515–534, 1982.
[27] A. Shamir, "The strongest knapsack-based cryptosystem?" presented at Crypto '82, Santa Barbara, CA, August 1982.
[28] Y. Desmedt, J. Vandewalle, and R. Govaerts, "A general public key cryptographic knapsack algorithm based on linear algebra," in *Proc. IEEE Int. Symp. Inform. Theory*, Abstract of papers, St. Jovite, Quebec, 1983, Sept. 26–30, 1983, pp. 129–130.
[29] E. F. Brickell, "A new knapsack based cryptosystem," Internal Rep., Sandia National Laboratories, Albuquerque, NM.
[30] J. C. Lagarias, "Knapsack-type public key cryptosystems and diophantine approximation," extend abstract in *Advances in Cryptology, Proc. Crypto'83*, D. Chaum, Ed. New York: Plenum, pp. 3–24.
[31] E. F. Brickell, "Solving low density knapsacks in polynomial time," in *Proc. IEEE Int. Symp. Inform. Theory*, Abstract of papers, St. Jovite, PQ, Canada, Sept. 26–30, 1983, p. 130.

On the Distribution of de Bruijn Sequences of Given Complexity

TUVI ETZION AND ABRAHAM LEMPEL, FELLOW, IEEE

Abstract—**The distribution $\gamma(c,n)$ of de Bruijn sequences of order n and linear complexity c is investigated. It is shown that for $n \geqslant 4$, $\gamma(2^n-1,n) \equiv 0 \pmod 8$, and for $k \geqslant 3$, $\gamma(2^{2k}-1,2k) \equiv 0 \pmod{16}$. It is also shown that $\gamma(c,n) \equiv 0 \pmod 4$ for all c, and $n \geqslant 3$ such that cn is even.**

I. Introduction

In this paper we investigate the distribution of binary de Bruijn sequences of given linear complexity. The linear complexity $C(S)$ of a sequence S is one of the measures of its predictability—S is completely determined by $2C(S)$ consecutive bits. Although high complexity does not necessarily mean low predictability, the converse is always true: low complexity implies high predictability. In many applications it is therefore important to know the linear complexity.

In the sequel we need the following definitions and notation.

Let $s_1, s_2, \cdots$, denote a string of binary digits. A cyclic, or closed, string is called a *sequence* and is denoted by $S = [s_0, s_1, \cdots, s_{k-1}]$, where $k = l(S)$ is the *length* of S. The *order* of a sequence $S = [s_0, s_1, \cdots, s_{k-1}]$, is the least integer n such that the n-tuples, $V_i = (s_i, s_{i+1}, \cdots, s_{i+n-1})$, $0 \leqslant i \leqslant k-1$, with subscripts taken modulo k, are all distinct. Such sequences can be viewed as k-cycles from a feedback shift register of n-stages, where the n-tuples V_i are successive *states* of the register (or of the sequence).

Two sequences S_1 and S_2 are said to be *equivalent*, $S_1 \simeq S_2$, if one is a cyclic shift of the other.

A sequence S of length 2^n and order n is called a *de Bruijn sequence*. Note that each of the possible 2^n n-tuples appears exactly once as a state of S. The set of all de Bruijn sequences of order n will be denoted by $DS(n)$.

The *complement* $\boldsymbol{c}S$ and the *reverse* $\boldsymbol{r}S$ of a string $S = s_0, s_1, \cdots, s_{k-1}$ are defined by $\boldsymbol{c}S = \bar{s}_0, \bar{s}_1, \cdots, \bar{s}_{k-1}$, where $\bar{s}_i$ is the binary complement of s_i, and $\boldsymbol{r}S = s_{k-1}, \cdots, s_1, s_0$.

Note that the operators $\boldsymbol{c}$ and $\boldsymbol{r}$ commute.

S is called a *CR-sequence* if $\boldsymbol{c}S \simeq \boldsymbol{r}S$, or equivalently $\boldsymbol{cr}S \simeq S$.

Every sequence $S = [s_0, s_1, \cdots, s_{k-1}]$, satisfies a linear recursion of degree $m \leqslant k$,

$$s_{i+m} + \sum_{j=1}^{m} a_j s_{i+m-j} = 0, \qquad i \geqslant 0.$$

In terms of a *shift operator* E, defined by

$$Es_i = s_{i+1},$$

the linear recursion takes the form

$$\left(E^m + \sum_{j=1}^{m} a_j E^{m-j}\right) s_i = 0, \qquad i \geqslant 0.$$

Let $f(E)s_i = 0$, $i \geqslant 0$, be the linear recursion of least degree satisfied by S. Then the *complexity* $C(S)$ of S is defined as the degree of $f(E)$ viewed as a polynomial in E. For later reference, we state the following known facts [1], [2]:

Fact 1: $S \in DS(n)$ implies $\boldsymbol{c}S \in DS(n)$ and $\boldsymbol{r}S \in DS(n)$. If S is a *CR*-sequence, so are $\boldsymbol{c}S$ and $\boldsymbol{r}S$.

Fact 2: If S is a sequence whose length is a power of 2 then $C(S) = c$ if and only if $(E+1)^{c-1}s_i = 1$, $i \geqslant 0$.

Fact 3: Let $\gamma(c,n)$ denote the number of de Bruijn sequences of order n and complexity c. Then, for $n \geqslant 3$ $\gamma(c,n) \equiv 0 \pmod 2$, and for all $n = 2k \geqslant 4$, $\gamma(c,n) \equiv 0 \pmod 4$.

Manuscript received February 24, 1983; revised December 19, 1983.
The authors are with the Department of Computer Science, Technion, Haifa, Israel.

0018-9448/84/0700-0611$01.00

The last result is obtained by considering, along with $S \in DS(n)$, the sequences $\boldsymbol{c}S$, $\boldsymbol{r}S$, and $\boldsymbol{cr}S$, which are pairwise *inequivalent* de Bruijn sequences of the same complexity. This technique does not work for odd n in which case S could be a *CR*-sequence.

In Section II we investigate the value of $\gamma(c, n)$ for $c = 2^n - 1$, and we prove that for $n \geqslant 4$, $\gamma(2^n - 1, n) \equiv 0 \pmod 8$, and for $k \geqslant 3$, $\gamma(2^{2k} - 1, 2k) \equiv 0 \pmod{16}$. Chan *et al.* [2] conjectured that $\gamma(c, n) \equiv 0 \pmod 4$. In Section III we prove this conjecture for all c and $n \geqslant 3$ such that cn is even.

II. On the Value of $\gamma(2^n - 1, n)$

It is well known [1] that the maximal complexity of de Bruijn sequences of length 2^n is $2^n - 1$. In this section we prove that $\gamma(2^n - 1, n) \equiv 0 \pmod 8$ for $n \geqslant 4$, and that $\gamma(2^{2k} - 1, 2k) \equiv 0 \pmod{16}$ for $k \geqslant 3$.

First, we derive a characterization of all sequences of length 2^n and complexity $2^n - 1$. To this end, we need the following definitions.

The *weight* $W(S)$ of a sequence S is the number of ONES in S.

For sequences of length 2^n and even weight, we define the *subparity*, $sp(S)$, of S as the parity of the number of ONES in the even (or odd) positions of S, i.e.,

$$\begin{aligned} sp(S) &= s_0 + s_2 + s_4 + \cdots + s_{2^n-2} \\ &= s_1 + s_3 + s_5 + \cdots + s_{2^n-1}. \end{aligned}$$

Lemma 1: For a sequence of length 2^n, $C(S) = 2^n - 1$ if and only if $sp(S) = 1$.

Proof: By Fact 2 $C(S) = c$ if and only if $(E + 1)^{c-1} s_i = 1$ for each i. Now,

$$\begin{aligned} (E+1)^{2^n-2} &= \frac{(E+1)^{2^n}}{(E+1)^2} = \frac{E^{2^n}+1}{E+1}\frac{1}{E+1} \\ &= \frac{E^{2^n-1} + E^{2^n-2} + \cdots + E + 1}{E+1} \\ &= E^{2^n-2} + E^{2^n-4} + \cdots + E^2 + 1. \end{aligned}$$

Hence, $C(S) = 2^n - 1$ if and only if for each i

$$\begin{aligned} 1 &= (E+1)^{2^n-2} s_i \\ &= s_{i+2^n-2} + s_{i+2^n-4} + \cdots + s_{i+2} + s_i = sp(S). \end{aligned}$$

Q.E.D.

Next, we show that the de Bruijn sequences of order n and complexity $2^n - 1$ can be partitioned into equivalence classes of order 8 or 16. To this end, we shall need some more definitions and lemmas.

Let $S \in DS(n)$ and let $\boldsymbol{z}S$ (resp. $\boldsymbol{u}S$) denote the sequence obtained from S, by interchanging the positions of the unique runs of n and $n - 2$ ZEROS (resp. ONES). One can readily verify that $\boldsymbol{z}S, \boldsymbol{u}S \in DS(n)$.

Example: For the de Bruijn sequence $S = [0000111101100101]$, we obtain

$$\boldsymbol{z}S = [0011110110000101],$$

$$\boldsymbol{u}S = [0000110111100101],$$

and

$$\boldsymbol{uz}S = \boldsymbol{zu}S = [0011011110000101].$$

Lemma 2: If $S \in DS(n)$ and $C(S) = 2^n - 1$, then $C(\boldsymbol{z}S) = C(\boldsymbol{u}Z) = C(\boldsymbol{zu}S) = 2^n - 1$.

Proof: It can be easily verified that $sp(S) = sp(\boldsymbol{z}S) = sp(\boldsymbol{u}S) = sp(\boldsymbol{zu}S)$. This and Lemma 1 imply Lemma 2. Q.E.D.

The following lemma characterizes sequences S of even length, for which $S \simeq \boldsymbol{r}S$.

Lemma 3: If S is a sequence of even length, and $S \simeq \boldsymbol{r}S$, then S takes one of the following forms:

a) $S \simeq [X\boldsymbol{r}X]$.
b) $S \simeq [b_1 X b_2 \boldsymbol{r}X]$, $\quad b_1, b_2 \in \{0, 1\}$.

Proof: Suppose $l(S) = m$. We can write $S = [s_1, s_2, \cdots, s_m]$ and $\boldsymbol{r}S = [s_m, \cdots, s_2, s_1]$. Since $S \simeq \boldsymbol{r}S$ there exists an integer k such that

$$[s_1, s_2, \cdots, s_m] = [s_k, \cdots, s_2, s_1, s_m, \cdots, s_{k+1}] \simeq \boldsymbol{r}S.$$

Let $Y_1 = s_1, \cdots, s_k$ and $Y_2 = s_{k+1}, \cdots, s_m$. Then $S = [Y_1 Y_2]$, $Y_1 = \boldsymbol{r}Y_1$, and $Y_2 = \boldsymbol{r}Y_2$. We distinguish between the following two cases.

Case 1: k is even. Here both k and $m - k$ are even and we can write $Y_1 = X_1 X_2$, $Y_2 = X_3 X_4$, and $S = [Y_1 Y_2] = [X_1 X_2 X_3 X_4] \simeq [X_4 X_1 X_2 X_3]$, where $l(X_1) = l(X_2)$ and $l(X_3) = l(X_4)$. Since $Y_1 = \boldsymbol{r}Y_1$ and $l(X_1) = l(X_2)$, we have $X_1 = \boldsymbol{r}X_2$. Since $Y_2 = \boldsymbol{r}Y_2$ and $l(X_3) = l(X_4)$, we have $X_3 = \boldsymbol{r}X_4$. Hence letting $X = X_4 X_1$, we obtain $\boldsymbol{r}X = (\boldsymbol{r}X_1 \boldsymbol{r}X_4) = X_2 X_3$, which implies a).

Case 2: k is odd. Here both k and $m - k$ are odd, and we can write

$$Y_1 = X_1 s_{(k+1)/2} X_2,$$

$$Y_2 = X_3 s_{(m+k+1)/2} X_4,$$

and

$$\begin{aligned} S = [Y_1 Y_2] &= \left[X_1 s_{(k+1)/2} X_2 X_3 s_{(m+k+1)/2} X_4\right] \\ &\simeq \left[s_{(k+1)/2} X_2 X_3 s_{(m+k+1)/2} X_4 X_1\right], \end{aligned}$$

where $l(X_1) = l(X_2)$ and $l(X_3) = l(X_4)$. As in Case 1, we obtain $X_1 = \boldsymbol{r}X_2$ and $X_3 = \boldsymbol{r}X_4$. Hence letting $X = X_2 X_3$, $b_1 = s_{(k+1)/2}$, and $b_2 = s_{(m+k+1)/2}$, we obtain b). Q.E.D.

Let G_1 denote the group generated by the operators r, z, and $\boldsymbol{u}$ on $DS(n)$. It is easy to verify that G_1 is commutative.

Lemma 4: $G_1 = \{\boldsymbol{e}, \boldsymbol{r}, \boldsymbol{z}, \boldsymbol{u}, \boldsymbol{rz}, \boldsymbol{ru}, \boldsymbol{zu}, \boldsymbol{rzu}\}$, where $\boldsymbol{e}$ is the identity operator. For $\boldsymbol{n} \geqslant 5$ and for each $S \in DS(n)$, $G_1 S \subseteq DS(n)$ consists of eight pairwise inequivalent sequences.

Proof: The given representation of G_1 follows from the commutativity of G_1 and from the fact that for each $g \in G_1$, $g^2 = \boldsymbol{e}$.

It is also easy to verify that each operator of G_1 preserves the defining property of de Bruijn sequences and, hence, $G_1 S \subseteq DS(n)$.

Since each n-tuple occurs exactly once in every de Bruijn sequence S the unique runs of n zeros, n ones, $n - 2$

TABLE I

	n ZEROS	n ONES	$n-2$ ZEROS	$n-2$ ONES
S	$x_1 10^n 1 x_2$	$x_3 01^n 0 x_4$	$\bar{x}_1 10^{n-2} 1 \bar{x}_2$	$\bar{x}_3 01^{n-2} 0 \bar{x}_4$
$\boldsymbol{z}S$	$\bar{x}_1 10^n 1 \bar{x}_2$	$x_3 01^n 0 x_4$	$x_1 10^{n-2} 1 x_2$	$\bar{x}_3 01^{n-2} 0 \bar{x}_4$
$\boldsymbol{u}S$	$x_1 10^n 1 x_2$	$\bar{x}_3 01^n 0 \bar{x}_4$	$\bar{x}_1 10^{n-2} 1 \bar{x}_2$	$x_3 01^{n-2} 0 x_4$
$\boldsymbol{uz}S$	$\bar{x}_1 10^n 1 \bar{x}_2$	$\bar{x}_3 01^n 0 \bar{x}_4$	$x_1 10^{n-2} 1 x_2$	$x_3 01^{n-2} 0 x_4$

zeros, and $n-2$ ones are nested in S as follows:

$$x_1 10^n 1 x_2, \quad x_3 01^n 0 x_4, \quad \bar{x}_1 10^{n-2} 1 \bar{x}_2, \quad \text{and} \quad \bar{x}_3 01^{n-2} 0 \bar{x}_4,$$

where $x_1, x_2 \in \{0,1\}$, and a^k denotes a sequence of k $\boldsymbol{a}$'s. Table I depicts the situation in S, $\boldsymbol{z}S$, $\boldsymbol{u}S$, and $\boldsymbol{zu}S$, with respect to the above runs. (Note that since $n-2 \geqslant 2$, the operators $\boldsymbol{z}$ and $\boldsymbol{u}$ preserve the value of the x_i's.)

It can be seen that the four sequences of this table are pairwise inequivalent. Hence, the four sequences $\boldsymbol{r}S$, $\boldsymbol{rz}S$, $\boldsymbol{ru}S$, and $\boldsymbol{rzu}S$ are pairwise inequivalent also.

Now, let $\boldsymbol{d}S$ denote the sequence obtained from S by deleting two ZEROS and two ONES from the unique runs of n ZEROS and n ONES, respectively. Note that each of the n-tuples $(10^{n-2}1)$ and $(01^{n-2}0)$, appears twice in $\boldsymbol{d}S$ and each of the other n-tuples of $\boldsymbol{d}S$ appears only once. Note further that $\boldsymbol{d}S$ is a sequence of order $n+1$.

One can readily verify that, viewed as an operator, $\boldsymbol{d}$ commutes with $\boldsymbol{c}$ and with each element of G_1. It is also easy to verify that

$$\boldsymbol{d}S = \boldsymbol{dz}S = \boldsymbol{du}S = \boldsymbol{dzu}S$$

and

$$\boldsymbol{dr}S = \boldsymbol{drz}S = \boldsymbol{dru}S = \boldsymbol{drzu}S.$$

Hence to complete the proof, it suffices to show that $\boldsymbol{d}S \neq \boldsymbol{dr}S$.

Assume $\boldsymbol{d}S \simeq \boldsymbol{dr}S$. Then, also $\boldsymbol{d}S \simeq \boldsymbol{rd}S$, and by Lemma 3, $\boldsymbol{d}S$ takes one of the following forms:

a) $\boldsymbol{d}S \simeq [X\boldsymbol{r}X]$.
b) $\boldsymbol{d}S \simeq [b_1 X b_2 \boldsymbol{r}X], \quad b_1, b_2 \in \{0,1\}$.

In either case, one of the following n-tuples, $(001^{n-4}00)$, $(110^{n-4}11)$, and $(010^{n-4}10)$, has more than half of its bits in X (or in $\boldsymbol{r}X$). Let V be this n-tuple. Then, $\boldsymbol{r}V$ has more than half of its bits in $\boldsymbol{r}X$ (or in X), which contradicts the fact that $V = \boldsymbol{r}V$ and that V appears only once in $\boldsymbol{d}S$. Q.E.D.

From Lemma 4 we infer that for $n \geqslant 5$, $DS(n)$ can be partitioned into equivalence classes of order 8. This, together with Lemma 2 and the facts that $\gamma(15,4) = 8$ and $C(S) = C(\boldsymbol{r}S)$ we have the following theorem.

Theorem 1: For $n \geqslant 4$, $\gamma(2^n - 1, n) \equiv 0 \pmod 8$.

The next lemma presents a characterization of *CR*-sequences, i.e., sequences S such that $\boldsymbol{c}S \simeq \boldsymbol{r}S$.

Lemma 5: A sequence S is a *CR*-sequence if and only if $l(S)$ is even and $S \simeq [X\boldsymbol{rc}X]$, for some X.

Proof: If $l(S)$ is even and $S \simeq [X\boldsymbol{rc}X]$, then $\boldsymbol{c}S \simeq [\boldsymbol{c}X\boldsymbol{r}X] \simeq \boldsymbol{r}S$.

Now, let $S = [s_1 s_2, \cdots, s_m]$ be a *CR*-sequence and suppose $l(S)$ is odd. Then $l(S) - W(S) \neq W(S)$, which implies $W(\boldsymbol{c}S) \neq W(\boldsymbol{r}S)$, or $\boldsymbol{c}S \neq \boldsymbol{r}S$. Therefore, $l(S)$ must be even.

Since $\boldsymbol{c}S \simeq \boldsymbol{r}S$, there exists an integer k such that

$$[\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_m] = [s_k, s_{k-1}, \cdots, s_1, s_m, s_{m-1}, \cdots, s_{k+1}].$$

Let $Y_1 = s_1, \cdots, s_k$ and $Y_2 = s_{k+1}, \cdots, s_m$. Then $S = [Y_1 Y_2]$, $\boldsymbol{c}Y_1 = \boldsymbol{r}Y_1$, $\boldsymbol{c}Y_2 = \boldsymbol{r}Y_2$ and, hence, k and $m-k$ are even. Therefore, we can split Y_1 and Y_2 in the middle to obtain $Y_1 = X_1 X_2$, $Y_2 = X_3 X_4$, and $S = [X_1 X_2 X_3 X_4] \simeq [X_4 X_1 X_2 X_3]$, with $\boldsymbol{c}X_1 = \boldsymbol{r}X_2$, and $\boldsymbol{c}X_3 = \boldsymbol{r}X_4$. Letting $X = X_4 X_1$, we obtain $\boldsymbol{rc}X = (\boldsymbol{rc}X_1 \boldsymbol{rc}X_4) = X_2 X_3$, which implies $S \simeq [X\boldsymbol{rc}X]$. Q.E.D.

Lemma 6[2]: If $S \in DS(n)$, $n \geqslant 3$, then $S \neq \boldsymbol{c}S$.

Lemma 7: If $S \in DS(2k)$, $k \geqslant 3$, then the union of $G_1 S$ and $G_1 \boldsymbol{c}S$ consists of sixteen pairwise inequivalent de Bruijn sequences.

Proof: By lemma 4, $G_1 S \subseteq DS(2k)$ consists of eight pairwise inequivalent sequences. Clearly, the same is true for $G_1 \boldsymbol{c}S$. Also, as in the proof of Lemma 4, we have

$$\boldsymbol{d}S = \boldsymbol{dz}S = \boldsymbol{du}S = \boldsymbol{dzu}S,$$
$$\boldsymbol{dr}S = \boldsymbol{drz}S = \boldsymbol{dru}S = \boldsymbol{drzu}S,$$
$$\boldsymbol{dc}S = \boldsymbol{dzc}S = \boldsymbol{duc}S = \boldsymbol{dzuc}S,$$

and

$$\boldsymbol{drc}S = \boldsymbol{drzc}S = \boldsymbol{druc}S = \boldsymbol{drzuc}S.$$

Furthermore, the inequivalence $\boldsymbol{d}S \neq \boldsymbol{dr}S$, from the proof of Lemma 4, implies $\boldsymbol{dc}S \neq \boldsymbol{drc}S$. To complete the proof, it suffices to show that $\boldsymbol{dc}S \neq \boldsymbol{dr}S$ and $\boldsymbol{dc}S \neq \boldsymbol{d}S$, since these inequivalences imply $\boldsymbol{drc}S \neq \boldsymbol{d}S$ and $\boldsymbol{drc}S \neq \boldsymbol{dr}S$, respectively.

a) Assume $\boldsymbol{dc}S \simeq \boldsymbol{dr}S$. Then $\boldsymbol{cd}S \simeq \boldsymbol{rd}S$, and by Lemma 5, $\boldsymbol{d}S \simeq [X\boldsymbol{rc}X]$, for some X. Once again, one of the three n-tuples, $(0^k 1^k)$, $(1^k 0^k)$, and $(1^{k-1}010^{k-1})$, $n = 2k$, has more than half of its bits in X (or in $\boldsymbol{rc}X$). Let V be this n-tuple. It follows that $\boldsymbol{rc}V$ has more than half of its bits in $\boldsymbol{rc}X$ (or in X), which contradicts the fact that $V = \boldsymbol{rc}V$ and that V appears only once in S. Hence $\boldsymbol{dc}S \neq \boldsymbol{dr}S$.

b) Assume $\boldsymbol{dc}S \simeq \boldsymbol{d}S$. $\boldsymbol{d}S$ has two runs of $n-2$ ONES and two runs of $n-2$ ZEROS. Hence $\boldsymbol{d}S$ takes one of the following forms:

1) $\boldsymbol{d}S \simeq [0^{n-2} X_1 0^{n-2} X_2 1^{n-2} X_3 1^{n-2} X_4]$.
2) $\boldsymbol{d}S \simeq [0^{n-2} X_1 1^{n-2} X_2 0^{n-2} X_3 1^{n-2} X_4]$.

If 1) holds, then

$$\boldsymbol{dc}S \simeq \left[1^{n-2} \boldsymbol{c}X_1 1^{n-2} \boldsymbol{c}X_2 0^{n-2} \boldsymbol{c}X_3 0^{n-2} \boldsymbol{c}X_4\right] \simeq \boldsymbol{d}S.$$

Hence, $\boldsymbol{c}X_1 = X_3$ and $\boldsymbol{c}X_2 = X_4$. This implies that

$$S_1 = \left[0^{n-2} X_1 0^n X_2 1^{n-2} X_3 1^n X_4\right]$$

is a de Bruijn sequence satisfying $S_1 \simeq \boldsymbol{c}S_1$, which contradicts Lemma 6.

If 2) holds, then

$$\boldsymbol{dc}S \simeq \left[1^{n-2} \boldsymbol{c}X_1 0^{n-2} \boldsymbol{c}X_2 1^{n-2} \boldsymbol{c}X_3 0^{n-2} \boldsymbol{c}X_4\right].$$

Comparing this with the form of $\boldsymbol{d}S$ in 2), we obtain $X_2 = \boldsymbol{c}X_1$, $X_3 = \boldsymbol{c}X_2$. This implies $X_1 \simeq X_3$, which means that S contains two identical strings, $0^{n-2} X_1 1^{n-2}$ and $0^{n-2} X_3 1^{n-2}$ of length $\geqslant n$, contradicting the de Bruijn property of S.

Hence $\boldsymbol{dc}S \neq \boldsymbol{d}S$. Q.E.D.

Let G_2 denote the group generated by the operators $\boldsymbol{c}$, $\boldsymbol{r}$, $\boldsymbol{z}$, and $\boldsymbol{u}$ on $DS(n)$. It is easy to verify that, except for the pairs $(\boldsymbol{c}, \boldsymbol{z})$ and $(\boldsymbol{c}, \boldsymbol{u})$, any two of these four generators commute; the exception pairs satisfy $\boldsymbol{cz} = \boldsymbol{uc}$ and $\boldsymbol{cu} = \boldsymbol{zc}$. This and Lemma 7 imply the following result.

Lemma 8: G_2 is the union of G_1 and $G_1\boldsymbol{c}$. For $k \geqslant 3$ and $S \in DS(2k)$, $G_2S \subseteq DS(2k)$ consists of sixteen pairwise inequivalence sequences.

From Lemma 8 we infer that for $k \geqslant 3$, $DS(2k)$ can be partitioned into equivalence classes of order 16. From this, Lemma 2, and the fact that $C(S) = C(\boldsymbol{c}S) = C(\boldsymbol{r}S)$, we obtain the following theorem.

Theorem 2: For $k \geqslant 3$, $\gamma(2^{2k} - 1, 2k) \equiv 0 \pmod{16}$.

III. On the Value of $\gamma(2k, n)$

Games and Chan [3] derived an algorithm for computing the complexity $C(S)$ of a sequence S of length 2^n. From this algorithm we derive a method of distinguishing between sequences of even and odd complexity.

The input to the Games and Chan algorithm is a sequence S of length $l(S) = 2^n$. If $S \neq 0^{2^n}$, the complexity c of S is computed recursively as follows. Initially, set $c_n = 0$ and $A_n = S$. At a typical step of the algorithm the left half of A_m, $L(A_m) = [a_0, \cdots, a_{2^{m-1}-1}]$, is added to the right half, $R(A_m) = [a_{2^{m-1}}, \cdots, a_{2^m-1}]$, the result being a sequence B_m, of length 2^{m-1}. If $B_m = 0^{2^{m-1}}$, A_m is replaced by $A_{m-1} = L(A_m)$, and the complexity is left unchanged, i.e., $c_{m-1} = c_m$. If $B_m \neq 0^{2^{m-1}}$, A_m is replaced by $A_{m-1} = B_m$, and c_m is replaced by $c_{m-1} = c_m + 2^{m-1}$. The complexity of S is given by $C(S) = c_0 + 1$.

Lemma 9: A nonzero sequence S of length 2^n has odd complexity if and only if application of the Games and Chan algorithm to S yields $A_1 = [11]$.

Proof: Since $c_n = 0$, and $c_{m-1} - c_m$ is even for all $m \geqslant 2$, it follows that c_1 is even. For $C(S)$ to be even, c_0 must be odd, which happens only if $L(A_1) \neq R(A_1)$. Hence if $A_1 = [11]$, $C(S)$ is odd. One can easily verify that if $S \neq 0^{2^n}$, then $A_m \neq 0^{2^m}$ for each m and, thus, if $C(S)$ is odd, $A_1 = [11]$. Q.E.D.

Lemma 10: Let Q be a string of even length. Then,

a) $[Q] + [\boldsymbol{rc}Q] = [XrX]$.

b) $[Q] + [\boldsymbol{r}Q] = [YrY]$.

c) If $Q = \boldsymbol{r}Q$, then $[Q] = [ZrZ]$.

Proof: Let $[Q] = [Q_1Q_2]$, where $l(Q_1) = l(Q_2)$. Then we obtain

a) $[\boldsymbol{rc}Q] = [\boldsymbol{rc}Q_2\boldsymbol{rc}Q_1]$ and $[Q] + [\boldsymbol{rc}Q] = [Q_1 + \boldsymbol{rc}Q_2Q_2 + \boldsymbol{rc}Q_1] = [\boldsymbol{c}Q_1 + \boldsymbol{r}Q_2\boldsymbol{r}(\boldsymbol{c}Q_1 + \boldsymbol{r}Q_2)]$.

b) $[\boldsymbol{r}Q] = [\boldsymbol{r}Q_2\boldsymbol{r}Q_1]$ and $[Q] + [\boldsymbol{r}Q] = [Q_1 + \boldsymbol{r}Q_2Q_2 + \boldsymbol{r}Q_1] = [Q_1 + \boldsymbol{r}Q_2\boldsymbol{r}(Q_1 + \boldsymbol{r}Q_2)]$.

c) Let $Q = q_1, q_2, \cdots, q_{2m}$ and $Z = q_1, q_2, \cdots, q_m$. If $Q = \boldsymbol{r}Q$, then $q_i = q_{2m-i+1}$, $1 \leqslant i \leqslant m$, and $[Q] = [ZrZ]$ as claimed. Q.E.D.

Lemma 11: Let $S \in DS(n)$, $n \geqslant 3$, be a *CR*-sequence. Then application of the Games and Chan algorithm to S yields $A_1 = [11]$.

Proof: By Lemma 5, $S \simeq [Q\boldsymbol{rc}Q]$ for some Q. Since $S \in DS(n)$, it is clear that $Q \neq \boldsymbol{rc}Q$. Applying the Games and Chan algorithm to $A_n = [Q\boldsymbol{rc}Q]$, we obtain $A_{n-1} = [Q + \boldsymbol{rc}Q]$. By Lemma 10a), we can write $A_{n-1} = [XrX]$. By parts b) and c) of Lemma 10, $A_m = [Y_m\boldsymbol{r}Y_m]$, for $1 \leqslant m \leqslant n - 1$. Since S is a nonzero sequence, we have $A_1 = [11]$. Q.E.D.

The following is an immediate corollary of Lemmas 9 and 11.

Corollary 1: If $S \in DS(n)$ is a *CR*-sequence, then $C(S)$ is odd.

The absence of de Bruijn *CR*-sequences of even complexity makes it possible now to extend Fact 3 to the following broader result.

Theorem 3: $\gamma(c, n) \equiv 0 \pmod 4$ for all c and n such that cn is even.

References

[1] H. Fredriksen, "A survey of full length nonlinear shift register cycle algorithm," *SIAM Rev.*, vol. 24, pp. 195–221, Apr. 1982.

[2] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *J. Combin. Theory, Ser. A*, vol. 33, pp. 233–246, Nov. 1982.

[3] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with a period 2^n," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 144–146, Jan. 1983.