COUNTING DE BRUIJN SEQUENCES AS
PERTURBATIONS OF LINEAR RECURSIONS

DON COPPERSMITH, ROBERT C. RHOADES, AND JEFFREY M. VANDERKAM

Abstract. Every binary De Bruijn sequence of order \( n \) satisfies a recursion
\[ 0 = x_n + x_0 + g(x_{n-1}, \ldots, x_1). \]
Given a function \( f \) on \( n - 1 \) bits, let \( N(f; r) \) be the number of functions generating a De Bruijn sequence
of order \( n \) which are obtained by changing \( r \) locations in the truth table
of \( f \). We prove a formula for the generating function \( \sum_r N(\ell; r)y^r \) when \( \ell \) is a linear function.

The proof uses a weighted Matrix Tree Theorem and a description of
the in-trees (or rooted trees) in the \( n \)-bit De Bruijn graph as perturba-
tions of the Hamiltonian paths in the same graph.

1. Introduction and Statement of Result

A (binary) De Bruijn sequence of order \( n \) is an infinite 0/1 sequence with
period \( 2^n \) such that every \( n \) long pattern appears exactly once in a period.
The appearance of De Bruijn sequences can be traced back to at least 1869,
to the invention of a Sanskrit word designed to help students remember all
three-syllable meters [19, Section 7.2.1.7]. In the last 100 years De Bruijn
sequences have found application in diverse areas such as robotic vision,
cryptography, DNA sequencing, and even magic [5, Chapters 2 and 3]. For
an overview of the history of De Bruijn sequences the reader may consult
[19, Section 7.2.1.1] and [11, 27, 29].

Every De Bruijn sequence of order \( n \), \((\ldots, x_{-1}, x_0, x_1, x_2, \ldots)\), satisfies an
\( n \)-bit recursion
\[ x_{i+n} = x_i + g(x_{i+n-1}, \ldots, x_{i+1}), \]
with \( g: \mathbb{F}_2^{n-1} \rightarrow \mathbb{F}_2 \). For example, the two De Bruijn sequences of order 3
are
\[ \ldots 10111000 \ldots \text{ and } \ldots 11101000 \ldots \]
The recursions for these two sequences are
\[ x_{i+3} = x_i + x_{i+1} + x_{i+2} \quad \text{and} \quad x_{i+3} = x_i + x_{i+2} + x_{i+1} x_{i+2}, \]
where \( x = 1 + x \) when \( x \in \mathbb{F}_2 \). Each of these recursions is nearly linear. For
instance, the distance between \( x_1 \) and the first function is only one, because
\( x_1 + x_1 x_2 = x_1 \), except when \( x_1 = x_2 = 0 \).

In 1894 Flye Sainte-Marie [6] showed the number of sequences, up to
cyclic equivalence, is \( 2^{2^n-1-n} \). This was rediscovered by De Bruijn in 1946
This paper provides a generalization of the 1894 result by counting De Bruijn sequence recursions which differ from a given linear recursion in exactly $k$ inputs to the functions.

Let $S(n)$ be the set of functions from $\mathbb{F}_2^{n-1} \to \mathbb{F}_2$ that generate a De Bruijn sequence of order $n$. For example, $S(3) = \{x_1 + x_2 x_2, x_2 + x_1 x_2\}$. For $f: \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, define $S(f; k)$ to be the set of $g \in S(n)$ such that the weight of $g + f$ is $k$. The weight of a function is the number of ones in the truth table. In other words, the weight of $f + g$ is the number of disagreements between the functions $f$ and $g$. Moreover, let $N(f; k) = |S(f; k)|$ and

$$G(f; y) := \sum_k N(f; k) y^k.$$  

For example, if $n = 3$ and $f = x_1$, then $S(x_1; 0) = S(x_1; 2) = S(x_1; 4) = \emptyset$, $S(x_1; 1) = \{x_1 x_1 x_2\}$, and $S(x_1; 3) = \{x_2 x_1 x_2\}$. Thus, $G(x_1; y) = y + y^3$.

The following notation is used to describe the main theorem of this paper. Given $f: \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, let $C(f)$ denote the set of sequences, up to cyclic equivalence, satisfying $x_{i+n} = x_i + f(x_{i+n-1}, \ldots, x_{i+1})$. A necklace of length $r$ is an equivalence class of strings of length $r$ consisting of 0s and 1s, taking all cyclic rotations as equivalent. A necklace of length $r$ is primitive if it is not periodic for any $p < r$. Thus, each element of $C(f)$ is represented by a primitive necklace class. For any $c \in C(f)$ let $d(c)$ be the number of ones in the primitive necklace class representing $c$.

**Theorem 1.1.** Let $\ell: \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ be a linear function with constant term equal to 0. Then

$$G(\ell; y) = \sum_k N(\ell; k) y^k = 2^{-n} \prod_{c \in C(\ell)} p_d(c)(y),$$

where $p_k(y) = (1 + y)^k - (1 - y)^k$ for $k > 0$ and $p_0(y) = 1$.

**Remark.** For each linear function $\ell: \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ this theorem gives a refinement of the 1894 result of Flye Sainte-Marie, since evaluating the generating function at $y = 1$ gives the total number of De Bruijn sequences of order $n$, namely $2^{2^{n-1}} - n$.

Remark. The analogous claim for linear $\ell$ with nonzero constant term follows from the fact that $G(\ell; y) = y^{2^{n-1}} \cdot G(1 + \ell; y^{-1})$.

**Remark.** Mayhew [21, 22, 23, 24], Fredricksen [11], Hauge and Mykkeltveit [14, 15] and others have considered the sets $S(0_n; k)$ where $0_n$ is the $(n - 1)$-bit zero function. Theorem 1.1 specializes to the following formula for the zero function:

$$G(0_n; y) = \frac{1}{2^n} \prod_i p_i(y)^{e_{n,i}}.$$  

\footnote{Also in 1946, the existence of such sequences (and generalizations to other alphabets) was rediscovered by Good [12]. More recently, many interesting analogs with more general combinatorial structures than binary strings have been investigated. See, for instance, [2].}
where
\[ e_{n,i} = \sum_{d|n} L(d, i) \]
and \( L(d, i) \) is the number of primitive necklace classes of length \( d \) with \( i \) ones and \( d - i \) zeros.

**Remark.** When a linear function \( \ell : \mathbb{F}_2^{n-1} \rightarrow \mathbb{F}_2 \) generates a \((2^n - 1)\)-periodic sequence without a run of \( n \) zeros the theorem gives
\[ G(\ell; y) = \frac{1}{2^n} \left( (1 + y)^{2^n-1} - (1 - y)^{2^n-1} \right) \]
which was proved previously by Michael Fryers in 2015 [7]. Fryers’ result can be viewed as a generalization of the result of Helleseth and Kővári [16], which computes \( N(\ell; 3) \) for any such linear \( \ell \). This case was conjectured by the second author upon comparison with random permutations [13]. Moreover, Fryers’ result, combined with experimental data for the zero function (see [21, 23, 24]), led to a conjecture for the formula in Theorem 1.1.

**Remark.** Recent works have considered modifying linear recursive sequences or other understood sequences to produce De Bruijn sequences. See, for instance, [20] and [26].

The proof of the theorem has three ingredients. The first ingredient is a correspondence between rooted spanning trees in the \( n \)-bit De Bruijn graph and Hamiltonian paths in the same graph. The basic construction is in [25] and [8 Chapter VI]. We recall this in Section 2. The second ingredient in our proof is a Matrix Tree Theorem. Such theorems are a common ingredient in many of the proofs enumerating De Bruijn sequences (see, for instance, [28]). Here, we use a weighted version of the Matrix Tree Theorem, which appears to go back to Maxwell and Kirchhoff [11, 17, 18] (see Section 3). Finally, the computation of the determinant arising in the Matrix Tree Theorem is established by moving to the character domain. The final ingredient results in a shift from the Fibonacci stepping linear recursion to the corresponding Galois stepping linear recursion. This is the only place in our proof where the linearity of \( \ell \) arises. See Section 4 for the details.

**Acknowledgments**

We thank Ron Fertig, Vidya Venkateswaran, and especially Michael Fryers for helpful conversations.

2. **Hamiltonian Paths and In-Trees**

The \( n \)-bit De Bruijn graph, denoted \( G_n \), is a 2-in 2-out directed graph with \( 2^n \) vertices corresponding to elements of \( \mathbb{F}_2^n \) and an edge \( x_{n-1} \ldots x_1 x_0 \rightarrow x_{n-1} \ldots x_1 \) for all choices of \( x_n, \ldots, x_1, x_0 \in \mathbb{F}_2 \). Every binary De Bruijn sequence of order \( n \) uniquely corresponds to a Hamiltonian tour through the vertices of \( G_n \). In turn, this tour gives a unique in-tree with root
0 = 0\ldots 0 \in \mathbb{F}_2^n$. An in-tree $T$ of $G_n$ is a subgraph of $G_n$ such that (1) $T$ contains exactly $2^n - 1$ edges and (2) every vertex other than $0$ is connected to $0$ by a directed path in $T$.

For example, the De Bruijn sequence $\ldots 11101000$ of order three corresponds to the in-tree $100 \rightarrow 010 \rightarrow 110 \rightarrow 111 \rightarrow 011 \rightarrow 001 \rightarrow 000$.

The Hamiltonian tour corresponding to this in-tree is obtained by adding the edge from $000 \rightarrow 100$, thus completing the cycle. In general, the in-tree is obtained from the Hamiltonian tour by removing the edge from $0$ to $10\ldots 0$.

The following lemma and theorem show how to obtain all in-trees in $G_n$ with root $0$ from the De Bruijn sequences of order $n$. The approach is contained in [25] or [8, Chapter VI], but are proven here to keep the exposition self-contained. Let $H_n$ be the set of in-trees rooted at $0$ which are constructed by removing the edge $0 \rightarrow 10\ldots 0$ in a Hamiltonian path of $G_n$.

Given $H \in H_n$, an edge $a \rightarrow b$ of $G_n$ is consistent with $H$ if $H$ visits $a$ before $b$. For each $H \in H_n$ define $\Lambda(H)$ to be the set of all in-trees of $G_n$ rooted at $0$ all of whose edges are consistent with $H$.

**Theorem 2.1.** Let $\Lambda_n$ be the set of all in-trees rooted at $0$ in $G_n$. Then $\Lambda_n = \bigcup_{H \in H_n} \Lambda(H)$ and $\Lambda(H_1) \cap \Lambda(H_2) = \emptyset$ for all $H_1, H_2 \in H_n$ whenever $H_1 \neq H_2$.

Moreover, let

$$S(H) := \{Xa \in \mathbb{F}_2^n : Xa \text{ occurs before } Xa \pi \text{ in } H \text{ and } X \neq 0\}.$$ 

Then each element of $\Lambda(H)$ is obtained by changing the out-edges of a unique subset of vertices in $S(H)$. Moreover, $|S(H)| = 2^{n-1} - 1$ and $|\Lambda(H)| = 2^{2^n-1} - 1$.

**Theorem 2.1** will be established via a counting argument. However, before turning to the proof we discuss the set of graphs $\Omega(H)$ for $H \in H_n$ which are obtained by modifying the out-edge of any subset of elements of $S(H)$. Theorem [2.1] claims that each element of $\Omega(H)$ is an in-tree consistent with $H$; this is established in the following lemma.

**Lemma 2.1.** Let $H \in H_n$ and let $S(H)$ and $\Omega(H)$ be defined as above. Then each $T \in \Omega(H)$ is an in-tree consistent with $H$.

**Proof.** Let $T$ be obtained from $H \in H_n$ by modifying the out-edges from the states in $S \subseteq S(H)$. It is easy to see that every node of $G_n$ has a path in $T$ to $0$ because it is true for $H$. Moreover, no loops can exist in $T$. Thus $T$ is an in-tree.

To see that $T$ is consistent with $H$, consider an edge in $T$, say $Xa \rightarrow bX$. If $Xa \notin S$, then $Xa \rightarrow bX$ is in $H$ and is thus consistent with $H$. If $Xa \in S$, then $Xa \rightarrow bX$ and $Xa \pi \rightarrow bX$ are edges in $H$, but $Xa$ appears before $Xa \pi$, etc.
thus the edge $Xa \rightarrow bX$ is consistent with $H$. Therefore, each element of $\Omega(H)$ is an in-tree consistent with $H$. \hfill \Box

The following lemmas are useful.

**Lemma 2.2.** Let $H \in \mathcal{H}_n$. Suppose $X \neq 0$ and $Xa \in S(H)$ with $Xa \rightarrow cX$ in $H$. For every $T \in \Omega(H)$ the edge $Xa \rightarrow \overline{a}X$ is in $T$ and $H$.

**Proof.** Since $Xa \rightarrow cX$ is in $H$, so is $X\overline{a} \rightarrow \overline{a}X$. Since $Xa \in S(H)$ every element of $T \in \Omega(H)$ must have the edge $X\overline{a} \rightarrow \overline{a}X$ and one of $Xa \rightarrow cX$ or $Xa \rightarrow \overline{a}X$. \hfill \Box

**Lemma 2.3.** Let $H_1, H_2 \in \mathcal{H}_n$. Then $\Omega(H_1) \cap \Omega(H_2) = \emptyset$.

**Proof.** Suppose $H_1 \neq H_2$ are elements of $\mathcal{H}_n$. Then $H_1 : 10\ldots00 \rightarrow \cdots \rightarrow 0$ and $H_2 : 10\ldots00 \rightarrow \cdots \rightarrow 0$. Let $X \in \mathbb{F}_2^{n-1}$ be the first $X$ such that for some $a$, $Xa \rightarrow cX$ is in $H_1$ and $Xa \rightarrow \overline{a}X$ is in $H_2$. That is, $X$ is the input to the function just before the first time the two cycles diverge. Then $Xa \in S(H_1) \cap S(H_2)$. Suppose $T \in \Omega(H_1)$. Then by Lemma 2.2, $X\overline{a} \rightarrow \overline{a}X$ is in $T$. If $T$ is also in $\Omega(H_2)$ then Lemma 2.2 gives that $X\overline{a} \rightarrow cX$ must be in $T$, which is a contradiction. \hfill \Box

We now turn to the proof of Theorem 2.1.

**Proof of Theorem 2.1.** Clearly, $|S(H)| = 2^{n-1} - 1$, because either $X0$ or $X1$, but not both, are in $S(H)$ for each $X \in \mathbb{F}_2^{n-1} \setminus 0$. Therefore, $|\Omega(H)| = 2^{2^n-1} - 1$. Hence, $|\Lambda(H)| \geq |\Omega(H)| = 2^{2^n-1} - 1$.

By Lemma 2.1, $\Lambda_n \supseteq \bigcup_{H \in \mathcal{H}_n} \Omega(H)$. Moreover, by Lemma 2.3 and the above calculation,

$$|\Lambda_n| \geq \sum_{H \in \mathcal{H}_n} |\Omega(H)| = 2^{2^n-1} - 1 \cdot |\mathcal{H}_n|.$$ 

It is well known [28, Chapter 10], that $|\Lambda_n| = 2^{2^n-1} - 1$ and $|\mathcal{H}_n| = 2^{2^n-1} - 1$ for all $n \geq 1$. Therefore, we must have

$$\Lambda_n = \bigcup_{H \in \mathcal{H}_n} \Omega(H).$$

The proof follows from the fact that $\Omega(H) \subseteq \Lambda(H)$. \hfill \Box

The following weighted version of the De Bruijn graph is used in Section 3.

**Theorem 2.2.** Fix $f : \mathbb{F}_2^{n-1} \rightarrow \mathbb{F}_2$. Label the edge $x_{n-1} \ldots x_1 x_0 \rightarrow x_n x_{n-1} \ldots x_1$ of $G_n$ by $1$ if $x_n = x_0 + f(x_{n-1}, \ldots, x_1)$ and by $y$ otherwise. Denote this weighted graph by $G_{n,f}$. For any in-tree $T \in \Lambda_n$ define the weight of $T$, denoted by $y^{\text{wt}(f;T)}$, to be the product of the weights of edges. Then

$$(1 + y)^{2^{n-1}-1} \cdot G(f;y) = \sum_{T \in \Lambda_n} y^{\text{wt}(f;T)}$$

where $G(f;y)$ is defined in (4).
Proof. By Theorem 2.1 we have

$$\sum_{T \in \Lambda_n} y^{wt(f; T)} = \sum_{H \in H_n} \sum_{S \subset S(H)} y^{wt(f; T_{S,H})}$$

where $T_{S,H}$ is the tree in $\Lambda(H)$ generated by modifying the out-edges of the set $S$, as described in Theorem 2.1. Since modifying the out-edge from each element of $S(H)$ either increases or decreases the weight of the tree by a single $y$, we see that

$$\sum_{S \subset S(H)} y^{wt(f; T_{S,H})} = (1 + y)^{2^{n-1} - 1} \cdot y^{\text{minimum wt}},$$

where we have used $|S(H)| = 2^{n-1} - 1$. Finally, the minimum weight is clearly the number of places that the feedback function that generates the De Bruijn sequence represented by $H$ differs from the function $f$. □

3. The Matrix Tree Theorem

The following Matrix Tree Theorem was proved by Kirchhoff [17] and stated by Maxwell [18]; see also Chajeken and Kleitman [1], and the references therein.

**Theorem 3.1.** Let $G$ have vertices $v_1, \ldots, v_n$. Suppose that an edge from $v_i \to v_j$ is given a weight $-M_{i,j}$, and choose $M_{j,j}$ so that $\sum M_{i,j} = 0$ for all $j$. Then the sum over all in-trees with root $v_1$ of the product of all weights assigned to the edges of the in-tree is the determinant of the matrix obtained by omitting the row and column corresponding to $v_1$ of the matrix $M = (M_{i,j})$.

In practice, the following lemma is often used with Theorem 3.1.

**Lemma 3.1 (\cite[Lemma 9.9]{28}).** Let $M$ be a $p \times p$ matrix such that the sum of the entries in every row and column is 0. Let $M_0$ be the matrix obtained from $M$ by removing the first row and first column. Then the coefficient of $z$ in the characteristic polynomial $\det(M - z \cdot I)$ (with $I$ the identity matrix) of $M$ is equal to $-p \cdot \det(M_0)$.

For any $f : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ let $G_{n,f}$ be the weighted De Bruijn graph defined in Section 2. Denote the weighted adjacency matrix by $W_{f,n}$. So $W_{f,n}$ is the $2^n \times 2^n$ matrix with a 1 in the row and column corresponding to $x_{n-1} \ldots x_1 x_0 \to x_n x_{n-1} \ldots x_1$ if $x_n = x_0 + f(x_{n-1}, \ldots, x_1)$ and a $y$ otherwise. For example, with $f(x_2, x_1) = 0$ the weighted adjacency matrix is

$$W_{1,3} = \begin{pmatrix}
1 & 0 & 0 & 0 & y & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & y & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & y & 0 \\
0 & 0 & y & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & y & 0 \\
0 & 0 & 0 & y & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Combining Theorems 2.1 and 3.1 and Lemma 3.1 one obtains the following:
Proposition 3.1. Let $f: \mathbb{F}_2^{n-1} \rightarrow \mathbb{F}_2$. With $G(f; y)$ defined as in [1] and $W_{f,n}$ the adjacency matrix of the weighted De Bruijn graph,

$$(1 + y)^{2^n-1} \cdot G(f; y) = \left( \frac{1}{2^n(z - (1 + y))} \cdot \det(z \cdot I - W_{f,n}) \right) \bigg|_{z = (1 + y)}.$$

Proof. Applying Theorems 2.1 and 3.1 we see that $(1 + y)^{2^n-1} \cdot G(f; y)$ is equal to the determinant of $(1 + y) \cdot I_{2^n} - W_{f,n}$ after deleting the first row and column. To apply Lemma 3.1 it is sufficient to notice that the row and column sums of $(1 + y) \cdot I_{2^n} - W_{f,n}$ are all zero because every state has an edge into it with weight 1 and an edge into it with weight $y$ as well as an edge out of it with weight 1 and out of it with weight $y$. □

4. Proof of Theorem 1.1

Let $\ell: \mathbb{F}_2^{n-1} \rightarrow \mathbb{F}_2$ such that $\ell(x_{n-1} \ldots x_1) = \sum_{i=1}^{n-1} \ell_i \cdot x_i$. By Proposition 3.1 the proof of Theorem 1.1 is reduced to that of computing the characteristic polynomial of $W_{\ell,n}$, where $W_{\ell,n}$ is the weighted adjacency matrix acting on formal linear combinations of elements of $\mathbb{F}_2^n$ by

$$[x_{n-1} \ldots x_0] \rightarrow [x_n x_{n-1} \ldots x_1] + y \cdot [\overline{x_n x_{n-1} \ldots x_1}]$$

where $x_n = x_0 + \sum_{i=1}^{n-1} x_i \cdot \ell_i$.

Before giving the proof, we define the Galois and Fibonacci cycles of a linear recursion. The proof of Theorem 1.1 will make use of the correspondence between these cycles.

The Fibonacci cycles of the linear recursion $x_n = x_0 + \ell(x_{n-1}, \ldots, x_1)$ are defined, as in the introduction, to be the set of binary sequences, up to cyclic shift, satisfying $x_{i+n} = x_i + \ell_{n-1} x_{i+n-1} + \cdots + \ell_1 x_{i+1}$. We remark that these cycles are in one-to-one correspondence with the Fibonacci cycles of $x_{i+n} = x_i + \tilde{\ell}(x_{n-1+i}, \ldots, x_{i+1}) := x_i + \ell_1 x_{i+n-1} + \cdots + \ell_{n-1} x_{i+1}$. The correspondence amounts to reversing the sequences. Moreover, the elements of $C(\ell)$ are in one-to-one correspondence with the cycles of $C(\tilde{\ell})$.

The Galois cycles of the linear recursion $x_n = x_0 + \ell(x_{n-1}, \ldots, x_1)$ are defined to be the set of sequences in $\mathbb{F}_2^n$, up to cyclic equivalence, which satisfy the linear recursion

$$\begin{bmatrix}
\ell_1 & 1 & 0 & \cdots & 0 & 0 \\
\ell_2 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & & & \ddots & & \vdots \\
\ell_{n-1} & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 0
\end{bmatrix} \mathbf{v}_i = \mathbf{v}_{i+1}.$$

Projecting the Galois cycles onto any coordinate gives the Fibonacci cycles of the same linear recursion. See [9, Corollary 3.4] or [10, Chapters 3 and 7], for example.

---

Footnote:

This corollary does not appear in the published version of this paper, but is in the version available on the second author’s website.
Proof of Theorem 1.1. For \( \alpha = \alpha_{n-1} \ldots \alpha_0 \in \mathbb{F}_2^n \) define the character \( \alpha(x) = (-1)^{\sum \alpha_i x_i} \) and the vector \( X_\alpha = \sum x \alpha(x)[x] \). Then

\[
W_{\ell,n}(X_\alpha) = \sum_x \alpha(x) W_{\ell,n}(x) = \sum_{x=x_{n-1} \ldots x_1 x_0} (-1)^{\sum \alpha_i x_i} [x_n x_{n-1} \ldots x_1]
\]

\[
+ y \sum_{x=x_{n-1} \ldots x_1 x_0} (-1)^{\sum \alpha_i x_i} [x_n x_{n-1} \ldots x_1]
\]

\[
= (1 + (-1)^{\alpha_0} y) \sum_{x=x_{n-1} \ldots x_1 x_0} \alpha(x)[x_n x_{n-1} \ldots x_1],
\]

where the last step comes from changing variables in the second summand. Next change variables by setting \( z = x_n x_{n-1} \ldots x_1 \). The sum is then

\[
W_{\ell,n}(X_\alpha) = (1 + (-1)^{\beta_{n-1} y}) \sum_{z=x_n x_{n-1} \ldots x_1} \beta(z)[z]
\]

where \( \beta = \beta_{n-1} \ldots \beta_1 \beta_0 \) and \( \beta_i = \alpha_i+1+\ell_i+1 \alpha_0 \) for \( i < (n-1) \) and \( \beta_{n-1} = \alpha_0 \).

In other words,

\[
W_{\ell,n}(X_\alpha) = (1 + (-1)^{\beta_{n-1} y})X_\beta
\]

where \( \beta \) is the character after \( \alpha \) in the Galois cycle induced by \( \ell \) on the character space.

Thus \( W_{\ell,n} \) has eigenspaces corresponding to the cycles of the Galois stepping register associated to the linear function \( \ell \). Say that there are \( r \) characters in the cycle, of which \( k \) have ones in their \( \beta_{n-1} \) position. The characteristic polynomial of \( W_{\ell,n} \) on this space is then \( z^r - (1+y)^{r-k}(1-y)^k \), so the product of the eigenvalues of \((1+y)I - W_{\ell,n}\) on this space is \((1+y)^r - (1+y)^{r-k}(1-y)^k = (1+y)^{r-k}p_k(y)\).

The proof is finished by noting that the Galois cycles induced by \( \ell \) in the character space have exactly the same sizes as the cycles induced by \( \ell \) in the state spaces, and we can map from one to the other by taking any linear functional of the one, in particular by taking \( \beta_{n-1} \) (see [9, 10] and the discussion above). So the product over all \( \ell \)-based Galois cycles of this expression is exactly the same as the product over all \( \ell \)-based state cycles of this same expression, where \( r \) is again the length of the cycle and \( k \) is the number of ones in the state cycle.

\[
\square
\]

Remark. The vectors \( X_\alpha \) appeared in Fryers’s proof of the case when \( \ell \) generates a cycle of length \( 2^n - 1 \) [7].

 REFERENCES

[1] S. Chaiken and D.J. Kleitman, Matrix tree theorems. J. Combinatorial Theory Ser. A 24 (1978), no. 3, 377–381.
[2] F. Chung, P. Diaconis, and R. Graham, Universal cycles for combinatorial structures. Discrete Math. 110 (1992), no. 1–3, 43–59.
COUNTING DE BRUIJN SEQUENCES AS PERTURBATIONS OF LINEAR RECURSION

[3] N. G. de Bruijn, A combinatorial problem. Indagationes Math. 8, (1946), 461–467.
[4] N. G. de Bruijn, Acknowledgment of priority to C. Flye Sainte-Marie on the counting of circular arrangements of 2ⁿ zeros and ones that show each n-letter word exactly once. Eindhoven: Technische Hogeschool Eidenhoven, (1975), 14 pages.
[5] P. Diaconis and R. Graham, Magical Mathematics. The mathematical ideas that animate great magic tricks. Princeton University Press, Princeton, NJ, 2012.
[6] C. Flye Sainte-Marie Solution to nr. 48, l’Intermédiaire des Mathématiciens, 1:107–110, 1894.
[7] M. J. Fryers, Perturbations of full-cycle linear feedback shift registers. (2015) preprint.
[8] S. Golomb, Shift Register Sequences. Holden-Day, Inc., 1967.
[9] M. Goeresky and A. Klapper, Fibonacci and Galois representations of Feedback with Carry Shift Registers. IEEE Trans. Inform. Theory 48 (2002), 2826–2836.
[10] M. Goeresky and A. Klapper, Algebraic Shift Register Sequences. Cambridge University Press, Cambridge, 2012.
[11] H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms. SIAM Rev. 24 (1982), no. 2, 195–221.
[12] I. J. Good, Normal Recurring decimals. J. London Math. Soc. 21, (1946), 167–169.
[13] J. Harer and D. Zagier, The Euler characteristic of the moduli space of curves. Inventiones Mathematicae, 85 (1986), 457–485.
[14] E. R. Hauge and J. Mykkeltveit, On the classification of de Bruijn sequences. Discrete Math. 148 (1996), no. 1–3, 65–83.
[15] E. R. Hauge and J. Mykkeltveit, The analysis of de Bruijn sequences of non-extremal weight. Discrete Math. 189 (1998), no. 1–3, 133–147.
[16] T. Helleseth and T. Klove, The number of cross-join pairs in maximum length linear sequences. IEEE Trans. Inform. Theory 37 (1991), no. 6, 1731–1733.
[17] G. Kirchhoff, Ueber die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verhältnisse galvanischer Strömegeführft wird. Ann. Phys. Chem., 148:497–508, 1847.
[18] Maxwell, A treatise on electricity and magnetism, I. Oxford University Press, 1892.
[19] D. E. Knuth, The art of computer programming. Vol 4, Part A. Addison-Wesley, Upper Saddle River, NJ. 2006.
[20] C. Li, X. Zeng, C. Li, and T. Helleseth, A class of de Bruijn sequences. IEEE Trans. Inform. Theory 60 (1014), no. 12, 7955–7969.
[21] G. Mayhew, Weight class distributions of de Bruijn sequences. Discrete Math. 126 (1994), no. 1–3, 425–429.
[22] G. Mayhew, Clues to the hidden nature of de Bruijn sequences. computers and Mathematics with Applications. 39 (2000), 57–65.
[23] G. Mayhew, Further results on de Bruijn weight classes. Discrete Math. 232 (2001), no. 1–3, 171–173.
[24] G. Mayhew, Extreme weight classes of de Bruijn sequences. Discrete Math. 256 (2002), no. 1–2, 495–497.
[25] J. Mykkeltveit and J. Szmidt, On cross joining de Bruijn sequences. Topics in finite fields, 335–346, Contemp. Math., 632, Amer. Math. Soc., Providence, RI, 2015.
[26] A. Ralston, de Bruijn sequences – a model example of the interaction of discrete mathematics and computer science. Math. Mag. 55 (1982), no. 3, 131–143.
[27] R. P. Stanley, Algebraic Combinatorics: Walks, Trees, Tableaux, and More. Springer, 2013.
[28] S. K. Stein, The mathematician as an explorer. Sci. Amer. May (1961) 149–158.

CENTER FOR COMMUNICATIONS RESEARCH; PRINCETON, NJ 08534