JOURNAL OF COMBINATORIAL THEORY, Series A **76**, 55–82 (1996)
ARTICLE NO. 0088

Permutation Polynomials, de Bruijn Sequences, and Linear Complexity

Simon R. Blackburn*

*Department of Mathematics, Royal Holloway, University of London,
Egham, Surrey TW20 0EX, United Kingdom*

Tuvi Etzion[†]

*Department of Computer Science, Royal Holloway, University of London,
Egham, Surrey TW20 0EX, United Kingdom*

and

Kenneth G. Paterson[‡]

*Department of Mathematics, Royal Holloway, University of London,
Egham, Surrey TW20 0EX, United Kingdom*

Communicated by the Managing Editors

Received June 14, 1995

The paper establishes a connection between the theory of permutation polynomials and the question of whether a de Bruijn sequence over a general finite field of a given linear complexity exists. The connection is used both to construct span 1 de Bruijn sequences (permutations) of a range of linear complexities and to prove non-existence results for arbitrary spans. Upper and lower bounds for the linear complexity of a de Bruijn sequence of span n over a finite field are established. Constructions are given to show that the upper bound is always tight, and that the lower bound is also tight in many cases. © 1996 Academic Press, Inc.

1. INTRODUCTION

A periodic sequence s over $\mathbb{F}_{p^m}$, the finite field with p^m elements, is called a span n de Bruijn sequence if each n-tuple of elements of $\mathbb{F}_{p^m}$ appears

* This author's research supported by EPSRC Grant GR/H23719.

[†] On leave of absence from the Computer Science Department, Technion—Israel Institute of Technology, Haifa, 32000, Israel. This author's research supported in part by the EPSRC under Grant GR/K38847.

[‡] This author's research supported by a Lloyd's of London Tercentenary Foundation Research Fellowship.

0097-3165/96 $18.00

exactly once as a window of n consecutive terms in a period of the sequence. De Bruijn sequences correspond to Hamiltonian cycles in the de Bruijn graph [1, 5]. These graphs and sequences have been extensively studied because of their wide applications, e.g. [3, 6, 12, 13] and their combinatorial interest [5, 10].

One of the most important measures of the complexity of a sequence is its linear complexity, this being the degree of the shortest linear recurrence which generates the sequence (see Section 2 for a formal definition). While the linear complexity of binary de Bruijn sequences has been thoroughly investigated [4, 7, 8, 9, 11], almost no work has been done on the linear complexities of de Bruijn sequences over general finite fields. In this paper we consider the linear complexities of such sequences. We find that both the results concerning linear complexities of de Bruijn sequences over general finite fields and the techniques required to prove them differ markedly from the binary case.

Our paper is organised as follows. Section 2 establishes our notation and a number of basic results that will be needed in the sequel. We also consider the enumeration of periodic sequences over $\mathbb{F}_{p^m}$ with specified complexities and give some computational results on the distribution of the linear complexity of de Bruijn sequences. In Section 3, we develop the connection between the linear complexity of sequences and the degrees of permutation polynomials and apply it to the study of permutations of $\mathbb{F}_{p^m}$, these being equivalent to span 1 de Bruijn sequences. We are able to prove a non-existence result for permutations (Corollary 12), which we may state as follows. Suppose k is a positive integer dividing $p-1$. If $m=1$, assume that $k>1$. Then there exists no permutation of $\mathbb{F}_{p^m}$ of linear complexity $1+k\sum_{i=0}^{m-1} p^i$. In contrast, we show that, for fields of characteristic 2, 3 and 5, permutations of all linear complexities between our upper and lower bounds do occur, provided their existence is not ruled out by Corollary 12.

In Section 4 we turn to the study of general span de Bruijn sequences over $\mathbb{F}_{p^m}$, again using the link to permutation polynomials to obtain both a powerful non-existence result (Corollary 19) and upper and lower bounds on the linear complexity of such a sequence. Our bounds generalise the results of [4]. We show that the upper bound is always attained, but that the lower bound is not tight in every case. In particular for span 2 sequences over prime fields, our bound is never achieved. We present an improved lower bound for this case and prove its tightness. On the other hand, we show by construction that, for span 2 sequences over $\mathbb{F}_{p^m}$, $m\geqslant 2$ and for some higher spans over non-prime fields of small characteristic, our lower bound is tight. Thus there is a sharp difference in the behaviour of minimal linear complexity of de Bruijn sequences over prime and non-prime fields.

Finally, in Section 5, we discuss some open questions and conjectures.

2. BASIC RESULTS

In this section, we introduce some notation and develop a number of basic results on the linear complexity of sequences. We also enumerate the sequences over $\mathbb{F}_{p^m}$ with period p^k and a fixed linear complexity and the de Bruijn sequences of small span over small fields.

Sequence $s = ..., s_{-1}, s_0, s_1, ...$ over $\mathbb{F}_{p^m}$ is said to be *periodic* if there exists non-zero integer t such that $s_i = s_{i+t}$ for every $i \in \mathbb{Z}$. The *period* of s is defined to be the least positive such t. We will write $[s_0, s_1, ..., s_{t-1}]$ for the sequence of period t with $s_0, s_1, ..., s_{t-1}$ as its first t terms. Thus $[a]$ denotes the constant sequence (of period 1) all of whose terms are a.

Definition 1. Sequence s over $\mathbb{F}_{p^m}$ is a *span n de Bruijn sequence over* $\mathbb{F}_{p^m}$ if it has period p^{mn} and the n-tuples

$$(s_i, s_{i+1}, ..., s_{i+n-1}), \qquad 0 \leqslant i < p^{mn}$$

are distinct.

From the above definition, it is clear that every n-tuple over $\mathbb{F}_{p^m}$ occurs exactly once as n consecutive terms in a period of a de Bruijn sequence.

We define the action of the left shift operator E on sequences as follows. Let s be an arbitrary sequence over $\mathbb{F}_{p^m}$. Then Es is defined to be the sequence whose ith term is s_{i+1}. For integer k, we can similarly define $E^k s$ to be the sequence with ith term s_{i+k}.

We say that two sequences s and t are *equivalent* if $E^k s = t$ for some integer k.

Suppose that for some elements $c_0, c_1, ..., c_{n-1} \in \mathbb{F}_{p^m}$, the sequence s over $\mathbb{F}_{p^m}$ satisfies:

$$s_{i+n} + c_{n-1} s_{i+n-1} + \cdots + c_1 s_{i+1} + c_0 s_i = 0 \qquad \text{for all} \quad i \in \mathbb{Z} \qquad (1)$$

that is, *a linear recurrence relation of degree n.* We then have

$$(E^n + c_{n-1} E^{n-1} + \cdots + c_1 E + c_0)\, s = [0]$$

and we call the polynomial $X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0$ a *characteristic polynomial* of s.

If s has period t, then s satisfies

$$s_{i+t} - s_i = 0, \qquad \text{for all} \quad i \in \mathbb{Z},$$

a linear recurrence of degree t with characteristic polynomial $X^t - 1$, so any periodic sequence satisfies a linear recurrence. We have the following result and definition.

Result 1 [14, Theorem 8.42, page 418]. Let s be a sequence of period t. Then there exists a uniquely determined monic polynomial m (called the *minimal polynomial* of s) having the following property: g is a characteristic polynomial for s if and only if m divides g.

DEFINITION 2. Suppose s is a periodic sequence over $\mathbb{F}_{p^m}$. Then the linear complexity of s, denoted $c(s)$, is the degree of the minimal polynomial m of s.

PROPOSITION 2. *A sequence s has period p^k for some k and linear complexity $c(s)$ if and only if the minimum polynomial of s is $(X-1)^{c(s)}$. Further, if s is non-zero and has period p^k, then*

$$p^{k-1}+1\leqslant c(s)\leqslant p^k,$$

unless $k=0$, in which case $c(s)=1$.

Proof. Suppose s is a sequence of period p^k over $\mathbb{F}_{p^m}$, with minimal polynomial m. Then $m(E)\,s$ is the all-zero sequence and from Result 1, m divides $X^{p^k}-1$. Over a field of characteristic p, we have $X^{p^k}-1=(X-1)^{p^k}$ since the binomial coefficients $\binom{p^k}{i}$ are zero for $1\leqslant i\leqslant p^k-1$. Thus the minimal polynomial of s is simply $(X-1)^{c(s)}$ and s satisfies the linear recurrence

$$(E-1)^{c(s)}\,s=[0]. \tag{2}$$

Conversely, if s satisfies (2), then

$$(E^{p^k}-1)\,s=(E-1)^{p^k-c(s)}\,(E-1)^{c(s)}\,s=[0]$$

for any k such that $p^k\geqslant c(s)$. Hence s has period a power of p. Now suppose further that $s\neq[0]$, so that s has minimum polynomial $(X-1)^{c(s)}$, where $c(s)\geqslant 1$. The case $c(s)=1$ is trivial, so we may in fact assume that $c(s)\geqslant 2$. Then there is a unique integer k such that $p^{k-1}+1\leqslant c(s)\leqslant p^k$. Now

$$(E^{p^k}-1)\,s=(E-1)^{p^k}\,s=(E-1)^{p^k-c}\,(E-1)^c\,s=(E-1)^{p^k-c}\,[0]=[0]$$

while

$$(E^{p^{k-1}}-1)\,s=(E-1)^{p^{k-1}}\,s\neq[0],$$

for otherwise s would have linear complexity at most p^{k-1} (from Result 1). We deduce that s has period exactly p^k. ▮

We define the *weight* of a sequence s of period t over $\mathbb{F}_{p^m}$ to be the sum $s_0 + s_1 + \cdots + s_{t-1}$. We have the following:

Result 3 [16, Corollary 2.6]. Let s be a sequence of period p^k over $\mathbb{F}_{p^m}$. Then $c(s) = p^k$ if and only if s has non-zero weight.

As a further deduction from Result 1 and Proposition 2, we note that if the sequence s is non-zero, has period p^k and has linear complexity $c(s)$, then the sequence $(E-1)\,s$ has linear complexity $c(s)-1$. The following lemma follows quickly from this and the characterisation of the sequences of linear complexity 1 as the non-zero constant sequences:

LEMMA 4. *A non zero sequence s of period p^k over $\mathbb{F}_{p^m}$ has linear complexity c if and only if there exists a non-zero $a \in \mathbb{F}_{p^m}$ such that*

$$(E-1)^{c-1}\, s = [a]$$

is a constant sequence.

Finally in this section, we introduce the notion of the component sequences of a sequence s over $\mathbb{F}_{p^m}$. We can represent each term s_i of such a sequence by an m-tuple $(s_i^0, ..., s_i^{m-1})$ of elements of $\mathbb{F}_p$. We call the sequence

$$s^j = \ldots, s_{-1}^j, s_0^j, s_1^j, \ldots$$

component sequence j of s and we have the following result [16, Section 2]:

Result 5. With notation as above,

$$(E-1)^{c-1}\, s = [a], \qquad \text{for some} \quad a \neq 0$$

if and only if

$$(E-1)^{c-1}\, s^j = [a_j] \qquad \text{for some} \quad a = (a_0, ..., a_{m-1}) \neq (0, ..., 0).$$

Moreover, $c(s) = \max\{c(s^j) \colon 0 \leqslant j \leqslant m-1\}$.

2.1. *Enumeration of Sequences with Specific Complexities*

We are interested in counting the number of sequences over $\mathbb{F}_{p^m}$ of period a power of p and linear complexity c. Let $N(p^m, c)$ denote this number. Of course, $N(p^m, 0) = 1$.

LEMMA 6. *Suppose $c \geqslant 1$. Then*

$$N(p^m, c) = (p^m - 1)\, p^{mc-m}.$$

TABLE I

Inequivalent Span 1 de Bruijn Sequences over $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_8$, $\mathbb{F}_9$, and $\mathbb{F}_{11}$

Linear complexity	Field				
	$\mathbb{F}_5$	$\mathbb{F}_7$	$\mathbb{F}_8$	$\mathbb{F}_9$	$\mathbb{F}_{11}$
2	4	6	0	0	10
3	0	0	0	0	0
4	20	0	0	144	110
5	0	84	336	0	0
6	—	630	672	432	0
7	—	0	4032	3456	2640
8	—	—	0	36288	24750
9	—	—	—	0	302940
10	—	—	—	—	3298350

Proof. Let c be such that $c \geqslant 1$. Consider the set of sequences having period a power of p and linear complexity at most c. It follows from Proposition 2 that a sequence s is in this set if and only if $(X-1)^c$ is a characteristic polynomial for s. Thus each of these sequences is uniquely determined by its first c terms, using the recurrence relation (1). Hence there are exactly p^{mc} sequences in this set. So there are $p^{mc} - p^{m(c-1)} = (p^m - 1)\, p^{mc-m}$ sequences of linear complexity exactly c and having period a power of p. It follows that $N(p^m, c) = (p^m - 1)\, p^{mc-m}$. ▮

COROLLARY 7. *Let* $k > 0$. *For* $p^{k-1} + 1 \leqslant c \leqslant p^k$, *there are exactly* $(p^m - 1)\, p^{mc-m-k}$ *inequivalent sequences with period* p^k *and linear complexity* c.

We now turn to the enumeration of de Bruijn sequences with specific linear complexities. We have exhaustively generated all de Bruijn sequences of small spans over small fields and counted the number of inequivalent sequences of each linear complexity. A backtracking method was used to

TABLE II

Inequivalent Span 2 de Bruijn Sequences over $\mathbb{F}_3$

Linear complexity	Number of sequences
7	12
8	12

TABLE III

Inequivalent Span 2 de Bruijn Sequences over $\mathbb{F}_4$

Linear complexity	Number of sequences	Linear complexity	Number of sequences
10	96	13	1200
11	144	14	3312
12	336	15	15648

generate sequences while the algorithm of [2] was used to calculate linear complexities. Of course, from Proposition 2, the linear complexity of a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ must lie between $p^{mn-1}+1$ and p^{mn}.

The distribution of de Bruijn sequences over $\mathbb{F}_2$ with span up to 6 can be found in [4]. There are 2 inequivalent permutations of $\mathbb{F}_3$, each of linear complexity 2, and 6 inequivalent permutations of $\mathbb{F}_4$, each of linear complexity 3. Tables I to V contain the linear complexity distribution for span 1 de Bruijn sequences over $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_8$, $\mathbb{F}_9$ and $\mathbb{F}_{11}$, for span 2 de Bruijn sequences over $\mathbb{F}_3$, $\mathbb{F}_4$ and $\mathbb{F}_5$ and for span 3 de Bruijn sequences over $\mathbb{F}_3$. An occurence of '—' in Table I indicates a linear complexity ruled out by Proposition 2. In the other tables, if no entry occurs for a particular linear complexity, then there are no sequences of that complexity. The tables suggest that the distribution of complexities of de Bruijn sequences varies markedly from the distribution one might expect for random sequences. We will explain some of these variations below. In particular, we can account for all the zeros that occur in Table I (see Section 3.4) as well as the zeros that occur when $c=13$ or 14 (but, interestingly, not when $c=12$) in Table IV—see Corollary 19.

TABLE IV

Inequivalent Span 2 de Bruijn Sequences over $\mathbb{F}_5$

Linear complexity	Number of sequences	Linear complexity	Number of sequences
11	240	18	54800
12	0	19	256360
13	0	20	1307520
14	0	21	6430280
15	760	22	31677520
16	1920	23	159523800
17	10080	24	796064720

TABLE V

Inequivalent Span 3 de Bruijn Sequences over $\mathbb{F}_3$

Linear complexity	Number of sequences	Linear complexity	Number of sequences
17	48	22	3096
18	60	23	9240
19	60	24	29556
20	504	25	82920
21	1620	26	246144

Recall that we consider two de Bruijn sequences as being equivalent if one is a shift of the other. In the context of linear complexity, we can consider other equivalences. Two non-zero sequences $s = [s_0, ..., s_{l-1}]$ and $t = [t_0, ..., t_{l-1}]$ over $\mathbb{F}_{p^m}$ certainly have the same linear complexity if either $s_i = t_i + d$ for some $d \in \mathbb{F}_{p^m}$ and for all i, or $s_i = dt_i$ for some $d \in \mathbb{F}_{p^m} \backslash \{0\}$ and for all i, or if $s_i = t_{-i}$ for all i. These sequences could also be considered equivalent, and divisibility properties of the numbers appearing in Tables I to V can be derived from this notion of equivalence.

3. PERMUTATION POLYNOMIALS

In this section, we construct a bijection between sequences over $\mathbb{F}_p$ of period dividing p^k and a certain collection of polynomials over $\mathbb{F}_p$ in k variables. We show that the linear complexity of a sequence can be easily recovered from its associated polynomial under this bijection. Using this approach, we present results on the existence and non-existence of permutations with specific linear complexities.

3.1. *Permutation Polynomials and Linear Complexity*

Let P_k be the set of polynomials in $\mathbb{F}_p[x_0, ..., x_{k-1}]$ of degree strictly less than p in each indeterminate. Suppose $i \in \{0, ..., p^k - 1\}$ can be written in base p as $i = \sum_{j=0}^{k-1} i_j p^j$, where $i_j \in \{0, ..., p-1\}$. Then we define $x^i \in \mathbb{F}_p[x_0, ..., x_{k-1}]$ to be the product $x_0^{i_0} x_1^{i_1} \cdots x_{k-1}^{i_{k-1}}$. Using this notation, we may write each $f \in P_k$ in the form

$$f = \sum_{i=0}^{p^k - 1} a_i x^i \tag{3}$$

for some unique $a_0, a_1, ..., a_{p^k - 1} \in \mathbb{F}_p$. We define the degree of f (written $\deg f$) by

$$\deg f = \begin{cases} \max\{i \mid a_i \neq 0\} & \text{if } f \neq 0, \\ -1 & \text{if } f = 0. \end{cases}$$

So for example, the polynomial $x_0^4 x_1^2 + x_0^6 x_1 + x_1 \in \mathbb{F}_7[x_0, x_1]$ has degree $\max\{4+2\cdot 7, 6+7, 7\} = 18$.

Finally, we define S_k to be the set of all sequences of elements in $\mathbb{F}_p$ whose period divides p^k.

THEOREM 8. *Define a map $\phi_k \colon P_k \to S_k$ by setting*

$$\phi_k f = ..., s_{-1}, s_0, s_1, ...$$

where

$$s_{i_0 + i_1 p + \cdots + i_{k-1} p^{k-1} + n p^k} = f(i_0, i_1, ..., i_{k-1})$$

for all $i_j \in \{0, ..., p-1\}$ and integers n. Then ϕ_k is a bijection and $\deg f = d$ *if and only if $\phi_k f$ has linear complexity $d+1$.*

Proof. That ϕ_k is a bijection follows from the fact that every map from $\mathbb{F}_p{}^k$ to $\mathbb{F}_p$ can be represented by a polynomial in P_k. This fact is well known [14, page 369, equation (7.20)].

It remains to establish the relation between the degree of f and the complexity of $\phi_k f$. We show this by induction on k and $\deg f$. Consider the case $k=0$. Now P_0 consists of the constant polynomials and S_0 consists of the constant sequences. The theorem follows in this case, since ϕ_0 maps the zero polynomial (of degree -1) to the zero sequence (of linear complexity 0) and any non-zero constant polynomial (of degree 0) to a corresponding non-zero constant sequence (of linear complexity 1).

As our inductive hypothesis, we assume that $k' > 0$ and that the theorem holds when $k < k'$ and when both $k = k'$ and $d < d'$. Let $f \in P_{k'}$ be such that $\deg f = d'$. Suppose that $d' < p^{k'-1}$. Then f has no terms involving $x_{k'-1}$, hence may be regarded as an element of $P_{k'-1}$. Since $\phi_{k'}$ restricted to $P_{k'-1}$ is equal to $\phi_{k'-1}$, we find that $\phi_{k'} f$ has complexity $d'+1$, by our inductive hypothesis. Similarly, our inductive hypothesis implies that if $\phi_k f$ has linear complexity $d'+1$, where $d' < p^{k'-1}$, then f has degree d'.

We may now assume that $d' \geqslant p^{k-1}$. Set $s = \phi_{k'} f$ and let c be the linear complexity of s. By the inductive hypothesis, $c > p^{k'-1}$. Let $t := (E-1)^{p^{k'-1}} s$ and set $g := \phi_{k'}^{-1} t$. Since $c > p^{k'-1}$, the linear complexity of t is equal to $c - p^{k'-1}$. Hence, by the inductive hypothesis, $\deg g = c - 1 - p^{k'-1}$. To finish our inductive step, it suffices to show that $\deg g = (\deg f) - p^{k'-1}$, for then $c = d'+1$. Now, $t_i = s_{i+p^{k'-1}} - s_i$, since $(E-1)^{p^{k'-1}} = E^{p^{k'-1}} - 1$. Therefore, by the definition of $\phi_{k'}$,

$$g(x_0, x_1, ..., x_{k'-1}) = f(x_0, x_1, ..., x_{k'-1}+1) - f(x_0, x_1, ..., x_{k'-1}). \qquad (4)$$

Let $d' = \sum_{i=0}^{k'-1} d_i' p^i$, where $d_i' \in \{0, ..., p-1\}$ and $d_{k'-1}' \neq 0$. Then we may write

$$f = \sum_{i=0}^{d_{k'-1}'} x_{k'-1}^i f_i$$

where $f_i \in P_{k'-1}$ for $i = 0, 1, ..., k'-1$ and where $\deg f_{k'-1} = \sum_{i=0}^{k'-2} d_i' p^i$. Now (4) implies

$$g = d_{k'-1}' x_{k'-1}^{d_{k'-1}'-1} f_{k'-1} + h$$

where h is a polynomial involving powers of $x_{k'-1}$ which are strictly less than $d_{k'-1}' - 1$. Thus $\deg g = \deg f - p^{k'-1}$ and so $c = d' + 1$.

We have now shown that $\deg f = d'$ implies that $\phi_{k'} f$ has linear complexity $d' + 1$. The converse follows since the number of sequences in $S_{k'}$ of linear complexity $d' + 1$ (as given in Lemma 6) is equal to the number of polynomials in $P_{k'}$ of degree d'. Hence, by induction on d and $k$, the theorem follows. ▌

Let $f_0, ..., f_{k-1} \in P_k$. We say that $(f_0, ..., f_{k-1})$ is a (complete) orthogonal system if for all $b_0, ..., b_{k-1} \in \mathbb{F}_p$, there exist uniquely defined elements $a_0, ..., a_{k-1} \in \mathbb{F}_p$ such that

$$f_i(a_0, ..., a_{k-1}) = b_i \qquad \text{for all} \quad i \in \{0, ..., k-1\}.$$

We define the degree of an orthogonal system to be the integer $\max\{\deg f_i \mid i \in \{0, ..., k-1\}\}$.

THEOREM 9. *An orthogonal system $(f_0, ..., f_{m-1})$ of degree d exists if and only if a permutation of $\mathbb{F}_{p^m}$ of linear complexity $d+1$ exists.*

Proof. Let $\alpha_0, ..., \alpha_{m-1}$ be a basis for $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. The bijection ϕ_m clearly induces a bijection ψ between the set of all m-tuples $(f_0, ..., f_{m-1})$ of elements of P_m and the set of all sequences over $\mathbb{F}_{p^m}$ of period dividing p^m, where $\psi(f_0, ..., f_{m-1})$ is the sequence s whose ith term s_i is defined to be $\sum_{j=0}^{m-1} (\phi_m f_j)_i \alpha_j$. Now $s_i = \sum_{j=0}^{m-1} b_j \alpha_j$ if and only if $f_j(i_0, ..., i_{m-1}) = b_j$ for all $j \in \{0, ..., m-1\}$, where the elements $i_k \in \{0, ..., p-1\}$ are defined by $i = \sum_{k=0}^{m-1} i_k p^k$. Thus s is a permutation if and only if $(f_0, ..., f_{m-1})$ is an orthogonal system. The theorem now follows from Theorem 8, the definition of the degree of an orthogonal system and Result 5. ▌

Motivated by the two theorems above, we make the following definition.

DEFINITION 3. The *degree* of a periodic sequence is defined to be one less than its linear complexity.

3.2. *A Non-existence Result for Permutations*

Suppose that there exists a permutation over $\mathbb{F}_{p^m}$ of degree d. Then there exists an orthogonal system $(f_0, ..., f_{m-1})$ of degree d. Clearly, $\deg f_i \leqslant p^m - 1$ for all $i = 0, ..., m-1$. Furthermore, one of the polynomials $f_0, ..., f_{m-1}$ must depend on x_{m-1}, so in fact $p^{m-1} \leqslant d \leqslant p^m - 1$. However, not all values in this range can be achieved, as the following will show.

Let I be the ideal of $\mathbb{F}_p[x_0, ..., x_{m-1}]$ generated by the polynomials $x_0^p - x_0,\ x_1^p - x_1, ..., x_{m-1}^p - x_{m-1}$. If $g \in \mathbb{F}_p[x_0, ..., x_{m-1}]$, then we define the reduction of g to be the unique $f \in P_m$ such that $f \equiv g \bmod I$. We make use of the following result, a special case of [14, Theorem 7.41, page 371].

Result 10. The system $f_0, ..., f_{m-1} \in \mathbb{F}_p[x_0, ..., x_{m-1}]$ is orthogonal if and only if

1. The coefficient of $x_0^{p-1} x_1^{p-1} \cdots x_{m-1}^{p-1}$ in the reduction of the polynomial $f_0^{p-1} f_1^{p-1} \cdots f_{m-1}^{p-1}$ is non-zero and
2. For all $t_0, ..., t_{m-1} \in \{0, ..., p-1\}$ such that not all the t_i are equal to $p-1$, the coefficient of $x_0^{p-1} x_1^{p-1} \cdots x_{m-1}^{p-1}$ in the reduction of the polynomial $f_0^{t_0} f_1^{t_1} \cdots f_{m-1}^{t_{m-1}}$ is zero.

This theorem allows us to prove a non-existence result. We say that a polynomial f_0 in m indeterminates is a *generalised permutation polynomial* if it is a part of an orthogonal system $(f_0, f_1, ..., f_{m-1})$. This can be shown [14] to be equivalent to the property that f_0 takes on every value in $\mathbb{F}_p$ an equal number of times.

THEOREM 11. *Let k be a positive integer dividing $p-1$. If $m = 1$, assume in addition that $k > 1$. Then there exists no generalised permutation polynomial of degree $k \sum_{i=0}^{m-1} p^i$.*

Proof. Let k be a positive integer dividing $p-1$ and define $d := k \sum_{i=0}^{m-1} p^i$. Suppose that $(f_0, ..., f_{m-1})$ is an orthogonal system such that $\deg f_0 = d$. Set $t := (p-1)/d$. Then the coefficient of $x_0^{p-1} x_1^{p-1} \cdots x_{m-1}^{p-1}$ in the reduction of f_0^t is non-zero. This contradicts Result 10, unless $d = 1$ and $m = 1$. ∎

COROLLARY 12. *Let k be a positive integer dividing $p-1$. If $m = 1$, assume that $k > 1$. Then there exists no permutation of $\mathbb{F}_{p^m}$ of degree $k \sum_{i=0}^{m-1} p^i$.*

3.3. *Existence Results for Permutations*

In this subsection, we use the polynomial setting developed above to give some direct and recursive constructions for permutations over $\mathbb{F}_{p^m}$

with a wide range of complexities. These will allow us to prove Theorem 16, our main constructive result.

We begin with the case when $m=1$. Theorem 9 implies that a permutation over $\mathbb{F}_p$ of linear complexity $d+1$ exists if and only if there exists a polynomial $f(x)$ of degree d such that for all $b \in \mathbb{F}_p$, there is a unique solution $a \in \mathbb{F}_p$ to the equation $f(a)=b$. In other words, f has degree d and induces a permutation of the elements of $\mathbb{F}_p$. Such a polynomial is called a permutation polynomial. It is well known ([14, Theorem 7.8, page 351]) that the polynomials x^d are permutation polynomials whenever $\gcd(d, p-1)=1$.

Proposition 13. *Let d be such that* $\gcd(d, p-1)=1$ *and* $d \leqslant p-1$. *Then there exists a permutation over $\mathbb{F}_p$ of degree d.*

This result is in contrast with the non-existence result of Corollary 12: if $d>1$ divides $p-1$, then there is no permutation polynomial of degree d over $\mathbb{F}_p$. The situation where d is neither co-prime to $p-1$ nor divides $p-1$ is in general complex. We do however have the following result (based on [14, Corollary 7.33, page 367]): For all positive integers d, there exists a constant P (depending only on d) such that for all primes $p \geqslant P$, there exist permutation polynomials over $\mathbb{F}_p$ of degree d if and only if $\gcd(d, p-1)=1$. Thus, if there exists a permutation polynomial of degree d, where $\gcd(d, p-1) \neq 1$, it is an ‘accident’ due to the small size of p when compared with d. An example of such an ‘accident’ is the permutation polynomial x^4+3x over $\mathbb{F}_7$.

We will now turn to some constructions for orthogonal systems for general m which, in view of Theorem 9, is equivalent to constructing permutations of $\mathbb{F}_{p^m}$. If the degrees of permutations are thought of as being expressed to the base p, the first proposition tells us that we can construct a permutation of degree d where one or more of the digits of d are zero, while the second can be thought of as showing where digits can be inserted into degrees of permutations over $\mathbb{F}_{p^{m-1}}$ to produce degrees of permutations over $\mathbb{F}_{p^m}$ when $m \geqslant 3$.

Proposition 14. *Assume that $m \geqslant 2$. Let $d_0, ..., d_{m-1} \in \{0, ..., p-1\}$. Suppose that $d_{m-1} \neq 0$ but that $d_l=0$ for some $l \in \{0, ..., m-2\}$. Then there exists a permutation of $\mathbb{F}_{p^m}$ of degree $d := \sum_{i=0}^{m-1} d_i p^i$.*

Proof. Define $f_i := x_i$ for $i \in \{0, ..., m-1\} \setminus \{l\}$ and set

$$f_l := \left(\prod_{i=0}^{m-1} x_i^{d_i} \right) + x_l.$$

Then for every $b_0, ..., b_{m-1}$, there is a unique solution $(a_0, ..., a_{m-1})$ to the system $f_i(a_0, ..., a_{m-1}) = b_i$, given by $a_i = b_i$ for $i \neq l$ and $a_l = b_l - \prod_{i=0}^{m-1} a_i^{d_i}$. Since $(f_0, ..., f_{m-1})$ has degree d, the proposition follows. ▮

Proposition 15. *Assume that $m \geqslant 3$. Let $d_0, ..., d_{m-2} \in \{0, ..., p-1\}$ and suppose there exists a permutation over $\mathbb{F}_{p^{m-1}}$ of degree $d := \sum_{i=0}^{m-2} d_i p^i$. Let $l \in \{0, ..., m-1\}$ and $e \in \{1, ..., p-1\}$. Then there exists a permutation over $\mathbb{F}_{p^m}$ of degree*

$$\sum_{i=0}^{l-1} d_i p^i + ep^l + \sum_{i=l}^{m-2} d_i p^{i+1}.$$

Proof. Let $(f_0, ..., f_{m-2})$ be an orthogonal system of degree d. Without loss of generality, we may assume that $\deg f_{m-3} = d$. Define $(f'_0, ..., f'_{m-1})$ by setting $f'_i = f_i(x_0, ..., x_{l-1}, x_{l+1}, ..., x_{m-1})$ for $i = 0, ..., m-3$, setting $f'_{m-2} = x_l^e f_{m-3}(x_0, ..., x_{l-1}, x_{l+1}, ..., x_{m-1}) + f_{m-2}(x_0, ..., x_{l-1}, x_{l+1}, ..., x_{m-1})$ and setting $f'_{m-1} = x_l$. We claim that for every $b_0, ..., b_{m-1}$, there is a unique solution $(a_0, ..., a_{m-1})$ to the system $f'_i(a_0, ..., a_{m-1}) = b_i$. Certainly, from the definition of f'_{m-1}, we have $a_l = b_{m-1}$, and then the remainder of the system reduces to:

$$f_i(a_0, ..., a_{l-1}, a_{l+1}, ..., a_{m-1}) = b_i, \qquad 0 \leqslant i \leqslant m-3,$$

$$f_{m-2}(a_0, ..., a_{l-1}, a_{l+1}, ..., a_{m-1}) = b_{m-2} - b_{m-1}^e b_{m-3}.$$

This orthogonal system has a unique solution $(a_0, ..., a_{l-1}, a_{l+1}, ..., a_{m-1})$. Hence $f'_0, ..., f'_{m-1}$ form an orthogonal system. The degree of this system is $\sum_{i=0}^{l-1} d_i p^i + ep^l + \sum_{i=l}^{m-2} d_i p^{i+1}$, so the proposition follows. ▮

Theorem 16. *Suppose that for some $m \geqslant 2$, there is a permutation over $\mathbb{F}_{p^m}$ of every degree d (where of course $p^{m-1} \leqslant d \leqslant p^m - 1$) not ruled out by Corollary 12. Then for every $m' > m$, there exists a permutation over $\mathbb{F}_{p^{m'}}$ of every degree d', $p^{m'-1} \leqslant d' \leqslant p^{m'} - 1$, not ruled out by Corollary 12.*

We show below that for fields of characteristic p where $p = 2$, 3 or 5, the hypothesis of Theorem 16 holds with $m = 2$. Thus there is some evidence to support the conjecture that for all primes p, there exists an integer m satisfying the hypothesis of Theorem 16.

Proof of Theorem 16. We will prove the result in the special case where $m' = m + 1$. The full result follows from this by induction.

Let $d' = \sum_{i=0}^{m} d_i p^i$ where $d_i \in \{0, ..., p-1\}$ and $d_m \neq 0$. Further, suppose that we do not have $d_0 = \cdots = d_m = k$, where k divides $p-1$. Thus d' is a degree not ruled out by Corollary 12. If $d_i = 0$ for some i, then an application of Proposition 14 can be used to obtain a permutation of $\mathbb{F}_{p^{m'}}$ of degree d'. Otherwise, we can assume that every d_i is non-zero and consider two cases. If $d_0 = \cdots = d_{m-1} = k$, where k divides $p-1$, then $d_m \neq k$ and there exists a permutation of $\mathbb{F}_{p^{m-1}}$ of degree $\sum_{i=0}^{m-1} d_{i+1} p^i$. Applying Proposition 15 with $l = 0$ and $e = d_0$, we obtain a permutation of $\mathbb{F}_{p^{m'}}$ of degree d'. Otherwise, in the second case, there exists a permutation of $\mathbb{F}_{p^m}$ of degree $\sum_{i=0}^{m-1} d_i p^i$. Applying Proposition 15 with $l = m$ and $e = d_m$, we obtain a permutation of $\mathbb{F}_{p^{m'}}$ of degree d'. ▮

Theorem 16 shows that in order to prove that there exist permutations of $\mathbb{F}_{p^m}$ for every $m \geqslant 2$ and for every degree, excluding those ruled out by our non-existence result, it is sufficient to prove the result for permutations over $\mathbb{F}_{p^2}$. We have already noted that the case $m = 1$ is equivalent to the existence of permutation polynomials of the appropriate degrees. Our next result gives a number of special constructions over $\mathbb{F}_{p^2}$ and will be applied to fields of small characteristic in the next subsection.

PROPOSITION 17. *Suppose that $d = d_0 + d_1 p$ where $d_0, d_1 \in \{0, ..., p-1\}$ and $d_1 \neq 0$. Then there exists a permutation over $\mathbb{F}_{p^2}$ of degree d if any one of the following conditions hold*:

(a) $d_0 = 0$,

(b) *a permutation over $\mathbb{F}_p$ of degree d_0 exists and $d_1 \geqslant 2$,*

(c) *a permutation over $\mathbb{F}_p$ of degree d_1 exists and $d_0 \geqslant 2$,*

(d) *there exists an integer e such that e divides d_0, e divides d_1, $d_1 \neq e$ and there exists a permutation over $\mathbb{F}_p$ of degree d_0/e,*

(e) *there exists an integer e such that e divides d_0, e divides d_1, $d_0 \neq e$ and there exists a permutation over $\mathbb{F}_p$ of degree d_1/e.*

Proof. (a) The case where $d_0 = 0$ follows by using Proposition 14.

(b) Suppose f is a permutation polynomial of $\mathbb{F}_p$ of degree d_0 and $d_1 \neq 1$. Let g be a polynomial in $\mathbb{F}_p[x]$ of degree d_1 with no roots in $\mathbb{F}_p$. Such a polynomial always exists, since we may take g to be irreducible of degree d_1. (Note that we cannot find a polynomial in $\mathbb{F}_p[x]$ of degree 1 with no roots). Define (f_0, f_1) by setting

$$f_0 = g(x_1) f(x_0),$$

$$f_1 = x_1.$$

Since $g(x_1)$ is never zero and $f(x_0)$ is a permutation polynomial, (f_0, f_1) is an orthogonal system. It clearly has degree $d_0 + d_1 p$, as required.

(c) This case is similar to the previous one, interchanging the roles of x_0 and x_1.

(d) Suppose that for some e we have that e divides d_0, e divides d_1 and there exists a permutation polynomial f of degree d_0/e. Suppose also that $d_1 \neq e$ so that $d_1/e > 1$. Let g be a polynomial of degree d_1/e with no roots in $\mathbb{F}_p$.

Define (f_0, f_1) by setting

$$f_0 = (g(x_1)\, f(x_0))^e + x_1,$$
$$f_1 = g(x_1)\, f(x_0).$$

We claim that for every b_0, b_1, there is a unique solution (a_0, a_1) to the system $f_i(a_0, a_1) = b_i$. For the first equation becomes $b_0 = b_1^e + a_1$ giving a unique value for a_1. Then since $g(a_1) \neq 0$ and f is a permutation polynomial, there is a unique solution a_0 to the second equation $b_1 = g(a_1)\, f(a_0)$. Hence (f_0, f_1) is an orthogonal system and its degree is clearly $d_0 + d_1 p$.

(e) This case is similar to the previous one. ▮

3.4. *Permutations Over Fields of Low Characteristic*

We now discuss the implications of the constructions presented above for the degrees of permutations over $\mathbb{F}_{p^m}$ when $p = 2$, 3, 5 and 7.

We begin by considering the case $m = 1$. We find, by Corollary 12, that all permutations over $\mathbb{F}_2$ or $\mathbb{F}_3$ have degree 1, permutations over $\mathbb{F}_5$ have degree 1 or 3 and permutations over $\mathbb{F}_7$ have degree 1, 4 or 5. Permutations of all these degrees exist, by Proposition 13 and the fact that $x^4 + 3x$ is a permutation polynomial over $\mathbb{F}_7$.

We now consider the case $m = 2$. We use Proposition 17 to construct permutations of degrees not ruled out by Corollary 12. Tables VI to IX show our results. Row i and column j of the characteristic p table contains an entry corresponding to permutations over $\mathbb{F}_{p^2}$ of degree $ip + j$. If the (i, j)th entry is '-' then degree $ip + j$ cannot occur, by Corollary 12. If the (i, j)th entry is 'a', 'b', 'c', 'd' or 'e', then a permutation of degree $ip + j$ exists, by Proposition 17, Part (a), (b), (c), (d) or (e) respectively. The entry marked '*' corresponds to a special construction for a permutation of degree 23 over $\mathbb{F}_{49}$, which is carried out as follows. Consider the system of equations given by:

$$f_0 = x_1,$$
$$f_1 = x_0^5 + 2x_1^3 x_0^2.$$

This system has degree 23 and is an orthogonal system since the polynomials x^5, $x^5 + 2x^2$ and $x^5 - 2x^2$ are all permutation polynomials over $\mathbb{F}_7$.

TABLE VI

Characteristic 2

	0	1
0	—	—
1	a	—

TABLE VII

Characteristic 3

	0	1	2
0	—	—	—
1	a	—	c
2	a	b	—

TABLE VIII

Characteristic 5

	0	1	2	3	4
0	—	—	—	—	—
1	a	—	c	c	c
2	a	b	—	b	e
3	a	b	c	c	c
4	a	b	d	b	—

TABLE IX

Characteristic 7

	0	1	2	3	4	5	6
0	—	—	—	—	—	—	—
1	a	—	c	c	c	c	c
2	a	b	—	?	b	b	e
3	a	b	*	—	b	b	e
4	a	b	c	c	c	c	c
5	a	b	c	c	c	c	c
6	a	b	d	d	b	b	—

Hence we have constructed a permutation over $\mathbb{F}_{49}$ of degree 23. The final entry in the characteristic 7 table, marked '?', corresponds to an unknown case. This case (degree 17) is not ruled out by Corollary 12, but we have been unable to construct a permutation of this degree.

For fields of characteristic 2, 3 and 5 we have shown that permutations over $\mathbb{F}_{p^2}$ of all degrees not ruled out by Corollary 12 do occur. Hence, by Theorem 16, we have classified the integers d such that a permutation over $\mathbb{F}_{p^m}$ of degree d exists for all positive m, when $p=2$, 3 or 5. We could say the same for the case $p=7$ if we were able to construct a permutation over $\mathbb{F}_{49}$ of degree 17.

4. DE BRUIJN SEQUENCES OF GENERAL SPAN

We begin this section by presenting some non-existence results for span n de Bruijn sequences over $\mathbb{F}_{p^m}$ of certain complexities. These include upper and lower bounds for the linear complexity of such sequences. We show that the upper bound is always tight and devote the rest of the section to the question of whether the lower bound is always achieved.

In Subsection 4.2, we concentrate on span 2 sequences and improve our lower bound for sequences over $\mathbb{F}_p$, showing that our new bound is tight. We also demonstrate, by construction, that our first lower bound is tight for span 2 sequences over $\mathbb{F}_{p^m}$, $m \geqslant 2$. Thus the linear complexity of span 2 de Bruijn sequences behaves quite differently in prime and in non-prime fields. This is similar to the behaviour for permutations highlighted by Proposition 13 and the results of Section 3.4.

In the final subsection, we give a construction for de Bruijn sequences over $\mathbb{F}_{p^m}$, $m \geqslant 2$ and apply it to construct infinite families of de Bruijn sequences of span greater than 2 with minimal linear complexity. Thus we demonstrate that at least in some cases our lower bound is also optimum for spans greater than 2.

4.1. *Non-existence Results*

THEOREM 18. *Let s be a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ such that $c(s)=d+1$. Then there exists an orthogonal system $(f_0, ..., f_{mn-1})$ of degree d such that* $\deg f_i = d-i$ *for all $i \in \{0, 1, ..., n-1\}$.*

Proof. We use s to define an orthogonal system as follows. Let $s^0, ..., s^{m-1}$ be the component sequences of s and suppose, without loss of generality, that $c(s^0)=d+1$. Define, using the notation of Subsection 3.1,

$$f_{i+jn} = \phi_{mn}^{-1}((E-1)^i s^j)$$

where $i = 0, 1, ..., n-1$ and $j = 0, 1, ..., m-1$. Since $c((E-1)^i s^0) = d+1-i$, Theorem 8 implies that $\deg f_i = d - i$ for all $i \in \{0, ..., n-1\}$. Since $c((E-1)^i s^j) \leqslant d+1$ for all $i \in \{0, ..., n-1\}$ and $j \in \{0, ..., m-1\}$, we find that the system $(f_0, ..., f_{mn-1})$ has degree d. It remains to show that $(f_0, ..., f_{mn-1})$ is an orthogonal system.

Let $b_0, ..., b_{mn-1} \in \mathbb{F}_p$. Now the system

$$f_k(a_0, ..., a_{mn-1}) = b_k, \qquad 0 \leqslant k \leqslant mn-1$$

has a solution $(a_0, ..., a_{mn-1})$ if and only if

$$\begin{aligned}((E-1)^i s^j)&_{a_0 + a_1 p + \cdots + a_{mn-1} p^{mn-1}} \\ &= b_{i+jp}, \qquad \text{where} \quad 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant m-1. \end{aligned} \tag{5}$$

For a fixed j, the equations (5) form an invertible linear system in variables $s^j_l, s^j_{l+1}, ..., s^j_{l+n-1}$, where $l = a_0 + a_1 p + \cdots + a_{mn-1} p^{mn-1}$. So (5) can be transformed into the form

$$s^j_{a_0 + a_1 p + \cdots + a_{mn-1} p^{mn-1} + i} = b'_{i+jp} \qquad \text{where} \quad 0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant m-1$$

for some uniquely defined $b'_0, ..., b'_{mn-1}$. This system has a unique solution $(a_0, ..., a_{mn-1}) \in \mathbb{F}_p{}^{mn}$ by the de Bruijn property of s. Hence $(f_0, ..., f_{mn-1})$ is an orthogonal system, as required. ∎

COROLLARY 19. *Suppose that there exists no generalised permutation polynomial over* $\mathbb{F}_p$ *in mn indeterminates of degree* $c-1$. *Then no span n de Bruijn sequence over* $\mathbb{F}_{p^m}$ *of linear complexity* $c, c+1, ..., c+(n-2)$ *or* $c+(n-1)$ *exists.*

In particular, suppose $c - 1 = k \sum_{i=0}^{mn-1} p^i$ *where k is a positive divisor of* $p-1$, *and where* $k > 1$ *if* $mn = 1$. *Then there exists no span n de Bruijn sequence over* $\mathbb{F}_{p^m}$ *with linear complexity* $c, c+1, ..., c+(n-2)$ *or* $c+(n-1)$.

Proof. Theorem 18 asserts that the existence of a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ of linear complexity $d+1$ implies the existence of generalised permutation polynomials of degrees $d, d-1, ..., d-(n-1)$. The first assertion of the Corollary now follows. The last assertion follows from Theorem 11. ∎

Corollary 19 explains the fact that there are no de Bruijn sequences of linear complexity 13 or 14 in Table IV. However, it leaves the gap at linear complexity 12 unexplained.

We now use Theorem 18 to obtain upper and lower bounds on the linear complexity of a de Bruijn sequence.

COROLLARY 20. *Let s be a span n de Bruijn sequence over $\mathbb{F}_{p^m}$. Then*

$$p^{mn-1}+n \leqslant c(s) \leqslant p^{mn}-1$$

unless $p=2$, $m=1$, $n=1$ where $c(s)=2$, or $p=2$, $m=1$, $n=2$ where $c(s)=3$.

Proof. Let s be a span n de Bruijn sequence over $\mathbb{F}_{p^m}$. Theorem 18 states that there exists an orthogonal system $(f_0, ..., f_{mn-1})$ of degree $c(s)-1$ such that $\deg f_i = c(s)-1-i$ when $i=0, 1, ..., n-1$. Clearly, the degree of the orthogonal system can be at most $p^{mn}-1$ and Corollary 12 implies that unless $p=2$ and $m=n=1$, the degree of the system can be at most $p^{mn}-2$. This establishes the upper bound.

To establish the lower bound, first note that the degree of the orthogonal system must be at least p^{mn-1}, so in particular $\deg f_0 \geqslant p^{mn-1}$. This establishes the lower bound when $n=1$, and when $p=2$, $m=1$ and $n=2$. We may therefore assume that $n \geqslant 2$ and that it is not the case that $p=2$, $m=1$ and $n=2$. Suppose that $\deg f_0 = p^{nm-1}+l$, where $l \leqslant n-2$. Then $\deg f_l = p^{mn-1}$ and $\deg f_{l+1} = p^{mn-1}-1$. But now the coefficient of $x_0^{p-1} x_1^{p-1} \cdots x_{mn-1}^{p-1}$ in the reduction of the polynomial $f_l^{p-1} f_{l+1}$ is nonzero. This contradicts Result 10. The contradiction establishes our lower bound. ▌

Corollary 20 can be proved in a more elementary fashion, avoiding the use of Theorem 18, by using a straightforward generalisation of the proof of [4, Corollary 4, Theorems 8 and 9].

It is easy to construct a de Bruijn sequence whose linear complexity meets the upper bound in the above Corollary:

LEMMA 21. *Let s be a maximal-length linear-recurring sequence of period $p^{mn}-1$ over $\mathbb{F}_{p^m}$ generated by a linear recurrence with characteristic polynomial of degree n, primitive over $\mathbb{F}_{p^m}$, and suppose that $s_0 = s_1 = \cdots = s_{n-2} = 0$. Let t denote the span n de Bruijn sequence $[0, s_0, s_1, ..., s_{p^{mn}-2}]$ obtained from s by inserting an extra zero among the first zeros. Then $c(t) = p^{mn}-1$, unless $p=2$, $m=1$ and $n=1$, in which case $c(t)=2$.*

Proof. The proof of this result follows exactly that of [4, Corollary 6], using the fact that the result of [15] used in the proof there was proved over any field. ▌

We know from the Propositions 13 and 14 that a permutation of $\mathbb{F}_{p^m}$ of degree p^{m-1} and linear complexity $p^{m-1}+1$ always exists, so that the lower bound above is tight for span 1 de Bruijn sequences. However the situation is more complicated for general spans. We will investigate this problem in the following subsections.

4.2. *Span 2 de Bruijn Sequences over Prime Fields*

In this subsection we will improve the lower bound of Corollary 20 for span 2 de Bruijn sequences over $\mathbb{F}_p$. We will then give a construction to show that our new bound is in fact tight. The case $p=2$ is covered by Corollary 20. For all other primes, we have:

THEOREM 22. *Suppose s is a span 2 de Bruijn sequence over $\mathbb{F}_p$, p odd. Then*

$$c(s) \geqslant 2p+1.$$

Proof. Let s be a span 2 de Bruijn sequence over $\mathbb{F}_p$. We write

$$S = s_0, s_1, ..., s_{p^2-1}$$

for one period of s. Without loss of generality, we can assume that $s_0 = 0$. By Corollary 20, $p+2 \leqslant c(s) \leqslant p^2-1$. Suppose $p+2 \leqslant c(s) \leqslant 2p$. Then $2 \leqslant c((E-1)^p\, s) \leqslant p$ and $(E-1)^p\, s$ has period p. Defining $x = (E-1)^p\, s$ and writing $X = x_0, x_1, ..., x_{p-1}$ for one period of x and $\hat{S} = s_0, s_1, ..., s_{p-1}$, we have

$$S = \hat{S}, \hat{S}+X, \hat{S}+2X, ..., \hat{S}+(p-1)\, X,$$

since $(E^p-1)\, s = (E-1)^p\, s = x$.

We define

$$d_i = \begin{cases} s_{i+1} - s_i & \text{for} \quad 0 \leqslant i \leqslant p-2, \\ x_0 - s_{p-1} & \text{for} \quad i = p-1 \end{cases}$$

and define

$$e_i = x_{i+1} - x_i \qquad \text{for} \quad 0 \leqslant i \leqslant p-1.$$

In the finite sequence

$$T = (s_0, s_1 - s_0), (s_1, s_2 - s_1), ..., (s_{p^2-1}, s_0 - s_{p^2-1})$$

every ordered pair of elements of $\mathbb{F}_p$ appears exactly once by virtue of the de Bruijn property of s. But T may be written in the form

$$
\begin{aligned}
&(s_0, d_0), (s_1, d_1), ..., (s_{p-1}, d_{p-1})\\
&(s_0+x_0, d_0+e_0), (s_1+x_1, d_1+e_1), ..., (s_{p-1}+x_{p-1}, d_{p-1}+e_{p-1})\\
&(s_0+2x_0, d_0+2e_0), (s_1+2x_1, d_1+2e_1), ..., (s_{p-1}+2x_{p-1}, d_{p-1}+2e_{p-1})\\
&\vdots\\
&(s_0+(p-1)\,x_0, d_0+(p-1)\,e_0), (s_1+(p-1)\,x_1, d_1+(p-1)\,e_1), ...,\\
&(s_{p-1}+(p-1)\,x_{p-1}, d_{p-1}+(p-1)\,e_{p-1}).
\end{aligned}
$$

Note that since s has period p^2, not all the terms of X are zero (for otherwise $c(x)=0$ and $c(s)=p$). In fact no term x_i is zero. For suppose $x_k=0$ and $x_l \neq 0$. Then $s_k, s_{k+p}, ..., s_{k+(p-1)p}$ are all equal but $s_l, s_{l+p}, ..., s_{l+(p-1)p}$ are all distinct, so that some element of $\mathbb{F}_p$ appears more than p times in a period of s. This contradicts the fact that each element of $\mathbb{F}_p$ appears p times in s, a consequence of the de Bruijn property. So there are two terms of X which are equal, say $x_k=x_l$. Since all $2p$ pairs

$$
\begin{gathered}
(s_k, d_k), (s_k+x_k, d_k+e_k), ..., (s_k+(p-1)\,x_k, d_k+(p-1)\,e_k),\\
(s_l, d_l), (s_l+x_l, d_l+e_l), ..., (s_l+(p-1)\,x_l, d_l+(p-1)\,e_l)
\end{gathered}
$$

are distinct we must have $e_k=e_l$. But from this and the fact that $x_k=x_l$ we have $x_{k+1}=x_{l+1}$. Repeatedly applying the argument above, we quickly find that all the x_i's are equal. But then $c(x)=1$ and consequently $c(s)=p+1$, a contradiction. ▮

Construction 23. Let p be an odd prime. We generate a sequence s over $\mathbb{F}_p$ as follows. For $0 \leqslant i, j \leqslant p-1$, we define

$$
s_{jp+i}=\begin{cases} i+\frac{1}{2}(j-1)\,j & \text{for} \quad i \text{ even},\\ i+\frac{1}{2}(j+1)\,j & \text{for} \quad i \text{ odd}\end{cases}
$$

and let $s=[s_0, s_1, ..., s_{p^2-1}]$.

THEOREM 24. *Construction* 23 *generates a span* 2 *de Bruijn sequence of linear complexity* $2p+1$.

Proof. We begin by calculating $c(s)$. We write $t=(E-1)^p\,s=(E^p-1)\,s$ so that for $0 \leqslant i, j \leqslant p-1$,

$$
t_{jp+i}=\begin{cases} j & \text{for} \quad i \text{ even},\\ j+1 & \text{for} \quad i \text{ odd}.\end{cases}
$$

From this it is easy to see that $(E-1)^{2p}\, s=(E^p-1)(E^p-1)\, s$ is equal to the constant sequence $[1]$ of linear complexity 1. By Lemma 4, s has linear complexity $2p+1$.

Next we show that for all $k, d \in \mathbb{F}_p$, $(k, k+d)$ appears as a pair of consecutive elements in s, so that s is a span 2 de Bruijn sequence. We consider a period of s as being built up from p blocks, the elements in the jth block being $s_{jp}, ..., s_{jp+p-1}$. It is easy to check from the definition of s that if i is even, then the difference between s_{jp+i} and s_{jp+i+1} is $1+j$, while if i is odd, the difference is $1-j$ (all arithmetic modulo p). It follows that to find all pairs $(k, k+d)$ in s, we need to show that the elements $s_{(d-1)p+i}$ in block $d-1$ with i even and the elements $s_{(1-d)p+i}$ in block $1-d$ with i odd together comprise $\mathbb{F}_p$. From the definition of s these elements are

$$i+\tfrac{1}{2}(d-2)(d-1) \qquad (\mathrm{mod}\, p), \quad i \text{ even}$$

and

$$i+\tfrac{1}{2}(2-d)(1-d) \qquad (\mathrm{mod}\, p), \quad i \text{ odd.}$$

Clearly these p elements have the desired property and so the theorem is proved. ▌

Note that if p is odd (but not necessarily prime) and all arithmetic is carried out modulo p, then the above method still produces p-ary span 2 de Bruijn sequences.

4.3. *Span 2 de Bruijn Sequences over Non-prime Fields*

From Corollary 20, we already know that the linear complexity of a span 2 de Bruijn sequence over $\mathbb{F}_{p^m}$, $m \geqslant 2$ is at least $p^{2m-1}+2$. We have the following construction and theorem:

Construction 25. Let $m \geqslant 2$ and suppose s is a span 2 de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$. Let T be the following sequence of p^{2m-1} elements:

$$0, 0, ..., 0, 1, 1, ..., 1, ..., p-1, p-1, ..., p-1,$$

consisting of p^{2m-2} copies of each element of $\mathbb{F}_p$. Let A be the sequence of p^{2m-1} elements:

$$0, 1, ..., p-1, 0, 1, ..., p-1, ..., 0, 1, ..., p-1.$$

Furthermore, define

$$v=[T, T+A, T+2A, ..., T+(p-1)\, A],$$

so that v has period p^{2m}. Let w be the sequence of period p^{2m} over $\mathbb{F}_{p^m}$ whose first $m-1$ components are the components of s and whose last component is the sequence v.

Theorem 26. *Sequence w constructed as in Construction 25 is a span 2 de Bruijn sequence over $\mathbb{F}_{p^m}$ with linear complexity $p^{2m-1}+2$.*

Proof. We begin by calculating the linear complexities of the component sequences of w. The first $m-1$ sequences are just the components of s, a sequence of period p^{2m-2}. So these components have linear complexity at most p^{2m-2}. The last component sequence of w is v, and it's easy to see that $(E-1)^{p^{2m-1}} v = [A]$, a sequence of linear complexity 2. Hence $c(v) = p^{2m-1}+2$ and using Result 5, we have $c(s) = p^{2m-1}+2$.

Next we show that w is a span 2 de Bruijn sequence. Let a and b be two arbitrary elements of $\mathbb{F}_{p^m}$. We can write $a = (a_0, a_1)$ and $b = (b_0, b_1)$ where $a_0, b_0 \in \mathbb{F}_{p^{m-1}}$ and $a_1, b_1 \in \mathbb{F}_p$. We will show that a and b appear consecutively as terms in the sequence w. Firstly, since s is a span 2 de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$, there exists a unique j with $0 \leqslant j < p^{2m-2}$ such that $(s_{j+kp^{2m-2}}, s_{j+1+kp^{2m-2}}) = (a_0, b_0)$ for every k. Therefore, we need only show that for some k, we have $(v_{j+kp^{2m-2}}, v_{j+1+kp^{2m-2}}) = (a_1, b_1)$. That this is the case is a simple consequence of the construction of v from T and A. ▮

4.4. *A Construction for de Bruijn Sequences of Minimal Complexity*

Construction 27. Let $m, n \geqslant 2$ and suppose r is a span n de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$. Let s be a maximal-length linear-recurring sequence of period $p^{n-1}-1$ over $\mathbb{F}_p$, with primitive minimal polynomial $f(X) = f_0 + f_1 X + \cdots + f_{n-2} X^{n-2} + X^{n-1}$ of degree $n-1$, and suppose that $s_0 = s_1 = \cdots = s_{n-3} = 0$ and $s_{-1}, s_{n-2} \neq 0$. Define t to be the sequence

$$[0, 0, ..., 0, s_0, s_1, ..., s_{p^{n-1}-2}, ..., s_0, s_1, ..., s_{p^{n-1}-2}]$$

consisting of $p^{(m-1)n}$ zeros followed by $p^{(m-1)n}$ copies of a period of s. Clearly, t has period p^{mn-1}.

Now suppose that $p^{k-1}+1 \leqslant n \leqslant p^k$ and let a be the sequence of period p^k and linear complexity n with $a_{-1} = a_0 = \cdots = a_{n-3} = 0$ and $a_{n-2} = 1$. Thus a satisfies $(E-1)^{n-1} a = [1]$.

Let T be the finite sequence $t_0, t_1, ..., t_{p^{mn-1}-1}$ consisting of the first p^{mn-1} terms of t. Let A be the finite sequence $a_0, a_1, ..., a_{p^{mn-1}-1}$ and define

$$v = [T, T+A, T+2A, ..., T+(p-1)A],$$

so that v has period p^{mn}. Let w be the sequence of period p^{mn} over $\mathbb{F}_{p^m}$ whose first $m-1$ components are the components of r and whose last component is the sequence v.

Lemma 28. *Let sequence t be constructed as in Construction 27. Let V be the vector space of dimension $n-1$ over $\mathbb{F}_p$ in which each vector $(x_0, ..., x_{n-1})$ satisfies the linear equation*

$$f_0 x_0 + f_1 x_1 + \cdots + f_{n-2} x_{n-2} + x_{n-1} = 0.$$

For $0 \leqslant i \leqslant p^{(m-1)n} - 1$, define V_i to be the set of n-tuples

$$\{(t_{i+jp^{(m-1)n}}, t_{i+1+p^{(m-1)n}}, ..., t_{i+n-1+p^{(m-1)n}}), \qquad 0 \leqslant j \leqslant p^{n-1} - 1\}.$$

Then

$$V_i = V, \quad 0 \leqslant i \leqslant p^{(m-1)n} - 2 \text{ and}$$

$$V_{p^{(m-1)n}-1} = V \backslash \{(0, ..., 0, 0), (s_{p^{n-1}-1}, 0, ..., 0, s_{n-2})\}$$
$$\cup \{(0, ..., 0, s_{n-2}), (s_{p^{n-1}-1}, 0, ..., 0, 0)\}.$$

Proof. Suppose $0 \leqslant i \leqslant p^{(m-1)n} - 2$ is fixed. Then because t begins with $p^{(m-1)n}$ zeros and s begins with a further $n-2$ zeros, the n-tuple $(t_i, t_{i+1}, ..., t_{i+n-1})$ is the all-zero vector. Since $\gcd(p^{(m-1)n}, p^{n-1} - 1) = 1$, the $p^{n-1} - 1$ integers

$$i + jp^{(m-1)n}, \qquad 1 \leqslant j \leqslant p^{n-1} - 1$$

are distinct modulo $p^{n-1} - 1$. Moreover, from the construction of t, if $1 \leqslant j \leqslant p^{n-1} - 1$ then the n-tuple $(t_{i+jp^{(m-1)n}}, t_{i+1+p^{(m-1)n}}, ..., t_{i+n-1+p^{(m-1)n}})$ is simply $(s_l, s_{l+1}, ..., s_{l+n-1})$ where $l = i + (j-1)\, p^{(m-1)n} \pmod{p^{n-1} - 1}$. This applies even for $j = p^{n-1} - 1$ because both s and t begin with $n-2$ zeros.

Therefore, the set V_i consists of the all-zero vector together with the $p^{n-1} - 1$ distinct n-tuples from s. Recall that s is generated by a linear recurrence corresponding to the primitive degree $n-1$ polynomial $f(X) = f_0 + f_1 X + \cdots + f_{n-2} X^{n-2} + X^{n-1}$. Thus the n-tuples of V_i are all the vectors that satisfy the linear equation $f_0 x_0 + f_1 x_1 + \cdots + f_{n-2} x_{n-2} + x_{n-1} = 0$ and so $V_i = V$.

Now suppose $i = p^{(m-1)n} - 1$ and consider the n-tuples

$$(t_{i+jp^{(m-1)n}}, t_{i+1+p^{(m-1)n}}, ..., t_{i+n-1+p^{(m-1)n}}), \qquad 0 \leqslant j \leqslant p^{n-1} - 1.$$

We pay special attention to the cases where $j = 0$ and where $j = p^{n-1} - 1$. When $j = 0$, we obtain the tuple $(0, ..., 0, s_{n-2})$ instead of the all-zero vector as previously. When $j = p^{n-1} - 1$, we obtain $(s_{p^{n-1}-1}, 0, ..., 0, 0)$ instead of $(s_{p^{n-1}-1}, 0, ..., 0, s_{n-2})$. For all other j, the argument above still applies and we obtain distinct n-tuples from s. Hence V_i is as in the statement of the lemma and the proof is complete. ∎

THEOREM 29. *Let p be a prime, let n be an integer such that $n \geqslant 2$ and define k to be the unique integer such that $p^{k-1}+1 \leqslant n \leqslant p^k$. Suppose there exists a primitive polynomial f of degree $n-1$ over $\mathbb{F}_p$ with the property that the degree p^k-1 polynomial $f(X)(X-1)^{p^k-n}$ has no zero coefficients. Then sequence w constructed in Construction 27 is a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ with linear complexity $p^{mn-1}+n$.*

Proof. The proof that w has linear complexity $p^{mn-1}+n$ is similar to the calculation in the proof of Theorem 26.

Suppose that $\mathbf{b}=(b_0, b_1, ..., b_{n-1})$ is an n-tuple of elements of $\mathbb{F}_{p^m}$. We aim to show that $\mathbf{b}$ occurs as n consecutive terms in w. We write $b_i=(c_i, d_i)$ where $c_i \in \mathbb{F}_{p^{m-1}}$ and $d_i \in \mathbb{F}_p$. Since r is a span n de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$, there exists an i with $0 \leqslant i < p^{(m-1)n}$ such that $(c_0, c_1, ..., c_{n-1})$ occurs at every position $i+jp^{(m-1)n}$ in r. So it is sufficient to show that $(d_0, d_1, ..., d_{n-1})$ occurs as an n-tuple in v at one of these positions $i+jp^{(m-1)n}$.

Now the n-tuples in t at positions $i+jp^{(m-1)n}$ for $0 \leqslant j \leqslant p^{n-1}-1$ are just the vectors of V_i, as defined in Lemma 28. We claim that the n-tuples in v at positions $i+jp^{(m-1)n}$ for $0 \leqslant j \leqslant p^n-1$ are the vectors

$$V_i + l\mathbf{a}_i, \qquad 0 \leqslant l \leqslant p-1, \tag{6}$$

where $\mathbf{a}_i=(a_i, a_{i+1}, ..., a_{i+n-1})$.

To prove this claim, we need to consider two cases. Firstly, suppose $0 \leqslant i \leqslant p^{(m-1)n}-2$. In this case, the fact that a begins with $n-2$ zeros guarantees that the n-tuples occurring in v at positions $i+jp^{(m-1)n}$, $0 \leqslant j \leqslant p^{n-1}-1$ are the same as those occuring in t at the same positions, i.e. the vectors of V_i. Then from the construction of v and the fact that a has period $p^k \leqslant p^{(m-1)n}$, we see that for $0 \leqslant j \leqslant p^n-1$, the n-tuples of v in positions $i+jp^{(m-1)n}$ are as given in (6). Secondly, consider the case where $i=p^{(m-1)n}-1$. In this case, $\mathbf{a}_i=(0, ..., 0, 1)$ and it is easy to see that the set of n-tuples occuring in v at positions $i+jp^{(m-1)n}$, $0 \leqslant j \leqslant p^{n-1}-1$ is

$$W_i := V_i \backslash \{(s_{p^{n-1}-1}, 0, ..., 0, 0)\} \cup \{(s_{p^{n-1}-1}, 0, ..., 0, 1)\}.$$

Then the n-tuples in v at positions $i+jp^{(m-1)n}$, $0 \leqslant j \leqslant p^n-1$ are just those of the sets $W_i + l\mathbf{a}_i$, $0 \leqslant l \leqslant p-1$. But because $\mathbf{a}_i=(0, ..., 0, 1)$, we have

$$\{W_i + l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\} = \{V_i + l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}$$

and the claim also holds when $i=p^{(m-1)n}-1$.

To prove that $\mathbf{b}$ occurs as an n-tuple of w, it is sufficient to show that the sets of vectors in (6) cover $(\mathbb{F}_p)^n$. We consider two cases. Firstly suppose $0 \leqslant i \leqslant p^{(m-1)n}-2$. Then $V_i=V$ is a vector space of dimension $n-1$, and

TABLE X

Suitable Polynomials over $\mathbb{F}_3$, $\mathbb{F}_5$, and $\mathbb{F}_7$

Span n	Primitive polynomial of degree $n-1$
	Characteristic 3
3	X^2+X+2
4	—
5	—
6	—
7	$X^6+X^5+X^3+2$
8	$X^7+2X^6+X^4+X^2+2X+1$
	Characteristic 5
3	X^2+X+2
4	X^3+3X+2
5	$X^4+X^3+X^2+X+3$
	Characteristic 7
3	X^2+X+3
4	X^3+3X+2
5	X^4+X^2+4X+5

the sets appearing in (6) are just a collection of cosets of V which cover $(\mathbb{F}_p)^n$ if and only if $\mathbf{a}_i \notin V$, or equivalently,

$$a_{i+n-1}+f_{n-2}a_{i+n-2}+\cdots+f_1 a_{i+1}+f_0 a_i \neq 0.$$

In obvious notation, we write this last equation as $f(E)\,\mathbf{a}_i \neq 0$. It is easy to show that if e is the sequence $[0, ..., 0, 1, 0]$ of period p^k, then $a=(E-1)^{p^k-n}\,e$, and $f(E)\,\mathbf{a}_i \neq 0$ if and only if $f(E)(E-1)^{p^k-n}\,\mathbf{e}_i \neq 0$. Here, $\mathbf{e}_i$ denotes the vector $(e_i, e_{i+1}, ..., e_{i+p^k-1})$. This last condition is equivalent to demanding that the coefficient of X^{p^k-2-i} (where exponents are taken modulo p^k) in $f(X)(X-1)^{p^k-n}$ be non-zero. In turn, this holds because of our choice of f.

Secondly, suppose that $i=p^{(m-1)n}-1$. From our choice of a and the fact that a has period $p^k \leqslant p^{(m-1)n}$, we have $\mathbf{a}_i=(0, ..., 0, 1)$. Reasoning as before, $\mathbf{a}_i \notin V$ and the vectors $\{V+l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}$ cover $(\mathbb{F}_p)^n$. So it is sufficient to show that for $i=p^{(m-1)n}-1$ we have

$$\{V_i+l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}=\{V+l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}.$$

In turn, to prove this set equality, it suffices to show that

$$\{(0, ..., 0, 0)+l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}=\{(0, ..., 0, s_{n-2})+l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}$$

and that

$$\{(s_{p^{n-1}-1}, 0, ..., 0, s_{n-2}) + l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\}$$
$$= \{(s_{p^{n-1}-1}, 0, ..., 0, 0) + l\mathbf{a}_i, 0 \leqslant l \leqslant p-1\},$$

all other vectors appearing in V_i also appearing in V and vice-versa. But these two set equalities are obvious in view of the fact that $\mathbf{a}_i = (0, ..., 0, 1)$. ▌

Using the tables of irreducible polynomials in [14], we can use Theorem 29 to construct families of minimal linear complexity de Bruijn sequences. A little thought shows that no suitable polynomial f exists when $n=2$ or when $p=2$. Table X gives, where possible, a degree $n-1$ polynomial with the required properties. A '—' in the table indicates that no polynomial with the required properties exists.

As an example, we can conclude from the first lines of the table that span 3, span 7 and span 8 de Bruijn sequences of linear complexities $3^{3m-1}+3$, $3^{7m-1}+7$ and $3^{8m-1}+8$ respectively exist over every field $\mathbb{F}_{3^m}$, $m \geqslant 2$.

5. CONCLUSION

We have completely characterised the linear complexities of permutations over fields of characteristic 2, 3 and 5. Which linear complexities occur in general? Is it the case that for all primes p, there exists an integer M (depending only on p) such that for all $m \geqslant M$, every integer not ruled out by Corollary 12 occurs as the linear complexity of a permutation over $\mathbb{F}_{p^m}$? Is it even the case that we may take $M=2$ always? (This last statement seems very strong.) In particular, is there a permutation of $\mathbb{F}_{7^2}$ of linear complexity 18?

We have developed upper and lower bounds on the linear complexity of de Bruijn sequences, showing these bounds to be tight in many cases. In particular, over $\mathbb{F}_p$ we showed that the minimum linear complexity of a span 2 de Bruijn sequences is $2p+1$, while over $\mathbb{F}_{p^m}$, $m \geqslant 2$ it is $p^{2m-1}+2$. We also showed that in some cases, the bound $p^{mn-1}+n$ is tight for span n sequences over $\mathbb{F}_{p^m}$, $m \geqslant 2$. From Table V, it is definitely not tight for sequences over $\mathbb{F}_3$. Notice however that this bound is best possible over $\mathbb{F}_2$ [9]. Thus there is an interesting divergence between $\mathbb{F}_2$ and odd prime fields, and between prime fields and non-prime fields. We believe that in general the bound $p^{n-1}+n$ is not tight for $\mathbb{F}_p$ and propose as an open problem the determination of the correct lower bound over $\mathbb{F}_p$. However, we conjecture the following.

Conjecture. Let p be a prime. For every $m \geqslant 2$, the lower bound of $p^{mn-1}+n$ on the linear complexity of a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ is achieved.

There are two reasons for our belief in this conjecture. Firstly, by Theorem 26, the conjecture holds when $n=2$. Secondly, Theorem 29 and Table X provide evidence that the conjecture is true in many other cases. Furthermore, the conjecture is in agreement with our feeling that for de Bruijn sequences, non-prime fields are well behaved in comparison to prime fields.

REFERENCES

1. T. Van Aardenne Ehrenfest and N. G. de Bruijn, Circuits and trees in oriented linear graphs, *in* "Classic papers in Combinatorics" (I. Gessel and G.-C. Rota, Eds.), Birkhäuser, Boston, 1987; reprinted from *Simon Stevin* **28** (1951), 203–217.
2. S. R. Blackburn, A generalization of the discrete Fourier transform: Determining the minimal polynomial of a periodic sequence, *IEEE Trans. Inform. Theory* **40** (1994), 1702–1704.
3. J. A. Bondy and U. S. R. Murty, "Graph Theory with Applications," Elsevier, Amsterdam, 1976.
4. A. H. Chan, R. A. Games, and E. L. Key, On the complexities of de Bruijn sequences, *J. Combin. Theory Ser. A* **33** (1982), 233–246.
5. N. G. de Bruijn, A combinatorial problem, *Proc. Kon. Nederl. Akad. Wetensch.* **49** (1946), 758–764.
6. S. Dolinar, T.-M. Ko, and R. McEliece, Some VLSI decompositions of the de Bruijn graph, *Discrete Math.* **106/107** (1992), 189–198.
7. T. Etzion, On the distribution of de Bruijn sequences of low complexity, *J. Combin. Theory Ser. A* **38** (1985), 241–253.
8. T. Etzion and A. Lempel, On the distribution of de Bruijn sequences of given complexity, *IEEE Trans. Inform. Theory* **30** (1984), 611–614.
9. T. Etzion and A. Lempel, Construction of de Bruijn sequences of minimal complexity, *IEEE Trans. Inform. Theory* **30** (1984), 705–709.
10. H. Fredricksen, A survey of full length shift register cycle algorithms, *SIAM Rev.* **24** (1982), 195–221.
11. R. A. Games, There are no de Bruijn sequences of span n with complexity $2^{n-1}+n+1$, *J. Combin. Theory Ser. A* **34** (1983), 248–251.
12. S. W. Golomb, "Shift Register Sequences," Holden–Day, San Francisco, 1967.
13. C. G. Günther, Alternating step generators controlled by de Bruijn sequences, *in* "Proceedings of EUROCRYPT '87" (D. Chaum and W. L. Price, Eds.), Lecture Notes in Computer Science, Vol. 304, Springer-Verlag, Berlin, 1988.
14. R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison–Wesley, London, 1983.
15. J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Inform. Theory* **15** (1969), 122–127.
16. K. G. Paterson, Perfect factors in the de Bruijn graph, *Designs, Codes and Cryptogr.* **5** (1995), 115–138.