). Thus if c, n are positive integers ($c > 1$), and $\mathbf{a} = [a_0, a_1, \ldots, a_{n-1}]$ is a c-ary cycle of period n, then $D\mathbf{a}$ is the following c-ary cycle of period n:*

$$[a_1 - a_0, a_2 - a_1, \ldots, a_{n-1} - a_{n-2}, a_0 - a_{n-1}],$$

where the arithmetic is computed modulo c.

DEFINITION 5.2. *Suppose c, n are positive integers ($c > 1$), and let*

$$\mathbf{a} = [a_0, a_1, \ldots, a_{n-1}]$$

be a c-ary cycle of period n and weight w. Then we define the pre-image *of* $\mathbf{a}$ *under D, denoted* $D^{-1}\mathbf{a}$ *or* $(E-1)^{-1}\mathbf{a}$*, to be the following set of* (w,c) *c-ary cycles of period* $nc/(w,c)$*:*

$$\{[s, s+a_0, s+a_0+a_1, \ldots, s+\sum_{i=0}^{n-2} a_i, s+w, s+w+a_0, s+w+a_0+a_1, \ldots,$$
$$s+w+\sum_{i=0}^{n-2} a_i, s+2w, \ldots, s+(c/(w,c)-1)w+\sum_{i=0}^{n-2} a_i] \ : \ 0 \le s < (w,c)\}.$$

Clearly, $\mathbf{a} \in D^{-1}D\mathbf{a}$ *for any cycle* $\mathbf{a}$*. We call the operator* $(E-1)^{-1}$ *the* Lempel inverse homomorphism (LIH)*.*

Of course, given a cycle $\mathbf{a}$ as in the above definition, we can apply $(E-1)^{-1}$ to the set $(E-1)^{-1}\mathbf{a}$ to obtain a second set of cycles, which we denote by $(E-1)^{-2}\mathbf{a}$. Notice that the cycles of this set need not all have the same period (because the cycles in $(E-1)^{-1}\mathbf{a}$ need not all have the same weight). We can continue in this way and write $(E-1)^{-k}\mathbf{a}$ for the set of cycles obtained by making k applications of $(E-1)^{-1}$ to $\mathbf{a}$.

We also need to define the action of the Lempel homomorphism and its inverse on c-ary tuples. For convenience we also denote these mappings by D and D^{-1} (the domain of the mapping should always be clear from the context).

DEFINITION 5.3. *Suppose* c, v *are positive integers* $(c > 1)$*, and let*

$$\mathbf{s} = (s_0, s_1, \ldots, s_{v-1})$$

be a c-ary v-tuple. Then define $D\mathbf{s}$ *to be the following c-ary* $(v-1)$*-tuple:*

$$(s_1 - s_0, s_2 - s_1, \ldots, s_{t-1} - s_{t-2}).$$

On the other hand if $\mathbf{w} = (w_0, w_1, \ldots, w_{v-2})$ *is a c-ary* $(v-1)$*-tuple, then we define* $D^{-1}\mathbf{w}$ *to be the following c-set of c-ary v-tuples:*

$$D^{-1}\mathbf{w} = \{(s, s+w_0, s+w_0+w_1, \ldots, s+\sum_{i=0}^{v-2} w_i) : s \in Z_c\}.$$

We will also use $E-1$ *and* $(E-1)^{-1}$ *to denote* D *and* D^{-1} *acting on c-ary tuples.*

We can now state the following result which follows immediately from the definitions:

LEMMA 5.4. *Let* $\mathbf{a}$ *be a c-ary cycle of period n,* $\mathbf{s}$ *a c-ary v-tuple and* $\mathbf{w}$ *a c-ary* $(v-1)$*-tuple. Then*

- $D\mathbf{s} = \mathbf{w}$ *if and only if* $\mathbf{s} \in D^{-1}\mathbf{w}$*,*
- *if* $\mathbf{s}$ *appears in* $\mathbf{a}$ *at position p, then* $D\mathbf{s}$ *appears in* $D\mathbf{a}$ *at position p, and*
- *if* $\mathbf{s}$ *appears in* $\mathbf{a}$ *at position p, then any* $(v+1)$*-tuple of* $D^{-1}\mathbf{s}$ *appears in some cycle of* $(E-1)^{-1}\mathbf{a}$ *at a position* p' *with* $p' \equiv p \bmod n$*.*

We use the following construction method, which is based on the Lempel inverse homomorphism, to construct Perfect Factors, PMFs and GPFs.

CONSTRUCTION 5.5. *Suppose* c, r *are positive integers, where* $c > 1$*, and let* A *be a set of c-ary cycles*

$$\{\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{t-1}\}$$

of periods $\ell_0, \ell_1, \ldots, \ell_{t-1}$ *and weights* $w_0, w_1, \ldots, w_{t-1}$ *respectively. Then let* B *be the following set of* $\sum_{i=0}^{t-1}(w_i, c)$ *cycles:*

$$B = \bigcup_{i=0}^{t-1} (E-1)^{-1}\mathbf{a}_i.$$

We now have:

THEOREM 5.6. *Suppose* c, m, n, v *are positive integers* ($c > 1$)*, and let* A *be a set of* c*-ary cycles of constant weight* w*. Suppose also that* B *is derived from* A *using Construction 5.5. Then*

- *if* A *is an* (n, c, v)*–PF, then* B *is a* $(nc/(w, c), c, v + 1)$*–PF,*
- *if* A *is an* (m, n, c, v)*–PMF, then* B *is a* $(mc/(w, c), n, c, v + 1)$*–PMF, and*
- *if* A *is an* (m, n, c, v)*–GPF, then* B *is a* $(mc/(w, c), n, c, v + 1)$*–GPF.*

Proof. This follows immediately from the definition of the Lempel inverse homomorphism and Lemma 5.4. □

By considering the special case where $w = 0$, we immediately have:

COROLLARY 5.7. *Suppose* c, m, n, v *are positive integers* ($c > 1$)*, and let* A *be a set of* c*-ary cycles of constant weight zero. Suppose also that* B *is derived from* A *using Construction 5.5. Then*

- *if* A *is an* (n, c, v)*–PF, then* B *is a* $(n, c, v + 1)$*–PF,*
- *if* A *is an* (m, n, c, v)*–PMF then* B *is a* $(m, n, c, v + 1)$*–PMF, and*
- *if* A *is an* (m, n, c, v)*–GPF then* B *is a* $(m, n, c, v + 1)$*–GPF.*

Of course, if the set of cycles B in Theorem 5.6 or Corollary 5.7 has constant weight, then Construction 5.5 can be applied again to B to produce a new set of cycles which will again form a Perfect Factor/PMF/GPF. This process can be repeated to produce a series of Perfect Factors/PMFs/GPFs with increasing window size, so long as the cycles in each set all have the same weight. In the next section we will see how the interleaving constructions of §3 and 4 can be combined with repeated use of Construction 5.5 to produce a powerful set of construction methods.

5.2. Examples. EXAMPLE 5.8. *The* $(5, 2, 5, 4)$*–PMF constructed in Example 3.3 has constant weight zero. Hence, if we apply Construction 5.5 then, by Corollary 5.7, we obtain a* $(5, 2, 5, 5)$*–PMF.*

EXAMPLE 5.9. *The* $(5, 2, 5, 4)$*–GPF constructed in Example 4.7 has constant weight zero. Hence, if we apply Construction 5.5 then, by Corollary 5.7, we obtain a* $(5, 2, 5, 5)$*–GPF.*

6. Combining Interleaving and the Lempel Homomorphism. Consider applying one of Constructions 3.1 or 4.1 to an (n, c, v)–PF A. The resulting set of cycles B will be either a (n, t, c, tv)–PMF, a (n, t, c, tv)–GPF or a (tn, c, tv)–PF. We ask: what is the maximum number of times that Construction 5.5 can be applied to the cycles of B whilst yielding a set of cycles of period tn? In order for the construction to be applicable δ times, we require that the set

$$\{(E-1)^{-(\delta-1)}\mathbf{b}, \mathbf{b} \in B\}$$

be constant weight zero. By repeated use of Corollary 5.7, it follows that if δ applications are possible whilst maintaining zero weight, then we can obtain either an $(n, t, c, tv + \delta)$–PMF, an $(n, t, c, tv + \delta)$–GPF or a $(tn, c, tv + \delta)$–PF.

The answer to our question depends on the maximum value of k such that the set

$$\{(E-1)^{-k}\mathbf{a}, \mathbf{a} \in A\}$$

is constant weight, as well as on the prime factorisations of t and c. Before giving the answer, we need some preliminary results.

LEMMA 6.1. *Suppose that c does not divide t. Then in $Z_c[E]$, $E-1$ divides E^t-1 exactly once.*

Proof. In $Z_c[E]$, we have $E^t - 1 = (E-1)g_t(E)$ where

$$g_t(E) := E^{t-1} + E^{t-2} + \cdots + E + 1$$

satisfies $g_t(1) = t$. When c does not divide t, we have $g_t(1) \neq 0 \bmod c$ and so $E-1$ does not divide $g_t(E)$. The lemma follows. □

LEMMA 6.2. *Suppose that c is square-free (i.e. c is a product of distinct primes). Let $t = \prod_i {p_i}^{\beta_i}$ and $c = \prod_i {p_i}^{\alpha_i}$, where $\beta_i \geq 0$ and $\alpha_i = 0$ or 1, be the prime factorisations of t and c. Then in $Z_c[E]$, $E-1$ divides E^t-1 exactly $\delta_{t,c}$ times, where*

$$\delta_{t,c} = \min_{\alpha_i=1} \left\{ {p_i}^{\beta_i} \right\}$$

Proof. Consider first the case where c is a prime p and $t = p^\beta$. Then in $Z_p[E]$,

$$E^t - 1 = E^{p^\beta} - 1 = (E-1)^{p^\beta}$$

since $\binom{p^\beta}{i} = 0 \bmod p$ for $1 \leq i \leq p^\beta - 1$. So in this case, $E-1$ divides E^t-1 exactly $t = p^\beta$ times.

Now let t and c have prime factorisations as in the statement of the lemma. Suppose $\alpha_i = 1$. Then in $Z_{p_i}[E]$,

$$E^t - 1 = (E^{{p_i}^{\beta_i}} - 1)(E^{(\ell-1){p_i}^{\beta_i}} + \cdots + E^{{p_i}^{\beta_i}} + 1)$$

where $\ell = t/{p_i}^{\beta_i}$ is coprime to p_i. So in $Z_{p_i}[E]$,

$$E^t - 1 = (E-1)^{{p_i}^{\beta_i}} g_\ell(E^{{p_i}^{\beta_i}}).$$

But $g_\ell(1) = \ell \neq 0 \bmod p_i$, so we deduce that in $Z_{p_i}[E]$, $E-1$ divides E^t-1 exactly ${p_i}^{\beta_i}$ times. But, by a Chinese Remainder Theorem argument, $E-1$ divides E^t-1 at least δ times in $Z_c[E]$ if and only if it does so at least δ times over each polynomial ring $Z_{p_i}[E]$ for which p_i divides c. The result follows. □

Now suppose A is an (n,c,v)–PF and that for some $w \in \mathbf{Z}_c$, some $k \geq 0$ and for each $\mathbf{a} \in A$, any cycle in $(E-1)^{-k}\mathbf{a}$ has period n and weight w. Then each $\mathbf{a} \in A$ satisfies

$$\frac{E^n-1}{E-1}(E-1)^{-k}\ \mathbf{a} = [w, w, \ldots, w]. \tag{6.1}$$

If $w = 0$, then this means that Theorem 5.7 can be applied up to $k+1$ times to the cycles of A to produce $(n, c, v+\delta)$–PFs for each $1 \leq \delta \leq k+1$. If $w \neq 0$, then we have

$$\frac{E^n-1}{E-1}(E-1)^{-(k-1)}\ \mathbf{a} = (E-1)[w, w, \ldots, w] = [0, 0, \ldots, 0]$$

and we see that up to k applications of Construction 5.5 to A are possible to produce $(n, c, v+\delta)$–PFs for each $1 \leq \delta \leq k$. Theorem 5.6 guarantees that a final application of Construction 5.5 can be used to yield a $(nc/(w,c), c, v+k+1)$–PF.

Now let B be obtained from A by t-fold interleaving, either as in Construction 3.1 (to obtain a PMF) or as in Construction 4.1 combined with Theorem 1.21 (to obtain a GPF). Then in either case (and by Remark 4.4 in the second case), each cycle of B satisfies relation (6.1) but with E replaced by E^t, i.e. if $\mathbf{b} \in B$, then

$$\frac{E^{tn}-1}{(E^t-1)^{(k+1)}}\,\mathbf{b} = [w, w, \ldots, w].$$

Writing $E^t - 1 = (E-1)^{\delta_{t,c}} h_{t,c}(E)$ where $h_{t,c}(E)$ is not divisible by $E-1$, we have, for each $\mathbf{b} \in B$:

$$\frac{E^{tn}-1}{(E-1)^{(k+1)\delta_{t,c}}} \cdot \frac{1}{h_{t,c}(E)^{k+1}}\,\mathbf{b} = [w, w, \ldots, w].$$

Multiplying by $h_{t,c}(E)^{k+1}$ and noting that $h_{t,c}(E)^{k+1}[w]$ is also a constant cycle, we see that for some w' (where $w' = 0$ if $w = 0$),

$$\frac{E^{tn}-1}{E-1} \cdot (E-1)^{-((k+1)\delta_{t,c}-1)}\,\mathbf{b} = [w', w', \ldots, w'], \qquad \mathbf{b} \in \mathbf{B}.$$

We can interpret this equation as follows. If $w' = 0$ (in particular, if $w = 0$), then the sequences of the set

$$\{(E-1)^{-((k+1)\delta_{t,c}-1)}\mathbf{b}, \mathbf{b} \in B\}$$

have zero weight and period tn, so that Construction 5.5 can be applied up to $(k+1)\delta_{t,c}$ times to the cycles of B. Similarly, if $w' \neq 0$, then Construction 5.5 can be applied up to $(k+1)\delta_{t,c} - 1$ times to the cycles of B.

We summarise with the following theorem:

THEOREM 6.3. *Suppose c is square-free. Let B be a (tn, c, tv)–PF/(n, t, c, tv)–PMF/ (n, t, c, tv)–GPF obtained from (n, c, v)–PF A by t-fold interleaving. Suppose that Construction 5.5 applied $k \geq 0$ times to the cycles of A results in cycles of period n all having weight w. We write $\ell = (k+1)\delta_{t,c}$. If $w = 0$ then Construction 5.5 can be applied up to ℓ times to the cycles of B, resulting in constant weight $(tn, c, tv+\delta)$–PFs/$(n, t, c, tv+\delta)$–PMFs/ $(n, t, c, tv+\delta)$–GPFs for each $1 \leq \delta \leq \ell$. If $w \neq 0$ then Construction 5.5 can be applied up to $\ell - 1$ times to the cycles of B, resulting in constant weight $(tn, c, tv+\delta)$–PFs/$(n, t, c, tv+\delta)$–PMFs/ $(n, t, c, tv+\delta)$–GPFs for each $1 \leq \delta \leq \ell - 1$.*

EXAMPLE 6.4. *Let A be the $(5, 5, 2)$–PF of Example 3.3. It is easy to verify that the sequences of A satisfy*

$$(E-1)^2\mathbf{a} = [1], \quad \mathbf{a} \in A.$$

Over Z_5, we have $E^5 - 1 = (E-1)^5$ and so we can write

$$\frac{E^5-1}{E-1}(E-1)^{-2}\mathbf{a} = (E-1)^2\mathbf{a} = [1], \quad \mathbf{a} \in A$$

and we can take $k = 2$ and $w = 1$ in Theorem 6.3. Applying Theorem 3.2 with $t = 2$, we can construct a $(5, 2, 5, 4)$–PMF B. Now $\delta_{2,5} = 1$, so according to Theorem 6.3,

Result 5.7 can be applied up to $l-1=2$ times to the cycles of B, resulting in a constant weight $(5,2,5,5)$–PMF and a constant weight $(5,2,5,6)$–PMF.

EXAMPLE 6.5. *The $(5,3,5,3)$–GPF constructed in Example 4.6 was obtained from the $(5,5,1)$–PF consisting of the single cycle $[01234]$. Arguing as in the above example, we can take $k=3$ and $w=1$ in Theorem 6.3 to see that Construction 5.5 can be applied up to $l-1=3$ times to the cycles of the GPF, resulting in a constant weight $(5,3,5,4)$–GPF, a constant weight $(5,3,5,5)$–GPF and a constant weight $(5,3,5,6)$–GPF.*

7. Perfect Factors for Small Windows.

7.1. A Reduction for the Existence Problem. Corollary 1.26 allows us to make an important reduction in the sets of parameters for which we need to consider the existence question for Perfect Factors.

Recall from the discussion in §1.2.2 that to prove Conjecture 1.4 for any fixed v, we need only construct Perfect Factors with parameters (n,c,v) $(n>v+1)$, where

$$c=\prod_{i=1}^{t}{p_i}^{r_i} \quad \text{and} \quad n=\prod_{i=1}^{t}{p_i}^{s_i}$$

and both $0\le s_i\le r_i v$ and ${p_i}^{s_i}\le v$ for each i.

For a particular choice of c and v as above, we write

$$c'=\prod_{s_i\neq 0} p_i.$$

Now for each i, ${p_i}^{s_i}\le v\le {p_i}^{v}$. Hence $s_i\le v$ and so $n|(c')^v$. Thus the parameters (n,c',v) satisfy the necessary conditions of Result 1.3. Moreover, by Corollary 1.26, the existence of such an (n,c',v)–PF implies the existence of a (n,c,v)–PF. So to settle Conjecture 1.4 for v, it is sufficient to construct Perfect Factors for all parameters (n,c,v) where $n>v+1$, $c=p_1\ldots p_t$ is square-free, and where $n=\prod_{i=1}^{t}{p_i}^{s_i}$ with $1\le s_i$ and ${p_i}^{s_i}\le v$ for each i.

Notice this means that every prime p_i that divides c must in turn divide n. Moreover, each p_i satisfies $p_i\le v$. So to settle the existence question for any particular v, it is sufficient to consider Perfect Factors for a finite set of alphabets (whose sizes are products of distinct primes) and for a small set of parameters for each of these alphabets.

We summarise the above reduction formally as

LEMMA 7.1. *Suppose $v\ge 1$ is fixed and that there exist (n,c,v)–PFs for every square-free $c=p_1\ldots p_t$ and every $n>v+1$ with $n=\prod_{i=1}^{t}{p_i}^{s_i}$ where $s_i\ge 1$ and ${p_i}^{s_i}\le v$ for each i. Then Conjecture 1.4 is true for v.*

REMARK 7.2. *Note that, because $v<n$, t is always at least 2 in the above lemma.*

7.2. Perfect Factors for $v\le 6$. We now show that Conjecture 1.4 is true for $v\le 6$. This has already been shown for $v\le 4$. However, in order to demonstrate the power of our new construction methods, we consider anew all v up to $v=6$.

7.2.1. Perfect Factors for $v=2$. For $v=2$, there is no parameter set satisfying the conditions of Lemma 7.1. We conclude that Conjecture 1.4 is true for $v=2$. In fact, this means that the methods of [7] are strong enough to settle the existence problem in this case, as already noted in the introductory section.

7.2.2. Perfect Factors for $v = 3$. By Lemma 7.1, we need only consider the existence of a $(6,6,3)$–PF. A Perfect Factor with these parameters was obtained in Example 2.6.

7.2.3. Perfect Factors for $v = 4$. Again by Lemma 7.1, only the following two parameter sets need to be considered: $(6,6,4)$ and $(12,6,4)$.

A PF for the first parameter set was obtained in Example 2.10. A $(12,6,4)$–PF can be obtained by applying Construction 4.1 to a $(6,6,2)$–PF with $t = 2$ (see Remark 4.5).

7.2.4. Perfect Factors for $v = 5$. By Lemma 7.1, only the following six parameter sets need to be considered:

$$(10,10,5),(12,6,5),(15,15,5),(20,10,5),(30,30,5) \text{ and } (60,30,5).$$

The parameter sets $(10,10,5)$, $(20,10,5)$, $(30,30,5)$ and $(60,30,5)$ fall to Theorem 2.7.

Consider the parameters $(12,6,5)$. The polynomial $X^{12}-1$ factorises as $(X+1)^4(X^2+X+1)^4$ in $Z_2[X]$ and as $(X-1)^3(X^3+X^2+X+1)^3$ in $Z_3[X]$. We take $g(X) = (X+1)(X^2+X+1)^3$, $p = 2$ and $r = l = 2$ in Construction 2.4 to obtain a $(4,3,2,5)$–GPF. Similarly, we take $g(X) = (X-1)(X^3+X^2+X+1)^2$, $p = 3$ and $r = l = 1$ in Construction 2.4 to obtain a $(3,4,3,5)$–GPF. Combining these GPFs using Construction 1.13, we obtain (according to Theorem 1.22) a $(12,6,5)$–PF.

Finally, consider the parameters $(15,15,5)$. By considering the factorisation of $X^{15}-1$ in $Z_3[X]$ and $\mathbf{Z}_5[X]$ and following a similar procedure to that above, we can obtain a $(15,15,5)$–PF. The polynomials $g(X)$ can be taken to be $(X-1)^2(X^4+X^3+X^2+X+1)^2$ in $Z_3[X]$ and $(X-1)^2(X^2+X+1)^4$ in $Z_5[X]$.

7.2.5. Perfect Factors for $v = 6$. By Lemma 7.1, only the following six parameter sets need to be considered:

$$(10,10,6),(12,6,6),(15,15,6),(20,10,6),(30,30,6) \text{ and } (60,30,6).$$

PFs with parameters $(12,6,6)$, $(20,10,6)$ and $(60,30,6)$ can be obtained by applying Construction 4.1 with $t = 2$ to PFs with parameters $(6,6,3)$, $(10,10,3)$ and $(30,30,3)$ respectively (c.f. §3.4 of [9]).

Consider the parameters $(10,10,6)$. A $(5,2,5,6)$–GPF can be obtained using the polynomial $(X-1)(X+1)^3$ in $Z_5[X]$. We can obtain a $(2,5,2,6)$-PMF using Construction 2.8 by taking $g(X) = X^4+X^3+X^2+X+1$ and $b(X) = 1$ in $Z_2[X]$. Combining these using Theorem 1.24, we obtain a $(10,10,6)$–PF.

A $(15,15,6)$–PF can be obtained by combining GPFs constructed using the polynomials $(X-1)(X^4+X^3+X^2+X+1)^2$ in $Z_3[X]$ and $(X-1)(X^2+X+1)^4$ in $Z_5[X]$.

Finally, consider the parameters $(30,30,6)$. It is easy to see from cyclotomic factorisations how to obtain degree 24 factors $g(X)$ of $X^{30}-1$ in each of $Z_3[X]$ and $Z_5[X]$. These can be used to construct a $(3,10,3,6)$–GPF and a $(5,6,5,6)$–GPF. Combining these using Construction 1.13, by Theorem 1.22 we obtain a $(15,2,15,6)$–GPF. By Theorem 1.12, there exists a $(2,15,2,6)$–PMF. Applying Theorem 1.24, we can obtain a $(30,30,6)$–PF.

7.3. Perfect Factors for $v = 7$ and $v = 8$. We finally consider the existence of perfect factors for $v = 7$ and $v = 8$, and in doing so list the smallest undecided cases.

By Lemma 7.1, for $v = 7$, the following 17 parameter sets need to be considered:

$$(10,10,7),\quad (12,6,7),\quad (14,14,7),\quad (15,15,7),\quad (20,10,7),\quad (21,21,7),$$
$$(28,14,7),\quad (30,30,7),\quad (35,35,7),\quad (42,42,7),\quad (60,30,7),\quad (70,70,7),$$
$$(84,42,7),\quad (105,105,7),\quad (140,70,7),\quad (210,210,7),\quad \text{and}\quad (420,210,7).$$

All these parameter sets, except $(10,10,7), (12,6,7), (15,15,7), (20,10,7), (30,30,7)$, $(35,35,7)$ and $(60,60,7)$, fall to Theorem 2.7. Constructions based on cyclic codes can be used to build PFs for six out of these seven remaining sets (we omit the details), the parameters $(10,10,7)$ resisting attack by such methods.

Similarly when $v = 8$, fourteen of the twenty-four parameter sets that remain after applying Lemma 7.1 fall to Construction 4.1 with $t = 2$. All but one of the remaining ten sets then fall to constructions based on cyclic codes. The parameter set $(10,10,8)$ remains undecided.

One reason for the difficulty with the sets $(10,10,7)$ and $(10,10,8)$ is that $X^{10}-1$ has no factors of degrees 2 or 3 in $Z_2[X]$ that are suitable for use in our cyclic code constructions. If a $(10,10,7)$–PF and a $(10,10,8)$–PF could be shown to exist, then Conjecture 1.4 would also be true for $v \leq 8$. Such PFs would contain 10^6 and 10^7 cycles of period 10, respectively, and as such appear to be out of the reach of computer search.

8. Conclusions. We have provided further evidence to support the conjecture that the necessary conditions of Lemma 1.3 are sufficient for the existence of a Perfect Factor. Indeed it is probably possible to extend our case by case analysis to cover most parameter sets for $v = 9$ and beyond.

More importantly, we have provided new and powerful construction methods which may have the potential to help establish the conjecture for general v. In this direction it may be worthwhile examining in more detail the different ways in which these methods can be combined to produce Perfect Factors. We have already done this for interleaving combined with the Lempel inverse homomorphism in §6 of this paper.

It is also worth noting that we have only used the coding-theoretic methods developed here to attack the existence question for small v. However, even for small v, these methods do have some limitations, as illustrated by our failure with parameters $(10,10,7)$ and $(10,10,8)$. Indeed, it is not hard to show that if $p \geq 5$ is prime and 2 is primitive modulo p, then $X^{2p}-1$ has factorisation $(X+1)^2(X^{p-1}+X^{p-2}+\cdots+1)^2$ in $\mathbf{Z}_2[X]$. So, in this case, $X^{2p}-1$ has no factors of degrees $2,3,\cdots,p-2$ that can be used in our cyclic code constructions. This means that the cyclic code techniques in this paper cannot be used to help construct $(2p,2p,v)$–PFs for any v with $p+2 \leq v \leq 2p-2$. These are examples of parameter sets for which no construction methods are currently known.

9. Acknowledgement. We would like to thank an anonymous referee for valuable comments.

REFERENCES

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

[2] H. Fredricksen, *A survey of full length nonlinear shift register cycle algorithms*, SIAM Review, **24** (1982), pp. 195–221.

[3] G. Hurlbert and G. Isaak, *On the de Bruijn torus problem*, J. Combin. Theory Ser. A, **64** (1993), pp. 50–62.

[4] A. Lempel, *On a homomorphism of the de Bruijn graph and its application to the design of feedback shift registers*, IEEE Trans. on Computers, **C-19** (1970), pp. 1204–1209.
[5] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986.
[6] F. MacWilliams and N. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
[7] C. Mitchell, *Constructing c-ary perfect factors*, Designs, Codes and Cryptography, **4** (1994), pp. 341–368.
[8] ———, *New c-ary perfect factors in the de Bruijn graph*, in Codes and Cyphers, P. Farrell, ed., Formara Ltd., Southend, 1995, pp. 299–313. Proceedings of the fourth IMA Conference on Cryptography and Coding, Cirencester, December 1993.
[9] ———, *De Bruijn sequences and perfect factors*, SIAM Journal on Discrete Mathematics, **10** (1997) pp. 270–281.
[10] C. Mitchell and K. Paterson, *Decoding perfect maps*, Designs, Codes and Cryptography, **4** (1994), pp. 11–30.
[11] K. Paterson, *Perfect maps*, IEEE Trans. on Inform. Theory, **40** (1994), pp. 743–753.
[12] ———, *Perfect factors in the de Bruijn graph*, Designs, Codes and Cryptography, **5** (1995), pp. 115–138.
[13] ———, *New classes of perfect maps I*, J. Combin. Theory Ser. A, **73** (1996), pp. 302–334.
[14] ———, *New classes of perfect maps II*, J. Combin. Theory Ser. A, **73** (1996), pp. 335–345.