PERGAMON Computers and Mathematics with Applications 39 (2000) 57–65

An International Journal
computers & mathematics
with applications

www.elsevier.nl/locate/camwa

Clues to the Hidden Nature of de Bruijn Sequences

G. L. MAYHEW*
Hughes Electronics

Abstract—Order n de Bruijn sequences are the period 2^n binary sequences produced by an n stage feedback shift register. Theoretical results are summarized and data are presented for feedback functions, generator polynomials, linear spans, and autocorrelation properties of modified de Bruijn sequences. © 2000 Elsevier Science Ltd. All rights reserved.

Keywords—De Bruijn sequences, Linear span, Autocorrelation, Generators.

1. INTRODUCTION

Algebraically constructed binary sequences with randomness properties have applications in logic synthesis [1], coding theory [2], cryptography [3], and spread spectrum communications [4]. Research has identified many families such as GMW sequences, bent sequences, no sequences, and de Bruijn sequences. Often these sequences are constructed using shift registers. Golomb provides a detailed treatment of the general properties of shift register sequences [5].

What is a de Bruijn sequence? This question is easily answered using a shift register or a graph. The *order n de Bruijn sequences* are the $2^{2^{n-1}-n}$ binary sequences with period length 2^n that are generated recursively using an n stage feedback shift register [6]. Equivalently, an order n de Bruijn sequence is the record of a Hamiltonian path through the de Bruijn good graph. But what can be said about de Bruijn sequences? Answering this question remains the equivalent of opening a Chinese puzzle box!

Traditionally, research on de Bruijn sequences has considered the sequences at their formal period of length 2^n. Since 1946, the total number of sequences has been determined, some construction methods for small subsets of the sequences have been determined, and their linear spans have been partially characterized [7,8]. Most else remains a mystery. The doubly exponential number of de Bruijn sequences has been a major impediment to characterizing the entire sequence family.

A few de Bruijn sequences are constructed by adding a zero to the unique run of $n-1$ zeros in maximal length linear feedback shift register sequences. M sequences have well researched properties whereas de Bruijn sequences do not. So instead, create a *modified de Bruijn sequence of order n* by removing a single zero from the unique run of n zeros in a de Bruijn sequence of order n. The M sequences are now the linear subset of the modified de Bruijn sequences. This ongoing research is attempting to characterize the nonlinear modified de Bruijn sequences in the

*Current mailing address: P. O. Box 2127, El Segando, CA 90245, U.S.A.

PII: S0898-1221(00)00109-7

same manner that M sequences have been characterized [9]. In particular, the feedback functions, generator polynomials, linear spans, and autocorrelation properties are examined. Data for order 6 modified de Bruijn sequences illustrate these properties. The focus is on properties for orders $n \geq 4$. Orders n for $1 \leq n \leq 3$ are trivial because every modified de Bruijn sequence is also an M sequence.

2. WEIGHT CLASS DISTRIBUTION

In his work, de Bruijn used multiplicative induction to count the number of full length shift register sequences but he did not provide any construction techniques. Most subsequent efforts regarding construction techniques have concentrated on creating subsets rather than all de Bruijn sequences. The most notable techniques find states which enable disjoint small cycles to be merged into one de Bruijn cycle [10,11]. Fredricksen found rules for 2^{2n-5} complete sets. Etzion and Lempel found rules for 2^{kg} complete sets, where $k < (n-5)/2$ and $g < n - 2\log(k)$. Table 1 compares the results of these methods.

Table 1. Comparison of construction methods for several de Bruijn sequence orders.

n	Number of de Bruijn Sequences	Fredricksen Method	Etzion and Lempel Method
4	16	8	12
5	2,048	32	100
6	67,108,864	128	1,782

Rather than examining cycle mergings further, examination of the feedback functions provides insight into a different construction method which has the potential for creating significantly larger sets of modified de Bruijn sequences.

The set of all order n de Bruijn sequences, $DS(n)$, are produced by an n stage feedback shift register. The next content of the least significant stage x_1 is computed as some feedback function $x_n \oplus g(x_{n-1}, \ldots, x_1)$ of the current values, where $\oplus$ denotes addition over $GF(2)$. The function $g(x_{n-1}, \ldots, x_1)$ is easily represented by a truth table. The *weight* $w(g)$ of the feedback function is the number of logical ones (Hamming weight) among the 2^{n-1} entries in the truth table of the feedback function $g(x_{n-1}, \ldots, x_1)$. The weight classes for truth tables which produce $DS(n)$ have specific values [7]. There exists $S \in DS(n)$ with truth table weight w for every odd w between $Z(n) - 1$ and $2^{n-1} - Z^*(n) + 1$, inclusive.

These bounds use the number of cycles from the Pure Cycling Register $Z(n)$ and the number of cycles from the Complementing Cycling Register $Z^*(n)$,

$$Z(n) = \frac{1}{n} \sum_{\substack{d|n \\ \text{all } d}} \phi(n) 2^{n/d} \qquad Z^*(n) = \frac{1}{2n} \sum_{\substack{d|n \\ \text{odd } d}} \phi(n) 2^{n/d},$$

where $\phi(n)$ is the Euler totient function [12].

As a shorthand, let 0 represent the all zero state $(0, 0, \ldots, 0)$. For an order n de Bruijn sequence, $g(0) = 1$. Removing a zero from the longest run of zeros means that the all zero state is now its own successor. Hence, $g(0) = 0$ for the set of all modified de Bruijn sequences, $mDS(n)$. Consequently, there exists $S \in mDS(n)$ with truth table weight w for every even w between $Z(n) - 2$ and $2^{n-1} - Z^*(n)$, inclusive. Note that M sequences are always found in weight class $w = 2^{n-2}$. The complete order 6 weight class distribution data are presented in Table 2. The number of modified de Bruijn sequences in each weight class for orders larger than six remains an unsolved problem.

The known entries in the weight class distributions for orders 4–7 are all divisible by 'large' powers of 2. These data items indicate the presence of large symmetry groups which can serve

as a construction technique. The exponent indicates the number of construction operators. Let $\eta(w,n)$ denote the number of $S \in mDS(n)$ in weight class w. For order 6, 2^{14} divides $\eta(w,6)$ for all w, so 14 operators should exist for the order 6 sequences. Given one sequence in a weight class, another $2^{14}-1$ sequences in that weight class could be constructed by applying all possible combinations of these 14 operators to the given sequence. This process could be repeated for each weight class.

Table 2. Weight class distribution for order 6 modified de Bruijn sequences.

Weight Class	Number of Sequences
12	2,211,840
14	11,059,200
16	21,086,208
18	19,841,024
20	9,912,320
22	2,637,824
24	344,064
26	16,384

One of these operators is already known from the properties of M sequences. An M sequence and its reverse sequence always exist as a pair. Complementation, another natural binary operation, is also a symmetrical construction operator.

For sequence $S = \{s_0, s_1, \ldots, s_{k-1}\}$, the *reverse sequence* $rS = \{s_{k-1}, \ldots, s_1, s_0\}$ and the *complement sequence* $cS = \{1 \oplus s_0, 1 \oplus s_1, \ldots, 1 \oplus s_{k-1}\}$. Two sequences S_1 and S_2 are *equivalent*, $S_1 = S_2$, if one is a cyclic shift of the other. Note that operators c and r commute. For $n > 2$, $rS \neq S$, and $cS \neq S$ [13]. For even $n > 2$, $rS \neq cS$, but for odd $n > 2$, $rS = cS$.

In addition to being distinct, a modified de Bruijn sequence and its reverse are also in the same weight class. Similarly, in addition to being distinct, a modified de Bruijn sequence and its complement are also in the same weight class. Let G_{even} be the group generated by both operators r and c. Then $G_{\text{even}} = \{e, r, c, rc\}$ partitions the even order n modified de Bruijn sequences into sets of four pairwise inequivalent sequences (e is the identity operator). Thus, for $k \geq 2$, $\eta(w, 2k) = 0 \bmod 4$. Let G_n denote the symmetry group which operates on the order n de Bruijn sequence weight classes. Note that G_{even} should be a subgroup of G_6 once the other 12 operators of G_6 are fully identified. Symmetry operators in the weight classes for the order 5 de Bruijn sequences have been identified, but these operators are based on cycle mergings and are different for each weight class [14]. This author believes that the same set of operators for any given order should apply to every weight class within that order.

3. FEEDBACK FUNCTION POLYNOMIAL DISTRIBUTION

In the simplest of shift register implementations, the feedback is modulo two addition of the contents in those stages out of the n stages that are selected. Picking a linear function at random, the chances are 1 in n that the function will produce a full period sequence. For small orders, such a shift register can be simulated and the resulting period determined. However, this procedure rapidly becomes impractical as n increases. Very early, the connection between these potential feedback functions and recurrence relations was made. The study of linear functions which produce sequences with period length $2^n - 1$ quickly became the study of polynomials over a Galois field of two elements, $GF(2)$. Reducible polynomials are factored using the rules of multiplication in a Galois field. Irreducibility and primitivity tests exist and can be applied to arbitrarily large polynomials [4]. Much literature has been devoted to trinomials—the minimal shift register implementation of a linear modified de Bruijn sequence (or M sequence) [2,5,15].

The process for developing the corresponding factorization, irreducibility tests, and primitivity tests for nonlinear modified de Bruijn sequences begins by considering the feedback functions. Explicit feedback functions are obtained by applying a logic reduction technique to each truth table. The appropriate logic reduction technique is Reed Muller decoding which is based on Galois field arithmetic rather than Karnaugh maps which are based on Boolean algebra [16]. Obviously, each truth table producing a modified de Bruijn sequence corresponds to a unique feedback function. Reed Muller decoding produces a unique function because the truth tables do not contain errors which must be corrected. An order $n-1$ Reed Muller decoding is applied to $g(x_{n-1}\dots x_1)$. In order $n-1$ Reed Muller decoding, the implicants are x_{n-1} through x_1 and 1, which are linear, and all possible products of x_{n-1} through x_1, which are nonlinear. Complemented variables are not present in any implicant. Note that the subscript notation is preferred so that cross products do not collapse into incorrect higher degree linear polynomial terms (i.e., $x_5x_4x_1$ looks like x^{10}). Data for the generator polynomials, $x_6 \oplus g(x_5\dots x_1) \oplus 1$, of order 6 modified de Bruijn sequences are presented in Table 3.

Let $\tau(n)$ denote the number of terms or implicants in the feedback function characteristic polynomial producing an order n modified de Bruijn sequence. Let $\delta(n)$ denote the degree of nonlinearity of this characteristic polynomial (or recursion). For example, the order 6 linear recursion $x_6 \oplus x_5 \oplus x_2 \oplus x_1 \oplus 1$ corresponding to the primitive pentanomial $x^6 \oplus x^5 \oplus x^2 \oplus x^1 \oplus 1$ has $\tau(6) = 5$ and $\delta(6) = 1$. Similarly, the order 6 nonlinear recursion $x_6 \oplus x_1 \oplus x_5x_4x_1 \oplus x_5x_3x_2x_1 \oplus 1$ has $\tau(6) = 5$ and $\delta(6) = 4$.

Table 3. Implicant class distribution for order 6 modified de Bruijn sequences.

Number of Implicants	Number of Sequences
3	2
5	246
7	11,238
9	198,204
11	1,562,562
13	6,444,000
15	14,773,700
17	19,559,816
19	15,288,166
21	7,081,094
23	1,893,854
25	275,052
27	20,294
29	628
31	8

Consistent with polynomials producing M sequences, the number of terms in a nonlinear polynomial producing a modified de Bruijn sequence is always odd. At the all ones state, the feedback function $x_n \oplus g(x_{n-1}\dots x_1)$ must produce a zero when each implicant is evaluated at 1 so the shift register does not get trapped in this state, hence $\tau(n) = 1 \bmod 2$.

Other results follow quickly. In the order $n-1$ Reed Muller decoding, $x_{n-1}\dots x_2x_1$ is the only implicant with $\delta(n) = n-1$. If the feedback function does not make explicit use of all $n-1$ variables, the corresponding shift register produces an even number of cycles [5]. Hence, $\delta(n) \le n-2$ and $\tau(n) \le 2^{n-1}-1$. The implicants x_n and 1 are always present and the Reed Muller decoding of any $g(x_{n-1}\dots x_1)$ with nonzero weight produces at least one implicant, so $3 \le \tau(n)$.

For M sequences, the characteristic polynomials of S and rS are related by the linear reciprocal transformation. When $f(x)$ is a polynomial of degree n over $GF(2)$, the reciprocal

polynomial $f^*(x)$ is given by $f^*(x) = x^n f(1/x)$. This transformation maps variable x^{n-j} into variable x^j. The reciprocal transformation concept carries over directly from the linear shift register recursions to nonlinear shift register recursions. In developing the $GF(2)$ logic reduction, subscripts replaced superscripts so that nonlinear implicants are clearly distinguishable. The nonlinear reciprocal transformation maps variable x_{n-j} into variable x_j for every variable in an implicant, where the variables x_0 and 1 are equivalent.

The nonlinear reciprocal transformation preserves $\tau(n)$ and $\delta(n)$. Let $\gamma(j,n)$ denote the number of order n modified de Bruijn sequences with $\tau(n) = j$. For $n > 2, S$ and rS exist as a distinct pair whose recursions have equal $\tau(n)$ so $\gamma(j,n) = 0 \bmod 2$. Also, let $\lambda(j,n)$ denote the number of order n modified de Bruijn sequences with $\delta(n) = j$. Similarly, $\lambda(j,n) = 0 \bmod 2$.

The reciprocal transformation process enables a second modified de Bruijn sequence to be created from any known generator function. The linear recursion $x_6 \oplus x_5 \oplus x_4 \oplus x_1 \oplus 1$ is the reciprocal of the linear recursion $x_6 \oplus x_5 \oplus x_2 \oplus x_1 \oplus 1$. The nonlinear recursion $x_6 \oplus x_5 \oplus x_5x_2x_1 \oplus x_5x_4x_3x_1 \oplus 1$ is the reciprocal of the nonlinear recursion $x_6 \oplus x_1 \oplus x_5x_4x_1 \oplus x_5x_3x_2x_1 \oplus 1$. Thus, the symmetry group $G_2 = \{e, r\}$ partitions the order n modified de Bruijn sequences into sets of two pairwise inequivalent sequences (e is the identity operator).

The unique recursions provided by the $GF(2)$ logic reduction via Reed Muller decoding brings the nonlinear theory into alignment with the familiar linear theory. Specifically, the recursions have an odd number of terms between well defined limits and reverse sequences are related by recursions with equal degree of nonlinearity and equal number of terms. The nonlinear recursions are the nonlinear duals to primitive polynomials over $GF(2)$. Nonlinear irreducibility and primitivity tests still need to be developed.

4. LINEAR SPAN DISTRIBUTION

Pseudo random (PN) sequences are more easily generated than truly random sequences but their resulting randomness properties must be checked. A variety of randomness properties are defined as design goals. For $n \geq 4$, the de Bruijn sequences exhibit the balance, run, and span n randomness properties [17]. However, high complexity does not guarantee low predictability. Corresponding statistical tests check the global and local randomness properties of the resulting PN stream. The *linear span* L of a sequence is the least degree linear recursion with binary coefficients that duplicates that given sequence [18]. Linear span is an upper bound on sequence unpredictability. If a sequence has linear span L, then after $2L$ successive elements of the sequence are known, the remainder of the sequence can be predicted exactly.

Examining de Bruijn sequences at their formal length 2^n rather than their more natural length $2^n - 1$ leads to an abberation when linear spans are considered. The absence or presence of one bit has a very radical effect. The de Bruijn sequences which are constructed from M sequences have the greatest linear spans. The linear span of order n de Bruijn sequences are between $2^{n-1} + n$ and $2^n - 1$, except for the linear span $2^{n-1} + n + 1$ which cannot be attained [8]. Yet, the linear span of order nM sequences is just n. On the other hand, when modified de Bruijn sequences are considered, the attainable linear spans are closely related to cyclotomic polynomials. The data for the linear spans of order 6 modified de Bruijn sequences are presented in Table 4 [19]. Note that the number of sequences with each linear span L is $0 \bmod 2$ because S and rS have the same linear span.

The *minimum polynomial of a sequence* is the polynomial over $GF(2)$ with least degree whose corresponding shift register feedback function generates the sequence. The linear span is then the degree of this minimal polynomial of the sequence. The linear spans attained by order n modified de Bruijn sequences are sums whose summands are constrained by the degrees of the irreducible polynomial over $GF(2)$ that are factors of $x^{p(n)} + 1$, where $p(n) = 2^n - 1$. These constraints can be expressed in terms of the $N_I(d)$, the number of irreducible polynomials over $GF(2)$ of

degree d,

$$N_I(d) = \frac{1}{d} \sum_{m|d} \mu\left(\frac{d}{m}\right) 2^m,$$

where $\mu(\ )$ is the Mobius function [12]. For $n \geq 4$, the linear spans L attained by order n modified de Bruijn sequences satisfy

$$L = \sum_{\substack{d|n \\ d \neq 1}} a_d \bullet d,$$

where a_d can take on all possible values in the range $0 \leq a_d \leq N_I(d)$. The degree one minimum polynomial, $x + 1$, never contributes to the linear span because every sequence satisfies the balance property. When the order n is a prime the attainable linear spans is even more restrictive because the cyclotomic polynomial corresponding to the period length has a special factorization. For $q \geq 4$, the linear spans L attained by order q modified de Bruijn sequences, where q is prime, satisfies $L = 0 \bmod q$. Thus, in general, fewer linear spans in the range $2^{n-1} + n$ and $2^n - 1$ are attained by modified de Bruijn sequences than by de Bruijn sequences.

Table 4. Linear spans distribution for order 6 modified de Bruijn sequences.

Linear Span L	Number of Sequences
6	6
27	10
30	8
32	12
33	8
35	62
36	152
38	478
39	1,036
41	3,572
42	6,100
44	17,240
45	28,702
47	86,056
48	134,290
50	401,102
51	453,734
53	1,364,978
54	1,819,148
56	5,453,680
57	3,190,982
59	9,557,084
60	11,148,860
62	33,441,564

5. AUTOCORRELATION BOUNDS

Sequences with sharp autocorrelation properties facilitate radar and communication system synchronization. The M sequences have a well known two level full-period autocorrelation function. This two level full-period autocorrelation function represents the theoretical limit for optimal autocorrelation performance. A question which has remained unanswered for over 30 years is whether or not any of the nonlinear modified de Bruijn sequences can achieve the two level full-period autocorrelation of the M sequences. The overwhelming number of modified de Bruijn sequences in comparison to other sequence categories makes investigating their autocorrelation properties very difficult. As such, the two level full-period autocorrelation "property" of nonlinear sequences has been approached using sequences which are constant on cyclotomic cosets but which are generally not modified de Bruijn sequences [20].

Let $\{b_n\}$ be the sequence which results from $\{a_n\}$ by $b_n = 1 - 2a_n$; that is, in the modified de Bruijn sequence the 0s are replaced by 1s and the 1s are replaced by -1s. Then the *unnormalized discrete periodic autocorrelation function* $C(\tau)$ is defined as

$$C(\tau) = \sum_{n=0}^{T-1} b_n b_{n+\tau},$$

where T is the period [5]. Let $A(\tau)$ denote the number of agreements and $D(\tau)$ denote the number of disagreements between the sequence and itself shifted by τ places. Then the unnormalized periodic autocorrelation function essentially determines the difference between the number of agreements and disagreements for the original and shifted version of the sequence.

$$C(\tau) = A(\tau) - D(\tau) = (2^n - 1) - 2D(\tau).$$

At the zero shift, the unnormalized autocorrelation value of any order n modified de Bruijn sequence is obviously the sequence period length, $C(0) = 2^n - 1$.

Four facts about the autocorrelation function of modified de Bruijn sequences are known [5,20]. First, the autocorrelation function is symmetric, i.e.,

$$C(k\tau) = C(-k\tau) = C\left([2^n - 1 - k]\,\tau\right).$$

Second, the autocorrelation function takes on discrete values given by $C(\tau) = -1 \bmod 4$ when $n > 2$. Third, a truth table $g(x_{n-1} \ldots x_1)$ with weight 2^{n-2} is a necessary but not sufficient condition for an order n modified de Bruijn sequence to have a two level autocorrelation function. Thus, all M sequences belong to the same truth table weight class. Finally, extensive computer searches using cyclotomic cosets have shown that for $n \leq 8$, there does not exist any nonlinear modified de Bruijn sequences having the two level autocorrelation of M sequences.

The autocorrelation functions of all order 6 modified de Bruijn sequences are catalogued in Table 5. This table agrees with the previous results in that only the M sequences have a two level autocorrelation function. However, this table also shows that there exist rather large sets of nonlinear modified de Bruijn sequences which approach the two level autocorrelation function (i.e., have small sidelobes).

For example, in weight class 16 there are 160,974 order 6 sequences whose autocorrelation value between $(n+1) \leq \tau \leq (2^n - n - 2)$ is within ± 8 of the optimal autocorrelation value of -1. Thus, whereas the order 6M sequences have 18.1 dB dynamic range between the in-phase ($\tau = 0$) and out-of-phase ($\tau \neq 0$) autocorrelation values, these particular modified de Bruijn sequences have 17.5 dB dynamic range between the in-phase ($\tau = 0$) and out-of-phase ($\tau \neq 0$) autocorrelation values. Yet the 0.6 dB decrease in dynamic range has yielded a 26,829 fold increase in the number of available sequences in this weight class alone.

Notice that the entries in the autocorrelation distributions are $0 \bmod 2$ because S and rS are in the same weight class and the autocorrelation function is symmetric. The peak out-of-phase

Table 5a. Distribution of order 6 modified de Bruijn sequences within specified autocorrelation $C(\tau)$ bound for $(n+1) \leq \tau \leq (2^n - n - 2)$.

$\lvert C(\tau)+1 \rvert$	$W(g)=12$	$W(g)=14$	$W(g)=16$	$W(g)=18$
$=0$	0	0	6	0
≤ 4	4	4	12	8
≤ 8	17890	89674	160974	154084
≤ 12	525286	2773774	5259832	4809678
≤ 16	1053822	5288918	10123094	9487952
≤ 20	492454	2340048	4463288	4331108
≤ 24	104842	489786	930078	913766
≤ 28	15682	68796	133034	129006
≤ 32	1696	7584	14400	14016
≤ 36	164	590	1386	1338
≤ 40	0	26	102	68
≤ 44	0	0	2	0

$\lvert C(\tau)+1 \rvert$	$W(g)=20$	$W(g)=22$	$W(g)=24$	$W(g)=26$
$=0$	0	0	0	0
≤ 4	6	2	0	0
≤ 8	79758	18188	796	0
≤ 12	2206202	472852	29608	0
≤ 16	4633874	1165896	122826	0
≤ 20	2358076	739014	130290	5432
≤ 24	542902	203572	50032	7950
≤ 28	80936	33644	9338	2780
≤ 32	9578	4226	1058	212
≤ 36	924	414	104	10
≤ 40	64	16	12	0
≤ 44	0	0	0	0

autocorrelation values in Table 5 are only listed between $(n+1) \leq \tau \leq (2^n - n - 2)$ because $C(\tau)$ at the remaining values of τ are predetermined. Due to the span n property, $C(\tau) = -1$ for $1 \leq \tau \leq n-1$ and $-n+1 \leq \tau \leq -1$. Comparing positions 1 and $n+1$ when $\tau = n$ while considering truth table state values yields that sequences produced by a truth table with weight W have $C(n) = C(-n) = (2^n - 1) - 4W$. Hence, because all modified de Bruijn truth tables have even weight, $C(\tau) = -1 \bmod 8$ for $\tau = \pm n$ when $n > 2$.

As examples, for order 6 modified de Bruijn sequences, $C(n) = C(-n) = -41$ in weight class 26, $C(n) = C(-n) = -1$ in weight class 16, and $C(n) = C(-n) = +15$ in weight class 12. Furthermore, among weight classes 14, 16, and 18, there are 404,762 sequences whose out-of-phase autocorrelation value is never more that ± 8 from the -1 limiting value. Thus, the nonlinear sequences which approach the two level autocorrelation function not only appear in weight class 2^{n-2} but also appear in the adjacent weight classes.

Ongoing research is attempting to determine if particular types of nonlinear generator polynomials are more likely to produce sequences which have minimal autocorrelation sidelobes or potentially even a two level autocorrelation function.

6. SUMMARY

By considering period $2^n - 1$ instead of period 2^n, modified de Bruijn sequences begin to show properties that are consistent with known properties of M sequences. Linear modified de Bruijn

sequences all belong in the same truth table weight class whereas nonlinear modified de Bruijn sequences belong in several truth table weight classes. Large symmetry groups underlie the weight classes and suggests operators for construction algorithms. Applying logic reduction over $GF(2)$ to these truth tables yields a unique polynomial for each function. These nonlinear polynomials share many of the same characteristics of the linear polynomials. However, multiplying and dividing linear polynomials is obvious but nonlinear is not. Similarly irreducibility and primitivity tests exist for linear polynomials but not for these nonlinear polynomials. Sequences generated by these linear and nonlinear polynomials share the same randomness properties—balance, run, span-n—but the linear sequences are cryptographically weak while the nonlinear sequences are all cryptographically strong. Finally, the optimal two level autocorrelation property of the linear sequences is well known, but, surprisingly, many nonlinear sequences have autocorrelations whose sidelobes approach the two level autocorrelation limit. Data for the order 6 modified de Bruijn sequences was used to illustrate the duality of linear and nonlinear modified de Bruijn sequences.

REFERENCES

1. O.S. Rothaus, On 'bent' functions, *Journal Combin. Theory* **20A**, 300–305, (1976).
2. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, New York, (1977).
3. W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, *Advances in Cryptology: Proc. of EUROCRYPT '89*, Springer-Verlag.
4. M. Simon, J. Omura, R. Scholtz and B. Levitt, *Spread Spectrum Communications*, Volume I, Computer Science Press, Rockville, MA, (1985).
5. S.W. Golomb, *Shift Register Sequences*, 2nd Edition, Aegean Park Press, Laguna Hills, CA, (1982).
6. N.G. de Bruijn, A combinatorial problem, *Koninklijke Nederlands Akademi van Wetenchappen, Proceedings*, Volume 49 (Part 2), 758–764, (1946).
7. H. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, *SIAM Review* **24**, 195–229, (April 1982).
8. A. Chan, R. Games and E. Key, On the complexities of de Bruijn sequences, *Journal Combin. Theory Series A* **33**, 233–246, (November 1982).
9. G.L. Mayhew, Statistical properties of modified de Bruijn sequences, Ph.D. Dissertation, University of Southern California, (December 1987).
10. H. Fredricksen, A class of nonlinear de Bruijn cycles, *Journal Combin. Theory* **19**, 192–199, (1975).
11. T. Etzion and A. Lempel, Algorithms for the generation of full length shift register sequences, *IEEE Trans. Info. Theory* **IT-30**, 480–484, (May 1984).
12. I. Niven and H.S. Zuckermann, *The Theory of Numbers*, John Wiley & Sons, New York, (1980).
13. T. Etzion and A. Lempel, On the distribution of de Bruijn sequences of given complexity, *IEEE Trans. on Inform. Theory* **IT-30** (4), 611–614, (July 1984).
14. J. Mykkeltveit, Classification of de Bruijn sequences, Rogaland Research Report 28/92, P.O. Box 2503 Ullandhaug, N-4004 Stavanger, Norway, (March 1992).
15. N. Zierler and J. Brilhart, On primitive trinomials (mod 2), *Inform. Contr.* **13**, 541–554, (December 1968).
16. I. Reed, A class of multiple error correcting codes and the decoding scheme, *IRE Trans. Inform. Theory* **4**, 38–49, (1954).
17. S.W. Golomb, On the classification of balanced binary sequences of period $2^n - 1$, *IEEE Trans. on Inform. Theory* **IT-26** (6), 730–732, (November 1980).
18. L. Welch and R. Scholtz, Continued fractions and Berlekamp's algorithm, *IEEE Trans. Inform. Theory* **IT-25**, 19–27, (January 1979).
19. G. Mayhew and S. Golomb, Linear spans of modified de Bruijn sequences, *IEEE Trans. Inform. Theory* **IT-36**, 1166–1167, (September 1990).
20. U. Cheng and S. Golomb, On the characterization of PN sequences, *IEEE Trans. Inform. Theory* **IT-29**, 600, (July 1983).