5 HEEL, J.: 'Dynamic motion vision'. IFAC Symposia Series, Proc. of Trienial World Congress, Vol. 5, pp. 99–104, 1989

## Crosscorrelations of Frank sequences and Chu sequences

P.Z. Fan, M. Darnell and B. Honary

*Indexing terms: Core division multiple access, Binary sequences*

Sets of Frank sequences and Chu sequences are two classes of polyphase sequence with ideal periodic autocorrelation functions, which at the same time have optimum crosscorrelation functions. In the Letter, the crosscorrelations of sets of combined Frank/Chu sequences, which contain a larger number of sequences than either of the two constituent sets, are considered. It is shown analytically that the crosscorrelations are similar to those of the original sets with one exception, while the autocorrelations remain perfectly impulsive.

*Introduction:* In code-division multiple-access (CDMA) communication systems, in order to permit unambiguous message synchronisation, to minimise cochannel interference, and to support a large number of simultaneous users, large families of sequences with good autocorrelation functions (ACFs) and small crosscorrelation function (CCF) values, are required.

Frank sequences [1] and Chu sequences [2] are two classes of sequence with perfect ACFs and optimum CCFs. However, the number of Frank sequences and Chu sequences available for a given length $L$ is relatively small. In this Letter we discuss the CCFs between any two sequences in combined Frank/Chu sequence sets which provides a larger family size.

*Properties of Frank and Chu sequence sets:* Frank sequences $F = \{f^{(1)}, \ldots, f^{(r)}, \ldots, f^{(q-1)}\}$ are a class of polyphase sequence of length $L = q^2$, in which the $q$th roots of unity are the elements of the sequence $f^{(r)} = (f_0^{(r)}, f_1^{(r)}, \ldots, f_{L-1}^{(r)})$, i.e.

$$f_n^{(r)} = f_{jq+k}^{(r)} = e^{\frac{i2\pi}{q} rkj} \quad 0 \le k, j < q \quad (r,q) = 1 \tag{1}$$

where $0 \le n \le q^2 - 1$ and $q$ is any integer.

For Chu sequences $C = (c^{(1)}, \ldots, c^{(r)}, \ldots, c^{(L-1)})$, the elements of the sequence $c^{(r)} = (c_0^{(r)}, c_1^{(r)}, \ldots, c_{L-1}^{(r)})$ of length $L$ are given by

$$c_n^{(r)} = e^{\frac{i\pi}{L} r(n+1)n} \quad 0 \le n < L \quad (r, L) = 1 \tag{2}$$

It has been shown that the periodic ACFs and CCFs of Frank sequences and Chu sequences are given by [1–4]:

$$R_{f^{(r)}}(\tau) = \sum_{n=0}^{L-1} f_n^{(r)} f_{n+\tau}^{*(r)} = \begin{cases} L & \tau = 0 \pmod{L} \\ 0 & \tau \ne 0 \pmod{L} \end{cases} \tag{3}$$

$$\begin{aligned} R_{f^{(r)},f^{(s)}}(\tau) &= \sum_{n=0}^{L-1} f_n^{(r)} f_{n+\tau}^{*(s)} \\ &= \sqrt{L} \quad \forall\tau\ r \ne s \quad (r-s, q) = 1 \quad q \text{ is odd} \end{aligned} \tag{4}$$

$$R_{c^{(r)}}(\tau) = \sum_{n=0}^{L-1} c_n^{(r)} c_{n+\tau}^{*(r)} = \begin{cases} L & \tau = 0 \pmod{L} \\ 0 & \tau \ne 0 \pmod{L} \end{cases} \tag{5}$$

$$\begin{aligned} R_{c^{(r)},c^{(s)}}(\tau) &= \sum_{n=0}^{L-1} c_n^{(r)} c_{n+\tau}^{*(s)} \\ &= \sqrt{L} \quad \forall\tau\ r \ne s \quad (r-s, L) = 1 \quad L \text{ is odd} \end{aligned} \tag{6}$$

*Periodic CCFs of sets of combined Frank/Chu sequences:* To obtain a larger set of sequences, we define the following combined sets of Frank/Chu sequence:

$$\begin{aligned} FC = \{&f^{(1)}, \cdots, f^{(s)}, \cdots, f^{(s')}, \cdots, f^{(q-1)}; \\ &c^{(1)}, \cdots, c^{(r)}, \cdots, c^{(r')}, \cdots, c^{(L-1)}\} \end{aligned} \tag{7}$$

where $L = q^2$, $(s, q) = 1$, $(s', q) = 1$, $(s - s', q) = 1$, and $(r, L) = 1$, $(r', L) = 1$, $(r - r', L) = 1$.

Obviously the ACFs of the sequences in the set are exactly the same as those of the original Frank sequences and Chu sequences. The CCF is equal to $\sqrt{L}$ if both the sequences to be correlated are Frank sequences or both the sequences are Chu sequences. When one sequence is a Frank sequence and the other is a Chu sequence, then the CCF is calculated as shown below.

Let $n = jq + k$ and $\tau = uq + v$, $0 \le j, k, u, v \le q - 1$, then the integer $n + \tau$ can be represented as

$$n + \tau = (j + u + \epsilon)q + (k + v - \epsilon q) \tag{8}$$

where $\varepsilon = 0$, if $k + v \le q - 1$, and $\in = 1$, if $k + v \ge q - 1$. Let $\alpha = e^{i2\pi/q}$, then $f_n^{(s)} = f_{jq+k}^{(s)} = \alpha^{skj}$, $c_n^{(r)} = \alpha^{r(n+1)n/2q}$. Thus

$$\begin{aligned} &R_{c^{(r)},f^{(s)}}(\tau) \\ &= \sum_{n=0}^{L-1} c_n^{(r)} f_{n+r}^{*(s)} = \sum_{n=0}^{q^2-1} c_{jq+k}^{(r)} f_{(j+u+\epsilon)q+(k+v-\epsilon q)}^{*(s)} \\ &= \sum_{k=0}^{q-1}\sum_{j=0}^{q-1} \alpha^{r(jq+k)(jq+k+1)/2q} \alpha^{-s(j+u+\epsilon)(k+v-\epsilon q)} \\ &= \sum_{k=0}^{q-1} \alpha^{rk(k+1)/2q-s(u+\epsilon)(k+v-\epsilon q)} \\ &\qquad \times \sum_{j=0}^{q-1} \alpha^{jr(jq+2k+1)/2-js(k+v-\epsilon q)} \\ &= \sum_{k=0}^{q-1} \alpha^{rk(k+1)/2q-s(u+\epsilon)(k+v)} \sum_{j=0}^{q-1} \alpha^{j(\frac{rq}{2}+rk+\frac{r}{2}-sk-sv)} \end{aligned} \tag{9}$$

The last equality is valid because $\alpha^{\pm cq} = 1$, $c$ is any integer, and $\alpha^{j^2rq/2} = e^{i\pi rj^2} = (-1)^{rj^2} = (-1)^{rj} = \alpha^{rjq/2}$. Let $l = (rq)/2 + rk + r/2 - sk - sv$; the above inner sum is equal to zero, if $l \ne 0$, and is equal to $q$, if $l = 0$. The equation $l = 0 \pmod{q}$ has a unique solution $k_0 = [sv - r(1 + q)/2]/(r - s)$ if $r \ne s \pmod{q}$. That is

$$\sum_{j=0}^{q-1} \alpha^{j(\frac{rq}{2}+rk+\frac{r}{2}-sk-sv)} = \begin{cases} 0 & k \ne k_0 = \frac{sv-r(1+q)/2}{r-s} \\ q & k = k_0 = \frac{sv-r(1+q)/2}{r-s} \end{cases} \tag{10}$$

Therefore, if $r \ne s \pmod{q}$, we have

$$|R_{c^{(r)},f^{(s)}}(\tau)| = |\alpha^{rk_0(k_0+1)/2q-s(u+\epsilon)(k_0+v)} q| = q = \sqrt{L} \tag{11}$$

For $r = s \pmod{q}$, the CCFs between Frank sequences and Chu sequences are given by

$$\begin{aligned} &R_{c^{(s+hq)},f^{(s)}}(\tau) \\ &= \sum_{n=0}^{L-1} c_n^{(s+hq)} f_{n+\tau}^{*(s)} \\ &= \sum_{k=0}^{q-1} \alpha^{(s+hq)k(k+1)/2q-s(u+\epsilon)(k+v)} \sum_{j=0}^{q-1} \alpha^{js(\frac{q}{2}+\frac{1}{2}-v)} \end{aligned} \tag{12}$$

where $h = 0, 1, \ldots, q - 1$ and

$$\sum_{j=0}^{q-1} \alpha^{js(\frac{q}{2}+\frac{1}{2}-v)} = \begin{cases} 0 & v \ne v_0 = \frac{q+1}{2} \\ q & v = v_0 = \frac{q+1}{2} \end{cases} \tag{13}$$

Hence

$$\begin{aligned} &R_{c^{(s+hq)},f^{(s)}}(\tau) \\ &= \begin{cases} 0 & v \ne v_0 = \frac{q+1}{2} \\ q \sum_{k=0}^{\frac{q-1}{2}-1} \alpha^{(s+hq)k(k+1)/2q-su(k+v_0)} + & \\ q \sum_{k=\frac{q-1}{2}}^{q-1} \alpha^{(s+hq)k(k+1)/2q-s(u+1)(k+v_0)} & v = v_0 = \frac{q+1}{2} \end{cases} \end{aligned} \tag{14}$$

As an example, the combined Frank/Chu sequences of length 25 are

$$\bar{F}C = \{f^{(1)}, f^{(2)}, f^{(3)}, f^{(4)}; c^{(1)}, c^{(2)}, c^{(3)}, c^{(4)}\} \qquad (15)$$

The CCFs between any two sequences, $R_{c(r)}$ , $_{c(s)}$ $(\tau)$, $R_{f(r)}$ , $R_{f(s)}$ $(\tau)$ and $R_{c(r)}$ , $_{f(s)}$ $(\tau)$ ($r \neq s$ mod 5), are constant and equal to 5. For $r = s$ mod 5, the CCFs, $R_{c(s)}$ , $_{f(s)}$ $(\tau)$, are listed in Table 1.

**Table 1:** CCFs of combined Frank/Chu sequences ($L$ = 25, $r = s$ mod 5)

| $\tau$ | 0 1 … 23 24 |
|---|---|
| $\lvert R_{c(1)}, {}_{f(1)} (\tau)\rvert$ | 0 0 0 24 0 0 0 0 4.4 0 0 0 0 1.8 0 0 0 0 1.8 0 0 0 0 4.4 0 0 |
| $\lvert R_{c(2)}, {}_{f(2)} (\tau)\rvert$ | 0 0 0 21 0 0 0 0 3.8 0 0 0 0 8.2 0 0 0 0 8.2 0 0 0 0 3.8 0 0 |
| $\lvert R_{c(3)}, {}_{f(3)} (\tau)\rvert$ | 0 0 0 18 0 0 0 0 6.2 0 0 0 0 11. 0 0 0 0 11. 0 0 0 0 6.2 0 0 |
| $\lvert R_{c(4)}, {}_{f(4)} (\tau)\rvert$ | 0 0 0 14 0 0 0 0 12. 0 0 0 0 8.8 0 0 0 0 8.8 0 0 0 0 12. 0 0 |

*Conclusions:* The CCFs between Frank sequences and Chu sequences are considered in this Letter. It is proved that $R_{f(r)}$ , $_{c(s)}$ $(\tau) = \sqrt{L}$ when $r \neq s$ (mod $q$). Although there exist some time shifts where the CCF values are relatively large (when $r = s$ (mod $q$)), in this case, the CCFs are zero for all other time shifts include those around the zero time shift position.

It should be noted that the methods presented here can also apply to generalised Frank sequences [3] and generalised Chu sequences [4].


17 January 1994
*Electronics Letters Online No: 19940340*

P. Z. Fan and M. Darnell (*Department of Electronic Engineering, University of Hull, Hull HU6 7RX, United Kingdom*)

B. Honary (*Department of Engineering, Lancaster University, Lancaster LA1 4YW, United Kingdom*)

**References**

1 FRANK, R.L., and ZADOFF, S.A.: 'Phase shift pulse codes with good periodic correlation properties', *IRE Trans. Inform. Theory*, 1962, **IT-8**, pp. 381–382
2 CHU, D.C.: 'Polyphase codes with good periodic correlation properties', *IEEE Trans. Inform. Theory*, 1972, **IT-18**, pp. 531–533
3 SUEHIRO, N., and HATORI, M.: 'Modulatable orthogonal sequences and their application to SSMA systems', *IEEE Trans. Inform. Theory*, 1988, **IT-34**, pp. 93–100
4 POPOVIC, B.M.: 'Generalized chirp-like polyphase sequences with optimum correlation properties', *IEEE Trans.*, 1992, **IT-38**, pp. 1406–1409

## Comment

# Improved identity-based key sharing system for multiaddress communication

C.-S. Laih and W.-C. Kuo

*Indexing terms: Information theory, Cryptosystems, Discrete logarithm problem, El-Gamal's public-key cryptosystem*

*Introduction:* Since Shamir [1] proposed the concept of identity-based (ID-based) cryptosystems, many realisable schemes for ID-based cryptosystems and key sharing systems have been proposed. One of the earliest concrete ID-based cryptosystems using the discrete logarithm problem was proposed by Tsujii *et al.* [2]. However, if $n$ entities conspire then the $n$ secret pieces of information of the trusted centre (TC) in their scheme can be disclosed. To improve the security, a modified version of the above scheme was developed by Laih and Lee [3]. However, it was shown that the modified version can be completely broken by the conspiracy of ($n$ + 1) entities with overwhelming probability [4]. In 1990, Chikazawa and Inoue proposed an ID-based key sharing system [5] whose key preparation in TC is an improvement of [2]. Shimbo and Kawamura, however, developed an attack (the so called SK attack) to show that the scheme is not secure when it is used for conference key distribution [6]. An improved version was then proposed by Chikazawa and Yamagishi [7] to counter the SK attack. In the improved ID-based key sharing system, the key preparation in TC is the same as the original scheme and it allows entities to use different random numbers to counter the SK attack. In this Comment, we show that even though the improved ID-based key sharing system can resist the SK attack, the improved scheme as well as the original scheme can be completely broken by the conspiracy of ($n$ + 1) entities with overwhelming probability.

*Key preparation by TC in [5, 7]:* The key preparation by the centre in the ID-based key sharing systems [5, 7] is the same as the RSA scheme. The TC first chooses ($e$, $N$) as its public information and calculates $d$ satisfying

$$e \cdot d \equiv 1 \pmod{L}$$

as its secret information, where $L = \mathrm{lcm}(p - 1, q - 1)$ and $p$ and $q$ are two distinct primes. To calculate the secret information for the entities in the system, the centre also generates $n$-dimensional vectors

$$\mathbf{a} = (a_1, a_2, \cdots, a_n) \quad 1 \le a_i \le L - 1 \quad (1 \le i \le n)$$

and

$$\mathbf{G} = (g^{a_1} \bmod N, g^{a_2} \bmod N, \cdots, g^{a_n} \bmod N)$$

where $g$ is an integer which is a primitive element in both $GF(p)$ and $GF(q)$. Suppose that entity $i$ has the identification information $ID_i$ and every entity in the system can easily generate the $k$-dimensional vector of entity $i$

$$\mathbf{I}_i = (x_{i1}, x_{i2}, \cdots, x_{ik}) \quad x_{il} \in \{0, 1\} \quad (1 \le l \le k < n)$$

and $n$-dimensional vector

$$f(\mathbf{I}_i) = (y_{i1}, y_{i2}, \cdots, y_{in}) \quad y_{il} \in \{0, 1\} \quad (1 \le l \le n)$$

where $f()$ is a one-to-one one-way function. Then, for entity $i$, the centre computes ($u_i$, $v_i$, $s_i$) satisfying

$$u_i = \mathbf{a} \cdot f(\mathbf{I}_i) \pmod{L} = \sum_{j=1}^{n} a_j y_{ij} \pmod{L} \qquad (1)$$

$$u_i \cdot v_i \equiv 1 \pmod{L} \qquad (2)$$

$$s_i = ID_i^d \pmod{N} \qquad (3)$$

and sends ($v_i$, $s_i$) to entity $i$ as its secret information. The main difference of the key preparation by the TC between the ID-based key sharing systems [5, 7] and ID-based cryptosystems [2, 3] is that the centre in [5, 7] sends $v_i$ as one of the secret pieces of information of entity $i$ instead of $u_i$. If the centre sends $u_i$ as one of the secret pieces of information of entity $i$, then it can be shown that the centre secret information **a** and $L$ can be completely disclosed by the conspiracy of ($n$ + 1) entities with overwhelming probability [4]. Because $u_i$ cannot be derived from $v_i$ without knowing $L$ it seems that the centre secret information **a** and $L$ cannot be computed when ($n$ + 1) entities conspire. However, as shown in the following, the ID-based key sharing system as well as the improved version can be completely broken by the conspiracy of ($n$ + 1) entities with overwhelming probability even if they can resist the SK attack.

*Attack:* The goal of this attack is to find the centre secret information $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $L$ by using the ($n$ + 1) entities' secret information $v_i$ and the common public information. From eqn. 1, we have

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \vdots & \vdots & & \vdots \\ y_{n+1,1} & y_{n+1,2} & \cdots & y_{n+1,n} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{n+1} \end{bmatrix} \pmod{L} \qquad (4)$$

Eqn. 4 can be rewritten as

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} & u_1 \\ y_{21} & y_{22} & \cdots & y_{2n} & u_2 \\ \vdots & \vdots & & \vdots & \vdots \\ y_{n+1,1} & y_{n+1,2} & \cdots & y_{n+1,n} & u_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \\ -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod{L} \qquad (5)$$