On Pairwise Shift-Invariant Protocol Sequences

Yijin Zhang, Kenneth W. Shum *Member, IEEE,* and Wing Shing Wong *Fellow, IEEE*

***Abstract*—Protocol sequences offer an approach to implement random-access channel without feedback. For these sequences, it is desirable that their cross-correlation should be as low as possible and that the length of their period should not be short. Completely shift-invariant sequences form an important class of protocol sequences which have perfect cross-correlation property but exponential growth period as a function of the number of users. We investigate in this paper a broader class of protocol sequences which are only pairwise shift-invariant. Results on minimum period and bit-pattern structure are presented.**

***Index Terms*—Hamming cross-correlation function, protocol sequence, random-access channel without feedback.**

I. Introduction

BINARY sequences have found applications in many civilian and military systems. One of such applications is to define multiple access protocols. In wireless sensor networks or ad hoc networks, due to computing power limitation and strict energy constraints, it is desirable to have simple multiple access protocols which do not require frequent monitoring of the channel for feedback information and complicated processing. This motivates the investigation of protocol sequences without feedback that was pioneered in [1].

A protocol sequence uses a periodic binary sequence to specify when a user can transmit and when to be idle. Some related works can be found in [2]–[5]. Guaranteed throughput and least common period are two common performance measures for such sequences. As users may join and depart at different times, sequences with long period are undesirable even if they can ensure high throughput. Since these performance measures are closely tied to the periodic cross-correlation function, the latter is the main object of study in this paper.

Ideally, the cross-correlation function should be invariant to relative shift delays among the sequences, as they cannot be assumed to be synchronized due to lack of feedback. More specifically, pairwise shift-invariant sequences are considered here.

II. System Model and Hamming cross-correlations

We follow Massey's model [1] to define a communication channel divided into time slots of equal duration that are shared by K active users. Each active user follows a binary protocol sequence, $S = \{S(0), S(1), S(2), \ldots\}$, and transmits a packet at time slot i if and only if $S(i)$ is equal to 1. It is assumed that the users know and align to the slot boundaries. However, they are not required to synchronize to each other and have different start time. At any time slot, a packet collision occurs if more than one user transmits simultaneously. All transmitted packets in this duration are considered lost. Otherwise, it is assumed that the receiver can receive the packet correctly and decode its content.

This work was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 416906.

The authors are with the Dept. of Information Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong (email: zyj007@ie.cuhk.edu.hk, kshum2009@gmail.com, wswong@ie.cuhk.edu.hk)

Definition 1: Let $S_1, \ldots, S_k$ be k periodic binary sequences with a common period L. Define the *k-wise Hamming cross-correlation* function among these k sequences for relative shifts $\tau_1, \ldots, \tau_{k-1}$ by

$$H_{S_1 \ldots S_k}(\tau_1, \ldots, \tau_{k-1}) := \sum_{t=0}^{L-1} S_1(t) S_2(t+\tau_1) \cdots S_k(t+\tau_{k-1})$$

The normalized version is defined to be

$$\bar{H}_{S_1 \ldots S_k}(\tau_1, \ldots, \tau_{k-1}) := H_{S_1 \ldots S_k}(\tau_1, \ldots, \tau_{k-1})/L.$$

The pairwise case $H_{S_1 S_2}$ is simply the usual Hamming cross-correlation function for a pair of sequences. For a periodic binary sequence with a period L, following [1], we define its *duty factor* by $R := \frac{1}{L}\sum_{t=0}^{L-1} S(t)$. The k-wise Hamming cross-correlation is said to be *shift-invariant* (SI) if $\bar{H}_{S_1 \ldots S_k}$ is identically equal to a constant. A set of protocol sequences is called *completely SI* if the k-wise Hamming cross-correlation is SI for all choices of k distinct sequences and for all k. A set of protocol sequences is called *pairwise SI* if the 2-wise Hamming cross-correlation is SI for all pairs of distinct protocol sequences.

The following is a basic result on Hamming cross-correlation [6]:

$$\frac{1}{L^{k-1}} \sum_{\tau_1=0}^{L-1} \cdots \sum_{\tau_{k-1}=0}^{L-1} \bar{H}_{S_1 \ldots S_k}(\tau_1, \ldots, \tau_{k-1}) = R_1 \cdots R_k, \quad (1)$$

where R_i denotes the duty factor of S_i, for $i = 1, \ldots, k$. If the k-wise Hamming cross-correlation is SI, then it follows from (1) that $\bar{H}_{S_1 \ldots S_k}$ is identically equal to $R_1 R_2 \cdots R_k$. In particular, $\bar{H}_{S_1 S_2}$ is identically equal to $R_1 R_2$ if it is SI.

Completely SI sequences enjoy a constant individual throughput property that is independent of any relative shift delays. Unfortunately, it is proved that SI sequences have long common periods [5]. This motivates the relaxation of the completely SI assumption to pairwise SI. Obviously, the collection of all completely SI sequence sets is a subset of the collection of pairwise SI sequences. However, pairwise SI sequences in general are not completely SI, which can be seen from the following example.

Example 1: Consider a set of 3 protocol sequences with duty factors $1/2$, $1/3$, and $1/5$. One can check that the

following sequence set is pairwise SI, but not completely SI:

$$S_1 : 11100\,01110\,00111\,00011\,10001\,11000$$
$$S_2 : 11111\,00000\,00000\,11111\,00000\,00000$$
$$S_3 : 11000\,00000\,11000\,00000\,11000\,00000$$

For zero shift-delay, the 3-wise cross-correlation value is 2. However, the 3-wise cross-correlation value cannot be 2 for all shift-delays as the averaged 3-wise cross-correlation value should be 1 by (1).

From simulation studies, one can show that some pairwise SI sequences enjoy throughput performance close to SI sequences. It is of interest to understand whether short pairwise SI sequences can be constructed. A surprising result proven in this paper is that for some combinations of duty factors, pairwise SI sequences are indeed completely SI. Moreover, we will show that for pairwise SI sequences the minimum period is exponential in the number of distinct sequences.

III. Pairwise SI Sequences

A. Discrete Fourier Analysis

Definition 2: A periodic sequence S can be represented by a polynomial with binary coefficients, denoted by $s(x)$,

$$s(x) := \sum_{t=0}^{L-1} S(t)x^t. \tag{2}$$

A complex number ω is called a *primitive* L-th root of unity if $\omega^L = 1$ but $\omega^n \neq 1$ for all $1 \leq n < L$. In this paper, we will choose and fix a complex primitive L-th root of unity and denote it by ω. The discrete Fourier transform of sequence S is defined as $s(\omega^n)$ with n varying from 0 to $L-1$. A complex L-th root of unity ψ is called a *spectral null* of the sequence S if $s(\psi) = 0$. A cyclic shift of a sequence S by τ corresponds to multiplying $s(x)$ by x^τ modulo $x^L - 1$. Therefore cyclically shifting a sequence does not alter the spectral nulls.

The next lemma is the discrete analog of Plancherel's identity [7].

Lemma 1. *Two sequences A and B with period L is pairwise SI if and only if $a(x)b(x)$ is divisible by $(x^L - 1)/(x - 1)$.*

Proof: Let $H_{AB}(\tau)$ be the Hamming cross-correlation function corresponding to A and B. We have

$$\begin{aligned}\sum_{\tau=0}^{L-1} H_{AB}(\tau)x^\tau &\equiv \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} a(t)b(t+\tau)x^\tau \\ &\equiv \sum_{t=0}^{L-1} a(t)x^{-t}\sum_{\tau=0}^{L-1} b(t+\tau)x^{t+\tau} \\ &\equiv a(x^{-1})b(x) \pmod{x^L - 1}. \end{aligned}\tag{3}$$

Hence $H_{AB}(\tau)$ is SI if and only if $a(x^{-1})b(x) \equiv h_0 \sum_{\tau=0}^{L-1} x^\tau \pmod{x^L - 1}$, where h_0 denotes the common Hamming cross-correlation value. As the coefficients of $a(x)$ are real numbers, the spectral nulls of $a(x^{-1})$ are closed under taking reciprocal. Thus, spectral nulls of $a(x)$ and $b(x)$ contains all spectral nulls of $\sum_{\tau=0}^{L-1} x^\tau = (x^L - 1)/(x - 1)$. It follows that sequences A and B is pairwise SI if and only if $a(x)b(x)$ is divisible by $(x^L - 1)/(x - 1)$. ∎

In Example 1, the three polynomials $s_1(x)$, $s_2(x)$ and $s_3(x)$ are respectively

$$(x^2 + x + 1)\frac{x^{30} - 1}{x^6 - 1},\ \frac{x^5 - 1}{x - 1}\frac{x^{30} - 1}{x^{15} - 1},\ (x + 1)\frac{x^{30} - 1}{x^{10} - 1}.$$

It can be verified that $s_1(x)s_2(x)$, $s_2(x)s_3(x)$ and $s_3(x)s_1(x)$ are all divisible by $(x^{30} - 1)/(x - 1)$. Hence $\{S_1, S_2, S_3\}$ is a pairwise SI protocol set by Lemma 1.

B. Minimum Period

In subsequent discussions, we consider a set of K pairwise SI sequences, $S_1, \ldots, S_K$, with associated polynomial $s_1(x), \ldots, s_K(x)$. Let the duty factors be n_i/d_i, for $i = 1, 2, \ldots, K$, with n_i and d_i being relatively prime. Denote the common period of this sequence set by L. Let $p_1, \ldots, p_m$ be the prime factors of L, and $L = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$. Since L must be a multiple of the denominator d_i of each duty factor, the prime factorization of d_i can be written as $p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_m^{e_{im}}$ with $e_{i1} \leq r_1$, $e_{i2} \leq r_2, \ldots, e_{im} \leq r_m$.

Definition 3: For $n \geq 1$, the n-th *cyclotomic polynomial*, $f_n(x)$, is the monic polynomial whose zeros are precisely the complex primitive n-th roots of unity, each with multiplicity 1 [8, p.194]. For example, the 6th cyclotomic polynomial is $f_6(x) = (x - e^{2\pi\sqrt{-1}/6})(x - e^{-2\pi\sqrt{-1}/6}) = x^2 - x + 1$.

We summarize below some results about cyclotomic polynomials that we will need in this paper.

Lemma 2 ([8] Chapter 13)**.** *(i) Cyclotomic polynomials are monic polynomials with integral coefficients.*

(ii) $f_n(x)$ is a factor of $x^L - 1$ if and only if n divides L.

(iii) For all n, $f_n(x)$ is irreducible in the ring of polynomials with integral coefficients, i.e., if $f_n(x)$ divides $a(x)b(x)$, where $a(x)$ and $b(x)$ are polynomials with integral coefficients, then $f_n(x)$ divides $a(x)$ or $b(x)$, or both.

(iv) For a prime number p and positive integer m, the cyclotomic polynomial $f_{p^m}(x)$ equals $(x^{p^m} - 1)/(x^{p^{m-1}} - 1)$. Hence $f_{p^m}(1) = p$.

Definition 4: For $j = 1, 2, \ldots, m$, let

$$\mathcal{N}_j := \{f_{p_j^k}(x) : k = 1, 2, \ldots, r_j\}, \tag{4}$$

where r_j is the exponent of p_j in the factorization of L.

By part (ii) in Lemma 2, every cyclotomic polynomial $f(x)$ in $\mathcal{N}_j$ divides $(x^L - 1)/(x - 1)$, and by part (iv) in Lemma 2, we have $f(1) = p_j$ for all $f(x) \in \mathcal{N}_j$. It is noted that elements in $\mathcal{N}_j$ do not have common factors.

Lemma 3.

(i) For $i = 1, \ldots, K$ and $j = 1, \ldots, m$, at least e_{ij} cyclotomic polynomials in $\mathcal{N}_j$ does not divide $s_i(x)$.

(ii) If $\Phi_1(x)$ and $\Phi_2(x)$ are polynomials in $\mathcal{N}_j$ such that $\Phi_1(x)$ does not divide $s_i(x)$ and $\Phi_2(x)$ does not divide $s_k(x)$, for $i \neq k$, then $\Phi_1(x)$ and $\Phi_2(x)$ must be distinct.

Proof: (i) Suppose there are c_{ij} polynomials in $\mathcal{N}_j$ that divides $s_i(x)$, say $g_1(x), \ldots, g_{c_{ij}}(x)$. As they are monic polynomials with integral coefficents, we can write $s_i(x) = g_k(x)h_k(x)$ for each $k = 1, 2, \ldots, c_{ij}$, where $h_k(x)$ is a polynomial with integral coefficients. Let $g(x)$ be the product

$g_1(x)\cdots g_{c_{ij}}(x)$. Because each factor $g_k(x)$ is irreducible, $s_i(x)$ is divisible by $g(x)$, i.e., $s_i(x) = g(x)h(x)$, for some polynomial $h(x)$ with integral coefficients. Then, by putting $x = 1$, and using the property that $g(1) = p_j^{c_{ij}}$ by part (iv) of Lemma 2, we see that $p_j^{c_{ij}}$ divides $s_i(1)$. On the other hand, $s_i(1) = n_i L/d_i$ by (2) and the definition of duty factor. Since n_i is relatively prime to d_i, $s_i(1)$ contains exactly $r_j - e_{ij}$ factors of p_j. Thus, $c_{ij} \le r_j - e_{ij}$. It follows that e_{ij} is less than or equal to $r_j - c_{ij}$, which is exactly the number of polynomials in $\mathcal{N}_j$ that does not divide $s_i(x)$.

(ii) Suppose on the contrary that we can find $\Phi(x) \in \mathcal{N}_j$ such that $\Phi(x)$ does not divide $s_i(x)$ and $s_k(x)$, for $i \neq k$. Then by part (iii) of Lemma 2, $\Phi(x)$ does not divide $s_i(x)s_k(x)$. As $\Phi(x)$ is a factor of $(x^L - 1)/(x - 1)$ by part (ii) of Lemma 2, this contradicts the fact that $s_i(x)s_k(x)$ is divisible by $(x^L - 1)/(x - 1)$. ∎

Theorem 1. *The common period of any set of K pairwise SI sequences with duty factors n_i/d_i, for $i = 1, 2, \ldots, K$, (with n_i and d_i relatively prime) is divisible by $d_1 d_2 \cdots d_K$. In particular, the minimum common period is at least $d_1 d_2 \cdots d_K$.*

Proof: From Lemma 3, we conclude that $\mathcal{N}_j$ must contain at least $b_j := e_{1j} + e_{2j} + \ldots + e_{Kj}$ cyclotomic polynomials. Hence, $r_j \ge b_j$. Since the above inequality holds for all j, it follows that $\prod_{j=1}^m p_j^{b_j}$ divides L. But $d_1 d_2 \cdots d_K = \prod_{j=1}^m p_j^{b_j}$ by the definition of b_j. Therefore $d_1 d_2 \cdots d_K$ divides L. ∎

It is shown in [5] that the minimum common period of a set of K *completely* SI sequences, with duty factors as in Theorem 1, is at least $d_1 d_2 \cdots d_K$. We conclude from Theorem 1 that relaxing the completely SI requirement to pairwise SI *cannot* shorten the common period.

C. Structural Theorem

Theorem 11 in [5], although stated for completely SI sequences, depends only on the pairwise SI property. These results imply interesting structures for pairwise SI sequences.

Theorem 2 ([5])**.** *Suppose that the duty factors of a set of K pairwise SI sequences are n_i/p, for $i = 1, \ldots, K$, and p is a prime number. If the common period meets the lower bound in Theorem 1, i.e., the common period is p^K, then the least periods of the sequences are $p, p^2, \ldots, p^K$. Moreover, suppose that the sequence with least period p^i has duty factor n_i/p. For each r with $0 \le r \le p^{i-1} - 1$, there are exactly n_i ones located among positions*

$$r, r + p^{i-1}, r + 2p^{i-1}, \ldots, r + (p-1)p^{i-1}. \qquad (5)$$

Theorem 3. *Let p be a prime. If K pairwise SI protocol sequences with duty factors n_i/p, for $i = 1, 2, \ldots, K$, have a common minimum period p^K, then they are completely SI.*

Proof: Theorem 2 implies that such pairwise SI sequences possess the structure described by (5). Theorem 8 in [5] established that such sequences are completely SI. ∎

Example 2: Consider the case that $K = 3$, $L = 27$ and the duty factors are all $2/3$. We can verify that the following sequence set is pairwise SI by Lemma 1. It follows from Theorem 3 that it must be also completely SI.

$$S_1 : 110\,110\,110\,110\,110\,110\,110\,110\,110$$
$$S_2 : 111\,111\,000\,111\,111\,000\,111\,111\,000$$
$$S_3 : 111\,111\,111\,111\,111\,111\,000\,000\,000$$

Remark: Theorem 3 explains why the construction in [3], which is targeted for pairwise SI sequences actually leads completely SI sequences.

D. Numerical Studies

Consider p pairwise SI sequences, each with duty factor R and period L. The sum throughput has a lower bound:

$$\sum_{i=1}^{p} \left[R - \sum_{j \neq i} \bar{H}_{S_i S_j}(0) \right] = p[R - R^2(p-1)] \qquad (6)$$

For prime p, we can take $R = (p+1)/(2p^2)$ in the construction of wobbling sequences to obtain a lower bound on the sum throughput that approaches $1/4$ as p approaches infinity [4]. Under the same condition, the sum throughput of pairwise SI sequences also approaches 1/4 from (6).

Protocol sequences	Max. pairwise cross-correlation	L	Asymp. throughput lower bound
Pairwise SI	R^2	p^p	$1/4$
Wobbling	$\frac{(p+3)R^2}{p+1}$	p^4	$1/4$

If the pairwise cross-correlation function can vary slightly, as in wobbling sequences, the minimum period can be reduced. The two families of sequence sets achieve roughly the same throughput performance when p is large.

IV. Conclusion

In this paper, pairwise SI protocol sequences are introduced. We have explored basic properties of its minimum period. Furthermore, if duty factors of the sequences satisfy some technical conditions, the sequence set is completely SI.

References

[1] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 31, no. 2, pp. 192–204, Mar. 1985.

[2] L. Györfi and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inform. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.

[3] C. S. Chen, W. S. Wong, and Y.-Q. Song, "Constructions of robust protocol sequences for wireless sensor and ad hoc networks," *IEEE Trans. Veh Tech.*, vol. 57, no. 5, pp. 3053–3063, 2008.

[4] W. S. Wong, "New protocol sequences for random access channels without feedback," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.

[5] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invariant protocol sequences for the collision channel without feedback," accepted for publication in IEEE Trans. Inform. Theory, Jul, 2009.

[6] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, 1980.

[7] E. M. Stein and R. Shakarchi, *Fourier Analysis: An Introduction*. Princeton, New Jersey: Princeton University Press, 2003.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1990.