JOURNAL OF ALGORITHMS 7, 331–340 (1986)

An Algorithm for Constructing m-ary de Bruijn Sequences

TUVI ETZION

Department of Computer Science, Technion–Israel Institute of Technology, Haifa, Israel

Received June 8, 1984

We present an algorithm for the generation of m-ary de Bruijn cycles. The algorithm generates $m^{kg(n,k)}$ cycles of length m^n, using $3n + kg(n, k)$ storage, where k is a free parameter in the range $1 \le k \le m^{(n-4)/2}$, and $g(n, k)$ is of order $(n - 2\log_m k)(1 - (1/(1 + \log_m k)))$. The time required to produce the next digit from the last n digits is close to n. © 1986 Academic Press, Inc.

1. INTRODUCTION

This paper deals with the construction of de Bruijn cycles over an alphabet $M = \{0, 1, \ldots, m - 1\}$. It is well known [2] that the number of de Bruijn cycles of length m^n is $(m - 1)!^{m^{n-1}} m^{m^{n-1}-n}$. A comprehensive survey about the construction of these cycles for $m = 2$ can be found in [3]. For $m > 2$ only two efficient algorithms are known. The first is by Fredricksen and Maiorana [4] which is an extension of an algorithm by Fredricksen and Kessler [5] for $m = 2$ and the second is by Ralston [6] which is similar to the algorithm by Fredricksen and Maiorana but has some computational advantages. Both algorithms produce only one de Bruijn cycle.

In Section 2 of this paper, we show how to construct $m^{kg(n,k)}$ de Bruijn cycles of length m^n using $kg(n, k)$ storage, where k is a constant in the range $1 \le k \le m^{(n-4)/2}$ and $g(n, k)$ is approximately $(n - 2\log_m k)(1 - (1/(1 + \log_m k)))$. In Section 3, we describe the structure of the de Bruijn cycles which was generated in Section 2. In Section 4, we present an algorithm to generate the de Bruijn cycles of Section 2. The algorithm uses $3n + kg(n, k)$ storage. The time to produce the next digit from the previous n digits is $O(n)$.

0196-6774/86 $3.00

2. Construction of the Cycles

In this section we describe a construction of m-ary de Bruijn cycles. The construction is an extension of the one for $m = 2$ in [1]. To present it, some definitions and lemmas are given.

Consider the set $M = \{0, 1, \ldots, m-1\}$ of m digits, $m \geq 2$, and the set M^n of all the n-tuples formed by the nth cartesian power of M. That is, any element (also called a state) $X \in M^n$ is an n-tuple $X = (x_1, x_2, \ldots, x_n)$ with components $x_i \in M$, $i = 1, 2, \ldots, n$.

The *set of companions* X' of a state $X = (x_1, x_2, \ldots, x_n)$ is a set of states, where $Y = (y_1, y_2, \ldots, y_n) \in X'$ iff $x_i = y_i$ for $i = 1, 2, \ldots, n-1$, $y_n \in M$ and $y_n \neq x_n$.

For $X = (x_1, x_2, \ldots, x_n) \in M^n$ and $Y = (y_1, y_2, \ldots, y_n) \in M^n$ the shift relation $X \to Y$ is defined by

$$X \to Y \quad \text{iff } (x_2, x_3, \ldots, x_n) = (y_1, y_2, \ldots, y_{n-1})$$

A *k-cycle* C is a cyclic sequence of k distinct states, $C = [X^{(1)}, X^{(2)}, \ldots, X^{(k)}]$, such that $X^{(k)} \to X^{(1)}$ and $X^{(i)} \to X^{(i+1)}$, $i = 1, 2, \ldots, k-1$. If $X^{(i)} = (x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)})$ then C can also be represented by the cyclic binary sequence $C = [x_1^{(1)}, x_1^{(2)}, \ldots, x_1^{(k)}]$, where contiguous n-tuples constitute states. Two cycles C_1 and C_2 are said to be *adjacent* if they are (state) disjoint and there exists a state X on C_1 such that a state $Y \in X'$ is on C_2.

The following theorem can be easily verified:

Theorem 1. *Two adjacent cycles C_1 and C_2 with a state X on C_1 and a state $Y \in X'$ on C_2 are forming a single cycle when the predecessors of X and Y are interchanged (the predecessor of X becomes the predecessor of Y, and the predecessor of Y becomes the predecessor X).*

Example 1. For $n = 6$ and $m = 3$ the cycles $C_1 = [0120201222]$ and $C_2 = [01202121112100]$ are adjacent with the state $X = (012020)$ on C_1 and the state $Y = (012021) \in X'$ on C_2. The two cycles are joined into a single cycle C when the predecessors of X and Y are interchanged, i.e., $C = [0120201222012021211121 00]$.

A *factor of* M^n is a set of state disjoint cycles which includes all the states of M^n. Let F be a factor of M^n, if $C = [X^{(1)}, X^{(2)}, \ldots, X^{(k)}] \in F$ we also write $X^{(k)} \xrightarrow{F} X^{(1)}$ and $X^{(i)} \xrightarrow{F} X^{(i+1)}$, $i = 1, 2, \ldots, k-1$.

The *necklaces factor* (NF) is a factor of M^n which is defined by the following property: $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ are on the same NF-cycle iff X is a cyclic shift of Y. The NF factor was used in [4] and [6] to produce de Bruijn cycles.

The σ-*weight* $W_\sigma(X)$ of a state $X = (x_1, x_2, \ldots, x_n)$, where all the x_i are less than or equal to σ, is the number of σ's in X.

The σ-weight $W_\sigma(C)$ of a cycle C from NF is the σ-weight of each of its states.

EXAMPLE 2. For $n = 6$ and $m = 3$ the cycle [120] has 2-weight 2 since its states have 2-weight 2, e.g., the state (120120) has 2-weight 2.

LEMMA 1. *Let C_1 be a cycle of σ-weight $k > 0$ from* NF. *Then there exists a state X on C_1 with a state $Y \in X'$ on a cycle C_2 whose σ-weight is $k - 1$.*

Proof. Since $W_\sigma(C_1) > 0$ there exists a state of the form $S = (s_1, \ldots, s_{n-1}, \sigma)$ on C_1. Hence, each of the states of the form $Y = (s_1, \ldots, s_{n-1}, \sigma - j)$, $1 \le j \le \sigma$, have σ-weight $k - 1$. Therefore, $(s_1, \ldots, s_{n-1}, \sigma - j)$ is a state on an NF-cycle C_2 with $W_\sigma(C_2) = k - 1$ and $Y \in X'$. Q.E.D.

Lemma 1 and Theorem 1 suggest a simple method of joining all the NF-cycles, in order to construct an m-ary de Bruijn cycle. At each step we have a main cycle obtained in the previous steps by joining a subset of the NF-cycles. Initially, the main cycle is chosen to be the unique NF-cycle of 1-weight zero. Next, the main cycle is extended by joining to it the unique cycle of 1-weight one. In general step $jn + i$, $(0 \le j \le m - 2, 1 \le i \le n)$, we extend the main cycle by joining to it all the NF-cycles of $(j + 1)$-weight i (in arbitrary order). This is always possible because the current main cycle contains all of the states whose $(j + 1)$-weight is less than i and since each NF-cycle of $(j + 1)$-weight $i \ge 1$ has a state ending in a $j + 1$, it can be joined (see Theorem 1 and Lemma 1) to the current main cycle. This procedure ends when all the NF-cycles have been joined together.

We proceed now to a precise and detailed description of the proposed construction. Consider the ordered set $V = \{V(i)\}_{i=0}^{k-1}$ of k states for some k, $1 \le k \le m^{(n-4)/2}$, constructed as follows:

(1) The first $\lfloor \log_m k \rfloor$ digits of each $V(i)$ are $m - 1$'s.

(2) The last two digits of each $V(i)$ are an $m - 1$ preceded by a ZERO.

(3) The $\lceil \log_m k \rceil + 1$ digits preceding the last two digits of $V(i)$ form the base-m representation of i. (Note that the first digit is always ZERO.)

(4) In position $(\lfloor \log_m k \rfloor + 1)j$ for integers j satisfying

$$1 \le j \le \left\lfloor \frac{n - \lceil \log_m k \rceil - \lfloor \log_m k \rfloor - 3}{\lfloor \log_m k \rfloor + 1} \right\rfloor$$

each $V(i)$ has a ZERO.

(5) The remaining digits for each $V(i)$ are chosen arbitrarily.

EXAMPLE 3. For $m = 3$, $n = 15$, and $k = 8$, the set V for these values of m, n, and $\hat{k}$, V takes the form

$$20x_1^{(1)}0x_2^{(1)}0x_3^{(1)}0x_4^{(1)}000002$$
$$20x_1^{(2)}0x_2^{(2)}0x_3^{(2)}0x_4^{(2)}000102$$
$$20x_1^{(3)}0x_2^{(3)}0x_3^{(3)}0x_4^{(3)}000202$$
$$20x_1^{(4)}0x_2^{(4)}0x_3^{(4)}0x_4^{(4)}001002$$
$$20x_1^{(5)}0x_2^{(5)}0x_3^{(5)}0x_4^{(5)}001102$$
$$20x_1^{(6)}0x_2^{(6)}0x_3^{(6)}0x_4^{(6)}001202$$
$$20x_1^{(7)}0x_2^{(7)}0x_3^{(7)}0x_4^{(7)}002002$$
$$20x_1^{(8)}0x_2^{(8)}0x_3^{(8)}0x_4^{(8)}002102$$

where the $x_j^{(i)}$ are free parameters.

It can be easily verified for each $V(i)$ that there is always a unique cyclic run of $\lfloor \log_m k \rfloor + 1$ $m-1$'s, and that every pair of states differ in their last $\lceil \log_m k \rceil + 2$ digits. Therefore, because the necklaces formed by permutation of the $V(i)$'s are all different, we have the following lemma:

LEMMA 2. *No two states of V belong to the same NF-cycle.*

The construction of a de Bruijn cycle from the NF-cycles proceeds by a sequence of joins where at each step a new NF-cycle is joined to the current main cycle. A join is performed by means of a state X and a state $Y \in X'$, with X on the NF-cycle C which is joined to the main cycle and Y on the current main cycle. The states X and Y are called the *bridging states* of the join. Let X be the chosen bridging state on C. The factor that contains the current main cycle and the remaining cycles is called FX. The bridging states X and $Y \in X'$ for a cycle C, with X on C are determined by the following two rules:

(R.1) If C contains a state from a chosen set V then this state is chosen as X. If $X = (x_1, x_2, \ldots, x_{n-1}, m-1)$ then $Y \in X'$ is chosen as the state that fulfills the condition $(m-2, x_1, \ldots, x_{n-1}) \overset{FX}{\rightarrow} Y$.

(R.2) Otherwise, if $C = [c_1, c_2, \ldots, c_r]$ and $t = \max_{1 \le i \le r} c_i$, then X is the minimal state that ends with a t (when the states are viewed as numbers in base-m notation) on the cycle. If $X = (x_1, x_2, \ldots, x_{n-1}, t)$ then $Y \in X'$ is chosen as the state that fulfill the condition $(t-1, x_1, \ldots, x_{n-1}) \overset{FX}{\rightarrow} Y$.

As stated Y is on the current main cycle and X is on the cycle C in line. By Theorem 1, the interchanging of the predecessors of X and Y on C and FX will generate the next main cycle.

LEMMA 3. *Let $V(i)$ be a state in an* NF*-cycle C, for some i. Then $V(i)$ is not the minimal state (viewed as a number in base-m notation) among all the states of C that end with $m-1$.*

Proof. Let $V(i) = ((m-1)^j 0 Q(m-1))$ for some $j \geq 1$ and where the number of digits in Q is $n-j-2$. Hence, $(0Q(m-1)^{j+1})$ is a state in C which is less than $V(i)$, where both states are viewed as numbers in base-m notation. Q.E.D.

Now, it can be readily verified that each state can serve only once as a bridging state.

3. The Structure of the Constructed de Bruijn Cycle

We describe the structure of the de Bruijn cycles that was constructed in Section 2. There are three possibilities for consecutive states on every main cycle during the construction of the de Bruijn cycle.

$$(x_1, x_2, \ldots, x_n) \to (x_2, \ldots, x_n, x_1), \tag{1}$$

$$(x_1, x_2, \ldots, x_n) \to (x_2, \ldots, x_n, x_1 + 1), \tag{2}$$

$$(x_1, x_2, \ldots, x_n) \to (x_2, \ldots, x_n, x_1 - j) \quad \text{for some } j,\ x_1 \geq j \geq 1. \tag{3}$$

In (1) both states come from the same NF-cycle. In (2) and (3) the two states come from different NF-cycles.

In the sequel, let DB be the factor which contains the de Bruijn cycle. The following lemmas present the situation of consecutive states on the de Bruijn cycle.

LEMMA 4. $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\to} (x_2, \ldots, x_n, x_1)$ *if* $x_1 + 1 < x_i$ *for some* i, $2 \leq i \leq n$.

Proof. $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\to} (x_2, \ldots, x_n, x_1 + 1)$ contradicts the fact that $x_i > x_1 + 1$ and rule (R.2) for choosing the bridging states. Assume $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\to} (x_2, \ldots, x_n, x_1 - j)$ for some $x_1 \geq j \geq 1$. Therefore $(x_1 - j, x_2, \ldots, x_n) \overset{\text{DB}}{\to} (x_2, \ldots, x_n, x_1 - j + 1)$. But this contradicts the fact that $x_i > x_1 + 1 > x_1 - j + 1$ and rule (R.2) for choosing the bridging states. Hence, $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\to} (x_2, \ldots, x_n, x_1)$. Q.E.D.

LEMMA 5. (1) *Let* $(x_1, x_2, \ldots, x_{n-1}, m-1)$ *be a state from the set* V. *Then*

$$(m-2, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\to} (x_1, x_2, \ldots, x_{n-1}, m-1),$$

$$(m-1, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\to} (x_1, x_2, \ldots, x_{n-1}, m-2).$$

(2) *Let* $(x_1, x_2, \ldots, x_{n-1}, m-1)$ *be the nonempty cyclic shift of a state from* V. *Then*

$$(m-2, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, m-2),$$

$$(m-1, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, m-1).$$

Proof. (1) By rule 1 for choosing the bridging states $(m-2, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, m-1)$. Since $x_j = m-1$ for some j, $1 \le j \le n-1$, then by Lemma 4 $(\sigma, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, \sigma)$ for $\sigma < m-2$. Hence, $(m-1, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, m-2)$.

(2) It follows from the facts that the only state of the cycle $[x_1, x_2, \ldots, x_{n-1}, m-1]$ chosen as the bridging states is from V, and by Lemma 4 $(\sigma, x_1, x_2, \ldots, x_{n-1}) \overset{\text{DB}}{\rightarrow} (x_1, x_2, \ldots, x_{n-1}, \sigma)$ for $\sigma < m-2$.

Q.E.D.

LEMMA 6. $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\rightarrow} (x_2, \ldots, x_n, x_1 + 1)$ *if* $x_1 \ge x_i$ *for every* i, $1 \le i \le n-1$, *and* $x_1 \ne m-1$.

Proof. By rule (R.2) of choosing the bridging states. Q.E.D.

LEMMA 7. $(m-1, 0, 0, \ldots, 0) \overset{\text{DB}}{\rightarrow} (0, 0, \ldots, 0)$.

Proof. By Lemma 6 we have

$$(0, 0, 0, \ldots, 0) \overset{\text{DB}}{\rightarrow} (0, 0, \ldots, 0, 1),$$

$$(1, 0, 0, \ldots, 0) \overset{\text{DB}}{\rightarrow} (0, 0, \ldots, 0, 2),$$

$$\vdots$$

$$(m-2, 0, 0, \ldots, 0) \overset{\text{DB}}{\rightarrow} (0, 0, \ldots, 0, m-1).$$

Hence, $(m-1, 0, 0, \ldots, 0) \overset{\text{DB}}{\rightarrow} (0, 0, \ldots, 0, 0)$. Q.E.D.

LEMMA 8. *Let* $S = (x_1, x_2, \ldots, x_n)$, $x_r = x_1 + 1 \triangleq t$ *for some* r, $2 \le r \le n$, $x_r \ge x_i$ *for every* i, *and* $(x_2, \ldots, x_n, t)$ *is not a state from* V.

(1) If $(x_2, \ldots, x_n, t)$, is the minimal state of this cycle from all the shifts that end with t then $(x_1, x_2, \ldots, x_n) \overset{\text{DB}}{\rightarrow} (x_2, \ldots, x_n, x_1 + 1)$;

(2) otherwise $(x_1, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, x_1)$.

Proof. Follows directly from rule (R.2) of choosing the bridging states. Q.E.D.

LEMMA 9. *Let* $S = (m-1, x_2, \ldots, x_n)$ *be a state which is not a shift of a state from* V *and* $t = \max_{2 \le i \le n} x_i$, $t \neq 0$. *Then,*

(1) If $(x_2, \ldots, x_n, t)$ is the minimal shift that ends with a t then

$$(m-1, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, t-1);$$

(2) otherwise $(m-1, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, t)$.

Proof. (1) By Lemma 5 $(\sigma, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, \sigma)$ for $0 \le \sigma \le t-2$. By Lemmas 6 and 8 we have

$$\begin{aligned}
(t-1, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, t), \\
(t, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, t+1), \\
&\vdots \\
(m-2, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, m-1).
\end{aligned}$$

Hence, $(m-1, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, t-1)$

(2) By Lemmas 6 and 8 we have:

$$\begin{aligned}
(t-1, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, t-1), \\
(t, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, t+1), \\
(t+1, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, t+2), \\
(m-2, x_2, \ldots, x_n) &\overset{DB}{\to} (x_2, \ldots, x_n, m-1),
\end{aligned}$$

Hence, $(m-1, x_2, \ldots, x_n) \overset{DB}{\to} (x_2, \ldots, x_n, t)$. Q.E.D.

4. A Digit-by-Digit Algorithm

Lemmas 4–9 of Section 3 lead to an algorithm which generate an m-ary de Bruijn cycle digit-by-digit. In the algorithm the $(i+n)$th digit σ_{i+n} is determined from the preceding n-digit state $S_i = (\sigma_i, \sigma_{i+1}, \ldots, \sigma_{i+n-1})$. The formal steps for determining σ_{i+n} are presented in the following algorithm.

Algorithm A

Choose k such that $1 \le k \le m^{(n-4)/2}$. Choose and store an ordered set of bridging states $V = \{V(i)\}_{i=0}^{k-1}$. Initially, set $S_0 = (0, 0, \ldots, 0) = 0^n$. Given $S_i = (\sigma_i, \sigma_{i+1}, \ldots, \sigma_{i+n-1})$, proceed to produce $S_{i+1} = (\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{i+n})$, as follows:

(A.1) If $S_i = (m-1, 0, 0, \ldots, 0)$ then set $\sigma_{i+n} = 0$ (see Lemma 7).

(A.2) If $\sigma_i \ge m-2$ then examine the cyclic shifts of $S_i^* = (\sigma_{i+1}, \ldots, \sigma_{i+n-1}, m-1)$ for the existence of a shift α that begins with $\lfloor \log_m k \rfloor$ $m-1$'s and ends with an $m-1$. If no such α exists or $\sigma_i < m-2$ go to (A.4).

(A.3) Let α^* be the first $\lceil \log_m k \rceil + 1$ digits of the last $\lceil \log_m k \rceil + 3$ digits of α, and let $|\alpha^*| = j$, the base-m value of α^*. If $j > k-1$ go to (A.4); if $\alpha = V(j) \ne S_i^*$ then set $\sigma_{i+n} = \sigma_i$; if $\alpha = V(j) = S_i^*$ then set $\sigma_{i+n} = m-1$ if $\sigma_i = m-2$ and set $\sigma_{i+n} = m-2$ if $\sigma_i = m-1$ (see Lemma 5).

(A.4) If $\sigma_i \ge \sigma_j$ for every j such that $i+1 \le j \le i+n-1$ and $\sigma_i \ne m-1$ then set $\sigma_{i+n} = \sigma_i + 1$ (see Lemma 6).

(A.5) If $\sigma_j > \sigma_i + 1$ for some j such that $i+1 \le j \le i+n-1$ then set $\sigma_{i+n} = \sigma_i$ (see Lemma 4).

(A.6) If $\sigma_i + 1 \ge \sigma_j$ for every j such that $i+1 \le j \le i+n-1$ and there exists an r such that $\sigma_r = \sigma_i + 1$ then find the cyclic shift β of $S_i^+ = (\sigma_{i+1}, \ldots, \sigma_{i+n-1}, \sigma_i + 1)$ such that β ends with a $t = \sigma_i + 1$, and β is minimal in base m notation among all the shifts that end with t. If $\beta = S_i^+$ then set $\sigma_{i+n} = \sigma_i + 1$; otherwise set $\sigma_{i+n} = \sigma_i$ (see Lemma 8).

(A.7) If $\sigma_i = m-1$ then let $t = \max_{i+1 \le j \le i+n-1} \sigma_j$. Find the cyclic shift γ of $S_i^x = (\sigma_{i+1}, \ldots, \sigma_{i+n-1}, t)$ such that γ ends with t and γ is minimal among all the shifts that end with t. If $\gamma = S_i^x$ then set $\sigma_{i+n} = t-1$; otherwise set $\sigma_{i+n} = t$ (see Lemma 9).

Example 4. For $m = 3$ $n = 4$, we have $k = 1$. The set V for these values of m, n, and k is $V = \{(0002)\}$ and only one 3-ary de Bruijn cycle is

produced by Algorithm A:

[00001111222212211211211102222
02210212021101220121011 2011
00220021001200101020201000 2]

THEOREM 2. (1) *For every choice of* k, *in the indicated range, and of the set* V *Algorithm* A *produces an* m-ary *de Bruijn cycle.*

(2) *For a given choice of* k *there are* $m^{kg(n,k)}$ *distinct choices for the set* V, *where*

$$g(n,k) = n - 3 - \lceil \log_m k \rceil - \lfloor \log_m k \rfloor - \left\lceil \frac{n - \lceil \log_m k \rceil - \lfloor \log_m k \rfloor - 3}{\lfloor \log_m k \rfloor + 1} \right\rceil.$$

Thus, Algorithm A *can be used to produce* $m^{kg(n,k)}$ *distinct* m-ary *de Bruijn cycles.*

(3) *The working space that Algorithm* A *requires to produce an* m-ary *de Bruijn cycle is* $3n + kg(n,k)$ *places and the work required to produce the next digit from the current* n *digits is* $O(n)$ *operations on* n-*digits.*

Proof. (1) follows directly the discussion preceding Algorithm A in Section 2.

(2) is due to the fact that each $V(i)$ is specified up to exactly $g(n,k)$ free parameters and no state can be chosen by both criteria of choosing X: either by being a member of the set V or by representing the minimal shift. This together with Lemma 2, imply that distinct choices for the set V correspond to distinct sets of bridging state and, hence to distinct de Bruijn cycles.

(3) follows directly from Algorithm A. Note that only information about members of the set V has to be stored and, there, only the $g(n,k)$ free digit-values of each $V(i)$ require storage. Q.E.D.

ACKNOWLEDGMENTS

The author wishes to thank the referee for his valuable comments. Also he thanks Oded Goldreich for his help and a special thanks to Orna Malinsky for her support.

REFERENCES

1. T. ETZION AND A. LEMPEL Algorithms for the generation of full-length shift-register sequences, *IEEE Trans. Inform. Theory* IT-30 (1984), 480–484.

2. C. FLYE-SAINTE MARIE, Solution to problem number 58, *Interme. Mathe.* 1 (1894), 107–110.
3. H. M. FREDRICKSEN, A survey of full length nonlinear shift register cycle algorithms, *SIAM Rev.* **24** (1982), 195–221.
4. H. M. FREDRICKSEN AND J. MAIORANA, Necklaces of beads in k colors and k-ary de Bruijn sequences, *Discrete Math.* **23** (1978), 207–210.
5. H. M. FREDRICKSEN AND I. J. KESSLER, Lexicographic compositions and de Bruijn sequences, *J. Combin. Theory* **22** (1977), 17–30.
6. A. RALSTON, A new memoryless algorithm for de Bruijn sequences, *J. Algorithms* **2** (1981), 50–62.