Randomness and Representation of Span n Sequences

Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. ggong@calliope.uwaterloo.ca

Dedicated to Solomon Golomb on his 75th Birthday

Abstract. Any span n sequences can be regarded as filtering sequences. From this observation, new randomness criteria for span n sequences are proposed. It is proved that the feedback function of a span n sequence can be represented as a composition of its trace representation, or equivalently, its discrete Fourier transform, and a permutation from the state space of the sequence to the multiplicative group of the finite field $GF(2^n)$, and vice versa. Significant enhancements for randomness of span n sequences, so that de Bruijn sequences, are illustrated by some examples.

Index Terms. Nonlinear feedback shift register sequences, span n sequences, de Bruijn sequences, randomness, discrete Fourier transform.

1 Introduction

In order to seek out good pseudorandom sequence generators (PRSG) in cryptographic practice, several randomness criteria have been proposed. From Shannon's work [22], the one-time-pad is unbreakable. Hence a good PRSG should generate pseudorandom sequences with large periods to guarantee that different messages are encrypted using different key streams. In the mid 1950s, Golomb proposed the well-known three randomness postulates [12], i.e., R-1(the balance property), R-2 (the run property), and R-3 (the ideal 2-level autocorrelation). In addition, the ideal n-tuple distribution is also introduced. By the end of the 1960s, Berlekamp [2] found a decoding algorithm which can reconstruct an entire codeword from a partial known consecutive bits of the codeword. Shortly after, Massey used this algorithm in linear feedback shift register (LFSR) sequences synthesis [18]. Using the algorithm, if the length of the shortest LFSR which generates a sequence, known as the linear span or linear complexity of the sequence, is equal to n, then from any known consecutive $2n$ bits, the full period of the sequence can be reconstructed. This result imposed the large linear span criterion to PRSGs [21]. To overcome the weakness of the sole linear span criterion, two more criteria related to linear spans were introduced in the mid 1980s [21] and early 1990s [8], namely, the linear span profile and k-error

linear span (or originally referred to as sphere linear complexity) of a sequence, respectively. However, no such sequences with simple implementation as well as a smoothly increased linear span profile and/or the k-error linear span property have been found. The normalized linear span of a sequence was also introduced as a complement of the linear span measurement (see below for the definition or [15]).

With popularity of the public-key cryptography, researchers look for PRSGs whose randomness is based on computational complexity. A pseudorandom sequence is said to have *indistinguishablity* if the sequence is indistinguishable from a random bit stream generated by a truly random bit generator using any polynomial time algorithm (see [11]).

The above constitutes a rough picture of the developments of randomness criteria for PRSGs up to now. In the following, we single out one class of pseudorandom sequences, the so-called span n sequences, and summarize their known results and their potential applications in cryptology.

A binary sequence with period $N = 2^n - 1$ is called *a span n* sequence if each non-zero n-tuple $(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{F}_2^n$ occurs exactly once in every period. This property was discussed in Golomb's paper [13] back in the early 1980s.

A. Pseudorandom number generators (PRNGs) and Span n Sequences: A PRNG, whenever employed in the Digital Signature Standard [16] [20] or session key generations, must generate different pseudorandom numbers at different time instances. On the other hand, each state of a span n sequence gives different binary numbers. Thus, a span n sequence can be employed as a PRNG.

B. Known Results on de Bruijn Sequences and Span n Sequences: A de Bruijn sequence of period 2^n is a binary sequence with period 2^n, which can be generated by a nonlinear feedback shift register (NLFSR) with n stages. A span n sequence can be obtained from a de Bruijn sequence of period 2^n by deleting one zero from the run of zeroes of length n, vice versa, i.e., any de Bruijn sequence can be obtained from a span n sequence by adding one zero into the zero run of length n. (A span n sequence is also referred to as a *modified de Bruijn sequence* in [17].) There are $2^{2^{n-1}-n}$ de Bruijn sequences, so does the span n sequences. (See [12].)

Chan, Games and Key [4] proved that the linear span of any de Bruijn sequence of period 2^n, denoted by L, is bounded by $2^{n-1} + n \leq L \leq 2^n - 1$ where both the lower bound and upper bound are achievable [9]. Therefore any de Bruijn sequence has a large linear span, the normalized linear span is $> 1/2$ (the normalized linear span of a sequence with period r and linear span s is defined by $\frac{s}{r}$), and satisfies the span n property. But it does not posses the 2-level autocorrelation property. On the other hand, a lower bound of the linear span of the corresponding span n sequence is dramatically dropped to n, i.e., $n \leq L \leq 2^n - 2$. No theoretical results on linear spans of span n sequences, except for m-sequences, have been established. Experimental results show that the linear span of an NLFSR span n sequence, i.e., it is not an m-sequence, varies in the range from $3n$ to $2^n - 2$ (see [17]). From a point of view in cryptographic applications, an "actual" linear span of a de Bruijn sequence should be measured in terms of

the linear span of its corresponding span n sequence, because the transformation between them are deterministic. This phenomenon has been observed in 1980s. However, up to now, no sub-classes of de Bruijn sequences are discovered such that their linear spans do not differ significantly from the linear spans of their corresponding span n sequences.

The Stream Cipher Project in ECRYPT has several submissions which used NLFSRs [10]. However, we know a little about cycle structures of NLFSRs. (Most of the known results are collected in Golomb's pioneering book [12].) It has no significant progress along this line for about 5 decades.

In this paper, we discuss the cryptographic properties of span n sequences and a new approach to represent span n sequences.

2 The Basic Definitions

For a positive integer n, we denote that $N = 2^n - 1$, $q = 2^n$, $F_q = GF(q)$, and $F_2^n = \{(x_0, x_1, \cdots, x_{n-1}) \,|\, x_i \in F_2\}$. All the sequences that are considered in this paper are binary.

A. LFSR and NLFSR Sequences. We say that $\{a_i\}$ is a binary sequence generated by a linear or nonlinear feedback shift register (LFSR or NLFSR) with n stages if the sequence satisfies the following recursive relation

$$a_{k+n} = f(a_k, a_{k+1}, \cdots, a_{k+n-1}), k = 0, 1, \cdots \tag{1}$$

where $(a_0, a_1, \cdots, a_{n-1})$ is an initial state, and the feedback function $f(x_0, x_1, \cdots, x_{n-1})$ is a boolean function in n variables. Any n consecutive terms of the sequence in (1), denoted by S_k,

$$S_k = (a_k, a_{k+1}, \cdots, a_{k+n-1})$$

represent a state of the shift register. If $f(x)$ is linear, say $f(x_0, x_1, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i, c_i \in \mathbb{F}_2$, then (1) becomes $a_{k+n} = \sum_{i=0}^{n-1} c_i a_{k+i}, k = 0, 1, \cdots$. The polynomial $t(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ is called a characteristic polynomial of the sequence a. For the theory of LFSR and NLFSR, the reader is referred to [12].

Note that any boolean function f in n variables can be represented as a polynomial function from $\mathbb{F}_q$ to $\mathbb{F}_2$ in terms of the Lagrange interpolation (which has the similar formula as DFT defined below, see [15] for details). In this paper, we restrict ourselves to the case $f(0) = 0$. (For $f(0) \neq 0$, replacing $f(x)$ by $g(x) = 1 + f(x)$, then all the results obtained in this paper are applicable to the case $f(0) = 1$). Furthermore, we will not make any distinction among a boolean function and its polynomial representation in notation, whose meaning depends on the context.

B. DFT and Inverse DFT of Binary Sequences: Let $\{a_t\}$ be a binary sequence with period $N = 2^n - 1$. We also write $\{a_t\} = (a_0, a_1, \cdots, a_{N-1})$ as a vector. Let α be a primitive element in $\mathbb{F}_q (q = 2^n)$. Then the *(discrete) Fourier Transform (DFT)* of $\{a_t\}$ is defined by

$$A_k = \sum_{t=0}^{N-1} a_t \alpha^{-tk}, \ k = 0, 1, \ldots, N-1. \tag{2}$$

The inverse DFT (IDFT) is given by

$$a_t = \sum_{k=0}^{N-1} A_k \alpha^{kt}, \quad t = 0, 1, \ldots, N-1. \tag{3}$$

The sequence $\{A_k\}$ is referred to as a *spectral sequence* of $\{a_t\}$. Let $A(x) = \sum_{k=0}^{N-1} A_k x^k$. Then $a_t = A(\alpha^t)$.

Fact 1 *1.* $A_{2^j k} = A_k^{2^j}, \forall j, k$.
2. $A(x)$ *can be written as*

$$A(x) = \sum_k Tr_1^{m_k}(A_k x^k) \tag{4}$$

where the k*'s are (cyclotomic) coset leaders modulo* N*,* $m_k \,|\, n$ *is the length of the coset which contains* k*, and* $Tr_1^{m_k}(x)$ *is a trace function from* $\mathbb{F}_{2^{m_k}}$ *to* $\mathbb{F}_2$ *(which will be written as* $Tr(x)$ *if* $m_k = n$ *in short). This is called a* trace representation *of* $\{a_t\}$.

C. Linear Spans: The linear span of a binary sequence a is defined as the length of the shortest LFSR which generates the sequence, denoted by $LS(a)$. The corresponding characteristic polynomial is referred to as the *minimal polynomial* of the sequence. If $f(x)$ generates a sequence, then the minimal polynomial of the sequence is a divisor of $f(x)$. Any pseudorandom sequences employed in key stream generators of stream ciphers or pseudorandom number generators should have large linear spans.

For a positive integer r, an r-shift (left) of a, denoted by $L^r(a)$, is a sequence given by $a_r, a_{r+1}, \cdots$. The shift operator does not change the linear span of the resulting sequence, i.e., $LS(a) = LS(L^r(a))$. If a has period N, then the linear span of a is equal to the number of nonzeros in the spectrum of a. Furthermore, let $\{A'_k\}$ be a spectral sequence of the r-shift of a.

Fact 2 *The spectral sequences of the sequence and its* r *shift are related by*

$$A'_k = \alpha^{rk} A_k, \forall k.$$

D. Filtering Sequence Generators: Let $u = \{u_t\}$ be an m-sequence of period $2^n - 1$, and $0 \le k_0 < k_1 < \cdots < k_{m-1} < n$. A sequence $a = \{a_t\}$ is called a filtering sequence if

$$a_t = f(u_{k_0+t}, u_{k_1+t}, \cdots, u_{k_{m-1}+t}), t = 0, 1, \cdots \tag{5}$$

where $f(x_0, x_1, \cdots, x_{m-1})$ is a boolean function in m variables. The boolean function f is referred to as a filtering function.

3 Randomness of Span n Sequences

In this section, we first show that any span n sequence can be regarded as a filtering sequence and propose several new randomness criteria for span n sequences, then we show that the corresponding de Bruijn sequence of a span n sequence with maximum linear span also has maximum linear span. In addition, some examples of span n sequences with maximum linear span, having very poor nonlinearity (this concept will be introduced below), are also presented in this section.

3.1 New Randomness Criteria

A known fact that has not received much attention is that a span n sequence in fact is a filtering sequence, which will be shown below. Recall that α is a primitive element in $\mathbb{F}_q$. Let $u = \{u_t\}$ be an m-sequence of period N with trace representation $Tr(x)$, i.e., $u_t = Tr(\alpha^t)$. Let $\{\alpha_0, \cdots, \alpha_{n-1}\}$ and $\{\beta_0, \cdots, \beta_{n-1}\}$ be a pair of the dual bases of $\mathbb{F}_q$ ($q = 2^n$) over $\mathbb{F}_2$, i.e.,

$$Tr(\alpha_i \beta_j) = \begin{cases} 1 \Longleftrightarrow i = j \\ 0 \Longleftrightarrow i \neq j. \end{cases}$$

For any element $x \in \mathbb{F}_q$, we have the following relationship

$$x = \sum_{i=0}^{n-1} x_i \alpha_i,\ x_i \in \mathbb{F}_2 \Longrightarrow x_i = Tr(\beta_i x),\ i = 0, \cdots, n-1.$$

Let $a = \{a_i\}$ be a sequence with period N, and $f(x)$ be its trace representation, i.e., $a_i = f(\alpha^i), 0 \leq i < N$. Let $\alpha^i = \sum_{j=0}^{n-1} c_{i,j}\alpha_j$, then $c_{i,j} = Tr(\beta_j \alpha^i)$. Let $\beta_j = \alpha^{k_j}$, then $\{Tr(\beta_j \alpha^i)\}_{i \geq 0} = L^{k_j}(u)$. Hence a can be written as

$$a_i = f(u_{k_0+i}, u_{k_1+i}, \cdots, u_{k_{n-1}+i}), i = 0, 1, \cdots. \tag{6}$$

According to (5), a is a filtering sequence where the filter function is equal to $f(x_0, x_1, \cdots, x_{n-1})$, the corresponding boolean form of $f(x)$ (here we use the same notation for $f : \mathbb{F}_q \leftarrow \mathbb{F}_2$ in both their respective polynomial form and boolean form), and the tap positions on u are given by $(k_0, k_1, \cdots, k_{n-1})$.

Since a span n sequence has period N, it can also be considered as a filtering sequence with the above form. So, when sequences of period N are employed either in stream ciphers or in pseudorandom number generators, one should consider the possibility of applying attacks on filtering generators. There exist several criteria for choosing f being a good filtering function. Thus, randomness of span n sequences with applications in cryptology should be measured not only by the randomness criteria summarized at the beginning of Section 1, but also by the following three properties which are related to filtering functions, i.e., boolean functions in n variables. Let a be a span n sequence and $f(x)$ be its trace representation.

(F1) Nonlinearity or linear resistancy of a (in terms of f): $N_a = \frac{q-c_f}{2} (= N_f)$ where $c_f = \max\{|\pm \widehat{f}(\lambda)|, \lambda \in \mathbb{F}_q\}$ where $\widehat{f}(\lambda)$ is the Hadamard transform of $f(x)$ defined by $\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_q} (-1)^{Tr(\lambda x)+f(x)}$, $\forall \lambda \in \mathbb{F}_q$. Then N_f should be large or equivalently, c_f, the maximum correlation between $f(x)$ and $Tr(x)$ or $f(x)$ and $Tr(x)+1$ should be small, in order to be resistant to correlation attacks [23] and linear cryptanalysis [19].

(F2) Propagation or differential resistancy of a (in terms of f): $D_a = \frac{q-P_f}{2} (= D_f)$ where

$$P_f = \max\{|A_f(\omega)|, \omega \in \mathbb{F}_q\}$$

where $A_a(\omega)$ is the additive autocorrelation defined by

$$A_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+f(x+\omega)}, \ \forall \omega \in \mathbb{F}_{2^n}.$$

The magnitude of the maximum additive autocorrelation, P_f, should be small, in order to have large differential resistancy D_a, i.e., the distance between $f(x)$ and $f(x+a)$ is large (or a small change in variable x results in a big change in $f(x)$), for combatting differential cryptanalysis [3]. A link between linear cryptanalysis and differential cryptanalysis is discussed in [5].

(F3) Algebraic immunity of a (in terms of f):

$$AI_a = AI_f = \min\{deg(g) \,|\, g \in \mathcal{F}_n, fg = 0 \text{ or } (f+1)g = 0\}$$

where $\mathcal{F}_n$ is the set consisting of all functions from $\mathbb{F}_q$ to $\mathbb{F}_2$. This should be large in order to be resistant to algebraic attacks, whose impact on breaking filtering generators have been recently shown in the literature [6] [7]. (*Note.* Using a lower degree polynomial to approximate a filtering sequence is not a new approach, which has been studied as a linearized method for NLFSR back in 1970s.)

There are considerably amount of publications for constructing boolean functions with some of these three properties. But none of those functions produce span n sequences. On the other hand, the corresponding de Bruijn sequence of a span n sequence always has a large linear span, at least $2^{n-1} + n$ (see Section 1). Thus, the genuine unpredictability of a de Bruijn sequence is determined by the unpredictability of the corresponding span n sequence. We define the linear span of the corresponding de Bruijn sequence of a span n sequence as an *illusional linear span* of the span n sequence. Let b be the corresponding de Bruijn sequence of a. In addition to the above randomness criteria F1-F3, we require that

(F4) The difference between the illusional linear span and the linear span of a span n sequence should be small, i.e., $\Delta = |LS(a) - LS(b)|$ is small or $LS(a) \geq 2^{n-1}$.

It is not easy to determine whether a span n sequence, regarded as a filtering sequence, satisfies the randomness properties F1-F4 as well as possessing

some other randomness properties. Up to now, there are no sub-classes of span n sequences whose feedback functions are algebraically known except for those constructed from m-sequences by adding one zero into the run of zeros of length $n-1$. However, these randomness criteria could be served as guidelines for future research in theory and test beds for design of secure communication systems in practice.

3.2 Examples

Example 1. Let

$$a = 01111101110010100110101100010 00$$

Then a is a span 5 sequence. Let $\mathbb{F}_{2^5}$ be defined by a primitive polynomial $t(x) = x^5 + x^4 + x^3 + x + 1$, and α be a root of $t(x)$. Using the DFT, we can obtain the trace representation of a as follows

$$f(x) = Tr(x + x^3 + \alpha x^5 + \alpha^{22} x^7 + \alpha^{18} x^{11} + \alpha^7 x^{15}).$$

Thus $LS(a) = 30$. The distributions of the autocorrelation, additive autocorrelation, and Hadamard transform are given as follows.

Autocorrelation					
$C_a(\tau)$	31	-1	-5	7	-9
$\#\tau's$	1	16	4	6	4

Hadamard Transform							
$\widehat{f}(\lambda)$	0	4	-4	8	-8	12	-12
$\#\lambda's$	8	7	7	6	2	1	1

Additive Autocorrelation				
$A_f(\omega)$	0	8	-8	-16
$\#\omega's$	16	7	7	2

Thus, we have the nonlinearity or linear resistancy of a: $N_a = 10$, which is smaller than the maximum linear resistancy 12 for $n = 5$, and the differential resistancy of a: $D_a = 8$, which is poor, compared to the maximum differential resistancy 12 for $n = 5$. The illusional linear span of a is equal to 27. Therefore $\Delta = 3$. Thus, this sequence has good linear span property whenever we consider the difference between a and b or the linear span of a solely.

Remark 1. The above randomness criteria F1-F4 are defined for span n sequences. However, they could apply to any binary sequences of period N. For n odd, both the optimal linear resistancy and optimal differential resistancy are given by $A = 2^{n-1} - 2^{(n-1)/2}$. For $n = 5$ and 7, $N_a = A$ is maximum. For the differential resistancy, no examples have been found which satisfies $D_a > A$.

In the following example, we show randomness of a class of span n sequences constructed by Golomb in [13].

Example 2. Let $f(x) = x^n + x + 1$, n odd, which is primitive over $\mathbb{F}_2$, let $1\underbrace{00\cdots0}_{n-1}$ be an initial state of the LFSR with $f(x)$ as the minimal polynomial which generates a. Then we have

$$a_{N-1}, a_0, \cdots, a_{n-1}, a_n, a_{n+1}, \cdots, a_{2n-1} = 11\underbrace{00\cdots0}_{n-1}1\underbrace{00\cdots0}_{n-2}1$$

In [13], Golomb constructed a class of span n sequences with the constant-on-cosets property for n odd as follows. (We say a sequence $a = \{a_i\}$ satisfies the constant-on-cosets property if there exists a k-shift of a such that $a_{k+2i} = a_{k+i}, i = 0, 1, \cdots.$) Let $b_i = a_i + 1$, $i = 1, \cdots, N-1$ and $b_0 = a_0$. Then b is a span n sequence with the constant-on-coset property. We notice that b is obtained by complementing every bit of a except for a_0. In the following, we show that the linear span of b is equal to $2^n - 2 - n$. Assume that $a_i = Tr(\beta\alpha^i), i = 0, 1, \cdots, n-1, \beta \in \mathbb{F}_{2^n}$ where α is a root of $x^n + x + 1$. Let $\{A_j\}$ and $\{B_j\}$ be the spectral sequences of a and b respectively. Since $\{a_i\}$ satisfies the constant-on-cosets property, then $\beta = 1$ (see [15] for this result). From the DFT, we have

$$\begin{aligned} B_j &= \textstyle\sum_{i=0}^{N-1} b_i\alpha^{-ij} = a_0 + \sum_{i=1}^{N-1}(a_i + 1)\alpha^{-ij} \\ &= \textstyle\sum_{i=1}^{N-1} \alpha^{-ij} + \sum_{i=0}^{N-1} a_i\alpha^{-ij} = 1 + A_j. \end{aligned}$$

Since a is an m-sequence, then $A_j = 0$ for all the coset leaders $j \neq 1$. Note that $A_1 = \beta$, and $\beta = 1$. Thus $LS(b) = 2^n - 2 - n$, which is very large, compared with the maximum linear span $2^n - 2$. However, the corresponding filtering function of b has very poor nonlinearity, which is demonstrated as follows. Let $f(x)$ and $g(x)$ be their respective trace representations of a and b. Then $f(x) = Tr(x)$ and

$$g(x) = \begin{cases} 1 + Tr(x) & \text{if } x \neq 0, 1 \\ 1 & \text{if } x = 1 \\ 0 & \text{if } x = 0. \end{cases}$$

Therefore, the Hadamard transform of $g(x)$ is computed by

$$\begin{aligned} \widehat{g}(\lambda) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr(\lambda x)+g(x)} \\ &= 2 - 2(-1)^{Tr(\lambda)} - \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr((\lambda+1)x)}. \end{aligned}$$

Note that n is odd, so $Tr(1) = 1$. By examining the above summations, we have $\widehat{g}(\lambda) \in \{0, 4, 4 - 2^n\}$. According to the definition of the nonlinearity, we have $c_g = 2^n - 4$ and $N_f = 2$, i.e., the nonlinearity of g is equal to 2, which is almost the worst nonlinearity of a nonlinear function.

Remark 2. The poor randomness of b can also be detected from the 1-error linear span of $\overline{b}$, the complement of b. (*Note.* The k-error linear span of a sequence u of period r is defined by $E_k(u) = \min\{LS(u+e) \,|\, e \in \mathbb{F}_2^r, H(e) = k\}$ where $H(e)$ is the Hamming weight of the r-dimensional vector e, and $LS(x)$ is the linear span of x.) According to the construction of b, we have $\overline{b} = a + e$ where $e = (1, 0, \cdots, 0)$. Thus $E_1(\overline{b}) = E_1(a+e) = n$. From this observation, it is worth to look at k-error linear spans of sequences through their nonlinearity, since the latter have received a tremendous large amount of publications in recent 30 years.

4 Relationships Between DFTs and Feedback Functions

In this section, we investigate how feedback functions of span n sequences can be derived from their trace representations, i.e., their DFTs, and vice versa. Let $a = \{a_k\}$ be a span n sequence, and $f(x)$ be its trace representation. Let $S_k = (a_k, \cdots, a_{k+n-1})$ be the kth state of a, $\mathcal{S} = \{S_k \,|\, 0 \le k < N\}$, and $\mathbb{F}_q^*$, the multiplicative group of $\mathbb{F}_q$ which are represented by powers of α, a primitive element in $\mathbb{F}_q$. Let

$$\begin{gathered} \sigma : S_k \to \alpha^k, 0 \le k < N, \text{ or equivalently} \\ \sigma : (a_k, a_{k+1}, \cdots, a_{k+n-1}) \to (c_{k,0}, c_{k,1}, \cdots, c_{k,n-1}) \end{gathered} \tag{7}$$

where $\alpha^k = \sum_{j=0}^{n-1} c_{k,j}\alpha^j$. This map induces a permutation on $\mathbb{Z}_N$ in the following fashion:

$$\pi = \begin{pmatrix} 0 & 1 & \cdots & k & \cdots & N-1 \\ t_0 & t_1 & \cdots & t_k & \cdots & t_{N-1} \end{pmatrix} \tag{8}$$

where t_k is determined by $\sum_{j=0}^{n-1} a_{k+j}\alpha^j = \alpha^{t_k}$. Since σ is a one-to-one map between $\mathcal{S}$ and $\mathbb{F}_q^*$, then σ^{-1} exists. Therefore, we may write

$$a_k = f(\alpha^k) = f(\sigma\sigma^{-1}(\alpha^k)) = f(\sigma(S_k)), k = 0, 1, \cdots. \tag{9}$$

We define $b = \{b_k\}$, and $b_{n+k} = g(S_k), k = 0, 1, \cdots$ where $g(x) = f \circ \sigma(x)$, the composition of f and σ, as a feedback function of an NLFSR, and an initial state of b is given by $(b_0, \cdots, b_{n-1}) = (a_{N-n}, \cdots, a_{N-1})$. According to (1) in Section 2, b is generated by the NLFSR with n stages and the feedback function g. From (9), we have $a = L^n(b)$. Thus, we have established the following theorem.

Theorem 1. *With the above notation, then $g = f \circ \sigma$ is the feedback function of an NLFSR which generates b, an $(N-n)$-shift of a, i.e., $b = L^{N-n}(a)$. So, they have equal linear spans.*

Given that $f(x)$ is a feedback function of an NLFSR which generates a span n sequence a, we would like to ask what the trace representation of a is. Again, using (1),

$$\begin{gathered} a_{n+k} = f(S_k), k = 0, 1, \cdots, \text{ where} \\ S_k = (a_k, a_{k+1}, \cdots, a_{k+n-1}). \end{gathered} \tag{10}$$

We now define the same map as defined in (7). From (10),

$$a_{n+k} = f(\sigma^{-1}\sigma(S_k)) = f(\sigma^{-1}(\alpha^k)), k = 0, 1, \cdots. \tag{11}$$

We denote $h(x) = f \circ \sigma^{-1}(x)$, and $c = \{c_k\}$ where $c_k = h(\alpha^k), k = 0, 1, \cdots$. Then $h(x)$ is the trace representation of c. However, from (11), $c = L^n(a)$, so that $a = L^{N-n}(c)$. Let $\{A_k\}$ and $\{C_k\}$ be the spectral sequences of a and c respectively. Applying Fact 2, we have $A_k = \alpha^{-nk}C_k$. Thus, we have proved the inverse of Theorem 1, which is shown below.

Theorem 2. *Let $f(x)$ be a feedback function of an NLFSR which generates a span n sequence a. Then the trace representation of a is given by $f \circ \sigma^{-1}(\alpha^{-n}x)$.*

For an easy comparison of these relationships, we summarize the results of Theorems 1 and 2 into the following table.

Relationships Between DFT and Feedback Functions

DFT	Feedback Function in an NLFSR
$a \leftrightarrow f(x)$	$f \circ \sigma(x)$ generates $L^{N-n}(a)$
$a \leftrightarrow f \circ \sigma^{-1}(\alpha^{-n}x)$	f generates a

In the following example, a feedback function is a linear function, since there are no span 3 sequences which are not m-sequences. This is only for demonstrating the principle of these two theorems.

Example 3. Let $n = 3$, and α be a primitive element in $\mathbb{F}_{2^3}$ with $\alpha^3+\alpha+1 = 0$. Let $f(x_0, x_1, x_2) = x_0 + x_1$, and let $(a_0, a_1, a_2) = (0, 0, 1)$ be an initial state of the LFSR. Then $a = 0010111$, an m sequence of period 7. Using the DFT (see Section 2), the trace representation of a is equal to $Tr(\alpha x)$. In the following, we use the method in Theorem 2 to obtain the trace representation of a. We compute the polynomial form $f(x_0, x_1, x_2) = Tr(\alpha^6 x)$. The map σ is given by the following table.

t_k	$\sigma : S_k \rightarrow$	α^k, exponents k
2	001	0
1	010	1
6	101	2
4	011	3
5	111	4
3	110	5
0	100	6

Using the DFT of functions (or the Lagrange interpolation), we compute that $\sigma^{-1}(x) = \alpha^4 x + x^2 + \alpha^3 x^4$. Thus

$$f \circ \sigma^{-1}(x) = Tr(\alpha^6(\alpha^4 x + x^2 + \alpha^3 x^4)) = Tr(\alpha^4 x).$$

According to Theorem 2, the trace representation of a is given by $f \circ \sigma^{-1}(\alpha^{-3}x) = Tr(\alpha x)$, which verifies the result computed directly from the DFT of a.

Remark 3. The power of Theorems 1 and 2 is a new look at the span n sequences. These results present specific relationships between a feedback function in an NLFSR which generates a span n sequence and the trace representation of the sequence through the one-to-one map from its state space to the multiplicative group of $\mathbb{F}_q$. On the other hand, this provides an algebraic way to construct span n sequences, which is different from all the known constructions for de Bruijn sequences. For example, one could find all span 7 sequences with linear span 21 by testing all the sums of three m-sequences of period 127. In other words, one does the search for span n sequences with trace representations of $Tr(\gamma_1 x^r + \gamma_2 x^s + \gamma_3 x^t)$ where γ_i's run through $\mathbb{F}_q^*$ and r, s and t are distinct coset leaders modulo $2^n - 1$. Since there are 18 different cosets modulo 127, the search complexity is of $18 \times 17 \times 16 \times 127^2 = 78967584$ trials. (Note a shifted sequence of a span n sequence preserves the span n property. Thus the choices of γ_i are reduced from 127^3 down to 127^2.) So, the corresponding de Bruijn sequences of period 128 are obtained.

Remark 4. For an arbitrary NLFSR, if the period of an output sequence, say r, divides N, then the results are similar as those of Theorems 1 and 2 in which the primitive element α is replaced by an element α in $\mathbb{F}_q$ with order r. However, if r is not a divisor of N, then such relationships do not exist.

Acknowledgment. The author wishes to thank the referees for their valuable and helpful comments. The research is supported by NSERC Discovery Grant and SPG.

References

1. H. Beker and F. Piper, *Cipher Systems*, John Wiley and Sons, New York, 1982.
2. E.R. Berlekamp, *Algebraic coding theory*, New York, McGraw-Hill, 1968.
3. Biham, E. and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, *Advances in Cryptology – CRYPTO 90*, Springer-Verlag, 1990, pp. 2-21.
4. A.H. Chan, R.A. Games and E.L. Key, On the complexities of de Bruijn sequences, *J. Combin. Theory*, Vol. 33, Nov. 1982, pp. 233-246.
5. F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis, *Advances in Cryptology - EUROCRYPT '94*, Springer-Verlag, 1994. pp. 363–374.
6. N. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology-EuroCrypt'2003*, Lecture Notes in Computer Science, vol. 2656, Springer-Verlag, 2003. pp. 345-359.
7. N. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, *Advances in Cryptology-Crypto'2003*, Lecture Notes in Computer Science, vol. 2729, Springer-Verlag, 2003. pp. 176-194.
8. C. Ding, G. Xiao and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science, Vol. 561, Springer-Verlag, 1991.
9. T. Etzion and A. Lempel, Construction of de Bruijn sequences of minimal complexity, *IEEE Trans. Inform. Theory*, Vol. IT-30, No. 5, September 1984, pp. 705-709.

10. eSTREAM - The ECRYPT Stream Cipher Project, http://www.ecrypt.eu.org/stream.
11. O. Goldreich, *Foundations of Cryptography: Basic Applications,* Cambridge University Press, 2004.
12. S.W. Golomb, *Shift Register Sequences,* Holden-Day, Inc., San Francisco, 1967, revised edition, Aegean Park Press, Laguna Hills, CA, (1982).
13. S.W. Golomb, On the classification of balanced binary sequences of period $2^n - 1$, *IEEE Trans. on Inform. Theory*, Vol. IT-26, No. 6, November 1980, pp. 730-732.
14. S.W. Golomb, Irreducible polynomials, synchronization codes, primitive necklaces, and the cyclotomic algebra, *Combinatorial Mathematics and its Applications*, edited by R.C. Bose and T.A. Dowling, University of North Carolina Press, Chapel Hill, (1969), pp. 358-370.
15. S.W. Golomb and G. Gong, *Signal Design with Good Correlation: for Wireless Communications, Cryptography and Radar Applications*, Cambridge University Press, 2005.
16. National Institute of Standards and Technology, Digital Signature Standard (DSS), *Federal Information Processing Standards Publication*, FIPS PUB 186-2, Reaffirmed January 27, 2000.
17. G.L. Mayhew and S.W. Golomb, Linear spans of modified de Bruijn sequences, *IEEE Trans. Inform. Theory*, Vol. IT-36, No. 5, September 1990, pp. 1166-1167.
18. J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. on Inform. Theory* Vol. 15, No. 1, January 1969, pp. 81-92.
19. M. Matsui, Linear cryptanalysis method for DES cipher, *Advances in Cryptology-Eurocrypt'93*, Lecture Notes in Computer Science, Vol. 765, Springer-Verlag, 1993, pp. 386-397.
20. A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, (1996).
21. R.A. Rueppel, *Analysis and Design of Stream Ciphers,* Springer-Verlag, (1986).
22. C.E. Shannon, Communication Theory of Secrecy Systems, *Bell System Technical Journal*, Volume XXVII, No. 4, October, 1949, pp. 656-715.
23. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory*, Vol. 30, No. 5, September 1984, pp. 776-780.