Minimal polynomials of the modified de Bruijn sequences

Gohar M. Kyureghyan

Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany

Received 5 February 2003; received in revised form 22 July 2003; accepted 2 November 2006

Available online 30 August 2007

Dedicated to the memory of Levon Khachatrian

Abstract

It is well known that a de Bruijn sequence over \( \mathbb{F}_2 \) has the minimal polynomial \((x + 1)^d\), where \( 2^{n-1} + n \leq d \leq 2^n - 1 \). We study the minimal polynomials of the modified de Bruijn sequences.

© 2007 Elsevier B.V. All rights reserved.

Keywords: Modified de Bruijn sequence; m-Sequence; Linear complexity; Cyclotomic numbers

1. Introduction

Sequences with some required properties have many practical applications. For cryptographic sequences it is necessary to have, for example, good autocorrelation properties, large linear complexity, and uniform pattern distribution. De Bruijn sequences provide the best pattern distribution, and it is interesting to study their other properties.

Let \( s = s_0, s_1, \ldots \) be a sequence of elements from \( \mathbb{F}_2 \). For any nonnegative integer \( k \), define the \( k \)th shift \( s^{(k)} \) of \( s \) to be the sequence \( s_k, s_{k+1}, \ldots \). The sequence \( s \) is said to be periodic with period \( p \) and denoted by \( s = (s_0, \ldots, s_{p-1}) \) if \( s_i + p = s_i \) for all nonnegative \( i \). A polynomial \( a_0 + a_1 x + \cdots + x^d \in \mathbb{F}_2[x] \) is a characteristic polynomial of \( s \) if

\[
s_{d+i} + \sum_{j=0}^{d-1} a_j s_{j+i} = 0 \quad \text{for all } i \geq 0.
\]

The set of all characteristic polynomials of \( s \) forms an ideal \( I \) in \( \mathbb{F}_2[x] \). The minimal polynomial of \( s \) is defined to be the unique generator of \( I \). The degree of the minimal polynomial of \( s \) is its linear complexity.

The order of polynomial \( f(x) = x^e g(x) \in \mathbb{F}_2[x] \), \( g(0) \neq 0 \), is the least positive integer for which \( g(x) \) divides \( x^e + 1 \). It is known (see [11]) that the least period of a sequence is equal to the order of its minimal polynomial. Further we assume that all sequences and polynomials are over \( \mathbb{F}_2 \).

A sequence \( b = (b_0, \ldots, b_{2^n-1}) \) is called an \( n \)th order de Bruijn sequence if

\[
\{b_i \ldots b_{i+n-1} : i \in \{0, \ldots, 2^n - 1\}\} = \mathbb{F}_2^n.
\]

There are \( 2^{2^n-1-n} \) many \( n \)th order de Bruijn sequences [7,3]. Clearly, \( x^{2^n} + 1 = (x + 1)^{2^n} \) is a characteristic polynomial for every \( n \)-order de Bruijn sequence. In [4] it is shown that the minimal polynomial of an \( n \)-order de Bruijn sequence
Theorem 1. The minimal polynomial of a sequence with the least period is worse than one of de Bruijn sequences, but they are expected to have better autocorrelation (cf. [9, 10]). The sequences by removing a zero from its unique allzero continue the study of the minimal polynomials of the modified de Bruijn sequences, originated in [12].

m-sequences, which we define and discuss later, are contained in the set of the modified de Bruijn sequences. Here we continue the study of the minimal polynomials of the modified de Bruijn sequences, originated in [12].

Theorem 1 (Mayhew and Golomb [12]). The minimal polynomial of a modified n-order de Bruijn sequence is a product of distinct irreducible polynomials of degrees not equal to 1 and dividing n.

Sketch of the proof. The minimal polynomial should divide characteristic polynomial \( x^{2^n-1} + 1 \), which is the square-free product of the irreducible polynomials of degrees dividing n. Since a modified de Bruijn sequence has an even number of 1’s and the minimal polynomial of sequence \( s = (s_0, \ldots, s_{d-1}) \) is

\[
\frac{x^p + 1}{\gcd(x^p + 1, s_0 x^{p-1} + s_1 x^{p-2} + \cdots + s_{d-1})},
\]

\( x + 1 \) cannot be a factor of its minimal polynomial. For more details, see [11, 12]. □

Observing that the proof in fact does not depend on the de Bruijn property of the sequence and recalling that the order of the minimal polynomial should be \( 2^n - 1 \), we can slightly improve Theorem 1.

Theorem 2. The minimal polynomial of a sequence with the least period \( 2^n - 1 \) is a product of distinct irreducible polynomials with

(a) degrees dividing n,
(b) the least common multiple of their orders is equal to \( 2^n - 1 \).

In this paper we show that the product of a primitive polynomial of degree n and a polynomial of degree 2 cannot be the minimal polynomial for a modified de Bruijn sequence. Further we generalize this result for a product of two primitive polynomials of degrees n and k.

2. Auxiliary results

2.1. m-Sequences

An irreducible polynomial \( f(x) \in \mathbb{F}_2[x] \) of degree n is called a primitive polynomial over \( \mathbb{F}_2 \) if its order is equal to \( 2^n - 1 \) (cf. [11]). A sequence, whose minimal polynomial is a primitive polynomial over \( \mathbb{F}_2 \), is called an n-order maximal period sequence (n-order m-sequence) in \( \mathbb{F}_2 \). An n-order m-sequence is a modified n-order de Bruijn sequence.

Trace representation: Let \( \alpha \) be a root of the minimal polynomial of an n-order m-sequence \( (a_0, \ldots, a_{2^n-2}) \), then

\[ a_i = \text{Tr}_{2^n/2}(\beta \alpha^i) \quad \text{for some } \beta \in \mathbb{F}_{2^n}, \]

where \( \text{Tr}_{2^n/2}(x) = x + x^2 + \cdots + x^{2^n-1} \) is the trace function from \( \mathbb{F}_{2^n} \) onto \( \mathbb{F}_2 \). Note that the sequence

\[ (\text{Tr}_{2^n/2}(\beta), \text{Tr}_{2^n/2}(\beta \alpha), \text{Tr}_{2^n/2}(\beta \alpha^2), \ldots, \text{Tr}_{2^n/2}(\beta \alpha^{2^n-2})), \quad \beta = \alpha^k \]

is the kth shift of the sequence

\[ (\text{Tr}_{2^n/2}(1), \text{Tr}_{2^n/2}(\alpha), \text{Tr}_{2^n/2}(\alpha^2), \ldots, \text{Tr}_{2^n/2}(\alpha^{2^n-2})). \]
Shift and add property: Let $a$ be an $n$-order m-sequence, then for all $i \neq j \in \{0, \ldots, 2^n-2\}$ there is $l \in \{0, \ldots, 2^n-2\}$ such that

$$a(i) + a(j) = a(l).$$

Moreover, the m-sequences are the only sequences over $\mathbb{F}_2$ having shift and add property [2].

2.2. Cyclotomic numbers

Let $2^n = d \cdot f + 1$, $x$ be a primitive element of $\mathbb{F}_{2^n}$ and $\langle x^d \rangle$ be the multiplicative subgroup generated by $x^d$. The cosets

$$C_i^d = x^i \cdot \langle x^d \rangle, \quad i = 0, \ldots, d-1$$

are called cyclotomic classes of order $d$ with respect to $\mathbb{F}_{2^n}$. Clearly,

$$\mathbb{F}_{2^n}^* = \bigcup_{i=0}^{d-1} C_i^d.$$

Set

$$C_{(l,m)}^d = (C_l^d + 1) \cap C_m^d, \quad l, m \in \{0, \ldots, d-1\}.$$

The constants

$$(l, m)_d = |C_{(l,m)}^d|$$

are called cyclotomic numbers of order $d$ with respect to $\mathbb{F}_{2^n}$. The determination of the cyclotomic numbers is a difficult problem, for more details see [1], for instance.

Further we will need the following simple properties of the cyclotomic numbers:

(i) $(i, j)_d = (j, i)_d$
(ii) $(i, j)_d = (2i, 2j)_d$
(iii) $(i, j)_d = (i - j, d - j)_d$
(iv) There is at least one $i \in \{1, \ldots, d-1\}$ such that $(i, 0)_d \neq 0$.

Lemma 1. If $2^n > \frac{1}{2}d^4$, then $(i, j)_d \neq 0$ for all $i, j$.

Proof. It is known that the equation

$$a_1x_1^d + a_2x_2^d = b, \quad a_1, a_2, b \in \mathbb{F}_{2^n}^*$$

has always a solution in $\mathbb{F}_{2^n}^*$ for such $n, d$ (see [11], Section 6.3). The lemma follows if in (1) we take $a_1 \in C_i^d, \ a_2 \in C_j^d$ and $b = 1$. □

3. Minimal polynomials of the modified de Bruijn sequences

Here we show that not all polynomials allowed by Theorem 2 are the minimal polynomial for some modified de Bruijn sequence.

Claim 1 (Lidl and Niederreiter [11]). Let $f(x), g(x) \in \mathbb{F}_2[x]$ be irreducible polynomials. Then a sequence, having the minimal polynomial $f(x)g(x)$, is the sum of a sequence with minimal polynomial $f(x)$ and a sequence with the minimal polynomial $g(x)$.

Theorem 3. Let $n > 2$, $f(x) \in \mathbb{F}_2[x]$ be a primitive polynomial of degree $n$ and $g(x) \in \mathbb{F}_2[x]$ be the primitive polynomial of degree 2. Then there is no $n$-order modified de Bruijn sequence with minimal polynomial $f(x)g(x)$. 
Theorem 4. Let \( n \geq 4k \), \( f(x) \in \mathbb{F}_2[x] \) be a primitive polynomial of degree \( n \) and \( g(x) \in \mathbb{F}_2[x] \) be a primitive polynomial of degree \( k \). Then there is no \( n \)-order modified de Bruijn sequence with minimal polynomial \( f(x)g(x) \).

Proof. If \( n \) is not divisible by \( k \), the statement follows from Theorem 2. Thus let \( n \) be a multiple of \( k \), implying that \( 2^n - 1 \) is a multiple of \( 2^k - 1 \). Using Claim 1, our goal is to show that the sum sequence \( c \) of an \( n \)-order \( m \)-sequence \( a \)
with a $k$-order m-sequence $b$ is never an $n$-order modified de Bruijn sequence. Assume, without loss of generality that 
\[ a_i = \text{Tr}_{2^n/2}(x^i) \]
and 
\[ b_i = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
for some $f \in \{0, \ldots, 2^k - 2\}$, where $\alpha$, resp. $\beta$, is a root of $f(x)$, resp. $g(x)$. In order to show that $c$ is not an $n$-order de Bruijn sequence we need to show that either it contains the allzero $n$-tuple, or there is $s > 0$ such that $c + c^{(s)}$ contains the allzero $n$-tuple. Clearly, 
\[ c + c^{(s)} = a + a^{(s)} + b + b^{(s)}. \]
Further, 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) = \text{Tr}_{2^n/2}(1 + x^i) x^i \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(1 + \beta^i) \beta^i. \]
Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]

Using (4) and (5), we have 
\[ a_i + a_{i+s} = \text{Tr}_{2^n/2}(x^i) + \text{Tr}_{2^n/2}(x^{i+s}) \]
\[ = \text{Tr}_{2^n/2}(x^i + x^{i+s}) = \text{Tr}_{2^n/2}((1 + x^i)x^i) \]
and 
\[ b_i + b_{i+s} = \text{Tr}_{2^k/2}(\beta^i) \beta^i \]
\[ + \text{Tr}_{2^k/2}(\beta^{i+s}) = \text{Tr}_{2^k/2}(\beta^i (1 + \beta^i) \beta^i). \]