On (n, k)-sequences : properties and applications to coding

Chang Hyun Eo, Hong-Yeop Song, and Kyu Tae Park
Dept. of Electronic Engineering, Yonsei University,
134 Shinchon-Tong, Sudaemoon-Ku, Seoul, 120-749, Korea
Tel: +82-2-361-4861, Fax: +82-2-312-4584
E-mail: hysong@bubble.yonsei.ac.kr

November 19, 1997

Extended Abstract

Consider the sequence $(a_0, a_1, \ldots, a_7) = (0, 1, 4, 6, 5, 3, 7, 2)$ of length 8 which uses the numbers from 0 to 7 exactly once, which is shown at the top row of Fig. 1. It is, in fact, a permutation of order 8, and has the property that the differences $a_{i+d} - a_i \pmod 4$ of two terms (if they are "comparable")

0		1		4		6		5		3		7		2
	1		*		2		3		*		*		*	
		*		*		1		*		2		3		
			*		*		*		1		*			
				*		2		3		*				
					3		*		*					
						*		1						
							2							

Figure 1: Example: a (4,2)-sequence and its triangle of differences mod 4

are all distinct for each i and d. Here, two terms a_{i+d} and a_i are said to be comparable if either they both belong to $\{0,1,2,3\}$ or they both belong to $\{4,5,6,7\}$. This sequence $(a_1,a_2,\ldots,a_8) = (0,1,4,6,5,3,7,2)$ is called a "$(4,2)$-sequence" in [SG94cm].

In general, a pair (a_i,a_j) is said to be "comparable" if the integer parts of a_i/n and a_j/n are the same. Now, an (n,k)-sequence is defined as a permutation $a_1,a_2,\ldots,a_{kn}$ of $0,1,2,\ldots,kn-1$, such that

$$a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod{n} \tag{1}$$

for every s,t and d with $1 \le s < t < t+d \le kn$, and for every comparable pairs (a_{s+d},a_s) and (a_{t+d},a_t).

An (n,k)-sequence has some interesting interpretaion as a generalization of, so-called, exponential Welch Costas sequence [SG94cm, GT82, GT84], some interesting combinatorial properties [SG94cm, Song91, EGT89], and some additional applications to designing various two-dimensional synchronization patterns such as "Vatican arrays" [GT85, GET90, Song91] and sets of sonar arrays with ideal auto and cross correlation functions [SG94isit].

In this presentation, we will briefly describe each of these aspects of (n,k)-sequences with emphasis on some new results. Specifically, we will talk about (1) a construction of (n,k)-sequences whenever $nk+1$ is a prime and its proof [SG94cm] with some new discussions; (2) existence of (n,k)-sequences [SG94cm] with some new existence results by computer, and a few corrections to Table 1 in [SG94cm]; and (3) an application to designing best known pair of sonar arrays better than those given in [SG94isit]. For each of these aspects, we include some brief discussions in the below.

I. Algebraic construction whenever $nk+1$ is prime

The only known algebraic construction is given by the following theorem. For the proof, see [SG94cm].

Theorem 1 (SongGo94cm) *Let α be a primitive root modulo $p = kn+1 > 2$ where p is a prime. For $i = 1, 2, \ldots, kn$, take the value of $\log_\alpha(i)$ to be between 0 and $kn-1$ such that $\log_\alpha(i) = j$ if $\alpha^j = i$. Let q_i and r_i be the quotient and remainder, respectively, when $\log_\alpha(i)$ is divided by k; that is, $\log_\alpha(i) = kq_i + r_i$, where $0 \le r_i \le k-1$. Then, $a_i = q_i + r_i n$ for $i = 1, 2, \ldots, kn$ is an (n,k)-sequence.*

We are interested in whether two (n,k)-sequences from this contruction with two distinct primitive roots are essentially the same. Now, we need to define what we mean by "essentially the same." For this purpose, we can think of the following transformations of an (n,k)-sequence into another: (1) S_{jc} is to add (mod n) some constant c to every term a_i with $\lfloor a_i/n \rfloor = j$, preserving the type of each term. Here, we say "a_i has type j" if $\lfloor a_i/n \rfloor = j$, any comparable pair has two terms of the same type. There are nk such transformations. (2) M_m is to multiply (mod n) some constant m times all the a_i's preserving also the type of each term, where m is relatively prime to n. There are $\phi(n)$ such transformations. (3) R is to take the mirror image (reversal of the a_i's). R has order 2 in the group of transformations of (n,k)-sequences. (4) P is to permute types of terms by either adding or subtrating some multiple of n. There are $k!$ such transformations corresponding to the permutation group of order k.

Note that the transformations S_{jc} and M_m are defined to fix the type of each term, and the the transfomration P may change the type of each term. It is easy to verify that all of the above transformations preserve the property that in the triangle of differences mod n, the differences of comparable pairs in a row are all distinct. In fact, one can obtain an (n,k)-sequence from a given (n,k)-sequence by taking any combination of the above transformations. This suggests that we should classify two (n,k)-sequences as the same (or, essentially the same) if one can be obtained from the other by some combination of the above transformations.

$$
\begin{aligned}
S_{01}: &\quad \dot{0}\dot{1}4\dot{6}5\dot{3}7\dot{2} \Rightarrow \dot{1}\dot{2}4\dot{6}5\dot{0}7\dot{3} \\
M_3: &\quad \dot{0}\dot{1}4\dot{6}5\dot{3}7\dot{2} \Rightarrow \dot{0}\dot{3}4\dot{6}7\dot{1}5\dot{2} \\
R: &\quad \dot{0}\dot{1}4\dot{6}5\dot{3}7\dot{2} \Rightarrow \dot{2}7\dot{3}56\dot{4}\dot{1}\dot{0} \\
P: &\quad \dot{0}\dot{1}4\dot{6}5\dot{3}7\dot{2} \Rightarrow 45\dot{0}\dot{2}\dot{1}7\dot{3}6
\end{aligned}
$$

Figure 2: Examples of transformations on a $(4,2)$-sequence

Figure 2 shows some examples of the above transformations on the $(4,2)$-sequence shown in the previous figure. Here, the dot represents the terms of type 0.

We will prove in this presentation that, if $nk+1=p$ is prime, any two primitive roots in the construction in Theorem 1 produce the same (n,k)-sequences in the above sense.

II. Existence of $(n,2)$-sequences, an update

In [SG94cm, SP95], the number $w_2(n)$ of essentially distinct $(n,2)$-sequences is reported for n up to 10, and it is to be noted that the non-existence of a $(10,2)$-sequence was determined using a computer.

In this presentation, we will give a brief update on this. Specifically, we will report that $w_2(11)=1$ was determined using only about 52 hours of CPU time on a PentiumPro 200MHz personal computer. The case for $n=12$ is still running over 30 days, but could be completed before the symposium.

Some minor corrections on $w_2(n)$ for $n=4$ and $n=8$ will also be reported relative to Table 1 in [SG94cm], which is a result of a recent independent check. Therefore, the sequence $w_2(n)$ for $n=1,2,...,11$ becomes

$$1,1,2,2,5,4,8,6,1,0,1.$$

It is interesting to note that the value increases not at all monotonically from $n=1$ to $n=7$ and then decreases to 0 at $n=10$. On the other hand, we

Figure 3: Top $2(=k)$ arrays $A = A_0$ and $B = B_0$ of size 4×8 are from the $(4, 2)$-sequence $0, 1, 4, 6, 5, 3, 7, 2$. The arrays $A_1, A_2, A_3, B_1, B_2, B_3$ are cyclically row-permuted versions of A or B.

Consider only the case where $k = 2$, or $(n, 2)$-sequences. From any $(n, 2)$-sequence, we can construct a pair of $n \times 2n$ arrays with exactly one dot per each row. This is illustrated using the (4,2)-sequence, and shown in Figure 3. Here, if you take any one from A's and any one from B's, the resulting pair will satisfy optimum auto and cross correlations. If you consider this pair transposed, you will obtain a pair of sonar arrays, but in terms of the number

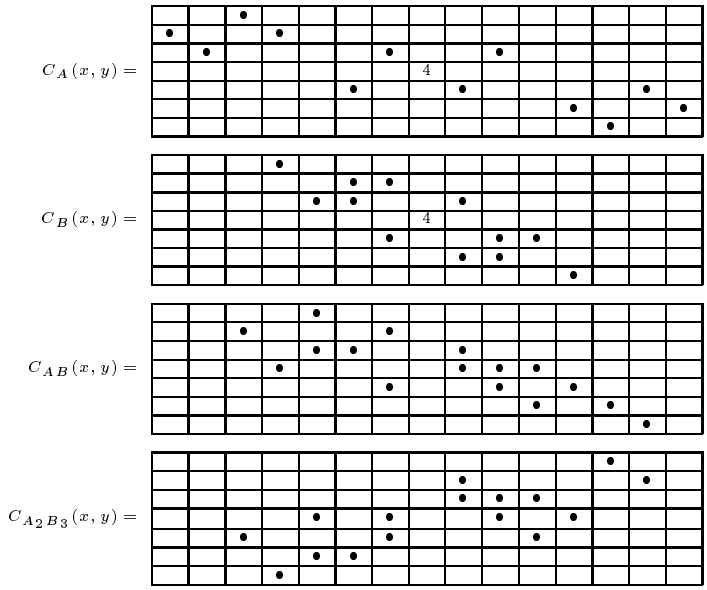

Figure 4: Correlations of signals A_i and B_j

of columns for a given number of rows this will not be the best known pair. In this case, it produces a pair of sonar arrays of size 8×4, which can also be obtained via the Lempel construction of Costas arrays [Gol84, GT84, MGT93] and then splitting the array in half. In terms of the ratio between the number of rows and the number or columns, this construction is not very efficient because it will produce the arrays having $2n$ rows and n columns. At any rate, this will produce a pair with optimum correlations, some of which are shown in Figure 4.

Now, consider the construction in Theorem 1 for $(n, 2)$-sequences. It can be illustrated for $2n + 1 = 13$ using 2 as a primitve root mod 13, which is shown in Figure 5. In this figure, the row corresponding to a_j represents the $(6, 2)$-sequence, and the column under the heading α^i represents the exponential-Welch construction of Costas sequence [Gol84, GT84, MGT93] of order 12. From this figure, it is obvious that the $(n, 2)$-sequences con-

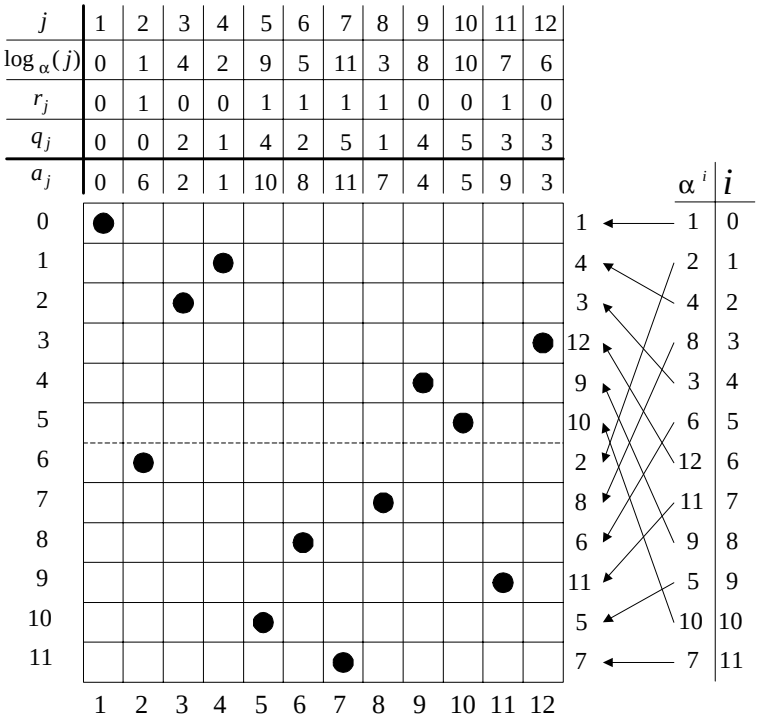

Figure 5: Relation of the (6,2)-sequence by Theorem 1 and the exponential Welch construction of Costas sequence of order 12

structed by the above method whenever $2n+1 = p$ is a prime is in fact easily described via the exponential-Welch construction of Costas sequence of order $p-1$. That is, if you write the sequence α^i in a column in the order $i = 0, 2, 4, \ldots, p-3, 1, 3, 5, \ldots, p-2$, put a dot at the position labeled by each term in each row of a $(p-1) \times (p-1)$ array, and finally read out the column indices from left to right, then you will have exactly the $(n,2)$-sequence given by the construction in Theorem 1.

This idea of "shuffling" the terms of exponential-Welch Costas sequences, together with the process of obtaining best known sonar arrays via "modular sonar arrays" in [MGT93], can be used to produce a better pair of sonar arrays with optimum auto and cross correlations. Note that one easy way to get a pair of sonar arrays with n rows is to first find a best known sonar

array of size $n \times m$ and split this into two parts, for example, as shown in Figure 6. Here, we introduce two different methods of splitting a given sonar array into two parts: middle-cut, and shuffle.

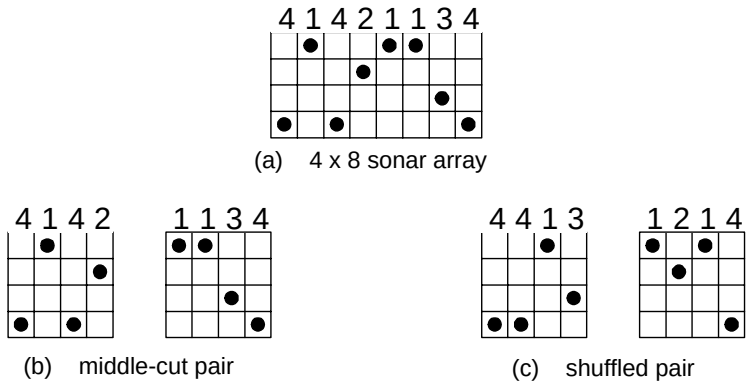

Figure 6: A given sonay array and two methods of splitting this into two parts

If we start with a best known sonar array, then we have a good chance of ending up with a best known pair of sonar arrays. However, we could do a little more by slightly modifying the process of obtaining the best known sonar arrays described in [MGT93]. The idea is to first split the "modular sonar arrays" and then take modular-sonar-preserving transformations, instead of taking the transformations first to obtain the best sonar array and then split the result into two parts. In [SG94isit], a rough idea of this kind was used to produce some of much better pair of sonar arrays from the extended Welch construction of modular sonar arrays. In this presentation, we will report the best known maximum number of columns of a pair of sonar arrays with optimum auto and cross correlations for a given number of row up to 100.

References

[EGT89] T. Etzion, S. W. Golomb, and H. Taylor, "Tuscan-k squares," *Adv. in Appl. Math.*, vol. 10, pp. 164-174, 1989.

[Gol84] S. W. Golomb, "Algebraic constructions for Costas arrays," *Journal of Combinatorial Theory*, series A., vol. 37, pp. 13-21, 1984.

[GET90] S. W. Golomb, T. Etzion and H. Taylor, "Polygonal path constructions for Tuscan-k squares," *Ars Combinatoria.*, vol. 30, pp. 97-140, 1990.

[GT82] S. W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity," *IEEE Trans. Information Theory.*, vol. IT-28, pp. 600-604, 1982.

[GT84] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays," *Proceedings of the IEEE.*, vol. 72, pp. 1143-1163, 1984.

[GT85] S. W. Golomb and H. Taylor, "Tuscan squares — A new family of combinatorial designs," *Ars Combinatoria.*, vol. 20-B, pp. 115-132, 1985.

[Song91] Hong Y. Song, "On aspects of Tuscan squares," *Ph.D. Thesis.*, University of Southern California, 1991.

[SG94cm] H. Y. Song and S. W. Golomb, "Generalized Welch-Costas sequences and their application to Vatican arrays"' *Contemporary Mathematics.*, vol. 168, American Mathematical Society, pp. 341-351, 1994.

[SG94isit] H. Y. Song and S. W. Golomb, "Two dimensional patterns with optimal auto- and cross-correlation functions," *Proceedings of 1994 International Symposium on Information Theory.*, pp. 362, 1994.

[SP95] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995.

[MGT93] O. Moreno, R. Games, and H. Taylor, "Sonar sequences from Costas arrays and the best known sonar sequences with up to 100 symbols," *IEEE Trans. on Info. Theory*, vol. 39, no. 6, pp. 1985-1987, 1993.