On Higher Dimensional Perfect Factors

Glenn Hurlbert*
Department of Mathematics
Arizona State University
Tempe, AZ 85287-1804

Garth Isaak
Department of Mathematics
Lehigh University
Bethlehem, PA 18015

ABSTRACT. A d-dimensional Perfect Factor is a collection of periodic arrays in which every k-ary $(n_1 \times \cdots \times n_d)$ matrix appears appears exactly once (periodically). The one dimensional case, with a collection of size one, is known as a De Bruijn cycle. The 1- and 2-dimensional versions have proven highly applicable in areas such as coding, communications, and location sensing. Here we focus on results in higher dimensions for factors with each $n_i = 2$.

1 Introduction

A *d-dimensional k-ary, order $\vec{N}$ perfect factor of size t* and *period $\vec{R}$* (called a De Bruijn *family* in [13]) is a family $\{B_1, \ldots, B_t\}$ of d-dimensional k-ary (entries from a k element set, typically $[k] = \{0, 1, \ldots, k-1\}$) toroidal (i.e. periodic) arrays, of period $\vec{R}$ each, with the property that for every d-dimensional k-ary matrix M of order $\vec{N}$ there is a unique j and a unique $\vec{I}$ so that M appears in B_j at position $\vec{I}$. (We will say that a particular matrix M of size $\vec{N}$ *appears in B at position* $\vec{I} = \langle i_1, \ldots, i_d \rangle$ if M appears in the positions $\vec{I}$ through $\vec{I} + \vec{N}$.) We call such a perfect factor a $(\vec{R}; \vec{N}; t)_k^d$ perfect factor and denote the set of all such perfect factors by $PF_k^d(\vec{R}; \vec{N}; t)$.

In the case that $d = t = 1$, perfect factors have been called De Bruijn cycles. Perfect factors with $t = 1$ and $d > 1$ have been called de Bruijn tori

*Partially supported by NSF grant DMS-9201467.

and perfect maps. It has become clear in past work that the existence of perfect factors greatly facilitates the construction of De Bruijn tori. See [13] for more details (or [17] for the two-dimensional case). The *De Bruijn graph* $dB(n,k)$ is defined as follows. Its vertex set consists of all k-ary n-tuples, and there is a directed arc from $x_1 \ldots x_n$ to $y_1 \ldots y_n$ whenever $y_i = x_{i+1}$ for each $i < n$ (see figure 1). The term 'factor' comes from the fact that when $d = 1$ the fundamental blocks of a k-ary order n perfect factor of period r actually give rise to a factoring of the arcs of $dB(n-1,k)$ into cycles of length r, since the arcs of $dB(n-1,k)$ correspond to the vertices of $dB(n,k)$.

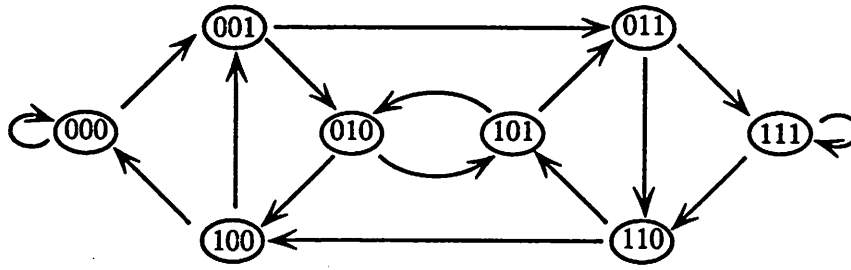

Figure 1. $dB(3,2)$

For example, $F = \{(000111),(01)\}$ factors the arcs of $dB(2,2)$ into two cycles, but they are of different lengths and so F is not a perfect factor. However, we do have that $\{(0001),(0111)\} \in PF_2^1(4;3;2)$. Likewise, if

$$A = \begin{array}{|cc|}\hline 0 & 0 \\ 0 & 1 \\ \hline \end{array} \qquad \textit{and} \qquad B = \begin{array}{|ccc|}\hline 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ \hline \end{array}$$

then every binary 2×2 matrix occurs exactly once in either A or B, exclusively. But $\{A,B\}$ is not a perfect factor since A and B are of different sizes. However, for the torus C below, we have that $C \in PF_2^2(4,4;2,2;1)$.

$$C = \begin{array}{|cccc|}\hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ \hline \end{array}$$

De Bruijn cycles were first discovered in [7] and later independently in [2] and [9] (see Frederickson [8] for a survey of De Bruijn cycles). 2-dimensional De Bruijn tori are examined in [1,4–6,11–18], among others. A 2-dimensional De Bruijn torus $(r_1,r_2;n_1,n_2;1)_k^2$ is *square* if $r_1 = r_2 = r$

and *totally square* if $n_1 = n_2 = n$ as well. It was asked in [3] whether such totally square tori exist. Except for small values of n_j, it has been shown (see [6] for $k = 2$ and [11] for general k) that the obvious necessary conditions $r > n$ and $r^2 = k^{n^2}$ are also sufficient for their existence.

We have conjectured [11] (as others have) that for general De Bruijn tori, the necessary conditions $r_j > n_j$ and $R = k^N$ ($R = \prod r_j$, $N = \prod n_j$) are also sufficient, except possibly for some "small" cases. Etzion [5] gave constructions for De Bruijn tori in $PF_2^2(2^t, 2^{n_1 n_2 - t}; n_1, n_2; 1)$ for all $n_1 < 2^t \leq 2^{n_1}$, except $n_1 = t$ and $n_2 = 2$, and for all $n_1 < 2^t \leq 2^{n_1 - 1}$ when $n_2 = 2$.

Paterson [16] finished off the 2-dimensional binary case, proving that $PF_2^2(r_1, r_2; n_1, n_2; 1) \neq \emptyset$ if and only if $r_i > n_i$ and $r_1 r_2 = 2^{n_1 n_2}$. Paterson [18] has recently extended this result to arbitrary base k, showing that the necessary conditions $r_i > n_i$ and $r_1 r_2 = k^{n_1 n_2}$ are nearly sufficient for the existence of De Bruijn tori in $PF_k^2(r_1, r_2; n_1, n_2; 1)$. His constructions miss the cases when k, r_1 and r_2 have prime factorizations $k = \prod_{j=1}^{s} p_j^{\alpha_j}$, $r_1 = \prod_{j=1}^{s} p_j^{\beta_j}$ and $r_2 = \prod_{j=1}^{s} p_j^{\gamma_j}$ with either $p_j^{\beta_j} < n_1$ or $p_j^{\gamma_j} < n_2$ for each $j \leq s$ ($PF_{30}^2(30, 30^{11}; 6, 2; 1)$ and $PF_6^2(2^9, 3^9; 3, 3; 1)$, for example).

As for the base a power of two, we proved in [12] that, for all s and t, $PF_{2st}^2(4st^2, 4s^3t^2; 2, 2; 1) \neq \emptyset$, extending the techniques of [14]. Implicitly, we proved in that paper that $PF_{2st}^2(4st, 4st; 2, 2; s^2t^2) \neq \emptyset$, which, because of the way in which we proved they could be linked together, implies that, for all $\alpha < \beta_1$, $\alpha < \beta_2$, and $\beta_1 + \beta_2 \leq 4\alpha$, we have $PF_{2^\alpha}^2(2^{\beta_1}, 2^{\beta_2}; 2, 2; 2^{4\alpha - \beta_1 - \beta_2}) \neq \emptyset$. We will use Theorem 2.1 below to improve this result to cover all the cases $1 < \beta_i$.

The purpose of this paper is to extend the methods of [13] (see also [5] and [18] for two dimensions and binary cases) in order to prove results about perfect factors in dimensions higher than two. Before we can state our main result we must first develop more notation and terminology.

We define d-dimensional vectors $\langle x \rangle^d = \langle x, \ldots, x \rangle$ and $\langle x \rangle^{\vec{\alpha}} = \langle x^{\alpha_1}, \ldots, x^{\alpha_d} \rangle$ for $\vec{\alpha} = \langle \alpha_1, \ldots, \alpha_d \rangle$.

A *fundamental block* of B is an array consisting of r_i consecutive rows in the ith dimension for each $i = 1, \ldots, d$. Repeating such a block produces B. We will sometimes refer to a fundamental block of B as B when there is no chance of confusion. Thus, we will say that a matrix appears uniquely in an infinite periodic array if it appears uniquely in a fundamental block. In this case, addition on subscripts in the i^{th} dimension is performed modulo r_i and we think of B toroidally. If $B = [b_{\vec{I}}]$ is any d-dimensional torus, the *projection of B along $i_j = h$* is the $(d-1)$-dimensional torus consisting of all entries $b_{\vec{I}}$ for which $i_j = h$.

As a necessary condition for perfect factors, we know that there are k^{N_d} k-ary d-dimensional matrices, where $N_d = \prod_{i=1}^{d} n_i$, and there are t tori

with R_d positions each for a matrix to appear, where $R_d = \prod_{i=1}^{d} r_i$, and so we must have $tR_d = k^{N_d}$. Also, if ever some $r_i = n_i$, then the all 0's matrix appears more than once (at least $r_i > 1$ times), and so we need $r_i > n_i$ for each i as well. It is believed that these conditions are also sufficient, though again "small" cases may cause difficulty. Note that the conditions above determine t from N_d and R_d, hence the notation $PF_k^d(\vec{R};\vec{N};t)$ is somewhat redundent. We include t for clarity.

Our main result is

Theorem 1.1. *Let $k = \prod_{i=1}^{s} p_i^{\alpha_i}$ for primes p_i and for $j \le d$ suppose that $r_j = \prod_{i=1}^{s} p_i^{\beta_{i,j}}$ with each $p_i^{\beta_{i,j}} > 2$. Further assume that for each $i \le s$ there is a permutation $\sigma_i = (\sigma_{i,1}, \ldots, \sigma_{i,d})$ of $\{1, \ldots, d\}$ so that for each $l \le d$ we have $\sum_{j=1}^{l} \beta_{i,\sigma_{i,j}} \le \alpha_i 2^l$. Then $PF_k^d(\vec{R};\vec{N};t) \neq \emptyset$ for $\vec{R} = \langle r_1, \ldots, r_d \rangle$, $\vec{N} = \langle 2, \ldots, 2 \rangle = \langle 2 \rangle^d$, and $t = k^{N_d}/R_d$.*

Observe that t is determined by $\vec{R}$ and $\vec{N}$ as in the previous paragraph. The goal is to determine, for given d, k, and $\vec{N}$, for which $\vec{R}$ $PF_k^d(\vec{R};\vec{N};t)$ is nonempty, so the value of t is really of no concern to us.

As an example, one can construct factors in $PF_{504}^4(2^{13}\cdot 3^5\cdot 7^3, 2^5\cdot 3^{14}\cdot 7^1, 2^5\cdot 3^1\cdot 7^8, 2^{13}\cdot 3^7\cdot 7^2; 2,2,2,2,2; t)$ where $t = (2^3\cdot 3^2\cdot 7)^{2^4}/(2^{36}\cdot 3^{27}\cdot 7^{14}) = 2^{12}\cdot 3^5\cdot 7^2$. The theorem comes from constructing perfect factors for each prime and then putting them together in a rather natural way. The role played by the permutation σ in Theorem 1.1 is to transpose the factors from, say, $PF_{3^2}^4(3^1, 3^5, 3^7, 3^{14}; 2,2,2,2; 3^5)$ to $PF_{3^2}^4(3^5, 3^{14}, 3^1, 3^7; 2,2,2,2; 3^5)$. Likewise, we construct $PF_{2^3}^4(2^5, 2^5, 2^{13}, 2^{13}; 2,2,2,2; 2^{12})$ and $PF_7^4(7^1, 7^2, 7^3, 7^8; 2,2,2,2; 7^2)$ from Lemma 3.3, below, and transpose them to $PF_{2^3}^4(2^{13}, 2^5, 2^5, 2^{13}; 2,2,2,2,2; 2^{12})$ and $PF_7^4(7^3, 7^1, 7^8, 7^2; 2,2,2,2; 7^2)$, respectively. Then Theorem 2.3, below, will combine these three perfect factors into one.

What Theorem 1.1 doesn't yield are factors near the "diagonal"; that is, with the r_i nearly equal. In fact, we cannot yet construct 3-dimensional versions of totally square tori in $PF_p^3(\langle r \rangle^d; \langle n \rangle^d; 1)$ for prime p.

2 Building Blocks

Crucial tools in our inductive construction are found in the following theorems.

Theorem 2.1. ([17]) *If p^α is a prime power and $n \ge 2$ with $n+1 \le p^\beta \le p^{\alpha n}$, then $PF_{p^\alpha}^1(p^\beta; n; p^{\alpha n - \beta}) \neq \emptyset$.* □

Let $B = [b_{\vec{I}}]$ be an infinite d-dimensional k-ary matrix, and let $B' = [b'_{\vec{I}}]$ be an infinite d-dimensional k'-ary matrix. The *term product* $B \odot B'$ is the kk'-ary matrix with entry $\vec{I}$ given by $k' b_{\vec{I}} + b'_{\vec{I}}$. In [13] we find

Theorem 2.2. *Let $\vec{R} = \langle r_1, \ldots, r_d \rangle$ and $\vec{R}' = \langle r'_1, \ldots, r'_d \rangle$ have gcd (r_j, r'_j)*

$= 1$ *for all* $j \leq d$. *If* $B \in PF_k^d(\vec{R};\vec{N};1)$ *and* $B' \in PF_{k'}^d(\vec{R}';\vec{N};1)$, *then* $(B \odot B') \in PF_{kk'}^d(\vec{R}'';\vec{N})$ *with* $\vec{R}'' = \langle r_1 r_1', \ldots, r_d r_d' \rangle$. □

It is straightforward to generalize Theorem 2.2 from De Bruijn tori to perfect factors. This yields

Theorem 2.3. *Let* $\vec{R} = \langle r_1, \ldots, r_d \rangle$ *and* $\vec{R}' = \langle r_1', \ldots, r_d' \rangle$ *have gcd* $(r_j, r_j') = 1$ *for all* $j \leq d$. *If* $\{B_1, \ldots, B_t\} \in PF_k^d(\vec{R};\vec{N};t)$ *and* $\{B_1', \ldots, B_{t'}'\} \in PF_{k'}^d(\vec{R}';\vec{N};t')$, *then* $\{B_i \odot B_j' : 1 \leq i \leq t, 1 \leq j \leq t'\} \in PF_{kk'}^d(\vec{R}'';\vec{N};t'')$ *with* $\vec{R}'' = \langle r_1 r_1', \ldots, r_d r_d' \rangle$ *and* $t'' = tt'$. □

In the next section we use Theorem 2.1 and wait until the very end to use Theorem 2.3 in the proof of Theorem 1.1. We will also need several technical lemmas about perfect factors of order one such that the sum of the entries in each factor is zero modulo the base k. They will be used as a control on the resulting periods of our constructions.

Lemma 2.4. *Let* $p > 2$ *be a prime,* $d \geq 1$, *and* $R_d = p^{\sum_{k=1}^d \beta_k}$. *Then there is a partition* $\{S_1, \ldots, S_{R_d/p}\}$ *of the set of vectors* $\prod_{k=1}^d [p^{\beta_k}]$ *into sets of size* p *such that, for each* $i \leq R_d/p$, *the following holds. Let* $S_i = \{V_{i,1}, \ldots, V_{i,p}\}$ *with* $V_{i,j} = \langle v_{i,j,1}, \ldots, v_{i,j,d} \rangle$. *Then for each* $k \leq d$ *we have* $\sum_{j=1}^p v_{i,j,k} \equiv 0 \pmod{p^{\beta_k}}$.

Proof: We use induction. For $d = 1$ we use the following factors $F_{h,i}$ (for the S_j), where $i = 0, 1, \ldots, p-1$ and $h = 0, 1, \ldots p^{\beta_1 - 2} - 1$.

$$F_{h,i} = \{hp^2 + ip + j \mid j = 0, 1, \ldots, p-2\} \cup \{p^{\beta_1} - \binom{p-1}{2} - ip(p-1) - hp^2(p-1)\}.$$

It is easy to see that these factors partition $[p_1^\beta]$ since since the former set making up each $F_{h,i}$ takes cares of those integers congruent to $0, 1, \ldots, p-2$ modulo p and the latter set takes care of those congruent to $p-1$ modulo p. The sum of the terms in $F_{h,i}$ is $(\sum_{j=0}^{p-2}(hp^2 + ip + j)) + p^{\beta_1} - \binom{p-1}{2} - ip(p-1) - hp^2(p-1) = p^{\beta_1}$ which is congruent to 0 modulo p_1^β.

For $d > 1$ we use the previous construction from the case $d-1$ and append a d^{th} coordinate onto every vector in the following way. Given a set $S_i = \{\langle v_{i,1,1}, \ldots, v_{i,1,d-1} \rangle, \ldots, \langle v_{i,p,1}, \ldots, v_{i,p,d-1} \rangle\}$ from the $(d-1)$- construction, and $x_j = \{x_1, x_2, \ldots x_p\} \in PF_{p^{\beta_d}}^1(p;1;p^{\beta_d - 1})$ (from the case $d = 1$), we construct the sets $S_{i,j,0}, S_{i,j,1}, \ldots, S_{i,j,p-1}$ where $S_{i,j,k} = \{\langle v_{i,1,1}, \ldots, v_{i,1,d-1}, x_{1+k} \rangle, \ldots, \langle v_{i,p,1}, \ldots, v_{i,p,d-1}, x_{p+k} \rangle\}$ and where the subscripts on the d^{th} coordinate are taken mod p. This yields the $p(p^{\beta_d - 1})(R_{d-1}/p) = R_d/p$ sets with the necessary modular properties. □

Lemma 2.4′. *Let* $p = 2$, $d \geq 2$, $2 \leq \beta_1 \leq \ldots \leq \beta_d$, *and* $R_d = 2^{\sum_{k=1}^d \beta_k}$. *Then there is a partition* $\{S_1, \ldots, S_{R_d/4}\}$ *of the set of vectors* $\prod_{k=1}^d [2^{\beta_k}]$

into sets of size 4 such that, for each $i \leq R_d/4$, the following holds. Let $S_i = \{V_{i,1}, \ldots, V_{i,4}\}$ with $V_{i,j} = \langle v_{i,j,1}, \ldots, v_{i,j,d}\rangle$. Then for each $k \leq d$ we have $\sum_{j=1}^{4} v_{i,j,k} \equiv 0 \pmod{2^{\beta_k}}$.

Proof: We use induction. For $d = 2$ we use the following matching to figure the set of k^{th} coordinates. Each $0 < x_k < 2^{\beta_k - 1}$ is matched with $y_k = 2^{\beta_k} - x_k$, and $x_k = 0$ is matched with $y_k = 2^{\beta_k - 1}$. To construct a particular set $S_i = \{\langle v_{i,1,1}, v_{i,1,2}\rangle, \ldots, \langle v_{i,4,1}, v_{i,4,2}\rangle\}$ we choose one of the $2^{\beta_1 - 1}$ matches (x_1, y_1) and one of the $2^{\beta_2 - 1}$ matches (x_2, y_2) to form the set $\{\langle x_1, x_2\rangle, \langle x_1, y_2\rangle, \langle y_1, x_2\rangle, \langle y_1, y_2\rangle\}$. This produces $(2^{\beta_1 - 1})(2^{/b_2 - 1}) = R_2/4$ sets with the necessary modular properties.

For $d > 2$ we use the previous construction from the case $d-1$ and append a d^{th} coordinate onto every vector in the following way. As above, we will use the set of matches $\{(x_d, y_d)\}$, defined analogously using β_d. Given a set $S_i = \{\langle v_{i,1,1}, \ldots, v_{i,1,d-1}\rangle, \ldots, \langle v_{i,4,1}, \ldots, v_{i,4,d-1}\rangle\}$ from the $(d-1)$-construction, and given a particular match (x_d, y_d), we construct the sets S_i' and S_i'' as follows. $S_i' = \{\langle v_{i,1,1}, \ldots, v_{i,1,d-1}, x_d\rangle, \langle v_{i,2,1}, \ldots, v_{i,2,d-1}, x_d\rangle, \langle v_{i,3,1}, \ldots, v_{i,3,d-1}, y_d\rangle, \langle v_{i,4,1}, \ldots, v_{i,4,d-1}, y_d\rangle\}$ and S_i'' switches the roles of x_d and y_d. This yields $2(2^{\beta_d - 1})(R_{d-1}/4) = R_d/4$ sets with the necessary modular properties. □

Corollary 2.5. *Let $p > 2$ be a prime, $d \geq 1$, and $R_d = p^{\sum_{k=1}^{d} \beta_k}$. Then for any integer $1 \leq m \leq \sum_{k=1}^{d} \beta_k$ there is a partition $\{S_1, \ldots, S_{R_d/p^m}\}$ of the set of vectors $\prod_{k=1}^{d} [p^{\beta_k}]$ into sets of size p^m such that, for each $i \leq R_d/p^m$, the following holds. Let $S_i = \{V_{i,1}, \ldots, V_{i,p^m}\}$ with $V_{i,j} = \langle v_{i,j,1}, \ldots, v_{i,j,d}\rangle$. Then for each $k \leq d$ we have $\sum_{j=1}^{p^m} v_{i,j,k} \equiv 0 \pmod{p^{\beta_k}}$.*

Proof: Concatenate as many of the sequences from Lemma 2.4 as needed. □

Corollary 2.5′. *Let $p = 2$, $d \geq 2$, $2 \leq \beta_1 \leq \ldots \leq \beta_d$, and $R_d = 2^{\sum_{k=1}^{d} \beta_k}$. Then for any integer $2 \leq m \leq \sum_{k=1}^{d} \beta_k$ there is a partition $\{S_1, \ldots, S_{R_d/2^m}\}$ of the set of vectors $\prod_{k=1}^{d} [2^{\beta_k}]$ into sets of size 2^m such that, for each $i \leq R_d/2^m$, the following holds. Let $S_i = \{V_{i,1}, \ldots, V_{i,2^m}\}$ with $V_{i,j} = \langle v_{i,j,1}, \ldots, v_{i,j,d}\rangle$. Then for each $k \leq d$ we have $\sum_{j=1}^{2^m} v_{i,j,k} \equiv 0 \pmod{2^{\beta_k}}$.*

Proof: Concatenate as many of the sequences from Lemma 2.4′ as needed. □

3 Proof of Theorem 1.1

Lemma 3.1. *Let $t_d = p^{\alpha 2^d - \sum_{i=1}^{d} \beta_i}$ and $t_{d+1} = p^{\alpha 2^{d+1} - \sum_{i=1}^{d+1} \beta_i}$. If $PF_{p^\alpha}^{d}(\langle p\rangle^{\vec{\beta}}; \langle 2\rangle^{d}; t_d) \neq \emptyset$ and $\beta_{d+1} \leq \alpha 2^{d+1} - \sum_{k=1}^{d} \beta_k$ (so that $\sum_{k=1}^{d+1} \beta_k \leq \alpha 2^{d+1}$; i.e., $R_{d+1} | p^{\alpha N_{d+1}}$), then $PF_{p^\alpha}^{d+1}(\langle p\rangle^{\vec{\beta}}, p^{\beta_{d+1}}; \langle 2\rangle^{d+1}; t_{d+1}) \neq \emptyset$.*

We note that many of the arguments below can be made for arbitrary $\vec{N}$ (with the modification $\beta_{d+1} \leq \alpha N_{d+1} - \sum_{k=1}^{d} \beta_k$ in the hypothesis), though we lose the ability later on to transpose freely the factors produced. Also, the statement for $\vec{N} = \langle n \rangle^d$ becomes more cumbersome, and so we aim here for clarity rather than generality. We also note that in the application of Lemma 3.1 to Lemma 3.3 which follows, it may be assumed that $\beta_i \leq \beta_{i+1}$ for each $i \leq d$, since reordering in this way will not violate the hypothesis of Lemma 3.1 (reordering in nonincreasing fashion, however, may at times violate the hypothesis).

Proof: Basically, the strategy is based on ideas and techniques found in [5,6,11,16]. However, since we are constructing perfect factors rather than De Bruijn tori (perfect maps), there is some added difficulty in ensuring that the arrays have the proper period. Given any p^α-ary $(d+1)$-dimensional matrix M of size $\langle 2 \rangle^{d+1}$ we see that its projection along $i_{d+1} = i$ is a d-dimensional matrix M_i, which occurs in a unique $A_{u(i)} \in \mathcal{A}$, for $\mathcal{A} \in PF_{p^\alpha}^d(\langle p \rangle^{\vec{\beta}}; \langle 2 \rangle^d; t_d)$, in the unique position $\vec{J}(A_{u(i)})$. So the matrix M can be partially encoded by the ordered pair $(u(0), u(1))$, since $i \in \{0,1\}$, and we are interested in using a 1-dimensional perfect factor $\mathcal{U}$ for pairs with base $|\mathcal{A}| = t_d = p^{\alpha N_d}/R_d$ to locate M. The rest of the encoding comes from the positions $\vec{J}(A_{u(x)})$. The difference $\vec{J}(A_{u(1)}) - \vec{J}(A_{u(0)})$ is a vector $\vec{S} = \langle s_1, s_2, \ldots, s_d \rangle$ where $s_i \in \{0, 1, \ldots, p^{\beta-1}\}$. This vector $\vec{S}$ can be assigned an integer via any bijection $g : \prod_{k=1}^{d} [p^{\beta_k}] \longrightarrow [\prod_{k=1}^{d} p^{\beta_k}] = [R_d]$, and so we are also interested in using a 1-dimensional perfect factor $\mathcal{V}$ for singletons with base R_d to locate M.

To show that the following constructions are indeed a perfect factors, we must show that each matrix M can be found uniquely and that the arrays are periodic with the correct period. Uniqueness will be shown by noting that the pair $(u(0), u(1))$ appears uniquely in the same position as the shift $\vec{J}(A_{u(1)}) - \vec{J}(A_{u(0)})$ in the constructions below.

What remains in the proof is to construct sequences which will match up the pairs $(u(0), u(1))$ with the images x_i of the shift vectors $\vec{S}_i$. There will be four cases, based on whether $r_{d+1} | (t_d)^2$ or $(t_d)^2 | r_{d+1}$ and whether $r_{d+1} | R_d$ or $R_d | r_{d+1}$. The perfect factors $\mathcal{U}$ and $\mathcal{V}$ will come from Theorem 2.1 and from Corollaries 2.5 and 2.5′, respectively.

Case 1: $r_{d+1} | (t_d)^2$ and $r_{d+1} | R_d$. Given any $U_i = (u_{i,0}, u_{i,1}, \ldots) \in \mathcal{U} = \{U_1, U_2, \ldots\} \in PF_{t_d}^1(r_{d+1}; 2; (t_d)^2/r_{d+1})$ and $V_j = (v_{j,0}, v_{j,1}, \ldots) \in \mathcal{V} = \{V_1, V_2, \ldots\} \in PF_{R_d}^1(r_{d+1}; 1; R_d/r_{d+1})$ we construct r_{d+1} periodic sequences $W_0(U_i, V_j), \ldots, W_{r_{d+1}-1}(U_i, V_j)$, each of period r_{d+1}, with the property that the k^{th} entry $W_l(U_i, V_j)_k$ of $W_l(U_i, V_j)$ is the ordered pair $(u_{i,k}, v_{j,k+l})$. Clearly, for every $(a,b) \in [t_d]^2$, $c \in [R_d]$, there are unique i, j, k and l such that $W_l(U_i, V_j)_k = (a, c)$, $W_l(U_i, V_j)_{k+1} = (b, \cdot)$, and $k < r_{d+1}$. Thus $\mathcal{W} = \{W_l(U_i, V_j) : i \in [(t_d)^2/r_{d+1}], j \in [R_d/r_{d+1}], l \in [r_{d+1}]\}$ forms an en-

coding of the $|\mathcal{W}| = ((t_d)^2/r_{d+1}) \cdot (R_d/r_{d+1}) \cdot r_{d+1} = (t_d)^2 R_d/r_{d+1} = t_{d+1}$ factors in the family $\mathcal{A}' \in PF_{p^\alpha}^{d+1}(\langle p\rangle^{\vec{\beta}}, p^{\beta_{d+1}}; \langle 2\rangle^{d+1}; t_{d+1})$ generated by $\mathcal{A} \in PF_{p^\alpha}^{d}(\langle p\rangle^{\vec{\beta}}; \langle 2\rangle^{d}; t_d)$.

Case 2: $r_{d+1}|(t_d)^2$ and $R_d|r_{d+1}$. $\mathcal{U}$ is as in case 1, but now we take $\mathcal{V} = \{V\} \in PF_{R_d}^1(R_d; 1; 1)$ and, for each i, construct R_d periodic sequences $W_l(U_i, V)$, defined as before, with $i \in [(t_d)^2/r_{d+1}]$ and $l \in [R_d]$. As before, we get $|\mathcal{W}| = (t_d)^2 R_d/r_{d+1} = t_{d+1}$ sequences to encode the factors in $\mathcal{A}'$.

Case 3: $(t_d)^2|r_{d+1}$ and $r_{d+1}|R_d$. $\mathcal{V}$ is as in case 1, but $\mathcal{U} = \{U\} \in PF_{t_d}^1((t_d)^2; 2; 1)$ and for each j we construct $(t_d)^2$ periodic sequences $W_l(U, V_j)$, defined above, with $j \in [R_d/r_{d+1}]$ and $l \in [(t_d)^2]$. Again, $|\mathcal{W}| = t_{d+1}$.

Case 4: $(t_d)^2|r_{d+1}$ and $R_d|r_{d+1}$ (and r_{d+1} $\not|R_d$). $\mathcal{V}$ is as in case 2, but now we use $\mathcal{U} \in PF_{t_d}^1(r_{d+1}/R_d;\ 2;\ (t_d)^2 R_d/r_{d+1})$. (See below for the case $r_{d+1}/R_d = 2$, in which case such a $\mathcal{U}$ does not exist.) We use a different technique here, first used in [6] and again in [11]. Let $V = (v_0, v_1, \ldots, v_{R_d-1}, v_0, v_1, \ldots)$. Denote by v_0^x the sequence $(v_0, v_0, \ldots, v_0)$ of length x, let $V' = (v_1, \ldots, v_{R_d-1})$ and denote by $(V')^x$ the concatenated sequence $V'V' \cdots V'$ of V' with itself x times. Now let $V'' = v_0^x (V')^x = (v_0'', v_1'', \ldots, v_{r_{d+1}}'')$, with $x = r_{d+1}/R_d$, and for each i construct the sequence $W(U_i, V'')$, of period r_{d+1} defined by $W(U_i, V'')_k = (u_{i,k}, v''_{k \pmod{R_d}})$. It is not difficult ([6,11]) to see that for every $(a, b) \in [t_d]^2$, $c \in [R_d]$, there are unique i and k such that $W(U_i, V'')_k = (a, c)$, $W(U_i, V'')_{k+1} = (b, \cdot)$, and $k < r_{d+1}$. Also, $|\mathcal{W}| = (t_d)^2 R_d/r_{d+1} = t_{d+1}$, completing the proof of Lemma 3.1 when $r_{d+1}/R_d \neq 2$.

If $r_{d+1}/R_d = 2$ take $U' \in PF_{t_d}^1((t_d)^2; 2; 1)$ and concatenate $r_{d+1}/(t_d)^2$ copies of U' to get U (with length r_{d+1}). Take $V = (v_0, v_1, \ldots, v_{R_d-1}) \in PF_{R_d}^1(R_d; 1; 1)$. For $j = 1, 2, \ldots, (t_d)^2 R_d/r_{d+1} = t_{d+1}$ let V_j have k^{th} entry v_{2j+k} if $0 \leq k < R_d$ and $v_{2j+1+(k-R_d)}$ if $R_d \leq k < 2R_d$. Now for $0 \leq j < t_{d+1}$, let $W(U, V_j)$ have k^{th} entry given by the ordered pair of k^{th} entries from U and V_j. Checking that this encoding has the correct uniqueness and modular properties is straightforward. □

Observe that in extending this to $n_i > 2$, the only difficulty in the above proof involves the last paragraph of case 4. Also, analogues of Corollaries 2.5 and 2.5′ are needed. However, these can be obtained as in the proof of Corollary 2.5 using results from [17].

Lemma 3.2. *For all $\beta_1 \geq 2, \beta_2 \geq 2$, and α with $\beta_1 + \beta_2 \leq 4\alpha$ we have $PF_{2^\alpha}^2(2^{\beta_1}, 2^{\beta_2}; 2, 2;\ 2^{4\alpha-\beta_1-\beta_2}) \neq \emptyset$.*

Proof: We assume that $\beta_1 \leq \beta_2$, otherwise we would simply switch the roles of β_1 and β_2 and transpose the result of what follows. This and the hypotheses imply that $\beta_1 \leq 2\alpha$ so that $PF_{2^\alpha}^1(2^{\beta_1}; 2; 2^{2\alpha-\beta_1}) \neq \emptyset$ by Theorem 2.1. Let $\mathcal{U} = \{U_1, \ldots, U_{2^{2\alpha-\beta_1}}\}$ be such a perfect factor.

Consider first the case that $2\beta_1 + \beta_2 \leq 4\alpha$. Then $\beta_2 \leq 2(2\alpha - \beta_1)$

so $PF^1_{2^{2\alpha-\beta_1}}(2^{\beta_2}; 2; 2^{4\alpha-2\beta_1-\beta_2}) \neq \emptyset$ by Theorem 2.1. Let $\mathcal{V} = \{V_1, \ldots, V_{2^{4\alpha-2\beta_1-\beta_2}}\}$ be such a perfect factor. If (x, y) is a particular pair of adjacent digits in some V_i then our encoding will tell us to juxtapose U_x and U_y as columns in a matrix. In order to construct a two-dimensional perfect factor we need that every ordered pair (U_x, U_y) appears exactly 2^{β_1} times, once with each possible shift of U_y with respect to U_x. In this case we use the sequences $S_x = (x)^{2^{\beta_2}}$, for each $x \in [2^{\beta_1}]$, each of which sums to 0 (mod 2^{β_1}) since $\beta_1 \leq \beta_2$. Each S_x gets paired with each V_i to create the $(2^{\beta_1})(2^{4\alpha-2\beta_1-\beta_2}) = 2^{4\alpha-\beta_1-\beta_2}$ matrices in the factor required by the theorem.

Consider, on the other hand, the case that $2\beta_1 + \beta_2 > 4\alpha$, and suppose that $\beta_1 < 2\alpha$. Use $\mathcal{U}$ as above and take $\mathcal{V} = \{V\} \in PF^1_{2^{2\alpha-\beta_1}}(2^{4\alpha-2\beta_1}; 2; 1)$. Now we denote by $(a, b)^k$ the sequence $(a, b, a, b, \ldots, a, b)$ of length $2k$ and, for $x \in [2^{\beta_1}]$, define the shift sequences $S_x = (x, 2^{\beta_1} - x)^{2^{\beta_1-1}}$, each of which sums to 0 (mod 2^{β_1}). We partition $[2^{\beta_1}]$ into index sets $I_1, \ldots, I_{2^{4\alpha-\beta_1-\beta_2}}$, of size $2^{2\beta_1+\beta_2-4\alpha}$ each, and for each $I_j = \{i(j, 1), \ldots, i(j, 2^{2\beta_1+\beta_2-4\alpha})\}$ we concatenate the sequences $S_{i(j,1)}, \ldots, S_{i(j,2^{2\beta_1+\beta_2-4\alpha})}$, to form the sequence $S(j)$. Form the sequence $V^{2^{2\beta_1+\beta_2-4\alpha}}$ by concatenating V with itself $2^{2\beta_1+\beta_2-4\alpha}$ times, and then pair each $S(j)$ with $V^{2^{2\beta_1+\beta_2-4\alpha}}$. As above, this produces the necessary $2^{4\alpha-\beta_1-\beta_2}$ matrices for the factor we need.

Lastly, consider the case $\beta_1 = 2\alpha$, which means that $\beta_2 = 2\alpha$ as well since $\beta_1 + \beta_2 \leq 4\alpha$. Thus we want to show that we can find a totally square De Bruijn torus in $PF^2_{2^\alpha}(2^{2\alpha}, 2^{2\alpha}; 2, 2, 1)$. But this set of tori has been shown to be nonempty in [11,14], and this completes the proof of Lemma 3.2. □

Lemma 3.3. *Let p^α be a prime power, for $j \leq d$ let $r_j = p^{\beta_j} > 2$ and suppose that for each $l \leq d$ we have $\sum_{j=1}^{l} \beta_j \leq \alpha 2^l$. Then $PF^d_{p^\alpha}(\vec{R}; \langle 2\rangle^d; t) \neq \emptyset$, where $\vec{R} = \langle r_1, \ldots, r_d\rangle$ and $t = p^{\alpha 2^d - \sum_{j=1}^{d} \beta_j}$.*

Proof: We will use induction on d. For the base cases, when $d = 1$ we have $PF^1_{p^\alpha}(p^\beta; 2; p^{2\alpha-\beta}) \neq \emptyset$ from Theorem 2.1. If $p = 2$ then we also need $d = 2$ as a base case. For this we have $PF^2_{2^\alpha}(2^{\beta_1}, 2^{\beta_2}; 2, 2; 2^{4\alpha-\beta_1-\beta_2}) \neq \emptyset$ from Lemma 3.2. For $d > 1$ (or $d > 2$ if $p = 2$) the hypotheses for case d imply those for case $d - 1$, which in turn imply those of Lemma 3.1, which finishes the proof. □

Proof of Theorem 1.1: Use Lemma 3.3 followed by Theorem 2.3. □

Acknowledgements

We thank the referees for some useful suggestions on the presentation of this paper.

References

[1] J. Burns and C.J. Mitchell, Coding schemes for 2-dimensional position sensing, to appear in *Cryptography and Coding, III*, ed. M. Ganley, Oxford University Press, 1993.

[2] N.G. De Bruijn, A combinatorial problem, *Nederl. Akad. Wetensch, Proc.* **49** (1946), 758–764.

[3] F.R.K. Chung, P. Diaconis, and R.L. Graham, Universal cycles for combinatorial structures, *Discrete Math.* **110** (1992), 43–59.

[4] J.C. Cock, Toroidal tilings from De Bruijn-Good cyclic sequences, *Disc. Math.*, **70** (1988), 209–210.

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

[6] C.T. Fan, S.M. Fan, S.L. Ma, and M.K. Siu, On De Bruijn arrays, *Ars Combin.*, **19** (1985), 205–213.

[7] C. Flye-Sainte Marie, Solution to problem number 58, *l'Intermediaire des Mathematiciens*, 1 (1894), 107–110.

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

[9] I.J. Good, Normally recurring decimals, *J. London Math. Soc.*, **21** (1946), 167–169.

[10] G. Hurlbert, *Universal cycles: on beyond De Bruijn*, Ph.D. dissertation, Rutgers University, 1990.

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

[12] G. Hurlbert and G. Isaak, A meshing technique for De Bruijn tori, *Contemp. Math.* **178** (1994), 153–160.

[13] G. Hurlbert and G. Isaak, New constructions for De Bruijn tori, *Designs, Codes, and Cryptography* **6** (1995), 47–56.

[14] A. Iványi and Z. Toth, Existence of De Bruijn words, in *Proceedings, 2nd Conf. on Automata, Languages, and Programming Systems*, Salgótarján, Hungary, 1988, DM88-4, 165–172.

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

[16] K.G. Paterson, Perfect maps, *IEEE Transactions on Information Theory* **IT–40** (1994), 743–753.

[17] K.G. Paterson, Perfect factors in the De Bruijn graph, to appear, *Designs, Codes, and Cryptography.*

[18] K.G. Paterson, New Classes of Perfect Maps II, to appear, *J. Combin. Theory Ser. A.* 1994.