Optimal Peak Sidelobe Level Sequences up to Length 74

Anatolii N. Leukhin
Informatics and Computing Faculty,
Volga State University of Technology
Yoshkar-Ola, Russia
leuhinan@volgatech.net

Egor N. Potekhin
Informatics and Computing Faculty,
Volga State University of Technology
Yoshkar-Ola, Russia
potehinen@gmail.com

***Abstract*— Results of an exhaustive search for minimum peak sidelobe (MPS) level sequences are presented. Several techniques for efficiency implementation of search algorithm are described. A table of number of non-equivalent optimal binary sequences with minimum peak sidelobe level up to length 74 is given. Such sequence families are important in low probability of intercept radar. Examples of optimal binary MPS sequences having high merit factor are shown.**

***Keywords*— exhaustive search; minimum peak sidelobe; aperiodic autocorrelation function; binary sequences; merit factor**

I. Introduction

Binary sequences with low autocorrelation sidelobe levels are useful in different applications radar, communication systems, information security, synchronization and channel estimation. The main point in pulse compression radar is to gain the signal-to-noise ratio benefits of a long pulse. This requires longer and longer sequences, with low aperiodic autocorrelation sidelobes. There are no theoretical methods to generate binary sequences with smallest level of aperiodic function, so such sequences have been produced by computer searches. Binary sequences are preferred. There are some global and local algorithms for computer search of binary sequences with minimum or low peak sidelobe level (PSL). The computational complexity of efficient known global algorithm is approximately $O\left(1.85^N\right)$ and computational complexity of efficient known local algorithm is approximately $O\left(1.4^N\right)$.

Lindner [1] in 1975 did an exhaustive search for binary MPS sequences up to $N=40$. Cohen et al. [2] in 1990 continued up to $N=48$. Coxson and Ruso [3] performed an exhaustive search of binary MPS sequences for $N=64$. All of these authors introduced a table with numbers of MPS sequences. Elders-Boll et al. [4] in 1997 found binary MPS sequences for the lengths up to 61 but they did not present the numbers of such sequences just only gave sample codes with lowest peak sidelobe for each lengths from $N=[49;61]$.

The number of sequences is important in low probability of intercept radar (LPIR). The greater the number the more difficult it is for an eavesdropper to determine which sequence is being used. Some MPS sequences can be generated from others using reversal, negation and sign alternation. Such sequences are called equivalent. In this paper we are concerned with the number of non-equivalent sequences. Finding all non-equivalent sequences requires an exhaustive search.

Apart from known results of global exhaustive search of binary MPS sequences, there are some useful results of local search of binary sequences with the low aperiodic autocorrelation. Kerdock et al. [5] in 1986 found binary sequences for lengths $N=51,69,88$ with $PSL=3,4,5$ respectively. Coxson and Ruso [3] in 2004 continued the list of best known binary PSL sequences with $PSL=4$ up to $N=70$. Nunn and Coxson [6] in 2008 found best known binary PSL sequences with $PSL=4$ up to $N=82$ and with $PSL=5$ for $N=[83,105]$.

So binary MPS sequences are only known for the lengths up to $N=61$ and for the length $N=64$ and numbers of such sequences are only known for the lengths up to $N=48$ and for the length $N=64$.

This paper adds to available knowledge for record length of binary MPS sequence and provides numbers of non-equivalent sequences for all lengths from $N=[49,63]$ and from $N=[65,74]$. We have made an exhaustive search of binary MPS sequences during 8 months implementation 1 supercomputer Flagman RX240T8.2 on the base of 8 NVIDIA TESLA C2059 with 3584 parallel graphical processors and on the base of 2 processors Intel Xeon X5670 (up to Six-Core) and using CUDA compilation. Our global algorithm is based on a concept of Mertens [7], the branch-and-bound algorithm, with slightly modification ("package" regime and parallelization) and using new assembler instructions for calculation of aperiodic autocorrelation.

II. Preliminaries

First, A binary sequence of length N is an N-tuple $A=\left(a_0,a_1,\ldots,a_{N-1}\right)$ where each $a_n\in\{-1,1\}$, $n=0,1,\ldots,N-1$. The aperiodic autocorrelation of A at shift τ defined as

$$C_\tau = \sum_{n=0}^{N-1-\tau} a_n \cdot a_{n+\tau} \quad (1)$$

There are two principal measures of level of sidelobe level. The primary measure is the peak sidelobe level (PSL):

$$PSL(C) = \max_{1 \le \tau \le N-1} |C_\tau| \quad (2)$$

For optimal binary sequences by PSL criteria the peak sidelobe has to be minimum:

$$MPS = \min_A PSL \quad (3)$$

A secondary measure, is the merit factor (MF):

$$MF(C) = \frac{N^2}{2\sum_{\tau=1}^{N-1} [C_\tau]^2} \quad (4)$$

PSL affects the maximum of self interference of the sequence and merit factor determines average interference. There are three transformations that preserve peak sidelobe level in binary codes: reversal: $R(a_n) = a_{N-1-n}$, negation: $N(a_n) = -a_n$, alternating sign $S(a_n) = (-1)^n a_n$. Such sequences form an equivalence class.

III. Modified Implemetation of Effective Global Algorithm for Exhaustive Search of Binary Minimum Peak Sidelobe Level Sequences

We are interested to find all non-equivalent classes of binary MPS sequences for each length N up to $N = 74$. We modified all achievements of Nunn and Coxson algorithm which based on the main idea of Mertens's branch-and-bound algorithm as described below:

1. Our main idea is to use new assembler instructions for computing autocorrelation function of binary sequences. We can find side lobes of aperiodic autocorrelation using XOR operation. To determine the level of sidelobe we have to calculate the numbers of zeros and units for each shift of sequences. New Intel processors have microarchitecture Intel Core of version SSE4.2 which operating with the set of command on low level. For example C/C++ Microsoft compiler has function __popcnt64 of intrin library and also compilers GCC and G++ has function _mm_popcnt_u64 of smmintrin library for calculation the number of units in binary sequences by 1 cycle.

2. We used recursive implementation of our algorithm using inline options for all external operations.

3. For excluding equivalent sequences we used reverse transformation for two bytes at the time instead of each bit. All possible reverses are stored in static massive with 65536 different bit variations.

4. We realized parallel computing in multiprocessor system for all set of non-equivalent sequences separately each from other. We implemented our algorithm on CUDA SDK using function __popcll() for calculating number of unit bits.

5. We used "package" regime to find some binary PSL sequences with the lengths $N, N+2, N+4, \ldots,$ because cross correlation functions for left and right parts of the sequences with lengths $N, N+2, N+4, \ldots,$ are the same, so they are computing just only once for minimum length N.

For example the time of exhaustive standard branch-and-bound algorithm even for one length $N = 72$ on a computing system with 1 TFlops is $T = \frac{1.85^{72}}{10^{12} \cdot 60 \cdot 60 \cdot 24} \approx 199$ days. Here we assume that check of aperiodic autocorrelation function of each sequence is implemented during 1 sample that is impossible today for Intel processors. We realized an exhaustive search of binary MPS sequences with length $N = 72$ using our modification ("package regime") and parallel implementation on graphical processors less than 20 days. To compare with longest length $N = 64$ for which exhaustive search was executed in 2004 it will need approximately more than $1.85^{10} \approx 470$ times of CPU for our longest length $N = 74$.

We calculate the number of estimations of aperiodic autocorrelation function and plot it in logarithmic scale by vertical axis. The runtime complexity of full search is

$$O((N-1) \cdot 2^N) \quad (5)$$

where 2^N is a number of binary codes with length N, $(N-1)$ - number of sidelobes of aperiodic autocorrelation.

So we will approximate experimental results using approximation function of the kind:

$$O(c \cdot b^N) \quad (6)$$

A runtime complexity of exhaustive search for binary minimum peak sidelobe sequences depends on level of PSL, so we find runtime complexity for $PSL = 2,3,4,5$. Our results of runtime complexity are shown in Table I.

TABLE I. Runtime Complexity Of Modified BB Algorithm For Exhaustive Search Of Binary MPS Sequences

PSL	Runtime complexity
2	$O(20.7 \cdot 1.42^N)$
3	$O(18.3 \cdot 1.57^N)$
4	$O(9.9 \cdot 1.7^N)$
5	$O(6.9 \cdot 1.79^N)$

IV. Results of Exhaustive Search of Binary MPS Sequences

Our results are presented in Table II. PSLi sequences have exactly $PSL = i$, not less. Synthesized sequences are available on our website [8].

The results of an exhaustive search of binary MPS sequences up to length $N = 74$ are presented in Table III. Also in the Table 2 there are the highest level of MF between binary MPS sequences and examples of such sequences in hexadecimal format.

TABLE II. Size of Set Non-Equivalent PSL sequences

Length N	Size of set non-equivalent PSL sequences				
	PSL1	*PSL2*	*PSL3*	*PSL4*	*PSL5*
2	1	0	0	0	0
3	1	1	0	0	0
4	1	1	1	0	0
5	1	3	1	1	0
6	0	4	4	1	1
7	1	7	5	5	1
8	0	8	12	8	6
9	0	10	23	20	29
10	0	5	46	35	30
11	1	7	53	97	52
12	0	16	87	133	152
13	1	11	126	287	246
14	0	9	152	486	583
15	0	13	223	800	1050
16	0	10	361	1173	2176
17	0	4	307	2243	3490
18	0	2	339	3025	7205
19	0	1	419	4661	11645
20	0	3	625	6245	21456
21	0	3	505	9826	32539
22	0	0	378	11840	58331
23	0	0	515	16533	86812
24	0	0	858	20673	148583
25	0	1	436	29794	206762
26	0	0	242	31205	329356
27	0	0	388	40193	469454
28	0	2	624	49884	753204
29	0	0	284	63059	966451
30	0	0	86	59506	1390617
31	0	0	251	71546	calc
32	0	0	422	89190	2894816
33	0	0	139	98644	calc
34	0	0	51	84636	4567602
35	0	0	111	98331	calc
36	0	0	161	118624	8951507
37	0	0	55	119053	calc
38	0	0	17	89067	11788025
39	0	0	30	101808	calc
40	0	0	57	118731	22333659
41	0	0	15	112039	calc
42	0	0	4	72716	24453952
43	0	0	12	83417	calc
44	0	0	15	98334	44270683
45	0	0	4	82538	calc
46	0	0	1	47331	41354620
47	0	0	1	54896	calc
48	0	0	4	64424	74010972
49	0	0	0	49088	calc
50	0	0	0	25169	57294359
51	0	0	1	28249	calc
52	0	0	0	33058	calc
53	0	0	0	23673	calc
54	0	0	0	10808	calc
55	0	0	0	11987	calc
56	0	0	0	15289	calc
57	0	0	0	9476	calc
58	0	0	0	4026	calc
59	0	0	0	4624	calc
60	0	0	0	5542	calc
61	0	0	0	3246	calc
62	0	0	0	1212	calc
63	0	0	0	1422	calc
64	0	0	0	1859	calc
65	0	0	0	1003	calc
66	0	0	0	324	calc
67	0	0	0	414	calc
68	0	0	0	489	calc
69	0	0	0	248	calc
70	0	0	0	72	calc
71	0	0	0	115	calc
72	0	0	0	107	calc
73	0	0	0	44	calc
74	0	0	0	18	calc

TABLE III. Size of Set Non-Equivalent PSL sequences

Length	*PSL*	*MF*	*Optimal by MF?*	*Sequence*	*Size of set*
2	1	2	yes	0	1
3	1	4.5	yes	1	1
4	1	4	yes	2	1
5	1	6.25	yes	02	1
6	2	2.571	yes	02	4
7	1	8.167	yes	0D	1
8	2	4	yes	1A	8
9	2	3.375	yes	02C	10
10	2	3.846	yes	02C	5
11	1	12.1	yes	0ED	1
12	2	7.2	yes	0A6	16
13	1	14.083	yes	00CA	1
14	2	5.158	yes	00CA	9
15	2	4.891	no	0329	13
16	2	4.571	no	1DDA	10
17	2	4.516	yes	0192B	4
18	2	6.48	yes	0168C	2
19	2	4.878	no	0EEDA	1
20	2	5.263	no	04D4E	3

Length	*PSL*	*MF*	*Optimal by MF?*	*Sequence*	*Size of set*
21	2	6.485	no	005D39	3
22	3	6.205	yes	013538	378
23	3	5.628	yes	084BA3	515
24	3	8	yes	31FAB6	858
25	2	7.102	no	031FAB6	1
26	3	7.511	no	07015B2	242
27	3	9.851	yes	0F1112D	388
28	2	7.84	yes	4B7770E	2
29	3	6.782	yes	04B7770E	284
30	3	7.627	yes	03F6D5CE	86
31	3	7.172	yes	07E736D5	251
32	3	7.111	no	01E5AACC	422
33	3	8.508	yes	003CB5599	139
34	3	8.892	yes	0CC01E5AA	51
35	3	7.562	no	00796AB33	111
36	3	6.894	no	3314A083E	161
37	3	6.985	no	031D5AD93F	55
38	3	8.299	yes	003C34AA66	17
39	3	6.391	no	13350BEF3C	30
40	3	7.407	yes	2223DC3A5A	57
41	3	7.504	no	038EA520364	15
42	3	8.733	yes	04447B874B4	4
43	3	6.748	no	005B2ACCE1C	12
44	3	6.286	no	202E2714B96	15
45	3	6.575	no	02AF0CC6DBF6	4
46	3	6.491	no	03C0CF7B6556	1
47	3	7.126	no	069A7E851988	1
48	3	6.128	no	24AC8847B87C	4
49	4	8.827	yes	05E859E984451	49088
50	4	8.17	yes	038FE23225492	25169
51	3	7.517	no	0E3F88C89524B	1
52	4	8.145	yes	05FB6D5D9D8E3	33058
53	4	7.89	no	00FF66EAE96B1C	23673
54	4	7.327	no	043B48A28793B3	10808
55	4	7.451	no	1658A2BC0A133B	11987
56	4	8.167	yes	0C790164F6752A	15289
57	4	7.963	no	01B4DE3455B93BF	9476
58	4	8.538	yes	008D89574E1349E	4026
59	4	8.328	no	1CAD63EFF126A2E	4624
60	4	8.108	no	119D01522ED3C34	5542
61	4	7.563	no	0024BA568EB83731	3246
62	4	8.179	yes	000C67247C59568B	1212
63	4	9.587	yes	1B3412F0501539CE	1422
64	4	9.846	yes	26C9FD5F5A1D798C	1859
65	4	8.252	no	04015762C784EC369	1003
66	4	7.751	no	03FEF2CCB0B8CAC54	324
67	4	7.766	no	073C2FADC44255264	414
68	4	8.438	no	562B8CA48E0C9027E	489
69	4	7.988	no	0292582AC6A767CC03	248
70	4	7.313	no	01C2FFD4AF33356596	72
71	4	8.105	no	12493BE76A5EE2A3F1	115
72	4	7.2	no	27C8D6E165A71577FE	107
73	4	8.327	no	012DE781C9167577AB7	44
74	4	7.039	no	00ABFA66C560E3094C2	18

V. CONCLUSION

This paper presents the size of optimal binary MPS sequences set are firstly shown for lengths 49 to 63 and 65 to 74. Also the number of non-equivalent PSL1, PSL2, PSL3, SPL4 and PSL5 sequences are found for lengths 2 to 74. Improvements of global branch-and-bound algorithm for exhaustive search are due to programming techniques. These include the use of new assembler instructions for new Intel processors with microarchitecture Intel Core of version SSE4.2 and parallel implementation on graphical processors and new algorithm insights dealing with “package” regime. A runtime complexity of our global algorithm of exhaustive search for binary minimum peak sidelobe sequences depends on level of PSL and is the same as some of known local algorithms.

The number of MPS and PSL sequences are useful for prediction of longest sequences possible for a given PSL. Such optimal sequences are highly sought after in radar. These sequences were considered from MF criteria and the MPS sequences with highest MF were identified. The number of PSL is sequences rapidly increased for increasing PSL. For example for the length 48 the number of nonequivalent binary sequences with PSL3 is 4, PSL4 is 64424, PSL5 is 74010972. This makes it possible for a radar designer to trade off SNR for LPIR.

ACKNOWLEDGMENT

This work is supported by the grants: grant RFBR №12-07-00552, grant RFBR № 13-07-12414, project №1.07.2012.

REFERENCES

[1] J. Lindner, “Binary sequences up to length 40 with best possible autocorrelation function,” Electronics Letters, vol. 11, no. 21 pp. 507, April 1975.

[2] M.N. Cohen, M.R. Fox, J.M. Baden, “Minimum peak sidelobes pulse compression codes,” Proceedings of the IEEE International Radar Conference, Arlington, VA, pp.633-638, May 1990.

[3] G.E. Coxson, J. Russo, “Efficient exhaustive search for optimal-peak-sidelobe binary codes,” IEEE Trans. Aerospace and Electron. Systems, vol. 41, pp. 302–308, 2005.

[4] H. Elders-Boll, H. Schotten, and A. Busboom, “A comparative study of optimization methods for the synthesis of binary sequences with good correlation properties,” in 5th IEEE Symposium on Communication and Vehicular Technology in the Benelux, IEEE, p. 24–31, 1997.

[5] A.M.Kerdock, R. Mayer, D. Bass, “Longest binary pulse compression codes with given peak sidelobe levels,” Proceedings of the IEEE, vol. 74, no.2, p.366, February 1986.

[6] C.J.Nunn, G.E. Coxson, “Best-known autocorrelation peak sidelobe levels for binary codes of length 71 to 105,” IEEE Transactions on Aerospace and Electronics Systems, vol. 44, no.1, p.392-395, January 2008.

[7] S. Mertens, “On the ground state of the Bernasconi model,” Journal of Physics A: Mathematical and General, vol. 41, p. 3731-3749, 1998.

[8] http://signalslab.marstu.net.

[9] A.N. Leukhin, E.N. Potekhin, “Binary Sequences with Minimum Peak Sidelobe Level up to Length 68,” unpublished.