A NEW FAMILY OF BINARY PSEUDORANDOM SEQUENCES HAVING OPTIMAL PERIODIC CORRELATION PROPERTIES AND LARGE LINEAR SPAN

Jong-Seon No and P. Vijay Kumar

Communication Sciences Institute, Department of Electrical Engineering
University of Southern California
Los Angeles, CA 90089-0272

ABSTRACT

A collection of families of binary {0,1} pseudorandom sequences (referred to as the families of *No* sequences) is introduced in this paper. 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 is large. The balance properties of such families are evaluated and a count of the number of distinct families of given period N that can be contructed also provided.

I. INTRODUCTION

In a spread-spectrum multiple-access communication system, it is desirable to employ as signature sequences, code sequences having low nontrivial auto and cross-correlation values and large linear span [1,2,3,14].

The families of bent [5,6,7] and Gold [8,9] sequences as well as the small and large families of Kasami sequences [10,11] are examples of families of sequences having desirable correlation properties. However, with the exception of the bent sequence families, the sequences in these families possess extremely small values of linear span.

In this paper, we present new families of binary sequences (hereafter, referred to as the families of *No* sequences) which possess optimal (with respect to the Welch bound [12]) correlation properties and large linear span.

Each sequence within a family has period = $2^n - 1$, 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 $2^m + 1$. Within each family is contained a Gordon-Mills-Welch (GMW) sequence [4], and the families of sequences include as a special case, the families of Kasami sequences (small set).

The linear span of these sequences is large.

A comparison of the properties of the various sequence families including the ones introduced here 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 are also discussed here. Section III shows how these sequences may be implemented and Section IV provides an example. The final section, Section V, presents a count of the number of distinct families (when the period is given) that are available.

II. OPTIMALITY OF THE CORRELATION VALUES

For any pair of integers $k, l > 0$, $k \mid l$, 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 $T = 2^m + 1$.

Let

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

be the family 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.

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

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

Jong-Seon No is currently with Hughes Network Systems, Germantown, Maryland. P. Vijay Kumar is with the Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-0272.

This work was supported by the National Security Agency on Contract No. MDA904-85-H-0010.

0802 CH2538-7/88/0000-0802 $1.00 © 1988 IEEE

Theorem 1: $\forall i, j, \tau,\ 1 \le i, j \le 2^m,\ 0 \le \tau \le N-1,$

$$R_{i,j}(\tau) \in \{-2^m-1, -1, 2^m-1\}, \tag{5}$$

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

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

$$t = T \cdot t_1 + t_2, \quad 0 \le t_1 \le 2^m-2,\ 0 \le t_2 \le T-1. \tag{6}$$

Noting that

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

and that

$$\alpha^{T^2 t_1} = \alpha^{2Tt_1}, \tag{8}$$

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

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

As a result, we have that

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

where we define

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

If, for a fixed value of t_2, $0 \le t_2 \le T-1$, $f_1(t_2) \ne 0$, 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 $f_1(t_2)$. When $f_1(t_2) = 0$, of course, 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 [13], it then follows that if z_1 denotes the number of values of t_2 for which $f_1(t_2) = 0$, i.e.,

$$z_1 = |\{t_2, 0 \le t_2 \le T-1 \mid f_1(t_2) = 0\}|, \tag{12}$$

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:

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

Thus we will have proven the theorem 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

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

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:

$$z_1 = \frac{z_2}{2^m-1}. \tag{15}$$

Next, define, $0 \le t \le N-1$,

$$f_2(t) = \mathrm{tr}_m^n\{\alpha^{2t} \cdot (1 + \alpha^{2\tau})\} + \alpha^{Tt} \cdot (\gamma_i \cdot \alpha^{T\tau} + \gamma_j), \tag{16}$$

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

$$f_2(t) = 0 \iff f_1(t) = 0, \quad 0 \le t \le N-1. \tag{17}$$

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 does 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:

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

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

Case (i) $\tau = 0,\ \gamma_i \ne \gamma_j$.

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 this implies

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

Case (ii) $\tau \ne 0$.

In this case, $f_2(x)$ vanishes iff 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 above 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 of No sequences with other well-known sequence sets, set $\gamma_i = 0$ in (3) to obtain the GMW sequence contained within each 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.

III. IMPLEMENTATION

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

$$s(t) = \mathrm{tr}_1^m\{[\ \mathrm{tr}_m^n(\alpha^t) + \alpha^{2^{m-1}\cdot T(t+z)}]^r\}, \qquad (20)$$

where we have rewritten the parameter γ identifying the particular sequence within the family in the form:

$$\gamma = \alpha^{Tz}, \quad 0 \le z \le 2^m - 2. \qquad (21)$$

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

The sequence $\mathrm{tr}_m^n(\alpha^t)$ that appears within parenthesis may be regarded as a (generalized m-sequence) sequence over $GF(2^m)$ satisfying a linear recursion of degree 2. Fig. 2 shows a schematic of how such a sequence may be implemented.

In practice, of course, one would replace arithmetic in the intermediate field $GF(2^m)$ with equivalent binary arithmetic.

IV. AN EXAMPLE

As an example consider the case, $n = 6$, $r = 3$, when $N = 63$, $m = 3$, and $T = 9$. Let $S(\alpha, 3)$ be the family of No sequences (each sequence has period 63) given by:

$$S(\alpha, 3) = \{\ \mathrm{tr}_1^3\{[\ \mathrm{tr}_3^6(\alpha^t) + \gamma\cdot\alpha^{4\cdot 9t}]^3\} \mid \gamma \in GF(2^3)\}, \qquad (22)$$

where α is a primitive element of $GF(2^6)$ having minimum polynomial $x^6 + x^5 + x^2 + x + 1$.

The eight sequences belonging to the family are listed in Table II.

For this family, the correlation function, $R_{i,j}(\tau)$, $i, j \in \{-\infty, 0, 1, \cdots, 6\}$, $0 \le \tau \le 2^6 - 2$, either $i \ne j$ or $\tau \ne 0$, takes on values in the set {-1, -9, 7}.

A binary implementation of the generator for a sequence belonging to the family is shown in Fig. 3. Here, computations over $GF(2^m)$ have been replaced by binary operations essentially by representing an element in $GF(2^m)$ as a linear combination of the basis vectors $\gamma_0 = 1$, $\gamma_1 = \alpha^9$, $\gamma_2 = \alpha^{18}$ for $GF(8)$ over $GF(2)$. Different sequences within the family are obtained by simply changing the initial contents of shift register $C = (c_0, c_1, c_2)$.

V. 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 equation (3)) be also given.

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:

$$S(\alpha, r) = \{\ \mathrm{tr}_1^m\{[\ \mathrm{tr}_m^n(\alpha^{2t}) + \gamma\cdot\alpha^{Tt}]^r\} \mid \gamma \in GF(2^m)\}. \qquad (23)$$

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

Lemma below, identifies necessary and sufficient conditions under which two families are distinct under this definition:

Lemma 1: 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

$$S(\alpha_1, r_1) = S(\alpha_2, r_2). \qquad (24)$$

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

$$s_1(t) = \mathrm{tr}_1^m\{[\ \mathrm{tr}_m^n(\alpha_1^{2t}) + \gamma_1\cdot\alpha_1^{Tt}]^{r_1}\} \qquad (25)$$

and

$$s_2(t) = \mathrm{tr}_1^m\{[\ \mathrm{tr}_m^n(\alpha_2^{2t}) + \gamma_2\cdot\alpha_2^{Tt}]^{r_2}\}, \qquad (26)$$

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

Assume

$$s_1(t) = s_2(t + \tau) \qquad (27)$$

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.,

$$t = T\cdot t_1 + t_2, \quad 0 \le t_1 \le 2^m - 2,\ 0 \le t_2 \le 2^m. \qquad (28)$$

Then upon expanding, (27) yields:

$$\mathrm{tr}_1^m\{\alpha_1^{2r_1Tt_1}[\ \mathrm{tr}_m^n(\alpha_1^{2t_2}) + \gamma_1\cdot\alpha_1^{Tt_2}]^{r_1}\}$$

$$= \mathrm{tr}_1^m\{\alpha_2^{2r_2Tt_1}[\ \mathrm{tr}_m^n(\alpha_2^{2(t_2+\tau)}) + \gamma_2\cdot\alpha_2^{T(t_2+\tau)}]^{r_2}\}. \qquad (29)$$

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:

$$\alpha_1^{Tr_1} = \alpha_2^{Tr_2\cdot 2^l} \qquad (30)$$

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

$$\alpha_2 = \alpha_1^d. \qquad (31)$$

Then (30) may be rewritten as:

$$r_1 = d\cdot r_2\cdot 2^l \mod (2^m - 1). \qquad (32)$$

Using (32), a property of the trace function, and the fact that $gcd(r_2, 2^m - 1) = 1$, one can prove that (29) is possible iff

$$[\,\mathrm{tr}_m^n(\alpha_1^{2t_2}) + \gamma_1 \cdot \alpha_1^{Tt_2}]^d$$

$$= [\,\mathrm{tr}_m^n(\alpha_2^{2(t_2+\tau)}) + \gamma_2 \cdot \alpha_2^{T(t_2+\tau)}],\quad 0 \le t_2 \le T-1. \quad (33)$$

It is simple to verify that (33) 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 (33).

Let $x = \alpha_1^{t_2}$. Then (33) may be rewritten in the form:

$$x^{2d}[1 + \gamma_1 \cdot x^{2^m-1} + x^{2(2^m-1)}]^d$$

$$= x^{2d}[\alpha_2^{2\tau} + \alpha_2^{T\tau} \cdot \gamma_2 \cdot x^{d(2^m-1)} + \alpha_2^{2^{m+1}\tau} \cdot x^{2d(2^m-1)}]. \quad (34)$$

The right hand side is a polynomial in x having 3 nonzero coefficients. Equality can hold in (34) iff the same is true for the left hand side. The number of powers of x having nonzero coefficients that appear in the expansion on the left hand side, may then be counted. It will then become apparent that the number of terms having a nonzero coefficient will equal 3 iff d is power of 2, i.e.,

$$d = 2^k, \text{ some } k, \quad 0 \le k \le n-1. \quad (35)$$

Inserting (35) into (32), we obtain that

$$r_1 = r_2 \cdot 2^{l+k} \mod (2^m - 1) \quad (36)$$

and thus we have established the necessary condition identified in the Lemma 1.

To prove sufficiency, note that when:

$$d = 2^k \quad \text{and} \quad r_1 = 2^l \cdot r_2, \quad (37)$$

we have

$$s_1(t) = \mathrm{tr}_1^m\{[\,\mathrm{tr}_m^n(\alpha_1^{2t}) + \gamma_1 \cdot \alpha_1^{Tt}]^{r_2}\} \quad (38)$$

and

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

$$= \mathrm{tr}_1^m\{[\,\mathrm{tr}_m^n(\alpha_1^{2t}) + \gamma_2^{2^{m-k}} \cdot \alpha_1^{Tt}]^{r_2}\}, \quad (39)$$

which equals $s_1(t)$, whenever

$$\gamma_2^{2^{m-k}} = \gamma_1. \quad (40)$$

However, since the operation of raising an element of $GF(2^m)$ to a power of 2 merely permutes the elements amongst themselves, it is clear that under the conditions stated in (37),

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

q.e.d.

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

(i) α_2 is a conjugate of α_1.
(ii) r_1 and r_2 belong to the same cyclotomic coset of $GF(2^m)$.

This proves:

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

$$N_{No} = \frac{\phi(2^m-1)}{m} \cdot \frac{\phi(2^n-1)}{n}, \quad (41)$$

where $\phi(\cdot)$ is Euler's *phi* function and $m = \frac{n}{2}$.

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

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, pp. 756-763, Aug. 1977.

[3] D. V. Sarwarte and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593-620, May 1980.

[4] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, 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, 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, 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, pp. 619-621, Oct. 1967.

[9] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inform. Theory*, vol. IT-14, 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] T. Kasami, "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, pp. 397-399, May 1974.

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

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

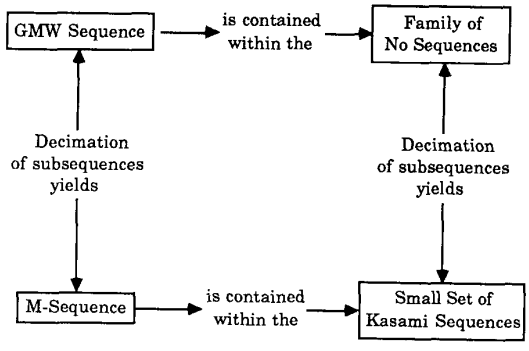

Fig. 1. Relating No sequences to Kasami sequences.

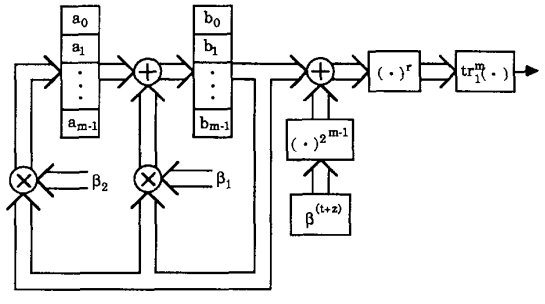

Fig. 2. No sequence generator in Galois configuration.

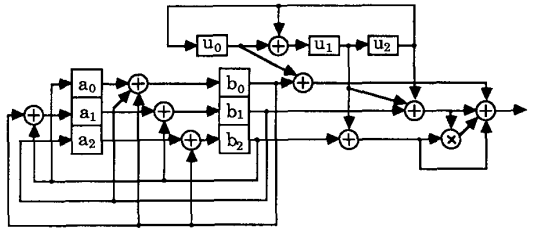

Fig. 3. Generator of No sequence of period 63 in Galois configuration.

TABLE I Comparison Of Various Families Of Sequences Of Period $2^n - 1$

Family	n	Size of Family	Maximum Correlation Value	Maximum Linear Span
Gold	$2m+1$	2^n+1	$1+2^{(n+1)/2}$	$2n$
Gold	$4m+2$	2^n+1	$1+2^{(n+2)/2}$	$2n$
Kasami (Small Set)	$2m$	$2^{n/2}$	$1+2^{n/2}$	$3n/2$
Kasami (Large Set)	$2m$	$2^{n/2}(2^n+1)$	$1+2^{(n+2)/2}$	$5n/2$
Bent	$4m$	$2^{n/2}$	$1+2^{n/2}$	$\geq\binom{n/2}{n/4}\cdot 2^{n/4}$
No	$2m$	$2^{n/2}$	$1+2^{n/2}$	Large

TABLE II An Example Of No Family Of Period $N = 63$

	Sequences
$s_{-\infty}(t)$	000001010010011101011101001011100011001111110010010111001110100
$s_0(t)$	100001000111000001101011010001010010110010011011001001010011011
$s_1(t)$	100011100000101100010000001110011101110110001100110000010101101
$s_2(t)$	110100011111100101000000110110100101001000000001000110111100011
$s_3(t)$	011110111011010111101011111010110001100011110001000001011110000
$s_4(t)$	101100110000011010101010100000110010000101000101111100101001110
$s_5(t)$	011111001100110010100110100111001101011111111111001011000000110
$s_6(t)$	011010101101101010011111011000101110101000100110111111111010001

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

TABLE III Number Of Distinct Families Of No Sequences Of Period $2^n - 1$

n	Period	N_{No}
6	63	12
8	255	32
10	1,023	360
12	4,095	864
14	16,383	13,608
16	65,535	32,768
18	262,143	373,248
20	1,048,575	1,440,000
22	4,194,303	21,125,632
24	16,777,215	39,813,120
26	67,108,863	1,083,537,000