Journal of Combinatorial Theory, Series A **86**, 127–139 (1999)
Article ID jcta.1998.2920, available online at http://www.idealibrary.com on IDEAL®

On the Minimum Linear Complexity of de Bruijn Sequences over Non-prime Finite Fields

Peter A. Hines

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

Communicated by the Managing Editors

Received December 18, 1997

It has been conjectured that over any non-prime finite field $\mathbb{F}_{p^m}$ and for any positive integer n, there exists a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ which has the minimum possible linear complexity $p^{nm-1}+n$. We give a proof by construction that this conjecture is true.

1. INTRODUCTION

In this paper we continue the study of the linear complexity of de Bruijn sequences over finite fields. Our aim is to establish the integer values of linear complexity for which there exist de Bruijn sequences of given span over arbitrary finite fields. The first, and perhaps most important objective is to establish maximum and minimum values. This has intrinsic combinatorial interest; and is also of relevance in applications where linear complexity is a consideration.

It is known that the maximum possible linear complexity of a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ is $p^{nm}-1$, and that such a sequence may be constructed in a straightforward manner (a Linear Feedback Shift Register m-sequence with an extra zero added to the run of $m-1$ zeroes will produce such a sequence) [1, 2].

The situation regarding the minimum linear complexity has proved more complex. In 1982 Chan, Games and Key [2] showed that the linear complexity of a span n de Bruijn sequence over $\mathbb{F}_2$ was not less than $2^{n-1}+n$ but did not show whether this bound was realized for $n>6$. In 1984 Etzion and Lempel [5] showed that this minimum was always realised and gave a recursive construction for sequences with these parameters.

0097-3165/99 $30.00

In 1996 the lower bound over $\mathbb{F}_2$ of $2^{n-1}+n$ was generalised to any finite field $\mathbb{F}_{p^m}$ by Blackburn, Etzion and Paterson [1] who showed that the linear complexity was never less than $p^{mn-1}+n$. On the question of whether this bound is ever realised, and under what circumstances, they gave partial solutions. For odd p, when $m=1$ (i.e., prime fields) they showed that, for $n=2$, the bound is *not* realized. The actual bound is $2p+1$. When $n=3$ they found by computer search that in the case $p=3$ the bound $3^2+3=12$ is not realized (Table V of [1] shows that the minimum linear complexity is 17). It may be that, for odd prime fields, a better minimum is yet to be found. However, this appeared to them not to be the case for non-prime fields. They showed that for $m \geqslant 2$ the lower bound $p^{nm-1}+n$ is realised for some n including $n=2$ (Theorems 26 and 29 of [1]) and they conjectured that over non-prime fields the lower bound is *always* realised.

In this paper we show that this conjecture is true.

Our proof is by construction. To construct a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ of minimal linear complexity, we begin by taking an arbitrary span n de Bruijn sequence s over $\mathbb{F}_{p^{m-1}}$ and "extend" it into a span n de Bruijn sequence over $\mathbb{F}_{p^m}$. Firstly we take p^n copies of s to form a sequence of length p^{nm} in which every n-tuple of elements occurs p^n times. Because s is a sequence over $\mathbb{F}_{p^{m-1}}$, its terms may be regarded as $(m-1)$-tuples in $(\mathbb{F}_p)^{m-1}$. Next we construct a new sequence s' over $\mathbb{F}_p$, also of length p^{nm}. Each term of s' is used to augment the corresponding $(m-1)$-tuple of s to form an m-tuple. The sequence s'' of m-tuples, which may be regarded as a sequence over $\mathbb{F}_{p^m}$, is shown to be a span n de Bruijn sequence. If we also show that the linear complexity of s'' is $p^{nm-1}+n$ then the proof is complete. We do this by using the result that the linear complexity of s'' is equal to the maximum linear complexity among its *component sequences* (the m sequences over $\mathbb{F}_p$ formed from the 1st, 2nd, ..., mth entries in the m-tuples of which s is composed). Of the m component sequences, the first $m-1$ are also component sequences of the original sequence s; and because s is a sequence of period $p^{n(m-1)}$ its linear complexity—and hence the linear complexity of all its component sequences—cannot exceed p^{nm-n}. The linear complexity of the newly-constructed s' is $p^{nm-1}+n$ by construction. So the linear complexity of s'' is $p^{nm-1}+n$; being the maximum among the component sequences.

Clearly the key step is the construction of s'. We use the established equivalence between sequences whose period is a power of p and whose linear complexity is $d+1$; and certain polynomials over $\mathbb{F}_p$ of degree d (with "degree" suitably defined—see Definition 8). We construct a polynomial of degree $p^{nm-1}+n-1$, and show that its corresponding sequence s' extends *any* span n de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$ to a span n de Bruijn sequence over $\mathbb{F}_{p^m}$. A numerical example follows the proof of the main theorem and illustrates the construction in detail.

2. BACKGROUND

We summarise below the Definitions and Results necessary to this work.

DEFINITION 1. A sequence $s = ..., s_{-1}, s_0, s_1, ...$ is said to be *periodic* if there exists a non-zero integer t such that $s_i = s_{i+t}$ for every integer i. The *period* of s is defined to be the least positive such t.

DEFINITION 2. A sequence s over $\mathbb{F}_{p^m}$ is a *span n de Bruijn sequence* if it has period p^{mn} and the n-tuples $(s_i, s_{i+1}, ..., s_{i+n-1})$, where $0 \leqslant i < p^{mn}$, are distinct.

DEFINITION 3. The left shift operator E acts on a sequence s ($= ..., s_{-1}, s_0, s_1 ...$) to produce the sequence Es, defined to be the sequence whose ith term is s_{i+1} [1, p. 57]. The action of E is linear given that addition of sequences is componentwise addition; and so $(E-1)$ acts on s to produce the sequence $(E-1)s = Es - s$ whose ith term is $s_{i+1} - s_i$.

DEFINITION 4. 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:

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

that is, *a linear recurrence relation of degree n*. This may be written

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

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

Result 1 [7, Theorem 8.42, p. 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 5. 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.

Result 2 [1, Proposition 2]. Let s be a sequence over $\mathbb{F}_p$ whose period is a power of p. Then s satisfies a linear recurrence with minimal polynomial $(X-1)^{c(s)}$. One important consequence is that the sequence $(E-1)s$ has linear complexity $c(s)-1$.

DEFINITION 6. Let s be a sequence over $\mathbb{F}_{p^m}$ whose period is a power of p. Regarding $\mathbb{F}_{p^m}$ as a vector space over $\mathbb{F}_p$, we can represent each term s_r

of such a sequence by an m-tuple $(s_r^{(0)}, ..., s_r^{(m-1)})$ of elements of $\mathbb{F}_p$. For each $j = 0, ..., m-1$, we call the sequence

$$s^{(j)} = ..., s_{-1}^{(j)}, s_0^{(j)}, s_1^{(j)}, ...$$

the jth *component sequence* of s. Moreover, $c(s) = \max\{c(s^{(j)}): 0 \leqslant j \leqslant m-1\}$ [8].

DEFINITION 7. The set of polynomials in $\mathbb{F}_p[x_0, ..., x_{k-1}]$ of degree strictly less than p in each indeterminate is denoted P_k.

We now define the degree of polynomials in more than one indeterminate in a manner which permits the link with linear complexity. This differs from the usual definition [7] in which the different indeterminates are given equal weight.

Any integer $i \in \{0, ..., p^k - 1\}$ can be written in base p as $i = \sum_{j=0}^{k-1} i_j p^j$ where $i_j \in \{0, ..., p-1\}$ for $j = 0, ..., k-1$. We define $x^i \in p_k$ 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

$$f = \sum_{i=0}^{p^k - 1} a_i x^i \qquad \text{where} \quad a_i \in \mathbb{F}_p.$$

DEFINITION 8. We define the *degree* of f to be $\deg(f) = \max\{i: a_i \neq 0\}$ (or -1 if all $a_i = 0$).

Result 3. Let P_k be as defined in Definition 7. Now let S_k denote the set of all sequences of elements in $\mathbb{F}_p$ whose period divides p^k. We exhibit an important correspondence between P_k and S_k. For $r \in \{0, ..., p^k - 1\}$, suppose $r = \sum_{j=0}^{k-1} r_j p^j$. Define a map $\phi_k: P_k \to S_k$ by setting

$$\phi_k f = s(= ..., s_{-1}, s_0, s_1, ...) \qquad \text{where} \qquad s_r = f(r_0, ..., r_{k-1}).$$

Then (i) ϕ_k is a linear bijective map; and (ii) the degree of f is d if and only if the linear complexity of $\phi_k f$ is $d+1$ [1, Theorem 8].

Result 3 is central to the proof of our main theorem. Given a polynomial f, we refer to its corresponding sequence $\phi_k f$, and vice versa. It is possible to define sequences very simply in terms of polynomials; and their linear complexity is immediately apparent from the degree. Conversely, properties of certain polynomials are proved by operations on the corresponding sequences.

In order to exploit the correspondence between certain sequences and certain polynomials, we need a polynomial equivalent to the de Bruijn property. Accordingly we define an "orthogonal system" of polynomials in P_k. The system acts on each k-tuple $(r_0, ..., r_{k-1})$ in $(\mathbb{F}_p)^k$ to produce a k-tuple $(c_0, ..., c_{k-1})$. The system is orthogonal if and only if this action permutes the elements of $(\mathbb{F}_p)^k$.

DEFINITION 9. If $f_0, f_1, ..., f_{k-1} \in P_k$, we call $\{f_0, f_1, ..., f_{k-1}\}$ a (complete) *orthogonal system* if for each $(c_0, c_1, ..., c_{k-1}) \in (\mathbb{F}_p)^k$, there exists a unique $(r_0, ..., r_{k-1}) \in (\mathbb{F}_p)^k$ such that

$$f_i(r_0, ..., r_{k-1}) = c_i \qquad \text{for all} \quad i \in \{0, 1, ..., k-1\}.$$

We define the degree of an orthogonal system to be $\max\{\deg(f_i)\colon 0 \leqslant i \leqslant k-1\}$. It is clear that, for each $i \in \{0, ..., k-1\}$, at least one polynomial in the orthogonal system is explicit in the indeterminate x_i. In particular at least one polynomial is explicit in x_{k-1} so the degree of the system is at least p^{k-1}.

3. NEW NOTATION

DEFINITION 10. The *difference operator* Δ acts on the polynomials in P_k. If $f \in P_k$ then $\Delta f = \phi_k^{-1}(E-1)\,\phi_k f$. So the action of Δ on f corresponds to the action of $(E-1)$ on the sequence $\phi_k f$.

LEMMA 1. *We note the following properties of* Δ *which are required later*:

1. *The action of* Δ *is linear.*

2. *If* $f \in P_k$ *then* $\phi_k[(1+\Delta)\,f] = E(\phi_k f)$; *i.e., the sequence corresponding to* $(1+\Delta)\,f$ *is the the sequence corresponding to* f *left-shifted one place.*

3. *If* $f \in P_k$ *is not the zero polynomial then* $\deg(\Delta f) = \deg(f) - 1$.

Outline Proof. 1. Both E and ϕ_k are linear.

2. Follows from linearity of Δ.

3. By Result 3 the degree of a polynomial is always one less than the linear complexity of the corresponding sequence. By Result 2 the action of $E-1$ reduces the linear complexity by one, so the action of Δ reduces the degree of the corresponding polynomial by one.

DEFINITION 11. Suppose f is a non-constant polynomial in P_s. Given some $k \leqslant s$ and $(r_0, ..., r_{k-1}) \in (\mathbb{F}_p)^k$ we write $[f]_{(r_0, ..., r_{k-1})}$ to denote the polynomial $f(r_0, ..., r_{k-1}, x_k, ..., x_{s-1})$ obtained from f by setting $x_j = r_j$ for $j = 0, ..., k-1$. We call this the *evaluation of f at* $(r_0, ..., r_{k-1})$.

The sequence interpretation of $[f]_{(r_0, ..., r_{k-1})}$ is important in the proof of the main theorem. Since $f \in P_s$ there exists some integer $i \leqslant s$ such that $f \in P_i$ but $f \notin P_{i-1}$; i.e., f is explicit in the indeterminate x_{i-1} but in no indeterminate of higher subscript. So the sequence corresponding to f has period p^i. We now consider the two cases according to whether i exceeds k or not. Suppose first that $i \leqslant k$. Then

$$[f]_{(r_0, ..., r_{k-1})} = f(r_0, ..., r_{i-1}) = c \in \mathbb{F}_p$$

where c is a constant. In this case the sequence interpretation of $[f]_{(r_0, ..., r_{k-1})}$ is simply a sequence all of whose terms are c and whose period is therefore 1.

Suppose now that $i > k$. The sequence corresponding to f has period p^i, and one complete period may be thought of as comprising p^{i-k} blocks of size p^k each. Given $(r_0, ..., r_{k-1})$ we set $r = \sum_{j=0}^{k-1} r_j p^j$ so that $0 \leqslant r \leqslant p^k - 1$. We may think of r as a position marker within each block of size p^k. Each different value of $(x_k, ..., x_{i-1})$ will determine a different block of size p^k; and the values $x_j = r_j$ for $j = 0, 1, ..., k-1$ determine the rth term within each block. So the sequence corresponding to $[f]_{(r_0, ..., r_{k-1})}$ is obtained from the sequence corresponding to f by replacing *every* element in each block of size p^k by a copy of the rth element of that block.

4. THE DE BRUIJN PROPERTY

In this section we establish the polynomial equivalent to the de Bruijn property. For this we need the concept of an *orthogonal system* of polynomials from Definition 9.

To show that a system is orthogonal it is sufficient to show that for each $(c_0, ..., c_{k-1})$ in $(\mathbb{F}_p)^k$ there is *at most* one solution $(r_0, ..., r_{k-1}) \in (\mathbb{F}_p)^k$ such that $f_i(r_0, ..., r_{k-1}) = c_i$ for $i = 0, ..., k-1$. Existence follows by the pigeonhole principle.

THEOREM 1. *There is a bijection between the set of span n de Bruijn sequences over* $\mathbb{F}_{p^m}$ *of linear complexity* $d+1$ *and the set of orthogonal systems of degree d of the form*

$$OS = \{\Delta^i f_j : i = 0, ..., n-1;\ j = 0, ..., m-1\}$$

where the f_j*s are polynomials in* P_{nm}.

Proof. The proof that, given a span n de Bruijn sequence over $\mathbb{F}_{p^m}$ of linear complexity $d+1$, there corresponds an orthogonal system of degree d of the form OS is given in Theorem 18 of [1]. We shall prove the converse.

Let $f_0, ..., f_{m-1}$ be polynomials in P_{nm} such that OS is an orthogonal system of degree d.

Since $\deg(\Delta^i f_j) < \deg(f_j)$ for $i \in \{1, ..., n-1\}$ we may suppose, without loss of generality, $\deg(f_{m-1}) = d$ and $\deg(f_j) \leqslant d$ for $j \in \{0, ..., m-2\}$.

For $j = 0, ..., m-1$ let $s^{(j)} = \phi_{nm} f_j$. Each $s^{(j)}$ has linear complexity not exceeding $d+1$ and a period which divides p^{nm}. Moreover $s^{(m-1)}$ itself has linear complexity $d+1$ and period precisely p^{nm} (because $p^{nm-1} <$ linear complexity $<$ period $\leqslant p^{nm}$). Let s be the sequence over $\mathbb{F}_{p^m}$ whose jth component sequence (Definition 6) is $s^{(j)}$ for $j = 0, ..., m-1$. Then s has period p^{nm} and linear complexity $d+1$.

We now show that s is a span n de Bruijn sequence over $\mathbb{F}_{p^m}$; i.e., we show that every n-tuple of elements of $\mathbb{F}_{p^m}$ occurs once as n consecutive terms of s. Let $(c_0, ..., c_{n-1})$ be an n-tuple in $(\mathbb{F}_{p^m})^n$ where, for $i \in \{0, ..., n-1\}$, we have $c_i = (c_{i,0}, ..., c_{i,m-1})$ with $c_{i,j} \in \mathbb{F}_p$ for $j \in \{0, ..., m-1\}$. For each j we may form the n-tuple $c'_j = (c_{0,j}, ..., c_{n-1,j})$. [We may visualise the c_is as the row vectors of a matrix $C = (c_{i,j})$ and the c'_js as the column vectors.]

The proof will be completed if it is shown there is a unique $r = \sum_{t=0}^{nm-1} r_t p^t$ such that, for each $j \in \{0, ..., m-1\}$, the jth component sequence $s^{(j)}$ has the n terms of c'_j as consecutive elements commencing with $(s^{(j)})_r$; i.e., if there is a unique r such that

$$(s^{(j)})_{r+i} = c_{i,j} \qquad \text{for all} \quad i \in \{0, ..., n-1\}, \quad j \in \{0, ..., m-1\}. \tag{1}$$

To see that there is a unique r satisfying equations (1) we write them in equivalent form

$$(E^i s^{(j)})_r = c_{i,j} \qquad \text{for all} \quad i \in \{0, ..., n-1\}, \quad j \in \{0, ..., m-1\}.$$

which is equivalent to $((E-1)^i s^{(j)})_r = \sum_{t=0}^{i} \binom{i}{t} (-1)^t c_{t,j}$ by elementary operations. The corresponding polynomial expression is

$$\Delta^i f_j(r_0, ..., r_{p^{nm}-1}) = \sum_{t=0}^{i} \binom{i}{t} (-1)^t c_{t,j}. \tag{2}$$

The system of equations (2) does indeed have a unique solution $r_0, ..., r_{nm-1}$ because OS is an orthogonal system. So the equations (1) have a unique solution, and s is a span n de Bruijn sequence. ∎

5. BASIS POLYNOMIALS

We introduce a family of polynomials which are used in the main construction.

DEFINITION 12. If s is a sequence over $\mathbb{F}_p$ whose period is a power of p and whose linear complexity is $d+1$ it satisfies a linear recurrence with minimal polynomial $(X-1)^{d+1}$ (Result 1). So it is uniquely determined by its first $d+1$ terms. Thus there is precisely one sequence whose period is a power of p and whose linear complexity is $d+1$ which begins with d zeroes followed by a one. The corresponding polynomial in P_k of degree d is called the dth *basis polynomial* and is denoted g_d. For completeness we define $g_0 = 1$ and $g_{-d} = 0$.

The main properties of the basis polynomials are summarized in the following:

LEMMA 2. *For all non-negative integers d and i,*

1. $\Delta^i g_d = g_{d-i}$.
2. $g_{p^i} = x_i$.
3. $g_{p^i+j} = g_{p^i} g_j$ *whenever* $j < p^i$.

Proof. 1. The sequence $\phi_k g_d$ corresponding to g_d has linear complexity $d+1$ and begins with d zeroes followed by one. So $(E-1)^i \phi_k g_d$ has linear complexity $d+1-i$ and must commence with $d-i$ zeroes followed by one. But $\phi_k g_{d-i}$ is the unique sequence of linear complexity $d+1-i$ which begins in this way, so $(E-1)^i \phi_k g_d = \phi_k g_{d-i}$ whence $\Delta^i g_d = g_{d-i}$.

2. Set $h = x_i - g_{p^i}$. Since $\deg(x_i) = \deg(g_{p^i}) = p^i$ it follows that $\deg(h) \leqslant p^i$. The sequence corresponding to x_i begins with p^i zeroes followed by p^i ones, so the first p^i+1 terms of $\phi_k x_i$ and $\phi_k g_{p^i}$ are the same, i.e., the first p^i+1 terms of h are 0. This is only possible if h is the zero polynomial, and so $g_{p^i} = x_i$.

3. By (2) $g_{p^i} g_j = x_i g_j$. The sequence corresponding to x_i has period p^{i+1} and begins with p^i zeroes followed by p^i ones. The sequence corresponding to g_j has a period which divides p^i (since $j < p^i$). So the sequence corresponding to $x_i g_j$ begins with p^i zeroes (because $x_i = 0$) followed by j zeroes (because $x_i = 1$ but $g_j = 0$) followed by a one (because $x_i = g_j = 1$). Thus g_{p^i+j} and $g_{p^i} g_j$ have their first $p^i + j + 1$ terms the same. Since both have degree $p^i + j$ they are identical. ∎

6. THE MAIN RESULT

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

Proof. By Theorem 1 the result will follow if we show there exist m polynomials $f_j \in P_{nm}$ such that $\{\Delta^i f_j : i=0, ..., n-1;\ j=0, ..., m-1\}$ is an orthogonal system of degree $p^{nm-1}+n-1$.

For ease of notation we set $k=n(m-1)$.

Let s be any span n de Bruijn sequence over $\mathbb{F}_{p^{m-1}}$. Then by Theorem 1 there exist polynomials $f_j \in P_k$ such that $OS(k)=\{\Delta^i f_j : i=0, ..., n-1;\ j=0, ..., m-2\}$ is an orthogonal system. The degree of the system does not exceed p^k-1 because the period of s, and hence the linear complexity of s, does not exceed p^k.

The principle of the proof is to extend $OS(k)$ in P_k to an orthogonal system $OS(k+n)$ in P_{k+n} of degree $p^{k+n-1}+n-1$. We construct a new polynomial $f_{m-1} \in P_{k+n}$ of degree $p^{k+n-1}+n-1$ and such that $OS(k+n)=\{\Delta^i f_j : i=0, ..., n-1;\ j=0, ..., m-1\}$ is an orthogonal system.

Construction. Let $f_{m-1}=\sum_{j=0}^{n-1} g_{p^{k+j}+j}$ where the $g_{p^{k+j}+j}$'s are Basis Polynomials.

Clearly, the degree of f_{m-1} is $p^{k+n-1}+n-1$. Since this exceeds the degree of $f_0, ..., f_{m-2}$ it will be the degree of the system $OS(k+n)$.

We now show that $OS(k+n)$ is an orthogonal system in P_{nm}. So let $(c_0, ..., c_{k+n-1}) \in (\mathbb{F}_p)^{k+n}$. We will show there is at most one solution $(r_0, ..., r_{k+n-1}) \in (\mathbb{F}_p)^{k+n}$ such that $[\Delta^i f_j]_{(r_0, ..., r_{k+n-1})} = c_{nj+i}$ for $i=0, ..., n-1;\ j=0, ..., m-1$.

We show this result inductively; i.e., if $r_0, ..., r_{k+i-1}$ are uniquely determined by $c_0, ..., c_{k+n-1}$ then so too is r_{k+i}.

The base of the induction is that $(r_0, ..., r_{k-1})$ are uniquely determined by $c_0, ..., c_{k+n-1}$ because $OS(k)$ is an orthogonal system.

For the inductive step, suppose that for some particular $i \in \{0, ..., n-1\}$ we have $(r_0, ..., r_{k+i-1})$ uniquely determined in terms of $c_0, ..., c_{k+n-1}$. We will show that r_{k+i} is uniquely determined. Set $r=\sum_{j=0}^{k+i-1} r_j p^j$. Now define

$$I_i=[(1+\Delta)^{p^{k+i}-r}\,\Delta^i f_{m-1}]_{(r_0, ..., r_{k+i-1})}.$$

We will analyse I_i in two ways.

Firstly, we set $A_{i,j}=[(1+\Delta)^{p^{k+i}-r}\, g_{p^{k+j}+j-i}]_{(r_0, ..., r_{k+i-1})}$; then from the definition of f_{m-1} we have

$$I_i = \sum_{j=0}^{n-1} [(1+\Delta)^{p^{k+i}-r} \Delta^i g_{p^{k+j}+j}]_{(r_0, \ldots, r_{k+i-1})}$$

$$= \sum_{j=0}^{n-1} [(1+\Delta)^{p^{k+i}-r} g_{p^{k+j}+j-i}]_{(r_0, \ldots, r_{k+i-1})}$$

$$= \sum_{j=0}^{n-1} A_{i,j}.$$

We claim that for $i, j \in \{0, \ldots, n-1\}$ we have

$$A_{i,j} = \begin{cases} 0 & \text{if } j \neq i \\ x_{k+i}+1 & \text{if } j = i \end{cases}$$

and that, consequently, $I_i = x_{k+i}+1$.

Proof of Claim. The rather daunting-looking expression represented by $A_{i,j}$ may be simplified by considering the corresponding sequences. We consider the sequence corresponding to $(1+\Delta)^{p^{k+i}-r} g_{p^{k+j}+j-i}$ and evaluate it at the rth point in each block of size p^{k+i} (that is, we obtain a new sequence by replacing each block of size p^{k+i} with p^{k+i} copies of the rth term in the block—see Definition 11). But what is the rth term in each block? Given blocks of size p^{k+i}, a left shift of $p^{k+i}-r$ will move the 0th term of a block to the rth position in the block to the left. So the rth term in each block of the sequence corresponding to $(1+\Delta)^{p^{k+i}-r} g_{p^{k+j}+j-i}$ is simply the 0th term of the block to the right in the sequence corresponding to $g_{p^{k+j}+j-i}$. In short, then, to form the sequence corresponding to $A_{i,j}$ we take the sequence associated with the Basis Polynomial $g_{p^{k+j}+j-i}$ and replace each block of size p^{k+i} by p^{k+i} copies of the 0th term of the next block. The outcome will depend on the size of j relative to i.

If $j < i$ the period of $g_{p^{k+j}+j-i}$ is a proper divisor of p^{k+i}. So a block of size p^{k+i} is made up of multiple complete periods of the sequence corresponding to $g_{p^{k+j}+j-i}$. So the 0th term of every block of size p^{k+i} must also be the 0th term of $g_{p^{k+j}+j-i}$ itself. This is 0 because $g_{p^{k+j}+j-i} \neq g_0$ (because $p^{k+j}+j-i > p^{k+j}-n \geqslant p^k - k > 0$). Thus the sequence corresponding to $A_{i,j}$ is the all-zero sequence, so $A_{i,j}$ is the zero polynomial.

If $j > i$ then $g_{p^{k+j}+j-i} = x_{k+j} g_{j-i}$ (by Lemma 2). Now $j-i < n < p^k$ so the period of the sequence corresponding to g_{j-i} divides p^{k+i}. Hence the first $j-i$ terms of each block of size p^{k+i}, being multiples of the first $j-i$ terms of g_{j-i}, are 0. Once again $A_{i,j}$ corresponds to the all-zero sequence, and so must be the zero polynomial.

If $j = i$ then $A_{i,j}$ simplifies greatly:

$$[(1+\Delta)^{p^{k+i}-r}\, g_{p^{k+j}+j-i}]_{(r_0,\ldots,r_{k+i-1})} = [(1+\Delta)^{p^{k+i}-r}\, g_{p^{k+i}}]_{(r_0,\ldots,r_{k+i-1})}$$
$$= [(1+\Delta)^{p^{k+i}-r}\, x_{k+i}]_{(r_0,\ldots,r_{k+i-1})}.$$

The sequence corresponding to x_{k+i} consists of p blocks of size p^{k+i} each, in which every element in the tth block (for $t = 0, \ldots, p-1$) is t. After shifting and evaluating as described above every element in the tth block is replaced by a copy of the 0th term in the next block, i.e., by $t+1$. So $A_{i,i}$ corresponds to the sequence of p blocks of size p^{k+i} in which every element in the tth block is $t+1$. The unique polynomial in P_{nm} which corresponds to this sequence is $x_{k+i}+1$. ∎

We now analyse I_i in a different way and show that it is uniquely determined in terms of $c_0, \ldots, c_{k+n-1}$. By equating the two expressions for I_i, we find that there is at most one possible value for x_{k+i}, i.e., r_{k+i} is uniquely determined in terms of $c_0, \ldots, c_{k+n-1}$.

$$\begin{aligned}
I_i &= [(1+\Delta)^{p^{k+i}-r}\, \Delta^i f_{m-1}]_{(r_0,\ldots,r_{k+i-1})} \\
&= \sum_{s=0}^{p^{k+i}-r} \binom{p^{k+i}-r}{s} [\Delta^{i+s} f_{m-1}]_{(r_0,\ldots,r_{k+i-1})} \\
&= \sum_{s=0}^{n-i-1} \binom{p^{k+i}-r}{s} [\Delta^{i+s} f_{m-1}]_{(r_0,\ldots,r_{k+i-1})} \\
&\quad + \sum_{s=n-i}^{p^{k+i}-r} \binom{p^{k+i}-r}{s} [\Delta^{i+s} f_{m-1}]_{(r_0,\ldots,r_{k+i-1})} \\
&= \sum_{s=0}^{n-i-1} \binom{p^{k+i}-r}{s} c_{k+i+s} \\
&\quad + \sum_{s=n-i}^{p^{k+i}-r} \binom{p^{k+i}-r}{s} \sum_{j=0}^{n-1} [\Delta^{i+s} g_{p^{k+j}+j}]_{(r_0,\ldots,r_{k+i-1})} \\
&= K_1(i) + \sum_{s=n-i}^{p^{k+i}-r} \sum_{j=0}^{n-1} \binom{p^{k+i}-r}{s} [g_{p^{k+j}+j-i-s}]_{(r_0,\ldots,r_{k+i-1})},
\end{aligned}$$

where $K_1(i)$ is uniquely determined in terms of i and $c_0, \ldots, c_{k+n-1}$.

We consider the polynomials $[g_{p^{k+j}+j-i-s}]_{(r_0,\ldots,r_{k+i-1})}$ for $s \in \{n-i, \ldots, p^{k+i}-r\}$ and $j \in \{0, \ldots, n-1\}$ and claim that

$$[g_{p^{k+j}+j-i-s}]_{(r_0,\ldots,r_{k+i-1})}=\begin{cases}0 & \text{if } j>i\\ 0 & \text{if } j\leqslant i \text{ and } p^{k+j}+j-i<s\leqslant p^{k+i}-r\\ K_2(i,j,s) & \\ & \text{if } j\leqslant i \text{ and } n-i\leqslant s\leqslant p^{k+j}+j-i\end{cases}$$

where $K_2(i, j, s)$ is uniquely determined in terms of i, j, s and $c_0, \ldots, c_{k+n-1}$.

Proof of Claim. Suppose $j>i$. Because $s\geqslant n-i$ and $j<n$ it follows that $j-i-s<0$. So $p^{k+j}+j-i-s<p^{k+j}$. However $s\leqslant p^{k+i}\leqslant p^{k+j-1}$ so $p^{k+j}+j-i-s>p^{k+j}-p^{k+j-1}\geqslant p^{k+j-1}$; and so the period of the sequence corresponding to $g_{p^{k+j}+j-i-s}$ is precisely p^{k+j}. This sequence therefore comprises $p^{k+j}-(s-(j-i))$ zeroes followed by $s-(j-i)$ terms which may be non-zero. But $s-(j-i)\leqslant s-1\leqslant p^{k+i}-(r+1)$, so the number of non-zero terms in a complete period is at most $p^{k+i}-(r+1)$. Thus, the complete period p^{k+j} comprises p^{j-i} blocks of size p^{k+i} each, and all these blocks except the last consist entirely of zeroes, and the last begins with at least $r+1$ zeroes. Thus the rth element of *every* block of size p^{k+i} is zero and so $[g_{p^{k+j}+j-i-s}]_{(r_0,\ldots,r_{k+i-1})}=0$.

Suppose now $j\leqslant i$. Then if $s>p^{k+j}+j-i$ we have $g_{p^{k+j}+j-i-s}=g_{-d}=0$.

If $j\leqslant i$ and $s\leqslant p^{k+j}+j-i$ then the period of the sequence corresponding to $g_{p^{k+j}+j-i-s}$ divides p^{k+j} and so divides p^{k+i}. Therefore $g_{p^{k+j}+j-i-s}\in P_{k+i}$. By the inductive hypothesis $[g_{p^{k+j}+j-i-s}]_{(r_0,\ldots,r_{k+i-1})}$ is uniquely determined. ∎

This completes the inductive step, and hence the proof that $OS(k+n)=\{\Delta^i f_j: i=0, \ldots, n-1;\ j=0, \ldots, m-1\}$ is a complete orthogonal system of degree $p^{nm-1}+n-1$, and so completes the proof of the theorem. ∎

EXAMPLE. To illustrate the method we give a numerical example. Let $p=3$ and $n=m=2$. We will construct s'', a span 2 de Bruijn sequence over $\mathbb{F}_{3^2}$ of minimal linear complexity $3^{2.2-1}+2=29$. Firstly, we select s, an arbitrary span 2 de Bruijn sequence over $\mathbb{F}_3$. Take $s=(0, 0, 1, 0, 2, 2, 1, 1, 2)$ which has linear complexity 8, the maximum possible for a span 2 de Bruijn sequence over $\mathbb{F}_3$. Using the construction of Theorem 2 we exhibit the polynomial $f=x_0x_3+x_2\in\mathbb{F}_3[x_0, x_1, x_2, x_3]$. It has degree $3^3+1=28$ (see Definition 8) so the corresponding sequence s' has linear complexity 29 (see Result 3).

$$s'=0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2,$$
$$0, 1, 2, 0, 1, 2, 0, 1, 2, 1, 2, 0, 1, 2, 0, 1, 2, 0, 2, 0, 1, 2, 0, 1, 2, 0, 1,$$
$$0, 2, 1, 0, 2, 1, 0, 2, 1, 1, 0, 2, 1, 0, 2, 1, 0, 2, 2, 1, 0, 2, 1, 0, 2, 1, 0.$$

We use s' to augment the 1-tuples of s repeated 3^2 times to produce

$$\begin{aligned} s'' = &(0,0),(0,0),(1,0),(0,0),(2,0),(2,0),(1,0),(1,0),(2,0),\\ &(0,1),(0,1),(1,1),(0,1),(2,1),(2,1),(1,1),(1,1),(2,1),\\ &(0,2),(0,2),(1,2),(0,2),(2,2),(2,2),(1,2),(1,2),(2,2),\\ &(0,0),(0,1),(1,2),(0,0),(2,1),(2,2),(1,0),(1,1),(2,2),\\ &(0,1),(0,2),(1,0),(0,1),(2,2),(2,0),(1,1),(1,2),(2,0),\\ &(0,2),(0,0),(1,1),(0,2),(2,0),(2,1),(1,2),(1,0),(2,1),\\ &(0,0),(0,2),(1,1),(0,0),(2,2),(2,1),(1,0),(1,2),(2,1),\\ &(0,2),(0,1),(1,0),(0,2),(2,1),(2,0),(1,2),(1,1),(2,0),\\ &(0,1),(0,0),(1,2),(0,1),(2,0),(2,2),(1,1),(1,0),(2,2). \end{aligned}$$

It may be verified that s'' is a span 2 de Bruijn sequence over $\mathbb{F}_{3^2}$. ∎

REFERENCES

1. S. R. Blackburn, T. Etzion, and K. G. Paterson, Permutation polynomials, de Bruijn sequences, and linear complexity, *J. Combin. Theory Ser. A* **76** (1996), 55–82.
2. 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.
3. T. Etzion, On the distribution of de Bruijn sequences of low complexity, *J. Combin. Theory Ser. A* **38** (1985), 241–253.
4. T. Etzion and A. Lempel, On the distribution of de Bruijn sequences of given complexity, *IEEE Trans. Inform. Theory* **30** (1984), 611–614.
5. T. Etzion and A. Lempel, Construction of de Bruijn sequences of minimal complexity, *IEEE Trans. Inform. Theory* **30** (1984), 705–709.
6. P. A. Hines, Characterising the linear complexity of span 1 de Bruijn sequences over finite fields, *J. Combin. Theory Ser. A* **81** (1998), 140–148.
7. R. Lidl and H. Niederreiter, "Finite Fields," Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison–Wesley, London, 1983.
8. K. G. Paterson, Perfect factors in the de Bruijn graph, *Designs, Codes Cryptography* **5** (1995), 115–138.