Construction of de Bruijn sequences from product of two irreducible polynomials

Chang, Zuling; Ezerman, Martianus Frederic; Ling, San; Wang, Huaxiong

2017

Chang, Z., Ezerman, M. F., Ling, S., & Wang, H. (2017). Construction of de Bruijn sequences from product of two irreducible polynomials. Cryptography and Communications, 10(2), 251-275.

https://hdl.handle.net/10356/83380

https://doi.org/10.1007/s12095-017-0219-8

manuscript No.
(will be inserted by the editor)

Construction of de Bruijn Sequences from Product of Two Irreducible Polynomials

Zuling Chang · **Martianus Frederic Ezerman** ·
San Ling · **Huaxiong Wang**

Received: date / Accepted: date

Abstract We study a class of Linear Feedback Shift Registers (LFSRs) with characteristic polynomial $f(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are distinct irreducible polynomials in $\mathbb{F}_2[x]$. Important properties of the LFSRs, such as the cycle structure and the adjacency graph, are derived. A method to determine a state belonging to each cycle and a generic algorithm to find all conjugate pairs shared by any pair of cycles are given. The process explicitly determines the edges and their labels in the adjacency graph. The results are then combined with the cycle joining method to efficiently construct a new class of de Bruijn sequences. An estimate of the number of resulting sequences is given. In some cases, using cyclotomic numbers, we can determine the number exactly.

Keywords Binary periodic sequence · de Bruijn sequence · cycle structure · adjacency graph · cyclotomic number

Mathematics Subject Classification (2010) 11B50 · 94A55 · 94A60

1 Introduction

A binary *de Bruijn sequence* of order n is a binary sequence with period $N = 2^n$ in which each n-tuple occurs exactly once in one period of the sequence. There are $2^{2^{n-1}-n}$ such sequences [2].

De Bruijn sequences have been studied for a long time using diverse mathematical tools and often show up in multiple disguises [21]. They have many applications in communication systems, coding theory, and cryptography due to their attractive characteristics, such as having long period and large linear complexity, and being balanced [3, 9]. Fredricksen's survey [8] discusses their various properties and constructions.

Z. Chang
School of Mathematics and Statistics, Zhengzhou University, Zhengzhou 450001, China
E-mail: zuling_chang@zzu.edu.cn

M. F. Ezerman · S. Ling · H. Wang
Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, 21 Nanyang Link, Singapore 639798
E-mail: {fredezerman,lingsan,HXWang}@ntu.edu.sg

A well-known construction approach called the *cycle joining (CJ) method* (see *e.g.*, [8] and [9]) joins all cycles produced by a given Feedback Shift Register (FSR) into a single cycle. Since the cycle structure of a Linear FSR (LFSR) has been well-studied, it is natural to construct de Bruijn sequences by applying the cycle joining method to LFSRs. Some LFSRs with simple cycle structure, such as the maximal length LFSRs, pure cycling registers, and pure summing registers, have been used to generate de Bruijn sequences using the said method in [6–8].

Hauge and Helleseth established a connection between the cycles generated by LFSRs and irreducible cyclic codes in [11]. The number of de Bruijn sequences obtained from these LFSRs is related to cyclotomic numbers. The cycle structure and the adjacency graph of LFSRs with simple reducible polynomials are then studied and several classes of de Bruijn sequences are constructed from these LFSRs.

Recent studies have considered cases where the characteristic polynomials are products of some simple or primitive polynomials. In [14], a class of de Bruijn sequences was derived from LFSRs with characteristic polynomials $(1+x)^3 p(x)$ with $p(x)$ a primitive polynomial of degree $n > 2$. In [15] the focus was on characteristic polynomials $(1+x^3)p(x)$. The characteristic polynomials studied in [16] are products of primitive polynomials whose degrees are pairwise coprime. Hence, the sequences forming the cycle structure have coprime periods. Although this set up leads to a structure that can be nicely studied and described, in most cases the number of de Bruijn sequences that the construction yields is small when compared with the construction that we are proposing in this paper. An example in Section 7 will highlight this fact.

In this paper, we construct new de Bruijn sequences based on LFSRs with characteristic polynomials $f(x) = p(x)q(x)$, where $p(x)$ and $q(x)$ are distinct irreducible polynomials. We study the corresponding cycle structure and construct the adjacency graph. We propose a method to find a set of representatives of the states, one belonging to each cycle, and design an algorithm to find all conjugate pairs shared by any two cycles. Deploying the cycle joining method, we construct the de Bruijn sequences and estimate their number. In some instances, the estimates are made exact.

This work contributes to the large literature on de Bruijn sequences on several fronts. We generalize the choices of characteristic polynomials to products of irreducible polynomials, instead of those of primitive polynomials. The structure of the resulting LFSRs is thoroughly studied. Our step-by-step construction of de Bruijn sequences from the LFSRs remains efficient to perform while handling more complex cycle structure, yielding a large number of de Bruijn sequences. The resulting class contains many known ones as special cases. In particular, the class derived from product of two primitive polynomials is a subclass of our construction. Finally, most of the methods developed in this paper generalize naturally to LFSRs with product of $s > 2$ pairwise distinct irreducible polynomials as characteristic polynomials.

The paper is organized as follows. After this introduction come preliminary notions and known results in Section 2. Section 3 presents the cycle structure. The main results are presented in Section 4 in two parts. The first part determines the adjacency graph. The second part provides an algorithm to find all conjugate pairs between any two cycles and gives a rough estimate of the number of constructed de Bruijn sequences. A detailed example in Section 5 showcases how the theoretical results fit together nicely in practice. Section 6 examines three special cases where the characteristic polynomial has certain simplifying properties. Section 7 briefly treats a more general case where the characteristic polynomial is the product of more than two irreducible polynomials. The last section contains a brief conclusion and some future directions.

2 Preliminaries

We use [10, Chapter 4] as a main reference for this section.

An *n-stage shift register* is a circuit consisting of n consecutive storage units, each containing a bit, regulated by a clock. As the clock pulses, the bit in each storage unit is shifted to the next stage in line. A shift register becomes a binary code generator when one adds a feedback loop which outputs a new bit s_n based on the n bits $\mathbf{s}_0 = (s_0, \ldots, s_{n-1})$ called an *initial state* of the register. The corresponding *feedback function* $f(x_0, \ldots, x_{n-1})$ is the Boolean function that outputs s_n on input $\mathbf{s}_0$.

A feedback shift register (FSR) outputs a binary sequence $\mathbf{s} = s_0, s_1, \ldots, s_n, \ldots$ satisfying the recursive relation $s_{n+\ell} = f(s_\ell, s_{\ell+1}, \ldots, s_{\ell+n-1})$ for $\ell = 0, 1, 2, \ldots$. For $N \in \mathbb{N}$, if $s_{i+N} = s_i$ for all $i \geq 0$, then $\mathbf{s}$ is *N-periodic* or *with period N* and one writes $\mathbf{s} = (s_0, s_1, s_2, \ldots, s_{N-1})$. We call $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+n-1})$ *the i-th state* of $\mathbf{s}$ and states $\mathbf{s}_{i-1}$ and $\mathbf{s}_{i+1}$ the *predecessor* and *successor* of $\mathbf{s}_i$, respectively.

Given two sequences $\mathbf{u} = u_0, u_1, \ldots$ and $\mathbf{v} = v_0, v_1, \ldots$, the sum $\mathbf{u} + \mathbf{v}$ and the scalar multiple $c\mathbf{u}$ are $\mathbf{u} + \mathbf{v} = u_0 + v_0, u_1 + v_1, \ldots$ and $c\mathbf{u} = cu_0, cu_1, \ldots$. A period of the sum is the least common multiple (lcm) of the periods of the given sequences.

For an FSR, distinct initial states generate distinct sequences. We collect all these sequences to form a set $\Omega(f)$ of cardinality 2^n. All sequences in $\Omega(f)$ are periodic if and only if the feedback function f is *nonsingular*, i.e., f can be written as

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + g(x_1, \ldots, x_{n-1}),$$

where $g(x_1, \ldots, x_{n-1})$ is some Boolean function with domain $\mathbb{F}_2^{n-1}$ [9, page 116]. In this paper, the feedback functions are all nonsingular. An FSR is called *linear* or an LFSR if its feedback function is linear, and *nonlinear* or an NLFSR otherwise.

The *characteristic polynomial* of an n-stage LFSR with feedback function

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i$$

is the polynomial $f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_2[x]$. A sequence $\mathbf{s}$ may have many characteristic polynomials. We call the monic characteristic polynomial with the lowest degree the *minimal polynomial* of $\mathbf{s}$. It represents the LFSR of shortest length that generates $\mathbf{s}$. More properties of the minimal polynomial can be found in [10, Sections 4.2 and 4.3]. For an LFSR with characteristic polynomial $f(x)$, the set $\Omega(f)$ is also denoted by $\Omega(f(x))$.

Example 1 A 3-stage NLFSR with initial state (110) and feedback function $f(x_0, x_1, x_2) = x_0 + x_1 x_2 + x_2 + 1$ outputs $(1100\ 0101)$, a de Bruijn sequence with period 8.

For a sequence $\mathbf{s}$, the *(left) shift operator L* is given by

$$L\mathbf{s} = L(s_0, s_1, \ldots, s_{N-1}) = (s_1, s_2, \ldots, s_{N-1}, s_0)$$

with the convention that $L^0\mathbf{s} = \mathbf{s}$. The set $[\mathbf{s}] := \{\mathbf{s}, L\mathbf{s}, L^2\mathbf{s}, \ldots, L^{N-1}\mathbf{s}\}$ is a *shift equivalent class* or a *cycle* in $\Omega(f)$. The set of sequences in $\Omega(f)$ can be partitioned into cycles.

If $\Omega(f(x))$ consists of exactly r cycles $[\mathbf{s}_1], [\mathbf{s}_2], \ldots, [\mathbf{s}_r]$ for some $r \in \mathbb{N}$, then the *cycle structure* of $\Omega(f(x))$ is

$$\Omega(f(x)) = [\mathbf{s}_1] \cup [\mathbf{s}_2] \cup \ldots \cup [\mathbf{s}_r].$$

When $r = 1$, the corresponding FSR is of *maximal length* and its output sequences are de Bruijn sequences of order n. A nonzero output sequence of a maximal length n-stage LFSR is said to be an *m-sequence of order n* or a *maximal length sequence* (MLS).

A state $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ and its *conjugate* $\widehat{\mathbf{v}} = (v_0 + 1, v_1, \ldots, v_{n-1})$ form a *conjugate pair*. Cycles C_1 and C_2 are *adjacent* if they are disjoint and there exists $\mathbf{v}$ in C_1 whose conjugate $\widehat{\mathbf{v}}$ is in C_2.

Adjacent cycles C_1 and C_2 with the same feedback function $g(x_0, x_1, \ldots, x_{n-1})$ can be joined into a single cycle by interchanging the successors of $\mathbf{v}$ and $\widehat{\mathbf{v}}$. The corresponding feedback function of the resulting cycle is

$$h(x_0, x_1, \ldots, x_{n-1}) = g(x_0, x_1, \ldots, x_{n-1}) + \prod_{i=1}^{n-1} (x_i + v_i + 1).$$

The basic idea in the cycle joining method is to provide the feedback functions of the new de Bruijn sequences by finding the corresponding conjugate pairs. Determining the conjugate pairs between cycles is, therefore, a crucial step in constructing de Bruijn sequences.

Definition 1 [12] For an FSR with feedback function f, its *adjacency graph G* is an undirected multigraph whose vertices correspond to the cycles in $\Omega(f)$. There exists an edge between two vertices if and only if they share a conjugate pair. The number of shared conjugate pairs labels the edge.

When the edges connecting two vertices are considered pairwise distinct, there is a one-to-one correspondence between the spanning trees of the adjacency graph G and the de Bruijn sequences constructed by the CJ method. The details can be found in [11] and [12]. The following result, a variant of the BEST (de **B**ruijn, **E**hrenfest, **S**mith, and **T**utte) Theorem adapted from [1, Section 7], provides the counting formula.

Theorem 1 *(BEST) Let G be the adjacency graph of an FSR with vertex set $\{v_1, v_2, \ldots, v_\ell\}$. Let G' be the graph obtained by removing all loops in G. Let $\mathscr{M} = (m_{i,j})$ be the $\ell \times \ell$ matrix derived from G' in which $m_{i,i}$ is the sum of the labels on the edges incident to v_i and $m_{i,j}$ is the negative of the label of edge (v_i, v_j) for $i \neq j$. Then the number of the spanning trees of G is the cofactor of any entry of $\mathscr{M}$.*

The *cofactor* of the entry $m_{i,j}$ in $\mathscr{M}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the i-th row and j-th column of $\mathscr{M}$. Relevant concepts and results on finite fields, such as the definitions and properties of minimal, irreducible, and primitive polynomials, can be found in [17].

With the preparatory notions in place, we proceed to determining the cycle structure.

3 The Cycle Structure of $\Omega(f(x))$

We start by recalling some useful properties and results.

Let $g(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n having $\beta \in \mathbb{F}_{2^n}$ as a root. Then there exists a primitive element $\alpha \in \mathbb{F}_{2^n}$ such that $\beta = \alpha^t$ for some $t \in \mathbb{N}$, and $e = \frac{2^n-1}{t}$ is the order of β. Using the *Zech logarithmic representation* (see. *e.g.*, [10, page 39]), we write

$$1 + \alpha^\ell = \alpha^{\tau_n(\ell)}$$

where $\tau_n(\ell)$ is the Zech logarithm relative to α that induces a permutation on $\{1, 2, \ldots, 2^n - 2\}$. For completeness, $\tau_n(\ell) := \infty$ for $\ell \equiv 0 \pmod{2^n - 1}$ and $\alpha^\infty := 0$.

The *cyclotomic classes* $C_i \subseteq \mathbb{F}_{2^n}$ for $0 \leq i < t$ are

$$C_i = \{\alpha^{i+s\cdot t} \mid 0 \leq s < e\} = \{\alpha^i \beta^s \mid 0 \leq s < e\} = \alpha^i C_0. \tag{1}$$

The *cyclotomic numbers* $(i,j)_t$, for $0 \leq i,j < t$ are given by

$$(i,j)_t = \left|\{(\xi, \xi+1) \mid \xi \in C_i, \xi+1 \in C_j\}\right| = \left|\{\xi \mid \xi \in C_i, \xi+1 \in C_j\}\right|. \tag{2}$$

Requiring $\xi \in C_i$ and $\xi+1 \in C_j$ is equivalent to requiring that there exist s and s' with $0 \leq s, s' < e$ such that

$$1+\alpha^{i+s\cdot t} = \alpha^{j+s'\cdot t} \iff \tau_n(i+s\cdot t) = j+s'\cdot t \iff \tau_n(i+s\cdot t) \equiv j \pmod t.$$

Thus, an equivalent expression to (2) is

$$(i,j)_t = \left|\{s \mid \tau_n(i+s\cdot t) \equiv j \pmod t\}\right|. \tag{3}$$

Remark 1 In general, it is hard to determine the cyclotomic numbers for all parameter sets. They are known for small parameters or under certain conditions. Some useful facts can be found in [23] and [5, Section 1.4]. The cyclotomic numbers used in this paper are all known.

Using $\{1, \beta, \ldots, \beta^{n-1}\}$ as a basis for $\mathbb{F}_{2^n}$ as an $\mathbb{F}_2$-vector space, for $0 \leq j < 2^n-1$, one can uniquely express α^j as

$$\alpha^j = \sum_{i=0}^{n-1} a_{j,i}\beta^i \text{ with } a_{j,i} \in \mathbb{F}_2.$$

Define the mapping $\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_2^n$ by

$$\varphi(0) = \mathbf{0}, \;\; \varphi(\alpha^j) = (a_{j,0}, a_{j+t,0}, \ldots, a_{j+(n-1)t,0}),$$

where the subscripts are reduced modulo 2^n-1. Let

$$\mathbf{u}_i = (a_{i,0}, a_{i+t,0}, \ldots, a_{i+(e-1)t,0}). \tag{4}$$

It is shown in [11, Theorem 3] that the class C_i corresponds to the cycle $[\mathbf{u}_i]$ under the mapping φ. In other words, $\mathbf{u}_i$ and the sequence of states $((\mathbf{u}_i)_0, (\mathbf{u}_i)_1, \ldots, (\mathbf{u}_i)_{e-1})$ of $\mathbf{u}_i$ where, for $0 \leq j < e$,

$$(\mathbf{u}_i)_j = (a_{i+jt,0}, a_{i+(j+1)t,0}, \ldots, a_{i+(j+n-1)t,0}) = \varphi(\alpha^i\beta^j),$$

are equivalent. Hence, $\mathbf{u}_i \longleftrightarrow C_i$.

The theory of LFSRs in [10, Chapter 4] tells us that

$$\Omega(g(x)) = [\mathbf{0}] \cup [\mathbf{u}_0] \cup [\mathbf{u}_1] \cup \ldots \cup [\mathbf{u}_{t-1}]. \tag{5}$$

If $g(x)$ is a primitive polynomial, then $e = 2^n-1$ and there exists only one cyclotomic class. Hence, $\Omega(g(x)) = [\mathbf{0}] \cup [\mathbf{u}]$, where $\mathbf{u}$ is the m-sequence with period 2^n-1. The sequence $\mathbf{u}$ has the following *shift-and-add property*.

Lemma 1 *[10, Theorem 5.3] Let $\mathbf{u}$ be an m-sequence with period 2^n-1. Then, for $0 < i < 2^n-1$, there exists $0 < j < 2^n-1$ such that $\mathbf{u}+L^i\mathbf{u} = L^j\mathbf{u}$ with $j = \tau_n(i)$.*

When $g(x)$ is not primitive, the situation is more involved.

Lemma 2 *Let $g(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n and order e (making $t = {}^{(2^n-1)}/_{e}$) with $\Omega(g(x))$ as presented in (5). Then, for each triple (i,j,k) with $0 \leq i,j,k < t$, we have*

$$(j-i,k-i)_t = \left|\{a \mid \mathbf{u}_i + L^a\mathbf{u}_j = L^b\mathbf{u}_k; 0 \leq a,b < e\}\right|. \tag{6}$$

Proof Using the correspondence

$$\mathbf{u}_i \longleftrightarrow (\varphi(\alpha^i\beta^0), \varphi(\alpha^i\beta^1), \ldots, \varphi(\alpha^i\beta^{e-1})) = \varphi(\alpha^i C_0),$$

we have

$$\mathbf{u}_i + L^a\mathbf{u}_j \longleftrightarrow \varphi(\alpha^i C_0) + \varphi(\alpha^j\beta^a C_0) = \varphi((\alpha^i + \alpha^j\beta^a)C_0) = \varphi((1+\alpha^{j-i}\beta^a)\alpha^i C_0).$$

Observe that as a runs through $\{0,1,\ldots,e-1\}$ there are $(j-i,k-i)_t$ such a, each of which satisfies $(1+\alpha^{j-i}\beta^a) = \alpha^{k-i}\beta^b$ for some b. In each occasion,

$$\varphi((1+\alpha^{j-i}\beta^a)\alpha^i C_0) = \varphi(\alpha^{k-i}\beta^b\alpha^i C_0) = \varphi(\alpha^k\beta^b C_0).$$

Note that the corresponding sequences are shifts of $\mathbf{u}_k$ and the proof is now complete. □

Lemma 3 *[10, Lemma 4.2] Let $g(x), h(x) \in \mathbb{F}_2[x]$ be two nonzero polynomials. Denote by $\Omega(g(x)) + \Omega(h(x))$ the set of sequences $\{\mathbf{g}+\mathbf{h} \mid \mathbf{g} \in \Omega(g(x)), \mathbf{h} \in \Omega(h(x))\}$. Then*

1. *$\Omega(g(x)) \subseteq \Omega(h(x))$ if and only if $g(x) \mid h(x)$.*
2. *$\Omega(g(x)) + \Omega(h(x)) = \Omega(\mathrm{lcm}(g(x),h(x)))$.*
3. *$\Omega(g(x)) \cap \Omega(h(x)) = \Omega(\gcd(g(x),h(x)))$.*

Lemma 4 *Let $f(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are two distinct irreducible polynomials in $\mathbb{F}_2[x]$ of degree m and n and order e_1 and e_2, respectively. Let $t_1 = \frac{2^m-1}{e_1}$ and $t_2 = \frac{2^n-1}{e_2}$. The cycle structure of $\Omega(f(x))$ is*

$$[\mathbf{0}] \cup \bigcup_{i=0}^{t_1-1}[\mathbf{u}_i] \cup \bigcup_{j=0}^{t_2-1}[\mathbf{s}_j] \cup \left(\bigcup_{i=0}^{t_1-1}\bigcup_{j=0}^{t_2-1}\bigcup_{k=0}^{\gcd(e_1,e_2)-1}[L^k\mathbf{u}_i + \mathbf{s}_j]\right). \tag{7}$$

Proof Based on (5), we have

$$\Omega(p(x)) = [\mathbf{0}] \cup [\mathbf{u}_0] \cup [\mathbf{u}_1] \cup \ldots \cup [\mathbf{u}_{t_1-1}] \text{ and } \Omega(q(x)) = [\mathbf{0}] \cup [\mathbf{s}_0] \cup [\mathbf{s}_1] \cup \ldots \cup [\mathbf{s}_{t_2-1}].$$

By Lemma 3, $\Omega(f(x))$ contains $\Omega(p(x))$ and $\Omega(q(x))$ as subsets. Hence,

$$[\mathbf{0}] \cup \bigcup_{i=0}^{t_1-1}[\mathbf{u}_i] \cup \bigcup_{j=0}^{t_2-1}[\mathbf{s}_j] \subseteq \Omega(f(x)).$$

The minimal polynomial of all other sequences in $\Omega(f(x))$ must be $f(x)$. The period of these sequences is the order of $f(x)$, which is $\mathrm{lcm}(e_1,e_2)$. The sequences are of the form

$$L^k\mathbf{u}_i + L^\ell\mathbf{s}_j = L^\ell(L^{k-\ell}\mathbf{u}_i + \mathbf{s}_j)$$

for some i,j,k, and ℓ, where $k-\ell$ is computed modulo e_1. They can be partitioned into

$$\frac{2^{m+n} - (2^m + 2^n - 1)}{\mathrm{lcm}(e_1,e_2)} = \frac{(2^m-1)(2^n-1)}{\mathrm{lcm}(e_1,e_2)} = \frac{(e_1 \cdot t_1)(e_2 \cdot t_2)}{\mathrm{lcm}(e_1,e_2)} = t_1 \cdot t_2 \cdot \gcd(e_1,e_2) \tag{8}$$

shift inequivalent classes.

Next, we show that $L^k\mathbf{u}_i + \mathbf{s}_j$ and $L^{k+t\cdot\gcd(e_1,e_2)}\mathbf{u}_i + \mathbf{s}_j$ are shift equivalent for $0 \leq k < \gcd(e_1,e_2)$ and $0 < t < {}^{e_1}/_{\gcd(e_1,e_2)}$. Since ${}^{e_1}/_{\gcd(e_1,e_2)}$ and ${}^{e_2}/_{\gcd(e_1,e_2)}$ are coprime, there exist $v, w \in \mathbb{Z}$ such that

$$v\,\frac{e_1}{\gcd(e_1,e_2)} + w\,\frac{e_2}{\gcd(e_1,e_2)} = 1 \iff t\,(\gcd(e_1,e_2) - v\cdot e_1) = t\cdot w\cdot e_2.$$

Since the periods of $\mathbf{u}_i$ and $\mathbf{s}_j$ are, respectively, e_1 and e_2,

$$L^{k+t\cdot\gcd(e_1,e_2)}\mathbf{u}_i + \mathbf{s}_j = L^{k+t\cdot\gcd(e_1,e_2)-t\cdot v\cdot e_1}\mathbf{u}_i + L^{t\cdot w\cdot e_2}\mathbf{s}_j = L^{t\cdot w\cdot e_2}(L^k\mathbf{u}_i + \mathbf{s}_j).$$

Because $0 \leq i < t_1$, $0 \leq j < t_2$, and $0 \leq k < \gcd(e_1,e_2)$, there are at most $t_1 \cdot t_2 \cdot \gcd(e_1,e_2)$ shift inequivalent cycles $[L^k\mathbf{u}_i + \mathbf{s}_j]$ for which the period of each sequence is $\operatorname{lcm}(e_1,e_2)$. Combined with (8), we conclude that there are exactly $t_1 \cdot t_2 \cdot \gcd(e_1,e_2)$ shift inequivalent classes and $[L^k\mathbf{u}_i + \mathbf{s}_j]$ with $0 \leq i < t_1$, $0 \leq j < t_2$, and $0 \leq k < \gcd(e_1,e_2)$ are the cycles. □

4 The Main Results

This most technical section contains two subsections. The first one studies the adjacency graph of $\Omega(f(x))$. The second one begins with a method to find a state belonging to a particular cycle and incorporates the results to design an algorithm that finds all conjugate pairs shared by any two cycles. It ends with a heuristic estimate of the number of de Bruijn sequences constructed.

4.1 The Adjacency Graph of $\Omega(f(x))$

Suppose that the special state $\mathbf{S} := (1,0,\ldots,0) \in \mathbb{F}_2^{m+n}$ is in a given cycle $[\mathbf{a}]$. Cycles $[\mathbf{b}]$ and $[\mathbf{c}]$ share a conjugate pair if and only if, for some $i, j, k \in \mathbb{Z}$,

$$L^i\mathbf{b} + L^j\mathbf{c} = L^k\mathbf{a} \iff \mathbf{b} + L^{j-i}\mathbf{c} = L^{k-i}\mathbf{a}.$$

This is the basic rule of finding the conjugate pairs shared by the cycles in $\Omega(f(x))$.

Since the degrees of the minimal polynomials of $\mathbf{u}_i$ and $\mathbf{s}_j$ are all $< m+n$, neither $\mathbf{u}_i$ nor $\mathbf{s}_j$ can contain $m+n-1$ consecutive 0s. Thus, for all i and j, $\mathbf{S} \notin [\mathbf{u}_i]$ and $\mathbf{S} \notin [\mathbf{s}_j]$. Hence, $\mathbf{S} \in [L^c\mathbf{u}_a + \mathbf{s}_b]$ for some nonnegative integers a, b, and c. From hereon, we use a, b, and c specifically to refer to the cycle $[L^c\mathbf{u}_a + \mathbf{s}_b]$ that contains the special state $\mathbf{S}$.

Proposition 1 *There exist some $a, b, c \in \mathbb{Z}$ such that $[\mathbf{0}]$ and $[L^c\mathbf{u}_a + \mathbf{s}_b]$ are adjacent. For arbitrary i and j, there is no conjugate pair between $[\mathbf{u}_i]$ and $[\mathbf{u}_j]$ and between $[\mathbf{s}_i]$ and $[\mathbf{s}_j]$.*

The next result determines the number of conjugate pairs between $[\mathbf{u}_i]$ and $[\mathbf{s}_j]$.

Proposition 2 *Let $0 \leq i < t_1$ and $0 \leq j < t_2$. Then $[\mathbf{u}_i]$ and $[\mathbf{s}_j]$ share a conjugate pair if and only if $i = a$ and $j = b$. When this is the case, the conjugate pair is unique.*

Proof $L^k\mathbf{u}_i + \mathbf{s}_j$ is a shift of $L^c\mathbf{u}_a + \mathbf{s}_b$ if and only if $i = a$, $j = b$, and $k \equiv c \pmod{\gcd(e_1,e_2)}$. By the proof of Lemma 4, for any $\ell \in \mathbb{Z}$, $[L^c\mathbf{u}_a + \mathbf{s}_b]$ and $[L^{c+\ell\cdot\gcd(e_1,e_2)}\mathbf{u}_a + \mathbf{s}_b]$ are shift equivalent. Thus, $[\mathbf{u}_a]$ and $[\mathbf{s}_b]$ share a unique conjugate pair. □

We now consider the number of conjugate pairs between $[\mathbf{u}_i]$ and $[L^\ell\mathbf{u}_j + \mathbf{s}_k]$.

Proposition 3 *Let $0 \leq i, j < t_1$ and $0 \leq \ell < \gcd(e_1, e_2)$. For a given (i, j), the following properties hold.*

1. *$[\mathbf{u}_i]$ and $[L^\ell \mathbf{u}_j + \mathbf{s}_k]$ share no conjugate pair when $k \neq b$.*
2. *The sum of the numbers of conjugate pairs between $[\mathbf{u}_i]$ and $[L^\ell \mathbf{u}_j + \mathbf{s}_b]$ from $\ell = 0$ to $\ell = \gcd(e_1, e_2) - 1$ is the cyclotomic number $\delta_1 := (i - j, a - j)_{t_1}$.*
3. *Suppose that after determining $\mathbf{u}_j + L^w \mathbf{u}_i$, for $0 \leq w < e_1$, we have found the δ_1 distinct shifts of $\mathbf{u}_a$, say*
$$L^{k_0}\mathbf{u}_a, L^{k_1}\mathbf{u}_a, \ldots, L^{k_{\delta_1 - 1}}\mathbf{u}_a.$$
The exact number of conjugate pairs between $[\mathbf{u}_i]$ and $[L^\ell \mathbf{u}_j + \mathbf{s}_b]$ is
$$\left|\{k_v \mid c - k_v \equiv \ell \ (\mathrm{mod}\ \gcd(e_1, e_2)) \text{ with } v = 0, 1, \ldots, \delta_1 - 1\}\right|. \tag{9}$$

Proof The first statement is clear.

Let $k = b$. Consider, for $0 \leq w < e_1$ and $0 \leq \ell < \gcd(e_1, e_2)$, the equation
$$L^\ell \mathbf{u}_j + \mathbf{s}_b + L^w \mathbf{u}_i = L^\ell(\mathbf{u}_j + L^{w-\ell}\mathbf{u}_i) + \mathbf{s}_b.$$
By Lemma 2, for a given ℓ, as w runs through $\{0, 1, \ldots, e_1 - 1\}$, there are δ_1 many $(w - \ell)$'s such that $\mathbf{u}_j + L^{w-\ell}\mathbf{u}_i$ is a shift of $\mathbf{u}_a$. By choosing an appropriate ℓ, we ensure that $L^\ell(\mathbf{u}_j + L^{w-\ell}\mathbf{u}_i) + \mathbf{s}_b$ is a shift of $L^c \mathbf{u}_a + \mathbf{s}_b$. Thus, for a given pair (i, j) with $0 \leq i, j < t_1$, the sum of the numbers of conjugate pairs between $[\mathbf{u}_i]$ and $[L^\ell \mathbf{u}_j + \mathbf{s}_b]$ from $\ell = 0$ to $\ell = \gcd(e_1, e_2) - 1$ is the cyclotomic number δ_1. This proves Statement 2.

Each of $L^{k_0}\mathbf{u}_a, L^{k_1}\mathbf{u}_a, \ldots, L^{k_{\delta_1 - 1}}\mathbf{u}_a$ corresponds to an $\ell_v \equiv c - k_v \ (\mathrm{mod}\ \gcd(e_1, e_2))$ with $0 \leq v < \delta_1$. Hence, $L^{\ell_v}L^{k_v}\mathbf{u}_a = L^{c'}\mathbf{u}_a$ where $c' \equiv c \ (\mathrm{mod}\ \gcd(e_1, e_2))$. Thus, the number of conjugate pairs between $[\mathbf{u}_i]$ and $[L^\ell \mathbf{u}_j + \mathbf{s}_b]$ for a given ℓ is indeed as given in (9). □

In an analogous way, we can obtain similar results on the number of conjugate pairs between $[\mathbf{s}_i]$ and $[L^\ell \mathbf{u}_k + \mathbf{s}_j]$ for $0 \leq i, j < t_2$.

Proposition 4 *Let $0 \leq i, j < t_2$ and $0 \leq \ell < \gcd(e_1, e_2)$. For a given (i, j), the following properties hold.*

1. *$[\mathbf{s}_i]$ and $[L^\ell \mathbf{u}_k + \mathbf{s}_j]$ share no conjugate pair when $k \neq a$.*
2. *The sum of the numbers of conjugate pairs between $[\mathbf{s}_i]$ and $[L^\ell \mathbf{u}_a + \mathbf{s}_j]$ from $\ell = 0$ to $\ell = \gcd(e_1, e_2) - 1$ is the cyclotomic number $\delta_2 := (i - j, b - j)_{t_2}$.*
3. *Suppose that after computing $(\mathbf{s}_j + L^w \mathbf{s}_i)$, for $0 \leq w < e_2$, we have determined the δ_2 distinct shifts of $\mathbf{s}_b$, say*
$$L^{k_0}\mathbf{s}_b, L^{k_1}\mathbf{s}_b, \ldots, L^{k_{\delta_2 - 1}}\mathbf{s}_b.$$
The exact number of conjugate pairs between $[\mathbf{s}_i]$ and $[L^\ell \mathbf{u}_a + \mathbf{s}_j]$ is
$$\left|\{k_v \mid c + k_v \equiv \ell \ (\mathrm{mod}\ \gcd(e_1, e_2)) \text{ with } v = 0, 1, \ldots, \delta_2 - 1\}\right|. \tag{10}$$

Let $0 \leq i_1, i_2 < t_1$, $0 \leq j_1, j_2 < t_2$, and $0 \leq \ell_1, \ell_2 < \gcd(e_1, e_2)$. We determine the number of conjugate pairs between $[L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $[L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$, using $\lambda := (j_2 - j_1, b - j_1)_{t_2}$ and $\mu := (i_2 - i_1, a - i_1)_{t_1}$ for brevity. Based on Lemma 2, we know of the following facts.

Fact 1: $L^{k_0}\mathbf{s}_b, L^{k_1}\mathbf{s}_b, \ldots, L^{k_{\lambda-1}}\mathbf{s}_b$ are the λ distinct shifts of $\mathbf{s}_b$ generated from $\mathbf{s}_{j_1} + L^\ell \mathbf{s}_{j_2}$. We denote the corresponding ℓ's modulo e_2 by $c_0, c_1, \ldots, c_{\lambda-1}$.

Fact 2: $L^{k'_0}\mathbf{u}_a, L^{k'_1}\mathbf{u}_a, \ldots, L^{k'_{\mu-1}}\mathbf{u}_a$ are the μ distinct shifts of $\mathbf{u}_a$ generated from $\mathbf{u}_{i_1} + L^\ell \mathbf{u}_{i_2}$. We denote the corresponding ℓ's modulo e_1 by $d_0, d_1, \ldots, d_{\mu-1}$.

Proposition 5 *With λ and μ as given above, let $0 \leq i_1, i_2 < t_1$, $0 \leq j_1, j_2 < t_2$, and $0 \leq \ell_1, \ell_2 < \gcd(e_1, e_2)$. For a given (i_1, i_2, j_1, j_2)-tuple, the following properties hold.*

1. *The sum of the numbers of conjugate pairs between cycles $[L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $[L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$ over all possible ℓ_1 and ℓ_2 is $\lambda \cdot \mu$.*
2. *The exact number of conjugate pairs between two <u>distinct</u> cycles $[L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $[L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$ is*

$$\begin{aligned} |\{(d_i, k_i', c_j, k_j) \mid \ell_1 \equiv c + k_j - k_i' \pmod{\gcd(e_1, e_2)} \text{ and} \\ \ell_2 \equiv c + k_j - k_i' + d_i - c_j \pmod{\gcd(e_1, e_2)}, \text{ with} \\ 0 \leq i < \mu \text{ and } 0 \leq j < \lambda\}|. \end{aligned} \tag{11}$$

Let $0 \leq i < t_1$, $0 \leq j < t_2$, and $0 \leq \ell < \gcd(e_1, e_2)$. The exact number of conjugate pairs between $[L^{\ell}\mathbf{u}_i + \mathbf{s}_j]$ and itself is

$$\begin{aligned} \frac{1}{2}|\{(d_i, k_i', c_j, k_j) \mid d_i \equiv c_j \pmod{\gcd(e_1, e_2)} \text{ and } \ell \equiv c + k_j - k_i' \pmod{\gcd(e_1, e_2)} \\ \text{with } 0 \leq i < (0, a-i)_{t_1} \text{ and } 0 \leq j < (0, b-j)_{t_2}\}|. \end{aligned} \tag{12}$$

Proof Let $C_1 = [L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $C_2 = [L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$. Let $0 \leq \ell < \operatorname{lcm}(e_1, e_2)$ and consider

$$\begin{aligned} L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1} + L^{\ell}(L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}) &= (L^{\ell_1}\mathbf{u}_{i_1} + L^{\ell+\ell_2}\mathbf{u}_{i_2}) + (\mathbf{s}_{j_1} + L^{\ell}\mathbf{s}_{j_2}) \\ &= L^{\ell_1}(\mathbf{u}_{i_1} + L^{\ell+\ell_2-\ell_1}\mathbf{u}_{i_2}) + (\mathbf{s}_{j_1} + L^{\ell}\mathbf{s}_{j_2}). \end{aligned} \tag{13}$$

To guarantee that this sequence is a shift of $L^c\mathbf{u}_a + \mathbf{s}_b$, we must ensure that $\mathbf{u}_{i_1} + L^{\ell+\ell_2-\ell_1}\mathbf{u}_{i_2}$ is a shift of $\mathbf{u}_a$ and $\mathbf{s}_{j_1} + L^{\ell}\mathbf{s}_{j_2}$ is a shift of $\mathbf{u}_b$. By Fact 1, ℓ must satisfy the system of congruences

$$\begin{cases} \ell \equiv d_i + \ell_1 - \ell_2 \pmod{e_1} \mid 0 \leq i < \mu, \\ \ell \equiv c_j \pmod{e_2} \mid 0 \leq j < \lambda. \end{cases} \tag{14}$$

By the Chinese Remainder Theorem [18, Theorem 2.9], the system has a unique solution if and only if, modulo $\gcd(e_1, e_2)$,

$$c_j \equiv d_i + \ell_1 - \ell_2 \iff \ell_2 - \ell_1 \equiv d_i - c_j. \tag{15}$$

If ℓ_1 and ℓ_2 satisfy (15) and ℓ satisfies (14), then (13) can be expressed as

$$L^{\ell_1}L^{k_i'}\mathbf{u}_a + L^{k_j}\mathbf{s}_b = L^{k_j}(L^{\ell_1+k_i'-k_j}\mathbf{u}_a + \mathbf{s}_b). \tag{16}$$

Computing modulo $\gcd(e_1, e_2)$ and taking

$$\ell_1 \equiv c + k_j - k_i' \text{ and } \ell_2 \equiv c + k_j - k_i' + d_i - c_j, \tag{17}$$

the sequence in (16) is indeed the required shift of $L^c\mathbf{u}_a + \mathbf{s}_b$. Thus, we get a conjugate pair between $[L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $[L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$. Note that, as ℓ_1 and ℓ_2 range through all of their respective values, it may happen that $C_1 = C_2$ for some (ℓ_1, ℓ_2) combination. When this is the case, we count the conjugate pairs $(\mathbf{v}, \hat{\mathbf{v}})$ and $(\hat{\mathbf{v}}, \mathbf{v})$ separately even though they are the same. There are $\mu \cdot \lambda$ choices for the tuple (d_i, k_i', c_j, k_j), proving Statement 1.

To verify Statement 2, notice that the exact number of conjugate pairs between two distinct cycles $[L^{\ell_1}\mathbf{u}_{i_1} + \mathbf{s}_{j_1}]$ and $[L^{\ell_2}\mathbf{u}_{i_2} + \mathbf{s}_{j_2}]$ is equal to the number of the tuples (d_i, k_i', c_j, k_j) that satisfy (17).

It remains to count the exact number of conjugate pairs between $[L^{\ell}\mathbf{u}_i + \mathbf{s}_j]$ and itself. By (15) and (17), computing modulo $\gcd(e_1, e_2)$, we have $d_i \equiv c_j$ and $\ell \equiv c + k_j - k_i'$. When considering the conjugate pairs between a cycle and itself, every conjugate pair is double counted. To get the correct number we halve the count. □

Theorem 2 *The adjacency graph of $\Omega(f(x))$ can be constructed based on the results in Propositions 1 to 5.*

In the earlier process of computing the number of conjugate pairs, we emphasize the *ordering of the cycles* by specifying the parameters i, j and ℓ in $[L^{\ell}\mathbf{u}_i + \mathbf{s}_j]$. The main reason is to benefit from the notions of cyclotomic classes and numbers. We also require $\mathbf{S} = (1,0,\ldots,0) \in [L^{c}\mathbf{u}_a + s_b]$. In practice, however, the order of the cycles does not matter. For two distinct orderings of the cycles, the corresponding matrices constructed based on Theorem 1 can be obtained from each other by properly permuting the rows and columns, which does not affect the cofactor.

4.2 Finding Conjugate Pairs

Recall the definition of $\mathbf{s}_i$ and its successor $\mathbf{s}_{i+1}$ of an n-stage FSR sequence $\mathbf{s}$ with feedback function $f(x_0,\ldots,x_{n-1})$ from Section 2. A *state operator T* turns $\mathbf{s}_i$ into $\mathbf{s}_{i+1}$ with $s_{i+n} = f(s_i,\ldots,s_{i+n-1})$. Hence, if the state $\mathbf{s}_i$ belongs to cycle $[\mathbf{s}]$, then all the states of $[\mathbf{s}]$ are $\mathbf{s}_i, T\mathbf{s}_i, T^2\mathbf{s}_i, \ldots$. If e is the period of $\mathbf{s}$, then the distinct states are

$$\mathbf{s}_i, T\mathbf{s}_i = \mathbf{s}_{i+1}, \ldots, T^{e-1}\mathbf{s}_i = \mathbf{s}_{i+e-1}.$$

Thus, finding one state in a given cycle is sufficient to generate all distinct states. To reduce clutters, T may be used to denote the state operator for distinct cycles with distinct stages and $\mathbf{0}$ is used to denote zero vectors and sequences with arbitrary lengths. The context provides enough information to avoid confusion.

For any irreducible polynomial of degree n and order e over $\mathbb{F}_2$, the corresponding cycle structure is given in (5). For each cycle, there are several ways to find one of its states. One can perform an exhaustive search or use the correspondence between cycles and cyclotomic classes defined in the Section 3 to accomplish the task.

Now, assume that a state belonging to each of the cycles in $\Omega(p(x))$ and in $\Omega(q(x))$ has been found. We propose an efficient way to determine a state belonging to each of the cycles in $\Omega(f(x) = p(x)q(x))$. Let $[L^{\ell}\mathbf{u}_i + \mathbf{s}_j]$ with $i, j, \ell \in \mathbb{Z}$ be a cycle in $\Omega(f(x))$. If $\mathbf{u}_i = u_0, u_1, u_2, \ldots$ and $\mathbf{s}_j = s_0, s_1, s_2, \ldots$, then we have

$$L^{\ell}\mathbf{u}_i + \mathbf{s}_j = u_{\ell} + s_0, u_{\ell+1} + s_1, u_{\ell+2} + s_2, \ldots$$

and the k-th state $\mathbf{v}_k = (v_0, v_1, \ldots, v_{m+n-1})$ of $[L^{\ell}\mathbf{u}_i + \mathbf{s}_j]$ satisfies

$$\begin{aligned}\mathbf{v}_k &= (u_{\ell+k} + s_k, \ldots, u_{\ell+k+m+n-1} + s_{k+m+n-1}) \\ &= (u_{\ell+k}, \ldots, u_{\ell+k+m+n-1}) + (s_k, \ldots, s_{k+m+n-1}).\end{aligned} \tag{18}$$

Note that $(u_{\ell+k}, \ldots, u_{\ell+k+m+n-1})$ and $(s_k, \ldots, s_{k+m+n-1})$ are uniquely and linearly determined by, respectively, $(u_{\ell+k}, \ldots, u_{\ell+k+m-1})$ and $(s_k, \ldots, s_{k+n-1})$. These last two are, respectively, the m-stage $(\ell+k)$-th state of $\mathbf{u}_i$ and the n-stage k-th state of $\mathbf{s}_j$. Thus, once the states of $\mathbf{u}_i$ and $\mathbf{s}_j$ are known, we can determine the corresponding state in $L^{\ell}\mathbf{u}_i + \mathbf{s}_j$.

Now, let $\mathbf{v}_k$ be known. Since $(u_{\ell+k}, \ldots, u_{\ell+k+m+n-1})$ and $(s_k, \ldots, s_{k+m+n-1})$ are uniquely and linearly determined by $(u_{\ell+k}, \ldots, u_{\ell+k+m-1})$ and $(s_k, \ldots, s_{k+n-1})$, respectively, one can use (18) to construct nonhomogeneous linear equations whose unique solution is, by the properties of LFSR, $(u_{\ell+k}, \ldots, u_{\ell+k+m-1}, s_k, \ldots, s_{k+n-1})$. Thus, from $\mathbf{v}_k$, the m-stage $(\ell+k)$-th state of $\mathbf{u}_i$ and the n-stage k-th state of $\mathbf{s}_j$ can be uniquely determined.

We construct an $(m+n) \times (m+n)$ matrix P from two matrices, namely an $m \times (m+n)$ matrix P_1 built from $p(x)$ and an $n \times (m+n)$ matrix P_2 based on $q(x)$. P_1 is the first m rows of P while P_2 is the last n rows. The i-th row of P_1 is the first $m+n$ bits of the sequence generated by the LFSR with characteristic polynomial $p(x)$ whose m-stage initial state has 1 in the i-th position and 0 elsewhere. Similarly, the j-th row of P_2 is the first $m+n$ bits of the sequence generated by the LFSR with characteristic polynomial $q(x)$ whose n-stage initial state has 1 in the j-th position and 0 elsewhere. Hence, the first m columns of P_1 is the I_m identity matrix and the first n columns of P_2 is the I_n identity matrix. Since $p(x)$ and $q(x)$ are distinct irreducible polynomials, P is full-rank.

Let $\mathbf{v} \in \mathbb{F}_2^{m+n}$, $\mathbf{a} \in \mathbb{F}_2^m$, and $\mathbf{b} \in \mathbb{F}_2^n$ be, respectively, the initial $(m+n)$-, m-, and n-stage states of $L^\ell \mathbf{u}_i + \mathbf{s}_j$, $\mathbf{u}_i$, and $\mathbf{s}_j$. We denote by $(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^{m+n}$ the simple concatenation of $\mathbf{a}$ and $\mathbf{b}$. There is a one-to-one correspondence between $\mathbf{v}$ and $(T^\ell \mathbf{a},\mathbf{b})$ through the mapping P

$$\mathbf{v} = (T^\ell \mathbf{a},\mathbf{b})P \text{ and } (T^\ell \mathbf{a},\mathbf{b}) = \mathbf{v}P^{-1}. \tag{19}$$

Notice that if $\mathbf{v}$ is the $(m+n)$-stage state of $[\mathbf{u}_i]$, then $\mathbf{v} = (\mathbf{a},\mathbf{0})P$ and, if $\mathbf{v}$ is the $(m+n)$-stage state of $[\mathbf{s}_j]$, then $\mathbf{v} = (\mathbf{0},\mathbf{b})P$. Clearly,

$$(T^k \mathbf{v})P^{-1} = T^k(\mathbf{v}P^{-1}) = (T^{\ell+k}\mathbf{a}, T^k \mathbf{b}) \text{ and } (\mathbf{v}_1+\mathbf{v}_2)P^{-1} = \mathbf{v}_1 P^{-1} + \mathbf{v}_2 P^{-1}.$$

We view $(T^\ell \mathbf{a},\mathbf{b})$ as a state of $[L^\ell \mathbf{u}_i + \mathbf{s}_j]$, keeping in mind that the actual state is $(T^\ell \mathbf{a},\mathbf{b})P$.

Let $\mathbf{p}_0,\mathbf{p}_1,\ldots,\mathbf{p}_{t_1-1}$ be arbitrary m-stage states of $[\mathbf{u}_0],[\mathbf{u}_1],\ldots,[\mathbf{u}_{t_1-1}]$. Similarly, let $\mathbf{q}_0,\mathbf{q}_1,\ldots,\mathbf{q}_{t_2-1}$ be arbitrary n-stage states of $[\mathbf{s}_0],[\mathbf{s}_1],\ldots,[\mathbf{s}_{t_2-1}]$. Then $(\mathbf{p}_i,\mathbf{q}_j)$ must be a state of $[L^\ell \mathbf{u}_i + \mathbf{s}_j]$ for some $0 \le \ell < \gcd(e_1,e_2)$. Similarly, $(T^k \mathbf{p}_i,\mathbf{q}_j)$, for $0 \le k < \gcd(e_1,e_2)$, must be a state of $[L^{\ell+k}\mathbf{u}_i + \mathbf{s}_j]$, where $\ell+k$ is reduced modulo $\gcd(e_1,e_2)$. Since the exact value of ℓ does not affect the final result, we let ℓ be any integer. Thus, we obtain one state of each cycle.

We now use this new representation of the states via the mapping P to construct a generic algorithm to find all conjugate pairs between any two cycles in $\Omega(f(x))$. For $C_1,C_2 \in \Omega(f(x))$, let $\mathbf{v}_1 = (T^{x_1}\mathbf{a}_1, T^{x_2}\mathbf{b}_1)P$ be a state of C_1 and $\mathbf{v}_2 = (T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)P$ a state of C_2 where $x_1,x_2,x_3,x_4 \in \mathbb{Z}$. Let e_1 and e_2 be the respective period of the sequences containing states $\mathbf{a}_1$, $\mathbf{a}_2$ and $\mathbf{b}_1$, $\mathbf{b}_2$. We assume that the period of $(\mathbf{0})$ is 1. Algorithm 1 outputs all conjugate pairs between C_1 and C_2. If $C_1 = C_2$, then each conjugate pair appears twice in the output, first as $(\mathbf{v},\hat{\mathbf{v}})$ and then as $(\hat{\mathbf{v}},\mathbf{v})$.

Theorem 3 *Algorithm 1 is correct.*

Proof If $counter_1 = 0$ or $counter_2 = 0$, then there does not exist a conjugate pair.

Let $(\mathbf{a}_3,\mathbf{b}_3)P = \mathbf{S}$ be the initial state of $[L^c \mathbf{u}_a + \mathbf{s}_b]$. Without loss of generality, let $C_1 = [\mathbf{s}_1]$ and $C_2 = [\mathbf{s}_2]$ with initial states $\mathbf{v}_1 = (T^{x_1}\mathbf{a}_1, T^{x_2}\mathbf{b}_1)P$ and $\mathbf{v}_2 = (T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)P$, respectively. If C_1 and C_2 share a conjugate pair, then there must exist an integer $0 \le \ell < \operatorname{lcm}(e_1,e_2)$ such that $L^\ell \mathbf{s}_1 + \mathbf{s}_2$ is a shift of $L^c \mathbf{u}_a + \mathbf{s}_b$ or $L^\ell \mathbf{s}_1 + L^c \mathbf{u}_a + \mathbf{s}_b$ is a shift of $\mathbf{s}_2$.

Suppose that none of $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$ is $\mathbf{0}$. Then there exist $0 \le \ell,\ell' < \operatorname{lcm}(e_1,e_2)$ such that $[T^\ell(T^{x_1}\mathbf{a}_1, T^{x_2}\mathbf{b}_1) + (\mathbf{a}_3,\mathbf{b}_3)]P = T^{\ell'}[(T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)P] = [T^{\ell'}(T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)]P$. Hence, $T^\ell(T^{x_1}\mathbf{a}_1, T^{x_2}\mathbf{b}_1) + (\mathbf{a}_3,\mathbf{b}_3) = T^{\ell'}(T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)$. Splitting the expression into two separate components, consider

$$T^{\ell+x_1}\mathbf{a}_1 + \mathbf{a}_3 = T^{\ell'+x_3}\mathbf{a}_2 \text{ and } T^{\ell+x_2}\mathbf{b}_1 + \mathbf{b}_3 = T^{\ell'+x_4}\mathbf{b}_2. \tag{20}$$

Algorithm 1 Finding All Conjugate Pairs between Two Cycles

```
Input: $P, \mathbf{v}_1 = (\mathbf{a}_1, \mathbf{b}_1)P$, $\mathbf{v}_2 = (\mathbf{a}_2, \mathbf{b}_2)P$, states of $C_1$ and of $C_2$, and $e_1$, $e_2$.
Output: All conjugate pairs between $C_1$ and $C_2$. If $C_1 = C_2$, each pair appears twice.
procedure PRECOMPUTATION $(P, \mathbf{S})$    ▷ Determining $\mathbf{a}_3, \mathbf{b}_3$
    return $(\mathbf{a}_3, \mathbf{b}_3) = \mathbf{S}P^{-1}$
end procedure
procedure SUBALGORITHM 1 ($\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{a}_3$, $e_1$)
    $counter_1 \leftarrow 0$
    for $i$ from 0 to $e_1 - 1$ do    ▷ If $\mathbf{a}_1 = \mathbf{0}$, then $e_1 = 1$
        $temp1 \leftarrow \mathbf{a}_1 + \mathbf{a}_3$
        for $i'$ from 0 to $e_1 - 1$ do    ▷ If $\mathbf{a}_2 = \mathbf{0}$, then $e_1 = 1$
            if $temp1 = \mathbf{a}_2$ then
                $counter_1 \leftarrow counter_1 + 1$
                Store and index $(i, i')$; break from this inner loop
            else
                $temp1 \leftarrow T(temp1)$
            end if
        end for
        $\mathbf{a}_1 \leftarrow T\mathbf{a}_1$
    end for
end procedure
procedure SUBALGORITHM 2 ($\mathbf{b}_1$, $\mathbf{b}_2$, $\mathbf{b}_3$, $e_2$)
    $counter_2 \leftarrow 0$
    for $j$ from 0 to $e_2 - 1$ do    ▷ If $\mathbf{b}_1 = \mathbf{0}$, then $e_2 = 1$
        $temp2 \leftarrow \mathbf{b}_1 + \mathbf{b}_3$
        for $j'$ from 0 to $e_2 - 1$ do    ▷ If $\mathbf{b}_2 = \mathbf{0}$, then $e_2 = 1$
            if $temp2 = \mathbf{b}_2$ then
                $counter_2 \leftarrow counter_2 + 1$
                Store and index $(j, j')$; break from this inner loop
            else
                $temp2 \leftarrow T(temp2)$
            end if
        end for
        $\mathbf{b}_1 \leftarrow T\mathbf{b}_1$
    end for
end procedure
procedure MAIN ($\mathbf{v}_1 = (T^{x_1}\mathbf{a}_1, T^{x_2}\mathbf{b}_1)P$, $\mathbf{v}_2 = (T^{x_3}\mathbf{a}_2, T^{x_4}\mathbf{b}_2)P$, $counter_1$, $counter2$)
    if $counter_1 = 0$ or $counter_2 = 0$ then
        return there is no conjugate pair    ▷ Propositions 1 and 2
    end if
    for $y$ from 1 to $counter_1$ do
        Take $(i, i')$ in order
        for $z$ from 1 to $counter_2$ do
            Take $(j, j')$ in order
            if Two elements among $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, $\mathbf{b}_2$ are $\mathbf{0}$ then
                $\mathbf{v} \leftarrow (T^i\mathbf{a}_1, T^j\mathbf{b}_1)P$; output $(\mathbf{v}, \hat{\mathbf{v}})$; break    ▷ Propositions 1 and 2
            end if
            if One element among $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, $\mathbf{b}_2$ is $\mathbf{0}$ then
                if $\mathbf{a}_1 = \mathbf{0}$ or $\mathbf{b}_1 = \mathbf{0}$ then
                    if $i' + x_3 \equiv j' + x_4 \pmod{\gcd(e_1, e_2)}$ then
                        $\mathbf{v} \leftarrow (T^i\mathbf{a}_1, T^j\mathbf{b}_1)P$; output $(\mathbf{v}, \hat{\mathbf{v}})$    ▷ Propositions 3 and 4
                    end if
                else
                    if $i - x_1 \equiv j - x_2 \pmod{\gcd(e_1, e_2)}$ then
                        $\mathbf{v} \leftarrow (T^i\mathbf{a}_1, T^j\mathbf{b}_1)P$; output $(\mathbf{v}, \hat{\mathbf{v}})$    ▷ Propositions 3 and 4
                    end if
                end if
            end if
            if $i - x_1 \equiv j - x_2$ and $i' + x_3 \equiv j' + x_4$ modulo $\gcd(e_1, e_2)$ then
                $\mathbf{v} \leftarrow (T^i\mathbf{a}_1, T^j\mathbf{b}_1)P$; output $(\mathbf{v}, \hat{\mathbf{v}})$    ▷ Proposition 5
            end if
        end for
    end for
end procedure
```

We have (i,i') and (j,j') satisfying $T^i\mathbf{a}_1+\mathbf{a}_3=T^{-i'}\mathbf{a}_2$ and $T^j\mathbf{b}_1+\mathbf{b}_3=T^{-i'}\mathbf{b}_2$ from the two subalgorithms. To ensure that (20) holds, it must be the case that

$$\begin{cases}\ell\equiv i-x_1 \pmod{e_1}\\ \ell\equiv j-x_2 \pmod{e_2}\end{cases} \quad\text{and}\quad \begin{cases}\ell'\equiv -i'-x_3 \pmod{e_1}\\ \ell'\equiv -j'-x_4 \pmod{e_2}\end{cases}.$$

To satisfy the requirements, we know from the Chinese Remainder Theorem that the congruences $i-x_1\equiv j-x_2$ and $i'+x_3\equiv j'+x_4$ modulo $\gcd(e_1,e_2)$ must be simultaneously satisfied. When (i,i') and (j,j') satisfy the congruences, $(T^i\mathbf{a}_1,T^j\mathbf{b}_1)P$ and $(T^{-i'}\mathbf{a}_2,T^{-j'}\mathbf{b}_2)P$ form a conjugate pair.

If $\mathbf{a}_1=\mathbf{0}$ or $\mathbf{a}_2=\mathbf{0}$ but $\mathbf{b}_1,\mathbf{b}_2$ are not $\mathbf{0}$, we assume $\mathbf{a}_1=\mathbf{0}$. Hence, $(i,i')=(0,i')$ and (20) becomes $\mathbf{a}_3=T^{\ell'+x_3}\mathbf{a}_2$ and $T^{\ell+x_2}\mathbf{b}_1+\mathbf{b}_3=T^{\ell'+x_4}\mathbf{b}_2$. If there exists (j,j') such that $T^j\mathbf{b}_1+\mathbf{b}_3=T^{-i'}\mathbf{b}_2$, then there is an ℓ with the required properties. It now suffices to check that ℓ' satisfies $\ell'\equiv -i'-x_3 \pmod{e_1}$ and $\ell'\equiv -j'-x_4 \pmod{e_2}$ to ensure $i'+x_3\equiv j'+x_4 \pmod{\gcd(e_1,e_2)}$.

The other cases can be similarly proved. □

We gain significantly from using the new representation of the states. Algorithm 1 relies on the representation to transform the problem of finding conjugate pairs between any two cycles in $\Omega(f(x))$ into the analogous problem in the smaller sets of cycles $\Omega(p(x))$ and $\Omega(q(x))$ whose characteristic polynomials are irreducible. The two subalgorithms ensure that the sum of the two states is equal to the indicated part in the new representation of $\mathbf{S}$. Finding a conjugate pair between any two cycles in $\Omega(f(x))$ by exhaustive search can be done in $(\mathrm{lcm}(e_1,e_2))^2$ times. Algorithm 1 requires at most $e_1^2+e_2^2$ times to complete the same task.

In particular, if $\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3$ are states of cycles in $\Omega(p(x))$ where $p(x)$ is primitive, then the connection can be made simpler by using the Zech logarithm $\tau_n(\ell)$. Recall that for a primitive element $\alpha\in\mathbb{F}_{2^n}$, $1+\alpha^\ell=\alpha^{\tau_n(\ell)}$ for $1\leq\ell<2^n-1$. If $\mathbf{a}$ is an n-stage state of an m-sequence, then Lemma 1 says that $\mathbf{a}+T^\ell\mathbf{a}=T^{\tau_n(\ell)}\mathbf{a}$. Suppose it has been established that $\mathbf{a}:=\mathbf{a}_1=\mathbf{a}_2$ and $\mathbf{a}_3=T^k\mathbf{a}$. Then the output (i,i') in the first subalgorithm implies $T^i\mathbf{a}_1+\mathbf{a}_3=T^{-i'}\mathbf{a}_2$. Hence,

$$T^i\mathbf{a}+T^k\mathbf{a}=T^k(\mathbf{a}+T^{i-k}\mathbf{a})=T^{k+\tau_n(i-k)}\mathbf{a}=T^{-i'}\mathbf{a},$$

with $i\in\{0,1,\ldots,2^n-2\}\setminus\{k\}$. Thus, as i ranges over the set $\{0,1,\ldots,2^n-2\}\setminus\{k\}$, all possible values for (i,i') are given by $\{(i,-k-\tau_n(i-k))\}$. In this special case, knowing $\tau_n(\ell)$ is sufficient to deduce all possible (i,i')s.

Remark 2 Several remarks regarding Algorithm 1 are in order.

1. The choice of a state belonging to a cycle affects neither the number of conjugate pairs nor the states being paired in each conjugate pair.
2. The ordering of $\mathbf{a}_1$ and $\mathbf{a}_2$ matters in Subalgorithm 1. If the output on input $(\mathbf{a}_1,\mathbf{a}_2,\mathbf{a}_3,e_1)$ is (i,i'), then that on input $(\mathbf{a}_2,\mathbf{a}_1,\mathbf{a}_3,e_1)$ is $(-i',-i)$.
3. Each subalgorithm finds ”conjugate pairs” between two cycles constructed from one irreducible minimal polynomial by exhaustive searching. An improvement on this approach may give a significant speed up. In $\Omega(p(x))$, suppose that $\mathbf{a}_1$, $\mathbf{a}_2$, and $\mathbf{a}_3$ are the respective states of cycles $[\mathbf{u}_i]$, $[\mathbf{u}_j]$, and $[\mathbf{u}_k]$. Then Subalgorithm 1 should output $(i-k,j-k)_{t_1}$ tuples and can be stopped once all of them have been found. If it has been established that the cyclotomic number is 0, then there is no need to run the algorithm on this particular input case. Knowing the cyclotomic numbers allows us to truncate the

running of the algorithm. Equivalently, up to some values of m and n, the two subalgorithms can determine the exact cyclotomic numbers computationally by using $counter_1$ and $counter_2$.

4. Let us consider the running time. The precomputation gives us $\mathbf{S}P^{-1} = (\mathbf{a}_3, \mathbf{b}_3)$. Hence, we immediately infer which cycle shares a conjugate pair with $[\mathbf{0}]$ without having to run the subalgorithms. By Item 2 above, the outputs of Subalgorithm $1(\mathbf{a}_2, \mathbf{a}_1, \mathbf{a}_3, e_1)$ follow directly from the outputs of Subalgorithm $1(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, e_1)$. Thus, Subalgorithm 1 needs to perform at most $\frac{t_1(t_1-1)}{2} + t_1 = \frac{t_1(t_1+1)}{2}$ operations. The total for the two subalgorithms is therefore $\frac{t_1(t_1+1)}{2} + \frac{t_2(t_2+1)}{2}$. The main procedure needs to be performed at most $e_1 \cdot e_2$ times. The total number one needs to repeat Algorithm 1 to complete the adjacency matrix is bounded above by the square of the number of cycles in $\Omega(f(x))$.

To end this subsection, we provide a rough estimate on the number of de Bruijn sequences generated by our method. Let G be the adjacency graph of $\Omega(p(x)q(x))$. The number is the cofactor of any entry of the symmetric and positive definite matrix $\mathscr{M}$ in Theorem 1. With $[\mathbf{0}]$ as the first vertex, we use the cofactor of the entry $\mathscr{M}_{1,1} = 1$. The product of the (remaining) entries in the main diagonal of $\mathscr{M}$ is a reasonably good heuristic to approximate the number.

In the main diagonal, 1 occurs once, e_1 appears t_1 times, e_2 appears t_2 times, and there are $\chi := \frac{(2^n-1)(2^m-1)}{\mathrm{lcm}(e_1,e_2)} = t_1 \cdot t_2 \cdot \gcd(e_1, e_2)$ other entries, each is approximately $\mathrm{lcm}(e_1, e_2)$. The product of these χ entries is

$$E \approx (\mathrm{lcm}(e_1,e_2))^{\chi} = \left(\frac{e_1 \cdot e_2}{\gcd(e_1,e_2)}\right)^{\chi} = \left(\frac{(2^m-1)(2^n-1)}{\chi}\right)^{\chi} \approx \left(\frac{2^{m+n}}{\chi}\right)^{\chi}. \tag{21}$$

We use the last expression as a rough estimate on the number of de Bruijn sequences constructed in this work.

5 A Detailed Example

This section demonstrates how the general techniques developed above fit together nicely by way of a worked-out example. Let $p(x) = x^4 + x^3 + x^2 + x + 1$ and $q(x) = x^4 + x + 1$. Note that $p(x)$ is not primitive. Let α be a root of $q(x)$. Then $\beta = \alpha^3$ and the order of β is 5. Given $0 \leq j < 15$, Table 1 provides the representation $(a_{j,0}, a_{j,1}, a_{j,2}, a_{j,3})$ of α^j in the β basis $\{1, \beta, \beta^2, \beta^3\}$ and $\varphi(\alpha^j) = \left(a_{j,0}, a_{j+3,0}, a_{j+6,0}, a_{j+9,0}\right)$.

Table 1 List of $\varphi(\alpha^j)$ for $0 \leq j < 15$

j	in β basis	$\varphi(\alpha^j)$	j	in β basis	$\varphi(\alpha^j)$	j	in β basis	$\varphi(\alpha^j)$
0	$(1,0,0,0)$	$(1,0,0,0)$	5	$(0,0,1,1)$	$(0,1,0,1)$	10	$(1,0,1,1)$	$(1,1,0,1)$
1	$(0,1,0,1)$	$(0,1,1,1)$	6	$(0,0,1,0)$	$(0,0,1,1)$	11	$(0,1,1,1)$	$(0,1,0,0)$
2	$(0,1,1,0)$	$(0,0,1,0)$	7	$(1,0,0,1)$	$(1,1,1,0)$	12	$(1,1,1,1)$	$(1,1,0,0)$
3	$(0,1,0,0)$	$(0,0,0,1)$	8	$(1,1,1,0)$	$(1,0,1,0)$	13	$(1,0,1,0)$	$(1,0,1,1)$
4	$(1,1,0,1)$	$(1,1,1,1)$	9	$(0,0,0,1)$	$(0,1,1,0)$	14	$(1,1,0,0)$	$(1,0,0,1)$

By (4), $\mathbf{u}_i = (a_{i,0}, a_{i+3,0}, a_{i+6,0}, a_{i+9,0}, a_{i+12,0})$. Therefore, $\mathbf{u}_0 = (10001)$, $\mathbf{u}_1 = (01111)$, $\mathbf{u}_2 = (00101)$, and $\mathbf{s} = (10001\ 00110\ 10111)$. We have $\Omega(p(x)) = [\mathbf{0}] \cup [\mathbf{u}_0] \cup [\mathbf{u}_1] \cup [\mathbf{u}_2]$ and

$\Omega(q(x)) = [\mathbf{0}] \cup [\mathbf{s}]$. Thus, there are 20 disjoint cycles in $\Omega(f(x))$. Writing explicitly,

$$\Omega(f(x)) = [\mathbf{0}] \,\cup\, [\mathbf{s}] \,\cup\, \bigcup_{i=0}^{2} [\mathbf{u}_i] \,\cup\, \left(\bigcup_{i=0}^{2} \bigcup_{j=0}^{4} [L^j \mathbf{u}_i + \mathbf{s}] \right).$$

The ordering of the 20 cycles in use is

$$[\mathbf{0}], [\mathbf{u}_0], [\mathbf{u}_1], [\mathbf{u}_2], [\mathbf{s}], [\mathbf{u}_0 + \mathbf{s}], \ldots, [L^4 \mathbf{u}_0 + \mathbf{s}], [\mathbf{u}_1 + \mathbf{s}], \ldots, [L^4 \mathbf{u}_1 + \mathbf{s}], [\mathbf{u}_2 + \mathbf{s}], \ldots, [L^4 \mathbf{u}_2 + \mathbf{s}].$$

We show how to implement Algorithm 1, work on the adjacency graph of $\Omega(f(x))$, and construct the associated matrix $\mathscr{M}_1$.

The 4-stage states of $\mathbf{u}_0, \mathbf{u}_1, \mathbf{u}_2$, and $\mathbf{s}$ are, respectively, $\mathbf{p}_0 = (1000)$, $\mathbf{p}_1 = (0111)$, $\mathbf{p}_2 = (0010)$, and $\mathbf{q} = (1000)$. The cycles in $\Omega(f(x))$ can be represented by their 8-stage states

$$\begin{aligned} &(\mathbf{0}, \mathbf{0}) \in [\mathbf{0}], \;\; (\mathbf{p}_i, \mathbf{0}) \in [\mathbf{u}_i] \text{ for } i \in \{0,1,2\}, \\ &(\mathbf{0}, \mathbf{q}) \in [\mathbf{s}], \;\; (T^j \mathbf{p}_i, \mathbf{b}) \in [L^j \mathbf{u}_i + \mathbf{s}] \text{ for } i \in \{0,1,2,3,4\}. \end{aligned}$$

Using sequences $\mathbf{u}_0, \mathbf{u}_2, \mathbf{u}_2$, and $\mathbf{s} = (10001\ 00110\ 10111)$,

$$P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \left(\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right).$$

We compute $\mathbf{S}P^{-1} = ((1101), (0101)) = (T^3 \mathbf{p}_1, T^9 \mathbf{q}) = T^9 (T^4 \mathbf{p}_1, \mathbf{q}) \in [L^4 \mathbf{u}_1 + \mathbf{s}]$ to conclude that $[\mathbf{0}]$ and $[L^4 \mathbf{u}_1 + \mathbf{s}]$ are adjacent and the unique conjugate pair shared by $[\mathbf{u}_1]$ and $[\mathbf{s}]$ is $(\mathbf{v} = (T^3 \mathbf{p}_1, \mathbf{0}) P, \hat{\mathbf{v}})$. In Algorithm 1, use $\mathbf{a}_3 = (1101) = T^3 \mathbf{p}_1$ and $\mathbf{b}_3 = (0101) = T^9 \mathbf{q}$.

Running Subalgorithm 1, we have

$$\begin{array}{r|c|c|c|c|c|c} (\mathbf{a}_1, \mathbf{a}_2) = & (\mathbf{p}_0, \mathbf{p}_0) & (\mathbf{p}_0, \mathbf{p}_1) & (\mathbf{p}_0, \mathbf{p}_2) & (\mathbf{p}_1, \mathbf{p}_2) & (\mathbf{p}_2, \mathbf{p}_2) & (\mathbf{0}, \mathbf{p}_1) \\ \{(i, i')\} = & \{(1,1), (4,4)\} & \{(2,3), (3,1)\} & \{(0,4)\} & \{(0,3), (1,0)\} & \{(3,1), (4,2)\} & \{(0,2)\} \end{array}. \tag{22}$$

There is no output corresponding to $(\mathbf{p}_1, \mathbf{p}_1)$. The rest of the outputs can be directly obtained by invoking Item 2 in Remark 2. Hence, for $(\mathbf{a}_1, \mathbf{a}_2) \in \{(\mathbf{p}_1, \mathbf{p}_0), (\mathbf{p}_2, \mathbf{p}_0), (\mathbf{p}_2, \mathbf{p}_1)\}$, the respective outputs $\{(i, i')\}$ are $\{(2,3), (4,2)\}, \{(1,0)\}$, and $\{(2,0), (0,4)\}$.

On input $(\mathbf{0}, \mathbf{q}, T^9 \mathbf{q}, 15)$, Subalgorithm 2 outputs $(j, j') = (0, 6)$. On $(\mathbf{q}, \mathbf{q}, T^9 \mathbf{q}, 15)$, it outputs $\{(j, j' = -9 - \tau_4(j - 9))\}$ with $j \neq 9$. The values of $\tau_4(y)$ for $1 \leq y < 15$ is reproduced here from [10, p. 39]

y	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\tau_4(y)$	4	8	14	1	10	13	9	2	7	5	12	11	6	3

The conjugate pair(s) shared by any two cycles in $\Omega(f(x))$ can now be determined. We consider three cases in details.

Table 2 Values obtained for Case 1

k	(i,i')	ℓ	C_2	$\mathbf{v}$	(i,i')	ℓ	C_2	$\mathbf{v}$
0	$(1,1)$	0	$[\mathbf{u}_0+\mathbf{s}]$	$(T\mathbf{p}_0,\mathbf{0})P$	$(4,4)$	2	$[L^2\mathbf{u}_0+\mathbf{s}]$	$(T^4\mathbf{p}_0,\mathbf{0})P$
1	$(2,3)$	3	$[L^3\mathbf{u}_1+\mathbf{s}]$	$(T^2\mathbf{p}_0,\mathbf{0})P$	$(3,1)$	0	$[\mathbf{u}_1+\mathbf{s}]$	$(T^3\mathbf{p}_0,\mathbf{0})P$
2	$(0,4)$	2	$[L^2\mathbf{u}_2+\mathbf{s}]$	$(\mathbf{p}_0,\mathbf{0})P$				

Case 1: The state $(\mathbf{p}_0,\mathbf{0})P$ belongs to $C_1=[\mathbf{u}_0]$.
We have $(i,i')\in\{(1,1),(4,4),(2,3),(3,1),(0,4)\}$ and $(j,j')=(0,6)$. Since $\mathbf{a}_1=\mathbf{p}_0$ and $\mathbf{a}_3=T^3\mathbf{p}_1$, $\mathbf{a}_2\neq\mathbf{0}$. Since $\mathbf{b}_3\neq\mathbf{0}$ and $\mathbf{b}_1=\mathbf{0}$, $\mathbf{b}_2\neq\mathbf{0}$. Hence, C_2 that shares at least a conjugate pair with $[\mathbf{u}_0]$ must be of the form $[L^\ell\mathbf{u}_k+\mathbf{s}]$ for $0\leq k<3$. The if loop to consider starts from Line 45 in Algorithm 1. Note that $x_3=\ell$ and $x_4=0$, so $i'+\ell\equiv j' \pmod 5$. Table 2 provides the relevant results. The state $\mathbf{v}$ in C_1 and the state $\hat{\mathbf{v}}$ in C_2 form a conjugate pair.

Case 2: $C_1=[L\mathbf{u}_0+\mathbf{s}]$ with $(\mathbf{a}_1=T\mathbf{p}_0,\mathbf{b}_1=\mathbf{q})P$ as a state and $C_2\in\{[\mathbf{0}],[\mathbf{s}],[\mathbf{u}_k]\}$.
Subalgorithm 1 does not output any (i,i') on input $(\mathbf{p}_0,\mathbf{0},T^3\mathbf{p}_1,5)$. Thus, there is no conjugate pair between $[L\mathbf{u}_0+\mathbf{s}]$ and either $[\mathbf{0}]$ or $[\mathbf{s}]$.
Let $[\mathbf{u}_k]$ have $(\mathbf{a}_2=\mathbf{p}_k,\mathbf{b}_2=\mathbf{0})P$ as a state. On input $(\mathbf{q},\mathbf{0},T^9\mathbf{q},15)$, $(j,j')=(-6,0)=(9,0)$. Refer to Line 51 in Algorithm 1. Since $x_1=1$ and $x_2=x_3=x_4=0$, there exists a conjugate pair between $[L\mathbf{u}_0+\mathbf{s}]$ and $[\mathbf{u}_k]$ if and only if $i\equiv 0 \pmod 5$. From (22), this holds only if $k=2$, *i.e.*, $\mathbf{a}_2=\mathbf{p}_2$. Thus, only $[L\mathbf{u}_0+\mathbf{s}]$ and $[\mathbf{u}_2]$ share a conjugate pair with $\mathbf{v}=(T^i\mathbf{p}_0,T^j\mathbf{q})P=(\mathbf{p}_0,T^9\mathbf{q})P$.

Case 3: $C_1=[L\mathbf{u}_0+\mathbf{s}]$ with $\mathbf{v}_1=(T\mathbf{p}_0,\mathbf{q})P$ and $C_2=[L^\ell\mathbf{u}_k+\mathbf{s}]$ with $\mathbf{v}_2=(T^\ell\mathbf{p}_k,\mathbf{q})P$.
It is clear that $x_1=1$, $x_2=x_4=0$, and $x_3=\ell$. Since none of $\mathbf{a}_1,\mathbf{a}_2,\mathbf{b}_1$, and $\mathbf{b}_2$ is $\mathbf{0}$, refer to Line 56 in the algorithm. There exists a conjugate pair between $[L\mathbf{u}_0+\mathbf{s}]$ and $[L^\ell\mathbf{u}_k+\mathbf{s}]$ if and only if $i-1\equiv j \pmod 5$ and $i'+\ell\equiv j' \pmod 5$. Table 3 summarizes our computation with $j=9$ excluded from consideration. The state $\mathbf{v}$ in C_1 and the state $\hat{\mathbf{v}}$ in C_2 form a conjugate pair.

Table 3 Values obtained for Case 3

k	(i,i')	Requirement (mod 5)	(j,ℓ)	C_2	$\mathbf{v}$
0	$(1,1)$	$\ell\equiv-\tau_4(j-9)$	$(0,2)$	$[L^2\mathbf{u}_0+\mathbf{s}]$	$(T\mathbf{p}_0,\mathbf{q})P$
			$(5,3)$	$[L^3\mathbf{u}_0+\mathbf{s}]$	$(T\mathbf{p}_0,T^5\mathbf{q})P$
			$(10,1)$	$[L\mathbf{u}_0+\mathbf{s}]$	$(T\mathbf{p}_0,T^{10}\mathbf{q})P$
	$(4,4)$	$\ell\equiv 2-\tau_4(j-9)$	$(3,0)$	$[\mathbf{u}_0+\mathbf{s}]$	$(T^4\mathbf{p}_0,T^3\mathbf{q})P$
			$(8,4)$	$[L^4\mathbf{u}_0+\mathbf{s}]$	$(T^4\mathbf{p}_0,T^8\mathbf{q})P$
			$(13,1)$	$[L\mathbf{u}_0+\mathbf{s}]$	$(T^4\mathbf{p}_0,T^{13}\mathbf{q})P$
1	$(2,3)$	$\ell\equiv 3-\tau_4(j-9)$	$(1,4)$	$[L^4\mathbf{u}_1+\mathbf{s}]$	$(T^2\mathbf{p}_0,T\mathbf{q})P$
			$(6,2)$	$[L^2\mathbf{u}_1+\mathbf{s}]$	$(T^2\mathbf{p}_0,T^6\mathbf{q})P$
			$(11,0)$	$[\mathbf{u}_1+\mathbf{s}]$	$(T^2\mathbf{p}_0,T^{11}\mathbf{q})P$
	$(3,1)$	$\ell\equiv-\tau_4(j-9)$	$(2,3)$	$[L^3\mathbf{u}_1+\mathbf{s}]$	$(T^3\mathbf{p}_0,T^2\mathbf{q})P$
			$(7,4)$	$[L^4\mathbf{u}_1+\mathbf{s}]$	$(T^3\mathbf{p}_0,T^7\mathbf{q})P$
			$(12,1)$	$[L\mathbf{u}_1+\mathbf{s}]$	$(T^3\mathbf{p}_0,T^{12}\mathbf{q})P$
2	$(0,4)$	$\ell\equiv 2-\tau_4(j-9)$	$(4,2)$	$[L^2\mathbf{u}_2+\mathbf{s}]$	$(\mathbf{p}_0,T^4\mathbf{q})P$
			$(14,2)$	$[L^2\mathbf{u}_2+\mathbf{s}]$	$(\mathbf{p}_0,T^{14}\mathbf{q})P$

The rest of the cases can be analyzed in a similar manner. Once all possible cases have been examined, the completed adjacency matrix is given in (23).

The last step is to compute the cofactor of any of the matrix's entries. Our approach constructs $2,003,859,941,621,760,000 \approx 2^{60.797}$ de Bruijn sequences. Our approximation in (21) gives $({}^{2^8}\!/_{15})^{15} \approx 2^{61.397}$.

$$\mathscr{M}_1 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 5 & 0 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 5 & 0 & -1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\
0 & 0 & 0 & 5 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\
0 & 0 & -1 & 0 & 15 & 0 & 0 & 0 & 0 & 0 & -3 & -3 & -3 & -3 & -2 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 15 & -1 & -3 & 0 & -1 & 0 & -1 & -2 & -1 & -2 & -1 & 0 & 0 & -1 & -1 \\
0 & 0 & 0 & -1 & 0 & -1 & 13 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -2 & 0 & 0 & -2 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & -3 & -1 & 15 & -1 & 0 & -1 & -2 & -1 & 0 & -2 & -1 & -1 & 0 & 0 & -1 \\
0 & 0 & -1 & 0 & 0 & 0 & -1 & -1 & 13 & -2 & 0 & -1 & -1 & -3 & 0 & -1 & -1 & 0 & -1 & 0 \\
0 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & -2 & 13 & -3 & -1 & -1 & 0 & 0 & 0 & -1 & 0 & -1 & -1 \\
0 & -1 & 0 & 0 & -3 & 0 & -1 & -1 & 0 & -3 & 15 & 0 & 0 & 0 & 0 & -2 & -1 & -1 & -1 & -1 \\
0 & 0 & 0 & -1 & -3 & -1 & -1 & -2 & -1 & -1 & 0 & 15 & 0 & 0 & 0 & 0 & 0 & -1 & -3 & -1 \\
0 & 0 & 0 & -1 & -3 & -2 & -1 & -1 & -1 & -1 & 0 & 0 & 15 & 0 & 0 & -1 & -3 & -1 & 0 & 0 \\
0 & -1 & 0 & 0 & -3 & -1 & -1 & 0 & -3 & 0 & 0 & 0 & 0 & 15 & 0 & -1 & -1 & -1 & -1 & -2 \\
-1 & 0 & 0 & 0 & -2 & -2 & -2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 15 & -2 & 0 & -2 & 0 & -2 \\
0 & 0 & 0 & -1 & 0 & -1 & 0 & -1 & -1 & 0 & -2 & 0 & -1 & -1 & -2 & 15 & 0 & -1 & -1 & -3 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & 0 & -3 & -1 & 0 & 0 & 13 & -1 & -2 & -1 \\
0 & -1 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -2 & -1 & -1 & 13 & -1 & -1 \\
0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & -1 & -1 & -1 & -3 & 0 & -1 & 0 & -1 & -2 & -1 & 13 & 0 \\
0 & 0 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 & -1 & -1 & 0 & -2 & -2 & -3 & -1 & -1 & 0 & 15
\end{pmatrix}. \tag{23}$$

6 Some Special Cases

Theorem 2 makes clear that, for general irreducible polynomials $p(x)$ and $q(x)$, determining all conjugate pairs between any two cycles can be quite complicated. This section highlights three special cases for which the process is much simpler.

6.1 The orders of $p(x)$ and $q(x)$ are relatively prime

Based on Lemma 4, when $\gcd(e_1,e_2) = 1$,

$$\Omega(f(x)) = [\mathbf{0}] \cup \bigcup_{i=0}^{t_1-1} [\mathbf{u}_i] \cup \bigcup_{j=0}^{t_2-1} [\mathbf{s}_j] \cup \left(\bigcup_{i=0}^{t_1-1} \bigcup_{j=0}^{t_2-1} [\mathbf{u}_i + \mathbf{s}_j] \right). \tag{24}$$

Directly applying Propositions 1 to 5 leads to the next result.

Proposition 6 *Let $\mathbf{S} \in [\mathbf{u}_a + \mathbf{s}_b]$ for some a and b. The following properties hold.*

1. *$[\mathbf{0}]$ and $[\mathbf{u}_a + \mathbf{s}_b]$ are adjacent.*
2. *Let $0 \leq i < t_1$ and $0 \leq j < t_2$. There is no conjugate pair between $[\mathbf{u}_i]$ and $[\mathbf{u}_j]$ and between $[\mathbf{s}_i]$ and $[\mathbf{s}_j]$. There is a conjugate pair shared by $[\mathbf{u}_i]$ and $[\mathbf{s}_j]$ if and only if $i = a$ and $j = b$, in which case the pair is unique.*

3. *There is no conjugate pair between* $[\mathbf{u}_i]$ *and* $[\mathbf{u}_j+\mathbf{s}_k]$ *if* $k \neq b$. *For* $0 \leq i,j < t_1$, *the number of conjugate pairs between* $[\mathbf{u}_i]$ *and* $[\mathbf{u}_j+\mathbf{s}_b]$ *is the cyclotomic number* $(i-j,a-j)_{t_1}$.
4. *There is no conjugate pair between* $[\mathbf{s}_i]$ *and* $[\mathbf{u}_k+\mathbf{s}_j]$ *if* $k \neq a$. *For* $0 \leq i,j < t_2$, *the number of conjugate pairs between* $[\mathbf{s}_i]$ *and* $[\mathbf{u}_a+\mathbf{s}_j]$ *is the cyclotomic number* $(i-j,b-j)_{t_2}$.
5. *For* $0 \leq i_1,i_2 < t_1$ *and* $0 \leq j_1,j_2 < t_2$, *the number of conjugate pairs between two* **distinct** *cycles* $[\mathbf{u}_{i_1}+\mathbf{s}_{j_1}]$ *and* $[\mathbf{u}_{i_2}+\mathbf{s}_{j_2}]$ *is* $(i_2-i_1,a-i_1)_{t_1} \cdot (j_2-j_1,b-j_1)_{t_2}$.
6. *The number of conjugate pairs between* $[\mathbf{u}_i+\mathbf{s}_j]$ *and itself is* $\frac{1}{2}(0,a-i)_{t_1} \cdot (0,b-j)_{t_2}$.

6.2 Both $p(x)$ and $q(x)$ are primitive polynomials

Let $p(x)$ and $q(x)$ be distinct primitive polynomials. Then, $t_1 = t_2 = 1$ and $r := \gcd(e_1,e_2) = \gcd(2^m-1,2^n-1) = 2^{\gcd(m,n)}-1$. Consulting (7),

$$\Omega(f(x)) = [\mathbf{0}] \cup [\mathbf{u}] \cup [\mathbf{s}] \cup \bigcup_{i=0}^{r-1} [L^i\mathbf{u}+\mathbf{s}]. \tag{25}$$

Proposition 7 *Let a be such that* $\mathbf{S} \in [L^a\mathbf{u}+\mathbf{s}]$ *and* $r = \gcd(e_1,e_2) = 2^{\gcd(m,n)}-1$. *Then*

1. $[\mathbf{0}]$ *and* $[L^a\mathbf{u}+\mathbf{s}]$ *are adjacent.*
2. $[\mathbf{u}]$ *and* $[\mathbf{s}]$ *share a unique conjugate pair.*
3. *There are* $e_1/r-1$ *conjugate pairs between* $[\mathbf{u}]$ *and* $[L^a\mathbf{u}+\mathbf{s}]$ *and* e_1/r *conjugate pairs between* $[\mathbf{u}]$ *and* $[L^i\mathbf{u}+\mathbf{s}]$ *when* $0 \leq i < r$ *and* $i \neq a$.
4. *There are* $e_2/r-1$ *conjugate pairs between* $[\mathbf{s}]$ *and* $[L^a\mathbf{u}+\mathbf{s}]$ *and* e_2/r *conjugate pairs between* $[\mathbf{s}]$ *and* $[L^i\mathbf{u}+\mathbf{s}]$ *when* $0 \leq i < r$ *and* $i \neq a$.
5. *Let* $0 \leq i \neq j < r$. *The number of conjugate pairs between* $[L^i\mathbf{u}+\mathbf{s}]$ *and* $[L^j\mathbf{u}+\mathbf{s}]$ *is*

$$\begin{aligned} &N(i,j) = N(j,i) := |\{0 \leq k < \operatorname{lcm}(e_1,e_2)\}| \text{ where} \\ &\tau_n(k) \equiv \tau_m(k+i-j)+j-a \pmod{r},\ k \not\equiv 0 \pmod{e_1}, \text{ and } k \not\equiv j-i \pmod{e_2}. \end{aligned} \tag{26}$$

If $i=j$, *we halve the count in (26).*

Proof Since $\mathbf{S} \in [L^a\mathbf{u}+\mathbf{s}]$, $[\mathbf{0}]$ and $[L^a\mathbf{u}+\mathbf{s}]$ are adjacent. So are $[\mathbf{u}]$ and $[\mathbf{s}]$, which share a unique conjugate pair.

Consider $[\mathbf{u}]$ and $[L^i\mathbf{u}+\mathbf{s}]$ for $0 \leq i < r$. By Lemma 1, for $0 \leq k < e_1$,

$$L^k\mathbf{u}+L^i\mathbf{u}+\mathbf{s} = L^i(L^{k-i}\mathbf{u}+\mathbf{u})+\mathbf{s} = L^iL^{\tau_m(k-i)}\mathbf{u}+\mathbf{s} = L^{i+\tau_m(k-i)}\mathbf{u}+\mathbf{s}$$

is shift equivalent to $L^a\mathbf{u}+\mathbf{s}$ if and only if

$$i+\tau_m(k-i) \equiv a \pmod{r} \iff \tau_m(k-i) \equiv a-i \pmod{r}. \tag{27}$$

Since τ_m is a permutation, (27) has $e_1/r-1$ solutions when $i=a$ and e_1/r solutions when $i \neq a$.

Consider $[\mathbf{s}]$ and $[L^i\mathbf{u}+\mathbf{s}]$ for $0 \leq i < r$. For $0 \leq k < e_2$, Lemma 1 says that

$$L^k\mathbf{s}+L^i\mathbf{u}+\mathbf{s} = L^i\mathbf{u}+\mathbf{s}+L^k\mathbf{s} = L^i\mathbf{u}+L^{\tau_n(k)}\mathbf{s} = L^{\tau_n(k)}(L^{i-\tau_n(k)}\mathbf{u}+\mathbf{s})$$

is shift equivalent to $L^a\mathbf{u}+\mathbf{s}$ if and only if

$$i-\tau_n(k) \equiv a \pmod{r} \iff \tau_n(k) \equiv i-a \pmod{r}. \tag{28}$$

Thus, (28) has ${}^{e_2}\!/_{r}-1$ solutions for $i=a$ and ${}^{e_2}\!/_{r}$ solutions for $i\neq a$.

For the last assertion, we count the number of conjugate pairs between $[L^i\mathbf{u}+\mathbf{s}]$ and $[L^j\mathbf{u}+\mathbf{s}]$ for $0\leq i,j<r$. By Lemma 1, for $0\leq k<\operatorname{lcm}(e_1,e_2)$,

$$\begin{aligned}L^k(L^i\mathbf{u}+\mathbf{s})+L^j\mathbf{u}+\mathbf{s}&=L^{k+i}\mathbf{u}+L^j\mathbf{u}+L^k\mathbf{s}+\mathbf{s}=L^j(L^{k+i-j}\mathbf{u}+\mathbf{u})+L^{\tau_n(k)}\mathbf{s}\\&=L^{\tau_n(k)}(L^{j-\tau_n(k)}L^{\tau_m(k+i-j)}\mathbf{u}+\mathbf{s})=L^{\tau_n(k)}(L^{j-\tau_n(k)+\tau_m(k+i-j)}\mathbf{u}+\mathbf{s})\end{aligned}$$

is shift equivalent to $L^a\mathbf{u}+\mathbf{s}$ if and only if $j-\tau_n(k)+\tau_m(k+i-j)\equiv a \pmod{r}$. Equivalently, the condition can be written as

$$\tau_n(k)\equiv\tau_m(k+i-j)+j-a \pmod{r}. \tag{29}$$

Thus, if $i\neq j$, the number of conjugate pairs is indeed given by (26), and we halve the number when $i=j$. □

When $\gcd(e_1,e_2)=1$, Item 5 in Proposition 7 is a special case of [15, Theorem 2]. We present it here as a corollary.

Corollary 1 *Adding* $\gcd(e_1,e_2)=1$ *to the assumptions of Proposition 7, the number of conjugate pairs between* $[\mathbf{u}+\mathbf{s}]$ *and itself is*

$$ {}^{1}\!/_{2}\cdot|\{0\leq k<e_1e_2 \mid k\not\equiv 0 \pmod{e_1};\ k\not\equiv 0 \pmod{e_2}\}|={}^{1}\!/_{2}\cdot(e_1-1)(e_2-1). \tag{30}$$

If $e_1\mid e_2$, that is when $\gcd(e_1,e_2)=e_1$, we can derive an explicit formula.

Corollary 2 *If* $e_1\mid e_2$*, the number of conjugate pairs between* $[L^i\mathbf{u}+\mathbf{s}]$ *and* $[L^j\mathbf{u}+\mathbf{s}]$*, for* $0\leq i\neq j<e_1$*, is*

$$N(i,j)=\sum_{\substack{\ell=0\\ \ell\not\equiv j-i \pmod{e_1}}}^{e_1-1}(\ell,\tau_m(\ell+i-j)+j-a)_{e_1}. \tag{31}$$

If $i=j$*, we halve the count in (31).*

Proof Since $\gcd(e_1,e_2)=e_1$, rewrite (26) as

$$\begin{aligned}N(i,j)=|\{0<k<e_2\}|\ \text{satisfying}\ k\not\equiv j-i \pmod{e_1}\\ \text{and}\ \tau_n(k)\equiv\tau_m(k+i-j)+j-a \pmod{e_1}.\end{aligned} \tag{32}$$

More explicitly, we compute for

$$\sum_{\substack{\ell=0,\\ \ell\neq j-i}}^{e_1-1}|\{\ell+t\cdot e_1\}|\ \text{with}\ 0\leq t<\frac{e_2}{e_1}\ \text{and}\ \tau_n(\ell+t\cdot e_1)\equiv\tau_m(\ell+i-j)+j-a \pmod{e_1}. \tag{33}$$

Based on the equivalence of (2) and (3), we confirm that (33) and (31) are the same. □

6.3 De Bruijn Sequences of order $n+2$

Let $p(x)$ be a primitive polynomial of degree $n > 2$. We look into the construction from LFSRs with characteristic polynomial $(x^2+x+1)p(x)$. The exact number of de Bruijn sequences constructed can be determined.

It is clear that $\Omega(p(x)) = [\mathbf{0}] \cup [\mathbf{s}]$ and $\Omega(x^2+x+1) = [\mathbf{0}] \cup [\mathbf{u}]$, where $\mathbf{s}$ and $\mathbf{u}$ are maximal length sequences with period 2^n-1 and 3, respectively. In fact, $\mathbf{u}$ must be a shift of (110). By Lemma 4 and the fact that $\gcd(3, 2^n-1)$ is 1 if n is odd and is 3 if n is even,

$$\Omega(f(x)) = \begin{cases} [\mathbf{0}] \cup [\mathbf{u}] \cup [\mathbf{s}] \cup [\mathbf{u}+\mathbf{s}] & \text{if } n \text{ is odd,} \\ [\mathbf{0}] \cup [\mathbf{u}] \cup [\mathbf{s}] \cup \bigcup_{i=0}^{2} [L^i\mathbf{u}+\mathbf{s}] & \text{if } n \text{ is even.} \end{cases}$$

The next proposition follows from Proposition 7 and Corollary 1.

Proposition 8 *Let $n \geq 3$ be odd. Figure 1 shows the adjacency graph, based on the following facts.*

1. *There is a unique conjugate pair each between $[\mathbf{0}]$ and $[\mathbf{u}+\mathbf{s}]$ and between $[\mathbf{u}]$ and $[\mathbf{s}]$.*
2. *$[\mathbf{u}]$ and $[\mathbf{u}+\mathbf{s}]$ share 2 conjugate pairs.*
3. *$[\mathbf{s}]$ and $[\mathbf{u}+\mathbf{s}]$ share 2^n-2 conjugate pairs.*
4. *$[\mathbf{u}+\mathbf{s}]$ shares 2^n-2 conjugate pairs with itself.*

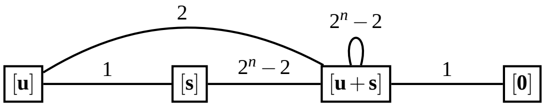


Fig. 1 The adjacency graph of $\Omega((x^2+x+1)\ p(x))$ for odd $n \geq 3$.

When n is even, we need some results on cyclotomic numbers.

Lemma 5 *(See [23] or [11, Section 4]) Let n be even. Then*

$$A := (0,0)_3 = \frac{1}{9} \cdot \left(2^n + (-2)^{\frac{n}{2}+1} - 8\right), C := (1,2)_3 = \frac{1}{9} \cdot \left(2^n + (-2)^{\frac{n}{2}+1} + 1\right), \textit{and}$$

$$B := (0,1)_3 = (1,1)_3 = (0,2)_3 = (2,2)_3 = \frac{1}{9} \cdot \left(2^n + (-2)^{\frac{n}{2}} - 2\right).$$

For $i > j$, we have $(i,j)_3 = (j,i)_3$.

The next result follows from Proposition 7 and Corollary 2.

Proposition 9 *Let $n \geq 4$ be even. Without loss of generality, suppose that $\mathbf{S} \in [\mathbf{u}+\mathbf{s}]$. Then*

1. *$[\mathbf{0}]$ and $[\mathbf{u}+\mathbf{s}]$ share a unique conjugate pair.*
2. *$[\mathbf{u}]$ shares a unique conjugate pair each with $[\mathbf{s}]$, $[L\mathbf{u}+\mathbf{s}]$ and $[L^2\mathbf{u}+\mathbf{s}]$.*
   There is no conjugate pair between $[\mathbf{u}]$ and $[\mathbf{u}+\mathbf{s}]$.
3. *$[\mathbf{s}]$ and $[\mathbf{u}+\mathbf{s}]$ share $\frac{2^n-1}{3}-1$ conjugate pairs.*
4. *For $\ell \in \{1,2\}$, $[\mathbf{s}]$ and $[L^\ell\mathbf{u}+\mathbf{s}]$ share $\frac{2^n-1}{3}$ conjugate pairs.*
5. *Let $N(i,j) = N(j,i)$, for $0 \leq i,j < 3$, be the number of conjugate pairs between $[L^i\mathbf{u}+\mathbf{s}]$ and $[L^j\mathbf{u}+\mathbf{s}]$. Based on Lemma 5, $N(0,0) = C$, $N(0,1) = 2B$, $N(0,2) = 2B$, $N(1,1) = B$, $N(1,2) = A+C$, and $N(2,2) = B$.*

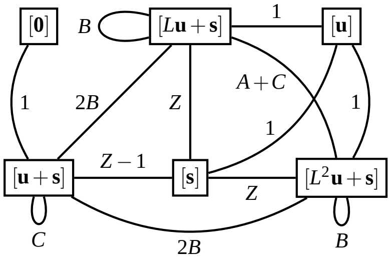


Fig. 2 The adjacency graph of $\Omega((x^2+x+1)\ p(x))$ for even $n \geq 4$.

The adjacency graph is shown in Figure 2 with $Z := \frac{2^n-1}{3}$.

Proof The first four items follow directly from Proposition 7. The last item is deduced from (31) using $\tau_2(1) = 2$ and $\tau_2(2) = 1$.

$$N(0,0) = \frac{1}{2}\sum_{\ell=1}^{3-1}(\ell, \tau_m(\ell+0-0)+0-0)_3 = \frac{1}{2}((1,2)_3+(2,1)_3) = (1,2)_3 = C,$$
$$N(0,1) = N(1,0) = (0,\tau_2(0-1)+1)_3+(2,\tau_2(2-1)+1)_3 = (0,2)_3+(2,0)_3 = 2B.$$

The other values can be obtained in a similar way. □

Theorem 4 *Let $\mathscr{A}_n$ be the set of all primitive polynomial of degree $n > 2$ over $\mathbb{F}_2$. Let $p(x) \in \mathscr{A}_n$. The total number of de Bruijn sequences constructed from LFSRs with characteristic polynomials $(x^2+x+1)\ p(x)$ is*

$$\begin{cases} (3\cdot 2^n - 4)\cdot \frac{\phi(2^n-1)}{n} & \textit{if } n \geq 3 \textit{ is odd} \\ \left[2^{3n} - \frac{9\cdot 2^{2n+4}-(-2)^{3n/2+4}-3\cdot 2^{n+6}+2^6}{27}\right] \frac{\phi(2^n-1)}{n} & \textit{if } n \geq 4 \textit{ is even.} \end{cases}.$$

Proof We count the number of spanning trees in the adjacency graph.

Let $n \geq 3$ be odd. Label the vertices $v_1 = [\mathbf{0}]$, $v_2 = [\mathbf{u}]$, $v_3 = [\mathbf{s}]$, and $v_4 = [\mathbf{u}+\mathbf{s}]$ to derive

$$\mathscr{M} = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 3 & -1 & -2 \\ 0 & -1 & 2^n-1 & 2-2^n \\ -1 & -2 & 2-2^n & 2^n+1 \end{pmatrix}$$

with cofactor $\mathscr{M}(3,3) = 3\cdot 2^n - 4$.

Let $n \geq 4$ be even. Label the vertices $v_1 = [\mathbf{0}]$, $v_2 = [\mathbf{u}]$, $v_3 = [\mathbf{s}]$, $v_4 = [\mathbf{u}+\mathbf{s}]$, $v_5 = [L\mathbf{u}+\mathbf{s}]$, and $v_6 = [L^2\mathbf{u}+\mathbf{s}]$ to derive

$$\mathscr{M}' = \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 3 & -1 & 0 & -1 & -1 \\ 0 & -1 & 2^n-1 & \frac{4-2^n}{3} & \frac{1-2^n}{3} & \frac{1-2^n}{3} \\ -1 & 0 & \frac{4-2^n}{3} & 4B+\frac{2^n-1}{3} & -2B & -2B \\ 0 & -1 & \frac{1-2^n}{3} & -2B & A+2B+C+\frac{2^n+2}{3} & -(A+C) \\ 0 & -1 & \frac{1-2^n}{3} & -2B & -(A+C) & A+2B+C+\frac{2^n+2}{3} \end{pmatrix}$$

with cofactor $\mathscr{M}'(5,5) = 2^{3n} - \frac{1}{27}\left(9 \cdot 2^{2n+4} - (-2)^{\frac{3n}{2}+4} - 3 \cdot 2^{n+6} + 2^6\right)$.

By [13, Theorem 5], applying the cycle joining method to two distinct LFSRs results in distinct de Bruijn sequences. Since there are $\phi(2^n-1)/n$ choices for the primitive polynomial $p(x)$ (see *e.g.* [10, page 70]), the desired conclusion follows. □

Table 4 provides the number for $3 \leq n \leq 10$ based on Theorem 4.

Table 4 Number of de Bruijn sequences of order $n+2$ in Theorem 4 for $3 \leq n \leq 10$.

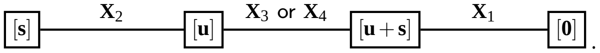
$\deg(p(x)) = n$	3	4	5	6	7	8	9	10
Order $= n+2$	5	6	7	8	9	10	11	12
# per $p(x)$	20	2,880	92	240,448	380	16,431,936	1,532	1,068,137,280
$\lvert\mathscr{A}_n\rvert$	2	2	6	6	18	16	48	60

Remark 3 One can also derive Theorem 4 by applying [16, Proposition 5] on relevant results in [15]. The latter reference uses $(1+x^3)p(x)$ as the characteristic polynomial. Hence, proper modifications are needed before the count can be established. In our present work, properties of cyclotomic numbers play a crucial role in establishing the count directly.

Example 2 Let $n = 3$ and $p(x) = x^3 + x + 1$, making $f(x) = x^5 + x^4 + 1$. This produces 20 distinct 32-periodic de Bruijn sequences.

$$\Omega(f(x)) = \{[\mathbf{0}], [\mathbf{u} = (110)], [\mathbf{s} = (0010111)], [\mathbf{u}+\mathbf{s} = (1111010\ 1001100\ 0100001)]\}.$$

Cycles $[\mathbf{0}]$ and $[\mathbf{u}+\mathbf{s}]$ share the pair $(\mathbf{X}_1 = (00000), \widehat{\mathbf{X}}_1)$. Cycles $[\mathbf{u}]$ and $[\mathbf{s}]$ are adjacent with a shared pair $(\mathbf{X}_2 = (11011), \widehat{\mathbf{X}}_2)$. Cycles $[\mathbf{u}]$ and $[\mathbf{u}+\mathbf{s}]$ share 2 conjugate pairs, namely $(\mathbf{X}_3 = (10110), \widehat{\mathbf{X}}_3)$ and $(\mathbf{X}_4 = (01101), \widehat{\mathbf{X}}_4)$. To derive one de Bruijn sequence, select the spanning tree



Applying the CJ method on $[\mathbf{0}]$ and $[\mathbf{u}+\mathbf{s}]$ using the conjugate pairs defined by $\mathbf{X}_1$ yields $(\ 1\underline{0000}\ \underline{0}1111101010011000)$; on $[\mathbf{u}]$ and $[\mathbf{s}]$ using $\mathbf{X}_2$ results in $(\ 11011\ 10\ 01011\ 0)$. We now choose $\mathbf{X}_3$ to combine the two larger cycles to get the de Bruijn sequence

$$(00000111110101\ 00110\ 11100\ 10110\ 001)$$

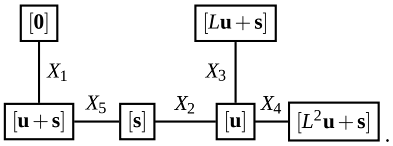
whose feedback function is $h(x_0, x_1, x_2, x_3, x_4) =$

$$x_0 + x_4 + (x_1+1)(x_2+1)(x_3+1)(x_4+1) + x_1(x_2+1)x_3x_4 + (x_1+1)x_2x_3(x_4+1) =$$
$$x_1x_2x_3x_4 + x_1x_2x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 + x_0 + x_1 + x_2 + x_3 + 1.$$

One can opt to use $\mathbf{X}_4$ instead of $\mathbf{X}_3$. The derivation is an easy exercise for the reader.

Example 3 Let $n = 4$ and $p(x) = x^4 + x + 1$. Hence, $f(x) = x^6 + x^5 + x^4 + x^3 + 1$, from which 2880 distinct de Bruijn sequences with period 64 can be constructed.

$$\Omega(f(x)) = \{[\mathbf{0}], [\mathbf{u} = (110)], [\mathbf{s} = (00010\ 01101\ 01111)], [\mathbf{u}+\mathbf{s} = (11001\ 00000\ 11001)],$$
$$[L\mathbf{u}+\mathbf{s} = (10100\ 10110\ 00010)], [L^2\mathbf{u}+\mathbf{s} = (01111\ 11011\ 10100)]\}.$$



Cycles $[\mathbf{0}]$ and $[\mathbf{u}+\mathbf{s}]$ share the pair $(\mathbf{X}_1=(000000),\widehat{\mathbf{X}}_1)$. Cycles $[\mathbf{u}]$ and $[\mathbf{s}]$ share the pair $(\mathbf{X}_2=(101101),\widehat{\mathbf{X}}_2)$. The pair $(\mathbf{X}_3=(110110),\widehat{\mathbf{X}}_3)$ is shared by $[\mathbf{u}]$ and $[L\mathbf{u}+\mathbf{s}]$. Cycles $[\mathbf{u}]$ and $[L^2\mathbf{u}+\mathbf{s}]$ share the pair $(\mathbf{X}_4=(011011),\widehat{\mathbf{X}}_4)$. Finally, the pair $(\mathbf{X}_5=(100110),\widehat{\mathbf{X}}_5)$ is between $[\mathbf{s}]$ and $[\mathbf{u}+\mathbf{s}]$. To construct one de Bruijn sequence, use the spanning tree

Table 5 lists down the joined cycles using the pairs defined by, in order, $\mathbf{X}_1$, $\mathbf{X}_5$, $\mathbf{X}_2$, $\mathbf{X}_4$, and $\mathbf{X}_3$. The one in the last row is de Bruijn with feedback function $h(x_0,x_1,x_2,x_3,x_4,x_5)=$

$$x_0+x_3+x_4+x_5+(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1)+(x_1+1)x_2x_3(x_4+1)x_5+\\ x_1(x_2+1)x_3x_4(x_5+1)+x_1x_2(x_3+1)x_4x_5+(x_1+1)(x_2+1)x_3x_4(x_5+1).$$

Table 5 Applying the cycle joining method on the spanning tree.

Link	Resulting Cycle
$\mathbf{X}_1$	(1 000 000 1 1001 1100)
$\mathbf{X}_5$	(1000 0001 10 10 1111 000 1 0011 0 011 100)
$\mathbf{X}_2$	(1000 0 001 101 1 0101 1110 0010 0110 0111 00)
$\mathbf{X}_4$	(1000 00 01 1011 1010 0011 1 111 011 0 1011 1100 0100 1100 1110 0)
$\mathbf{X}_3$	(1000 0001 1011 1010 0011 11 11 0110 0001 0101 0 010 110 1 0111 1000 1001 1001 1100)

7 More General Characteristic Polynomials

This section briefly touches upon the construction of de Bruijn sequences based on LFSRs with characteristic polynomials other than those discussed above.

When the characteristic polynomial takes a certain form, the adjacency graph contains no loops (see, *e.g.*, [15, Proposition 2]). The same holds for a much larger class of polynomials. Since $1+x^3=(1+x)(1+x+x^2)$, [15, Proposition 2] is subsumed by the next result.

Proposition 10 *Let $1+x,p_1(x),p_2(x),\ldots,p_s(x)\in\mathbb{F}_2[x]$ be pairwise distinct irreducible polynomials and $f(x)=(1+x)\ \prod_{i=1}^{s}p_i(x)$. The adjacency graph of $\Omega(f(x))$ contains no loops.*

Proof Let C be a cycle in $\Omega(f(x))$ that shares a conjugate pair with itself. Then the minimal polynomial of C must be $f(x)$. Hence, $C=[\mathbf{1}+L^{i_1}\mathbf{u}_1+\ldots+L^{i_{s-1}}\mathbf{u}_{s-1}+\mathbf{u}_s]$ for some integers $i_1,i_2,\ldots,i_{s-1}$ with $p_i(x)$ being the minimal polynomial of $\mathbf{u}_i$ for $1\leq i\leq s$. Thus, for some $\ell\in\mathbb{Z}$, we get $(\mathbf{1}+L^{i_1}\mathbf{u}_1+\cdots+L^{i_{s-1}}\mathbf{u}_{s-1}+\mathbf{u}_s)+L^{\ell}(\mathbf{1}+L^{i_1}\mathbf{u}_1+\cdots+L^{i_{s-1}}\mathbf{u}_{s-1}+\mathbf{u}_s)=L^{i'_1}\mathbf{u}'_1+\cdots+L^{i'_{s-1}}\mathbf{u}'_{s-1}+L^{i'_s}\mathbf{u}'_s$, where the characteristic polynomial of $\mathbf{u}'_i$ is $p_i(x)$. Now, the degree of the minimal polynomial of the resulting sequence must be $<\deg(f(x))$. Thus, it cannot contain $\mathbf{S}$. □

Consider the characteristic polynomial $h(x) = (1+x)f(x)$ with $f(x)$ given in Lemma 4. The only nonzero sequence having $1+x$ as its characteristic polynomial is $\mathbf{1}$. The cycle structure of $\Omega(h(x))$ follows directly from Lemmas 3 and 4.

Lemma 6 *The cycle structure of $\Omega(h(x))$ is*

$$[\mathbf{0}] \cup [\mathbf{1}] \cup \bigcup_{i=0}^{t_1-1} [\mathbf{u}_i] \cup \bigcup_{i=0}^{t_1-1} [\mathbf{1}+\mathbf{u}_i] \cup \bigcup_{j=0}^{t_2-1} [\mathbf{s}_j] \cup \bigcup_{j=0}^{t_2-1} [\mathbf{1}+\mathbf{s}_j] \cup$$
$$\left(\bigcup_{i=0}^{t_1-1} \bigcup_{j=0}^{t_2-1} \bigcup_{k=0}^{\gcd(e_1,e_2)-1} [L^k\mathbf{u}_i+\mathbf{s}_j] \right) \cup \left(\bigcup_{i=0}^{t_1-1} \bigcup_{j=0}^{t_2-1} \bigcup_{k=0}^{\gcd(e_1,e_2)-1} [\mathbf{1}+L^k\mathbf{u}_i+\mathbf{s}_j] \right).$$

Any cycle in $\Omega(h(x))$ can be described as $[a_0\mathbf{1}+a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j]$ with $i,j,k \in \mathbb{Z}$ and $a_0,a_1,a_2 \in \mathbb{F}_2$. Lemma 6 leads us directly to the next result.

Proposition 11 *If $[a_0\mathbf{1}+a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j]$ and $[a'_0\mathbf{1}+a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'}]$ share a conjugate pair, then $a_0+a'_0=1$ and, for $i \in \{1,2\}$, a_i and a'_i must never be simultaneously 0.*

Combining the main results in Section 4 with Propositions 10 and 11, the adjacency graph of $\Omega(h(x))$ can be constructed.

Proposition 12 *$\Omega(h(x))$ has the following properties.*

1. *The adjacency graph of $\Omega(h(x))$ contains no loops.*
2. *The number of conjugate pairs between $[a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j]$ and $[\mathbf{1}+a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'}]$ is equal to the number of conjugate pairs between $[\mathbf{1}+a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j]$ and $[a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'}]$.*
3. *Let $\mathbf{S} \in [\mathbf{1}+L^c\mathbf{u}_a+\mathbf{s}_b]$ for some $a,b,c \in \mathbb{Z}$. Then $[\mathbf{1}+a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j]$ and $[a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'}]$ share a conjugate pair if and only if $\mathbf{1}+a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j+L^\ell(a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'})$ is a shift of $\mathbf{1}+L^c\mathbf{u}_a+\mathbf{s}_b$ for some ℓ or, equivalently, $a_1L^k\mathbf{u}_i+a_2\mathbf{s}_j+L^\ell(a'_1L^{k'}\mathbf{u}_{i'}+a'_2\mathbf{s}_{j'})$ is a shift of $(0,\mathbf{1}) \in L^c\mathbf{u}_a+\mathbf{s}_b$ with $\mathbf{1}$ of length $m+n$.*
4. *The number of conjugate pairs between any two cycles in $\Omega(h(x))$ can be determined completely based on Propositions 1 to 5 and Algorithm 1 after small modifications.*

Propositions 1 to 5 form a good foundation to study and derive the adjacency graph for $\Omega(h(x))$. Since the required modifications mentioned in the last item of Proposition 12 are straightforward, the details are omitted here.

Once we have determined how the conjugate pairs are shared, we can perform steps analogous to those detailed in Section 4 to determine the states in a given cycle, to find conjugate pairs between any two cycles, and to estimate the number of de Bruijn sequences constructed. The non existence of loops in the adjacency graph is an advantage.

In particular, we can construct a $(1+m+n)\times(1+m+n)$ matrix P'. Any state belonging to the cycles in $\Omega(h(x))$ can then be described as $(\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3)P'$ with $\mathbf{v}_1 \in \mathbb{F}_2^1$, $\mathbf{v}_2 \in \mathbb{F}_2^m$, and $\mathbf{v}_3 \in \mathbb{F}_2^n$. Let $\mathbf{S} = (1,\mathbf{a}_3,\mathbf{b}_3)P'$ and let $(1,\mathbf{a}_1,\mathbf{b}_1)P'$ and $(0,\mathbf{a}_2,\mathbf{b}_2)P'$ be the respective states of cycles C_1 and C_2 in $\Omega(h(x))$. Run Algorithm 1 on $(\mathbf{a}_1,\mathbf{b}_1)$, $(\mathbf{a}_2,\mathbf{b}_2)$, and $(\mathbf{a}_3,\mathbf{b}_3)$. If Algorithm 1 yields a conjugate pair $(\mathbf{v},\hat{\mathbf{v}})$ with $\mathbf{v} = (\mathbf{a}',\mathbf{b}')P \in \mathbb{F}_2^{m+n}$, then $(\mathbf{v}' = (1,\mathbf{a}',\mathbf{b}')P',\hat{\mathbf{v}'})$ is the conjugate pair between C_1 and C_2.

To conclude this section, we show some advantages of our more general approach of using product of irreducible polynomials over that of [16] which is limited to using primitive polynomials.

Let $\mathscr{I}_2(n)$ and $\mathscr{P}_2(n)$ denote, respectively, the number of irreducible and primitive polynomials of degree n in $\mathbb{F}_2[x]$. We know that $\mathscr{P}_2(n) = |\mathscr{A}_n| = {}^{\phi(2^n-1)}/_{n}$. Let $\mu(n)$ be the Möbius function. From Gauss' general formula [17, Theorem 3.25]

$$\mathscr{I}_2(n) = \frac{1}{n}\sum_{d|n}\mu(d)2^{\frac{n}{d}}.$$

Let $N_n = \mathscr{I}_2(n) - \mathscr{P}_2(n)$. Consulting Sequences A001037 and A011260 in [19] that list down $\mathscr{I}_2(n)$ and $\mathscr{P}_2(n)$, respectively, one gets

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
N_n	1	0	3	0	14	8	39	10	191	0	405	382	2032	0	6756	0	28377	15186 .

$N_n = 0$ if and only if $2^n - 1$ is a (Mersenne) prime. As n grows larger, primes of the form $2^n - 1$ appear to grow increasingly sparse. Hence, for most n, our method draws polynomials from a larger pool of choices than the one used in [16].

Another advantage is that we get more de Bruijn sequences by using irreducible but non-primitive polynomial. The three irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$ are $f_1(x) = x^4+x+1$, $f_2(x) = x^4+x^3+1$, and $f_3(x) = x^4+x^3+x^2+x+1$. The first two are primitive while $f_3(x)$ is not.

Let $\Omega((1+x)f_1(x)) = \{[\mathbf{0}],[\mathbf{1}],[\mathbf{s}],[\mathbf{s}+\mathbf{1}]\}$. Then $[\mathbf{0}]$ and $[\mathbf{s}+\mathbf{1}]$ as well as $[\mathbf{1}]$ and $[\mathbf{s}]$ each share a unique conjugate pair. There are 14 conjugate pairs shared by $[\mathbf{s}]$ and $[\mathbf{s}+\mathbf{1}]$. The number of sequences constructed is only 14.

Consider $\Omega((1+x)f_3(x)) = \{[\mathbf{0}],[\mathbf{1}],[\mathbf{s}_0],[\mathbf{s}_1],[\mathbf{s}_2],[\mathbf{s}_0+\mathbf{1}],[\mathbf{s}_1+\mathbf{1}],[\mathbf{s}_2+\mathbf{1}]\}$. Lemma 5 helps us compute the number of conjugate pairs shared by any two cycles. The adjacency graph is shown in Figure 3. By Theorem 1, the number of de Bruijn sequences constructed is 576.

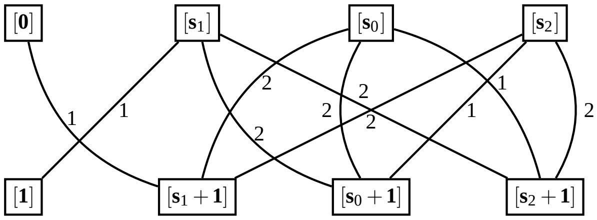


Fig. 3 The adjacency graph of $\Omega((1+x)(x^4+x^3+x^2+x+1))$.

8 Conclusion and Future Directions

This paper constructs new de Bruijn sequences by the cycle joining method using products of two distinct irreducible polynomials as characteristic polynomials. We present results on the cycle structure, provide the corresponding adjacency graph, and exhibit a connection between relevant cyclotomic numbers and the new de Bruijn sequences. Many of the results naturally extend to the case where $f(x) = p_1(x)\cdots p_s(x)$, where $p_i(x) \in \mathbb{F}_2[x]$ are pairwise distinct irreducible polynomials for $1 \leq i \leq s$.

Possible applications of de Bruijn sequences merit deeper investigation. The large number of de Bruijn sequences that can be efficiently constructed based on specific choices of polynomials may be beneficial for implementations in spread spectrum, more specifically in the design of control systems for autonomous vehicles. Crucial aspects to look at in this direction are the auto and cross correlation properties of the sequences as discussed in [22]. Various modifications of de Bruijn sequences have been known to result in powerful tools in DNA analysis [20] and DNA-based data storage systems [4].

Acknowledgements The work of Z. Chang is supported by the Joint Fund of the National Natural Science Foundation of China under Grant U1304604. Research Grants TL-9014101684-01 and MOE2013-T2-1-041 support the research carried out by M. F. Ezerman, S. Ling, and H. Wang. The collaboration leading to this paper was performed while Z. Chang was a visiting scholar at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University.

References

1. T. van Aardenne-Ehrenfest and N. G. de Bruijn. Circuits and trees in oriented linear graphs. *Simon Stevin*, vol. 28, pp. 203–217, 1951. Reprinted in *Classic Papers in Combinatorics*, eds.: I. Gessel and G-C. Rota, pp. 149–163. Boston: Birkhäuser, 1987.
2. N. G. de Bruijn. A combinatorial problem. *Proc. Kon. Ned. Akad. Wetensh.*, vol. 49, no. 7, pp. 758–764, Jun. 1946.
3. A. H. Chan, R. A. Games, and E. L. Key. On the complexities of de Bruijn sequences. *J. Combin. Theory Ser. A*, vol. 33, no. 3, pp. 233–246, Nov. 1982.
4. Z. Chang, J. Chrisnata, M. F. Ezerman, and H. M. Kiah. Rates of DNA sequence profiles for practical values of read lengths. *Preprint, available online ArXiv:1607.02279*.
5. C. Ding. *Codes from Difference Sets*. Singapore: World Scientific, 2014.
6. T. Etzion and A. Lempel. Algorithms for the generation of full-length shift-register sequences. *IEEE Trans. Inform. Theory*, vol. 30, no. 3, pp. 480–484, May 1984.
7. H. Fredricksen. A class of nonlinear de Bruijn cycles. *J. Combin. Theory Ser. A*, vol. 19, no. 2, pp. 192–199, Sep. 1975.
8. H. Fredricksen. A survey of full length nonlinear shift register cycle algorithms. *SIAM review*, vol. 24, no. 2, pp. 195–221, 1982.
9. S. W. Golomb. *Shift Register Sequences*. Laguna Hills: Aegean Park Press, 1981.
10. S. W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge: Cambridge Univ. Press, 2005.
11. E. R. Hauge and T. Helleseth. De Bruijn sequences, irreducible codes and cyclotomy. *Discrete Math.*, vol. 159, no. 1–3, pp. 143–154, Nov. 1996.
12. E. R. Hauge and J. Mykkeltveit. On the classification of de Bruijn sequences. *Discrete Math.*, vol. 148, no. 1–3, pp. 65–83, Jan. 1996.
13. C. J. A. Jansen, W. G. Franx, and D. E. Boekee. An efficient algorithm for the generation of de Bruijn cycles. *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1475–1478, Sep. 1991.
14. C. Li, X. Zeng, T. Helleseth, C. Li, and L. Hu. The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs. *IEEE Trans. Inform. Theory*, vol. 60, no. 5, pp. 3052–3061, May 2014.
15. C. Li, X. Zeng, C. Li, and T. Helleseth. A class of de Bruijn sequences. *IEEE Trans. Inform. Theory*, vol. 60, no. 12, pp. 7955–7969, Dec. 2014.
16. C. Li, X. Zeng, C. Li, T. Helleseth, and M. Li. Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomials. *IEEE Trans. Inform. Theory*, vol. 62, no. 1, pp. 610–624, Jan. 2016.
17. R. Lidl and H. Niederreiter. *Finite Fields*, Encyclopedia Math. Appl. vol. 20. Cambridge: Cambridge Univ. Press, 1997.
18. M. B. Nathanson. *Elementary Methods in Number Theory*. Grad. Texts in Math. vol. 195. New York: Springer-Verlag, 2000.
19. The On-Line Encyclopedia of Integer Sequences, published electronically at http://oeis.org.
20. P. A. Pevzner, H. Tang, and M. S. Waterman. An Eulerian path approach to DNA fragment assembly. *Proc. Natl. Acad. Sci. USA*, vol. 98, no. 17, pp. 9748–9753, Aug. 2001.
21. A. Ralston. De Bruijn sequences: A model example of the interaction of discrete mathematics and computer science. *Math. Mag.*, vol. 55, no. 3, pp. 131–143, May 1982.
22. S. Spinsante and E. Gambi. De Bruijn binary sequences and spread spectrum applications: A marriage possible?. *IEEE Aerosp. Electron. Syst. Mag.*, vol. 28, no. 11, pp. 28–39, Nov. 2013.
23. T. Storer. *Cyclotomic and Difference Sets* (Lectures in Mathematics). Chicago: Markham Publishing Company, 1967.