

Article

A New Approach to Determine the Minimal Polynomials of Binary Modified de Bruijn Sequences

Musthofa^{1,2}, Indah Emilia Wijayanti¹, Diah Junia Eksi Palupi¹ and Martianus Frederic Ezerman^{3,*}

¹ Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada, Sekip Utara BLS 21, Yogyakarta 55281, Indonesia; musthofa2019@mail.ugm.ac.id or musthofa@uny.ac.id (M.); ind_wijayanti@ugm.ac.id (I.E.W.); diah_yunia@ugm.ac.id (D.J.E.P.)

² Department of Mathematics Education, Universitas Negeri Yogyakarta, 1 Colombo Road, Yogyakarta 55281, Indonesia

³ School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore

* Correspondence: fredezerman@ntu.edu.sg

Abstract: A binary modified de Bruijn sequence is an infinite and periodic binary sequence derived by removing a zero from the longest run of zeros in a binary de Bruijn sequence. The minimal polynomial of the modified sequence is its unique least-degree characteristic polynomial. Leveraging a recent characterization, we devise a novel general approach to determine the minimal polynomial. We translate the characterization into a problem of identifying a Hamiltonian cycle in a specially constructed graph. The graph is isomorphic to the modified de Bruijn–Good graph. Along the way, we demonstrate the usefulness of some computational tools from the cycle joining method in the modified setup.

Keywords: binary sequence; Hamiltonian cycle; linear span; minimal polynomial; modified de Bruijn sequence

MSC: 11B50; 94A55; 94A60



Citation: Musthofa; Wijayanti, I.E.; Palupi, D.J.E.; Ezerman, M.F. A New Approach to Determine the Minimal Polynomials of Binary Modified de Bruijn Sequences. *Mathematics* **2022**, *10*, 2577. <https://doi.org/10.3390/math10152577>

Academic Editors: Jiyou Li, Antanas Cenys and Patrick Solé

Received: 25 June 2022

Accepted: 20 July 2022

Published: 25 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Given a positive integer n , a *binary de Bruijn sequence of order n* is an infinite sequence over $\mathbb{F}_2$ with period 2^n . Each binary n -tuple appears exactly once per period. Much has been found in the studies of such sequences. One can start from a primitive polynomial $p(x) \in \mathbb{F}_2[x]$ with $\deg(p(x)) = n$. The linear feedback shift register (LFSR) whose characteristic polynomial is $p(x)$ produces a maximum length sequence $\mathbf{m}$, also known as an m -sequence, of period $2^n - 1$. Appending a 0 to the longest run of zeroes in $\mathbf{m}$ results a de Bruijn sequence.

We know from [1], who independently rediscovered the result in [2], that the number of binary de Bruijn sequences of order n is $2^{2^{n-1}-n}$. The number of primitive polynomials over $\mathbb{F}_2$ is $n^{-1} \varphi(2^n - 1)$, where $\varphi(\cdot)$ is the Euler totient function. The number of de Bruijn sequences from the set of all primitive polynomials becomes minuscule compared to $2^{2^{n-1}-n}$ as n grows.

There are other methods than the route via m -sequences. Interested readers may want to consult Fredricksen's survey [3] and more recent works, such as the ones by Chang, Ezerman, Ling and Wang in [4], by Gabric, Sawada, Williams and Wong in [5] and in many of their respective references.

The sequence $\mathbf{m}$ produced by a primitive polynomial $p(x)$ can also be seen as a modification of the corresponding de Bruijn sequence by removing a 0 from the longest run of zeros. We call a sequence modified from any de Bruijn sequence, by such a removal of a 0, a *modified de Bruijn sequence*.

A sequence's measure of predictability is given by its *linear span* or *linear complexity*. This is defined to be the degree of the shortest linear recursion or minimal polynomial that produces the sequence. The higher the span is, the less predictable the sequence becomes. For cryptographic applications, for example, sequences with large spans are desirable.

The respective minimal and maximal values for the linear span of de Bruijn sequences are $2^{n-1} + n$ and $2^n - 1$, for $n \geq 3$. This fact and further results on the distribution of the linear span values can be found in [6]. The extremal values were initially established as bounds in [7], where the upper bound was then shown to be achievable. Etzion and Lempel showed how to construct de Bruijn sequences of minimal span in [8].

Let $\mathbf{s}$ denote a modified binary de Bruijn sequence of order n and period $2^n - 1$. Let $\tilde{\mathbf{s}}$ be its corresponding de Bruijn sequence. One often prefers using $\mathbf{s}$, instead of $\tilde{\mathbf{s}}$, since the presence of the all zero strings of length n can be undesirable. On the other hand, there are instances where $\tilde{\mathbf{s}}$ has an optimal linear complexity but $\mathbf{s}$ performs poorly in this measure.

Example 1. The sequence $\tilde{\mathbf{s}} := (0000100110101111)$ with $n = 4$ has linear complexity 15. The linear complexity of $\mathbf{s} = (000100110101111)$ drops significantly to 4.

Much less is known regarding the minimal polynomials of modified de Bruijn sequences. An early work on this topic was conducted by Mayhew and Golomb in [9]. Subsequent works by Kyureghyan in [10], by Tan, Xu and Qi in [11] and a more recent one by Wang, Zheng, Wang and Qi in [12] have not managed to supply any systematic method to determine the minimal polynomials.

For any $n \geq 4$, let Ω be the set of all nonzero polynomials of degree $< n$ —that is,

$$\Omega := \{0 \neq h(x) : h(x) \in \mathbb{F}_2[x] \text{ with } \deg(h(x)) < n\}. \quad (1)$$

In this work, we propose a general method to design the minimal polynomial of a modified de Bruijn sequence. To briefly outline our method, we defer the formal definition of terms related to polynomials to Section 2. We pick up from where the work by Tan et al. in [11] ends. In particular, we rely on the following useful characterization.

Theorem 1 ([11], Theorem 3.2). Let m and n be positive integers satisfying $m \geq n > 1$. A polynomial $f(x) \in \mathbb{F}_2[x]$ of degree m is the minimal polynomial of a modified de Bruijn sequence of order n if and only if the following conditions hold:

1. The polynomial $f(x)$ satisfies

$$f(0) = 1, \text{ and its period is } \text{per}(f(x)) = 2^n - 1. \quad (2)$$

2. Let $f^*(x)$ be the reciprocal polynomial of $f(x)$. There exist $g(x) \in \mathbb{F}_2[x]$ with $\deg(g(x)) = m - n$ such that

$$g(0) = 1, \quad (3)$$

$$\gcd(g(x), f^*(x)) = 1, \text{ and} \quad (4)$$

$$\Omega = \{(g(x) x^i \bmod f^*(x)) \bmod x^n : 0 \leq i < 2^n - 1\}. \quad (5)$$

Theorem 1 requires the two polynomials $f(x)$ and $g(x)$ to not only satisfy their respective conditions in (2) and (3) but also to simultaneously meet the requirements in (4) and (5) with Ω as defined in (1).

Our first step is to posit an auxiliary self-reciprocal polynomial

$$F(x) := \sum_{i=0}^{2^n-2} x^i = 1 + x + \dots + x^{2^n-3} + x^{2^n-2} \quad (6)$$

by taking the product of *all* elements in the set

$$\mathcal{A} := \bigcup_{\substack{\delta|n \\ \delta \neq 1}} \{\text{irreducible } r(x) \in \mathbb{F}_2[x] : \deg(r(x)) = \delta\}. \quad (7)$$

Since the product of all irreducible polynomials whose degrees divide n is $x^{2^n} + x$ and the only irreducible polynomials of degree 1 are x and $x + 1$, it is clear that

$$F(x) = \prod_{r(x) \in \mathcal{A}} r(x) = \frac{x^{2^n} + x}{x(x+1)}.$$

The next move is to transform the problem of finding a suitable $g(x)$ into a problem of determining a Hamiltonian cycle $\mathcal{H}$ in a specially constructed graph Γ_n . We give a systematic way to determine $g(x)$. The details are covered in Sections 3 and 4.

Our main contributions

1. For a given $n \geq 3$, we construct a graph Γ_n with the property that every Hamiltonian cycle $\mathcal{H}$ in Γ_n corresponds to a modified de Bruijn sequence. We then propose basic algorithms to identify numerous Hamiltonian cycles in Γ_n .
2. To each Hamiltonian cycle $\mathcal{H}$ in Γ_n , we associate a canonical generator polynomial $c_{\mathcal{H}}(x)$. Once $c_{\mathcal{H}}(x)$ is found, we compute $d(x) := \gcd(c_{\mathcal{H}}(x), F(x))$ and prove that the minimal polynomial $m_{\mathbf{s}}(x)$ of $\mathbf{s}$ is $f^*(x)$, where $f(x) := \frac{F(x)}{d(x)}$.
3. We supply basic computational tools as proofs of concept.

2. Preliminaries

Let $\mathbf{s} := s_0, s_1, \dots$ be an infinite sequence over a given finite field $\mathbb{F}_q$. If there is a positive integer N for which N is the smallest number such that $s_i = s_{i+N}$ for all $i \geq 0$, then $\mathbf{s}$ is an N -periodic sequence, and we write $\mathbf{s} = (s_0, s_1, \dots, s_{N-1})$. Such an N is the *period* $\text{per}(\mathbf{s})$ of $\mathbf{s}$. The sum of two infinite sequences $\mathbf{s} := s_0, s_1, \dots$ and $\mathbf{t} := t_0, t_1, \dots$ over the same finite field is $\mathbf{s} + \mathbf{t} = s_0 + t_0, s_1 + t_1, \dots$, and the scalar multiple $c\mathbf{s}$ with $c \in \mathbb{F}_q$ is simply $c s_0, c s_1, \dots$. Henceforth, unless otherwise stated, all sequences in this work are binary—that is, $q = 2$.

Let L be the (left) shift operator that sends

$$\mathbf{s} = (s_0, s_1, \dots, s_{N-1}) \mapsto L(\mathbf{s}) = (s_1, \dots, s_{N-1}, s_0). \quad (8)$$

By convention, L^0 fixes the sequence. Two sequences $\mathbf{a}$ and $\mathbf{b}$ are called *distinct* or (cyclically) *inequivalent* if one is not the cyclic shift of the other—that is, there is no integer $k \geq 0$ such that $\mathbf{a} = L^k \mathbf{b}$.

A monic polynomial $f(x)$ in the ring of binary polynomials $\mathbb{F}_2[x]$ of indeterminate x is a *characteristic polynomial* of $\mathbf{s} = (s_0, s_1, \dots, s_{N-1})$ if $f(L)(\mathbf{s}) = (0, 0, \dots, 0)$. One can then call $\mathbf{s}$ a *linear feedback shift register* (LFSR) sequence. As an LFSR sequence, $\mathbf{s}$ may have many characteristic polynomials. We identify the unique characteristic polynomial $m_{\mathbf{s}}(x)$ of least degree as its *minimal polynomial*. Any characteristic polynomial of $\mathbf{s}$ is divisible by $m_{\mathbf{s}}(x)$.

The minimal polynomial of a sequence gives the sequences *measure of predictability*. The degree $\Delta := \Delta_{\mathbf{s}} = \deg(m_{\mathbf{s}}(x))$ is the *linear complexity* or the *linear span* of $\mathbf{s}$. Knowing any Δ -tuple in $\mathbf{s}$ allows us to reconstruct $\mathbf{s}$ completely. The zero sequence has linear span 0.

The *reciprocal polynomial* of $a(x) := 1 + a_1 x + \dots + a_{n-1} x^{n-1} + x^n$ is the polynomial

$$a^*(x) := x^n a(x^{-1}) = 1 + a_{n-1} x + \dots + a_1 x^{n-1} + x^n. \quad (9)$$

A polynomial is *self-reciprocal* if it is its own reciprocal. The *order* of $a(x)$, denoted by $\text{ord}(a(x))$, is the least positive integer λ for which $a(x)$ divides $x^\lambda - 1$. The minimal polynomial of an N -periodic sequence has order N .

We will use the *rational fraction representation* of any $\mathbf{s} = (s_0, s_1, \dots, s_{N-1})$. Further details can be found in Chapter 6, Section 3 of [13]. The *generating function* of $\mathbf{s}$ is the element

$$s(x) := s_0 + s_1 x + \dots = \sum_{i=0}^{\infty} s_i x^i \quad (10)$$

in the *ring of formal power series* over $\mathbb{F}_2$. Since $\mathbf{s}$ is periodic, it can be represented as a rational function

$$s(x) = \sum_{i=0}^{\infty} s_i x^i = \frac{g(x)}{f(x)}, \quad (11)$$

with $f(x)$ and $g(x)$ in $\mathbb{F}_2[x]$ such that

$$\deg(g(x)) < \deg(f(x)), \quad \gcd(g(x), f(x)) = 1, \quad f(0) = 1. \quad (12)$$

The minimal polynomial $m_{\mathbf{s}}(x)$ of $\mathbf{s}$ is the reciprocal $f^*(x)$ of the denominator $f(x)$ in (11). The converse also holds. For any $f(x)$ and $g(x)$ in $\mathbb{F}_2[x]$ satisfying (12), there exists a periodic sequence $\mathbf{s}$ for which (11) holds.

The requirement that $\gcd(g(x), f(x)) = 1$ is not strictly necessary. Indeed, there will be occasions in the sequel that we relax this condition and allow for a rational function representation $s(x)$ with $\gcd(g(x), f(x)) = d(x) \neq 1$. The context will make it clear whether the representation is the simplest one or the more relaxed version.

Theorem 2 ([7], Section 2). *If $\mathbf{a}$ is binary de Bruijn sequence, then the minimal polynomial of $\mathbf{a}$ has the form $a(x) = (x+1)^z$ for some integer z satisfying $2^{n-1} + 1 \leq z \leq 2^n$.*

Let $\mathcal{I}(n)$ denote the number of binary irreducible polynomials of degree n in $\mathbb{F}_2[x]$. Let $\mu(n)$ be the Möbius function. Gauss' general formula in Theorem 3.25 of [13] says that $\mathcal{I}(n) = \frac{1}{n} \sum_{j|n} \mu(j) 2^{\frac{n}{j}}$. Sequence A001037 in [14] lists $\mathcal{I}(n)$.

Theorem 3 ([9], Theorem 2). *If $\tilde{\mathbf{s}}$ is a de Bruijn sequence of order $n \geq 4$ whose modified sequence is $\mathbf{s}$, then*

$$\Delta(\mathbf{s}) = \sum_{d|n} a_d \cdot d, \text{ with } 0 \leq a_d \leq \mathcal{I}(d). \quad (13)$$

Let $\mathbf{s}$ be a modified de Bruijn sequence of order n . For small values of n , it is known that $n \leq \Delta_{\mathbf{s}} \leq 2^n - 2$. It is conjectured in [11] that $\Delta_{\mathbf{s}} \notin \{n+1, n+2, \dots, 3n-1\}$. If $\mathbf{s}$ is not an m -sequence, then we know from Corollary 3 in [12] that $\Delta_{\mathbf{s}} > \frac{5}{4}n$.

We now recall useful results on the rational fraction representations of modified de Bruijn sequences over $\mathbb{F}_q$ established by Tan et al. in [11]. For any nonnegative integer k , the k -shifted sequence of $\mathbf{a} = (a_0, a_1, \dots, a_{N-1})$ is

$$L^k \mathbf{a} := (a_k, a_{k+1}, \dots, a_{N-1}, a_0, \dots, a_{k-1}). \quad (14)$$

The set of all shifted sequences of $\mathbf{a}$ is $\{L^k \mathbf{a} : 0 \leq k < N\}$.

Lemma 1 ([11], Lemma 3.5). *If $\mathbf{a} = (a_0, a_1, \dots, a_{N-1})$ is a given N -periodic sequence with rational fraction representation $\frac{g(x)}{f(x)}$, then, for any $0 \leq k < N$, the rational fraction representation of its k -shifted sequence $L^k \mathbf{a}$ is*

$$\frac{g_k(x)}{f(x)}, \text{ where } g_k(x) := (g(x) x^{N-k}) \bmod f(x). \quad (15)$$

Lemma 2 ([11], Lemma 3.6). If $\mathbf{a} = (a_0, a_1, \dots, a_{2^n-2})$ is a sequence of period $2^n - 1$ with $\frac{g(x)}{f(x)}$ as its rational fraction representation, then $\mathbf{a}$ is a modified de Bruijn sequence of order n if and only if

$$\Omega = \{(g(x)x^i \bmod f(x)) \bmod x^n : 0 \leq i < 2^n - 1\}.$$

Lemma 2 asserts that $\mathbf{a}$ is a modified de Bruijn sequence if and only if $g_k(x) \bmod x^n$ traverses all nonzero polynomials of degree less than n as k goes from 0 to $2^n - 2$. The preparation in Lemmas 1 and 2 leads to Theorem 1 in the introduction.

We use graph theoretic notions commonly defined in standard textbooks. A *directed graph* or a *digraph* is an ordered pair $G := (V, E)$, where V is a set of vertices and E is a set of ordered pairs called *directed edges* or *arcs*. In this work, a digraph does not have multiple arcs on the same ordered pair of vertices, although it may contain a loop. A *Hamiltonian path (cycle)* is a path (cycle) that visits every vertex exactly once, with each arc traced according to its direction. We will often use the terms Hamiltonian cycle and Hamiltonian path interchangeably, without causing ambiguity or losing generality.

3. From Polynomials to Directed Graphs

From the work of Mayhew and Golomb in [9] we know that the minimal polynomial of modified binary de Bruijn sequences of order n is a product of distinct irreducible polynomials of degree $d \neq 1$, with $d \mid n$. Setting aside the m -sequences built from primitive polynomials of degree n , there had not been any systematic way to determine the minimal polynomial of a given modified de Bruijn sequence.

Not all possible values given in (13) are the actual values of the linear span. For $n = 5$ —for instance, there is no modified binary de Bruijn sequence with minimal polynomial $f(x) = (x^5 + x^2 + 1)(x^5 + x^3 + 1)$, which is a product of two distinct irreducible polynomials of degree 5. Table 1 lists the degrees taken by the actual minimal polynomials for $n \in \{4, 5, 6\}$.

Table 1. The degrees of actual minimal polynomials of modified de Bruijn sequences of order $n \in \{4, 5, 6\}$, reproduced from [9].

n	Degrees of Actual Minimal Polynomials
4	4, 12, 14
5	5, 15, 20, 25, 30
6	6, 27, 30, 32, 33, 35, 36, 38, 39, 41, 42, 44, 45, 47, 48, 50, 51, 53, 54, 56, 57, 59, 60, 62

Example 2. For $n = 4$, there are exactly 10 modified de Bruijn sequences with the maximal linear span 14. Their minimal polynomial is $F(x) = 1 + x + x^3 + \dots + x^{14}$. Table 2 gives the 10 polynomials $g(x)$ that each satisfy the requirements in Theorem 1 with $F(x)$ taking the place of $f(x)$. Performing long division, we easily confirm that the first entry in Table 2 with $g(x) = x^{10} + x^8 + x^5 + x + 1$ has a representation

$$\frac{g(x)}{F(x)} = \left(1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10} + x^{11}\right) + x^{15} \left(\frac{g(x)}{F(x)}\right),$$

corresponding to the modified de Bruijn sequence $(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$. The rest of the entries can be similarly interpreted.

We define a digraph $\Gamma_n(V, E)$, or simply Γ , when n is clear from the context, based on the set Ω in (1) as follows. We associate each nonzero polynomial

$$a(x) = a_0 + a_1 x + \dots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1} \in \Omega$$

with the n -string

$$\mathbf{a} = a_{n-1}, a_{n-2}, \dots, a_1, a_0 \quad (16)$$

and its integer representation

$$A = a_{n-1} 2^{n-1} + a_{n-2} 2^{n-2} + \dots + a_1 2 + a_0. \quad (17)$$

Table 2. Degree 10 polynomials $g(x) = \sum_{j=0}^{10} g_j x^j$, written as $g_{10} g_9 \dots g_1 g_0$, that generate the set Ω in (1) and their corresponding sequences.

$g(x)$	Modified de Bruijn Sequence s	$g(x)$	Modified de Bruijn Sequence s
10100100011	(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)	11011000101	(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)
10011010111	(1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)	10100011011	(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)
11101011001	(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)	11010111011	(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)
10001101011	(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)	11011101011	(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)
11010110001	(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)	11000100101	(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)

Hence, there is a one-to-one correspondence between elements in Ω and the integers in $\{1, 2, \dots, 2^n - 1\}$, which we use as the vertex set V . Let $a(x), b(x) \in \Omega$ be seen as vertices $A, B \in V$. By Equations (5) and (6), we add an arc from A to B if and only if

$$b(x) = x a(x) \bmod x^n \text{ or} \quad (18)$$

$$b(x) = x a(x) \bmod x^n + \sum_{i=0}^{n-1} x^i. \quad (19)$$

The arc governed by (18) is from A to $B := 2A \bmod 2^n$, while the one defined by (19) is from A to $B := (2^n - 1) - (2A \bmod (2^n))$. We call the former the *doubling arc*, marked in blue and labeled by 0, and the latter the *double-then-complement arc*, marked in red and labeled by a 1. For brevity, the names are abbreviated to *double* and *complement* arcs.

The outdegree of each vertex is 2, except for the vertex 2^{n-1} whose outdegree is 1 since $0 \notin \Omega$. This vertex has only a red arc to its complement vertex $2^n - 1$. Each vertex has indegree 2, except for the vertex $2^n - 1$ whose only inbound edge comes from 2^{n-1} . There is a loop from vertex A to itself if and only if $3A \bmod 2^n = 2^n - 1$. This vertex is clearly unique. The graph Γ_n is simple for all n such that $3 \nmid (2^n - 1)$.

Example 3. The graph Γ_4 is in Figure 1 Top. The loop is from $A = 5$ to itself.

Let us briefly review the *de Bruijn graph* on 2^n vertices, denoted by B_n or simply B when n is understood. The graph, which is also known as the *Good graph* and the *de Bruijn–Good graph*, was introduced independently by N. de Bruijn in [1] and by I. J. Good in [15]. Its set of vertices consists of binary n -strings

$$\{v_1, v_2, \dots, v_n : v_j \in \mathbb{F}_2 \text{ for all } 1 \leq j \leq n\}.$$

Each vertex has indegree 2 and outdegree 2. The two arcs from vertex $c_1, c_2, \dots, c_n$ are to vertices $c_2, c_3, \dots, c_n, 0$ and $c_2, c_3, \dots, c_n, 1$. For our purposes, we relabel the vertices by integers from 0 to $2^n - 1$ by replacing $v_1, v_2, \dots, v_n$ with $v_1 + 2v_2 + \dots + 2^{n-1}v_n$.

We denote, by D_n , the graph obtained by deleting vertex 0 and its incident arcs in B_n . In D_n , there is an arc from vertex A to vertex B if and only if $B = 2A \bmod 2^n$ or $B = (2A + 1) \bmod 2^n$. Moreover, the only vertex with a loop is $2^n - 1$, and the only vertex with outdegree 1 is 2^{n-1} .

Theorem 4. For any positive integer n , the graphs D_n and Γ_n are isomorphic.

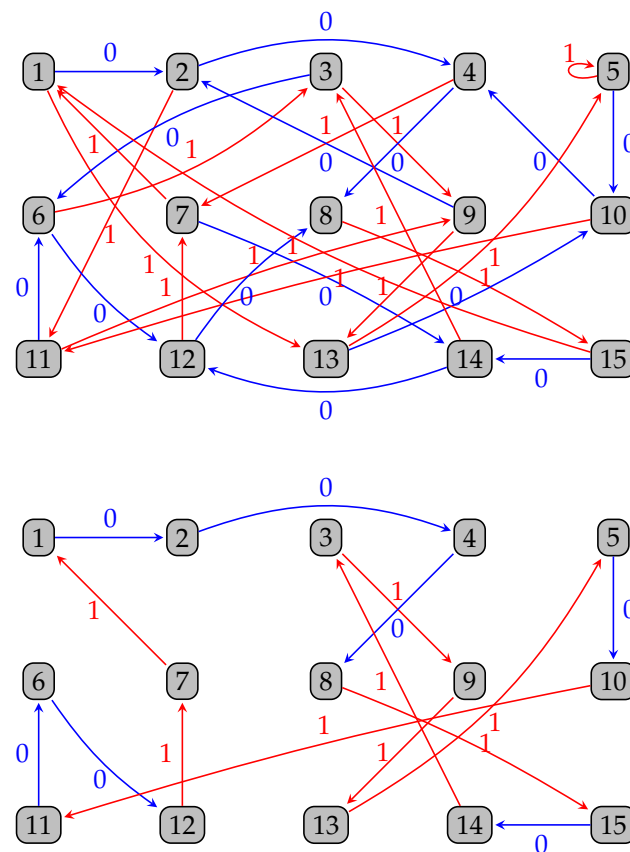


Figure 1. (Top): The graph Γ_4 with blue arcs based on (18) and red arcs based on (19). (Bottom): A Hamiltonian cycle $\mathcal{H}$ in Γ_4 .

Proof. Since all arithmetic operations are performed modulo 2^n , we omit $\text{mod } 2^n$ for brevity. It is clear that D_n and Γ_n have the same number of vertices and edges. To devise a recursive mapping $\sigma : D_n \mapsto \Gamma_n$, we start by sending vertex $2^n - 1$ in D_n to vertex $3^{-1}(2^n - 1)$ in Γ_n . In their respective graphs, the vertices are the only ones with a loop. Since $\gcd(3, 2^n) = 1$, the inverse of 3 always exists for all n . Now that we have $\sigma(2^n - 1) = 3^{-1}(2^n - 1)$, we assign, for $y = \sigma(x)$, the images

$$\sigma(2x) = 2y \text{ and } \sigma(2x + 1) = (2^n - 1) - 2y.$$

A vertex labeled by an even number in D_n is sent to an even-numbered vertex in Γ_n . Similarly, a vertex labeled by an odd number in D_n is mapped to an odd-numbered vertex in Γ_n . By definition, $\sigma(2^{n-1}) = 2^{n-1}$, which means that the unique vertex in D_n whose outdegree is 1 is sent to the unique vertex with outdegree 1 in Γ_n . Let A and B be vertices in D_n such that there is an arc from A to B . It is immediate to verify that there is an arc from $\sigma(A)$ to $\sigma(B)$.

We note that, since B_n is a Hamiltonian graph, then so is D_n . To show that σ is injective, let $\mathcal{H}$ be a Hamiltonian path that starts from vertex $2^n - 1$ in D_n . Let A and B be two distinct vertices in $\mathcal{H}$ such that $\sigma(A) = \sigma(B)$. If vertex C is the predecessor of B in $\mathcal{H}$, then there exists an arc from $\sigma(C)$ to $\sigma(B) = \sigma(A)$ in Γ_n . Hence, there must be an arc from C to A , contradicting the fact that $\mathcal{H}$ is a Hamiltonian path. Thus, $A = B$. $\square$

Example 4. For $n = 4$, we start with $\sigma(15) = 3^{-1} 15 = 5$. Proceeding recursively, we obtain

$$\begin{aligned} \sigma(14) &= 10, & \sigma(12) &= 4, & \sigma(13) &= 11, & \sigma(8) &= 8, & \sigma(9) &= 7, \\ \sigma(10) &= 6, & \sigma(11) &= 9, & \sigma(1) &= 15, & \sigma(2) &= 14, & \sigma(3) &= 1, \\ \sigma(4) &= 12, & \sigma(5) &= 3, & \sigma(6) &= 2, & \sigma(7) &= 13. \end{aligned}$$

Definition 1. Let $F(x) = \sum_{i=0}^{2^n-2} x^i$ be as in (6). The indexed set

$$W_g := \{(x^i g(x) \bmod F(x)) \bmod x^n : i \geq 0\}$$

forms a walk generated by $g(x)$ and we say that $g(x)$ generates the walk W_g .

Our task is to identify polynomials $g(x)$, with $g(0) = 1$ and $\gcd(g(x), F(x)) = d(x)$, that generate Hamiltonian cycles in Γ_n . Once such a $g(x)$ is found, Theorem 1 concludes that the reciprocal polynomial $f^*(x)$ of $f(x) := \frac{F(x)}{d(x)}$ is the minimal polynomial of a modified binary de Bruijn sequence.

4. Hamiltonian Cycles in Γ_n

Deciding whether a directed graph is Hamiltonian is difficult. A survey on this topic was performed by Kühn and Osthus in [16]. Further references and discussion can be found in Section 6.1 of [17]. Fortunately, Γ_n has many properties that allow us to explicitly determine some Hamiltonian cycles for all n .

4.1. Hamiltonian Cycles by Two Greedy Algorithms

Inspired by some greedy algorithms in the construction of certain classes of de Bruijn sequences discussed by Chang, Ezerman and Fahreza in [18], we devise two basic algorithms. Algorithm 1 prefers the complement over the double arcs when moving from the current vertex to the next vertex. Algorithm 2 swaps the preference with a modification imposed to avoid the inclusion of 0, since $0 \notin \Omega$.

Algorithm 1 Prefer Complement

Input: The order n of the sequences.

Output: Paths in Γ_n .

```

1: for  $i \in \{1, 2, \dots, 2^n - 1\}$  do
2:   Initiate the indexed set  $S = \{i\}$   $\triangleright v_{\text{init}} = i$ 
3:    $j \leftarrow$  element in  $S$  with largest index
4:    $d \leftarrow 2j \bmod 2^n$ 
5:    $c \leftarrow 2^n - 1 - d$ 
6:   while  $c \notin S$  or  $d \notin S$  do
7:     if  $c \notin S$  then
8:       Append  $c$  to  $S$ 
9:     else
10:      Append  $d$  to  $S$ 
11:   Path is  $(s_1, s_2), (s_2, s_3), \dots, (s_{\ell-1}, s_\ell)$ , where  $S := \{s_1 = i, s_2, \dots, s_{\ell-1}, s_\ell\}$ .
```

The two algorithms produce paths, starting from an initial vertex v_{init} . While each initial vertex produces a path, only several of them lead to Hamiltonian cycles. Table 3 lists the Hamiltonian cycles produced for $n \in \{4, 5, 6\}$.

For a given $n \geq 4$, Algorithm 1 yields $n - 1$ distinct—that is, cyclically-inequivalent—Hamiltonian cycles: $n - 2$ of them have two distinct initial vertices, whereas one cycle has three possible initial vertices. Let $1 \leq j < n$. Then, $v_{\text{init}} \in \{2^j - 1, 2^n - 2^{j-1}\}$ for each j . When $v_{\text{init}} = 2^{n-1}$, the generated cycle is the same as the one produced when $j = 1$ —that is, with $v_{\text{init}} \in \{1, 2^n - 1\}$. This is because the only arc from 2^{n-1} is to $2^n - 1$ and the complement of the double of $2^n - 1$ is $1 = (2^n - 1) - (2^n - 2)$. Algorithm 2 produces a unique Hamiltonian cycle. It occurs if and only if the initial vertex is either $\lfloor (2^n - 1)/3 \rfloor$ or its complement $(2^n - 1) - \lfloor (2^n - 1)/3 \rfloor$.

Algorithm 2 Modified Prefer Double**Input:** The order n of the sequences.**Output:** Paths in Γ_n .

```

1: for  $i \in \{1, 2, \dots, 2^n - 1\}$  do
2:   Initiate indexed set  $S = \{i\}$ 
3:    $j \leftarrow$  element in  $S$  with largest index
4:    $d \leftarrow 2j \bmod 2^n$ 
5:    $c \leftarrow 2^n - 1 - d$ 
6:   while  $c \notin S$  or  $d \notin S$  do
7:     if  $d = 0$  and  $c \notin S$  then
8:       Append  $c$  to  $S$ 
9:     else
10:      if  $d \notin S$  then
11:        Append  $d$  to  $S$ 
12:      else
13:        Append  $c$  to  $S$ 
14:   Path is  $(s_1, s_2), (s_2, s_3), \dots, (s_{\ell-1}, s_\ell)$ , where  $S := \{s_1 = i, s_2, \dots, s_{\ell-1}, s_\ell\}$ .

```

Table 3. Hamiltonian cycles constructed by Algorithms 1 and 2 for $n \in \{4, 5, 6\}$.

n	v_{init}	The Resulting Hamiltonian Cycle
Algorithm 1: Prefer Complement		
4	1, 15, 8	(1, 13, 5, 10, 11, 9, 2, 4, 7, 14, 3, 6, 12, 8, 15)
	3, 14	(3, 9, 13, 5, 10, 11, 6, 12, 7, 1, 2, 4, 8, 15, 14)
	7, 12	(7, 1, 13, 5, 10, 11, 9, 2, 4, 8, 15, 14, 3, 6, 12)
5	1, 31, 16	(1, 29, 5, 21, 10, 11, 9, 13, 26, 20, 23, 17, 2, 27, 22, 19, 25, 18, 4, 8, 15, 30, 3, 6, 12, 7, 14, 28, 24, 16, 31)
	3, 30	(3, 25, 13, 5, 21, 10, 11, 9, 18, 27, 22, 19, 6, 12, 7, 17, 29, 26, 20, 23, 14, 28, 24, 15, 1, 2, 4, 8, 16, 31, 30)
	7, 28	(7, 17, 29, 5, 21, 10, 11, 9, 13, 26, 20, 23, 14, 3, 25, 18, 27, 22, 19, 6, 12, 24, 15, 1, 2, 4, 8, 16, 31, 30, 28)
	15, 24	(15, 1, 29, 5, 21, 10, 11, 9, 13, 26, 20, 23, 17, 2, 27, 22, 19, 25, 18, 4, 8, 16, 31, 30, 3, 6, 12, 7, 14, 28, 24)
6	1, 63, 32	(1, 61, 5, 53, 21, 42, 43, 41, 45, 37, 10, 20, 23, 17, 29, 58, 11, 22, 19, 25, 13, 26, 52, 40, 47, 33, 2, 59, 9, 18, 27, 54, 44, 39, 49, 34, 4, 55, 46, 35, 57, 50, 36, 8, 16, 31, 62, 3, 6, 51, 38, 12, 24, 15, 30, 60, 7, 14, 28, 56, 48, 32, 63)
	3, 62	(3, 57, 13, 37, 53, 21, 42, 43, 41, 45, 26, 11, 22, 19, 25, 50, 27, 9, 18, 36, 55, 17, 29, 5, 10, 20, 23, 46, 35, 6, 51, 38, 12, 39, 49, 34, 59, 54, 44, 24, 15, 33, 61, 58, 52, 40, 47, 30, 60, 7, 14, 28, 56, 48, 31, 1, 2, 4, 8, 16, 32, 63, 62)
	7, 60	(7, 49, 29, 5, 53, 21, 42, 43, 41, 45, 37, 10, 20, 23, 17, 34, 59, 9, 18, 27, 54, 19, 25, 13, 26, 11, 22, 44, 39, 14, 35, 57, 50, 36, 55, 46, 28, 56, 15, 33, 61, 58, 52, 40, 47, 30, 3, 6, 51, 38, 12, 24, 48, 31, 1, 2, 4, 8, 16, 32, 63, 62, 60)
	15, 56	(15, 33, 61, 5, 53, 21, 42, 43, 41, 45, 37, 10, 20, 23, 17, 29, 58, 11, 22, 19, 25, 13, 26, 52, 40, 47, 30, 3, 57, 50, 27, 9, 18, 36, 55, 46, 35, 6, 51, 38, 12, 39, 49, 34, 59, 54, 44, 24, 48, 31, 1, 2, 4, 8, 16, 32, 63, 62, 60, 7, 14, 28, 56)
	31, 48	(31, 1, 61, 5, 53, 21, 42, 43, 41, 45, 37, 10, 20, 23, 17, 29, 58, 11, 22, 19, 25, 13, 26, 52, 40, 47, 33, 2, 59, 9, 18, 27, 54, 44, 39, 49, 34, 4, 55, 46, 35, 57, 50, 36, 8, 16, 32, 63, 62, 3, 6, 51, 38, 12, 24, 15, 30, 60, 7, 14, 28, 56, 48)
Algorithm 2: Modified Prefer Double		
4	5, 10	(5, 10, 4, 8, 15, 14, 12, 7, 1, 2, 11, 6, 3, 9, 13)
5	10, 21	(10, 20, 8, 16, 31, 30, 28, 24, 15, 1, 2, 4, 23, 14, 3, 6, 12, 7, 17, 29, 26, 11, 22, 19, 25, 18, 27, 9, 13, 5, 21)
6	21, 42	(21, 42, 20, 40, 16, 32, 63, 62, 60, 56, 48, 31, 1, 2, 4, 8, 47, 30, 3, 6, 12, 24, 15, 33, 61, 58, 52, 23, 46, 28, 7, 14, 35, 57, 50, 36, 55, 17, 34, 59, 54, 44, 39, 49, 29, 5, 10, 43, 22, 19, 38, 51, 25, 13, 26, 11, 41, 18, 27, 9, 45, 37, 53)

Example 5. For $n = 4$, Algorithm 1 yields the Hamiltonian cycle $\tilde{\mathcal{H}}$ in Figure 2 on $v_{\text{init}} = 1$. The path consists of arcs:

$$(1, 13), (13, 5), (5, 10), (10, 11), (11, 9), (9, 2), (2, 4), \\ (4, 7), (7, 14), (14, 3), (3, 6), (6, 12), (12, 8), (8, 15),$$

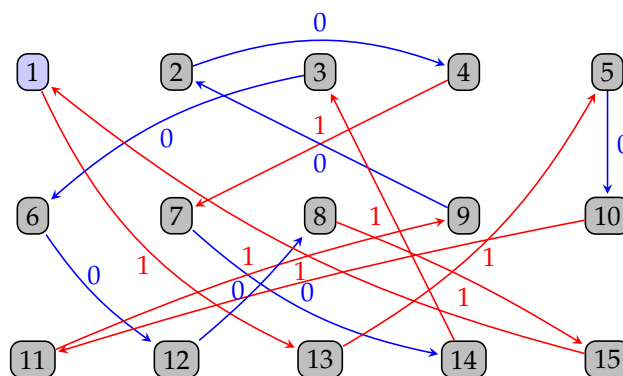


Figure 2. The Hamiltonian cycle $\tilde{\mathcal{H}}$ in Γ_4 produced by Algorithm 1 on $v_{\text{init}} = 1$. It is generated by $g(x) = x^{10} + x^8 + x^5 + x + 1$. The resulting sequence $(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$ has linear complexity 14, which is maximal.

For brevity, we will only prove, in Theorem 6, that Algorithm 1 on $v_{\text{init}} = 1$ always yields a Hamiltonian cycle. The respective proofs for the other valid initial vertices and on Algorithm 2 when using the two specified initial vertices follow a similar line of reasoning. To identify Hamiltonian cycles beyond those produced by the two algorithms, we establish a general result on the paths produced by Algorithm 1. The result will be used in the next subsection to identify many more Hamiltonian cycles in Γ_n by cycle joining.

Theorem 5. Let $V(\Gamma_n) = \{1, \dots, 2^n - 1\}$. Given an indexed set whose elements are vertices in Γ_n in the form of

$$\Theta := \{\alpha_1, \dots, \alpha_{2^n-1} : \alpha_i \in V \text{ and } \alpha_i \neq \alpha_j \text{ for } i \neq j\}, \quad (20)$$

let Ψ be a mapping on Θ defined by, for $1 \leq i < 2^n$,

$$\Psi : \alpha_i \mapsto \begin{cases} \beta_i = (2^n - 1) - (2\alpha_i \bmod 2^n), & \text{if } \alpha_i \text{ had not been mapped to } \beta_i, \\ 2\alpha_i \bmod 2^n, & \text{otherwise.} \end{cases} \quad (21)$$

Then, Ψ is a permutation on Θ .

Proof. We show that Ψ is a bijection on Θ . It is immediate to verify that there exist indices $1 \leq k \neq \ell < 2^n$ such that $\alpha_\ell = (\alpha_k + 2^{n-1}) \bmod 2^n$. If $k < \ell$, then

$$\Psi(\alpha_k) = (2^n - 1) - (2\alpha_k \bmod 2^n) \neq \Psi(\alpha_\ell) = 2\alpha_k \bmod 2^n. \quad (22)$$

If $\ell < k$, then

$$\Psi(\alpha_\ell) = (2^n - 1) - (2\alpha_k \bmod 2^n) \neq \Psi(\alpha_k) = 2\alpha_k \bmod 2^n. \quad (23)$$

Thus, Ψ is injective.

Let α be an arbitrarily selected element of Θ . If α is even, then there exists an integer $k \in \{1, 2, \dots, \frac{2^n-2}{2}\}$ such that $\alpha = 2k$. Hence, either $\Psi(k) = \alpha$ or $\Psi(k + 2^{n-1}) = \alpha$. If α is odd, then there exists an integer $t \in \{0, 1, 2, \dots, \frac{2^n-2}{2}\}$ such that $\alpha = 2t + 1$. Then, either

$\Psi\left(\frac{2^n-2t-2}{2}\right) = \alpha$ or $\Psi\left(\frac{2^n-2t-2}{2} + 2^{n-1}\right) = \alpha$. We conclude that Ψ is surjective, and the proof is now complete. $\square$

Since the function Ψ in (21) is a permutation on a finite set Θ , then Ψ can be written as a composition of j disjoint cycles

$$\Psi = C_1 \circ C_2 \circ \dots \circ C_j. \quad (24)$$

Definition 2. Let $(\alpha_{k,1}, \alpha_{k,2}, \dots, \alpha_{k,\ell})$ be a cycle C_k generated by Ψ . We say that C_k starts at $\alpha_{k,1}$ and ends at $\alpha_{k,\ell}$ since, by then, both possible images $\Psi(\alpha_{k,\ell})$, one of which being $\alpha_{k,1}$, have appeared. The elements $\alpha_{k,1}$ and $\alpha_{k,\ell}$ are, respectively, the starting element and the terminating element of C_k .

Lemma 3. Let the indexed set Θ and the function Ψ be as defined in Theorem 5. Let $\gamma \in \Theta$ be an even number that is not a starting element in any cycle. Then, the complement $2^n - 1 - \gamma$ of γ is an odd number that occurs before γ in the said cycle.

Proof. By how Ψ is defined and since $\gamma \in \Theta$ is not the starting element, it is impossible for γ to appear in the cycle before its complement, which is an odd number. $\square$

Lemma 4. Let $\beta \in \{1, 2, \dots, 2^{n-1} - 1\}$, and then $\{\Psi(\beta), \Psi(\beta + 2^{n-1})\} = \{2^n - 1 - 2\beta, 2\beta\}$. By the time both $2^n - 1 - 2\beta$ and 2β appear in a cycle C , we know that both β and $\beta + 2^{n-1}$ must have appeared earlier.

Proof. Since Ψ is bijective, the appearance of both $2^n - 1 - 2\beta$ and 2β requires the prior inclusion of both possible predecessors in the cycle. $\square$

The conclusion that Γ_n is Hamiltonian for all $n \geq 4$ follows from the next theorem.

Theorem 6. Let the set Θ and function Ψ be as defined in Theorem 5. The function Ψ produces a single cycle of length $2^n - 1$ that starts at 1 and ends at $2^n - 1$.

Proof. Let C be the cycle

$$(1, \Psi(1), \Psi(\Psi(1)), \dots, \delta, \alpha). \quad (25)$$

Consider the shift-equivalent cycle $(\Psi(\delta) = \alpha, \Psi(\alpha) = 1, \Psi(1), \dots, \delta)$. Since $\Psi(\alpha) = 1$, α must be either $2^{n-1} - 1$ or $2^n - 1$.

For a contradiction, let us assume that $\alpha = 2^{n-1} - 1$. Since 1 has already appeared in C , the only other possible successor of $2^{n-1} - 1$ —namely, $2^n - 2$ —must have appeared in C . The two possible predecessors of $2^n - 2$ are $2^{n-1} - 1$ and $2^n - 1$. Hence, C must have the form

$$C = (1, \dots, 2^n - 1, 2^n - 2, \dots, 2^{n-1} - 1). \quad (26)$$

On the other hand, since $2^{n-1} - 1$ is both an odd number and the terminating element, then its complement—namely, 2^{n-1} —must not have appeared in C . However, this rules out $2^n - 1$ from C as well, contradicting (26). Thus, the terminating element must be $\alpha = 2^n - 1$.

We now show that all elements of Θ appear in C . The computations are performed modulo 2^n . It is clear that $\delta = 2^{n-1}$, since it is the only preimage of $2^n - 1$. Hence, we have

$$C = (1, \Psi(1), \dots, 2^{n-1}, 2^n - 1). \quad (27)$$

Aided by Lemmas 3 and 4, we proceed by induction to confirm that each even number $2 \leq k \leq 2^n - 2$ appears.

- Since $\delta = 2^{n-1}$ is an even number, Lemma 3 says that its complement $\delta^* := 2^n - 2^{n-1} - 1 = 2^{n-1} - 1$ appears. By Lemma 4, both 2^{n-2} and $2^{n-1} + 2^{n-2}$ must have appeared before both δ and δ^* do.

- Since 2^{n-2} is even, by Lemma 3, its complement appears. We infer by Lemma 4 that 2^{n-3} and $2^{n-1} + 2^{n-3}$ appear.
- We repeat the same reasoning on $2^{n-1} + 2^{n-2}$. Its complement appears, and so do both $2^{n-2} + 2^{n-3}$ and $2^{n-1} + 2^{n-2} + 2^{n-3}$.
- Continuing the process, we establish the appearance of

$$\begin{aligned} &2, 2^2, \dots, 2^{n-1}, \\ &2 + 2^{n-1}, 2^2 + 2^{n-1}, \dots, 2^{n-2} + 2^{n-1}, \\ &2 + 2^{n-2} + 2^{n-1}, 2^2 + 2^{n-2} + 2^{n-1}, \dots, 2^{n-3} + 2^{n-2} + 2^{n-1}, \\ &\dots, \dots, \dots, \dots, \\ &2 + 2^2 + \dots + 2^{n-2} + 2^{n-1}, \end{aligned} \quad (28)$$

which covers all even numbers in the desired range.

Lemma 3 ensures the appearance of each odd number j such that $3 \leq j \leq (2^n - 3)$, completing the proof. $\square$

Corollary 1. The graph Γ_n for each $n \geq 4$ is Hamiltonian.

Proof. We built $\mathcal{C} = (1, \Psi(1), \Psi(\Psi(1)), \dots, 2^{n-1}, 2^n - 1)$ in the proof of Theorem 6. Following the sequence of vertices in $\mathcal{C}$, a Hamiltonian path in Γ_n is formed by the edges

$$(1, \Psi(1)), (\Psi(1), \Psi(\Psi(1))), \dots, (2^{n-1}, 2^n - 1).$$

$\square$

4.2. More Hamiltonian Cycles by Cycle Joining

Theorem 6 guarantees that, starting from $v_{\text{init}} = 1$, Algorithm 1 produces a cycle of length $2^n - 1$. However, for most other v_{init} , we obtain disjoint cycles as in (24) with $j > 1$. The following lemma gives a condition for when two disjoint cycles can be joined into a longer cycle.

Lemma 5. Two disjoint cycles $\mathcal{C}$ and $\hat{\mathcal{C}}$ can be joined into one cycle if there exist $c \in \mathcal{C}$ and $d \in \hat{\mathcal{C}}$ such that d is the complement of c —that is, $d = 2^n - 1 - c$.

Proof. Let $\mathcal{C} = (c_1, \dots, c_{i-1}, c_i, c_{i+1}, \dots, c_k)$ and $\hat{\mathcal{C}} = (d_1, \dots, d_{j-1}, d_j, d_{j+1}, \dots, d_\ell)$, with c_i and d_j forming a complementary pair—that is, $c_i + d_j = 2^n - 1$. We exchange the predecessors of c_i and d_j to obtain the joined cycle

$$(c_1, \dots, c_{i-1}, d_j, d_{j+1}, \dots, d_\ell, d_1, \dots, d_{j-1}, c_i, c_{i+1}, \dots, c_k).$$

$\square$

Theorem 7. If Ψ generates disjoint cycles as in (24), then all of the cycles can be joined into a single cycle of length $2^n - 1$.

Proof. If Ψ generates only one cycle, then it is clear that the length of the cycle must be $2^n - 1$. Suppose that Ψ generates at least two cycles, and we take any cycle $\mathcal{C}$. It suffices to show that there exists $c \in \mathcal{C}$ whose complement $\hat{c} := 2^n - 1 - c$ does not appear in $\mathcal{C}$. For a contradiction, let there be no such element. Hence, every element in $\mathcal{C}$ has its complement in $\mathcal{C}$ —that is, $\hat{c} \in \mathcal{C}$ for any $c \in \mathcal{C}$. By definition, exactly one of either c or $\hat{c}$ is an even number e . Therefore, the predecessors of c and $\hat{c}$, namely, $k := \frac{e}{2}$ and $2^{n-1} + k$ also appear in $\mathcal{C}$. Following this fact, all integers in $\{1, 2, \dots, 2^n - 1\}$ appear in $\mathcal{C}$. This contradicts the assumption that Ψ generates two or more cycles. $\square$

We can implement Theorem 7 and enumerate the number of resulting Hamiltonian cycles that can be constructed by adopting the *cycle joining method* from the theory of feedback shift registers.

Let Ψ be expressed in terms of its disjoint cycles as in (24). For distinct $1 \leq i \neq k \leq j$, let $\tau_{i,k} := (r, s)$ denote $r \in C_i$ and $s \in C_k$ with $r + s = 2^n - 1$. The tuple joins C_i and C_k by interchanging the respective predecessors of r and s .

To count the number of inequivalent Hamiltonian cycles that can be produced from Ψ , we build the associated undirected multigraph G_Ψ as follows. The vertices are $C_1, \dots, C_j$. We add an edge labeled (r, s) between C_i and C_k whenever there is a pair (r, s) with the property that $r \in C_i$, $s \in C_k$ and $r + s = 2^n - 1$. The graph G_Ψ has no loops but may have multiple edges connecting the same pair of vertices. The number of Hamiltonian cycles that can be constructed in this manner is equal to the number of subgraphs of G_Ψ that are rooted spanning trees.

The following well-known counting formula is a variant of the BEST (de Bruijn, Ehrenfest, Smith and Tutte) Theorem. Further details on graphical approaches to the generation of full cycles, including the BEST Theorem and its history, can be found in Section 2 of [3]. The cofactor of entry $m_{i,k}$ in a matrix $M := (m_{i,k})$ is $(-1)^{i+k}$ times the determinant of the matrix obtained by deleting the i th row and k th column of M .

Theorem 8. (BEST) Let $V := \{C_1, \dots, C_j\}$ be the vertex set of G_Ψ . Let $M = (m_{i,k})$ be the $j \times j$ matrix derived from G_Ψ in which $m_{i,i}$ is the number of edges incident to C_i , and $m_{i,k}$ is the negative of the number of edges between vertices C_i and C_k for $i \neq k$. Then, the number of rooted spanning trees of G_Ψ is the cofactor of any entry of M .

Example 6. A randomized instance for $n = 4$ chooses

$$\Psi = (6, 3, 9, 13, 5, 10, 11) \circ (4, 7, 1, 2) \circ (14, 12, 8, 15).$$

We label the cycles from left to right as C_1 , C_2 and C_3 to obtain the associated graph G_Ψ in Figure 3.

The associated matrix is

$$M := \begin{bmatrix} 3 & -2 & -1 \\ -2 & 4 & -2 \\ -1 & -2 & 3 \end{bmatrix}.$$

By the BEST Theorem, there are eight Hamiltonian cycles that can be constructed from Ψ . Table 4 lists them. All but one of the sequences have maximal linear complexity 14.

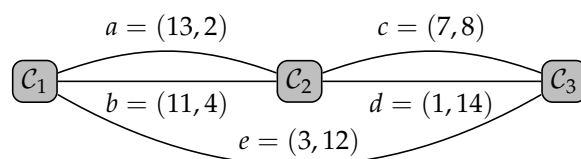


Figure 3. The associated graph G_Ψ for Example 6.

Table 4. The eight Hamiltonian cycles produced from Ψ by cycle joining in Example 6. For $n = 4$, we have $F(x) = 1 + x + x^2 + \dots + x^{14}$. The edges a, b, c, d and e are specified in Figure 3.

Joining	Hamiltonian Cycle	Modified de Bruijn Sequence s	$m_s(x)$
a, c	(6, 3, 9, 2, 4, 8, 15, 14, 12, 7, 1, 13, 5, 10, 11)	(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)	$F(x)$
a, d	(6, 12, 8, 15, 14, 3, 9, 2, 4, 7, 1, 13, 5, 10, 11)	(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)	$F(x)$
b, c	(6, 3, 9, 13, 5, 10, 4, 8, 15, 14, 12, 7, 1, 2, 11)	(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)	$x^4 + x + 1$
b, d	(6, 3, 9, 13, 5, 10, 4, 7, 14, 12, 8, 15, 1, 2, 11)	(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)	$F(x)$
e, a	(6, 12, 8, 15, 14, 3, 9, 2, 4, 7, 1, 13, 5, 10, 11)	(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)	$F(x)$
e, b	(6, 12, 8, 15, 14, 3, 9, 13, 5, 10, 4, 7, 1, 2, 11)	(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)	$F(x)$
e, c	(6, 12, 7, 1, 2, 4, 8, 15, 14, 3, 9, 13, 5, 10, 11)	(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)	$F(x)$
e, d	(6, 12, 8, 15, 1, 2, 4, 7, 14, 3, 9, 13, 5, 10, 11)	(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)	$F(x)$

5. The Canonical Generator Polynomial

In this section, we show that there exists a canonical generator $c_{\mathcal{H}}(x) \in \mathbb{F}_2[x]$ for every Hamiltonian cycle $\mathcal{H} \in \Gamma_n$.

Corollary 2. *If $\mathcal{H}$ is a Hamiltonian cycle in Γ_n , then there exists a polynomial $g(x) \in \mathbb{F}_2[x]$ that generates $\mathcal{H}$. The consecutive elements in*

$$W_g = \{(x^i g(x) \bmod F(x)) \bmod x^n : 0 \leq i < 2^n - 1\}$$

form the Hamiltonian path in $\mathcal{H}$.

Proof. Since $\mathcal{H}$ is a Hamiltonian cycle in Γ_n , and Γ_n is isomorphic to B_n by Theorem 4, then $\mathcal{H}$ corresponds to a modified binary de Bruijn sequence $\mathbf{s}$, which can be represented as $\frac{g(x)}{F(x)}$, with $\deg(g(x)) < 2^n - 2$. Lemma 2 ensures the existence of the required $g(x)$ and, by Definition 1, $g(x)$ generates $\mathcal{H}$. $\square$

We recall Lemma 1 before establishing our next result. If $\mathbf{s}$ is a modified binary de Bruijn sequence whose rational fraction representation is $\frac{g(x)}{F(x)}$, for some $g(x) \in \mathbb{F}_2[x]$, then, for any $0 \leq k < 2^n - 1$, the rational fraction representation of the k -shifted sequence $L^k \mathbf{s}$ in Equation (15) is $\frac{g_k(x)}{F(x)}$ where $g_k(x) = g(x) x^{2^n-1-k} \bmod F(x)$. Two polynomials $g(x)$ and $h(x)$ may generate the same Hamiltonian cycle $\mathcal{H}$ in Γ_n . The following lemma explains how to relate the polynomials to one another.

Lemma 6. *Let $n \geq 4$ be given, and let $F(x) := \sum_{i=0}^{2^n-2} x^i = 1 + x + x^2 + \dots + x^{2^n-2}$. Two polynomials $g(x)$ and $h(x)$ in $\mathbb{F}_2[x]$ generate the same Hamiltonian cycle $\mathcal{H}$ in Γ_n if and only if*

$$h(x) = x^k g(x) \bmod F(x) \text{ for some } 0 \leq k < 2^n - 1. \quad (29)$$

Proof. To verify that $x^{2^n-1} g(x) \bmod F(x) = g(x)$, it suffices to use the fact that $F(x)$ divides $x^{2^n-1} + 1$, which implies $x^{2^n-1} \bmod F(x) = 1$.

Let $a(x)$ be any element of Ω . If $g(x)$ and $h(x)$ generate the same Hamiltonian cycle $\mathcal{H}$, then there exist i and j , where $0 \leq i, j < 2^n - 1$, such that

$$a(x) = (x^i g(x) \bmod F(x)) \bmod x^n = (x^j h(x) \bmod F(x)) \bmod x^n. \quad (30)$$

If $i \geq j$, then letting $k := i - j$ yields

$$(x^k g(x) \bmod F(x)) \bmod x^n = h(x). \quad (31)$$

If $i < j$, then multiplying both sides of (31) by x^{2^n-1} gives us

$$(x^{2^n-1+k} g(x) \bmod F(x)) \bmod x^n = x^{2^n-1} h(x). \quad (32)$$

Since $x^{2^n-1} h(x) \bmod F(x) = h(x)$, we conclude that

$$h(x) = (x^k g(x) \bmod F(x)) \bmod x^n.$$

Conversely, let $h(x) = x^k g(x) \bmod F(x)$ for some k with $0 \leq k < 2^n - 1$. We take two vertices A and B in Γ_n that correspond, respectively, to

$$\begin{aligned}a(x) &= \left(x^i h(x) \bmod F(x)\right) \bmod x^n \text{ and} \\b(x) &= \left(x^{i+1} h(x) \bmod F(x)\right) \bmod x^n\end{aligned}$$

for some $0 \leq i < 2^n - 1$. Then,

$$\begin{aligned}a(x) &= \left(x^i x^k g(x) \bmod F(x)\right) \bmod x^n \text{ and} \\b(x) &= \left(x^{i+1} x^k g(x) \bmod F(x)\right) \bmod x^n.\end{aligned}\quad (33)$$

Using $j := (i + k) \bmod 2^n - 2$, one writes

$$\begin{aligned}a(x) &= \left(x^j g(x) \bmod F(x)\right) \bmod x^n \text{ and} \\b(x) &= \left(x^{j+1} g(x) \bmod F(x)\right) \bmod x^n.\end{aligned}\quad (34)$$

Thus, both $g(x)$ and $h(x)$ generate the same $\mathcal{H}$ in Γ_n . $\square$

Example 7. Each of the polynomials

$$\begin{aligned}g(x) &= x^{10} + x^9 + x^7 + x^5 + x^4 + 1, \\x g(x) &= x^{11} + x^{10} + x^8 + x^6 + x^5 + x, \\x^2 g(x) &= x^{12} + x^{11} + x^9 + x^7 + x^6 + x^2, \\x^3 g(x) &= x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^3, \\x^4 g(x) &= x^{12} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1.\end{aligned}$$

generates the Hamiltonian cycle $\mathcal{H}$ in Figure 1 Bottom.

Lemma 6 tells us to focus on the polynomial with the least degree that generates $\mathcal{H}$. We formally define this polynomial.

Definition 3. Let $\mathcal{H}$ be a Hamiltonian cycle in Γ_n . The polynomial with the least degree ℓ among all of the polynomials that generate $\mathcal{H}$ is the canonical generator $c_{\mathcal{H}}(x)$ of $\mathcal{H}$.

Theorem 9. Let $n \geq 4$ be given, and let $\frac{g(x)}{F(x)}$ be a rational fraction representation of a modified binary de Bruijn sequence $\mathbf{s}$. Then, there exists a polynomial $g_k(x) \in \mathbb{F}_2[x]$ of degree $2^n - n - 2$ such that $\frac{g_k(x)}{F(x)}$ is a rational fraction representation of the k -shifted sequence $L^k \mathbf{s}$ for some $0 \leq k < N$. The polynomial $g_k(x)$ is the canonical generator of the Hamiltonian cycle $\mathcal{H}$ that corresponds to $\mathbf{s}$.

Proof. We claim that $\deg(g_k(x)) \geq 2^n - n - 2$. Suppose, on the contrary, that there exists some r , with $0 \leq r < 2^n - 1$, such that $\deg(g_r(x)) < 2^n - n - 2$. Let

$$[n - r] = \begin{cases} n - r & \text{if } n \geq r, \\ n - r + 2^n - 1 & \text{if } n < r. \end{cases}$$

Then, $g(x) x^{[n-r]} = g(x) x^{2^n-1-r+n} = g_r(x) x^n \bmod F(x)$. Therefore,

$$g(x) x^{[n-r]} = (0 \bmod F(x)) \bmod x^n, \quad (35)$$

which contradicts the fact that $0 \notin \Omega$.

Next, we show the existence of $g_u(x)$, for some $0 \leq u < 2^n - 1$, which satisfies $\deg(g(x)) = 2^n - n - 2$ and $g_u(0) = 1$. Since $\Omega = \{g_k(x) \bmod x^n : 0 \leq k < 2^n - 1\}$,

then there exists some t , with $0 \leq t < 2^n - 1$, such that $g_t(x) = x^{n-1} \bmod x^n$. If $g_t(x) = \tilde{g}_t(x) x^n + x^{n-1}$ with $\deg(\tilde{g}_t(x)) < 2^n - n - 2$, then

$$g(x) x^{2^n-1-t} = \tilde{g}_t(x) x^n + x^{n-1} \bmod F(x).$$

Since $\gcd(x, F(x)) = 1$, we multiply both sides by x^{1-n} . If $u = (t + n - 1) \bmod (2^n - 1)$, then $g(x) x^{2^n-1-u} = g_u(x) = \tilde{g}_t(x) x + 1 \bmod F(x)$. Finally, we infer

$$\deg(g_u(x)) = \deg(\tilde{g}_t(x)) + 1 \leq 2^n - n - 2.$$

Thus, $\deg(g_u(x)) = 2^n - n - 2$. By Corollary 2 and Definition 3, we confirm that $g_k(x)$ is precisely $c_{\mathcal{H}}(x)$ of $\mathbf{s}$. $\square$

Every Hamiltonian cycle $\mathcal{H}$ in Γ_n has $c_{\mathcal{H}}(x)$ of degree $2^n - n - 2$. We now show how to determine $c_{\mathcal{H}}(x)$ for a given $\mathcal{H}$.

Theorem 10. *If $\mathcal{H}$ is a Hamiltonian cycle in $\Gamma_{n \geq 4}$ and $h_n = \sum_{i=0}^{n-1} x^i \in \mathcal{H}$, then its canonical generator $c_{\mathcal{H}}(x)$ can be determined by the following procedure.*

1. *Begin by writing $c_{\mathcal{H}}(x) = x^{2^n-n-2} + \sum_{i=1}^{2^n-n-3} c_i x^i + 1$.*
2. *Let $k = 0, 1, \dots, 2^n - 2$ and $i = 2^n - 2 - n - k$. Determine each c_i by solving $x^{n+k} c_{\mathcal{H}}(x) = h_{n+k} \bmod F(x) \bmod x^n$.*

Proof. Since $c_{\mathcal{H}}(x) := x^{2^n-2-n} + \sum_{i=1}^{2^n-n-3} c_i x^i + 1$ and $h_n = \sum_{i=0}^{n-1} x^i$ satisfies

$$h_n = x^n c_{\mathcal{H}}(x) \bmod F(x) \bmod x^n,$$

then the solution of $x^{n+k} c_{\mathcal{H}}(x) = h_{n+k} \bmod F(x) \bmod x^n$ determines the value of $c_{2^n-2-n-k}$. Thus, all c_i s can be determined. $\square$

Example 8. *Let $\mathcal{H} \in \Gamma_4$ be given in terms of its successive vertices*

$$(1, 13, 5, 10, 11, 9, 2, 4, 7, 14, 3, 6, 12, 8, 15).$$

We have $c_{\mathcal{H}}(x) = x^{10} + \sum_{i=1}^9 c_i x^i + 1$ and $F(x) = \sum_{i=0}^{14} x^i$. Hence, $x^4 c_{\mathcal{H}}(x) = x^3 + x^2 + x + 1$, which is vertex 15. Consequently, $(c_{\mathcal{H}}(x) \bmod F(x)) \bmod x^4 = x + 1$ is vertex 3. Hence, $c_{\mathcal{H}}(x) = x^{10} + c_9 x^9 + c_8 x^8 + c_7 x^7 + c_6 x^6 + c_5 x^5 + c_4 x^4 + x + 1$. We iterate the process and read the resulting polynomials in terms of their vertices in Γ_4 . Since $x^5 c_{\mathcal{H}}(x)$ is vertex 1, we obtain $c_9 = 0$. Since $x^6 c_{\mathcal{H}}(x)$ is vertex 13, we infer $c_8 = 1$. We end with $c_{\mathcal{H}}(x) = x^{10} + x^8 + x^5 + x + 1$ from Example 7.

Finally, we are ready to determine the minimal polynomial of a modified binary de Bruijn sequence.

Theorem 11. *Let $F(x) = x^{2^n-2} + x^{2^n-3} + \dots + x^2 + x + 1$. Let $\mathcal{H}$ be a Hamiltonian cycle in Γ_n whose canonical generator is $c_{\mathcal{H}}(x)$. The reciprocal polynomial $f^*(x)$ of*

$$f(x) = \frac{F(x)}{d(x)}, \text{ where } d(x) := \gcd(c_{\mathcal{H}}(x), F(x)), \quad (36)$$

is the minimal polynomial $m_{\mathbf{s}}(x)$ of the modified de Bruijn sequence $\mathbf{s}$ that corresponds to the given $\mathcal{H}$.

Proof. Since $c_{\mathcal{H}}(x)$ is the canonical generator of $\mathcal{H}$ in Γ_n , we know that

$$\Omega = \left\{ (x^i c_{\mathcal{H}}(x) \bmod F(x)) \bmod x^n : 0 \leq i \leq 2^n - 2 \right\}.$$

Hence, $\frac{c_{\mathcal{H}}(x)}{F(x)}$ is a rational fraction representation of $\mathbf{s}$. If $d(x) = \gcd(c_{\mathcal{H}}(x), F(x))$, then

$$c_{\mathcal{H}}(x) = d(x) \tilde{c}(x) \text{ and } F(x) = d(x) f(x).$$

Thus, $\frac{\tilde{c}(x)}{f(x)}$ is also a rational fraction representation of $\mathbf{s}$, whose minimal polynomial is $m_{\mathbf{s}}(x) = f^*(x)$. $\square$

Example 9. When $n = 4$, the canonical polynomial $c_{\mathcal{H}}(x) = x^{10} + x^7 + x^5 + x + 1$ generates the cycle of vertices $(1, 2, 11, 9, 13, 5, 10, 4, 7, 14, 3, 6, 12, 8, 15)$. The arcs forming the Hamiltonian path are

$$(1, 2), (2, 11), (11, 9), (9, 13), (13, 5), (5, 10), (10, 4), \\ (4, 7), (7, 14), (14, 3), (3, 6), (6, 12), (12, 8), (8, 15),$$

and the corresponding sequence is $\mathbf{s} = (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$. Since $d(x) = \gcd(F(x), c_{\mathcal{H}}(x)) = x^2 + x + 1$,

$$m_{\mathbf{s}}(x) = f^*(x) = f(x) = \frac{F(x)}{d(x)} = x^{12} + x^9 + x^6 + x^3 + 1.$$

6. Conclusions and Future Works

This work provides a systematic method to determine the minimal polynomial of a modified binary de Bruijn sequence. As a concluding remark, we highlight that, if, for any $n \geq 3$, one can characterize the occasions for which $\gcd((c_{\mathcal{H}}(x), F(x))) = 1$, then we can confirm that there exist modified de Bruijn sequences with maximal complexity $2^n - 2$. The computational evidence for small values of n strongly suggests that most modified de Bruijn sequences have maximal complexity. Determining a closed formula for the number of such sequences is a worthy research challenge to solve.

Author Contributions: Conceptualization, M., I.E.W., D.J.E.P. and M.F.E.; investigation, M., I.E.W., D.J.E.P. and M.F.E.; writing—original draft preparation, M.; writing—review and editing, I.E.W., D.J.E.P. and M.F.E.; visualization, M.F.E.; supervision, I.E.W., D.J.E.P. and M.F.E.; project administration, M.; funding acquisition, M. and I.E.W. All authors have read and agreed to the published version of the manuscript.

Funding: Musthofa is supported by the Indonesian Endowment Fund for Education, known by its abbreviation LPDP in Bahasa Indonesia, a full-ride scholarship from the Indonesian Ministry of Finance. Nanyang Technological University Grant 04INS000047C230GRT01 supports the research conducted by M.F.E.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. De Bruijn, N.G. A combinatorial problem. *Proc. Sect. Sci. K. Ned. Akad. Wet.* **1946**, *49*, 758–764.
2. Sainte-Marie, C.F. Solution to question nr. 48. *Interméd. Math.* **1894**, *1*, 107–110.
3. Fredricksen, H. A survey of full length nonlinear shift register cycle algorithms. *SIAM Rev.* **1982**, *24*, 195–221. [\[CrossRef\]](#)
4. Chang, Z.; Ezerman, M.F.; Ling, S.; Wang, H. On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials. *Des. Codes Cryptogr.* **2019**, *87*, 1137–1160. [\[CrossRef\]](#)
5. Gabric, D.; Sawada, J.; Williams, A.; Wong, D. A successor rule framework for constructing k -ary de Bruijn sequences and universal cycles. *IEEE Trans. Inform. Theory* **2020**, *66*, 679–687. [\[CrossRef\]](#)
6. Etzion, T. Linear complexity of de Bruijn sequences—old and new results. *IEEE Trans. Inform. Theory* **1999**, *45*, 693–698. [\[CrossRef\]](#)

7. Chan, A.H.; Games, R.A.; Key, E.L. On the complexities of de Bruijn sequences. *J. Comb. Theory Ser. A* **1982**, *33*, 233–246. [[CrossRef](#)]
8. Etzion, T.; Lempel, A. Construction of de Bruijn sequences of minimal complexity. *IEEE Trans. Inform. Theory* **1984**, *30*, 705–709. [[CrossRef](#)]
9. Mayhew, G.; Golomb, S. Linear spans of modified de Bruijn sequences. *IEEE Trans. Inform. Theory* **1990**, *36*, 1166–1167. [[CrossRef](#)]
10. Kyureghyan, G.M. Minimal polynomials of the modified de Bruijn sequences. *Discrete Appl. Math.* **2008**, *156*, 1549–1553. [[CrossRef](#)]
11. Tan, L.; Xu, H.; Qi, W.-F. Preliminary results on the minimal polynomial of modified de Bruijn sequences. *Finite Fields Appl.* **2018**, *50*, 356–365. [[CrossRef](#)]
12. Wang, H.-Y.; Zheng, Q.-X.; Wang, Z.-X.; Qi, W.-F. The minimal polynomials of modified de Bruijn sequences revisited. *Finite Fields Appl.* **2020**, *68*, 101735. [[CrossRef](#)]
13. Lidl, R.; Niederreiter, H. *Finite Fields, Encyclopaedia of Mathematics and Its Applications*; Cambridge University Press: New York, NY, USA, 1997.
14. Sloane, N.J.A. Sequence No. A0001037. In *The Online Encyclopedia of Integer Sequences*; The OEIS Foundation Inc.: Highland Park, NJ, USA, 2009. Available online: <https://oeis.org/A0001037> (accessed on 20 June 2022).
15. Good, I.J. Normal recurring decimals. *J. London Math. Soc.* **1946**, *s1-21*, 167–169. [[CrossRef](#)]
16. Kühn, D.; Osthus, D. A survey on Hamilton cycles in directed graphs. *Eur. J. Comb.* **2012**, *33*, 750–766. [[CrossRef](#)]
17. Bang-Jensen, J.; Gutin, G.Z. *Digraphs: Theory, Algorithms and Applications*, 2nd ed.; Springer: Berlin/Heidelberg, Germany, 2009.
18. Chang, Z.; Ezerman, M.F.; Fahreza, A.A. On greedy algorithms for binary de Bruijn sequences. *Appl. Algebra Eng. Commun.* **2020**. [[CrossRef](#)]