A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span

JONG-SEON NO AND P. VIJAY KUMAR, MEMBER, IEEE

***Abstract*—A collection of families of binary {0,1} pseudorandom sequences is introduced. Each sequence within a family has period $N = 2^n - 1$, where $n = 2 \cdot m$ is an even integer. There are 2^m sequences within a family, and the maximum over all (nontrivial) auto and cross-correlation values equals $2^m + 1$. Thus these sequences are optimum with respect to the Welch bound on the maximum correlation value. Each family contains a Gordon–Mills–Welch (GMW) sequence, and the collection of families includes as a special case the small set of Kasami sequences. The linear span of these sequences varies within a family but is always greater than or equal to the linear span of the GMW sequence contained within the family. Exact closed-form expressions for the linear span of each sequence are given. The balance properties of such families are evaluated, and a count of the number of distinct families of given period N that can be constructed is also provided.**

I. Introduction

For signature sequences in a spread-spectrum multiple-access communication system, it is desirable to employ code sequences having low nontrivial auto and cross-correlation values and large linear span [1]–[3], [15].

The families of bent [5]–[7] and Gold [8], [9] sequences, as well as the small and large families of Kasami sequences [10], [11] all have desirable correlation properties. However, of these all but the bent sequences possess extremely small values of linear span.

We present new families of binary sequences (which we call families of No sequences[1]) which have optimal (with respect to the Welch bound [12]) correlation properties and large linear span. Each sequence within a No family has period $= 2^n - 1$, where $n = 2 \cdot m$ is an even integer. There are 2^m sequences within the family and the maximum over all nontrivial auto- and cross-correlation values equals $2^m + 1$. Within each family is contained a Gordon–Mills–Welch (GMW) sequence [4], and the families of sequences include the families of Kasami sequences (small set) [3] as a special case. The linear span of these sequences varies within a family but is always greater than or equal to the linear span of the GMW sequence contained within the family. A comparison of the properties of the various sequence families including the No families is presented in Table I.

The No sequence families are introduced in Section II and their correlation properties proven to be optimal with respect to the Welch bound. The balance properties of these sequences, as well as their relation to GMW and Kasami sequences, also are discussed here. Closed-form expressions for the linear spans of these sequences are derived in Section III. In Section IV we show how these sequences may be implemented; Section V provides an example. In Section VI we conclude with a count of the number of distinct families of a given period.

Manuscript received October 26, 1987; revised May 6, 1988. This paper was partially presented at the International Communications Conference, Philadelphia, PA, June 1988 and at the IEEE International Symposium on Information Theory, Kobe, Japan, June 1988. This work was supported by the National Security Agency under Contract No. MDA904-85-H-0010.

The authors are with the Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-0272.

IEEE Log Number 8926623.

[1]The sequences were discovered by No; the closed-form expression for the linear span is chiefly due to Kumar.

II. Optimality of the Correlation Values

For any pair of integers $k, l > 0$, $k|l$, the trace function $\mathrm{tr}_k^l(\cdot)$ is a function mapping from GF(2^l) to GF(2^k) according to the rule

$$\mathrm{tr}_k^l(x) = \sum_{j=0}^{\frac{l}{k}-1} x^{2^{k \cdot j}}. \tag{1}$$

Let $n, n > 0$ be even, set $N = 2^n - 1$, $m = \frac{n}{2}$, and $T = 2^m + 1$. Then a family of No sequences is a collection

$$S = \{s_i(t) | 0 \le t \le N-1, 1 \le i \le 2^m\} \tag{2}$$

of 2^m binary {0,1} sequences given by

$$s_i(t) = \mathrm{tr}_1^m\{[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma_i \alpha^{T \cdot t}]^r\}, \tag{3}$$

where α is a primitive element of GF(2^n), the integer r, $1 \le r < 2^m - 1$, satisfies $gcd(r, 2^m - 1) = 1$, and the elements γ_i range over all of GF(2^m) taking on each value exactly once as i ranges between 1 and 2^m.

0018-9448/89/0300-0371$01.00

TABLE I
COMPARISON OF VARIOUS FAMILIES OF SEQUENCES

Family	Period	n	Size of Family	Maximum Correlation Value	Linear Span Range[a]	Range of Sequence Imbalance
Gold	2^n-1	$2m+1$	2^n+1	$1+2^{(n+1)/2}$	$=2n$	$[1,2^{(n+1)/2}+1]$
Gold	2^n-1	$4m+2$	2^n+1	$1+2^{(n+2)/2}$	$=2n$	$[1,2^{(n+2)/2}+1]$
Kasami (Small Set)	2^n-1	$2m$	$2^{n/2}$	$1+2^{n/2}$	$\leq 3n/2$	$[1,2^{n/2}+1]$
Kasami (Large Set)	2^n-1	$4m+2$	$2^{n/2}(2^n+1)$	$1+2^{(n+2)/2}$	$\leq 5n/2$	$[1,2^{(n+2)/2}+1]$
Bent	2^n-1	$4m$	$2^{n/2}$	$1+2^{n/2}$	$\geq \binom{n/2}{n/4}\cdot 2^{n/4}$	1
No	2^n-1	$2m$	$2^{n/2}$	$1+2^{n/2}$	$\geq m\cdot 2^{m-1}$	$[1,2^{n/2}+1]$

[a] Values tabulated correspond within each collection to the family having largest possible linear span.

Let $R_{i,j}(\cdot)$, $1 \leq i,\ j \leq 2^m$, denote the correlation function associated with the ith and jth sequences in the family S:

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t+\tau)+s_j(t)}, \qquad 0 \leq \tau \leq N-1. \quad (4)$$

Theorem 1:

$$R_{i,j}(\tau) \in \{-2^m-1, -1, 2^m-1\},$$
$$\forall i,j,\tau, 1 \leq i,\ j \leq 2^m, \qquad 0 \leq \tau \leq N-1, \quad (5)$$

provided either $i \neq j$ or $\tau \neq 0$.

Proof: Let t_1 and t_2 be the digits in the base-T expansion of t, $0 \leq t \leq N-1$; i.e.,

$$t = T\cdot t_1 + t_2, \qquad 0 \leq t_1 \leq 2^m-2, \qquad 0 \leq t_2 \leq T-1. \quad (6)$$

Noting that

$$\mathrm{tr}_m^n(\alpha^{2(Tt_1+t_2)}) = \alpha^{2Tt_1}\cdot \mathrm{tr}_m^n(\alpha^{2t_2}) \quad (7)$$

and that

$$\alpha^{T^2t_1} = \alpha^{2Tt_1}, \quad (8)$$

one can express each sequence $s_i(t)$, $1 \leq i \leq 2^m$, in the form

$$s_i(t) = \mathrm{tr}_1^m\left\{\alpha^{2rTt_1}\cdot\left[\mathrm{tr}_m^n(\alpha^{2t_2}) + \gamma_i\cdot\alpha^{Tt_2}\right]^r\right\}. \quad (9)$$

As a result, we have that

$$s_i(t+\tau)+s_j(t) = \mathrm{tr}_1^m\{\alpha^{2rTt_1}\cdot f_1(t_2)\}, \quad (10)$$

where we define

$$f_1(t) = \left[\mathrm{tr}_m^n(\alpha^{2(t+\tau)}) + \gamma_i\cdot\alpha^{T(t+\tau)}\right]^r + \left[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma_j\cdot\alpha^{Tt}\right]^r, \qquad 0 \leq t \leq N-1. \quad (11)$$

If for a fixed value of t_2, $0 \leq t_2 \leq T-1$, $f_1(t_2) \neq 0$, then as a function of t_1 the sequence $s_i(t+\tau)+s_j(t)$ is (from (10)) simply an m-sequence of length 2^m-1 whose phase is determined by the value of $f_1(t_2)$. Of course, when $f_1(t_2)=0$ one obtains a string of 2^m-1 zeroes as t_1 varies over the range 0 to 2^m-2.

From the balance properties of m-sequences [14], it then follows that if z_1 denotes the number of values of t_2 for which $f_1(t_2)=0$, i.e.,

$$z_1 = |\{t_2, 0 \leq t_2 \leq T-1 | f_1(t_2)=0\}|, \quad (12)$$

then the sum sequence $s_i(t+\tau)+s_j(t)$ takes on the value 0 a total of $z_1\cdot(2^m-1)+(T-z_1)(2^{m-1}-1)$ times and the value 1 a total of $(T-z_1)\cdot 2^{m-1}$ times. As a result, all possible nontrivial values of the correlation function $R_{i,j}(\cdot)$ are of the form

$$R_{i,j}(\tau) = z_1\cdot(2^m-1)+(T-z_1)(2^{m-1}-1)-(T-z_1)\cdot 2^{m-1} = 2^m\cdot(z_1-1)-1. \quad (13)$$

Thus the theorem is proved if we can show that z_1 can only take on the values 0, 1, or 2 as γ_i and γ_j vary over $GF(2^m)$ and τ varies over the range 0 to $N-1$ (disregarding, of course, the case $\gamma_i=\gamma_j$, $\tau=0$).

To show this, we first note that

$$f_1(t+T) = \alpha^{2rT}\cdot f_1(t), \qquad 0 \leq t \leq N-1. \quad (14)$$

Consequently, if z_2 denotes the number of zeroes of the function $f_1(t)$ as t varies over the range 0 to $N-1$, then it must be that:

$$z_1 = \frac{z_2}{2^m-1}. \quad (15)$$

Next, define

$$f_2(t) = \mathrm{tr}_m^n\{\alpha^{2t}\cdot(1+\alpha^{2\tau})\} + \alpha^{Tt}\cdot(\gamma_i\cdot\alpha^{T\tau}+\gamma_j), \qquad 0 \leq t \leq N-1 \quad (16)$$

and note that as $gcd(r, 2^m-1)=1$,

$$f_2(t)=0 \Leftrightarrow f_1(t)=0, \qquad 0 \leq t \leq N-1. \quad (17)$$

Thus it suffices to count the number of zeroes of the function $f_2(\cdot)$ (note that by this we have established that a family of No sequences possesses the same correlation properties as a small set of Kasami sequences [3], [10], [11]; however, we continue for the sake of completeness).

Let $x=\alpha^t$ so that x ranges over all the nonzero elements of $GF(2^n)$ as t ranges over 0 to $N-1$. Abusing notation, we write

$$\begin{aligned} f_2(x) &= \mathrm{tr}_m^n\left\{x^2(1+\alpha^{2\tau})\right\} + x^{2^m+1}\left(\gamma_i\alpha^{T\tau}+\gamma_j\right) \\ &= x^2(1+\alpha^{2\tau}) + x^{2^{m+1}}(1+\alpha^{2\tau})^{2^m} + x^{2^m+1}\left(\gamma_i\alpha^{T\tau}+\gamma_j\right) \\ &= x^2\left\{y^2(1+\alpha^{2\tau})^{2^m} + y\left(\gamma_i\alpha^{T\tau}+\gamma_j\right)+(1+\alpha^{2\tau})\right\}, \end{aligned} \tag{18}$$

where $y = x^{2^m-1}$. Here one must distinguish between two cases:

Case 1: $\tau = 0$, $\gamma_i \neq \gamma_j$.

Here $f_2(x) = x^2 y(\gamma_i + \gamma_j)$ and thus $f_2(x)$ does not vanish for any nonzero value of x, i.e., $z_1 = z_2 = 0$. Note that by (13) this implies

$$R_{i,j}(0) = -2^m - 1, \qquad \text{for } i \neq j. \tag{19}$$

Case 2: $\tau \neq 0$.

In this case, $f_2(x)$ vanishes if and only if the quadratic in y in (18) vanishes. Since the coefficients of the quadratic lie in GF(2^n), the quadratic has 0, 1, or 2 roots over GF(2^n). In the first case there are no values of t_2 for which $f_2(t_2) = 0$, i.e., $z_1 = z_2 = 0$. In the other case, $z_2 = 0$, $2^m - 1$ or $2(2^m - 1)$, depending upon whether the roots of the quadratic in y can be expressed as (2^m-1)th powers in the field. Thus, in either case, $z_1 = 0$, 1, or 2, and we are done. Q.E.D.

By arguing as in the proof of the preceding theorem, one can establish that for any sequence $s_i(t)$, the sum $\sum_{t=0}^{N-1}(-1)^{s_i(t)}$ equals -1 (when $\gamma_i = 0$), and either -2^m-1 or $2^m - 1$ otherwise. Thus the imbalance (number of ones–number of zeroes) in these sequences ranges in magnitude between 1 and 2^m+1.

To link the family[2] of No sequences with other well-known sequence sets, set $\gamma_i = 0$ in (3) to obtain the GMW sequence contained within the family and set $r = 1$ to obtain the small set of Kasami sequences. These relationships are summarized in Fig. 1. Table I presents a comparison of the relevant properties of some of the better-known pseudorandom sequence families available to the user, including the family introduced here.

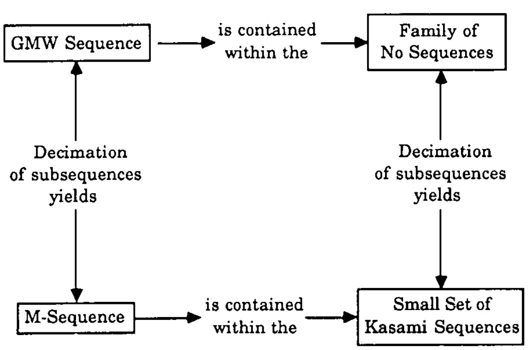

Fig. 1. Relating No sequences to other well-known pseudorandom sequences.

[2] For the sake of brevity, we shall at times refer to the collection of No families of sequences as simply a family of No sequences.

III. Linear Span

The linear span of a typical sequence $s(t) \in S$

$$s(t) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma\cdot\alpha^{T\cdot t}\right]^r\right\} \tag{20}$$

may be determined by expanding the sequence as a polynomial in α^t and counting the number of powers of α^t occurring in this expansion that have nonzero coefficients [13]. As before, for simplicity let $x = \alpha^t$ and use $s(x)$ to denote

$$s(x) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n(x^2) + \gamma\cdot x^{2^m+1}\right]^r\right\}. \tag{21}$$

Then

$$\begin{aligned} s(x) &= \mathrm{tr}_1^m\left\{x^{2r}\left[1+\gamma\cdot y + y^2\right]^r\right\} \\ &= \sum_{j=0}^{m-1} x^{2r\cdot 2^j}\left[1+\gamma\cdot y+y^2\right]^{r\cdot 2^j}, \end{aligned} \tag{22}$$

where $y = x^{2^m-1}$. By reducing exponents of x modulo (2^m-1), it is easy to see that the exponents of x occurring in the expansion of any two terms $x^{2r\cdot 2^{j_1}}[1+\gamma\cdot y+y^2]^{r\cdot 2^{j_1}}$ and $x^{2r\cdot 2^{j_2}}[1+\gamma\cdot y+y^2]^{r\cdot 2^{j_2}}$ present in the sum in (22) are disjointed, and hence the linear span of the sequence $s(t)$ is precisely m times the number of distinct powers of x (having nonzero coefficients) in the expansion of the term

$$g(y) \triangleq \left[1+\gamma\cdot y+y^2\right]^r. \tag{23}$$

Consider the binary $\{0,1\}$ expansion of the integer r. Let R be the total number of runs occurring within this expansion and let L_j be the length of the jth run, $1 \le j \le R$, with the runs being numbered consecutively from the least to the most significant bit. Thus r may be expressed in the form

$$r = \sum_{j=1}^{R} 2^{e_j}\cdot\left(\sum_{k=0}^{L_j-1} 2^k\right), \tag{24}$$

where e_j denotes the lowest exponent of 2 associated with the jth run. Note that by definition,

$$e_{j+1} \ge e_j + L_j + 1, \qquad j = 1, 2, \cdots, R-1. \tag{25}$$

Using (24), one can rewrite $g(y)$ in the form

$$g(y) = \prod_{j=1}^{R}\left[1+(\gamma\cdot y)^{2^{e_j}} + (y^2)^{2^{e_j}}\right]^{r_j}, \tag{26}$$

where $r_j = \sum_{k=0}^{L_j-1} 2^k = 2^{L_j} - 1$, $1 \le j \le R$.

Define

$$g_j(y) = \left[1+(\gamma\cdot y)^{2^{e_j}} + (y^2)^{2^{e_j}}\right]^{r_j} \tag{27}$$

and note that when considered as a polynomial in y, each nonzero exponent of y (that can possibly have a nonzero coefficient) in $g_j(y)$ is a multiple of 2^{e_j} that lies between 2^{e_j} and $2^{e_j+1}\cdot r_j$.

As

$$g(y) = \prod_{j=1}^{R} g_j(y), \tag{28}$$

the exponents of y that can possibly occur (with nonzero coefficients) in the expansion of $g(y)$ as a polynomial in y are, by the preceding, of the form

$$a = \sum_{j=1}^{R} a_j, \tag{29}$$

where $2^{e_j} \le a_j < 2^{e_j+1}\cdot r_j < 2^{e_{j+1}}$ and $2^{e_j}|a_j$.

Therefore two such exponents, $a = \sum_{j=1}^{R} a_j$ and $b = \sum_{j=1}^{R} b_j$, can only be equal if and only if $a_j = b_j$, $j = 1,2,\cdots,R$. Thus one can count the number M of distinct exponents occurring in the expansion of $g(y)$ by counting the corresponding number M_j for each polynomial $g_j(y)$ and multiplying; i.e.,

$$M = \prod_{j=1}^{R} M_j. \tag{30}$$

At this point we consider two cases separately.

Case 1: $\gamma = 0$.

Let $z = y^{2^{e_j}}$. Then

$$g_j(z) = [1+z^2]^{r_j} = \sum_{k=0}^{r_j} z^{2k}. \tag{31}$$

Hence $M_j = r_j + 1$ and

$$M = \prod_{j=1}^{R} 2^{L_j} = 2^{\sum_{j=1}^{R} L_j} = 2^w, \tag{32}$$

where w is the Hamming weight of the binary representation of r. Thus the linear span of the sequence $s(t)$ in this case equals $m\cdot 2^w$, a result that is not surprising because, in this case, $s(t)$ is in fact a GMW sequence [4].

Case 2: $\gamma \ne 0$.

As before, let $z = y^{2^{e_j}}$. Set $\eta = \gamma^{2^{e_j}}$. Then

$$g_j(z) = [1+\eta z + z^2]^{r_j} \tag{33}$$

and by factoring the quadratic (whose coefficients lie in GF(2^m)) over GF(2^n), one can write

$$g_j(z) = (z+\delta)^{r_j}(z+\delta^{-1})^{r_j} = \left(\sum_{k=0}^{r_j} \delta^{r_j-k} z^k\right)\left(\sum_{l=0}^{r_j} \delta^{l-r_j} z^l\right), \tag{34}$$

which after some work reduces to

$$g_j(z) = \sum_{k=0}^{r_j} \delta^{k\cdot}z^{k}\cdot\left[\frac{(\delta^{-2})^{k+1}+1}{\delta^{-2}+1}\right] + \sum_{k=1}^{r_j} \delta^{k-1} z^{2r_j-(k-1)}\cdot\left[\frac{(\delta^{-2})^{k}+1}{\delta^{-2}+1}\right]. \tag{35}$$

Let P_j be the number of values of k, $1 \le k \le r_j$, such that $\delta^k = 1$. Then the number of coefficients in $g_j(z)$ that vanish equals $2P_j$. Therefore,

$$M_j = 2r_j + 1 - 2P_j = 2^{L_j+1} - 1 - 2P_j. \tag{36}$$

Clearly the quantity P_j is a function of the parameter γ, and some additional information is required before P_j can be determined.

Lemma 1: There exists a 1–1 correspondence between quadratic equations of the form

$$y^2 + \gamma_i y + 1 = 0, \qquad 1 \le i \le 2^m, \tag{37}$$

where the γ_i ranges over all of GF(2^m) as i ranges over the range 1 to 2^m and elements of the set

$$Q = \{1, \alpha^{2^m+1}, \alpha^{2(2^m+1)}, \cdots, \alpha^{(2^{m-1}-1)(2^m+1)}, \alpha^{2^m-1}, \alpha^{2(2^m-1)}, \cdots, \alpha^{2^{m-1}(2^m-1)}\}. \tag{38}$$

The correspondence is obtained by associating each equation with its root.

Proof: Consider an equation

$$y^2 + \gamma\cdot y + 1 = 0, \qquad \gamma \in \mathrm{GF}(2^m). \tag{39}$$

Clearly the roots are of the form $\{\delta, \delta^{-1}\}$ for some δ. If the quadratic is reducible over GF(2^m), then one of its two roots is contained in Q. If the quadratic is irreducible, then its roots have order dividing 2^m+1 as $\delta^{-1} = \delta^{2^m}$ (by conjugacy) for a root δ. Thus, once again, one of the two roots is contained in Q. The proof is then completed by noting that, conversely, for every element δ in Q the polynomial $(y-\delta)(y-\delta^{-1})$ has coefficients in GF(2^m). Q.E.D.

Returning to the problem of estimating the linear span of the sequence $s(t)$ in (20), let us consider first the case when γ is such that $\delta = \alpha^{a(2^m+1)}$, $1 \le a \le 2^{m-1}-1$, is a root of the quadratic $y^2+\gamma\cdot y+1=0$ (the quadratic is reducible in this case). Note that as $\gamma \ne 0$, $\delta \ne 1$. Then

$$P_j = \left|\{k, 1 \le k \le r_j | \delta^{2^{e_j}\cdot k} = 1\}\right|. \tag{40}$$

But $\delta^{2^{e_j}\cdot k} = 1 \Rightarrow \alpha^{2^{e_j}\cdot ak(2^m+1)} = 1$, i.e., $a\cdot k = 0$ modulo $(2^m - 1) \Rightarrow k = 0$ modulo $((2^m-1)/g)$, where $g = gcd(a, 2^m - 1)$. Consequently,

$$P_j = \left\lfloor \frac{r_j}{(2^m-1)/g} \right\rfloor. \tag{41}$$

Thus the sequence $s(t)$ has the linear span l_{span} given by

$$l_{\text{span}} = m\cdot\prod_{j=1}^{R}\left(2^{L_j+1} - 1 - 2\left\lfloor\frac{2^{L_j}-1}{(2^m-1)/g}\right\rfloor\right). \tag{42}$$

To compare the preceding value of the linear span l_{span} with that for a GMW sequence, note that since $a \le 2^{m-1}$

TABLE II
LINEAR SPANS[a] OF FAMILIES OF NO SEQUENCES OF PERIOD 2^n-1, $n \le 14$

n	$\|S\|$	r	Linear Span (Frequency)
6	8	3	12(1), 15(1), 21(6)
8	16	7	32(1), 44(1), 52(2), 60(12)
10	32	3	20(1), 25(1), 35(30)
		5	20(1), 45(31)
		7	40(1), 55(1), 75(30)
		11	40(1), 75(1), 105(30)
		15	80(1), 105(1), 145(5), 155(25)
12	64	5	24(1), 54(63)
		11,13	48(1), 90(1), 126(62)
		23	96(1), 198(1), 234(5), 270(57)
		31	192(1), 258(1), 306(2), 330(3), 342(3), 354(6), 366(6), 378(42)
14	128	3	28(1), 35(1), 49(126)
		5,9	28(1), 63(127)
		7	56(1), 77(1), 105(126)
		11,13,19	56(1), 105(1), 147(126)
		21	56(1), 189(127)
		15	112(1), 147(1), 217(126)
		23,29	112(1), 231(1), 315(126)
		27	112(1), 175(1), 343(126)
		43	112(1), 315(1), 441(126)
		31	224(1), 301(1), 441(126)
		47	224(1), 441(1), 651(126)
		55	224(1), 385(1), 735(126)
		63	448(1), 595(1), 875(21), 889(105)

[a]The smallest value in each row corresponds to the linear span of a GMW sequence.

-1, $g \le 2^{m-1}-1 \rightarrow ((2^m-1)/g) > 2$, and therefore

$$l_{\text{span}} > m \cdot \prod_{j=1}^{R} \left(2^{L_j+1}-1-(2^{L_j}-1)\right)$$
$$= m \cdot \prod_{j=1}^{R} 2^{L_j} = m \cdot 2^w. \tag{43}$$

Thus the linear span of each such sequence $s(t)$ equals or exceeds that of the GMW sequence contained within the family.

For the case when γ is such that $\delta = \alpha^{a(2^m-1)}$, $1 \le a \le 2^{m-1}$ is a root of the quadratic $y^2+\gamma \cdot y+1=0$, the linear span can in the same manner be shown to equal

$$l_{\text{span}} = m \cdot \prod_{j=1}^{R} \left(2^{L_j+1}-1-2\left\lfloor \frac{2^{L_j}-1}{(2^m+1)/g} \right\rfloor\right), \tag{44}$$

where now $g = gcd(a, 2^m+1)$.

In this case also l_{span} exceeds the linear span of the corresponding GMW sequence. These results are summarized next using the notation introduced in this section.

Theorem 2: Let S be the family of 2^m sequences defined in (2). For each element γ_i in GF(2^m), $\gamma_i \ne 0$, set $\epsilon_i = -1$ or $+1$, depending upon whether or not the quadratic $y^2+\gamma_i \cdot y+1=0$ is reducible over GF(2^m). Also, for each γ_i let δ_i be the root of the quadratic $y^2+\gamma_i \cdot y+1=0$ lying in Q (see (38)). Let the integer a_i be determined from either

$$\delta_i = \alpha^{a_i(2^m+1)}, \qquad \text{when } \epsilon_i = -1$$

or

$$\delta_i = \alpha^{a_i(2^m-1)}, \qquad \text{when } \epsilon_i = +1$$

and set $g_i = gcd(a_i, 2^m+\epsilon_i)$. Then the linear span $l_{\text{span}}(i)$ of the ith sequence $s_i(t)$ in S is given by

$$l_{\text{span}}(i) = m \cdot \prod_{j=1}^{R} \left\{2^{L_j+1}-1-2\left\lfloor \frac{2^{L_j}-1}{(2^m+\epsilon_i)/g_i} \right\rfloor\right\}. \tag{45}$$

When $\gamma_i = 0$, the linear span $l_{\text{span}}(i)$ is given by

$$l_{\text{span}}(i) = m \cdot 2^w. \tag{46}$$

Table II shows the linear span distribution for all possible families of No sequences of period $\le 2^{14}-1 = 16\,383$.

IV. Implementation

For the purposes of implementation, we note that the expression for a No sequence can be rewritten in the form

$$s_z(t) = \text{tr}_1^m\left\{\left[\text{tr}_m^n(\alpha^t) + \alpha^{2^{m-1} \cdot T \cdot (t+z)}\right]^r\right\}, \tag{47}$$

where we have used a property of the trace function and rewritten the parameter γ identifying the particular sequence within the family in the form

$$\gamma = \alpha^{T \cdot z}, \qquad 0 \le z \le 2^m-2. \tag{48}$$

We set $z = -\infty$ for the case $\gamma = 0$.

The sequence $\text{tr}_m^n(\alpha^t)$ that appears within brackets may be regarded as a (generalized) m-sequence [15, p. 315] over GF(2^m) satisfying a linear recursion of degree 2. Let $m_\alpha(z)$ be the minimum (primitive) polynomial of α over GF(2^m). Then $m_\alpha(x)$ is of the form

$$m_\alpha(x) = x^2 + \beta_1 \cdot x + \beta_2 \tag{49}$$

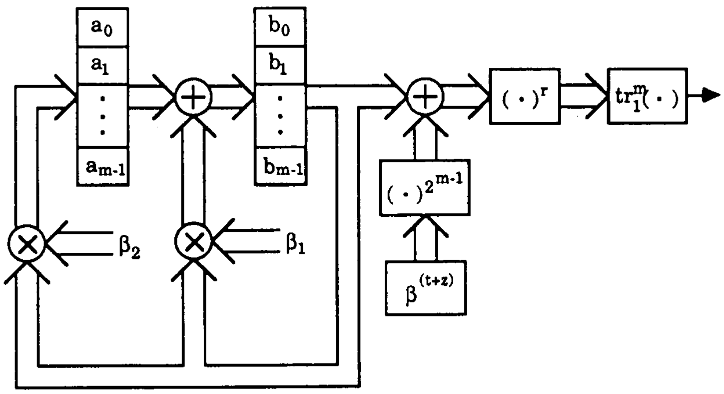

Fig. 2. No sequence generator in Galois configuration.

for some β_1 and β_2 in GF(2^m). Let $\beta=\alpha^T$, $T=2^m+1$. Then β is a primitive element of GF(2^m) and $\{1,\beta,\beta^2,\cdots,\beta^{m-1}\}$, a basis for GF($2^m$) over GF(2). Clearly any element in GF(2^m) can be expressed as an m-dimensional vector over GF(2). Using (49), as discussed in the previous section, we can realize the generalized m-sequence generator in the Galois configuration [15] (Fig. 2). Each block in the shift register contains m registers and each arrow (except the final arrow at the output) represents the flow of information along m binary channels. Let β^t be the output of the second shift register block in Fig. 2. For every value of t the output can be expressed in terms of the preceding polynomial basis for GF(2^m) as follows:

$$\beta^t=\sum_{i=0}^{m-1}\nu_i\cdot\beta^i, \tag{50}$$

with the coefficients ν_i (which are functions of t) lying in GF(2). In order to determine the input to the first two shift register stages, we need to find the (Boolean) coefficient functions $f_i(\nu_0,\nu_1,\cdots,\nu_{m-1})$ and $g_i(\nu_0,\nu_1,\cdots,\nu_{m-1})$ satisfying the following equations:

$$\beta_2\cdot\beta^t=\sum_{i=0}^{m-1}f_i(\nu_0,\nu_1,\cdots,\nu_{m-1})\cdot\beta^i \tag{51}$$

$$\beta_1\cdot\beta^t=\sum_{i=0}^{m-1}g_i(\nu_0,\nu_1,\cdots,\nu_{m-1})\cdot\beta^i. \tag{52}$$

Clearly, $f_i(\nu_0,\nu_1,\cdots,\nu_{m-1})$ is fed into location a_i in the first shift register block and the sum of $g_i(\nu_0,\nu_1,\cdots,\nu_{m-1})$, and the i output of the first shift register (corresponding to location a_i) is fed into the shift register b_i in the second shift register block. We need another m shift registers to generate $\beta^{(t+z)}$ as a sequence of m-dimensional vectors over GF(2) (these registers simply constitute a *binary m-sequence generator*). The nonlinear function $(\cdot)^{2^{m-1}}$ can be realized by implementing the logic needed to generate the coefficient functions $h_{1,i}(\nu_0,\nu_1,\cdots,\nu_{m-1})$ in the following equation:

$$\left(\beta^{(t+z)}\right)^{2^{m-1}}=\left(\sum_{i=0}^{m-1}\nu_i\cdot\beta^i\right)^{2^{m-1}}=\sum_{i=0}^{m-1}h_{1,i}(\nu_0,\nu_1,\cdots,\nu_{m-1})\cdot\beta^i. \tag{53}$$

Finally, with regard to the nonlinear function $(\cdot)^r$, we need calculate only one of the m coefficient functions $h_{2,i}(\nu_0,\nu_1,\cdots,\nu_{m-1})$ in the equation

$$\left(\beta^t\right)^r=\sum_{i=0}^{m-1}h_{2,i}(\nu_0,\nu_1,\cdots,\nu_{m-1})\cdot\beta^i \tag{54}$$

because the function $\mathrm{tr}_1^m(\cdot)$ corresponds precisely to a choice of one of these coefficients. By changing the initial conditions of shift registers of β^{t+z} for a given (fixed) set of initial conditions for the first and second shift register blocks (this corresponds to changing the value z), we accomplish the switch from one No sequence to another without any change in the circuitry. Thus a circuit that can generate any one of the No sequences within a family can be implemented using $3\cdot m$ shift registers and some additional logic.

V. An Example

As an example, consider the case $n=6$, $r=3$ when $N=63$, $m=3$, and $T=9$. The corresponding family S of No sequences (each sequence has period 63) is then given by

$$S=\{s_z(t)\,|\,z=-\infty,0,1,2,3,4,5,6\}, \tag{55}$$

where

$$s_z(t)=\mathrm{tr}_1^3\left\{\left[\mathrm{tr}_3^6(\alpha^t)+\alpha^{4\cdot 9\cdot(t+z)}\right]^3\right\} \tag{56}$$

and α is a primitive element of GF(2^6) having minimum polynomial $x^6+x^5+x^2+x+1$. The generation of a GMW sequence using the same primitive element is dis-

TABLE III
AN EXAMPLE NO FAMILY OF PERIOD $N = 63$

	No Sequences	Linear Span
$s_{-\infty}(t)$	000001010010011101011101001011100011001111110010010111001110100	12
$s_0(t)$	100001000111000001101011010001010010110010011011001001010011011	15
$s_1(t)$	1000111000001011000100000001110011101110110001100110000010101101	21
$s_2(t)$	110100011111110010100000011011010010100100000000100011011110001 1	21
$s_3(t)$	011110111011010111110101111101011000110001111000100000101111000	21
$s_4(t)$	1011001100000110101010101000001100100000101000101111100101001110	21
$s_5(t)$	011111001100110010100110100111001101011111111111001011000000110	21
$s_6(t)$	011010101101101010011111011000101110101000100110111111110010001	21

cussed in [15, Example 5.12]. The eight sequences belonging to the family are listed in Table III.

For this family, the correlation function (from Theorem 1)

$$R_{i,j}(\tau), \qquad i, j \in \{-\infty, 0, 1, \cdots, 6\}, 0 \le \tau \le 62, \quad (57)$$

takes on values in the set $\{-1, -9, 7\}$ whenever either $i \neq j$ or $\tau \neq 0$.

With reference to the expansion for r given in (24), we have in this example $R = 1$ and $L_1 = 2$. Using (45) and (46) the linear spans of the sequences belonging to the family S can be shown to lie in the set $\{12, 15, 21\}$ (see Table III).

A binary implementation of the generator for a sequence belonging to the family is shown in Fig. 3. Here,

$$\beta = \alpha^9 \quad (58)$$

and is a primitive element of GF(2^3). The minimum polynomials $m_\alpha(x)$ and $m_\beta(x)$ of α and β over GF(2^3) and GF(2), respectively, turn out to be

$$m_\alpha(x) = x^2 + \beta^6 \cdot x + \beta \quad (59)$$

and

$$m_\beta(x) = x^3 + x + 1. \quad (60)$$

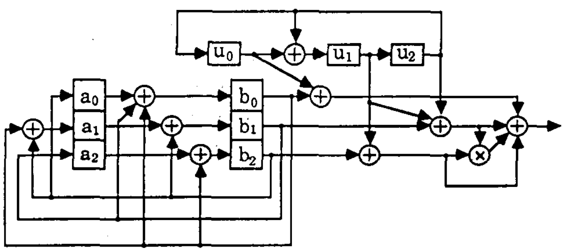

Fig. 3. Generation of No sequence of period 63.

Choosing $\{1, \beta, \beta^2\}$ as a basis for GF(2^3) over GF(2), the elements β^t can be expressed in the form

$$\beta^t = \nu_0 \cdot 1 + \nu_1 \cdot \beta + \nu_2 \cdot \beta^2, \quad (61)$$

where the coefficients ν_i are functions of t and lie in $\{0, 1\}$. The coefficient functions $\{f_i, g_i | i = 0, 1, 2\}$ are easily determined by noting, using (60), that

$$\begin{aligned} \beta \cdot \beta^t &= \beta \cdot (\nu_0 \cdot 1 + \nu_1 \cdot \beta + \nu_2 \cdot \beta^2) \\ &= \nu_2 \cdot 1 + (\nu_0 + \nu_2) \cdot \beta + \nu_1 \cdot \beta^2 \end{aligned} \quad (62)$$

$$\begin{aligned} \beta^6 \cdot \beta^t &= \beta^6 \cdot (\nu_0 \cdot 1 + \nu_1 \cdot \beta + \nu_2 \cdot \beta^2) \\ &= (\nu_0 + \nu_1) \cdot 1 + \nu_2 \cdot \beta + \nu_0 \cdot \beta^2. \end{aligned} \quad (63)$$

The nonlinear functions $\{h_{1,i}, h_{2,i} | i = 0, 1, 2\}$ corresponding to raising to the fourth and third powers $(\cdot)^4$ and $(\cdot)^3$ are found just as easily from (60):

$$\begin{aligned} (\beta^t)^4 &= (\nu_0 \cdot 1 + \nu_1 \cdot \beta + \nu_2 \cdot \beta^2)^4 \\ &= \nu_0 \cdot 1 + (\nu_1 + \nu_2) \cdot \beta + \nu_1 \cdot \beta^2 \end{aligned} \quad (64)$$

$$\begin{aligned} (\beta^{(t+z)})^3 &= (\nu_0 \cdot 1 + \nu_1 \cdot \beta + \nu_2 \cdot \beta^2)^3 \\ &= (\nu_0 + \nu_1 + \nu_2 + \nu_1 \cdot \nu_2) \cdot 1 + \cdots. \end{aligned} \quad (65)$$

As observed earlier, it is sufficient for the purpose of implementation to determine only one coefficient function $h_{2,0}$. Finally, different sequences within the family are obtained by simply changing the initial contents of shift register (u_0, u_1, u_2) for a fixed set of initial contents for the other shift registers.

VI. NUMBER OF DISTINCT FAMILIES AVAILABLE

Complete specification of a family of No sequences requires that, in addition to the length of each sequence within the family, the primitive element α and the integer r (see (3)) be given also.

Our interest in this section is to determine the number of distinct families available when only the length N of the sequences is specified.

Accordingly we modify our earlier notation and rewrite:

$$S(\alpha, r) = \left\{ \mathrm{tr}_1^m \left\{ \left[\mathrm{tr}_m^n(\alpha^{2t}) + \gamma \cdot \alpha^{Tt} \right]^r \right\} \middle| \gamma \in \mathrm{GF}(2^m) \right\}. \quad (66)$$

For our purposes, we define two families to be distinct if and only if no sequence belonging to one family is a cyclic shift of a sequence that is an element of a second family.

Lemma 2, which follows, identifies necessary and sufficient conditions under which, with this definition, two families are distinct.

Lemma 2: Let n, N, m, T, and $S(\cdot, \cdot)$ be as defined earlier. Let α_1 and α_2 be primitive elements of GF(2^n) and let r_1 and r_2, $1 \le r_1, r_2 \le 2^m - 2$ be integers relatively prime to $2^m - 1$. Then $S(\alpha_1, r_1)$ and $S(\alpha_2, r_2)$ are distinct unless for some integers k and l, $0 \le k \le n-1$, $0 \le l \le m-1$, $\alpha_2 = \alpha_1^{2^k}$, and $r_1 = 2^l \cdot r_2$, in which case

$$S(\alpha_1, r_1) = S(\alpha_2, r_2). \tag{67}$$

Proof: Let $s_1(t)$ and $s_2(t)$ be elements of $S(\alpha_1, r_1)$ and $S(\alpha_2, r_2)$, respectively, given by

$$s_1(t) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n\left(\alpha_1^{2t}\right) + \gamma_1 \cdot \alpha_1^{Tt}\right]^{r_1}\right\} \tag{68}$$

and

$$s_2(t) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n\left(\alpha_2^{2t}\right) + \gamma_2 \cdot \alpha_2^{Tt}\right]^{r_2}\right\}, \tag{69}$$

in which γ_1 and γ_2 are elements of $\mathrm{GF}(2^m)$, not necessarily distinct. Assume

$$s_1(t) = s_2(t + \tau) \tag{70}$$

for some cyclic shift τ, $0 \le \tau \le 2^n - 2$. Let t_1 and t_2 be the *digits* in the base-T expansion of t as before, i.e.,

$$t = T \cdot t_1 + t_2, \qquad 0 \le t_1 \le 2^m - 2, 0 \le t_2 \le 2^m. \tag{71}$$

Then upon expanding, (70) yields

$$\mathrm{tr}_1^m\left\{\alpha_1^{2 r_1 T t_1}\left[\mathrm{tr}_m^n\left(\alpha_1^{2t_2}\right) + \gamma_1 \cdot \alpha_1^{Tt_2}\right]^{r_1}\right\} = \mathrm{tr}_1^m\left\{\alpha_2^{2 r_2 T t_1}\left[\mathrm{tr}_m^n\left(\alpha_2^{2(t_2+\tau)}\right) + \gamma_2 \cdot \alpha_2^{T(t_2+\tau)}\right]^{r_2}\right\}. \tag{72}$$

For a fixed value of t_2, either sequence $s_1(t)$ or $s_2(t+\tau)$ (when regarded as a sequence in the variable t_1, $0 \le t_1 \le 2^m - 2$) is either the all-zero sequence or else a cyclic shift of an m-sequence of period $2^m - 1$, $\mathrm{tr}_1^m(\alpha_1^{2Tr_1t_1})$, or $\mathrm{tr}_1^m(\alpha_2^{2Tr_2t_1})$, respectively.

Clearly the two m-sequences must be the same (to within a cyclic shift), and we therefore obtain

$$\alpha_1^{Tr_1} = \alpha_2^{Tr_2 \cdot 2^l} \tag{73}$$

for some integer l, $0 \le l \le m-1$. Let

$$\alpha_2 = \alpha_1^d. \tag{74}$$

Then (73) may be rewritten as

$$r_1 = d \cdot r_2 \cdot 2^l \bmod (2^m - 1). \tag{75}$$

Using (75), a property of the trace function, and the fact that $gcd(r_2, 2^m - 1) = 1$, one can prove that (72) is possible if and only if

$$\left[\mathrm{tr}_m^n\left(\alpha_1^{2t_2}\right) + \gamma_1 \cdot \alpha_1^{Tt_2}\right]^d = \left[\mathrm{tr}_m^n\left(\alpha_2^{2(t_2+\tau)}\right) + \gamma_2 \cdot \alpha_2^{T(t_2+\tau)}\right], \quad 0 \le t_2 \le T-1. \tag{76}$$

It is simple to verify that (76) is true for all t_2, $0 \le t_2 \le 2^n - 2$ if it is true for all values of t_2 specified in (76).

Let $x = \alpha_1^{t_2}$. Then (76) may be rewritten in the form

$$x^{2d}\left[1 + \gamma_1 \cdot x^{2^m - 1} + x^{2(2^m-1)}\right]^d = x^{2d}\left[\alpha_2^{2\tau} + \alpha_2^{T\tau} \cdot \gamma_2 \cdot x^{d(2^m-1)} + \alpha_2^{2^{m+1}\tau} \cdot x^{2d(2^m-1)}\right]. \tag{77}$$

The right side is a polynomial in x having three nonzero coefficients. Equality can hold in (77) if and only if the same is true for the left side. The number of powers of x having nonzero coefficients that appear in the expansion on the left side may be counted using precisely the same technique used in determining the linear span of the sequence. It will then become apparent that the number of terms having a nonzero coefficient equals 3 if and only if d is power of 2, i.e.,

$$d = 2^k, \qquad \text{some } k, \qquad 0 \le k \le n-1. \tag{78}$$

Inserting (78) into (75), we obtain

$$r_1 = r_2 \cdot 2^{l+k} \bmod (2^m - 1) \tag{79}$$

and we have thus established the necessary condition identified in the Lemma 2.

To prove sufficiency, note that when

$$d = 2^k, \qquad \text{and} \qquad r_1 = 2^l \cdot r_2, \tag{80}$$

we have

$$s_1(t) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n\left(\alpha_1^{2t}\right) + \gamma_1 \cdot \alpha_1^{Tt}\right]^{r_2}\right\} \tag{81}$$

and

$$s_2(t) = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n\left(\alpha_1^{2^{k+1} \cdot t}\right) + \gamma_2 \cdot \alpha_1^{Tt \cdot 2^k}\right]^{r_2}\right\} = \mathrm{tr}_1^m\left\{\left[\mathrm{tr}_m^n\left(\alpha_1^{2t}\right) + \gamma_2^{2^{m-k}} \cdot \alpha_1^{Tt}\right]^{r_2}\right\}, \tag{82}$$

which equals $s_1(t)$ whenever

$$\gamma_2^{2^{m-k}} = \gamma_1. \tag{83}$$

However, since the operation of raising an element of $\mathrm{GF}(2^m)$ to a power of 2 merely permutes the elements amongst themselves, it is clear that under the conditions stated in (80),

$$S(\alpha_1, r_1) = S(\alpha_2, r_2).$$

Q.E.D.

Thus $S(\alpha_1, r_1)$ and $S(\alpha_2, r_2)$ are cyclically distinct whenever at least one of the following conditions is violated:

1) α_2 is a conjugate of α_1;
2) r_1 and r_2 belong to the same cyclotomic coset of $\mathrm{GF}(2^m)$.

This proves the following.

Theorem 3: For a given period $N = 2^n - 1$, the number N_{No} of distinct No sequence families that can be constructed equals

$$N_{\mathrm{No}} = \frac{\phi(2^m - 1)}{m} \cdot \frac{\phi(2^n - 1)}{n}, \tag{84}$$

where $\phi(\cdot)$ is Euler's phi function and $m = n/2$.

Table IV contains a listing of the values of N_{No} for $n \le 26$, n even.

TABLE IV
NUMBER OF DISTINCT FAMILIES OF NO SEQUENCES OF PERIOD $2^n - 1$

n	Period	N_{No}
6	63	12
8	255	32
10	1023	360
12	4095	864
14	16383	13608
16	65535	32768
18	262143	373248
20	1048575	1440000
22	4194303	21125632
24	16777215	39813120
26	67108863	1083537000

REFERENCES

[1] R. A. Scholtz, "The origins of spread-spectrum communications," *IEEE Trans. Commun.*, vol. COM-30, pp. 822–854, May 1982.

[2] M. P. Ristenbatt and J. L. Daws, Jr., "Performance criteria for spread spectrum communications," *IEEE Trans. Commun.*, vol. COM-25, no. 8, pp. 756–763, Aug. 1977.

[3] D. V. Sarwarte and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–620, May 1980.

[4] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 3, pp. 548–553, May 1984.

[5] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 6, pp. 858–864, Nov. 1982.

[6] P. V. Kumar and R. A. Scholtz, "Bounds on the linear span of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 6, pp. 854–862, Nov. 1983.

[7] A. Lempel and M. Cohn, "Maximal families of bent sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 865–868, Nov. 1982.

[8] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, no. 5, pp. 619–621, Oct. 1967.

[9] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

[10] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285 (AD632574), 1966.

[11] ——, "Weight distribution of Bose–Chaudhuri–Hocquenghem codes," in *Combinatorial Mathematics and its Applications*. Chapel Hill, NC: University of North Carolina Press, 1969.

[12] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.

[13] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 732–736, Nov. 1976.

[14] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967; revised edition, Laguna Hills, CA: Aegean Park Press, 1982.

[15] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I. Rockville, MD: Computer Science Press, 1985.

[16] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[18] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics. New York: Springer-Verlag, 1974.