JOURNAL OF COMBINATORIAL THEORY, Series A 34, 248–251 (1983)

Note

There Are No De Bruijn Sequences of Span n with Complexity $2^{n-1}+n+1$

RICHARD A. GAMES

Department of Mathematics, Colorado State University, Fort Collins, Colorado 80523

Communicated by the Managing Editors

Received March 19, 1982

If $\mathbf{s} = (s_0, s_1, ..., s_{2^n-1})$ is a binary de Bruijn sequence of span n, then it has been shown that the least length of a linear recursion that generates $\mathbf{s}$, called the complexity of $\mathbf{s}$ and denoted by $c(\mathbf{s})$, is bounded for $n \geqslant 3$ by $2^{n-1}+n \leqslant c(\mathbf{s}) \leqslant 2^n - 1$. A numerical study of the allowable values of $c(\mathbf{s})$ for $3 \leqslant n \leqslant 6$ found that all values in this range occurred except for $2^{n-1}+n+1$. It is proven in this note that there are no de Bruijn sequences of complexity $2^{n-1}+n+1$ for all $n \geqslant 3$.

A binary de Bruijn sequence $\mathbf{s} = (s_0, s_1, s_2, ...)$ of span n is a periodic sequence of period 2^n with the property that the 2^n vectors $\mathbf{s}_i = (s_i, s_{i+1}, ..., s_{i+n-1})$, $i = 0, 1, 2, ..., 2^n - 1$ are all the distinct binary n tuples. In this note the sequence $\mathbf{s}$ will be represented by a single period, $\mathbf{s} = (s_0, s_1, ..., s_{2^n-1})$. If $\mathbf{s}$ is a binary de Bruijn sequence of span n, then [1] showed that the least length of a linear recursion that generates $\mathbf{s}$, called the *complexity* of $\mathbf{s}$ and denoted by $c(\mathbf{s})$, is bounded for $n \geqslant 3$ by $2^{n-1}+n \leqslant c(\mathbf{s}) \leqslant 2^n - 1$. A numerical study of the allowable values of $c(\mathbf{s})$ for $3 \leqslant n \leqslant 6$ found that all values in this range occurred except for $2^{n-1}+n+1$, see [1]. We show that there are no de Bruijn sequences of complexity $2^{n-1}+n+1$ for all $n \geqslant 3$ by first showing that the weight of one period of $D^n(\mathbf{s})$ is twice an odd number. Here $D = E + 1$, where E is the sequence shift operator, $(E\mathbf{s})_i = s_{i+1}$; so that if $\mathbf{s} = (s_0, s_1, ..., s_{2^n-1})$, then $D\mathbf{s} = ((D\mathbf{s})_0, (D\mathbf{s})_1, ..., (D\mathbf{s})_{2^n-1}) = (s_0 + s_1, s_1 + s_2, ..., s_{2^n-1} + s_0)$. We remark that if $\mathbf{s}$ is regarded as a sequence of n tuples, $\mathbf{s} = (\mathbf{s}_0, \mathbf{s}_1, ..., \mathbf{s}_{2^n-1})$, then $D\mathbf{s}$ corresponds to a sequence of $(n-1)$ tuples, namely, $(\hat{D}\mathbf{s}_0, \hat{D}\mathbf{s}_1, ..., \hat{D}\mathbf{s}_{2^n-1})$, where $\hat{D}\mathbf{s}_i = \hat{D}(s_i, s_{i+1}, ..., s_{i+n-1}) = (s_i + s_{i+1}, s_{i+1} + s_{i+2}, ..., s_{i+n-2} + s_{i+n-1})$. So $\hat{D}: GF(2)^n \to GF(2)^{n-1}$ is the homomorphism of [3] which maps the de Bruijn graph G_n to the de Bruijn graph G_{n-1}.

A de Bruijn sequence $\mathbf{s} = (s_0, s_1, ..., s_{2^n-1})$ of span n satisfies an n-stage

0097-3165/83 $3.00

nonlinear recursion; that is, $\mathbf{s}$ is a sequence of maximum period 2^n generated by some n-stage (nonlinear) feedback shift register. This recursion has the form, for $i = 0, 1, 2, \ldots, 2^n - 1$ (all subscripts computed modulo 2^n) $s_{i+n} = s_i + f(s_{i+1}, s_{i+2}, \ldots, s_{i+n-1})$ for some Boolean function $f\colon GF(2)^{n-1} \to GF(2)$ [2, p. 115]. The *weight* of f, denoted by $\mathrm{wt}(f)$, is the number of ones in the image vector $(f(\mathbf{x})\colon \mathbf{x} \in GF(2)^{n-1})$. The *weight* of a periodic sequence $\mathbf{s}$, denoted by $\mathrm{wt}(\mathbf{s})$, is the number of ones in a single period of $\mathbf{s}$.

THEOREM 1. *If* $\mathbf{s}$ *is a de Bruijn sequence of span n generated by the Boolean function* $f\colon GF(2)^{n-1} \to GF(2)$, *then* $\mathrm{wt}(f)$ *is odd.*

Proof. See [2, p. 122].

In general, if $g(E) = a_0 + a_1 E + \cdots + a_{n-1} E^{n-1}$ with $a_i \in GF(2)$, $i = 0, 1, \ldots, n-1$, and if $(x_0, x_1, \ldots, x_{n-1}) \in GF(2)^n$ (regarded as a sequence of period n), then $g(E)\,\mathbf{x} = ((g(E)\,\mathbf{x})_0, (g(E)\,\mathbf{x})_1, \ldots, (g(E)\,\mathbf{x})_{n-1})$, where $(g(E)\,\mathbf{x})_i = a_0 x_i + a_1 x_{i+1} + \cdots + a_{n-1} x_{i+n-1}$ (subscripts mod n). For convenience we write $g(E)_i\,\mathbf{x}$ for $(g(E)\,\mathbf{x})_i$ so that, in particular, $g(E)_0$ can be regarded as a linear transformation from $GF(2)^n$ to $GF(2)$ defined by $g(E)_0$: $(x_0, x_1, \ldots, x_{n-1}) \mapsto a_0 x_0 + a_1 x_1 + \cdots + a_{n-1} x_{n-1}$.

THEOREM 2. *If* $g(E) = a_0 + a_1 E + \cdots + a_{n-1} E^{n-1}$ *with* $a_i \in GF(2)$, $i = 0, 1, \ldots, n-1$, *and some* $a_i \neq 0$, *then* $|\{\mathbf{x} \in GF(2)^n\colon g(E)_0\,\mathbf{x} = 0\}| = |\{\mathbf{x} \in GF(2)^n\colon g(E)_0\,\mathbf{x} = 1\}| = 2^{n-1}$.

Proof. Here, $g(E)_0$ is a nonzero linear transformation so image$(g(E)_0) = GF(2)$ and kernel$(g(E)_0) = \{\mathbf{x} \in GF(2)^n\colon g(E)_0\,\mathbf{x} = 0\}$. Since image$(g(E)_0) \cong GF(2)^n/$kernel$(g(E)_0)$, $|$kernel$(g(E)_0| = 2^{n-1}$ and $|\{\mathbf{x} \in GF(2)^n\colon g(E)_0\,\mathbf{x} = 1\}| = 2^n - 2^{n-1} = 2^{n-1}$.

COROLLARY 3. *Let* $\mathbf{s}$ *be a binary de Bruijn sequence of span n, then*

$$\mathrm{wt}(\mathbf{s}) = \mathrm{wt}(D\mathbf{s}) = \cdots = \mathrm{wt}(D^{n-1}\mathbf{s}) = 2^{n-1}.$$

Proof. Let $g(E) = (E+1)^k = D^k$, $k = 0, 1, 2, \ldots, n-1$, and let $\mathbf{s} = (\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{2^n-1})$. Writing, as before, $D_i^k\mathbf{s}$ for $(D^k\mathbf{s})_i$, then $D_i^k\mathbf{s} = D_0^k\mathbf{s}_i$ since degree $D^k \leqslant n-1$ so that $D_i^k\mathbf{s}$ can only involve at most $s_i, s_{i+1}, \ldots, s_{i+n-1}$, which are the coordinates of $\mathbf{s}_i$. Thus, $D^k\mathbf{s} = (D_0^k\mathbf{s}_0, D_0^k\mathbf{s}_1, \ldots, D_0^k\mathbf{s}_{2^n-1})$, and now the theorem applies since $GF(2)^n = \{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{2^n-1}\}$. See also [1, Theorem 8].

In Theorem 4 the weight of $D^n(\mathbf{s})$ is considered.

THEOREM 4. *If* $\mathbf{s} = (s_0, s_1, \ldots, s_{2^n-1})$ *is a de Bruijn sequence of span n, then* $\mathrm{wt}(D^n\mathbf{s}) = 2x$, *where x is odd.*

Proof. If $\mathbf{s} = (\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{2^n-1})$, where $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+n})$ ($(n+1)$ tuples), then, as in Corollary 3, $D^n(\mathbf{s}) = (D_0^n \mathbf{s}_0, D_0^n \mathbf{s}_1, \ldots, D_0^n \mathbf{s}_{2^n-1})$. In addition, $D_0^n(\mathbf{s}_i) = (E+1)_0^n (s_i, s_{i+1}, \ldots, s_{i+n}) = (1 + Eg(E) + E^n)_0 (s_i, s_{i+1}, \ldots, s_{i+n}) = s_i + s_{i+n} + g(E)_0 (s_{i+1}, s_{i+2}, \ldots, s_{i+n-1})$, where $g(E) = ((E+1)^n - 1 - E^n)/E$ is a polynomial in E of degree $\leqslant n-2$. If $f: GF(2)^{n-1} \to GF(2)$ represents the Boolean function which generates s, then $s_{i+n} = s_i + f(s_{i+1}, s_{i+2}, \ldots, s_{i+n-1})$ so that $D_0^n \mathbf{s}_i = f(s_{i+1}, s_{i+2}, \ldots, s_{i+n-1}) + g(E)_0 (s_{i+1}, s_{i+2}, \ldots, s_{i+n-1})$. Note that $D_0^n(\mathbf{s}_i)$ only depends on $s_{i+1}, s_{i+2}, \ldots, s_{i+n-1}$.

Let $I = \{i: 0 \leqslant i \leqslant 2^n - 1, s_i = 0\}$ and $J = \{j: 0 \leqslant j \leqslant 2^n - 1, s_j = 1\}$. Then $I \cap J = \phi$ and since s is de Bruijn, $|I| = |J| = 2^{n-1}$ and $\{(s_{i+1}, s_{i+2}, \ldots, s_{i+n-1}): i \in I\} = \{(s_{j+1}, s_{j+2}, \ldots, s_{j+n-1}): j \in J\} = GF(2)^{n-1}$. Since $D_0^n(\mathbf{s}_i)$ does not depend on s_i, $\mathrm{wt}(D_0^n \mathbf{s}_i: i \in I) = \mathrm{wt}(D_0^n \mathbf{s}_j: j \in J)$ so that, since $\mathrm{wt}(D^n(\mathbf{s})) = \mathrm{wt}(D_0^n \mathbf{s}_i: i \in I) + \mathrm{wt}(D_0^n \mathbf{s}_j: j \in J)$, it is enough to show that $\mathrm{wt}(D_0^n \mathbf{s}_i: i \in I)$ is odd.

Note that $\mathrm{wt}(D_0^n \mathbf{s}_i: i \in I) = \mathrm{wt}(H\mathbf{x}: \mathbf{x} \in GF(2)^{n-1})$, where $H: GF(2)^{n-1} \to GF(2)$ is defined by $H\mathbf{x} = f(\mathbf{x}) + g(E)_0 \mathbf{x}$. It then follows, by summing over $GF(2)^{n-1}$ that $\mathrm{wt}(H) \equiv \mathrm{wt}(f) + \mathrm{wt}(g(E)_0) \pmod 2$. Now $\mathrm{wt}(f)$ is odd by Theorem 1 and $\mathrm{wt}(g(E)_0)$ is even, either because $g(E)_0 \equiv 0$ or by Theorem 2. Hence, $\mathrm{wt}(D_0^n \mathbf{s}_i: i \in I)$ is odd.

COROLLARY 5. *If* s *is a de Bruijn sequence of span* 2^k, $k \in \mathbb{N}$, *generated by the Boolean function* $f: GF(2)^{n-1} \to GF(2)$, *then* $\mathrm{wt}(D^n(\mathbf{s})) = 2\mathrm{wt}(f)$.

Proof. For $n = 2^k$, $(E+1)^n = E^n + 1$, and so $g(E) \equiv 0$ in the theorem. Thus, $H = f$ and $\mathrm{wt}(D^n \mathbf{s}_i: i \in I) = \mathrm{wt}(f)$. Thus, $\mathrm{wt}(D^n \mathbf{s}) = 2\mathrm{wt}(f)$.

THEOREM 6. *Let* $\mathbf{s} = (s_0, s_1, \ldots, s_{2^n-1})$ *be a periodic sequence of period* 2^n, *then* $c(\mathbf{s}) = 2^{n-1} + 1$ *if and only if* $\mathbf{s} = (\mathbf{r} \,\vdots\, \bar{\mathbf{r}})$, *where* $\mathbf{r}$ *is a vector of length* 2^{n-1}, *and* $\bar{\mathbf{r}}$ *denotes the complement of* $\mathbf{r}$.

Proof. See [1, Theorem 2].

THEOREM 7. *There are no de Bruijn sequences of span* $n \geqslant 3$ *with complexity* $2^{n-1} + n + 1$.

Proof. Suppose s is a de Bruijn sequence of span n with complexity $2^{n-1} + n + 1$. Since $c(D\mathbf{s}) = c(\mathbf{s}) - 1$ (see [1]), the complexity of $D^n(\mathbf{s})$ is $2^{n-1} + 1$. So Theorem 6 implies $D^n \mathbf{s} = (\mathbf{r} \,\vdots\, \bar{\mathbf{r}})$, where $\mathbf{r}$ is a vector of length 2^{n-1}. Then it follows that $\mathrm{wt}(D^n \mathbf{s}) = 2^{n-1}$ which contradicts Theorem 4, for $n \geqslant 3$.

ACKNOWLEDGMENT

The author wishes to acknowledge the referee's suggestions concerning the final form of this paper.

REFERENCES

1. A. H. CHAN, R. A. GAMES, AND E. L. KEY, On the complexities of de Bruijn sequences, *J. Combin. Theory Ser. A* **33** (1982), 233–246.
2. S. W. GOLOMB, "Shift Register Sequences," Holden–Day, San Francisco, 1967.
3. A. LEMPEL, On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers, *IEEE Trans. Comput.* **C–19** (1970), 1204–1209.