(n,k)-sequences and its Application to FH Design

ChangHyun Eo and Hong-Yeop Song

Department of Electronics Engineering
Yonsei University

Coding and Information Theory Workshop
Feb. 20, 1998

■ Example: a sequence of length 8

$$
\begin{array}{ccccccccccccccc}
0 & & 1 & & 4 & & 6 & & 5 & & 3 & & 7 & & 2 \\
\hline
 & 1 & & * & & 2 & & 3 & & * & & * & & * & \\
 & & * & & * & & 1 & & * & & 2 & & 3 & & \\
 & & & * & & * & & * & & 1 & & * & & & \\
 & & & & * & & 2 & & 3 & & * & & & & \\
 & & & & & 3 & & * & & * & & & & & \\
 & & & & & & * & & 1 & & & & & & \\
 & & & & & & & 2 & & & & & & &
\end{array}
$$

- The sequence itself is a permutation of order 8.

- Triangle below the sequence calculates differences of corresponding terms mod 4 if both less than 3 or if both larger than or equal to 4.

- In any row of this triangle, differences do not repeat.

0		6		2		1		10		8		11		7		4		5		9		3
	*		*		5		*		4		3		2		*		1		*		*	
		2		*		*		*		1		5		*		*		*		4		
			1		4		*		*		3		*		*		2		5			
				*		2		*		*		*		*		4		*				
					*		5		*		3		*		1		*					
						*		1		2		4		5		*						
							*		*		3		*		*							
								4		*		*		2								
									5		3		1									
										*		*										
											3											

■ **Example of a sequence of length 12**

```
0 1 11 2 15 8 14 16 19 7 12 9 6 18 3 10 17 13 5 4 20
------------------------------------------------------
 1 * * * * * 2 3 * 5 4 * * * * * * * 6 *
  * 1 * * 6 * 5 * * 2 * * 4 * * 3 * * *
   2 * 4 * 1 * * * * * * * * 6 * * * *
    * * * * 4 6 * * * * * 1 * * 2 * 3
     * * * * * 4 * * 6 * 5 * * * 1 *
      * * * * * 1 * 2 * 3 * 4 6 * *
       * * 3 * * * 4 * * * 1 * 5 2
        * * 1 * * * * * 5 6 * * *
         * * 5 4 3 * * 1 * * * *
          * * * * * 2 3 * * * *
           * 5 * 1 * * * * * *
            6 * * * 2 5 * * 1
             * 2 6 * * * * 4
              3 * * * * * 6
               * * 2 3 * *
                * * * 2 5
                 * 4 * *
                  5 3 *
                   4 *
                    *
```

■ Example of a sequence of length 21

■ Definition: (n, k)-Sequences

Let $a_1, a_2, \ldots, a_{kn}$ be a permutation of $0, 1, 2, \ldots, kn-1$. Let (a_i, a_j) be called a "comparable pair" if $\lfloor a_i/n \rfloor = \lfloor a_j/n \rfloor$, where $\lfloor x \rfloor$ is the integer part of x.

Then, $a_1, a_2, \ldots, a_{kn}$ is called an "(n, k)-sequence" if

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

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

■ Existence whenever $nk + 1$ is prime

Let $kn + 1 = p > 2$ be a prime, and α be a primitive root mod p.

For each $i = 1, 2, \ldots, kn$, we denote

$$\log_\alpha(i) = j \quad \Longleftrightarrow \quad \alpha^j = i$$

where $0 \leq j \leq kn - 1$.

Let q_i and r_i be determined by the relation

$$\log_\alpha(i) = kq_i + r_i, \quad \text{where} \quad 0 \leq r_i \leq k - 1.$$

Then

$$a_i = q_i + nr_i$$

is an (n, k)-sequence.

■ Proof of Existence

$$(a_i, a_j) \quad \text{comparable} \quad \leftrightarrow \quad r_i = r_j$$

Therefore, we have (mod p)

$$\alpha^{k(a_i - a_j)} \equiv \frac{\alpha^{ka_i}}{\alpha^{ka_j}} \equiv \frac{\alpha^{k(q_i + nr_i)}}{\alpha^{k(q_j + nr_j)}} \equiv \frac{\alpha^{kq_i + r_i}}{\alpha^{kq_j + r_j}} \equiv \frac{i}{j}$$

Assume (a_{s+d}, a_s) and (a_{t+d}, a_t) are "distinct" comparable pairs. Then

$$\begin{aligned}
&\text{if} \quad a_{s+d} - a_s \equiv a_{t+d} - a_t \pmod{n},\\
&\Longrightarrow \; k(a_{s+d} - a_s) \equiv k(a_{t+d} - a_t) \pmod{kn},\\
&\Longrightarrow \; \alpha^{k(a_{s+d} - a_s)} \equiv \alpha^{k(a_{t+d} - a_t)} \pmod{p},\\
&\Longrightarrow \; \frac{s+d}{s} \equiv \frac{t+d}{t} \pmod{p},\\
&\Longrightarrow \; d \equiv 0 \quad \text{or} \quad s \equiv t \pmod{p}.
\end{aligned}$$

Since $0 < d < kn = p - 1$ and $1 \leq s \neq t \leq kn$, we have a contradiction. (q.e.d)

■ Transformations of $(n,2)$-sequences

Let $a_1, a_2, \ldots, a_{2n}$ be an $(n,2)$-sequence.

Call a_i of type A if $0 \le a_i \le n-1$,

and of type B if $n \le a_i \le 2n-1$.

- S_A : add (mod n) some constant to every term of type A
- S_B : add (mod n) some constant to every term of type B
- M : multiply (mod n) some constant m to every a_i's, where gcd$(m,n) = 1$
- R : take the backward reading
- P : interchange type A and type B by adding n if $a_i < n$ or by subtracting n if $a_i \ge n$

Note that S_A, S_B and M preserve the type of each term and P transposes two types.

■ Examples of Transformations

S_A : $\dot{0}\dot{1}465\dot{3}7\dot{2} \Rightarrow \dot{1}\dot{2}465\dot{0}7\dot{3}$

S_B : $\dot{0}\dot{1}465\dot{3}7\dot{2} \Rightarrow \dot{0}\dot{1}647\dot{3}5\dot{2}$

M : $\dot{0}\dot{1}465\dot{3}7\dot{2} \Rightarrow \dot{0}\dot{3}467\dot{1}5\dot{2}$

R : $01465372 \Rightarrow 27356410$

P : $\dot{0}\dot{1}465\dot{3}7\dot{2} \Rightarrow 45\dot{0}\dot{2}\dot{1}7\dot{3}6$

Here, the dot represents the term of type A.

■ Number of distinct $(n,2)$-sequences

The number of "essentially distinct" $(n,2)$-sequences for $n \leq 11$ is determined by computer search, and is shown in the next table.

n	$2n$	#	CPU	$b_i \longrightarrow a_i$
1	2	1		$01 \longrightarrow 01\star$
2	4	1		$0110 \longrightarrow 0231\star$
3	6	2		$001011 \longrightarrow 013254\star$
				$011001 \longrightarrow 035124$
4	8	2		$00111010 \longrightarrow 01465372$
				$01001110 \longrightarrow 04217563$
5	10	5		$0011101001 \longrightarrow 0159738246$
				$0100011101 \longrightarrow$ 0513476928 $0514367928\star$
				$0111010001 \longrightarrow$ 0589173246 0596184237
6	12	4	0.0 Sec	$001110010101 \longrightarrow 026B831A4957$
				$010011110010 \longrightarrow$ $06218A7B4593$ $0621A8B74593\star$
				$010111000110 \longrightarrow 061BA8452793$
7	14	8	2.0 Sec	$00110010110011 \longrightarrow$ $017B24D5CA3698$ $017B64C3D825A9$
				$01001110001101 \longrightarrow 07148AB6539D2C$
				$01011000111010 \longrightarrow 071CA524D986B3$
				$01100010111001 \longrightarrow 07A124958DC63B$
				$01100101011001 \longrightarrow 07B1395A48D62C$
				$01101110001001 \longrightarrow 0791AB8365D42C$
				$01110010110001 \longrightarrow 079A14D28C653B$
8	16	6	1.6 Min	$0010111001110100 \longrightarrow$ $0182AFD379BE6C54$ $0182E9B37FDA6C54\star$
				$0011101001011100 \longrightarrow$ $018AD3B26F79EC54$ $018EB3D2697FAC54$
				$0111001001001110 \longrightarrow$ $089F27E51A36BDC4$ $089F61E37A52BDC4$
9	18	1	20 Min	$011000010101111001 \longrightarrow$ $09F1873A4H6GBCE25D\star$
10	20	0	10 Hrs	NONE
11	22	1	51 Hrs	$0000101001100110101111 \longrightarrow$ $0182B9K35CFA7LJ4E6IDHG\star$
12	24	0	130 days	NONE
13	26	?		

■ (circular) Vatican arrays [a new frequency-hopping codes]

From the $(4,2)$-sequences of length 8, we can construct a 4×8 array V of 8 symbols in which the top row is $a_1, a_2, \ldots, a_8$ and the columns are cyclic shifts of either $0, 1, 2, 3$ or $4, 5, 6, 7$.

$$V = \boxed{\begin{matrix} 0 & 1 & 4 & 6 & 5 & 3 & 7 & 2 \\ 1 & 2 & 5 & 7 & 6 & 0 & 4 & 3 \\ 2 & 3 & 6 & 4 & 7 & 1 & 5 & 0 \\ 3 & 0 & 7 & 5 & 4 & 2 & 6 & 1 \end{matrix}}$$

The array V has the two properties that (1) each row is a permutation of $0, 1, 2, \ldots, 7$, and (2) for any two symbols a and b and for any integer m from 1 to 7 there exists at most one row in which b is m steps to the right of a.

■ Vatican array from the $(7, 2)$-sequence

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

0	1	11	2	15	8	14	16	19	7	12	9	6	18	3	10	17	13	5	4	20
1	2	12	3	16	9	15	17	20	8	13	10	0	19	4	11	18	7	6	5	14
2	3	13	4	17	10	16	18	14	9	7	11	1	20	5	12	19	8	0	6	15
3	4	7	5	18	11	17	19	15	10	8	12	2	14	6	13	20	9	1	0	16
4	5	8	6	19	12	18	20	16	11	9	13	3	15	0	7	14	10	2	1	17
5	6	9	0	20	13	19	14	17	12	10	7	4	16	1	8	15	11	3	2	18
6	0	10	1	14	7	20	15	18	13	11	8	5	17	2	9	16	12	4	3	19

■ Vatican array from the (7,3)-sequence

■ Open Problems and Concluding Remarks

1. Structure of the transformation group of (n, k)-sequences. It has the order at most $2kn\phi(n)k!$.

2. In the "prime construction" where $nk + 1 = p$ is a prime, two different primitive roots produce essentailly the same (n, k)-sequences.

3. A $(p, 2)$-sequence exists for every prime p. (confirmed for $p \leq 11$)

4. There exists at least one (p, k)-sequence for each positive integer $k > 1$ and for every prime p. (confirmed for (i) $p = 3$ and $2 \leq k \leq 10$, (ii) $p = 5$ and $2 \leq k \leq 6$, and (iii) $p = 7$ and $2 \leq k \leq 4$)

5. The *only known* family of $(n, 1)$-sequences is from the "Welch construction" for $n = p - 1$, which is usually called as *Costas sequences by Welch*. The converse is one of the famous open problem: Every $(n, 1)$-sequence essentially comes from the Welch construction.

6. There does not exists a $(10, 2)$-sequence of length 20.

7. Application to designing an $n \times nk$ frequency hopping patterns with **optimal Hamming correlation** from an (n, k)-sequence.