Generalization of GMW Sequences and No Sequences

Jong-Seon No, Member, IEEE

Abstract—In this correspondence, GMW sequences and families of No sequences are generalized. Generalized GMW sequences have ideal autocorrelation and balance properties and generalized No sequences also have optimal correlation properties in terms of Welch’s lower bound. The linear spans of the generalized GMW and No sequences appear to be large although we do not at present have a closed-form expression for the linear span. A count of the numbers of cyclically distinct generalized GMW sequences and generalized No sequences that can be constructed is provided. Generalized GMW sequences have also been found in the literature by Klapper et al. under the name “cascaded GMW sequences.”

Index Terms—Generalized GMW sequences, generalized No sequences, linear span, autocorrelation values, correlation functions.

I. INTRODUCTION

Pseudonoise (PN) sequences have been successfully employed as spreading sequences for low probability of intercept and as signature sequences for code-division multiple access in a spread-spectrum communication system [2]. Several characteristics which are desirable in a family of PN sequences are the above applications are long period, low out-of-phase autocorrelation values, low crosscorrelation values, low nontrivial partial period correlation values, large linear span, a balance of symbols, the availability of a large number of distinct sequences, and ease of implementation.

Several families of pseudorandom sequences having good correlation properties such as m-sequences, GMW sequences, Kasami sequences, Gold sequences, bent sequences, No sequences, and d-form sequences [1], [4]–[6], [8]–[11], [13]–[15] have been discovered. But the linear spans of m-sequences, Kasami sequences, and Gold sequences are very short. PN sequences with large linear span, which are needed for low probability of intercept system, have been found such as GMW sequences, bent sequences, and No sequences.

In this correspondence, the generalization of GMW sequences is introduced, which has ideal autocorrelation and balance properties. Families of No sequences are generalized, which also have optimal correlation properties in terms of Welch’s lower bound [12]. The linear spans of the generalized GMW sequences and generalized No sequences appear to be very large although we do not at present have closed-form expressions for the linear spans. In Section II, GMW sequences are generalized, these ideal full-period autocorrelation properties are derived, and a count of the number of cyclically distinct generalized GMW sequences that can be constructed is provided. It is also shown how the families of No sequences can be generalized in a similar manner and optimal correlation properties are derived in Section III. Here, the number of distinct families of generalized No sequences of given period is derived, too. Proofs of all theorems, which are just straightforward extensions of the proofs for GMW and No sequences [2], [6], [8] are omitted.

REFERENCES


Manuscript received October 13, 1994; revised May 29, 1995. The work of some parts of this correspondence were carried out independently in the author’s Ph.D. dissertation [5], in the paper by Klapper et al. [13], and in the paper by Klapper [14].

The author is with the Department of Electronic Engineering, Kon-kuk University, 93-1 Mokjin-Dong, Kwangjin-Gu, Seoul, 133-701, Korea. Publisher Item Identifier S 0018-9448(96)00020-X.
II. GENERALIZATION OF GMW SEQUENCES

The GMW sequences analyzed in [8] are the characteristic functions of certain Gordon, Mills, and Welch difference sets. We consider the characteristic functions of a larger class of GMW difference sets. These sequences, of course, share the ideal autocorrelation and balance properties of an \( m \)-sequence and may be regarded as a straightforward generalization of the GMW sequences considered in [8]. We begin by defining generalized GMW sequences.

**Definition 1:** Let \( n \) and \( m_i, i = 1, 2, \ldots, d \), be integers satisfying

\[
m_d \mid n \quad \text{and} \quad m_i \mid m_{i+1}, \quad \text{for} \ 1 \leq i \leq d - 1.
\]

A **generalized GMW sequence** is then defined as the multiple trace function sequence of period \( N \) given by

\[
s_g(t) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\alpha^t) \right]^{\ast} \right] \cdots \right] \right] \right]^{\ast}
\]

where \( \alpha \) is an element of order \( N = 2^n - 1 \) and for \( 1 \leq i \leq d \)

\[
\text{gcd}(r_i, 2^{m_i} - 1) = 1, \quad 1 \leq r_i < 2^{m_i} - 1.
\]

We use the base-\( T \) expression of \( t \) to obtain a two-variable representation.

\[
t = t_1 \cdot T + t_2, \quad 0 \leq t_1 \leq 2^{m_d} - 2, \quad 0 \leq t_2 \leq T - 1
\]

where \( T = 2^n - 2 \). Using a two-variable representation of \( t \), the GMW sequences can be expressed in the two-dimensional representation (matrix form). That is, we can write the GMW sequence \( s_g(t) \) in the first row from \( t = 0 \) to \( T - 1 \), in the second row from \( t = T \) to \( 2T - 1 \), in the third row from \( t = 2T \) to \( 3T - 1 \), etc. This yields the expression

\[
s_g(t) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\alpha^{t_1}) \right]^{\ast} \right] \cdots \right] \right]^{\ast} \right]^{\ast}
\]

where \( \beta = \alpha^T \) and the subsequence of period \( 2^{m_d} - 1 \) obtained by fixing \( t_2 \) is given by

\[
s_{sub}(t_1) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\delta^{t_1}) \right]^{\ast} \right] \cdots \right] \right]^{\ast} \right]^{\ast}
\]

where \( \delta = \alpha^{T - t_2} \). Hence, the subsequence of period \( 2^{m_d} - 1 \) is given by

\[
s_{sub}(t_1) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\delta^{t_1}) \right]^{\ast} \right] \cdots \right] \right]^{\ast} \right]
\]

where \( \delta = \alpha^{T - t_2} \). Thus, in this case, the subsequence is a GMW sequence. The locations of the all-zero columns in the two-dimensional representation of the above generalized GMW sequence and the GMW sequence remain unchanged. The only difference is that the columns of \( m \)-sequences in the GMW sequence are now replaced by GMW sequences. As GMW sequences have the balance property, the above generalized GMW sequences in (8) also possess the balance property. Using the same proof as in the case of GMW sequences [8], we can prove that this generalized GMW sequence has the ideal full-period autocorrelation property. By mathematical induction, it is easy to prove that all generalized GMW sequences with \( d \) arbitrary have the balance property and ideal full-period autocorrelation values.

The generalized GMW sequence defined in (2) has the ideal full-period autocorrelation values [13], i.e.

\[
R_n(\tau) = \begin{cases} N, & \tau = 0 \mod N \\ -1, & \text{otherwise}. \end{cases}
\]

By extending the proof used in counting the number of cyclically distinct GMW sequences available (of period \( N \)), we can determine the number of cyclically distinct generalized GMW sequences of given period that can be generated.

**Theorem 1:** The number of cyclically different generalized GMW sequences of given period \( N \) is given by

\[
N_{GGMW} = \phi(2^n - 1) \cdot \prod_{i=1}^{d} \phi(2^{m_i} - 1)
\]

where \( \phi(\cdot) \) is Euler’s \( \phi \) function.

It is very difficult to find an exact closed-form expression for the linear span for a generalized GMW sequence. The author’s conjecture is that the linear span of a generalized GMW sequence is larger than that of the associated GMW sequence. Implementation, of course, is more complicated than in the case of GMW sequences.

III. GENERALIZATION OF NO SEQUENCES

The generalization of No sequences may be carried out exactly as in the case of GMW sequences. By replacing the subsequence, which are \( m \)-sequences, by generalized GMW sequences in the two-variable representation of No sequences, we obtain generalized families of No sequences [6]. Proofs for optimality of the correlation values of the generalized No sequence family can be easily given using the proof given in [6] for the No sequence family and the correlation property of subsequecnes, the columns of the generalized No sequences which in this case are generalized GMW sequences. The balance property of families of generalized No sequences is identical to that of the No sequence families because a generalized GMW sequence also has the balance property. The definition of a generalized No sequence family is given as follows.

**Definition 2:** Let \( n \) and \( m_i, i = 1, 2, \ldots, d \), be integers satisfying

\[
n = 2 \cdot m_d \quad \text{and} \quad m_i \mid m_{i+1}, \quad \text{for} \ 1 \leq i \leq d - 1.
\]

A family of **generalized No sequences**

\[
s_g = \{ s(t) \mid 0 \leq t \leq N - 1, \quad 1 \leq i \leq 2^n \}
\]

is a set of multiple trace function sequences defined as

\[
s_g(t) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\alpha^t) \right] \right] \cdots \right] \right]^{\ast} \right]^{\ast}
\]

where \( N = 2^n - 1, \gamma_{i} \) in \( GF(2^{m_d}) \), \( T = 2^{m_d} + 1 \), and for \( 1 \leq i \leq d 

\[
\text{gcd}(r_i, 2^{m_i} - 1) = 1, \quad 1 \leq r_i < 2^{m_i} - 1.
\]

The subsequence of period \( 2^{m_d} - 1 \) of the generalized No sequences in (14) are shown to be generalized GMW sequences using the two-variable representation of the generalized No sequences. Using the expansion

\[
t = t_1 \cdot T + t_2, \quad 0 \leq t_1 \leq 2^{m_d} - 2, \quad 0 \leq t_2 \leq T - 1,
\]

we obtain the two-variable representation

\[
s_g(t) = \text{tr}^{\alpha^{-1}} \left[ \text{tr}^{m_0} \left[ \text{tr}^{m_1} \left[ \cdots \left[ \text{tr}^{m_{d-1}} \left[ \text{tr}^{m_d} (\alpha^2) \right] + \gamma_{i} \cdot \alpha^{T - t_2} \right] \right] \cdots \right] \right]^{\ast}
\]
TABLE I
EXAMPLES OF NONTRIVIAL GENERALIZED NO SEQUENCES

<table>
<thead>
<tr>
<th>n</th>
<th>Period, N</th>
<th>Generalized No Sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4,095</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 63 )) = 1, 1 \leq r &lt; 63</td>
</tr>
<tr>
<td>16</td>
<td>65,535</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 335 )) = 1, 1 \leq r &lt; 335</td>
</tr>
<tr>
<td>18</td>
<td>202,143</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 511 )) = 1, 1 \leq r &lt; 511</td>
</tr>
<tr>
<td>20</td>
<td>1,048,575</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 31 )) = 1, 1 \leq r &lt; 31, gcd(( r, 1023 )) = 1, 1 \leq r &lt; 1023</td>
</tr>
<tr>
<td>24</td>
<td>16,777,215</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 4095 )) = 1, 1 \leq r &lt; 4095</td>
</tr>
<tr>
<td>28</td>
<td>268,435,455</td>
<td>( \text{tr}[{[\alpha^{3n}]^{2} + \gamma \cdot \alpha^{m-2}]}] )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 127 )) = 1, 1 \leq r &lt; 127</td>
</tr>
<tr>
<td></td>
<td></td>
<td>gcd(( r, 16383 )) = 1, 1 \leq r &lt; 16383</td>
</tr>
</tbody>
</table>

where \( \beta = \alpha^{T} \) is a primitive element of \( GF(2^{m}d) \) and the subsequence of period \( 2^{m}d - 1 \) is given by

\[
s_{\text{sub}}(t_1) = \text{tr}^{\alpha^2} \left[ \left\{ \left[ \left[ \sum_{i=1}^{m} \left( \delta^{i-1} \right) \left[ \alpha^{(i+1)d-1} \right] \right] \alpha^{(i+1)d-1} \right] \alpha^{(i+1)d-1} \right\} \right] \right. \tag{18}
\]

where \( \delta = \beta^{d} \) is a primitive element of \( GF(2^{m}d) \) and the phase function \( f_{1}(\alpha, \cdot) \) is defined via

\[
\beta f_{1}(\alpha, t_2) = \text{tr}^{\alpha^2} \left[ \left\{ \left[ \sum_{i=1}^{m} \left( \delta^{i-1} \right) \left[ \alpha^{(i+1)d-1} \right] \right] \alpha^{(i+1)d-1} \right\} \right. \tag{19}
\]

The phase function \( f_{1}(\alpha, t_2) \) of generalized No sequences is the same as that of No sequences and the subsequences have ideal autocorrelation values because generalized GMW sequences have the ideal full-period autocorrelation property. Therefore, the family of generalized No sequences has the optimal correlation property in terms of Welch’s lower bound [6], [12] and the proof for the correlation properties of No sequences [6], [8] works for the case of generalized No sequences as well. Further, the distribution of correlation values in a family of generalized No sequences is exactly the same as those in a family of No sequences and a family of Kasami sequences.

**Theorem 2.** The full-period correlation function \( \mathcal{R}(\tau) \) of the family of generalized No sequences defined in (14) takes on values in the set

\[
\{ -2^{m}d - 1, -1, 2^{m}d - 1 \} \tag{20}
\]

which means that the generalized No sequences have optimal correlation properties.

We already know that the counting problem for GMW sequences is the same as that of No sequences [6], [8]. Therefore, counts for the number of cyclically distinct generalized GMW sequences and generalized No sequence families are the same.

**Theorem 3:** The number of distinct families of generalized No sequences for a given period \( N \) is given as

\[
N_{\text{GWM}} = \frac{\phi(2^{n} - 1)}{n} \prod_{i=1}^{d} \frac{\phi(2^{m_{i}} - 1)}{m_{i}} \tag{21}
\]

where \( \phi(s) \) is Euler’s phi function.

The author’s conjecture is that the linear span of a generalized No sequence is larger than that of the associated No sequences and that it is possible to derive the lower and upper bounds on the linear span of the generalized No sequences. Linear spans for some cases of generalized No sequences are found by Klapper [14]. Implementation in the case of a generalized No sequence family needs to be investigated. All of nontrivial generalized No sequences are listed in Table I for period \( N \leq 2^{28} - 1 \).

**References:**


