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 $2 \notin Q$. The proof of Theorem 1 has shown that in this case

$$S^p(\beta^j) \neq 0, \qquad \text{for } 0 < j \leq p-1.$$

Further, $S^p(1) = 1$ if $p = 3 \bmod 8$ and $S^p(1) = 0$ if $p = 5 \bmod 8$. It follows that

$$\gcd(x^p - 1,\ S^p(x)) = \begin{cases} 1, & \text{if } p = 3 \bmod 8 \\ x - 1, & \text{if } p = 5 \bmod 8. \end{cases}$$

Hence, by (1)

$$m(x) = \frac{x^p - 1}{\gcd(x^p - 1, S^p(x))} = \begin{cases} x^p - 1, & \text{if } p = 3 \bmod 8 \\ \dfrac{x^p - 1}{x - 1}, & \text{if } p = 5 \bmod 8. \end{cases}$$

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

[1] A. J. Bromfield and F. C. Piper, "Linear recursion properties of unrelated binary sequences," *Discr. Appl. Math.*, vol. 27, pp. 187–193, 1990.
[2] I. Damgaard, "On the randomness of Legendre and Jacobi sequences," in *Advances in Cryptology: Crypto'88*, S. Goldwasser, Ed. Berlin, Germany: Springer-Verlag, 1990, LNCS 403, pp. 163–172.
[3] C. Ding, "The differential cryptanalysis and design of the natural stream ciphers," in *Fast Software Encryption*, B. Preneel, Ed. Berlin, Germany: Springer-Verlag, 1994, LNCS 809, pp. 101–115.
[4] T. Helleseth, "Legendre sums and codes related to QR codes," *Discr. Appl. Math.*, vol. 35, pp. 107–113, 1992.
[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. Berlin, Germay: Springer-Verlag, 1982.
[6] D. Jungnickel, *Finite Fields, Structure and Arithmetics*. Mannheim, Germany: Bibliographishes Institut & F.A. Brockhaus AG, 1993.
[7] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20. Reading, MA: Addison-Wesley, 1983.

Binary Pseudorandom Sequences of Period $2^m - 1$ 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 $2^m - 1$ 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 is $3k \pm 1$, 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 $N = 2^m - 1$ is said to have the *ideal autocorrelation property* if its periodic autocorrelation function $R_a(\tau)$ is given by

$$R_a(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \bmod N \\ -1, & \text{for } \tau \not\equiv 0 \bmod N \end{cases} \tag{1}$$

where $R_a(\tau)$ is defined as

$$R_a(\tau) = \sum_{t=0}^{N-1} (-1)^{a(t+\tau)+a(t)} \tag{2}$$

and $t + \tau$ is computed modulo N.

Some of the well-known binary sequences of period $2^m - 1$ 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 $\mathrm{GF}(2^m)$ be the finite field with 2^m elements. Let $m = en > 1$ for some positive integers e and n. Then the trace function $\mathrm{tr}_n^m(\cdot)$ is a mapping from $\mathrm{GF}(2^m)$ to its subfield $\mathrm{GF}(2^n)$ given by [2]

$$\mathrm{tr}_n^m(x) = \sum_{i=0}^{e-1} x^{2^{ni}}. \tag{3}$$

In this correspondence, we present a construction for binary pseudorandom sequences of period $2^m - 1$ 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 is $3k \pm 1$, 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-I1 and 96190-CT-I2 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

$$I_d = \{u | u = z^d + (z+1)^d,\ z \in \mathrm{GF}(2^m)\}. \tag{4}$$

Let the sequence $a_d(t)$, $t = 0, 1, 2, \cdots, 2^m - 2$, 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 α is a primitive element in GF(2^m). The sequence $a_d(t)$ is invariant under "the decimation by 2," i.e., $a_d(t) = a_d(2^i t)$, since $u(= z^d + (z+1)^d) \in I_d$ implies that $u^{2^i}(= (z^{2^i})^d + (z^{2^i}+1)^d) \in I_d$. Also, we can easily see that $a_d(t) = a_{2^i d}(t)$, since $I_d = I_{2^i d}$. 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 $a_d(t) = \mathrm{tr}_1^m(\alpha^t)$.

Proof: To verify that $a_d(t) = \mathrm{tr}_1^m(\alpha^t)$, 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, $\mathrm{tr}_1^m(u) = 1$.

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 $\mathrm{tr}_1^m(u) = 1$. 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. □

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 $a_d(t) = \mathrm{tr}_1^m(\alpha^t)$.

Proof: To verify that $a_d(t) = \mathrm{tr}_1^m(\alpha^t)$, 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. □

The following theorem tells us an interesting relation between $a_d(t)$ and $a_{d^{-1}}(t)$.

Theorem 3: Let d be a positive integer and s be its inverse element in Z_{2^m-1}, i.e.,

$$d \cdot s \equiv 1 (\mathrm{mod}\, 2^m - 1). \tag{8}$$

Then

$$a_s(t) = a_d(-dt). \tag{9}$$

Proof: Let $(I_d)^r$ be defined as

$$(I_d)^r = \{u^r | u \in I_d\}. \tag{10}$$

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

$$I_d = \left\{u | u = \frac{1+x^d}{(1+x)^d},\ x \in \mathrm{GF}(2^m)/\{1\}\right\}. \tag{12}$$

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

$$u^{-s} = \frac{(1+x)^{ds}}{(1+x^d)^s} = \frac{1+x}{(1+x^d)^s} \tag{13}$$

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

$$\begin{aligned} I_s &= \left\{u | u = \frac{1+y^s}{(1+y)^s},\ y \in \mathrm{GF}(2^m)/\{1\}\right\} \\ &= \left\{u | u^{-s} \in I_d\right\} = (I_d)^{-s}. \end{aligned} \tag{15}$$

Therefore, $a_s(t) = a_d(-(t/s)) = a_d(-dt)$. □

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 $a_d(t) = \mathrm{tr}_1^m(\alpha^{dt})$.

Proof: To verify that $a_d(t) = \mathrm{tr}_1^m(\alpha^{dt})$, 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 $\mathrm{tr}_1^m(1) = 0$. From the fact that $(I_d)^d = (I_{2d})^{2d} = (I_{-1})^{-1}$, (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 $\mathrm{tr}_1^m(w) = 0$. Since (17) has exactly two solutions of z for any given w such that $\mathrm{tr}_1^m(w) = 0$, $|(I_d)^d| = 2^{m-1} - 1$. Therefore, $(I_d)^d$ is the set of all the elements but zero of GF(2^m) whose trace values are zero. □

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 I
PN SEQUENCES GENERATED BY THE POLYNOMIAL $z^d + (z+1)^d$

N	d	sequences	N	d	sequences	N	d	sequences
2^4-1	3	m-1	$2^{14}-1$	3,9,33	m-1	$2^{21}-1$	3,5,9,17,33,65,	m-1
$=15$	7	m-7	$=16383$	993	MIS-1	$=2097151$	129,257,513,1025	
2^5-1	3,5	m-1		8191	m-8191		2047(1025)	m-1047551
$=31$	7(5)	m-11	$2^{15}-1$	3,5,17,129	m-1		16257(129)	m-1040383
	11(3)	m-7	$=32767$	255(129)	m-16255		63551(33)	m-1015807
2^6-1	3	m-1		1935(17)	m-15359		204007(257)	m-1044479
$=63$	31	m-31		6555(5)	m-12287		224841(513)	m-1046527
2^7-1	3,5,9	m-1		10923(3)	m-8191		225849(65)	m-1032191
$=127$	11	MIS-23	$2^{16}-1$	3,9,33,129	m-1		233017(9)	m-917503
	13(11)	MIS-1	$=65535$	993	MIS-1		370093(17)	m-983039
	15(9)	m-55		32767	m-32767		419431(5)	m-786431
	27(5)	m-47	$2^{17}-1$	3,5,9,17,33,65,	m-1		699051(3)	m-524287
	43(3)	m-31	$=131071$	129,257		$2^{22}-1$	3,9,33,129,513	m-1
2^8-1	3,9	m-1		683	MIS-2015	$=4194303$	16257	MIS-1
$=255$	57	MIS-1		4033(683)	MIS-1		2097151	m-2097151
	127	m-127		511(257)	m-65279	$2^{23}-1$	3,5,9,17,33,65,	m-1
2^9-1	3,5,17	m-1		7711(17)	m-61439	$=8388607$	129,257,513,	
$=511$	31(17)	m-239		14567(9)	m-57343		1025,2049	
	103(5)	m-191		19309(129)	m-65023		10923	MIS-32639
	171(3)	m-127		19867(33)	m-63487		65281(10923)	MIS-1
$2^{10}-1$	3,9	m-1		22197(65)	m-64511		4095(2049)	m-4192255
$=1023$	57	MIS-1		26215(5)	m-49151		129087(65)	m-4128767
	511	m-511		43691(3)	m-32767		493455(17)	m-3932159
$2^{11}-1$	3,5,9,17,33	m-1	$2^{18}-1$	3,33,129	m-1		845427(129)	m-4161535
$=2047$	43	MIS-119	$=262143$	131071	m-131071		932071(9)	m-3670015
	241(43)	MIS-1	$2^{19}-1$	3,5,9,17,33,65,	m-1		1203053(1025)	m-4190207
	63(33)	m-991	$=524287$	129,257,513			1271003(33)	m-4063231
	231(9)	m-895		2731	MIS-8063		1357229(513)	m-4186111
	365(17)	m-959		4033(2731)	MIS-1		1387221(257)	m-4177919
	411(5)	m-767		1023(513)	m-261631		1677723(5)	m-3145727
	683(3)	m-511		15903(33)	m-253951		2796203(3)	m-2097151
$2^{12}-1$	3,33	m-1		52851(129)	m-260095			
$=4095$	2047	m-2047		58255(9)	m-229375			
$2^{13}-1$	3,5,9,17,33,65	m-1		75483(257)	m-261119			
$=8191$	171	MIS-479		88757(65)	m-258047			
	241(171)	MIS-1		92525(17)	m-245759			
	127(65)	m-4031		104859(5)	m-196607			
	911(9)	m-3583		174763(3)	m-131071			
	1243(33)	m-3967	$2^{20}-1$	3,9,129,513	m-1			
	1453(17)	m-3839	$=1048575$	16257	MIS-1			
	1639(5)	m-3071		524287	m-524287			
	2731(3)	m-2047						

Conjecture 5: Let k be a positive integer and $m = 3k - 1$ or $3k + 1$. If d has the form given by

$$d = 2^{2k} - 2^k + 1 \tag{18}$$

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

$$a_d(t) = \sum_{i \in J} \mathrm{tr}_1^m(\alpha^{it}) \tag{19}$$

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

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

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

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

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

$m = 13$, $k = 4$, $d = 241$:
$J = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 67, 133, 135, 265, 267, 269, 271, 305, 337, 369, 401, 433, 465, 479\}$

$m = 14$, $k = 5$, $d = 993$:
$J = \{49, 67, 81, 113, 133, 135, 145, 177, 209, 241, 265, 267, 269, 271, 273, 305, 337, 369, 401, 433, 465, 497, 531, 533, 535, 537, 539, 541, 543\}$

$m = 16$, $k = 5$, $d = 993$:
$J = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 131, 261, 263, 521, 523, 525, 527, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1121, 1185, 1249, 1313, 1377, 1441, 1505, 1569, 1633, 1697, 1761, 1825, 1889, 1953, 2017\}$

$m = 17$, $k = 6$, $d = 4033$:
$J = \{97, 131, 161, 225, 261, 263, 289, 353, 417, 481, 521, 523, 525, 527, 545, 609, 673, 737, 801, 865, 929, 993, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1057, 1121, 1185, 1249, 1313, 1377, 1441, 1505, 1569, 1633, 1697, 1761, 1825, 1889, 1953, 2017, 2083, 2085, 2087, 2089, 2091, 2093, 2095, 2097, 2099, 2101, 2103, 2105, 2107, 2109, 2111\}$

$m = 19$, $k = 6$, $d = 4033$:
$J = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 259, 517, 519, 1033, 1035, 1037, 1039, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 4129, 4131, 4133, 4135, 4137, 4139, 4141, 4143, 4145, 4147, 4149, 4151, 4153, 4155, 4157, 4159, 4289, 4417, 4545, 4673, 4801, 4929, 5057, 5185, 5313, 5441, 5569, 5697, 5825, 5953, 6081, 6209, 6337, 6465, 6593, 6721, 6849, 6977, 7105, 7233, 7361, 7489, 7617, 7745, 7873, 8001, 8129\}$

$m = 20$, $k = 7$, $d = 16257$:
$J = \{193, 259, 321, 449, 517, 519, 577, 705, 833, 961, 1033, 1035, 1037, 1039, 1089, 1217, 1345, 1473, 1601, 1729, 1857, 1985, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 2113, 2241, 2369, 2497, 2625, 2753, 2881, 3009, 3137, 3265, 3393, 3521, 3649, 3777, 3905, 4033, 4129, 4131, 4133, 4135, 4137, 4139, 4141, 4143, 4145, 4147, 4149, 4151, 4153, 4155, 4157, 4159, 4161, 4289, 4417, 4545, 4673, 4801, 4929, 5057, 5185, 5313, 5441, 5569, 5697, 5825, 5953, 6081, 6209, 6337, 6465, 6593, 6721, 6849, 6977, 7105, 7233, 7361, 7489, 7617, 7745, 7873, 8001, 8129, 8259, 8261, 8263, 8265, 8267, 8269, 8271, 8273, 8275, 8277, 8279, 8281, 8283, 8285, 8287, 8289, 8291, 8293, 8295, 8297, 8299, 8301, 8303, 8305, 8307, 8309, 8311, 8313, 8315, 8317, 8319\}$

$m = 22$, $k = 7$, $d = 16257$:
$J = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255, 515, 1029, 1031, 2057, 2059, 2061, 2063, 4113, 4115, 4117, 4119, 4121, 4123, 4125, 4127, 8225, 8227, 8229, 8231, 8233, 8235, 8237, 8239, 8241, 8243, 8245, 8247, 8249, 8251, 8253,$

8255, 16449, 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, 16769, 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}

$m = 23$, $k = 8$, $d = 65281$:

$J = \{385, 515, 641, 897, 1029, 1031, 1153, 1409,$
1665, 1921, 2057, 2059, 2061, 2063, 2177,
2433, 2689, 2945, 3201, 3457, 3713, 3969,
4113, 4115, 4117, 4119, 4121, 4123, 4125,
4127, 4225, 4481, 4737, 4993, 5249, 5505,
5761, 6017, 6273, 6529, 6785, 7041, 7297,
7553, 7809, 8065, 8225, 8227, 8229, 8231,
8233, 8235, 8237, 8239, 8241, 8243, 8245,
8247, 8249, 8251, 8253, 8255, 8321, 8577,
8833, 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, 16449,
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, 16769, 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], subtituting 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-i or MIS-i represents the sequence obtained by decimating the corresponding sequence by i.

REFERENCES

[1] L. D. Baumert, "Cyclic difference sets," in *Lecture Notes in Mathematics.* Berlin, Germany: Springer-Verlag, 1971.

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

[3] L. D. Baumert and Fredrickson, "The cyclotomic numbers of order 18 with applications to difference sets," *Math. Comp.*, vol. 21, pp. 204–219, 1967.

[4] U. Cheng, "Exhaustive construction of (255, 127, 63) cyclic difference sets," *J. Comb. Theory*, vol. A-35, pp. 115–125, 1983.

[5] R. Drier, "(511, 255, 127) cyclic difference sets," in *IDA Talk*, July 1992.

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

[7] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, Mar. 1989.

[8] J.-S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. Southern California, Los Angeles, CA, May 1988.

[9] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548–553, May 1984.

[10] J.-S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 260–262, Jan. 1996.

[11] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2254–2255, Nov. 1996.

[12] J.-S. No, K. Yang, C. Chung, and H.-Y. Song, "Extension of binary sequences with ideal autocorrelation property," Mar. 1996, preprint.

[13] ——, "A new family of binary sequences with optimal correlation properties," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1596–1602, Sept. 1997.

[14] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, "Binary sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.