1-1-1992

# On The De Bruijn Torus Problem

Glenn Hurlbert
*Arizona State University*

Garth Isaak
*Dartmouth College*

# ON THE DE BRUIJN TORUS PROBLEM

Glenn Hurlbert
Arizona State University

Garth Isaak
Dartmouth College

Technical Report PCS-TR92-181

# ON THE DE BRUIJN TORUS PROBLEM

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

Garth Isaak
Dept. of Math. & Comp. Sci.
Dartmouth College
Hanover, NH 03755

**Abstract.** A $(k^n; n)_k$-de Bruijn Cycle is a cyclic $k$-ary sequence with the property that every $k$-ary $n$-tuple appears exactly once contiguously on the cycle. A $(k^r, k^s; m, n)_k$-de Bruijn Torus is a $k$-ary $k^r \times k^s$ toroidal array with the property that every $k$-ary $m \times n$ matrix appears exactly once contiguously on the torus. As is the case with de Bruijn cycles, the 2-dimensional version has many interesting applications, from coding and communications to pseudo-random arrays, spectral imaging, and robot self-location. J.C. Cock proved the existence of such tori for all $m, n$, and $k$, and Chung, Diaconis, and Graham asked if it were possible that $r = s$ and $m = n$ for $n$ even. Fan, Fan, Ma and Siu showed this was possible for $k = 2$. Combining new techniques with old, we prove the result for $k \geq 2$ and show that actually much more is possible. The cases in 3 or more dimensions remain.

# 1. Introduction.

A $(k^n; n)_k$-*de Bruijn Cycle* is a cyclic $k$-ary sequence with the property that every $k$-ary $n$-tuple appears exactly once contiguously on the cycle. Such cycles, first discovered in 1894 by Flye St. Marie (see [5]), have found applications in the study of pseudo-random numbers, cryptography, nonlinear shift registers and coding theory, and a vast literature exists (see [1], [6–11], [14], [18]).

For $r, s > 0$ a $(k^r, k^s; m, n)_k$-*de Bruijn torus* is a $k$-ary $(k^r \times k^s)$ toroidal array with the property that every $k$-ary $(m \times n)$ matrix appears exactly once contiguously on the torus (see Figure 1). In addition to the above we find interesting applications in robot self-location [19], pseudo-random arrays [18], and the design of mask configurations for spectrometers [13]. (For an interesting variation on this theme see [16]). Even cloth patterns have used these designs, long before their mathematical properties were discovered (see [12]).

$$\begin{array}{cccc} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{array}$$

Figure 1. A $(4, 4; 2, 2)_2$-de Bruijn torus.

In [3], J.C. Cock proves the following (see also [17] for the binary case).

**Theorem 1.1.** *For all $m, n$, and $k$ (except $n = 2$ if $k$ even) there is a $(k^r, k^s; m, n)_k$-de Bruijn torus with $r = m$ and $s = m(n-1)$.*

One might also define $(R, S; m, n)_k$-de Bruijn tori as $R \times S$ toroidal arrays with the same uniqueness property for $m \times n$ matrices, but our concern here will be with $R$ and $S$ both powers of $k$ only. We will say more about this in Section 5.

The reader may have noticed that the relations $r + s = mn$, $k^r > m$, and $k^s > n$, are necessary for the existence of a $(k^r, k^s; m, n)$-de Bruijn torus. (If $k^r = m$, say, then the all 0's matrix is found $m$ times.) The sufficiency of these relations seems to be a rather tricky problem, and we conjecture that, except possibly for very small values of $m$ and $n$, the conditions $r + s = mn$, $k^r > m$ and $k^s > n$ are sufficient for all $k$. In [2], Chung, Diaconis, and Graham ask whether it is possible that "square" tori exist for even $n$. That is, can it be that $r = s$ and $m = n$? This question was resolved for the binary case by Fan, Fan, Ma, and Siu [4], who proved

**Theorem 1.2.** *There exists a $(2^r, 2^r; n, n)_2$-de Bruijn torus if and only if $n$ is even.*

Again, one should notice that $r = n^2/2$, so either $n$ is even or $k$ is a perfect square. Our purpose here is to prove a bit more than was conjectured in [2].

**Theorem 1.3.**

a) *For $k$ odd there is a $(k^r, k^r; n, n)_k$-de Bruijn torus if and only if $n$ is even or $k$ is a perfect square, and*

b) *For $k$ even and $n \geq 10$, there is a $(k^r, k^r; n, n)_k$-de Bruijn torus if and only if $n$ is even or $k$ is a perfect square.*

For part b) we will actually show that such tori exist for even $n \geq 4$ and for square $k$ and odd $n \geq 11$. Though we believe they exist, we have not found de Bruijn tori (when $k$ is even) for $n = 3, 5$, or 7 (see [15] for the case $n = 2$). However, when $n = 9$ we can construct examples if $k$ is an even square divisible by 16.

## 2. Proof of Theorem 1.3.

We will prove Theorem 1.3 by using induction on $n$. If we write $A \in dB_k\ (k^r, k^s; m, n)$ we will mean that the array $A$ is a $(k^r, k^s; m, n)$-de Bruijn torus. (Likewise, $dB_k(k^n; n)$ is the set of all $(k^n; n)_k$-de Bruijn cycles.) If each column (resp. row) of $A$ sums to 0 mod $k$ we will say that $A$ has *property* $\sigma$ (resp. $\tau$). Also, we say that $A$ has *property* $\sigma^*$ if the columns $A_1, \ldots, A_{k^s}$ satisfy $\boldsymbol{\eta} \cdot A_i \equiv 0 \bmod k$, where the row vector $\boldsymbol{\eta} = (1, 2, \ldots, k^r)$, and *property* $\tau^*$ if its transpose $A^T$ has property $\sigma^*$.

**Fact 2.1.**

a) For $k$ odd there is an array $A \in dB_k(k^2, k^2; 2, 2)$ with property $\sigma$, and for $k$ an odd perfect square there is an array $A \in dB_k(k^{1/2}, k^{1/2}; 1, 1)$ with property $\sigma$.

b) For $k$ even there is an array $A \in dB_k(k^8, k^8; 4, 4)$ with property $\sigma$, and for $k$ an even perfect square there is an array $A \in dB_k(k^{121/2}, k^{121/2}; 11, 11)$ with property $\sigma$.

**Lemma 2.2.** *There is a function $f$ such that if $A \in dB_k(k^r, k^s; m, n)$ has property $\sigma$, then $f(A) \in dB_k(k^r, k^{s+n}; m+1, n)$ and has property $\tau$. Furthermore, if $s > 1$, $n \geq 2$, or $k$ odd, then $f(A)$ has property $\tau^*$, and if $A$ has property $\sigma^*$ then $f(A)$ has property $\sigma$.*

Theorem 1.3 then follows from Fact 2.1 and Lemma 2.2 by repeated applications of Lemma 2.2, as the following argument shows (see Figure 2, where $T$ is the transposition operator).

$$dB_k(k^{n^2/2}, k^{n^2/2}; n, n) \quad \sigma$$
$$\downarrow f$$
$$dB_k(k^{n^2/2}, k^{(n^2+2n)/2}; n+1, n) \quad \tau, \tau^*$$
$$\downarrow T$$
$$dB_k(k^{(n^2+2n)/2}, k^{n^2/2}; n, n+1) \quad \sigma, \sigma^*$$
$$\downarrow f$$
$$dB_k(k^{(n^2+2n)/2}, k^{(n^2+2n+2)/2}; n+1, n+1) \quad \sigma$$
$$\downarrow f$$
$$dB_k(k^{(n^2+2n)/2}, k^{(n^2+4n+4)/2}; n+2, n+1) \quad \tau, \tau^*$$
$$\downarrow T$$
$$dB_k(k^{(n^2+4n+4)/2}, k^{(n^2+2n)/2}; n+1, n+2) \quad \sigma, \sigma^*$$
$$\downarrow f$$
$$dB_k(k^{(n+2)^2/2}, k^{(n+2)^2/2}; n+2, n+2) \quad \sigma$$

Figure 2. Induction using Lemma 2.2.

If $A \in dB_k(k^{n^2/2}, k^{n^2/2}; n, n)$ has property $\sigma$ then $A_1 = f(A) \in dB_k(k^{n^2/2}, k^{(n^2+2n)/2}; n+1, n)$ has properties $\tau$ and $\tau^*$, $A_2 = A_1^T \in dB_k(k^{(n^2+2n)/2}, k^{n^2/2}; n, n+1)$ has properties $\sigma$ and $\sigma^*$, and $A_3 = f(A_2) \in dB_k(k^{(n^2+2n)/2}, k^{(n^2+2n+2)/2}; n+1, n+1)$ has property $\sigma$. Furthermore, $A_4 = f(A_3) \in dB_k(k^{(n^2+2n)/2}, k^{(n+2)^2/2}; n+2, n+1)$ has properties $\tau$ and $\tau^*$, so $A_5 = A_4^T \in dB_k(k^{(n+2)^2/2}, k^{(n^2+2n)/2}; n+1, n+2)$ has properties $\sigma$ and $\sigma^*$. Finally, $A_6 = f(A_5) \in dB_k(k^{(n+2)^2/2}, k^{(n+2)^2/2}; n+2, n+2)$ has property $\sigma$. □

Thus we always obtain "square" tori with the extra property $\sigma$.

We continue to assume Lemma 2.2 in order to handle Fact 2.1. Lemma 2.2 will be proved in the next section.

**Proof of Fact 2.1a.** We follow Cock's construction from Theorem 1.1 to find $A \in dB_k(k^2, k^2; 2, 2)$ for $k$ odd, needing only to check for property $\sigma$. First, an example to illustrate the method.

Let $k = 3$, $\mathbf{a} = (001121022) \in dB_3(3^2; 2)$, and $\mathbf{b} = (012345678) \in dB_9(9^1; 1)$. Let the first column of $A$ be $\mathbf{a}^T$, the second be the first shifted cyclically by the first digit, 0, of $\mathbf{b}$, the third be the second shifted cyclically by the second digit, 1, of $\mathbf{b}$, ... and the $9^{\text{th}}$ be the

$8^{\text{th}}$ shifted cyclically by the $8^{\text{th}}$ digit, 7, of $\mathbf{b}$. Notice now that the first column is the $9^{\text{th}}$ shifted cyclically by 8 (see Figure 3).

$$A = \begin{matrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 0 & 0 & 2 & 0 & 0 & 2 \\ 2 & 2 & 1 & 2 & 0 & 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 2 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 0 & 1 & 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 & 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{matrix}$$

Figure 3. $A \in dB_3(3^2, 3^2; 2, 2)$ with property $\sigma$.

The reason why this construction works is the way we encode a $2 \times 2$ $k$-ary matrix $B$. For example, if we have $B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right)$ then the $1^{\text{st}}$ column of $B$ is the $3^{\text{rd}}$ pair listed in $\mathbf{a}^T$, and the second column is the $7^{\text{th}}$ pair listed in $\mathbf{a}^T$. To get from the $3^{\text{rd}}$ to the $7^{\text{th}}$ pair so that they are next to each other, we shift by 4. Thus, $B$ must be in columns 5 and 6 of $A$ since the shift 4 is the $5^{\text{th}}$ digit of $\mathbf{b}$, as in Figure 3. In this way we can find every $2 \times 2$ $k$-ary matrix in $A$ (see [3] for the actual proof of Theorem 1.1).

Also, $A$ has property $\sigma$ since each column is a de Bruijn cycle. Every digit of a $(k^n; n)$-de Bruijn cycle is listed $k^{n-1}$ times, so the sum of all digits in the cycle is $k^{n-1}\binom{k}{2}$, which is divisible by $k$ if $k$ is odd and $n \geq 1$.

For $k$ an odd square, any $k^{1/2} \times k^{1/2}$ array $A \in dB_k(k^{1/2}, k^{1/2}; 1, 1)$, provided each integer $\{0, 1, \ldots, k-1\}$ appears exactly once in the array. To obtain property $\sigma$ let the first column of $A$ be $(\frac{-(\sqrt{k}-1)}{2}, \ldots, 0, \ldots, \frac{\sqrt{k}-1}{2})^T$, add $\sqrt{k}$ to get the second column, $\sqrt{k}$ more to get the third, and so on. □

**Proof of 2.1b.** In Section 4 we will show how to find $A \in dB_k(k^2, k; 3, 1)$ and how to use $A$ to obtain $D \in dB_k(k^4, k^2; 2, 3)$ with properties $\sigma$ and $\sigma^*$. Assuming this, we can now use a sequence of $f$ functions and transpositions to obtain our result. To ease the eye notationally, we suppress $k$ and write $[r, s; m, n](\alpha, \beta)$ for some $A \in dB_k(k^r, k^s; m, n)$ satisfying properties $\alpha$ and $\beta$. Then we have

$$\begin{aligned} & [4, 2; 2, 3](\sigma, \sigma^*) \\ & \xrightarrow{f} [4, 5; 3, 3](\sigma) \\ & \xrightarrow{f} [4, 8; 4, 3](\tau, \tau^*) \\ & \xrightarrow{T} [8, 4; 3, 4](\sigma, \sigma^*) \\ & \xrightarrow{f} [8, 8; 4, 4](\sigma). \end{aligned}$$

The details are left to the reader.

As for $k$ an even square and $n$ odd, we refer the reader to Claim 2.3 below to discover $A \in dB_k(k^{3/2}, k^{1/2}; 2, 1)$ with property $\sigma$. From there we have

$$\{3,1;2,1\} \xrightarrow{f} \{3,3;3,1\} \xrightarrow{T} \{3,3;1,3\} \xrightarrow{f} \{3,9;2,3\} \xrightarrow{T} \{9,3;3,2\}$$
$$\xrightarrow{f} \{9,7;4,2\} \xrightarrow{T} \{7,9;2,4\} \xrightarrow{f} \{7,17;3,4\} \xrightarrow{f} \{7,25;4,4\} \xrightarrow{T} \{25,7;4,4\}$$
$$\xrightarrow{f} \{25,15;5,4\} \xrightarrow{T} \{15,25;4,5\} \xrightarrow{f} \{15,35;5,5\} \xrightarrow{f} \{15,45;6,5\}$$
$$\xrightarrow{T} \{45,15;5,6\} \xrightarrow{f} \{45,27;6,6\} \xrightarrow{T} \{27,45;6,6\} \xrightarrow{f} \{27,57;7,6\}$$
$$\xrightarrow{f} \{27,69;8,6\} \xrightarrow{T} \{69,27;6,8\} \xrightarrow{f} \{69,43;7,8\} \xrightarrow{f} \{69,59;8,8\}$$
$$\xrightarrow{T} \{59,69;8,8\} \xrightarrow{f} \{59;85;9,8\} \xrightarrow{f} \{59,101;10,8\} \xrightarrow{T} \{101,59;8,10\}$$
$$\xrightarrow{f} \{101,79;9,10\} \xrightarrow{f} \{101,99;10,10\} \xrightarrow{T} \{99,101;10,10\}$$
$$\xrightarrow{f} \{99,121;11,10\} \xrightarrow{T} \{121,99;10,11\} \xrightarrow{f} \{121,121;11,11\},$$

where $\{r,s;m,n\}$ denotes $[\frac{r}{2}, \frac{s}{2}; m, n]$. It is easily checked that $[3,1;2,1](\sigma)$ implies $[\frac{121}{2}, \frac{121}{2}; 11, 11](\sigma)$. □

**Claim 2.3.** *There is an array $A \in dB_k(k^{3/2}, k^{1/2}; 2, 1)$ with property $\sigma$.*

**Proof.** Here we merely point the reader in the right direction. The details are not difficult.

We observe that each of the columns of such an array may be thought of as segments of a sequence from $dB_k(k^2; 2)$, each segment having length $k^{3/2}$. The de Bruijn graph (see [1]) in this case has all singleton elements as vertices and all ordered pairs as directed edges. In other words, it is the complete graph $K_k$ with every edge replaced by two directed edges, one going each way, and with a loop added at each vertex. An Eulerian subgraph with $k^{3/2}$ edges corresponds to a column of $A$, and a decomposition into $k^{1/2}$ such subgraphs then produces $A$.

To guarantee property $\sigma$, we need that each subgraph $G_i$ has $\sum_{j \in V(G_i)} j \deg_i(j) \equiv 0 \bmod k$ where $\deg_i(j)$ is the number of edges entering vertex $j$ in $G_i$. We can accomplish this easily if we ensure that, for every $i$, $d_i(k-j) = d_i(j)$ for each $1 \leq j < k/2$ and $d_i(k/2)$ is even. This can be done in a myriad of ways; let the reader find his or her favorite. □

In [15] Iványi and Toth construct $A \in dB_k(k^2, k^2; 2, 2)$ for even $k$. However, we can show that property $\sigma$ holds (crucial to induction) only when 4 divides $k$. Also, although there is an $A \in dB_k(k^{1/2}, k^{1/2}; 1, 1)$ for even square $k$, it cannot have property $\sigma$, crucial to the induction process. Indeed the sum $\sum_{i=0}^{k^{1/2}-1} i = \binom{k^{1/2}}{2} = \left(\frac{k^{1/2}}{2}\right)(k^{1/2} - 1)$, which $k$ does not divide, and so some column sum is not divisible by $k$.

## 3. Proof of Lemma 2.2

Our function $f$ is a generalization of the construction used in [4]. Of course, there are more considerations in the $k$-ary case. Also, the reader will soon observe that $f$ is really a

multivalued function. That is, $f(A)$ depends on the choice of a $(k^n;n)_k$-de Bruijn cycle, and we obtain a different array for each choice.

Let $\mathbf{0}$ be the sequence of $k^s$ 0's, $\mathbf{c} = c_1c_2\cdots c_{k^n}$ be any sequence in $dB_k(k^n;n)$ which begins with $n$ 0's, and $\mathbf{c}'$ be $\mathbf{c}$ with its first 0 removed. Finally, let $\mathbf{c}_1 = \cdots = \mathbf{c}_{k^s} = \mathbf{c}'$ and $\mathbf{u} = \mathbf{0}\mathbf{c}_1\mathbf{c}_2\cdots\mathbf{c}_{k^s}$. Then $\mathbf{u}$ has length $t = k^s + k^s(k^n-1) = k^{s+n}$ and has the following convenient property.

Let $\mathbf{u} = u_1\cdots u_t$ and $\mathbf{u}_i = u_i\cdots u_{i+n-1}$. Then for each $1 \le i \le k^s$ the set of $n$-tuples $\{\mathbf{u}_i, \mathbf{u}_{i+k^s}, \mathbf{u}_{i+2k^s}, \ldots, \mathbf{u}_{i+(k^n-1)k^s}\}$ are distinct (index addition modulo $t$). This is so because the starting points $u_i, u_{i+k^s}, \ldots, u_{i+(k^n-1)k^s}$, are distinct with respect to $\mathbf{c}$. That is, $u_iu_{i+k^s}\cdots u_{i+(k^n-1)k^s} = 0c'_jc'_{j+k^s}\cdots c'_{j+(k^n-2)k^s}$ for some $j$ (indices of $\mathbf{u}$ are modulo $t$, of $\mathbf{c}'$ are modulo $k^n-1$), and since $k^s$ and $k^n-1$ (the length of $\mathbf{c}'$) are relatively prime, no index of $\mathbf{c}$ is repeated.

Next let $A \in dB_k(k^r, k^s; m, n)$ have rows $\mathbf{a}_1, \ldots, \mathbf{a}_{k^r}$, and $A'$ be the $(k^r \times k^{s+n})$ array given by $A$ repeated horizontally $k^n$ times and having rows $\mathbf{a}'_1, \ldots, \mathbf{a}'_{k^r}$. We now define $F = f(A)$ as the $(k^r \times k^{s+n})$ matrix having rows $\mathbf{f}_1, \ldots, \mathbf{f}_{k^r}$ satisfying $\mathbf{f}_1 = \mathbf{u}, \mathbf{f}_2 = \mathbf{f}_1 + \mathbf{a}'_1, \mathbf{f}_3 = \mathbf{f}_2 + \mathbf{a}'_2, \ldots, \mathbf{f}_{k^r} = \mathbf{f}_{k^r-1} + \mathbf{a}'_{k^r-1}$. Notice that if $A$ has property $\sigma$ then $\mathbf{f}_1 = \mathbf{f}_{k^r} + \mathbf{a}'_{k^r}$. Furthermore,

$$\sum_{i=1}^{k^r} \mathbf{f}_i = k^r(\mathbf{u}) + \sum_{i=1}^{k^r}(k^r - i)\mathbf{a}'_i \equiv -\sum_{i=1}^{k^r} i\mathbf{a}'_i \bmod k,$$

so that if $A$ has property $\sigma^*$ then $F$ has property $\sigma$.

To show that $F \in dB_k(k^r, k^{s+n}; m+1, n)$ we follow an argument similar to that of the proof of fact 2.1a. Given a $k$-ary $(m+1) \times n$ matrix $B$ with rows $B_1, \ldots, B_{m+1}$, define the $k$-ary $m \times n$ matrix $C$ to have rows $C_1, \ldots, C_m$ so that $B_i + C_i = B_{i+1}$ for $1 \le i \le m$. Then $C$ is found uniquely in $A$, periodically in $A'$.

Suppose $C$ is found in rows $(j+1)$ through $(j+m)$ (addition mod $k^r$) and columns $i$ through $(i+n-1)$ (addition mod$k^s$) of $A$. Let $A_C$ be the $j \times n$ subarray of $A$ consisting of its first $j$ rows restricted to columns $i$ through $(i+n-1)$ and let its column sum be the vector $\mathbf{a}_C$ of length $n$. Finally, let $B_0 = B_1 - \mathbf{a}_C$. Then $B_0$ is a $k$-ary $n$-tuple, found uniquely amongst $\mathbf{u}_i, \mathbf{u}_{i+k^s}, \ldots, \mathbf{u}_{i+(k^n-1)k^s}$, say $B_0 = \mathbf{u}_{i+\alpha k^s}$. Thus $B$ is found in rows $(j+1)$ through $(j+m+1)$ and columns $(i+\alpha k^s)$ through $(i+\alpha k^s+n-1)$ of $F$, implying $F \in dB_k(k^r, k^{s+n}; m+1, n)$.

To show that $F$ has property $\tau$, we observe that

$$\mathbf{f_i} = \mathbf{u} + \mathbf{a}'_1 + \cdots + \mathbf{a}'_{i-1}.$$

$\mathbf{u}$ consists of $k^s$ copies of $\mathbf{c}$, so the sum of its digits is 0 mod $k$ if $s \ge 1$. If $s < 1$ then $\mathbf{c}$ has sum $\binom{k}{2}k^{n-1}$ so $\mathbf{u}$ has sum $k^s\binom{k}{2}k^{n-1}$, which is 0 mod $k$ whether $k$ is even or odd. As for the sum of the digits of $\mathbf{a}'_j$, it is simply $k^n$ times the sum of the digits of row $\mathbf{a}_j$ of $A$, and so $F$ does indeed have property $\tau$.

To verify property $\tau^*$ we must show that $\eta_{k^{s+n}} \cdot \mathbf{f}_i \equiv 0 \bmod k$, where $\eta_x = (1, 2, \ldots, x)$. Since $\eta_{k^{s+n}} \cdot \mathbf{a}'_i \equiv k^n(\eta_{k^s} \cdot \mathbf{a}_i) \equiv 0 \bmod k$ for all $i$, we have

$$\begin{aligned}\eta_{k^{s+n}} \cdot \mathbf{f}_i &\equiv \eta_{k^{s+n}} \cdot \mathbf{u} \bmod k \\ &\equiv \sum_{i=1}^{k^s} i \sum_{j=0}^{k^n-1} u_{i+jk^s} \bmod k \quad \text{if } s \geq 1 \qquad (*) \\ &= \sum_{i=1}^{k^s} i \sum_{j=0}^{k^n-1} c_j\end{aligned}$$

(by the "convenient property")

$$\begin{aligned}&= \binom{k^s+1}{2}\binom{k}{2}k^{n-1} \\ &\equiv 0 \bmod k \text{ if } s > 1,\ n \geq 2, \text{ or } k \text{ odd.}\end{aligned}$$

For the last remaining case of $k$ odd, $n = 1$, and $s \leq 1$ (notice $s \geq 1$ in $(*)$ above), one can show that for $\mathbf{c} = 0, 1, \ldots, k-1$ we have $\eta_{k^{s+n}} \cdot \mathbf{f}_i \equiv 0 \bmod k$. We need this last case in the top line of Figure 2. □

## 4. $D \in dB_k(k^4, k^2; 2, 3)$ with properties $\sigma$ and $\sigma^*$.

It is interesting in its own right to consider the existence of what we call *equivalence-class de Bruijn cycles* (and their higher-dimensional analogs). Let $J_x$ be the all-1's sequence of length $x$ and let $\mathbf{u}$ and $\mathbf{v}$ be two $k$-ary $m$-tuples. We say they are *equivalent* if $\mathbf{v} - \mathbf{u} \bmod k$ is a multiple of $J_m$. For example, (0142) and (3420) are equivalent with $m = 4$ and $k = 5$. A cyclic sequence $\mathbf{a}$ is a *$k$-ary equivalence-class de Bruijn cycle of order $m$*, written $\mathbf{a} \in \overline{dB_k}(k^m, m)$, if each equivalence class of $k$-ary $m$-tuples is represented exactly once as a contiguous $m$-tuple of $\mathbf{a}$. The existence of such an $\mathbf{a}$ follows immediately from the existence of $\mathbf{c} \in dB_k(k^{m-1}; m-1)$. Indeed, let $\mathbf{c} = c_1 \cdots c_{k^{m-1}}$ and define for any $a_1 \in \{0, 1, \ldots, k-1\}$, $\mathbf{a} = a_1 \cdots a_{k^{m-1}}$ by the relations $a_2 = a_1 + c_1, \ldots, a_{k^{m-1}} = a_{k^{m-1}-1} + c_{k^{m-1}-1}$, addition being modulo $k$. Of course, $a_1 = a_{k^m} + c_{k^m}$ since $\sum_{i=1}^{k^{m-1}} c_i \equiv 0 \bmod k$, and so equivalence-class de Bruijn cycles do exist (see Figure 4).

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 2 | 2 | 1 | 2 | 1 |
| 1 | 1 | 1 | 2 | 0 | 0 | 2 | 0 | 2 |
| 2 | 2 | 2 | 0 | 1 | 1 | 0 | 1 | 0 |

Figure 4. Each row is an element of $\overline{dB_3}(3^3; 3)$ generated by $001102122 \in dB_3(3^2; 2)$.

By choice of $a_1$ we can obtain $k$ different cycles $\mathbf{a}$. For $1 \leq i \leq k$, let $\mathbf{a}(i)$ be that obtained from $a_1 = i$. If we define the $(k^{m-1} \times k)$ array $A$ as having columns $\mathbf{a}(0)^T, \ldots, \mathbf{a}(k-1)^T$, then clearly $A \in dB_k(k^{m-1}, k; m, 1)$. For our purposes we have $m = 3$.

Given any sequence $\mathbf{v} = v_1 \cdots v_t$ let $\mathbf{v}^i = v_{i+1} \cdots v_t v_1 \cdots v_i$ be its cyclic shift by $i$ digits. Let $\mathbf{c} = c_1 \cdots c_{k^2} \in dB_k(k^2; 2)$ and define the $(k^2 \times k^2)$ array $D_j$ to have columns $\mathbf{a}(c_1)^T, \mathbf{a}^j(c_2)^T, \ldots, \mathbf{a}^{j(k^2-1)}(c_{k^2})^T$, where $j = 0, 1, \ldots, (k^2 - 1)$ and shift arithmetic is carried out modulo $k^2$. Finally define the $(k^2 \times k^4)$ array $D$ by juxtaposing the arrays $D_0 D_1 \cdots D_{k^2-1}$. We now need to show that $D \in dB_k(k^2, k^4; 3, 2)$ and has properties $\tau$ and $\tau^*$ so that actually $D^T \in dB_k(k^4, k^2; 2, 3)$, having $\sigma$ and $\sigma^*$.

Suppose $M$ is the $k$-ary $3 \times 2$ matrix $\begin{pmatrix} m_{11} & m_{21} & m_{31} \\ m_{12} & m_{22} & m_{32} \end{pmatrix}^T$. Then $m_{11} m_{21} m_{31}$ appears uniquely in $\mathbf{a}(x_1)$ and $m_{12} m_{22} m_{32}$ appears uniquely in $\mathbf{a}(x_2)$ for some $x_1$ and $x_2$. Also, $x_1 x_2$ appears uniquely in $\mathbf{c}$. Suppose $\mathbf{a}^{i_1}(x_1)$ begins with $m_{11} m_{21} m_{31}$, $\mathbf{a}^{i_2}(x_2)$ begins with $m_{12} m_{22} m_{32}$, and $x_1, x_2$ are the $t^{\text{th}}$ and $(t+1)^{\text{st}}$ elements of $\mathbf{c}$. If $j = i_2 - i_1$ then we find $M$ in the $t^{\text{th}}$ and $(t+1)^{\text{st}}$ columns of $D_j$. Thus $D \in dB_k(k^2, k^4; 3, 2)$.

To verify property $\tau$ we consider only the first row of $D$, as the argument for other rows is identical. Suppose the last row of $D$ is $d_1 d_2 \cdots d_{k^4}$. Then (with mod$k^4$ subscripts for $d$ and mod$k^2$ subscripts for $a$ and $c$) we have

$$\begin{aligned}
\sum_{i=1}^{k^4} d_i &= \sum_{h=0}^{k^2-1} \sum_{i=0}^{k^2-1} d_{k^2 i + h + 1} \\
&= \sum_{h=0}^{k^2-1} \sum_{i=0}^{k^2-1} a_{ih}(c_{h+1}) \\
&\equiv \sum_{h=0}^{k^2-1} \sum_{i=0}^{k^2-1} a_{ih}(0) \bmod k
\end{aligned}$$

(since $a_{ih}(c_{h+1}) = a_{ih}(0) + c_{h+1}$)

$$\begin{aligned}
&= \sum_{g | k^2} \sum_{\substack{h \text{ s.t.} \\ \gcd(h, k^2) = g}} \sum_{i=0}^{k^2-1} a_{ih}(0) \\
&\equiv \sum_{g | k^2} \sum_{\substack{h \text{ s.t.} \\ \gcd(h, k^2) = g}} \sum_{j=1}^{k^2/g} g a_j(0) \bmod k \qquad (1) \\
&= \sum_{g | k^2} g n(g) \sum_{j=1}^{k^2/g} a_j(0)
\end{aligned}$$

(where $n(g) =$ the number of integers $h$ s.t. $\gcd(h, k^2) = g$)

$$= \sum_{g | k^2} g \phi(k^2/g) \sum_{j=1}^{k^2/g} a_j(0)$$

(where $\phi$ is Euler's totient function)

$$\equiv 0 \bmod k$$

since $g\phi(k^2/g) \equiv 0 \bmod k$ for all $g|k^2$.

If we make similar calculations with $\sum_{i=1}^{k^4} id_i$ we discover that property $\tau^*$ holds as well. In fact, equation (1) becomes

$$\sum_{i=1}^{k^4} id_i \equiv \sum_{g|k^2} \sum_{\substack{h \text{ s.t.} \\ \gcd(h,k^2)=g}} h \sum_{j=1}^{k^2/g} g a_{gj}(0) \bmod k. \tag{1'}$$

But

$$\sum_{g|k^2} \sum_{\substack{h \text{ s.t.} \\ \gcd(h,k^2)=g}} h \equiv k^2/2 \bmod k$$

since both $h$ and $(k^2 - h)$ have gcd $g$ with $k^2$ (remember that $k$ is even). Thus, we find

$$\sum_{i=1}^{k^4} id_i \equiv 0 \bmod k.$$

□

One should observe that the analogous construction using $A \in dB_k(k^{m-1}, k; m, 1)$ yields $D \in dB_k(k^{m-1}, k^{m+1}; m, 2)$ with $\tau$ and $\tau^*$.

## 5. Remarks

**Conjecture 5.1.** *If $k, m, n, r, s$ satisfy*

i) $k^r > m$,

ii) $k^s > n$, and

iii) $r + s = mn$

*then there is an array $A \in dB_k(k^r, k^s; m, n)$.*

We have already remarked on the necessity of the three conditions. The flexibility of the function $f$, iterated and combined with transpositions in similar fashion to our induction step, lends credence to this conjecture (as do constructions like $dB_k(k^4, k^2; 2, 3)$), at least for large values of $m$ and $n$. Other functions like $f$ would of course be of great use. The techniques of Section 4 might also be of service here and in Question 2 below.

We can also define an $(R, S; m, n)_k$-de Bruijn torus $A$ having dimensions $R \times S$ rather than simply $k^r \times k^s$. When $k$ is a power of a prime $p$ then the sidelengths must be powers of $p$, but in other cases this need not be. Of course we need that $R > m$, $S > n$, and $RS = k^{mn}$, and we are in no position to conjecture that these conditions are also sufficient, as they may very well not be. However, we ask

**Question 5.2.** Does there exist an array $A \in dB_{pq}(p^{mn}, q^{mn}; m, n)$?

Try (!) for example $k = pq = 6$. It seems we most definitely need a new $f$-type function since we may not have property $\sigma$ to use $f$ and we may not obtain property $\tau$ once we do.

In $d$ dimensions we can do the following. Let $\mathbf{R} = (k^{r_1}, \ldots, k^{r_d})$ and $\mathbf{n} = (n_1, \ldots, n_d)$ with $k^{r_i} > n_i$ and $\sum r_i = \Pi n_i$. We call a $d$-dimensional toroidal $k$-ary block $A$ an $(\mathbf{R}; \mathbf{n})_k$-*de Bruijn $d$-torus* if $A$ has dimensions $k^{r_1} \times \cdots \times k^{r_d}$ and every $k$-ary $n_1 \times \cdots \times n_d$ block $B$ appears exactly once contiguously in the $d$-dimensional torus, and write $A \in dB_k^d(\mathbf{R}; \mathbf{n})$.

The methods of Cock [3] can be used in $d$ dimensions to obtain

**Theorem 5.3.** *For all $k, d$, and $\mathbf{n}$ there is an $\mathbf{R}$ such that there is an $(\mathbf{R}; \mathbf{n})_k$-de Bruijn $d$-torus, with the exception that $n_i = 2$ for at most one index $i$ when $k$ is even.*

**Conjecture 5.4.** *If $k, r_1, \ldots, r_d, n_1, \ldots, n_d$ satisfy*

i) $k^{r_i} > n_i$ for all $1 \leq i \leq d$, and

ii) $r_1 + \cdots + r_d = n_1 \cdots n_d$

*then there is an $A \in dB_k^d(\mathbf{R}; \mathbf{n})$.*

In particular, we believe this is true for $n_1 = \cdots = n_d = n$ and $r_1 = \cdots = r_d = n^d/d$; i.e., de Bruijn "$d$-cubes." In dimension 2 we saw that this required either $n$ to be even or $k$ a perfect square when $n$ is odd. More generally, if $d = \Pi p_i^{q_i}$ we require either $(\Pi p_i) | n$ or $k$ is a perfect $p_i^{\text{th}}$ power for all $p_i \nmid n$ (for example $d = 10$, $n = 8$ and $k = 32$). We see in dimension 3 that our main difficulty again lies in finding other $f$-type functions. By using transpositions in dimension 2 we were able to sequentially move from $(\frac{n^2}{2}, \frac{n^2}{2})$ to $(\frac{(n+2)^2}{2}, \frac{(n+2)^2}{2})$. So far this

has not worked for $(\frac{n^3}{3}, \frac{n^3}{3}, \frac{n^3}{3})$. It should also be mentioned that we can ask these questions for general $\mathbf{R} = (R_1, \ldots, R_d)$, where each $R_i$ is not necessarily a power of $k$.

**Conjecture 5.5.** *$d$-dimensional equivalence-class tori exist. That is, for all $k, d$, and* $\mathbf{n}$ *(except $k = d = n_1 = n_2 = 2$) there is an* $\mathbf{R}$ *and an $A \in \overline{dB}_k(\mathbf{R}; \mathbf{n})$ such that every equivalence class of $k$-ary $(n_1 \times \cdots \times n_d)$ blocks is represented uniquely in $A$.*

We mention this conjecture since the 2-dimensional case may very well help us find "3-cubes."

## 6. Acknowledgments

The authors wish to thank the Boston Red Sox and Chicago White Sox for playing the longest 9-inning regular-season game in Major League history (4 hours, 11 minutes, Boston 9–Chicago 6, Fenway Park, May 15, 1991), 7 minutes short of the record set by San Francisco at Los Angeles, (NL Playoff Game 2, LA 8–SF 7, October 2, 1962). Had the game ended on time, we may very well have not finished Lemma 2.2.

## 7. References

1. N.G. de Bruijn, A Combinatorial Problem, Proc. Nederl. Akad. Wetensch. 49 (1946), 758–764.

2. F.R.K. Chung, P. Diaconis and R.L. Graham, Universal Cycles for Combinatorial Structures, to appear in Discrete Math.

3. J.C. Cock, Toroidal tilings from de Bruijn-Good Cyclic Sequences, Disc. Math. 70 (1988), 209–210.

4. C.T. Fan, S.M. Fan, S.L. Ma and M.K. Siu, On de Bruijn arrays, ARS Comb., Vol. 19A (1985), 205–213.

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

6. H.M. Fredricksen, The lexicographically least de Bruijn cycle, J. Combin. Theory 9 (1970), 1–5.

7. H.M. Fredricksen, Generation of the Ford sequence of length $2^n$, $n$ large, J. Combin. Theory 12 (1972), 153–154.

8. H.M. Fredricksen, A class of nonlinear de Bruijn cycles, J. Combin. Theory 19 (1975), 192–199.

9. H.M. Fredricksen and I.J. Kessler, Lexicographic compositions and de Bruijn sequences, J. Combin. Theory 22 (1977), 17–30.

10. H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, SIAM Review 24 (1982), 195–221.

11. I.J. Good, Normally recurring decimals, J. London Math. Soc. 21 (1946), 167–169.

12. B. Grünbaum and G.C. Shephard, Satins and twills: An introduction to the geometry of fabrics, Math. Mag. 53 (1980), 139–161.

13. M. Harwit, Spectrometer imager, Appl. Optics, vol. 10, 1415–1421 (1971).

14. G. Hurlbert, Universal Cycles–On Beyond de Bruijn, Ph.D. Thesis, 1990.

15. A. Iványi and Z. Toth, Existence of deBruijn words, $2^{nd}$ Conf. on Automata, Languages and Programming Systems, Salgótarján, Hungary, 1988, DM88-4, 165–172.

16. J.H. van Lint, E.J. MacWilliams and N.J.A. Sloane, On pseudo-random arrays, SIAM J. Appl. Math. 36 (1979), 62–72.

17. S.L. Ma, A note on binary arrays with a certain window property, IEEE Trans. on Inform. Th., vol. IT-30, No. 5, September 1984, 774–775.

18. F.J. MacWilliams and N.J.A. Sloane, Pseudo-random sequences and arrays, Proc. IEEE 64 (1976), 1715–1729.

19. F.W. Sinden, Sliding Window Codes, AT&T Bell Labs. Tech. Memo, 1985.