Design and Construction of Protocol Sequences: Shift Invariance and User Irrepressibility

Kenneth W. Shum, Wing Shing Wong
Dept. of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong

Chi Wan Sung
Dept. of Electronic Engineering
City University of Hong Kong
Kowloon, Hong Kong

Chung Shue Chen
Centrum Wiskunde & Informatica
1098 XG Amsterdam
The Netherlands

***Abstract*—Protocol sequences are used for channel access in the collision channel without feedback. Each user is assigned a deterministic zero-one pattern, called protocol sequence. The zeros and ones in a protocol sequence are read out periodically, and a packet is sent if and only if it is one. A collision occurs if two or more users transmit at the same time. Due to the lack of feedback from the receiver and cooperation among users, the beginning of the protocol sequences cannot be synchronized and relative delay offsets are incurred. We study the design of protocol sequences from two different perspectives. Under the first one, called shift invariance, we aim at minimizing the fluctuation of throughput due to relative delay offsets. As for the second one, called user irrepressibility, we want to guarantee that each user can send at least one packet successfully in each period. For both design criteria, we derive a lower bound on sequence period and give an optimal construction that achieves this lower bound.**

I. Introduction

A. Channel Model

We consider a time slotted system with K transmitters and one receiver. Within a slot duration, each transmitter either sends out packet, or remains idle. If two or more users transmit at the same slot, a collision occurs and the collided packets are assumed unrecoverable. If there is only one user transmitting in a time slot, the packet will be received successfully. Forward error correction can be applied across packets to recover erasures and errors. We will assume that all successfully received packets are error-free, and define the effective throughput as the fraction of packets that can be sent without suffering any collision. We also assume that there is no cooperation among the users, and no feedback from the receiver.

The access of channel is done by assigning each user a deterministic and periodic zero-one sequence, called protocol sequence [1]. For $i = 1, 2, \ldots, K$, the protocol sequence associated with user i is specified by a row vector $\mathbf{s}_i := [s_i(0)\ s_i(1)\ \ldots\ s_i(L-1)]$, where L is the common period. As there is no feedback from the receiver and no cooperation among the users, each user has a relative delay offset τ, which is random but remains fixed throughout the communication session. User i sends a packet at slot t if $s_i(t+\tau) = 1$, and remains silent if $s_i(t+\tau) = 0$. Here, the addition by τ is modulo L addition.

This channel model is applicable to wireless sensor networks with limited computing capability [2]. Instead of implementing collision avoidance and backoff protocol, we design specific protocol sequences satisfying some favorable statistical properties. Each user can simply store the assigned protocol sequence in the memory and repeatedly read out the sequence.

B. Design Criteria of Protocol Sequences

The goal behind the first criterion, called *shift invariance*, is to minimize variance and fluctuation of throughput due to delay offsets. Shift-invariant sequences are used in the capacity achieving scheme for the collision channel without feedback [1]. Some constructions of shift-invariant sequences are provided in [1]–[3]. We present in this paper a general construction method that contains the constructions in [1]–[3] as special cases. We also establish a lower bound on sequence period and show that the construction is optimal.

The second criterion is called *user irrepressibility*. The objective is to guarantee that a user can send at least one packet within a predefined tolerable delay. The worst-case delay is bounded by the period of the sequences. We note that this is a strict guarantee with probability one, in contrast to random access scheme, like slotted ALOHA, where in a fixed period of time it is only guaranteed that with high probability each user has at least one successfully sent packet. Application of this strict guarantee is mentioned in [4] for medical systems. Some constructions of sequences with the property of user irrepressibility can be found in [5]–[8]. We establish a lower bound on sequence period and give a construction of sequences that achieves this lower bound asymptotically.

Remark: Protocol sequences is related to *optical orthogonal code* [9], and binary *cyclically permutable codes* [10]. The main difference is that Hamming autocorrelation is inessential in the design of protocol sequences. Only Hamming crosscorrelation is considered.

II. Shift-Invariant Sequences

The *Hamming weight* of a sequence is the number of ones in a period. The *duty factor* [1] of a sequence is the Hamming

This work was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 416906, and a grant from City University of Hong Kong under Project 7002386. This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme.

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

weight divided by the period, which measures the fraction of time a user is transmitting. The duty factor of user i is denoted by $f_i := (1/L)\sum_{t=0}^{L-1} s_i(t)$. We identify the K users with $\mathcal{K} := \{1, 2, \ldots, K\}$. Let $\mathcal{O}_K$ be the set

$$\{(i_1, \ldots, i_n) \in \mathcal{K}^K : i_1 < i_2 < \ldots < i_n, n = 1, \ldots, K\}$$

which represents the collection of all ordered n-tuples of users, for $n = 1, 2, \ldots, K$. We define a generalized notion of *Hamming crosscorrelation* for two or more sequences as follows. For $\mathsf{A} = (i_1, \ldots, i_n) \in \mathcal{O}_K$, let

$$H(\tau_1, \ldots, \tau_n; \mathsf{A}) := \sum_{t=0}^{L-1} \prod_{j=1}^{n} s_{i_j}(t + \tau_j).$$

It is the number of slots in a period where all users in A transmit at the same time, given that the delay offset of user i_j is τ_j, for $j = 1, \ldots, n$. When $n = 2$, it reduces to the usual notion of pairwise Hamming crosscorrelation. When $n = 1$, it is simply the Hamming weight of the sequence.

Given an ordered tuple $\mathsf{A} \in \mathcal{O}_K$, the Hamming crosscorrelation $H(\tau_1, \ldots, \tau_n; \mathsf{A})$ is said to be *shift-invariant* (SI) if it is a constant function of $\tau_1, \ldots, \tau_n$. We say that a protocol sequence set is shift-invariant if, for all ordered tuples of users $\mathsf{A} \in \mathcal{O}_K$, the Hamming crosscorrelation $H(\tau_1, \ldots, \tau_n; \mathsf{A})$ is shift-invariant.

When only users $i_1, \ldots, i_n$ are active in a period, with relative delay offsets $\tau_1, \ldots, \tau_n$, the *throughput* of user i_j, denoted by $\theta_j(\tau_1, \ldots, \tau_n; \mathsf{A})$ for $j = 1, \ldots, n$, is given by

$$\frac{1}{L} \sum_{t=0}^{L-1} s_{i_j}(t + \tau_j) \prod_{\ell \neq j} \big(1 - s_{i_\ell}(t + \tau_\ell)\big).$$

It is the fraction of time slots where user i_j transmits and users $i_1, \ldots, i_{j-1}, i_{j+1}, \ldots, i_n$ remain silent.

Example 1: The following are three shift-invariant sequences with duty factors 1/2, 1/3 and 2/3:

$$\mathbf{s}_1 = [1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0]$$
$$\mathbf{s}_2 = [1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0]$$
$$\mathbf{s}_3 = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0].$$

We can check that, for all τ_1, τ_2 and τ_3, the values of the Hamming crosscorrelations are $H(\tau_1, \tau_2; (1, 2)) = 3$, $H(\tau_2, \tau_3; (2, 3)) = 4$, $H(\tau_1, \tau_3; (1, 3)) = 6$ and $H(\tau_1, \tau_2, \tau_3; (1, 2, 3)) = 2$.

A. Throughput

In order to reduce the fluctuation due to delay offsets, we want to design protocol sequences such that the throughput of each user is as stable as possible for all possible delay offsets. In the extreme case, we want the throughput to be invariant and independent of the delay offsets. This motivates the following definition. Given n distinct users, $i_1, i_2, \ldots, i_n$ $(i_1 < i_2 < \ldots < i_n)$, we say that the throughput $\theta_j(\tau_1, \ldots, \tau_n; (i_1, \ldots, i_n))$ is shift-invariant if it is a constant function of $\tau_1, \ldots, \tau_n$. The next theorem says that the requirement that all throughput functions are shift-invariant is equivalent to the requirement that the Hamming crosscorrelations are shift-invariant.

Theorem 1. *A set of binary sequences $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K\}$ is shift-invariant if and only if the throughput function $\theta_j(\tau_1, \tau_2, \ldots, \tau_n; \mathsf{A})$ is shift-invariant for every $\mathsf{A} \in \mathcal{O}_K$, and $j = 1, 2, \ldots, n$.*

Proof: ($\Rightarrow$) Suppose that the Hamming crosscorrelation $H(\tau_1, \ldots, \tau_n; \mathsf{A})$ is SI for all $\mathsf{A} \in \mathcal{O}_K$. By re-labeling the users, it is sufficient to show that the throughput of user 1 is SI when users 1, $2, \ldots, n$ are active, for all $n \leq K$.

Let $\mathcal{B}$ be the set $\{1, 2, \ldots, n\}$, and B be the ordered tuple $(1, 2, \ldots, n)$. By the principle of inclusion-and-exclusion, the number of time slots in a period where user 1 transmits and users 2 to n are silent, is equal to

$$L\theta_1(\tau_1, \ldots, \tau_n; \mathsf{B}) = H(\tau_1; (1)) - \sum_{\alpha \in \mathcal{B} \setminus \{1\}} H(\tau_1, \tau_\alpha; (1, \alpha)) \ldots + (-1)^{n+1} H(\tau_1, \ldots, \tau_n; \mathsf{B}). \quad (1)$$

Since all Hamming crosscorrelations on the right hand side are SI, we conclude that the left hand side is also SI. Therefore, $\theta_1(\tau_1, \ldots, \tau_n; \mathsf{B})$ is SI.

($\Leftarrow$) Suppose that all throughput functions are SI. We will prove that the Hamming crosscorrelations are SI by mathematical induction. For $k = 1, 2, \ldots, K$, $H(\tau_k; (k))$ is the Hamming weight of the k-th sequence, and is easily seen to be SI.

Suppose that $H(\tau, \ldots, \tau_k; \mathsf{A})$ is SI for every order tuple A with length less than or equal to $n - 1$. Consider $\mathsf{B} = (1, 2, \ldots, n)$ as in the first part of the proof. We can rearrange the terms in (1), and express $H(\tau_1, \ldots, \tau_n; \mathsf{B})$ in terms of throughput $\theta_1(\tau_1, \ldots, \tau_n; \mathsf{B})$ and Hamming crosscorrelations associated with strictly less than n users. Since $\theta_1(\tau_1, \ldots, \tau_n; \mathsf{B})$ is SI by our assumption, and the Hamming crosscorrelations associated with strictly less than n users are also SI by the induction hypothesis, we see that $H(\tau_1, \ldots, \tau_n; \mathsf{B})$ is SI. This shows that the Hamming crosscorrelation corresponding to $\mathsf{B} = (1, 2, \ldots, n)$ is SI. The proof for other choices of n-tuples in $\mathcal{O}_K$ is similar. ■

After showing that the throughput is SI, we now determine the throughput. Since throughput is SI, it is the same as the mean value, averaged over all possible delay offsets. When the K users are all active and the duty factor of user i is f_i, for $i = 1, \ldots, K$, the throughput of user i is given by

$$f_i \prod_{j \neq i} \big(1 - f_j\big). \quad (2)$$

A detailed proof can be found in [11].

B. Lower Bound on Period

We have seen that SI sequences achieve zero variance in throughput. However, the cost for this is the exponential growth of period as a function of the number of users.

Theorem 2. *Let the duty factors of K shift-invariant sequences be n_i/d_i, for $i = 1, 2, \ldots, K$, such that n_i and d_i*

are relatively prime for all i. Then the common period of the sequence set is divisible by $d_1 d_2 \cdots d_K$.

Proof: Suppose that p is a prime number that divides $\prod_{i=1}^{K} d_i$. By re-labeling the users, we assume without loss of generality that d_1, $d_2, \ldots, d_j$ are all divisible by p, but $d_{j+1}, \ldots d_K$ are not divisible by p. Let p^e be the largest power of p that divides $\prod_{i=1}^{j} d_i$.

Consider the Hamming crosscorrelation associated with $\mathsf{A} = (1, 2, \ldots, j)$. By the SI assumption, $H(\tau_1, \ldots, \tau_j; \mathsf{A})$ is identically equal to an integer h for all τ_i's. After summing over all $\tau_1, \ldots, \tau_j$, we get

$$\sum_{\tau_1=0}^{L-1} \cdots \sum_{\tau_j=0}^{L-1} H(\tau_1, \ldots, \tau_j; \mathsf{A}) = L^j h. \tag{3}$$

On the other hand, by the definition of Hamming crosscorrelation, we have

$$\sum_{\tau_1=0}^{L-1} \cdot \cdot \sum_{\tau_j=0}^{L-1} H(\tau_1, \ldots, \tau_j; \mathsf{A}) = \sum_{\tau_1=0}^{L-1} \cdot \cdot \sum_{\tau_j=0}^{L-1} \sum_{t=0}^{L-1} \prod_{i=1}^{j} s_i(t + \tau_i).$$

Exchange the order of summation,

$$\sum_{t=0}^{L-1} \prod_{i=1}^{j} \sum_{\tau_i=0}^{L-1} s_i(t + \tau_i) = L \prod_{i=1}^{j} \frac{L n_i}{d_i}. \tag{4}$$

Here, Ln_i/d_i is the Hamming weight of the i-th sequence. From (3) and (4), we have $h \prod_{i=1}^{j} d_i = L \prod_{i=1}^{j} n_i$. Since h is an integer, we see that $L \prod_{i=1}^{j} n_i$ is divisible by $\prod_{i=1}^{j} d_i$, and hence is also divisible by p^e. However, for $i = 1, 2, \ldots, j$, n_i/d_i is a reduced fraction, and consequently $\prod_{i=1}^{j} n_i$ is not divisible by p. Therefore L must be divisible by p^e.

Since the above argument is valid for all prime factors of $\prod_{i=1}^{K} d_i$, we conclude that L is divisible by $\prod_{i=1}^{K} d_i$. ■

Theorem 2 has the following important corollary: the period of SI sequence set is at least K^K when the duty factors of the K users are all $1/K$.

C. An Optimal Construction for SI Sequences

The period of the generated sequences by the following construction is optimal in the sense that it achieves the lower bound in Theorem 2.

Construction: Suppose that, for $j = 1, \ldots, K$, the duty factor of the j-th sequence to be constructed is a reduced fraction n_j/d_j. The least period of the j-th is the product $\prod_{i=1}^{j} d_i$. To generate the j-th sequence, we construct an $\prod_{i=1}^{j-1} d_i$ by d_j zero-one matrix, with exactly n_i ones in each row. The j-th sequence is obtained by "interleaving", i.e., reading out the columns from left to right. We illustrate the procedure by constructing the sequences in Example 1.

In Example 1, the duty factors are 1/2, 1/3 and 2/3. The first sequence has least period 2 and is obtained by extending $[0\ 1]$ periodically. The second sequence has least period 6. We construct the following 2×3 matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

The duty factor condition implies that each row must contain exactly one "1". By writing down the first, second and third column one by one, we have $[1\ 0\ 0\ 1\ 0\ 0]$, which can be periodically extended to $\mathbf{s}_2$ in Example 1. The third sequence is generated from the 6×3 matrix which has $[1\ 1\ 0]$ in each of the six rows. The proof that the sequence set so generated is SI can be found in [11].

III. User-Irrepressible Sequences

A sequence set is called *user-irrepressible* (UI) if for all j between 1 and K, the individual throughput $\theta_j(\tau_1, \ldots, \tau_K; (1, 2, \ldots, K))$ is strictly positive for all possible delay offsets, i.e., in the worst case, at least one successfully sent packet for each user in each period is guaranteed. A set of UI sequences has the favorable property of bounded delay, namely, each user needs not wait for longer than the duration of one period before a packet can be sent without collision. We remark that a SI sequence set, unless the all-zero or the all-one sequence are included, is user-irrepressible. This can be seen by observing the throughput calculated in (2) is a positive constant. However, the SI sequences have the drawback that the period grows exponentially in the number of users. In order to minimize delay, our objective is to design UI sequences with period as short as possible.

If K users are active simultaneously, each user must transmit at least K packets in a period in order to avoid complete blockage by others. Otherwise, if a user, say user K, transmits only $K-1$ packets in a period, we can arrange the delay offsets of users 1 to $K-1$, so that the j-th packet of user K in a period collides with a packet from the j-th user, for $1 = 2, \ldots, K-1$. Then the throughput of user K will drop to zero. In this paper, we restrict out attention to the case where each user transmits exactly K packets in a period, and assume that the Hamming weight of each sequence is exactly K. The sequence that satisfies this requirement has the additional property that it is the most energy-efficient while user irrepressibility is maintained.

The following is a running example that we shall refer to continually.

Example 2: $\mathbf{s}_1$, $\mathbf{s}_2$ and $\mathbf{s}_3$ form a set of three UI sequences:

$$\mathbf{s}_1 = [1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0]$$
$$\mathbf{s}_2 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0]$$
$$\mathbf{s}_3 = [1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0].$$

We can verify that no matter how we cyclically shift the three sequences, each user can send out at least one packet successfully in a period.

A sequence will be represented in a compact way by specifying the *characteristic set* of a sequence, which is the set of locations of the K ones in a period. For example, the characteristic sets of the three sequences in Example 2 are respectively, $\mathcal{I}_1 := \{0, 6, 9\}$, $\mathcal{I}_2 := \{0, 4, 8\}$, $\mathcal{I}_3 := \{0, 1, 2\}$. Cyclic shift of a sequence by τ is equivalent to adding τ modulo L to the corresponding characteristic set.

A. An Equivalent Condition for User Irrepressibility

A necessary and sufficient condition for K sequences, each of Hamming weight K, being user-irrepressible is that the

pairwise Hamming crosscorrelation is either 0 or 1, for all pairs of distinct sequences, i.e., $H(\tau_1, \tau_2; (i, j)) \leq 1$ for all i, j such that $1 \leq i < j \leq K$. Suppose, on the contrary, that the pairwise Hamming crosscorrelation between user 1 and 2 is larger than or equal to 2. Then there are at least 2 packets of user 1 are in collision. There are at most $K-2$ remaining packets, which can be completely blocked by users 2 to K if the delay offsets are chosen appropriately.

This motivates the following notation: *set of differences*. Let $\mathbb{Z}_L$ be the additive group of residues modulo L. For a subset $\mathcal{S}$ of $\mathbb{Z}_L$, we let $d(\mathcal{S}) := \{a_1 - a_2 : a_1, a_2 \in S\}$, and call it the set of differences in $\mathcal{S}$. If $\delta \in d(\mathcal{S})$ occurs as difference of two distinct pairs of elements in $\mathcal{S}$, it is only counted once; multiplicity is irrelevant. Since zero is always in $d(\mathcal{S})$ for any subset $\mathcal{S}$, we will consider $d^*(\mathcal{S}) := d(\mathcal{S}) \backslash \{0\}$, the differences between pairs of distinct elements in $\mathcal{S}$.

We have the following equivalent condition for user irrepressibility.

Theorem 3. *Let $\mathcal{I}_j$, $j = 1, 2, \ldots, K$, be the characteristic sets of K sequences of period L, such that $\mathcal{I}_j$ contains exactly K elements in $\mathbb{Z}_L$ for all j. The corresponding sequence set is user-irrepressible iff for all pairs of distinct i and j, $d^*(\mathcal{I}_i)$ and $d^*(\mathcal{I}_j)$ are disjoint.*

B. A Lower Bound on Period

For $j = 1, \ldots, K$, let $\mathcal{I}_j$ be the characteristic set of the j-th sequence. From Theorem 3, we see that the number of nonzero elements in $\mathbb{Z}_L$ must be at least $\sum_{j=1}^{K} |d^*(\mathcal{I}_j)|$, where $|\cdot|$ denotes the cardinality of a set. A lower bound on sequence period can be obtained by lower bounding the size of $d^*(\mathcal{I}_j)$. This is done by appealing to a theorem in additive number theory, called Kneser's theorem. We state a version of Kneser's theorem, which is tailored to what we need here. A proof of Kneser's theorem can be found in [12].

Theorem 4 (Kneser [13])**.** *If a subset $\mathcal{I}$ in $\mathbb{Z}_L$ satisfies*

$$|d^*(\mathcal{I})| < 2|\mathcal{I}| - 2,$$

then there exists a proper divisor α of L such that

$$d^*(\mathcal{I}) \supseteq \{k\alpha : k = 1, 2, \ldots, (L/\alpha) - 1\},$$

i.e., $d^*(\mathcal{I})$ contains all multiples of α.

As an illustration of Theorem 4, consider the three characteristic sets $\mathcal{I}_1$, $\mathcal{I}_2$ and $\mathcal{I}_3$ in Example 2. We have $d^*(\mathcal{I}_1) = \{3, 6, 9\}$ and $|d^*(\mathcal{I}_1)| < 2|\mathcal{I}_1| - 2 = 4$. By Theorem 4, $d^*(\mathcal{I})$ must contain the multiples of a proper divisor of $L = 12$. Indeed, $d^*(\mathcal{I})$ consists of the multiples of 3, which is a proper divisor of 12. For $\mathcal{I}_2$, it satisfies $|d^*(\mathcal{I}_2)| = |\{4, 8\}| < 2|\mathcal{I}_2| - 2 = 4$. We can again verify Theorem 4 by observing that the elements in $d^*(\mathcal{I}_2)$ are precisely the multiples of 4. For $\mathcal{I}_3$, we have $|d^*(\mathcal{I}_3)| = |\{1, 2, 10, 11\}| = 2|\mathcal{I}_3| - 2 = 4$. The condition in Theorem 4 is not satisfied.

Theorem 5. *For a set of K user-irrepressible sequences, in which every sequence has Hamming weight K, then we have*

$$L \geq 1 + (K - \omega(L))(2K - 2), \tag{5}$$

where $\omega(L)$ denotes the number of distinct prime divisors of L.

Proof: In view of Kneser's theorem, we classify the sequences into two types. We say that a sequence is in *class 1* if the associated set of differences contains the multiples of a proper divisor of L, otherwise, we say that it is in *class 2*.

Suppose that we have two sequences in class 1, whose sets of differences contain multiples of α and multiples of β respectively. We claim that L/α and L/β must be relatively prime. Suppose on the contrary that the greatest common divisor of L/α and L/β, denoted by g, is larger than 1. Since g divides L/α, we can find an integer x such that $gx = L/\alpha$. Hence, we have $\alpha x = L/g$ and thus L/g is a multiple of α. By similar argument, we can find another integer y such that $gy = L/\beta$, and conclude that L/g is a multiple of β. So, L/g is contained in two sets of differences associated with two distinct sequences. However, the UI assumption implies that the two sets of differences can only have zero as the common element. This contradiction completes the proof of the claim.

If there are m sequences in class 1, then there are m proper divisors of L, namely $\alpha_1, \ldots, \alpha_m$, such that $L/\alpha_1, \ldots, L/\alpha_m$ are mutually relatively prime. The largest set of mutually relative prime divisors of L is the set of distinct prime divisors of L, which has cardinality $\omega(L)$ by definition. We thus have m less than or equal to $\omega(L)$.

The above argument implies that there are no more than $K - \omega(L)$ sequences in class 2. By the UI assumption, the sets of differences associated with the sequences in class 2 are mutually disjoint sets of nonzero elements in $\mathbb{Z}_L$. Ignoring the sequences in class 1, we have $L - 1 \geq \sum_{\mathcal{I} \text{ in class } 2} |d^*(\mathcal{I})|$, with the summation running over all sequences in class 2. By Theorem 4, each summand is larger than or equal to $2K - 2$. Therefore, $L - 1 \geq (K - \omega(L))(2K - 2)$. ■

We will use the inequality $\log_2(L) \geq \omega(L)$, which holds for all positive integers L, and replace $\omega(L)$ by $\log_2(L)$ in (5). We obtain

$$L \geq 1 + (K - \log_2(L))(2K - 2). \tag{6}$$

For a given integer K larger than 1, let L_K be the smallest L such that (6) is satisfied. It yields a lower bound for the period of a set of K UI sequences with Hamming weight K.

We have the following asymptotic version of Theorem 5.

Theorem 6. *Given an arbitrarily small $\epsilon > 0$,*

$$L_K \geq 1 + 2(1 - \epsilon)K(K - 1) \tag{7}$$

for all $K \geq C(\epsilon)$, where $C(\epsilon)$ is a constant that depends on ϵ. Hence, $\liminf_{K \to \infty} L_K/(2K^2) \geq 1$.

Proof: Suppose that ϵ and K are given and fixed. We consider two cases: (1) $L > 2^{\epsilon K}$ and (2) $L \leq 2^{\epsilon K}$. In the second case, we replace $\log_2(L)$ by ϵK in (6),

$$L \geq 1 + (K - \epsilon K)(2K - 2) = 1 + 2(1 - \epsilon)K(K - 1).$$

Therefore, every integer L that satisfies (6) must be larger than or equal to the minimum of $2^{\epsilon K}$ and $1 + 2(1 - \epsilon)K(K - 1)$,

$$L_K \geq \min\{2^{\epsilon K}, 1 + 2(1 - \epsilon)K(K - 1)\}.$$

Let $C(\epsilon)$ be the smallest value of K such that

$$2^{\epsilon K} \geq 1 + 2(1-\epsilon)K(K-1).$$

The constant $C(\epsilon)$ certainly exists because $2^{\epsilon K}$ increases exponentially in K but $2(1-\epsilon)K(K-1) = O(K^2)$. The inequality in (7) holds for for all $K \geq C(\epsilon)$. The result about $\liminf$ of L_K follows directly from (7). ■

C. An Asymptotically Optimal Construction

Theorem 6 asserts that the period of a set of K UI sequences with Hamming weight K is lower bounded by approximately $2K^2$ when K is large. In the remainder of this section we will give a construction that achieves this lower bound asymptotically.

Theorem 7. *Let Φ_K be the shortest period among all sets of K UI sequences, each with Hamming weight K. Then*

$$\liminf_{K\to\infty} \Phi_K/(2K^2) = 1.$$

The construction is based on Chinese remainder theorem. The mapping $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \oplus \mathbb{Z}_q$ defined by $f(a) := (a \bmod p, a \bmod q)$ is a bijection from $\mathbb{Z}_{pq}$ to $\mathbb{Z}_p \oplus \mathbb{Z}_q$ when p and q are relatively prime [14], and preserves addition and multiplication by integers. When the period of a sequence is in the form of pq, with p and q relatively prime, the characteristic set can be mapped to a subset of $\mathbb{Z}_p \oplus \mathbb{Z}_q$, which consists of ordered pairs in the form (x, y) with $0 \leq x < p$ and $0 \leq y < q$. We will construct sequences by specifying characteristic sets in $\mathbb{Z}_p \oplus \mathbb{Z}_q$.

Construction: Given K, we set q to be $2K-1$, and p the smallest prime larger than or equal to K and relatively prime to $2K-1$. For $j = 0, 1, \ldots, K-1$, we let

$$\mathcal{I}'_j := \{(jy \bmod p, y) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2K-1} : y = 0, 1, \ldots, K-1\}$$

and obtain the characteristic sets of the sequences, $\mathcal{I}_j$, by taking the inverse image $f^{-1}(\mathcal{I}'_j)$ for $j = 0, \ldots, K-1$.

Since f is a bijection, we have $|\mathcal{I}_j| = K$ for all j, and the Hamming weight of each constructed sequence is K. To show that the resulting sequences are UI, we define $d^*(\mathcal{I}'_j)$ in the same way as $d^*(\mathcal{I}_j)$, but with the addition and subtraction done in $\mathbb{Z}_p \oplus \mathbb{Z}_{2K-1}$ instead of $\mathbb{Z}_{p(2K-1)}$. UI holds if $d^*(\mathcal{I}'_0)$, $d^*(\mathcal{I}'_1), \ldots, d^*(\mathcal{I}'_{K-1})$ are mutually disjoint. Suppose for the sake of contradiction that, we can find two distinct α and β in $\{0, 1, \ldots, K-1\}$ such that $d^*(\mathcal{I}'_\alpha)$ and $d^*(\mathcal{I}'_\beta)$ share a common element. Then

$$(\alpha y'_1, y'_1) - (\alpha y_1, y_1) = (\beta y'_2, y'_2) - (\beta y_2, y_2)$$

for some $y'_1 \neq y_1$ and $y'_2 \neq y_2$. By equating the second components on both sides, we see that $y'_1 - y_1 = y'_2 - y_2 \bmod 2K-1$. Since the range of y_1, y'_1, y_2 and y'_2 is between 0 and $K-1$, we must have $y'_1 - y_1 = y'_2 - y_2$. From the first component, we obtain $(\alpha - \beta)(y'_1 - y_1) \equiv 0 \bmod p$, which implies that $y'_1 = y_1$. This contradicts the assumption that $y'_1 \neq y_1$.

In order to show the asymptotic result in Theorem 6, we consider the sequence of prime numbers $p_1, p_2, \ldots$, and let $q_\ell = 2p_\ell - 1$ for $\ell = 1, 2, \ldots$. It is clear that p_ℓ and q_ℓ are relatively prime. So, we obtain a sequence of UI sequence sets. The ℓ-th sequence set comprises p_ℓ sequences of period $p_\ell(2p_\ell - 1)$ and Hamming weight p_ℓ. This sequence of UI sequence sets shows that the asymptotic lower bound in Theorem 6 is tight. This proves Theorem 7.

IV. Concluding Remarks

Two extreme ends in the design of protocol sequences are investigated. We proved that the shortest UI sequences studied in this paper have period $2K^2$, where K is the number of users. In the worst case, there is only one successful packet per user in a period; the worst-case individual throughput decays as $1/(2K^2)$. On the other hand, SI sequences have good and stable performance measure in terms of throughput; when the duty factor of every user is $1/K$, the worst-case individual throughput is around e^{-1}/K, yet the period grows like K^K. There is clearly a tradeoff between period length and worst-case throughput. Sequence sets that lie between these two extreme cases are of interests. One such construction, called wobbling sequences, is studied in [6]. The wobbling sequences are of period $O(K^4)$ with worst-case individual throughput lower bounded by $0.25/K$. The optimal tradeoff between period and worst-case throughput is an interesting direction for further studies.

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] 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.

[3] V. C. da Rocha, Jr., "Protocol sequences for collision channel without feedback," *IEE Electron. Lett.*, vol. 36, no. 24, pp. 2010–2012, Nov. 2000.

[4] U. Roedig, A. Barroso, and C. J. Sreenan, "f-MAC: A deterministic media access control protocol without time synchronization," in *3rd European Workshop on Wireless Sensor Networks*, ser. Lecture Notes in Computer Science, K. Römer, H. Karl, and F. Mattern, Eds., no. 3868. Berlin: Springer-Verlag, 2006, pp. 276–291.

[5] A. A. Shaar and P. A. Davies, "Prime sequences: quasi-optimal sequences for OR channel code division multiplexing," *IEE Electron. Lett.*, vol. 19, no. 21, pp. 888–890, Oct. 1983.

[6] 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.

[7] K. Momihara, M. Müller, J. Satoh, and M. Jimbo, "Constant weight conflict-avoiding codes," *SIAM J. Discrete Math.*, vol. 21, no. 4, pp. 959–979, 2007.

[8] M. Jimbo, M. Mishima, S. Janiszewski, A. Y. Teymorian, and V. D. Tonchev, "On conflict-avoiding codes of length $n = 4m$ for three active users," *IEEE Trans. Inform. Theory*, vol. 53, pp. 2732–2742, Aug. 2007.

[9] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Trans. Inform. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.

[10] N. Q. A, 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.

[11] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invariant protocol sequences for the collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 55, Jul. 2009.

[12] H. B. Mann, *Addition Theorems: the Addition Theorems of Group Theory and Number Theory*. New York: Interscience Publisher, 1965.

[13] M. Kneser, "Abschätzungen der asymptotischen dichte von summenmengen," *Math. Zeit.*, vol. 58, pp. 459–484, 1953.

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