On the Classification of Binary Sequences of Period $2^n - 1$ with Ideal Autocorrelation[1]

Jong-Seon No*, Hwan-Keun Lee*, Habong Chung†, Kyeongcheol Yang‡, and Hong-Yeop Song‡

*Dept. of Electronic Eng., Konkuk Univ., Seoul 143-701, Korea; jsno@eng.konkuk.ac.kr
†School of Electronics and Electrical Eng., Hongik Univ., Seoul 121-791, Korea; habchung@wow.hongik.ac.kr
‡Dept. of Electronic Communication Eng., Hanyang Univ., Seoul 133-791, Korea; kcyang@coding.hanyang.ac.kr
‡Dept. of Electronic Eng., Yonsei Univ., Seoul 120-749, Korea; hysong@bubble.yonsei.ac.kr

Abstract — **In this paper, the number of inequivalent binary sequences with ideal autocorrelation in each category is listed, including some newly found sequences.**

I. Introduction

Let $\{a(t), t = 0, 1, \ldots, N-1\}$ and $\{b(t), t = 0, 1, \ldots, N-1\}$ be two binary (0 or 1) sequences of period $N = 2^n - 1$. Two sequences $\{a(t)\}$ and $\{b(t)\}$ are said to be *inequivalent* if there are no integers r and τ such that $b(t) = a(r[t + \tau])$ for all t, where the arithmetics are modulo N. The sequence $\{a(t)\}$ is said to have the *ideal autocorrelation property* if its periodic autocorrelation takes only the value N or -1.

In the literature, known binary sequences of period $2^n - 1$ with ideal autocorrelation can be categorized into m-sequences, GMW sequences [7], generalized GMW sequences [4], Legendre sequences [5], Hall's sextic residue sequences [6], extended sequences [6], or miscellaneous sequences [6] whose general constructions are not known so far.

II. Main Results

Several new miscellaneous sequences with ideal autocorrelation are found in a closed-form expression using trace function up to period $2^{23} - 1$. The number of inequivalent binary sequences in each category is listed in Table I, including newly found miscellaneous sequences. For convenience, we use the following short notations in Table I:

m: m-sequences
G: GMW sequences
L: Legendre sequences
H: Hall's sextic residue sequences
GG: generalized GMW sequences
E: extended sequences
M: miscellaneous sequences

In Table I, the numbers up to $n = 9$ come from previous works done by an exhaustive computer search [1]-[3]. The Hall's sextic residue sequence of period 31 is just an m-sequence. Since m-sequences are a special case of GMW sequences and are already counted in their own category, they are excluded in counting the number of inequivalent GMW sequences. In the same reason, m-sequences and GMW sequences are also excluded in counting the number of inequivalent generalized GMW sequences. Newly found sequences with ideal autocorrelation property are also counted in Table I. For example, a closed form of the newly found sequence $\{a(t)\}$ of length $2^{20} - 1$ in the table is given by

$$a(t) = \mathrm{tr}_1^{20}\left(\alpha^t + \alpha^{127t} + \alpha^{3969t} + \alpha^{12287t} + \alpha^{16383t}\right)$$

where α is primitive in GF(2^{20}) and $\mathrm{tr}_1^{20}(\cdot)$ is the trace from GF(2^{20}) to GF(2).

TABLE I. Number of Inequivalent Binary Sequences of Period $2^n - 1$ with Ideal Autocorrelation.

n	m	G	L	H	GG	E	M	Total
3	1	0	0	0	0	0	0	1
4	1	0	0	0	0	0	0	1
5	1	0	1	0	0	0	0	2
6	1	1	0	0	0	0	0	2
7	1	0	1	1	0	0	3	6
8	1	1	0	0	0	0	2	4
9	1	1	0	0	0	0	2	4
10	1	5	0	0	0	2	≥ 1	≥ 9
11	1	0	0	0	0	0	≥ 2	≥ 3
12	1	7	0	0	5	0	≥ 0	≥ 13
13	1	0	1	0	0	0	≥ 1	≥ 3
14	1	17	0	0	0	62	≥ 1	≥ 81
15	1	6	0	0	0	2	≥ 1	≥ 10
16	1	16	0	0	15	32	≥ 1	≥ 65
17	1	0	1	1	0	0	≥ 2	≥ 5
18	1	53	0	0	52	96	≥ 0	≥ 202
19	1	0	1	0	0	0	≥ 2	≥ 4
20	1	65	0	0	295	≥ 180	≥ 1	≥ 542
21	1	18	0	0	0	62	≥ 1	≥ 82
22	1	175	0	0	0	≥ 352	≥ 0	≥ 528
23	1	0	0	0	0	0	≥ 2	≥ 3

[1]This work was supported by the Korean Ministry of Information and Communications.

References

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

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

[3] R. Drier, "(511, 255, 127) cyclic difference sets," IDA talk, July 1992.

[4] J. -S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory.* vol. 35, pp. 260-262, Jan. 1996.

[5] 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.

[6] J. -S. No, K. Yang, H. Chung, and H. -Y. Song, "On the construction of binary sequences with ideal autocorrelation property," *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications* (ISITA '96), pp. 837-840, Victoria, B.C., Canada, Sept. 17-20, 1996.

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