Hence, by (1) we have
\[ m(x) = \frac{x^p - 1}{\gcd(x^p - 1, S^p(x))} = q(x). \]

Now we consider the case \( 2 \not\in Q \). The proof of Theorem 1 has shown that in this case
\[ S^p(\beta^j) \neq 0, \quad \text{for } 0 < j \leq p - 1. \]
Further, \( S^p(1) = 1 \) if \( p = 3 \mod 8 \) and \( S^p(1) = 0 \) if \( p = 5 \mod 8 \).

It follows that
\[ \gcd(x^p - 1, S^p(x)) = \begin{cases} 1, & \text{if } p = 3 \mod 8 \\ x - 1, & \text{if } p = 5 \mod 8. \end{cases} \]

Hence, by (1)
\[ m(x) = \frac{x^p - 1}{\gcd(x^p - 1, S^p(x))} = \begin{cases} x^p - 1, & \text{if } p = 3 \mod 8 \\ x^p - 1, & \text{if } p = 5 \mod 8. \end{cases} \]

Hence, we have completed the proof of Theorem 2.

ACKNOWLEDGMENT

The authors wish to thank the referees for their comments and suggestions that improved the correspondence, and for pointing out [6].

REFERENCES


Binary Pseudorandom Sequences of Period \( 2^n - 1 \) with Ideal Autocorrelation Generated by the Polynomial \( z^d + (z + 1)^d \)

Jong-Seon No, Habong Chung, and Min-Seon Yun

Abstract—In this correspondence, we present a construction for binary pseudorandom sequences of period \( 2^n - 1 \) with ideal autocorrelation property using the polynomial \( z^d + (z + 1)^d \). We show that the sequence obtained from the polynomial becomes an \( m \)-sequence for certain values of \( d \). We also find a few values of \( d \) which yield new binary sequences with ideal autocorrelation property when \( m = 3k \pm 1 \), where \( k \) is a positive integer. These new sequences are represented using trace function and the results are tabulated.

Index Terms—Binary sequences, ideal autocorrelation, polynomial, pseudorandom sequences.

I. INTRODUCTION

A binary (0 or 1) sequence \( \{a(t), \ t = 0, 1, \cdots, N-1\} \) of period \( N = 2^n - 1 \) is said to have the ideal autocorrelation property if its periodic autocorrelation function \( R_a(\tau) \) is given by
\[ R_a(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \mod N \\ -1, & \text{for } \tau \not\equiv 0 \mod N \end{cases} \]
where \( R_a(\tau) \) is defined as
\[ R_a(\tau) = \sum_{t=0}^{N-1} (-1)^{a(t)} \] (2)
and \( t + \tau \) is computed modulo \( N \).

Some of the well-known binary sequences of period \( 2^n - 1 \) include \( m \)-sequences, GMW sequences, generalized GMW sequences, “Legendre” sequences, Hall’s sextic residue sequences, extended sequences, and miscellaneous sequences of which the construction methods are not known yet. These sequences are best described in terms of the trace function over a finite field. Let \( GF(2^n) \) be the finite field with \( 2^n \) elements. Let \( m = cn + 1 \) for some positive integers \( c \) and \( n \). Then the trace function \( \text{tr}_{2^n}^m(\cdot) \) is a mapping from \( GF(2^n) \) to its subfield \( GF(2^m) \) given by [2]
\[ \text{tr}_{2^n}^m(x) = \sum_{i=0}^{m-1} x^{2^{ni}}. \]

In this correspondence, we present a construction for binary pseudorandom sequences of period \( 2^n - 1 \) with ideal autocorrelation property using the polynomial \( z^d + (z + 1)^d \). These sequences are found by a computer search. In Section II, we show that \( m \)-sequences can be obtained by this method for certain values of \( d \). In Section III, we also find a few values of \( d \) which yield new binary sequences with ideal autocorrelation property when \( m = 3k \pm 1 \), where \( k \) is a positive integer. These new sequences are represented using trace function and the results are tabulated.

Manuscript received September 24, 1997; revised November 29, 1997. This work was supported by the Institute of Information Technology Assessment under Grants 96003-RT-11 and 96190-CT-12 from the Korean Ministry of Information and Communications.

J.-S. No and M.-S. Yun are with the Department of Electronic Engineering, Konkuk University, Seoul 143-701, Korea.

H. Chung is with the School of Electronic and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea.

Publisher Item Identifier S 0018-9448(98)02365-7.
II. CONSTRUCTION OF $m$-SEQUENCES
USING THE POLYNOMIAL $z^d + (z + 1)^d$

Let $I_d$ be a set defined on GF$(2^m)$ as
\[ I_d = \{ u | u = z^d + (z + 1)^d, \ z \in \text{GF}(2^m) \}. \tag{4} \]
Let the sequence $a_d(t), \ t = 0, 1, 2, \ldots, 2^m - 2$, associated with the set $I_d$ be defined as

i) for an odd $m$:
\[ a_d(t) = \begin{cases} 1, & \text{if } \alpha^t \in I_d \\ 0, & \text{otherwise} \end{cases} \tag{5} \]

ii) for an even $m$:
\[ a_d(t) = \begin{cases} 0, & \text{if } \alpha^t \in I_d \\ 1, & \text{otherwise} \end{cases} \tag{6} \]

where $\alpha$ is a primitive element in GF$(2^m)$. The sequence $a_d(t)$ is invariant under the decimation by $2^m$, i.e., $a_d(t) = a_d(2^m t)$, since $u(z^d + (z + 1)^d) \in I_d$ implies that $u(\alpha^d(z^d + (z + 1)^d)) \in I_d$. Also, we can easily see that $a_d(t) = a_2a_d(t)$, since $I_d = I_2I_d$. The following theorems tell us that the sequence $a_d(t)$ is an $m$-sequence under certain conditions on $d$ and $m$.

Theorem 1: Let $m$ be a positive odd integer. If $d$ has the form $d = 2^i + 1$, and $i$ is relatively prime to $m$, then the sequence $a_d(t)$ in (5) is an $m$-sequence given by $a_d(t) = \text{tr}_m^i(\alpha^t)$.

Proof: To verify that $a_d(t) = \text{tr}_m^i(\alpha^t)$, it is enough to show that $I_d$ is the set of all the elements of GF$(2^m)$ whose trace values are 1. Any element $u$ in $I_d$ can be expressed as
\[ u = z^d + (z + 1)^d = z^{2^i} + z + 1. \tag{7} \]

Thus, $\text{tr}_m^i(u) = 1$.

Also, if $z = z_1$ and $z_2$ are solutions of (7) for given $u$, then $z_1 + z_2$ is a solution of $z^{2^i} + z = 0$. Since gcd$(m, i) = 1$, the only two possible values for $z_1 + z_2$ are either 0 or 1, which implies (7) has exactly two solutions for any given $u$ such that $\text{tr}_m^i(u) = 1$. Therefore, $|I_d| = 2^m - 1$, i.e., $I_d$ is the set of all the elements of GF$(2^m)$ whose trace values are 1. \Box

Theorem 2: Let $m$ be a positive even integer. If $d$ has the form $d = 2^i + 1$, and $i$ is relatively prime to $m$, then the sequence $a_d(t)$ in (6) is an $m$-sequence given by $a_d(t) = \text{tr}_m^i(\alpha^t)$.

Proof: To verify that $a_d(t) = \text{tr}_m^i(\alpha^t)$, it is enough to show that $I_d$ is the set of all the elements but zero of GF$(2^m)$ whose trace values are 0, which can be easily proven using the similar argument in the proof of Theorem 1. \Box

The following theorem tells us an interesting relation between $a_d(t)$ and $a_d(d-t)$.

Theorem 3: Let $d$ be a positive integer and $s$ be its inverse element in $\mathbb{Z}_{2^m-1}$, i.e.,
\[ d \cdot s \equiv 1 \pmod{2^m - 1}. \tag{8} \]
Then
\[ a_d(t) = a_d(-dt). \tag{9} \]

Proof: Let $(I_d)^r$ be defined as
\[ (I_d)^r = \{ u' | u \in I_d \}. \tag{10} \]
Then the sequence associated with the set $(I_d)^r$ similarly as in (5) or (6) is the decimation by $r^{-1}$ of the sequence $a_d(t)$. Any element $u(z^d + (z + 1)^d)$ in $I_d$ can be expressed by substituting $z$ with $1/(x + 1)$ as
\[ u = \left( \frac{1}{1+x} \right)^d + \left( \frac{x}{1+x} \right)^d = \frac{1 + x^d}{(1 + x)^d}. \tag{11} \]
Thus $I_d$ can be rewritten as
\[ I_d = \left\{ u | u = \frac{1 + x^d}{(1 + x)^d}, \ x \in \text{GF}(2^m)/\{1\} \right\}. \tag{12} \]
Note that excluding $x = 1$ does not affect $I_d$, since $z = 0$ and $z = 1$ yield the same $u$. By raising to the power $-s$ of (11), we have
\[ u^{-s} = \frac{1 + y^s}{(1 + y)^s}. \tag{13} \]
and by replacing $y$ by $x^d$, we have
\[ u^{-s} = \frac{1 + y^s}{(1 + y)^s}. \tag{14} \]
Thus the set $I_s$ can be rewritten as
\[ I_s = \left\{ u | u = \frac{1 + y^s}{(1 + y)^s}, \ y \in \text{GF}(2^m)/\{1\} \right\} = \{ u | u^{-s} \in I_d \} = (I_d)^{-s}. \tag{15} \]
Therefore, $a_s(t) = a_d(-t/s) = a_d(-dt)$. \Box

All the $m$-sequences of period $2^m-1$ obtained from the polynomial $z^d + (z + 1)^d$ for the case of an odd $m$ can be explained by Theorems 1 and 3. When $m$ is even, any $m$-sequences generated from the polynomial for $d$ with Hamming weight 2 in its binary representation can be also explained by Theorem 2, but the $m$-sequence obtained from the polynomial with $d = 2^m-1 - 1$ is explained in the following theorem.

Theorem 4: Let $m$ be a positive even integer and $d = 2^m-1 - 1$. Then the sequence $a_d(t)$ in (6) is an $m$-sequence given by $a_d(t) = \text{tr}_m^i(\alpha^d)$.

Proof: To verify that $a_d(t) = \text{tr}_m^i(\alpha^d)$, it is enough to show that $(I_d)^d$ is the set of all the elements but zero of GF$(2^m)$ whose trace values are 0. Any element $w$ in $(I_d)^d$ can be written as
\[ w = u^d = (z^d + (z + 1)^d)^d. \tag{16} \]
For $z = 0$ or 1, $w$ becomes 1 and $\text{tr}_m^i(1) = 0$. From the fact that $(I_d)^d = (I_d^2)^{2d} = (I_{2d})^{-1}$, (16) can be rewritten as
\[ w = (z^{-1} + (z + 1)^{-1})^{-1} = \left( \frac{1}{z(z + 1)} \right)^{-1} = z^2 + z \tag{17} \]
for values of $z$ other than 0 or 1. Thus $\text{tr}_m^i(w) = 0$. Since (17) has exactly two solutions of $z$ for any given $w$ such that $\text{tr}_m^i(w) = 0$, $|I_d|^d = 2^m-1 - 1$. Therefore, $(I_d)^d$ is the set of all the elements but zero of GF$(2^m)$ whose trace values are zero. \Box

III. NEW BINARY PSEUDORANDOM SEQUENCES
OBTAINED BY THE POLYNOMIAL $z^d + (z + 1)^d$

We found by a computer search, a few values of $d$ which yield new binary sequences with ideal autocorrelation property when $m$ is $3k \pm 1$, where $k$ is a positive integer. These results are summarized as the following conjecture.
<table>
<thead>
<tr>
<th>$N$</th>
<th>$d$</th>
<th>sequences</th>
<th>$N$</th>
<th>$d$</th>
<th>sequences</th>
<th>$N$</th>
<th>$d$</th>
<th>sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^4 + 1$</td>
<td>3</td>
<td>m-1</td>
<td>$2^{14} + 1$</td>
<td>3,9,33</td>
<td>m-1</td>
<td>$2^{21} + 1$</td>
<td>3,5,9,17,33,65,</td>
<td>m-1</td>
</tr>
<tr>
<td>= 15</td>
<td>7</td>
<td>m-7</td>
<td>= 16383</td>
<td>993</td>
<td>MIS-1</td>
<td>=2097151</td>
<td>129,257,513,1025</td>
<td></td>
</tr>
<tr>
<td>$2^5 - 1$</td>
<td>3,5</td>
<td>m-1</td>
<td>$2^{15} - 1$</td>
<td>3,5,17,129</td>
<td>m-1</td>
<td></td>
<td>2047(1025)</td>
<td>m-1047551</td>
</tr>
<tr>
<td>= 31</td>
<td>7(5)</td>
<td>m-11</td>
<td>=32767</td>
<td>255(129)</td>
<td>m-16255</td>
<td></td>
<td>16257(129)</td>
<td>m-1040383</td>
</tr>
<tr>
<td></td>
<td>11(3)</td>
<td>m-7</td>
<td></td>
<td>6355(13)</td>
<td>m-1015807</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^6 - 1$</td>
<td>3</td>
<td>m-1</td>
<td></td>
<td>1935(17)</td>
<td>m-15359</td>
<td></td>
<td>204007(257)</td>
<td>m-1044479</td>
</tr>
<tr>
<td>= 63</td>
<td>31</td>
<td>m-31</td>
<td></td>
<td>6555(5)</td>
<td>m-12287</td>
<td></td>
<td>224841(513)</td>
<td>m-1046527</td>
</tr>
<tr>
<td>$2^7 - 1$</td>
<td>3,5,9</td>
<td>m-1</td>
<td></td>
<td>10923(3)</td>
<td>m-8191</td>
<td></td>
<td>225849(65)</td>
<td>m-1032191</td>
</tr>
<tr>
<td>= 127</td>
<td>11</td>
<td>MIS-23</td>
<td>$2^{16} - 1$</td>
<td>3,9,33,129</td>
<td>m-1</td>
<td></td>
<td>233017(9)</td>
<td>m-917503</td>
</tr>
<tr>
<td></td>
<td>13(11)</td>
<td>MIS-1</td>
<td>=65535</td>
<td>993</td>
<td>MIS-1</td>
<td></td>
<td>370093(17)</td>
<td>m-983039</td>
</tr>
<tr>
<td></td>
<td>15(9)</td>
<td>m-55</td>
<td></td>
<td>32767</td>
<td>m-32767</td>
<td></td>
<td>419431(5)</td>
<td>m-786431</td>
</tr>
<tr>
<td></td>
<td>27(5)</td>
<td>m-47</td>
<td>$2^{17} - 1$</td>
<td>3,5,9,17,33,65,</td>
<td>m-1</td>
<td></td>
<td>699051(3)</td>
<td>m-524287</td>
</tr>
<tr>
<td></td>
<td>43(3)</td>
<td>m-31</td>
<td>=131071</td>
<td>129,257</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^8 - 1$</td>
<td>3,9</td>
<td>m-1</td>
<td>$2^{18} - 1$</td>
<td>3,3,129</td>
<td>m-1</td>
<td>$2^{22} - 1$</td>
<td>3,5,9,17,33,65,</td>
<td>m-1</td>
</tr>
<tr>
<td>= 255</td>
<td>57</td>
<td>MIS-1</td>
<td>=683</td>
<td>MIS-2015</td>
<td></td>
<td>=4194303</td>
<td>16257</td>
<td>MIS-1</td>
</tr>
<tr>
<td></td>
<td>127</td>
<td>MIS-1</td>
<td></td>
<td>4033(683)</td>
<td>MIS-1</td>
<td></td>
<td>2097151</td>
<td>m-2097151</td>
</tr>
<tr>
<td></td>
<td>65117</td>
<td>m-127</td>
<td></td>
<td>511(257)</td>
<td>m-65279</td>
<td></td>
<td>223(17)</td>
<td>m-32639</td>
</tr>
<tr>
<td>$2^9 - 1$</td>
<td>3,5,17</td>
<td>m-1</td>
<td></td>
<td>7711(17)</td>
<td>m-61439</td>
<td></td>
<td>129,257,513,</td>
<td></td>
</tr>
<tr>
<td>= 511</td>
<td>31(17)</td>
<td>m-239</td>
<td></td>
<td>14567(9)</td>
<td>m-57343</td>
<td></td>
<td>1025,2049</td>
<td></td>
</tr>
<tr>
<td></td>
<td>103(5)</td>
<td>m-191</td>
<td></td>
<td>19309(129)</td>
<td>m-65023</td>
<td></td>
<td>10923</td>
<td>MIS-32639</td>
</tr>
<tr>
<td></td>
<td>171(3)</td>
<td>m-127</td>
<td></td>
<td>19867(33)</td>
<td>m-63487</td>
<td></td>
<td>65281(10923)</td>
<td>MIS-1</td>
</tr>
<tr>
<td>$2^{10} - 1$</td>
<td>3,9</td>
<td>m-1</td>
<td></td>
<td>22197(65)</td>
<td>m-64511</td>
<td></td>
<td>4095(2049)</td>
<td>m-4192255</td>
</tr>
<tr>
<td>= 1023</td>
<td>57</td>
<td>MIS-1</td>
<td></td>
<td>26215(5)</td>
<td>m-49151</td>
<td></td>
<td>129087(65)</td>
<td>m-4128767</td>
</tr>
<tr>
<td></td>
<td>511</td>
<td>m-511</td>
<td></td>
<td>43691(3)</td>
<td>m-32767</td>
<td></td>
<td>493455(17)</td>
<td>m-3932159</td>
</tr>
<tr>
<td>$2^{11} - 1$</td>
<td>3,5,9,17,33</td>
<td>m-1</td>
<td></td>
<td>3,3,129</td>
<td>m-1</td>
<td></td>
<td>845427(129)</td>
<td>m-4161535</td>
</tr>
<tr>
<td>= 2047</td>
<td>43</td>
<td>MIS-119</td>
<td>$2^{18} - 1$</td>
<td>3,3,129</td>
<td>m-1</td>
<td></td>
<td>932071(9)</td>
<td>m-3670015</td>
</tr>
<tr>
<td></td>
<td>241(43)</td>
<td>MIS-1</td>
<td>=262143</td>
<td>131071</td>
<td>m-131071</td>
<td></td>
<td>1203053(1025)</td>
<td>m-4190207</td>
</tr>
<tr>
<td></td>
<td>63(33)</td>
<td>m-991</td>
<td></td>
<td>526287</td>
<td>m-526287</td>
<td></td>
<td>1271003(33)</td>
<td>m-4063231</td>
</tr>
<tr>
<td></td>
<td>231(9)</td>
<td>m-895</td>
<td></td>
<td>2731</td>
<td>MIS-8063</td>
<td></td>
<td>1357220(513)</td>
<td>m-4186111</td>
</tr>
<tr>
<td></td>
<td>365(17)</td>
<td>m-959</td>
<td></td>
<td>4033(2731)</td>
<td>MIS-1</td>
<td></td>
<td>1387221(257)</td>
<td>m-4177919</td>
</tr>
<tr>
<td></td>
<td>411(5)</td>
<td>m-767</td>
<td></td>
<td>1023(513)</td>
<td>m-261631</td>
<td></td>
<td>1677723(5)</td>
<td>m-3145277</td>
</tr>
<tr>
<td></td>
<td>683(3)</td>
<td>m-511</td>
<td></td>
<td>15963(33)</td>
<td>m-253951</td>
<td></td>
<td>2796203(3)</td>
<td>m-2097151</td>
</tr>
<tr>
<td>$2^{12} - 1$</td>
<td>3,33</td>
<td>m-1</td>
<td></td>
<td>52851(129)</td>
<td>m-260095</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>= 4095</td>
<td>2047</td>
<td>m-2047</td>
<td></td>
<td>58255(9)</td>
<td>m-229375</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$2^{13} - 1$</td>
<td>3,5,9,17,33,65</td>
<td>m-1</td>
<td></td>
<td>75483(257)</td>
<td>m-261119</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>= 8191</td>
<td>171</td>
<td>MIS-479</td>
<td></td>
<td>88757(65)</td>
<td>m-258047</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>241(171)</td>
<td>MIS-1</td>
<td></td>
<td>92525(17)</td>
<td>m-245759</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>127(65)</td>
<td>m-4031</td>
<td></td>
<td>104859(5)</td>
<td>m-196607</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>91(9)</td>
<td>m-3583</td>
<td></td>
<td>174763(3)</td>
<td>m-131071</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1243(33)</td>
<td>m-3967</td>
<td>$2^{20} - 1$</td>
<td>3,9,129,513</td>
<td>m-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1453(17)</td>
<td>m-3839</td>
<td>=1048575</td>
<td>16257</td>
<td>MIS-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1639(5)</td>
<td>m-3071</td>
<td></td>
<td>524287</td>
<td>m-524287</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2731(3)</td>
<td>m-2047</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TABLE I**

PN Sequences Generated by the Polynomial $z^d + (z + 1)^d$
Conjecture 5: Let \( k \) be a positive integer and \( m = 3k - 1 \) or \( 3k + 1 \). If \( d \) has the form given by

\[
d = 2^{4k} - 2^{k} + 1
\]

then the sequence \( a_d(t) \) given in (5) or (6) is a binary pseudorandom sequence of period \( 2^m - 1 \) with ideal autocorrelation property.

When \( m = 2, 4 \), or 5, the period \( N \) of sequences is 3, 15, or 31, respectively, and the resulting sequences are the same as \( m \)-sequences. When \( m \geq 7 \), the new sequences \( a_d(t) \) are expressed by using trace representation as

\[
a_d(t) = \sum_{\alpha \in J} \text{tr}_k^{i7}\end{array}(\alpha^t)\]

where for each \( m \), the set \( J \) is given by computer search as

\[
m = 7, k = 2, d = 13:
J = \{1, 3, 7, 19, 29\}
\]

\[
m = 8, k = 3, d = 57:
J = \{13, 19, 21, 29, 39\}
\]

\[
m = 10, k = 3, d = 57:
J = \{1, 3, 5, 7, 11, 13, 15, 35, 69, 71, 89, 105, 121\}
\]

\[
m = 11, k = 4, d = 241:
J = \{25, 35, 41, 57, 69, 71, 73, 89, 105, 121, 139, 141, 143\}
\]

\[
m = 13, k = 4, d = 241:
\]

\[
m = 14, k = 5, d = 993:
\]

\[
m = 16, k = 5, d = 993:
\]

\[
m = 17, k = 6, d = 4033:
\]

\[
m = 19, k = 6, d = 4033:
\]
m = 23, k = 8, d = 5281:

\[ J = \{385, 515, 641, 897, 1029, 1063, 1153, 1409, 1665, 1921, 2057, 2099, 2031, 2169, 2345, 2433, 2689, 2941, 3201, 3457, 3713, 3969, 4113, 4115, 4117, 4121, 4123, 4125, 4127, 4225, 4481, 4737, 4993, 5249, 5505, 5761, 6017, 6273, 6529, 6785, 7041, 7297, 7533, 7809, 8065, 8225, 8227, 8229, 8231, 8233, 8235, 8237, 8239, 8241, 8243, 8245, 8247, 8249, 8251, 8253, 8255, 8257, 8258, 8333, 9089, 9345, 9601, 9857, 10113, 10369, 10625, 10881, 11137, 11393, 11649, 11905, 12161, 12417, 12673, 12929, 13185, 13441, 13697, 13953, 14209, 14465, 14721, 14977, 15233, 15489, 15745, 16001, 16257, 16499, 16451, 16453, 16455, 16457, 16459, 16461, 16463, 16465, 16467, 16469, 16471, 16473, 16475, 16477, 16479, 16481, 16483, 16485, 16487, 16489, 16491, 16493, 16495, 16497, 16499, 16501, 16503, 16505, 16507, 16509, 16511, 16513, 16519, 17025, 17281, 17537, 17793, 18049, 18305, 18561, 18817, 19073, 19329, 19585, 19841, 20097, 20353, 20609, 20865, 21121, 21377, 21633, 21889, 22145, 22401, 22657, 22913, 23169, 23425, 23681, 23937, 24193, 24449, 24705, 24961, 25217, 25473, 25729, 25985, 26241, 26497, 26753, 27009, 27265, 27521, 27777, 28033, 28289, 28545, 28801, 29057, 29313, 29569, 29825, 30081, 30337, 30593, 30849, 31105, 31361, 31617, 31873, 32129, 32385, 32641, 32899, 32901, 32903, 32905, 32907, 32909, 32911, 32913, 32915, 32917, 32919, 32921, 32923, 32925, 32927, 32929, 32931, 32933, 32935, 32937, 32939, 32941, 32943, 32945, 32947, 32949, 32951, 32953, 32955, 32957, 32959, 32961, 32963, 32965, 32967, 32969, 32971, 32973, 32975, 32977, 32979, 32981, 32983, 32985, 32987, 32989, 32991, 32993, 32995, 32997, 32999, 33001, 33003, 33005, 33007, 33009, 33011, 33013, 33015, 33017, 33019, 33021, 33023\}.

Conjecture 5 is verified up to \( m \leq 23 \) by a computer simulation. The sequences constructed by Conjecture 5 seem to be the same as the sequences recently conjectured in [14], but their construction methods are totally different from ours. It may be an interesting research topic to consider other polynomials than \( z^d + (z + 1)^d \) in our construction. For example, replacing the polynomial \( z^d + (z + 1)^d \) by \( z^d + (z + 1)^d + 1 \) in our construction corresponds to Welch–Gong transformation [14], substituting \( x \) by \( x + 1 \) in trace representation of an ideally correlated binary sequences. Theorem 3 can be applied to the sequences in Conjecture 5 for the case of an odd \( m \).

The binary sequences with ideal autocorrelation property generated from the polynomial \( z^d + (z + 1)^d \) are listed in Table I. These sequences are classified into \( m \)-sequences and newly found sequences according to the value of \( d \). In Table I, the number in the parenthesis indicates the inverse element in \( Z_2^{m-1} \) of the value in front of it. Also, \( m \) stands for \( m \)-sequences and MIS stands for the miscellaneous sequences constructed by the previous two conjectures. The notation \( m \)-S or MIS-i represents the sequence obtained by decimating the corresponding sequence by \( i \).

REFERENCES