On (n, k)-sequences

Hong-Yeop Song

Department of Electronics Engineering
Yonsei University

The Korean Mathematical Society,
Conference 97
October 24, 1997

■ Example: a sequence of length 8

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

- 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.

■ 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 $1 \leq s < t < t + d \leq kn$ 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 comparable pairs. Then

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

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

■ Transformations of $(n, k=2)$-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

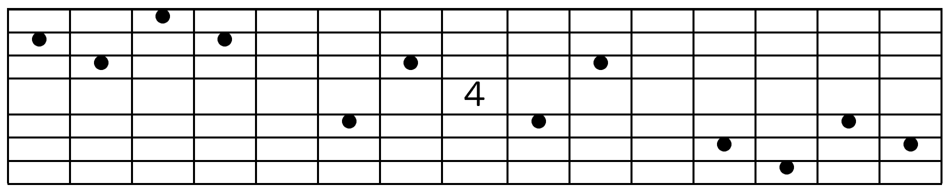
The number of "essentially distinct" $(n, 2)$-sequences for $n \leq 11$ is determined by computer search.

For convenience, $10, 11, 12, \ldots$ are represented by $A, B, C, \ldots$. The sequences followed by "$\star$" are essentially the same as those given by "prime construction."

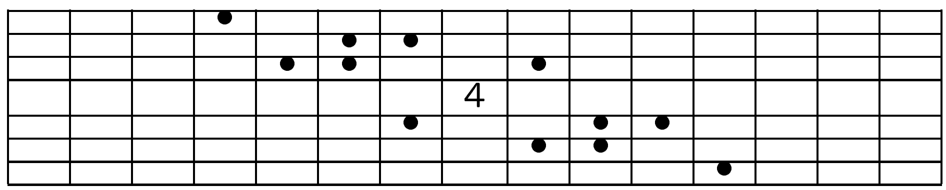
n	$2n$	#	CPU time	a_i
1	2	1		01 $\star$
2	4	1		0231 $\star$
3	6	2		013254 $\star$
				035124
4	8	2		01465372
				04217563
5	10	5		0159738246
				0513476928 0514367928$\star$
				0589173246 0596184237
6	12	4	$\sim$ 0.0 sec	026B831A4957
				06218A7B4593 0621A8B74593$\star$
				061BA8452793
7	14	8	$\sim$ 2.0 sec	017B24D5CA3698 017B64C3D825A9
				07148AB6539D2C
				071CA524D986B3
				07A124958DC63B
				07B1395A48D62C
				0791AB8365D42C
				079A14D28C653B
8	16	6	$\sim$ 1.6 min	0182AFD379BE6C54 0182E9B37FDA6C54$\star$
				018AD3B26F79EC54 018EB3D2697FAC54
				089F27E51A36BDC4 089F61E37A52BDC4
9	18	1	$\sim$ 20 min	09F1873A4H6$GBCE$25D $\star$
10	20	0	$\sim$ 10 hours	NONE
11	22	1	$\sim$ 52 hours	0182B9K35CFA7LJ4E6$IDHG$ $\star$
12	24	?		still running over 30 days

■ **Every primitive root produces the same example**

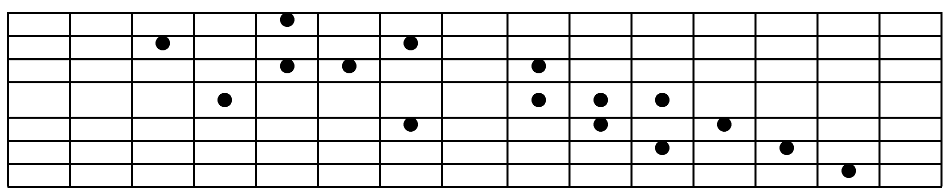
$C_A(x,y) =$



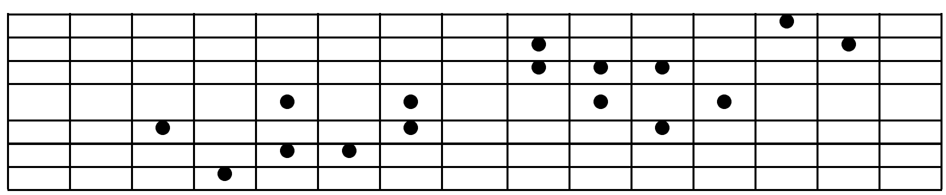
$C_B(x,y) =$



$C_{AB}(x,y) =$



$C_{A_2B_3}(x,y) =$



■ Concluding Remarks

- 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*.

- There does not exists a $(10,2)$-sequence of length 20.
  — 100 hours of CPU time in Sun Sparc station 600 (1993)
  — 10 hours in PentiumPro200 (1997)

- **Conjecture** Whenever p is a prime there exists at least one (p,k)-sequence of length kp for each positive integer $k > 1$.

True	for $p = 3$ and $2 \le k \le 10$
True	for $p = 5$ and $2 \le k \le 6$
True	for $p = 7$ and $2 \le k \le 4$

- Two applications to designing communication signals having **optimal correlations**.