Existence of Modular Sonar Sequences of Twin-Prime Product Length

Sung-Jun Yoon and Hong-Yeop Song

School of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea
{sj.yoon,hysong}@yonsei.ac.kr

Abstract. In this paper, we investigate the existence of modular sonar sequences of length v and mod v where v is a product of twin primes. For $v = 3 \cdot 5 = 15$, we have found some old and new examples by exhaustive search. However, the very next case $v = 5 \cdot 7 = 35$ is completely open, in that neither we know (have) an example, nor we prove the nonexistence. We describe simply some approach to locate a single example of modular sonar sequences of length 35 and mod 35, assuming (or hoping) that one exists.

Dedicated to Solomon W. Golomb on his 75^{th} birthday

1 Introduction

A family of pseudorandom sequences with low cross correlation, good randomness, and large linear span has important application to code-division multiple-access (CDMA) communications and cryptology. [4] [7] [15]

It has long been conjectured that if a balanced binary sequence of period v has the ideal two-level autocorrelation, then v must be either $2^n - 1$ for some positive integer n, a prime p of type $4k+3$, or a product of twin-prime. [1] [6] [7] [8] [13] [16] It is interesting to note that those three types of integers seem to have no common property except for the above. For the lengths v other than those listed above, no such binary sequences of period v are currently known, neither the proof of non-existence of such examples are completed. [8] [13] [16] On the other hand, for each of these types of lengths, at least one easy construction for such sequences are well-known. [1] [6] [7] [8] [12] [13] [16]

In [10] and [11], Gong introduced a new design for families of binary sequences with low cross correlation, balance property, and large linear span. The key idea of this new design is to use short binary periodic sequences with two-level autocorrelation function and an interleaved structure to construct a set of long binary sequences with the desired properties. This property also has significant meaning with the application on signal detection of high-speed broad-band communication system. [10] [11]

Gong's construction [11] gives a $(v^2, v, 2v+3)$ signal set consisting of v binary sequences of period v^2 whose out-of-phase autocorrelation and cross-correlation maximum is bounded by $2v+3$. The construction requires two binary sequences

S.W. Golomb et al. (Eds.): SSC 2007, LNCS 4893, pp. 184–191, 2007.

of period v with the ideal two-level autocorrelation, and a so-called shift sequence of $\mathbf{e} = (e_0, e_1, \cdots, e_{v-1})$ of length v defined over $\{0, 1, ..., v-1\}$. She proved that the construction works in general if there exists two sequences with the ideal autocorrelation together with a shift sequence $\mathbf{e}$ with a desired property, and specifically gave constructions for $\mathbf{e}$ in the following two cases: (1) when $v = p^n - 1$ for a prime p and a positive integer n, and (2) when $v = p$ which is a prime of type $4k + 3$. [11]

As long as binary sequences are concerned, the above construction uses two well-known types of balanced binary sequences of period v with the ideal two-level autocorrelation : (1) $v = 2^n - 1$ and (2) $v = p$ is a prime of type $4k + 3$. These two cases cover all types of two-level binary autocorrelation sequences as building blocks except for a class of two-level autocorrelation sequences of period v where v is a product $p(p + 2)$ of twin primes.

We first recognized that "shift sequence" $\mathbf{e}$ in [11] is the same as modular sonar sequence of length v mod v [14]. In fact, it is essentially the same as the one given by Games in [3] for the case $v = 2^n - 1$ or $p^n - 1$, or the exponential-Welch construction in [5] [14] for the case $v = p$ of type $4k + 3$. This is in fact given in her earlier paper published in 1995. [10]

A sonar sequence $a_1, a_2, ..., a_n$ of length n over the integers $\{0, 1, ..., m-1\}$ is defined by the property that

$$a_i - a_{i+r} = a_j - a_{j+r} \quad \Longrightarrow \quad i = j, \tag{1}$$

for any i, j and r in the appropriate range. [9] When this sequence is represented as an $m \times n$ matrix (or pattern, or array) of dots and blanks, there is exactly one dot per column corresponding to the integer a_i in i-th column, and this pattern possesses the non-periodic two-dimensional ideal autocorrelation function, where the value of autocorrelation at shift (t, τ) is the number of dots matched when it is shifted horizontally by t and vertically by τ with respect to itself. [9] This property was used in the design of active sonar signals. [2] Here, a_i represents the carrier frequency at time slot i. So, m is the number of frequencies to be used in the system. In general, one would hope the sonar sequence be as long as possible given the number m of frequencies is fixed. In this sense, *known best* sonar sequences (or $m \times n$ arrays) up to $m = 100$ are listed in [14]. They started from a modular sonar sequence $\{a_i\}$ (mod m) and transform this into $\{b_i\}$ where

$$b_i = ua_i + si + c \pmod{m} \quad 0 \le i < n, \tag{2}$$

where u is relatively prime to m, and s, c are any integers, and see if one can find a long run of empty rows to be deleted so that the resulting sonar array is *best* optimized. [14] Here, a modular sonar sequence is the same as a sonar sequence except that the condition (1) is replaced by

$$a_i - a_{i+r} = a_j - a_{j+r} \pmod{m} \quad \Longrightarrow \quad i = j. \tag{3}$$

It is called an $m \times n$ modular sonar array, or a modular sonar sequence of length n and mod m.

To investigate the missing case, that is, the case $v = p(p+2)$, we have to find modular sonar sequences of length v mod v. Unfortunately, however, we were not able to show the non-existence, nor we could find one single example, except for the one special case $v = 15$. Note that the case $v = 15$ is very special in that it is the only case which is both a product of twin-prime and of the form $2^n - 1$. For the case $v = 15$, using any of these examples, the construction gives easily the families of $(v^2, v, 2v + 3)$ signal sets by way of the interleaved construction as in [11], since the existence of balanced binary sequence of period $v = p(p+2)$ with the ideal two-level autocorrelation is well-known [1] [7].

In the following, we will briefly describe some results for the case $v = 15$ in Section 2, and some ad-hoc tries to find an example for $v = 35$ in Section 3, all of which turned out to be not successful. Following are some open questions in this direction:

Q1: Does there exist a modular sonar sequence of length 35 and mod 35? No example is currently known and no proof of nonexistence is known either.
Q2: Find any example of modular sonar sequence of length v and mod v where $v = p(p + 2) > 15$ is a product of twin primes.

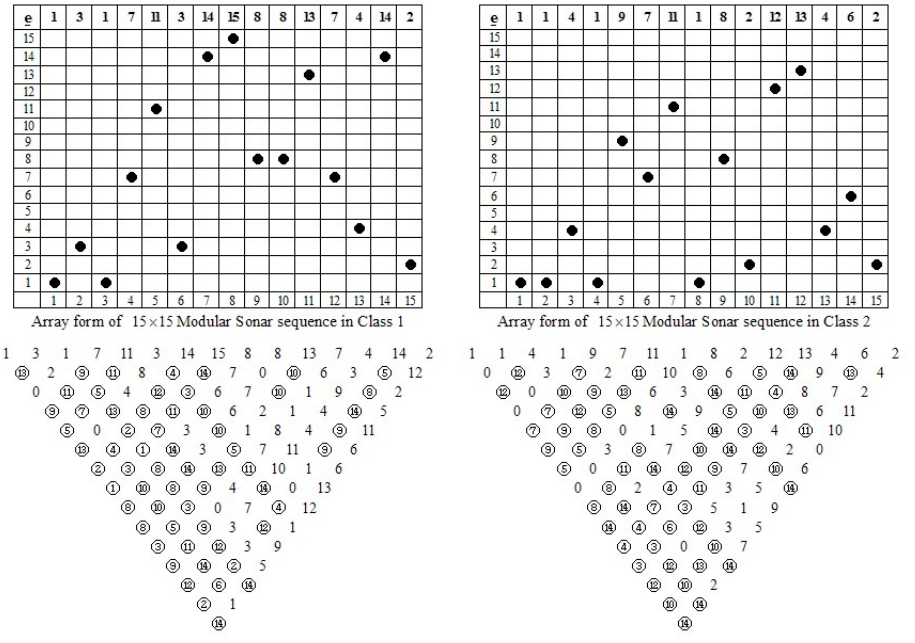
2 Case $v = 3 \times 5 = 15$

By an exhaustive search, we found all the 9000 modular sonar sequences of length 15 and mod 15. In the sense of the transformations given in (2) originally given in [14], these are classified into 5 inequivalent classes, each containing 1800 sequences. For any two sequences $\{a_i\}$ and $\{b_i\}$ in the same class, there exist some u, s, c such that $b_i = ua_i + si + c \pmod{15}$ for $0 \le i < n$. There are 8 choices for u, and 15 choices for both s and c, and this counts $1800 = 8$ members of each class. Representatives of these 5 inequivalent classes are

$$\textbf{Class 1} : \mathbf{e}_1 = (1, 3, 1, 7, 11, 3, 14, 15, 8, 8, 13, 7, 4, 14, 2)$$
$$\textbf{Class 2} : \mathbf{e}_2 = (1, 1, 4, 1, 9, 7, 11, 1, 8, 2, 12, 13, 4, 6, 2)$$
$$\textbf{Class 3} : \mathbf{e}_3 = (1, 1, 2, 14, 2, 13, 4, 9, 13, 12, 4, 2, 11, 6, 8)$$
$$\textbf{Class 4} : \mathbf{e}_4 = (1, 1, 4, 9, 4, 11, 10, 8, 5, 9, 10, 1, 9, 5, 7)$$
$$\textbf{Class 5} : \mathbf{e}_5 = (1, 6, 12, 13, 10, 14, 7, 9, 7, 14, 10, 13, 12, 6, 1)$$

If we expand the concept of equivalence so that one is regarded to be equivalent to its mirror image (reverse reading), then Class 3 is equivalent to Class 1, and Class 4 is equivalent to Class 2. Thus, we have only 3 super-inequivalent classes: Classes 1, 2, and 5.

Figures 1 and 2 show both array forms and modular difference triangles of these three representative sequences. Here, the condition (3) can easily be checked by the fact that each row of triangle (except for the top row corresponding to the sequence itself) contains no repetitions. Here the circle denotes the ordinary difference is negative and hence converted to a positive value by adding 15. Some observations follow as Remarks.



(a) Class 1 (b) Class 2

Fig. 1. Array form and modular difference triangle of sequences in Classes 1 and 2

Remark 1 (Classes 1 and 2 are NOT new). Sequences from Class 1 and Class 2 are the same as those given by Games in [3] and their transformed versions using (2). In fact, all the sequences constructed in [3] of length 15 and mod 15 are in either Class 1 or Class 2.

Remark 2 (Class 5 is new). Sequences in Class 5 are new, in the sense that no previously known algebraic constructions produce them.

Remark 3. Some sequences in Class 5 are palindromic. That is, for example, $\mathbf{e}_5 = (e_1, e_2, ..., e_{15})$ shown earlier has the property that

$$e_i = e_{14-i}, \quad 0 \le i < 15. \quad \text{[palindromic property]} \tag{4}$$

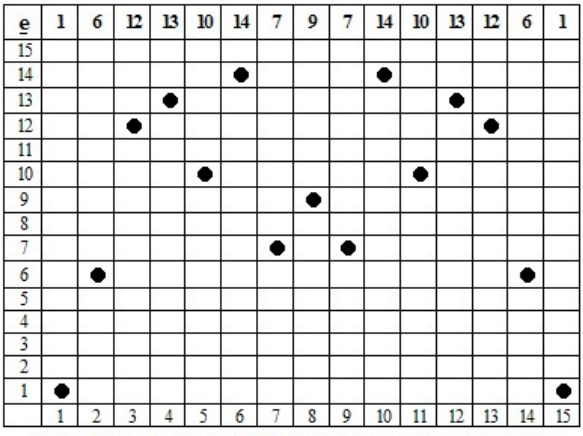
Furthermore, the first 8 terms satisfy the following:

$$|\{e_j \ominus e_{j+s} | 0 \le j < 8 - s\}| = 8 - s, \quad 1 \le s < 8, \quad \text{[modified DT property]} \tag{5}$$

where

$$e_j \ominus e_{j+s} = \begin{cases} 15 - (e_j - e_{j+s}), & \text{if} \quad 8 \le e_j - e_{j+s} < 15, \\ e_j - e_{j+s}, & \text{if} \quad 0 < e_j - e_{j+s} < 8, \\ |e_j - e_{j+s}|, & \text{if} \quad -7 \le e_j - e_{j+s} < 0, \\ 15 + (e_j - e_{j+s}), & \text{if} \quad -14 \le e_j - e_{j+s} < -7 \end{cases}$$

and $0 < e_j \ominus e_{j+s} < 8$. This property is shown in Fig. 3.



Array form of 15×15 Modular Sonar sequence in Class 5

1 6 12 13 10 14 7 9 7 14 10 13 12 6 1
⑩ ⑨ ⑭ 3 ⑪ 7 ⑬ 2 ⑧ 4 ⑫ 1 6 5
④ ⑧ 2 ⑭ 3 5 0 ⑩ ⑫ 1 ⑬ 7 11
③ ⑪ ⑬ 6 1 7 ⑧ ⑭ ⑨ 2 4 12
⑥ ⑦ 5 4 3 0 ⑫ ⑪ ⑩ 8 9
② ⑭ 3 6 ⑪ 4 ⑨ ⑫ 1 13
⑨ ⑫ 5 ⑭ 0 1 ⑩ 3 6
⑦ ⑭ ⑬ 3 ⑫ 2 1 8
⑨ ⑦ 2 0 ⑬ 8 6
② ⑪ ⑭ 1 4 13
⑥ ⑧ 0 7 9
③ ⑨ 6 12
④ 0 11
⑩ 5
0

Fig. 2. Array form and modular difference triangle of sequences in Class 5

3 Case $v = 5 \times 7 = 35$

First try was to generalize Class 5 of case $v = 15$ with palindromic property and modified DT property. For the faster check in a computer search, we were able to prove the following:

Lemma 1. *Let* $\boldsymbol{e} = (e_0, e_1, ..., e_{v-1})$ *be a sequence over* $\{0, 1, ..., v-1\}$ *of odd length* v *that is palindromic as in* (4)*. If* $\boldsymbol{e}$ *is a modular sonar sequence mod* v*, then its first* $(v+1)/2$ *elements satisfy the following condition, similar to* (5)*:*

$$|\{e_j \ominus e_{j+s} | 0 \le j < (v+1)/2 - s\}| = (v+1)/2 - s, \quad 1 \le s < (v+1)/2, \quad (6)$$

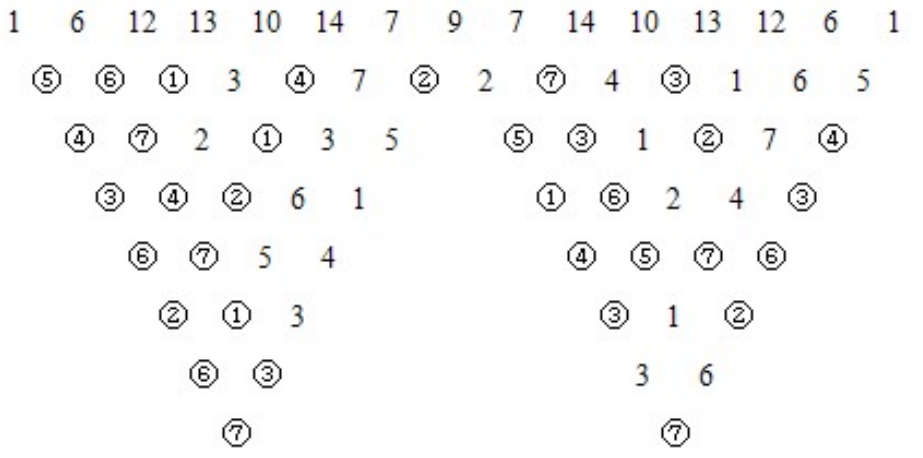


Fig. 3. Modified DT property of some sequences in Class 5

where

$$e_j \ominus e_{j+s} = \begin{cases} v-(e_j-e_{j+s}), & \text{if } (v+1)/2 \le e_j - e_{j+s} < v, \\ e_j - e_{j+s}, & \text{if } 0 < e_j - e_{j+s} < (v+1)/2, \\ |e_j - e_{j+s}|, & \text{if } -((v-1)/2) \le e_j - e_{j+s} < 0, \\ v+(e_j-e_{j+s}), & \text{if } -(v-1) \le e_j - e_{j+s} < -((v-1)/2) \end{cases}$$

and $0 < e_j \ominus e_{j+s} < (v+1)/2$.

Proof. If $e_j \ominus e_{j+s} = 0$, then the value $e_j - e_{j+s} \pmod v$ appears twice in row s of the original modular difference triangle, which is impossible.

Now, suppose the sequence does not satisfy the condition (6). Then, there exist $0 \le j \ne j' < (v+1)/2 - s$ such that, for some $1 \le s < (v+1)/2$, $e_{j'} \ominus e_{j'+s} = e_j \ominus e_{j+s}$. Denote

$$\begin{aligned} a &= e_j - e_{j+s}, & d(s,j) &= e_j \ominus e_{j+s}, \\ a' &= e_{j'} - e_{j'+s}, & d'(s,j') &= e_{j'} \ominus e_{j'+s}. \end{aligned}$$

From the definition of $\ominus$, then we have

$$\begin{aligned} a &\in \{v-d(s,j), d(s,j), -d(s,j), v+d(s,j)\}, \\ a' &\in \{v-d(s,j'), d(s,j'), -d(s,j'), v+d(s,j')\}. \end{aligned}$$

Since $a = v - d(s,j)$ or $a = d(s,j)$ and $a' = v - d(s,j')$ or $a' = d(s,j')$ all mod v, we have 4 cases all mod v:

$$\begin{aligned} A &: a = v - d(s,j) \text{ and } a' = v - d(s,j') &\Rightarrow\quad & a = a', \\ B &: a = d(s,j) \text{ and } a' = d(s,j') &\Rightarrow\quad & a = a', \\ C &: a = v - d(s,j) \text{ and } a' = d(s,j') &\Rightarrow\quad & a = v - a', \\ D &: a = d(s,j) \text{ and } a' = v - d(s,j') &\Rightarrow\quad & a = v - a'. \end{aligned}$$

For Cases A and B,

$$e_j - e_{j+s} = e_{j'} - e_{j'+s} \pmod{v}, \quad 0 \le j \ne j' < (v+1)/2 - s,$$

which is a contradiction. Similarly for the cases C and D. □

Hoping that the new example in Class 5 of length 15 above belongs to a general family, we have done a search for the same kind $\mathbf{e} = (e_0, e_1, ..., e_{34})$ of length 35 mod 35, by checking only the first 18 terms using Lemma 1. It took about 7 days on a PC to conclude that no such example exists.

Second try was to generalize and emulate the process of constructing the binary ideal 2-level autocorrelation sequences of period $v = p(p+2)$ from those of period p and $p+2$. [6] However, we do not have any further idea on this approach.

Third try was to generalize the method of Welch-Costas array of order $p-1$. [9] [6] There exists an integer n such that $v = p(p+2)$ is a divisor of $2^n - 1$. Consider the finite field F_{2^n} and an element β of order v in it. Successive powers of β will produce a sequence of length v over F_{2^n}. This sequence will surely satisfy the difference triangle property. However, the values are not over $\{0, 1, 2, ..., v-1\}$ but over F_{2^n}. Therefore, we have to see if there exists a transformation that sends this sequence into that over $\{0, 1, 2, ..., v-1\}$ preserving the difference triangle property. Various approach were tested for $n = 12$ and $v = 35$, but all failed to find any example. However, this approach finds a $2^{12} \times 35$ modular sonar array by transforming the elements of F_{2^n} into binary 12-tuples, and then by reading them (or their cyclic shifts) as binary expansions of ordinary integers. This example gives a hope for the next approach, and explicitly, it is

$$(3417, 1107, 2707, 1682, 2516, 413, 1607, 3489, 1591, 599, 3075, 2675,\\ 2390, 3517, 468, 3268, 532, 1842, 165, 2947, 3486, 3124, 1271, 2954,\\ 899, 199, 2151, 3684, 3352, 2647, 346, 3616, 965, 2863, 2048).$$

Fourth try was to use and modify the transformation (2) as done in [14], using the example of length 35 but mod 2^{12} found above. The goal is to find u, s, c such that the resulting transformed version has as long run of empty rows as possible to be deleted. The resulting array may not be modular, but we just tried, in vain.

References

1. Baumert, L.D.: Cyclic Difference Sets. Lecture Notes in Mathematics, vol. 182. Springer, Heidelberg (1971)
2. Costas, J.P.: Medium constraints on sonar design and performance. In: FASCON CONV. Rec., pp. 68A–68L (1975)
3. Games, R.A.: An algebraic construction of sonar sequences using M-sequences. SIAM J. Algebraic Discrete Methods 8, 753–761 (1987)
4. Golomb, S.W.: Shift Resister Sequences (revised ed.), p. 39. Aegean Park Press, Laguna Hills, CA (1982)

5. Golomb, S.W.: Algebraic constructions for Costas arrays. J. Combinatorial Theory, ser. A, 37, 13–21 (1984)
6. Golomb, S.W.: Construction of signals with favorable correlation properties. In: Keedwell, A.D. (ed.) Survey in Combinatorics. LMS Lecture Note Series, vol. 166, pp. 1–40. Cambridge University Press, Cambridge (1991)
7. Golomb, S.W., Gong, G.: Sequence Design for Good Correlation. Cambridge University Press, Cambridge (2005)
8. Golomb, S.W., Song, H.-Y.: A conjecture on the existence of cyclic Hadamard difference sets. Journal of Statistical Planning and Inference 62, 39–41 (1997)
9. Golomb, S.W., Taylor, H.: Two-dimensional synchronization patterns for minimum ambiguity. IEEE Trans. Inform. Theory IT-28, 263–272 (1982)
10. Gong, G.: Theory and applications of q-ary interleaved sequences. IEEE Trans. Inform. Theory 41(2), 400–411 (1995)
11. Gong, G.: New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case. IEEE Trans. Inform. Theory 48, 2847–2867 (2002)
12. Hall Jr., M.: A survey of difference sets. Proc. Amer. Math. Soc. 7, 975–986 (1956)
13. Kim, J.-H.: On the Hadamard Sequences, PhD Thesis, Dept. of Electronics Engineering, Yonsei University (February 2002)
14. Moreno, O., Games, R.A., Taylor, H.: Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols. IEEE Trans. Inform. Theory 39, 1985–1989 (1993)
15. Simon, M.K., Omura, J.K., Scholtz, R.A., Levitt, B.K.: Spread Spectrum Communications Handbook. Computer Science Press, Rockville (1985), revised edition, McGraw-Hill (1994)
16. Song, H.-Y., Golomb, S.W.: On the existence of cyclic Hadamard difference sets. IEEE Trans. Inform. Theory 40(4), 1266–1268 (1994)