Completely Irrepressible Sequences for the Asynchronous Collision Channel Without Feedback

Yijin Zhang, Kenneth W. Shum and Wing Shing Wong

***Abstract*— A collision channel is asynchronous if it is neither frame nor slot synchronized. We consider protocol sequences with the property that each user is able to send at least one packet successfully in each sequence period, for the asynchronous collision channel without feedback. Such property is called user irrepressibility in the asynchronous channel. In this paper, we focus on the class of the most energy-efficient completely irrepressible protocol sequence set. We derive lower bounds on the minimum period and present a construction method that meets the asymptotic bound of equi-difference sequence set.**

I. Introduction

A. Background and Motivation

Consider a wireless sensor network [1] with M users and one data sink. The channel is divided into time slots of equal duration. We model the system by a collision channel without feedback [2]. Since there is no central coordination and no feedback from the data sink, we cannot do packet scheduling for media access control. Another option is a random transmission scheme like ALOHA [3] [4], where each user send a packet in a time slot with certain probability, independent of what it did in previous time slots, and independent from the other users. However, implementing a random number generator is sometimes too costly for users, which are both power and complexity limited. As we do not assume that the users are equipped with any receiver, contention based protocols, which require listening to the channel, is not feasible. In both random transmission and contention based protocol, there is no guarantee on transmission delay in the worst case.

To investigate the transmission scheme with strict guarantee of zero blocking probability within one period, we will follow the approach in [2], and specify the transmission pattern by a deterministic periodic sequence, called a *protocol sequence*. The components of the protocol sequence are either zero or one. Each user is assigned a protocol sequence, and reads off the components one by one periodically. It transmits a packet of one time slot duration if it is one, and keeps silent for one time slot if it is zero. Suppose that the minimum common period of assigned M protocol sequences is L slots time. For $i = 1, 2, \dots, M$, the protocol sequence associated with user i is specified by a row vector $s_i := \big[s_i[0]\ s_i[1]\ \dots\ s_i[L-1]\big]$. The n-th component of user i's protocol sequence is equal to $s_i[n \mod L]$ for any non-negative integer n. Without loss of generality, $s_i[0]$ here is assumed to be 1 for all i.

As there is no feedback from the receiver and no cooperation among the users, the channel is not frame-synchronized, i.e., there is no guaranteed that the protocol sequence will start at the same time slot. Each user has a delay offset, which is random but remains fixed throughout the communication session. Let δ_i be the time offset of user i for $i = 1, 2, \dots, M$, on the unit of one time slot duration. It can be interpreted as the difference between the time shown on the receiver's clock and the time shown on user i's clock. In this paper, all time indices and time intervals mentioned are both on the receiver's clock and on the unit of one time slot duration. Thus user i would start its protocol sequence or transmission scheme at the time index δ_i. Then if the assigned sequence of user i is equal to 1 at its n_0-th component for some non-negative integer n_0, user i will make its packet transmission at time interval $[n_0 + \delta_i, n_0 + \delta_i + 1)$. Furthermore by distinguishing two cases for the possible values of the unknown time offsets, there are two different models of synchronization:

1) The channel is slot-synchronized if all users know the slot boundaries of the channel, i.e., the time offsets $\delta_1, \delta_2, \dots, \delta_M$ are arbitrary integers.
2) The channel is asynchronous if it is neither frame nor slot synchronized. In this model, all users do not know the slot boundaries of the channel. It implies the time offsets $\delta_1, \delta_2, \dots, \delta_M$ are arbitrary real numbers.

Thus, if all users start their packet transmissions at an integral time index, collisions will result only when received packets completely overlap. In the asynchronous case, however, the users have no way to avoid collisions that result from partial overlapping of packets. We further assume one packet in the asynchronous channel is received correctly without suffering any collision and is unrecoverable when collided. In other words, a packet is assumed to be successful if and only if it is not completely or partially overlapped by any other packet. For the asynchronous channel, some studies were made in [5] by using RS coding for recovery from tail-end collisions. However, this more general scenario is not considered in this paper.

For some sensor network applications, the required minimum number of successful packets by each user within one period may be low, however, it is important to ensure that all users can successfully transmit information at least once in a period L time slots. We call such a property *user irrepressibility* [6]. Considering user irrepressibility in the slot-synchronized channel, we say that a protocol sequence set

This work was partially supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 417909.

Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N. T., Hong Kong. Emails: zyj007@ie.cuhk.edu.hk, kshum2009@gmail.com, wswong@ie.cuhk.edu.hk.

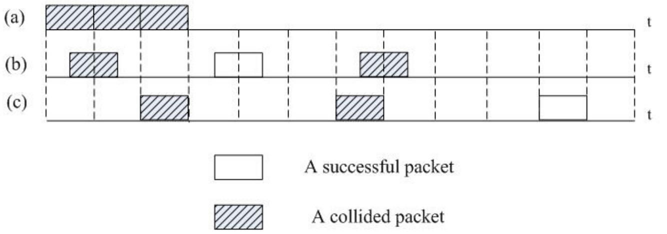

Fig. 1. (a) Packets from user 1, (b) packets from user 2, (c) packets from user 3.

is *user-irrepressible* (UI) if each user can send out at least one packet successfully in each L slots, no matter what the integer-delay offsets are. It guarantees that each user can transmit a message within L time slots delay in the worst case in the slot-synchronized channel. UI sequence sets have been studied extensively in [6]–[10] and is also addressed in another context, under the name of *conflict-avoiding codes* (CAC) (see e.g [11]–[14] and the references therein) with different perspective. However, one can check all known UI sequence sets cannot guarantee the user irrepressibility for the asynchronous channel if some delay shifts are non-integer numbers, from the following example.

Example 1: s_1, s_2 and s_3 form a UI sequence set:

$$s_1 = [1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$$
$$s_2 = [1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]$$
$$s_3 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0].$$

In the asynchronous channel, for $\delta_1 = 0$, $\delta_2 = 0.5$ and $\delta_3 = 2$, as illustrated in Fig. 1, we can find all packets from user 1 are lost due to two partial overlapping collisions and one completely overlapping collision.

In this paper, we consider the user irrepressibility in the asynchronous channel. More strictly, a protocol sequence set with period L is said to be *completely irrepressible* (CI) if user i can send out at least one packet successfully in each time interval $[\delta_i + k, \delta_i + k + L)$ with any non-negative integer k for any $\delta_1, \delta_2, \ldots, \delta_M$ and any $i \in \{1, 2, \ldots, M\}$. Obviously, given M, the collection of all CI sequence sets is a subset of the collection of all UI sequence sets. It is because that the collection of all possible time offsets in the slot-synchronized channel is just a subset of that in the asynchronous channel. In other words, a CI sequence set must be UI.

B. Notations

If x is a real number, the notation $\lfloor x \rfloor$ represents the largest integer less than or equal to x. The smallest integer larger than or equal to x is denoted by $\lceil x \rceil$. We use $|\cdot|$ to denote the cardinality of a set.

Given a binary sequence $s := \big[s[0]\ s[1]\ \ldots\ s[L-1]\big]$, we define its *Hamming weight* as

$$w(s) := \sum_{n=0}^{L-1} s[n].$$

We say the one at position n of s is *unblocked* in a given sequence set if the n-th bit of other sequences are all equal to zero. Otherwise, it is *blocked*. If all ones in s are blocked, we say sequence s is blocked. Otherwise, s is unblocked.

Given that the delay offset of s is an integer τ. The *cyclic shift* of s by τ is denoted by

$$s^{[\tau]} := \big[s[0-\tau]\ s[1-\tau]\ \ldots\ s[L-1-\tau]\big].$$

The substraction $n - \tau$ is performed modulo L for $n = 0, 1, \ldots, L-1$.

Define $f_s(t)$ as a protocol signal *generated* by s with

$$f_s(t) := s\big[\lfloor t \rfloor\big]$$

for all $t \in [0, L)$.

Given two sequences s_1 and s_2, define the *asynchronous Hamming crosscorrelation* of f_{s_1} and f_{s_2} by

$$h_{f_{s_1} f_{s_2}}(\delta) := \int_0^L f_{s_1}(t) f_{s_2}(t-\delta)\ dt.$$

The substraction $t - \delta$ is performed modulo L. When δ is an integral number τ, it reduces to the usual notion of *Hamming crosscorrelation* and can be written by

$$H_{s_1 s_2}[\tau] := \sum_{n=0}^{L-1} s_1[n] s_2[n-\tau].$$

A sequence can also be represented in a compact way by specifying the *characteristic set* of a sequence, which is defined as the set of all time indices in a period where the value of the protocol sequence is equal to 1. For a sequence s, its characteristic set can be written as

$$\mathcal{I}_s := \{a_1, a_2, \ldots, a_{w(s)}\}.$$

Cyclic shift of a sequence by integer τ is equivalent to adding τ modulo L to the corresponding characteristic set. For Example 1, the characteristic sets of s_3 and ${s_3}^{[2]}$ are respectively $\mathcal{I}_{s_3} = \{0, 4, 8\}$ and $\mathcal{I}_{s_3^{[2]}} = \{2, 6, 10\}$.

Let $\mathbb{Z}_L$ be the additive group of residues modulo L. For a subset $\mathcal{S}$ of $\mathbb{Z}_L$, we let $d(\mathcal{S}) := \{a_i - a_j : a_i, a_j \in \mathcal{S}\}$, and call it the set of differences in $\mathcal{S}$. Since zero is always in $d(\mathcal{S})$ for any subset $\mathcal{S}$, we will consider $d^*(\mathcal{S}) := d(\mathcal{S}) \setminus \{0\}$, the differences between pairs of distinct elements in $\mathcal{S}$.

A sequence s is called *equi-difference* if the elements in $\mathcal{I}_s$ form an arithmetic progression in $\mathbb{Z}_L$, i.e.,

$$\mathcal{I}_s = \{0, g, 2g, \ldots, \big(w(s)-1\big)g\}$$

for some $g \in \mathbb{Z}_L$. In the above equation, the product jg is reduced mod L, for $j = 1, 2, \ldots, w(s) - 1$. The element g or $L - g$ is called a *generator* or *common difference* of this sequence. For an equi-difference sequence generated by g or $L - g$, the set of differences is equal to

$$d(\mathcal{I}_s) = \{0, \pm g, \pm 2g, \ldots, \pm\big(w(s)-1\big)g\}.$$

If each sequence in a sequence set is equi-difference, this sequence set is said to be an equi-difference sequence set. Given two equi-difference sequences s_1 and s_2 with $w(s_1)g_1 \neq 0 \mod L$ and $w(s_2)g_2 \neq 0 \mod L$, we say they are *distinct* if we have

$$g_1 \neq g_2 \text{ or } L - g_2.$$

Example 1 continued: We have $d^*(\mathcal{I}_{s_1}) = \{1, 2, 10, 11\}$, $d^*(\mathcal{I}_{s_2}) = \{3, 6, 9\}$ and $d^*(\mathcal{I}_{s_3}) = \{4, 8\}$. Thus, the sequence set is equi-difference and has three distinct sequences.

C. Preliminaries

We have the following property for asynchronous Hamming crosscorrelation considering all $\delta \in [0, L)$.

Proposition 1. *Given two binary sequences s_1 and s_2, both with period L, we have*

$$\int_0^L h_{f_{s_1} f_{s_2}}(\delta)\ d\delta = w(s_1)w(s_2).$$

Proof:

$$\begin{aligned}\int_0^L h_{f_{s_1} f_{s_2}}(\delta)\ d\delta &= \int_0^L \int_0^L f_{s_1}(t) f_{s_2}(t-\delta)\ dtd\delta \\ &= \int_0^L f_{s_1}(t) \int_0^L f_{s_2}(t-\delta)\ dtd\delta \\ &= \int_0^L f_{s_1}(t) \int_0^L f_{s_2}(\delta)\ dtd\delta \\ &= \int_0^L f_{s_1}(t) w(s_2)\ dt = w(s_1)w(s_2).\end{aligned}$$

■

When just considering all integer δ at $[0, L)$, the result in Proposition 1 reduces to the below elementary property of Hamming crosscorrelation due to [15].

Proposition 2 ([15]). *Given two binary sequences s_1 and s_2, both with period L, we have*

$$\sum_{\tau=0}^{L-1} H_{s_1 s_2}[\tau] = w(s_1)w(s_2).$$

The following proposition provides a lower bound of Hamming weight of each sequence in any CI sequence set.

Proposition 3. *If a sequence set $\{s_1, s_2, \ldots, s_M\}$ is CI, then we have $w(s_i) \geq M$ for $i = 1, 2, \ldots, M$.*

Proof: We will prove the claim by contradiction. Suppose $w(s_i) < M$ for some i. Then we can arrange the delay offsets of other $M - 1$ sequences, so that the i-th one of user i in a period is blocked by a one from s_j, for $j = 1, \ldots, j \neq i, \ldots, M$. Then the sequence s_i is blocked and the number of successful packets from s_i will drop to zero, which contradicts the definition of CI sequence set. Thus, we obtain $w(s_i) \geq M$ for $i = 1, 2, \ldots, M$. ■

Then from the construction presented in section IV, for any M, we can see there exists a CI sequence set of M sequences, each with Hamming weight M. Thus we find the lower bound in Proposition 3 can be achieved for any M. In order to enhance battery life of sensor network, we want to design CI protocol sequence set with the number of packets sent in each period as small as possible. Thus we say a CI sequence set of M sequences is *the most energy-efficient CI* (ECI) if the Hamming weight of each sequence is M. We use $\mathsf{ECIS}(L, M)$ to denote a ECI sequence set of M sequences with period L. Specially we denote an equi-difference $\mathsf{ECIS}(L, M)$ by $\mathsf{ECIS}^e(L, M)$.

D. Main Results

In order to minimize the transmission delay or latency in the worst case, the objective in this paper is to construct ECI protocol sequence set with period as small as possible. Furthermore, to investigate the shortest latency that we can achieve, we are interesting in $L_{\min}(M)$, the smallest period L such that a $\mathsf{ECIS}(L, M)$ exists.

Equi-difference sequence set is an important class of protocol sequence sets with user irrepressibility. Some bounds and constructions of equi-difference UI sequence set have been investigated in [13] and [14]. Thus we also focus on $L^e_{\min}(M)$, the smallest period L such that a $\mathsf{ECIS}^e(L, M)$ exists.

This paper is organized as follows. After proving several important properties of CI sequence set in Section II, we establish a lower bound on $L_{\min}(M)$ and an asymptotic lower bound on $L^e_{\min}(M)$ in Section III. Then a construction that meets the asymptotic bound on $L^e_{\min}(M)$ is presented in Section IV. Section V gives a comparison with random accessing scheme in terms of blocking probability and period. Finally, we close in Section VI with some concluding remarks.

II. Properties of Completely Irrepressible Sequence Set

In our channel model, if user i starts its packet transmission at time index $k_0 + \delta_i$ for some non-negative integer k_0, this packet is successfully received if and only if no any other user would start or end its transmission at interval $[k_0 + \delta_i, k_0 + \delta_i + 1)$. For studying the individual successful transmission amount in the asynchronous channel to see whether a protocol sequence set is CI or not, we present the following result by generalizing the observation in [2]. δ_{max} is used to denote the maximum value of δ_i for $i = 1, 2, \ldots, M$. Given a sequence s, we construct s' as:

$$s'[n] := \begin{cases} 1 & \text{if } s[n-1] = 1 \text{ and } n \geq 1; \\ s[n] & \text{otherwise.} \end{cases}$$

Given $s_1, s_2, \ldots, s_M$ and $\delta_1, \delta_2, \ldots, \delta_M$, the sequence set $T_i = \{s_{i\_1}, s_{i\_2}, \ldots, s_{i\_M}\}$ for $i = 1, 2, \ldots, M$, is constructed as the following rule:

(i) For any $j \in \{1, 2, \ldots, M\}$ such that $\lfloor \delta_j - \delta_i \rfloor \neq \delta_j - \delta_i$, we set $s_{i\_j} = s_j'^{[\lfloor \delta_j - \delta_i \rfloor]}$;

(ii) Otherwise, we set $s_{i\_j} = s_j^{[\lfloor \delta_j - \delta_i \rfloor]}$.

Proposition 4.

(i) In each interval $[\delta_i + k, \delta_i + k + L)$ for any non-negative integer k such that $\delta_i + k \geq \delta_{max}$, the resulting number of successful packets from user i is exactly equal to the number of unblocked ones of s_{i_i} in T_i.

(ii) In each interval $[\delta_i + k, \delta_i + k + L)$ for any non-negative integer k such that $\delta_i + k < \delta_{max}$, the resulting number of successful packets from user i is larger than or equal to the number of unblocked ones of s_{i_i} in T_i.

Proof of Proposition 4 is presented in Appendix A. It is different from the argument in [2]. Furthermore, the following equivalent condition for user irrepressibility in the asynchronous channel just directly follows Proposition 4.

Theorem 5. *A sequence set $\{s_1, s_2, \dots, s_M\}$ is CI iff s_{i_i} is unblocked in T_i for any $\delta_1, \delta_2, \dots, \delta_M$ and any $i \in \{1, 2, \dots, M\}$.*

As an example, consider the protocol sequence set in Example 1 with the time offset $(\delta_1 = 0.5, \delta_2 = 1, \delta_3 = 2.5)$ in the asynchronous channel. To obtain the number of successful slots from user 1, we find T_1 as

$$\begin{aligned} s_{1\_1} &= [1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0] \\ s_{1\_2} &= [1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0] \\ s_{1\_3} &= [0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0]. \end{aligned}$$

Obviously, we can check all ones of s_{1_1} are blocked in T_1. Thus we know this sequence set is not CI.

Following Proposition 4, we know that T_i is determined by i and δ_j for $j = 1, 2, \dots, M$. Thus for every distinct user, we have T_i may be different from T_j if $i \neq j$. For example, T_3 can be found as

$$\begin{aligned} s_{3\_1} &= [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1] \\ s_{3\_2} &= [0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1] \\ s_{3\_3} &= [1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0]. \end{aligned}$$

Then we have the following equivalent condition for the most energy-efficient user irrepressibility in the asynchronous channel.

Theorem 6. *A sequence set $\{s_1, s_2, \dots, s_M\}$ with $w(s_i) = M$ for $i = 1, 2, \dots, M$ is ECI iff we have $H_{s_i s'_j}[\tau] \leq 1$ for any integer τ and any pair of distinct i and j.*

Proof: We prove the "only if" part by contradiction. Suppose $H_{s_i s'_j}[\tau_0] > 1$ for some integer τ_0 and some j with $j \neq i$. Then by letting $\tau_0 < \delta_j - \delta_i < \tau_0 + 1$, we have $s_{i\_i} = s_i$ and $s_{i\_j} = s_j'^{[\tau_0]}$ in T_i. Thus we have at least two ones of s_{i_i} are blocked by s_{i_j}. Then from $w(s_{i\_i}) = w(s_i) = M$, we know there are at most $M - 2$ remaining ones in s_{i_i}. We can choose some delay offsets of other $M - 2$ sequences such that the remaining $M - 2$ ones are totally blocked in T_i. Thus we find s_{i_i} is blocked in T_i. Following Theorem 5, we further have $\{s_1, s_2, \dots, s_M\}$ is not CI, which contradicts the condition.

For the "if" part, we first have the following simple fact from the construction of s'_j:

$$H_{s_i s_j}\big[\lfloor \delta_j - \delta_i \rfloor\big] \leq H_{s_i s'_j}\big[\lfloor \delta_j - \delta_i \rfloor\big].$$

Then with the condition we find the number of unblocked ones of s_{i_i} in T_i for any i and any $\{\delta_1, \delta_2, \dots, \delta_M\}$ is lower bounded by one due to

$$\begin{aligned} \sum_{j=1, j\neq i}^{M} H_{s_{i\_i} s_{i\_j}}[0] &\leq \sum_{j=1, j\neq i}^{M} H_{s_i s'_j}\big[\lfloor \delta_j - \delta_i \rfloor\big] \\ &\leq M - 1. \end{aligned}$$

Thus we can conclude s_{i_i} is unblocked in T_i for any i and any $\{\delta_1, \delta_2, \dots, \delta_M\}$. It implies $\{s_1, s_2, \dots, s_M\}$ is thus CI following Theorem 5. It is also ECI as each sequence has Hamming wight M. ■

In the view of the difference sets, we have the following version of Theorem 6.

Theorem 7. *Let $\mathcal{I}_{s_j}$, $j = 1, 2, \dots, M$, be the characteristic sets of M sequences of period L, such that $\mathcal{I}_{s_j}$ contains exactly M elements in $\mathbb{Z}_L$ for all j. Let α_j be any element in $d^*(\mathcal{I}_{s_j})$ for $j = 1, 2, \dots, M$. The corresponding sequence set is ECI iff*

(i) $1, L-1 \notin d^*(\mathcal{I}_{s_j})$ for $j = 1, 2, \dots, M$;

(ii) $\alpha_i - \alpha_j \neq 0$ i.e., $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s_j})$ are disjoint for all pairs of distinct i and j;

(iii) $\alpha_i - \alpha_j \neq \pm 1$ for all pairs of distinct i and j.

Proof: Let us prove the "only if" part first.

(i) Suppose $1, L-1 \in d^*(\mathcal{I}_{s_i})$. We also have $1 \in d^*(\mathcal{I}_{s'_j})$ following the construction of s'_j. Then we can find some integer τ_0 such that $H_{s_i s'_j}[\tau_0] = 2$ as there is a common element 1 between $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s'_j})$. From Theorem 6, we know the sequence set is not CI contradicting the condition. We thus have $1, L-1 \notin d^*(\mathcal{I}_{s_j})$ for $j = 1, 2, \dots, M$.

(ii) Suppose $\alpha_i = \alpha_j$ for some distinct i and j. Then we have $H_{s_i s_j}[\tau_0] = 2$ for some integer τ_0. It implies $H_{s_i s'_j}[\tau_0] \geq 2$ which contradicts Theorem 6. Thus we have $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s_j})$ are disjoint for all pairs of distinct i and j.

(iii) If $\alpha_j \in d^*(\mathcal{I}_{s_j})$, we can find $\alpha_j \pm 1 \in d^*(\mathcal{I}_{s'_j})$ from the construction of s'_j. Suppose $\alpha_i - \alpha_j = 1$. Then we can find some integer-delay τ_0 such that $H_{s_i s'_j}[\tau_0] = 2$ as there is a common element $(\alpha_j + 1)$ between $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s'_j})$. Thus from Theorem 6 we know the sequence set is not CI contradicting the condition. By the same argument, $\alpha_i - \alpha_j = -1$ would also make the contradiction. Therefore, $\alpha_i - \alpha_j \neq \pm 1$ is a necessary condition here.

Next we will prove the "if" part.

With the conditions and the construction of s'_j, we must have $H_{s_i s'_j}[\tau] \leq 1$ for any integer τ and any pair of distinct i and j. Following Theorem 6, it suffices to show that the entire sequence set is ECI. ■

Remark: For the slot-synchronous channel, i.e., δ_i is an integer for all i, we have $s'_j = s_j$ for $j = 1, 2, \dots, M$. Thus the equivalent condition in Theorem 6 is reduced to $H_{s_i s_j}[\tau] \leq 1$ for any integer τ and any pair of distinct i and j. Furthermore, we have (ii) of Theorem 7 is an equivalent condition here.

III. Lower Bounds on $L_{\min}(M)$ and $L^e_{\min}(M)$

A. A Lower Bound on $L_{\min}(M)$

The following lower bound on $L_{\min}(M)$ hinges on elementary property of Hamming crosscorrelation in Proposition 2.

Theorem 8. *For $M \geq 2$, we have*

$$L_{\min}(M) \geq 2M^2. \qquad (1)$$

Proof: For distinct i and j, the Hamming weight of s_i and s_j are both known as M. With (i) of Theorem 7 we know there is no adjacent ones in s_j. Then by the construction of s'_j, we find the Hamming weight of s'_j is equal to $2M$. Thus from

Proposition 2, we know $H_{s_i s'_j}[\tau]$ averaged over all integer τ, is equal to $2M^2/L$. Then if $2M^2/L > 1$, we can find some τ_0 such that $H_{s_i s'_j}[\tau_0] \geq 2$, which contradicts Theorem 6. Therefore, we can conclude that $2M^2/L \leq 1$ or equivalently $L \geq 2M^2$. ■

Example 2: s_1 and s_2 form a $\mathsf{ECIS}(8,2)$:

$$s_1 = [1\ 0\ 0\ 0\ 1\ 0\ 0\ 0]$$
$$s_2 = [1\ 0\ 1\ 0\ 0\ 0\ 0\ 0].$$

It is easy to see that the bit structure is in accordance with Theorem 7 from the following:

$$d^*(\mathcal{I}_{s_1}) = \{4\},\ d^*(\mathcal{I}_{s_2}) = \{2,6\}.$$

From Theorem 8, we know the above is the shortest ECI sequence set for $M = 2$.

Remark: To compare different models of synchronization , the shortest UI sequence set for $M = 2$ is given below.

$$s_1 = [1\ 0\ 1\ 0]$$
$$s_2 = [1\ 1\ 0\ 0].$$

For the slot-synchronized channel, one can check the difference sets below are just in accordance with (ii) of Theorem 7.

$$d^*(\mathcal{I}_{s_1}) = \{2\},\ d^*(\mathcal{I}_{s_2}) = \{1,3\}.$$

B. An Asymptotic Lower Bound on $L^e_{\min}(M)$

The following result is essential in this subsection to derive an asymptotic lower bound on $L^e_{\min}(M)$.

Given a positive integer $x \geq 2$, let $\pi(x)$ denote the number of distinct prime numbers between 2 and x,

$$\pi(x) := |\{i : 2 \leq i \leq x, i \text{ is prime}\}|.$$

Note that $\pi(x)$ also counts the maximum number of relatively prime integers between 2 and x.

Given a $\mathsf{ECIS}^e(L,M)$, let Γ_M be the collection of sequences in the $\mathsf{ECIS}^e(L,M)$ such that if $s \in \Gamma_M$, then the difference of any pair distinct elements in $d^*(\mathcal{I}_s)$ is at least two.

Theorem 9. *For any $\mathsf{ECIS}^e(L,M)$, we have*

$$|\Gamma_M| \geq M - \pi(2M-2). \tag{2}$$

Proof: Let g_j be the common difference of equi-difference s_j for $j = 1,2,\ldots,M$. The characteristic set $\mathcal{I}_{s_j}$ can be written as

$$\{0, g_j, \ldots, (M-1)g_j\} \bmod L.$$

Then for $j = 1,2,\ldots,M$, we have

$$d^*(\mathcal{I}_{s_j}) = \{g_j, -g_j, \ldots, (M-1)g_j, -(M-1)g_j\} \bmod L.$$

Suppose $s_1 \notin \Gamma_M$. Let m_i be some integral number ranged from 0 to $M-1$ for $i = 1,2,\ldots,6$. From the definition of Γ_M, we have the following three possible cases:

case 1: $m_1 g_1 - (-m_2 g_1) = 1 \bmod L$;
case 2: $(-m_4 g_1) - m_3 g_1 = 1 \bmod L$;
case 3: $m_5 g_1 - m_6 g_1 = 1 \bmod L$.

It is easy to see that case 3 implies there exists two consecutive ones in s_1. It contradicts (i) of Theorem 7. Thus we can rule out the case 3 and just need to consider the first two cases. The case that $m_1 + m_2 < M$ or $m_3 + m_4 < M$ can also be ruled out due to it also implies that there exists a consecutive two ones' run in s_1 contradicting (i) of Theorem 7. By letting $n_1 = (m_1 + m_2)$ and $n_2 = (m_3 + m_4)$, both ranged from M to $2M-2$, we can further simplify the two cases into

$$n_1 g_1 = 1 \bmod L; \tag{3}$$

$$n_2 g_1 = -1 \bmod L. \tag{4}$$

Also, we can find n_1 is relatively prime to L. Otherwise over $\mathbb{Z}_L$, the result of $n_1 g_1$ should be located in $[2, L-2]$, which contradicts (3). The same result can also be found for n_2 and L.

Now we consider another sequence, $s_2 \notin \Gamma_M$. Let r_1 and r_2 be some integer ranged from M to $2M-2$ respectively. For the same reason, there are following two possible cases:

$$r_1 g_2 = 1 \bmod L; \tag{5}$$

$$r_2 g_2 = -1 \bmod L. \tag{6}$$

By the same argument, we find that r_1, r_2 are relatively prime to L respectively.

Consider (3) and (5) first. Combining them we have

$$n_1 g_1 - r_1 g_2 = 0 \bmod L.$$

Let v_1 be the largest common factor of n_1 and r_1. Now we will prove $v_1 = 1$ by contradiction. v_1 is relatively prime to L from the fact that n_1 and r_1 are relatively prime to L respectively. Given v_1, we thus have

$$(n_1/v_1)g_1 = (r_1/v_1)g_2 \bmod L$$

If $v_1 > 1$, we can find (n_1/v_1) and (r_1/v_1) are both smaller than M from $n_1, r_1 \leq 2M-2$. It further implies that there is a common element between $d^*(\mathcal{I}_{s_1})$ and $d^*(\mathcal{I}_{s_2})$, which contradicts (ii) of Theorem 7. Therefore we find that $v_1 = 1$, i.e., n_1 and r_1 are relatively prime.

Then consider (3) and (6). Combining them we have

$$n_1 g_1 + r_2 g_2 = 0 \bmod L.$$

We also can find n_1 and r_2 are relatively prime. Let v_2 be the largest common factor of n_1 and r_2. Given v_2 which is relatively prime to L, we thus have

$$(n_1/v_2)g_1 = L - (r_2/v_2)g_2 \bmod L$$

By the similar argument, we find that $v_2 = 1$.

For (4) and (5), similarly we also can get that n_2 and r_1 are relatively prime. The result is also true for n_2 and r_2 considering (4) and (6). Therefore, by the above argument we can conclude that the four pairs (n_1, r_1), (n_1, r_2), (n_2, r_1), (n_2, r_2) are all relatively prime respectively. In other words, if there are two sequences not in Γ_M, at least one case of the above would occur, then there are at least two proper integral numbers, ranged from M to $2M-2$, such that they are relatively prime.

The above claim can be easily generalized to that there are $M-|\Gamma_M|$ sequences not in Γ_M. Then there are $M-|\Gamma_M|$ proper integral numbers, ranged from M to $2M-2$, namely $\beta_1,\beta_2,\dots,\beta_{M-|\Gamma_M|}$, such that they are mutually relatively prime. The number of these integers is less than or equal to the maximal number of relatively prime integers between 2 and $2M-2$, namely $\pi(2M-2)$. We thus have $M-|\Gamma_M|$ less than or equal to $\pi(2M-2)$. ■

We state a version of Kneser's theorem, which is tailored to what we need here. It will be useful to derive the asymptotic lower bound on $L^e_{\min}(M)$. A proof of Kneser's theorem can be found in [16].

Theorem 10 (Kneser [17])**.** *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

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

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

Furthermore, in view of Kneser's theorem, we classify M sequences in any $\mathsf{ECIS}^e(L,M)$ 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*. Denote the set of sequences in class 2 as Υ_M. As proved in [9], we have the following asymptotic result:

$$\liminf_{M\to\infty}\frac{|\Upsilon_M|}{M}=1. \tag{7}$$

Theorem 11.

$$\liminf_{M\to\infty}\frac{L^e_{\min}(M)}{4M^2}\geq 1. \tag{8}$$

Proof: By the prime number theorem, we know $\pi(x)$ is close to $x/\ln x$ for large M. Thus following (2) we have

$$\liminf_{M\to\infty}\frac{|\Gamma_M|}{M}\geq\frac{M-(2M-2)/\ln(2M-2)}{M}$$

which implies

$$\liminf_{M\to\infty}\frac{|\Gamma_M|}{M}=1, \tag{9}$$

by the condition $|\Gamma_M|\leq M$.

Given a $\mathsf{ECIS}^e(L,M)$, let Ω_M be $\Gamma_M\cap\Upsilon_M$. With Theorem 10 and $\Omega_M\subseteq\Upsilon_M$, we see the total number of distinct elements in all $d^*(\mathcal{I}_{s_j})$ for $s_j\in\Omega_M$ is at least

$$|\Omega_M|(2M-2).$$

Following Theorem 7, the definition of Γ_M and $\Omega_M\subseteq\Gamma_M$, we know the difference of any pair elements in all $d^*(\mathcal{I}_{s_j})$, $s_j\in\Omega_M$, is at least two. Thus, the nonzeros in $\mathbb{Z}_L$ should contain at least $|\Omega_M|(2M-2)$ distinct elements whose mutual difference is at least two. Also we have 1 and $L-1$ are not contained in these elements from (i) of Theorem 7. Then we have

$$L-1\geq 1+2|\Omega_M|(2M-2). \tag{10}$$

We define ε_1 and ε_2 as the following respectively:

$$\varepsilon_1:=\{1,2,\dots,M\}\setminus\Gamma_M;$$

$$\varepsilon_2:=\{1,2,\dots,M\}\setminus\Upsilon_M.$$

Combining them, we have

$$\begin{aligned}\{1,2,\dots,M\}&=(\Gamma_M\cup\varepsilon_1)\cap(\Upsilon_M\cup\varepsilon_2)\\&\subseteq(\Gamma_M\cup\varepsilon_1\cup\varepsilon_2)\cap(\Upsilon_M\cup\varepsilon_2\cup\varepsilon_1)\\&=(\Gamma_M\cap\Upsilon_M)\cup(\varepsilon_2\cup\varepsilon_1)\\&=\Omega_M\cup(\varepsilon_2\cup\varepsilon_1)\end{aligned}$$

which implies

$$\begin{aligned}M=|\{1,2,\dots,M\}|&\leq|\Omega_M\cup(\varepsilon_2\cup\varepsilon_1)|\\&\leq|\Omega_M|+|\varepsilon_2|+|\varepsilon_1|.\end{aligned}$$

Then following (7), (9) and the above, we have

$$\begin{aligned}\liminf_{M\to\infty}\frac{|\Omega_M|}{M}&\geq\liminf_{M\to\infty}1-\frac{|\varepsilon_1|}{M}-\frac{|\varepsilon_2|}{M}\\&=1\end{aligned}$$

By the condition that $|\Omega_M|\leq M$, we further obtain

$$\liminf_{M\to\infty}\frac{|\Omega_M|}{M}=1. \tag{11}$$

Hence the following result can be found from (10) and (11):

$$\begin{aligned}\liminf_{M\to\infty}\frac{L^e_{\min}(M)}{4M^2}&\geq\liminf_{M\to\infty}\frac{2+2|\Omega_M|(2M-2)}{4M^2}\\&=\liminf_{M\to\infty}\frac{2+2M(2M-2)}{4M^2}=1.\end{aligned}$$

In other words, $L^e_{\min}(M)$ is lower bounded by approximately $4M^2$ when M is large.

■

IV. An Asymptotically Optimal Construction

First, we present the following general construction of CI sequence set based on UI sequence set. We use $\mathsf{EUIS}(L,M)$ to denote a UI sequence set of M sequences with period L and Hamming weight M. Specially we denote an equi-difference $\mathsf{EUIS}(L,M)$ by $\mathsf{EUIS}^e(L,M)$.

Theorem 12. *Given a $\mathsf{EUIS}(L,M)$, then we can construct a $\mathsf{ECIS}(2L,M)$ by doubling all elements in the characteristic set of each sequence.*

Proof: In the slot-synchronized channel, following the construction of s'_j, Theorem 6 can be found reduced to $H_{s_is_j}[\tau]\leq 1$ for any integer τ and any pair of distinct i and j, for any $\mathsf{EUIS}(L,M)$. Thus we find (ii) of Theorem 7 holds. By doubling all elements in the characteristic set of each sequence and period, we further find (i) and (iii) of Theorem 7 hold since the difference of any two distinct even numbers is even. Therefore, from Theorem 7 we can conclude this new sequence set is a $\mathsf{ECIS}(2L,M)$. ■

Remark: The variation is found as a special case of [2] which is targeted for achieving the capacity of the asynchronous collision channel without feedback.

Theorem 11 asserts that $L^e_{\min}(M)$ is lower bounded by $4M^2$ approximately when M is large. In order to design a $\mathsf{ECIS}^e(L,M)$ with period achieving $4M^2$ asymptotically, the following construction for UI sequence set is introduced.

M	L	subsets in $\mathbb{Z}_L$
2	8	{0,2},{0,4}
3	24	{0,2,4},{0,6,12},{0,8,16}
4	52	{0,2,4,6},{0,8,16,24},{0,10,20,30},{0,12,26,38}
5	84	{0,2,4,6,8},{0,10,20,30,40},{0,12,24,36,48}, {0,14,28,42,56}, {0,16,32,50,66}

TABLE I
THE SHORTEST KNOWN PERIODS OF ECI SEQUENCE SET WITH M SEQUENCES FOR $M = 2, 3, 4, 5$.

CRT Construction: 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 [18], and preserves addition and multiplication by integers. Given M, we set q to be $2M-1$, and p any prime larger than or equal to M and relatively prime to $2M-1$. Let u be any integer ranged from 1 to $M-1$, relatively prime to $2M-1$. For $j = 0, 1, \dots, M-1$, we let

$$\mathcal{I}'_{s_j} := \{(jy, yu) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2M-1} : y = 0, 1, \dots, M-1\}$$

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

Remark: When $u = 1$, the CRT construction is the same as the original construction in [9].

Let h be the number of integers ranged from 1 to $M-1$ and relatively prime to $2M-1$.

Theorem 13. *For all M, the sequences by CRT construction form h distinct $\mathsf{EUIS}^e(p(2M-1), M)$s consisting of hM distinct sequences.*

Proof of Theorem 13 is a generalization of that in [9] and can be found in Appendix B.

We modify the CRT construction via the method stated in Theorem 12. We call it *mCRT construction*.

Theorem 14. *For all M, the sequences by mCRT construction form h distinct $\mathsf{ECIS}^e(2p(2M-1), M)$s consisting of hM distinct sequences.*

Proof: It directly follows Theorem 12 and 13. ■

Example 4: By mCRT construction for $p = M = 3$, we can design the following two distinct $\mathsf{ECIS}^e(30, 3)$s including six distinct sequences.

The first $\mathsf{ECIS}^e(30, 3)$ with $g_1 = 6, g_2 = 4$ and $g_3 = 14$:

$$s_1 = [100000100000100000000000000000]$$
$$s_2 = [100010001000000000000000000000]$$
$$s_3 = [100000000000001000000000000010].$$

The second $\mathsf{ECIS}^e(30, 3)$ with $g_1 = 12, g_2 = 2$ and $g_3 = 8$:

$$s_1 = [100000000000100000000000100000]$$
$$s_2 = [101010000000000000000000000000]$$
$$s_3 = [100000001000000010000000000000].$$

By mCRT construction, we will show the asymptotic lower bound in Theorem 11 can be achieved.

Theorem 15.

$$\liminf_{M\to\infty} \frac{L^e_{\min}(M)}{4M^2} = 1. \tag{12}$$

Proof: Let p_M be the smallest prime larger than or equal to M. By Bertrand's postulate, we know if $M \geq 2$, then there always exists at least one prime number not smaller than M and smaller than $2M-1$. It implies $p_M < 2M-1$ for $M \geq 2$. Then as p_M is a prime, we find the smallest two integers not relatively prime to p_M, are p_M and $2p_M$. Because $p_M < 2M-1 < 2M \leq 2p_M$, we further find p_M and $2M-1$ are always relatively prime for $M \geq 2$. Thus we can obtain a $\mathsf{ECIS}^e(2p_M(2M-1), M)$ from mCRT construction with p_M for $M \geq 2$.

Also we have the following fact:

$$\liminf_{M\to\infty} p_M/M = 1,$$

since there are infinitely many primes and $p_M = M$ if M is a prime. Therefore we have

$$\liminf_{M\to\infty} \frac{2p_M(2M-1)}{4M^2} = 1.$$

This shows that the asymptotic lower bound in Theorem 11 is tight and proves Theorem 15. ■

Remark: For $M = 2, 3, 4, 5$, the shortest known period of ECI sequence set with M sequences is listed in Table I. We note the sequence set for $M = 2, 3$ is equi-difference, but not for $M = 4, 5$. However, these sequence sets are all constructed from UI sequence set following Theorem 12. For example, when $M = 4$, it is constructed from

$$\{0, 1, 2, 3\}, \{0, 4, 8, 12\}, \{0, 5, 10, 15\}, \{0, 6, 13, 19\}$$

in $\mathbb{Z}_{26}$.

V. Discussion on Blocking Probability

In the unslotted random access scheme, we can compute the probability of at least one of the users cannot send any packet successfully in a period of L time slots. We call this the blocking probability. The blocking probability is nonzero and user irrepressibility in the asynchronous channel does not hold for unslotted random access scheme.

The power consumption is measured by the fraction of ones of a protocol sequence in each period, also known as the *duty factor*, p_d. In order to make a fair comparison with ECI protocol sequence set, in the random access scheme, we pick the probability of sending a packet such that the duty factor is the same as in the sequence including in ECI sequence set. The blocking probability of the unslotted random access scheme with p_d in a given period can be easily found by

$$1 - \big(1 - (1 - p_d(1 - 2p_d)^{M-1})^L\big)^M.$$

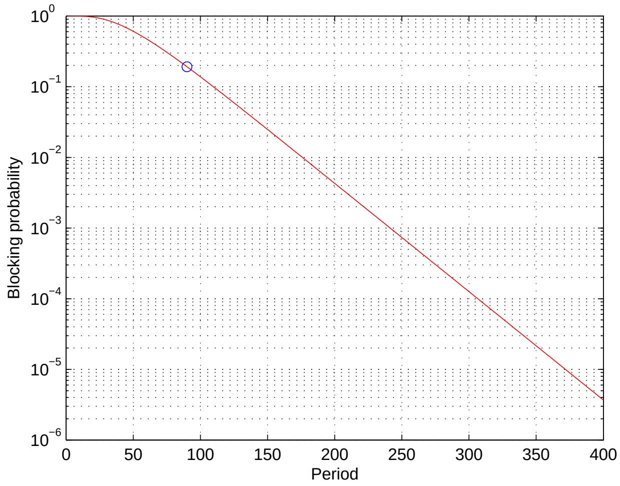

Fig. 2. The blocking probability for 5 users in a unslotted random access scheme with duty factor fixed at $1/18$. When the period is the same as that in mCRT sequence set, i.e., 90, the blocking probability is about 0.2.

The period of the mCRT sequence set for 5 users is 90 and the duty factor is $1/18$. We plot the blocking probability of unslotted random access for 5 users in Fig. 2, with duty factor fixed at 1/18. We see that in a block length of 90 time slots, the blocking probability is about 0.2, meanwhile, the blocking probability for ECI sequence set is zero. If we want blocking probability less than, say 10^{-4}, in a period of L time slots, we must have L larger than 306 time slots.

VI. Conclusion

We consider the property of user irrepressibility for the asynchronous channel in the design of protocol sequences. CI protocol sequence set provides strict guarantee of zero blocking probability within one period for each user in the asynchronous channel. The minimum period for equi-difference ECI sequence set with M sequences is shown to be asymptotically $4M^2$. A construction that meets this asymptotic bound is given.

The minimum period of ECI sequence set which is not equi-difference may be between $2M^2$ and $4M^2$ asymptotically for M users. However, we do not think such construction can be found. Thus we have the following:

Conjecture 1. *Given M, then we have*

$$\liminf_{M\to\infty} \frac{L_{\min}(M)}{4M^2} = 1.$$

Furthermore, for all $M \geq 2$, we have the following improvements over the asymptotic bounds in Conjecture 1.

Conjecture 2. *Let Φ_M be the shortest period among all sets of M UI sequences, each with Hamming weight M. Then for $M \geq 2$ we have*

$$L_{\min}(M) = 2\Phi_M.$$

The result has been verified by computer on the range of $2 \leq M \leq 5$. The mathematical proof of the above two conjectures is an interesting and challenging direction for further studies.

Appendix A
Proof of Proposition 4

Given two binary value a and b, their *logical OR* is defined as

$$(a \vee b) := \begin{cases} 1 & \text{if } a = 1 \text{ or } b = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let k_0 be any non-negative integral number such that $k_0+\delta_i \geq \delta_{max}$. We know all users started their transmission schemes at the time index $k_0 + \delta_i$ or earlier. Suppose $f_{s_i}(t - \delta_i) = 1$ for any $t \in [k_0 + \delta_i, k_0 + \delta_i + 1)$. Then we know there is a packet from user i located in $[k_0 + \delta_i, k_0 + \delta_i + 1)$. Furthermore we know this packet is successful iff no other users start or end their packet transmission in $[k_0+\delta_i, k_0+1+\delta_i)$ or equivalently we have

$$\bigvee_{j=1, j\neq i}^{M} f_{s_j}(t - \delta_j) = 0 \tag{13}$$

for any $t \in [k_0 + \delta_i, k_0 + \delta_i + 1)$.

Let ξ_1 be the collection of all $j \in \{1, 2, \ldots, M\} \setminus \{i\}$ such that $\lfloor \delta_j - \delta_i \rfloor \neq \delta_j - \delta_i$. Let ξ_2 be $\{1, 2, \ldots, M\} \setminus \{i, \xi_1\}$. Then from (13) we have the following formula to find this packet is not successful if it is equal to one.

$$\begin{aligned}
&\left\lceil \int_{k_0+\delta_i}^{(k_0+1+\delta_i)^-} \bigvee_{j=1,j\neq i}^{M} f_{s_j}(t-\delta_j)\ dt \right\rceil \\
&= \Big\{ \bigvee_{j\in\xi_1} f_{s_j}(k_0+\delta_i-\delta_j) \vee f_{s_j}(k_0+1+\delta_i-\delta_j) \Big\} \\
&\qquad \vee \Big\{ \bigvee_{j\in\xi_2} f_{s_j}(k_0+\delta_i-\delta_j) \Big\} \\
&= \Big\{ \bigvee_{j\in\xi_1} f_{s_j}(\lfloor k_0+\delta_i-\delta_j \rfloor) \vee f_{s_j}(\lfloor k_0+1+\delta_i-\delta_j \rfloor) \Big\} \\
&\qquad \vee \Big\{ \bigvee_{j\in\xi_2} f_{s_j}(\lfloor k_0+\delta_i-\delta_j \rfloor) \Big\} \\
&= \Big\{ \bigvee_{j\in\xi_1} s_j\big[k_0-1-\lfloor \delta_j-\delta_i \rfloor\big] \vee s_j\big[k_0-\lfloor \delta_j-\delta_i \rfloor\big] \Big\} \\
&\qquad \vee \Big\{ \bigvee_{j\in\xi_2} s_j\big[k_0-\lfloor \delta_j-\delta_i \rfloor\big] \Big\} \\
&= \Big\{ \bigvee_{j\in\xi_1} s_{j'}\big[k_0-\lfloor \delta_j-\delta_i \rfloor\big] \Big\} \vee \Big\{ \bigvee_{j\in\xi_2} s_j\big[k_0-\lfloor \delta_j-\delta_i \rfloor\big] \Big\} \\
&= \bigvee_{j=1,j\neq i}^{M} s_{i\_j}[k_0].
\end{aligned}$$

The last two equalities follow respectively from the constructions of s'_j and s_{i_j}. Furthermore, the total number of unsuccessful packets from user i at time interval $[\delta_i + k, \delta_i + k + L)$ for any non-negative integral number k such that $k+\delta_i \geq \delta_{max}$

can be found as:

$$\begin{aligned}&\sum_{k_0=k}^{k+L-1}\Big[\int_{k_0+\delta_i}^{(k_0+1+\delta_i)^-} f_{s_i}(t-\delta_i)\bigvee_{j=1,j\neq i}^{M} f_{s_j}(t-\delta_j)\ dt\Big]\\ &=\sum_{k_0=k}^{k+L-1} s_i[k_0]\bigvee_{j=1,j\neq i}^{M} s_{i\_j}[k_0]\\ &=\sum_{k_0=0}^{L-1} s_{i\_i}[k_0]\bigvee_{j=1,j\neq i}^{M} s_{i\_j}[k_0],\end{aligned}$$

which implies the number of blocked ones of s_{i_i} in T_i. Thus the claim (i) of Proposition 4 is proved.

For any non-negative integer k such that $k+\delta_i<\delta_{max}$, we know there exists at least one user with its time offset smaller than $k+\delta_i$ so that it would start their transmission schemes later than the time index $k+\delta_i$. Thus, the number of successful packets from user i in time interval $[\delta_i+k,\delta_i+k+L)$ would be equal to or larger than the number in claim (i). It proves the result of (ii).

Appendix B
Proof of Theorem 13

First we know that all sequences formed by CRT construction are equi-difference. For $s_{j,u}$, its common difference can be found as (j,u) or $(p-j,2M-1-u)$.

Then we will show $s_{j,u}$ for $j=0,1,\dots,M-1$ form a $\mathsf{EUIS}^e(p(2M-1),M)$. Suppose for the sake of contradiction that, we can find two distinct i and j in $\{0,1,\dots,M-1\}$ such that $d^*(\mathcal{I}'_{s_{i,u}})$ and $d^*(\mathcal{I}'_{s_{j,u}})$ share a common element. Then

$$(iy_1',y_1'u)-(iy_1,y_1u)=(jy_2',y_2'u)-(jy_2,y_2u)$$

for some $y_1'\neq y_1$ and $y_2'\neq y_2$. By equating the second components on both sides, we see that $u(y_1'-y_1)=u(y_2'-y_2)\bmod 2M-1$. Since the range of y_1, y_1', y_2 and y_2' is between 0 and $M-1$, we must have $y_1'-y_1=y_2'-y_2$ due to u is prime to $2M-1$. From the first component, we obtain $(i-j)(y_1'-y_1)\equiv 0\bmod p$, which implies that $y_1'=y_1$. This contradicts the assumption that $y_1'\neq y_1$. It implies the condition in (ii) of Theorem 7 holds for $\mathcal{I}_{s_{j,u}}$ here for $j=0,\dots,M-1$. Therefore, following Theorem 7 we can conclude that the sequences formed by the CRT construction with the same value of u form a $\mathsf{EUIS}^e(p(2M-1),M)$.

Now we know there are total h sequence set formed by CRT construction with different value of u. Then we will show that all hM sequences here are distinct. For sequences constructed by the same value of u, we can easily find that these M sequences are distinct, otherwise any two non-distinct sequences would be totaly blocked each other for some relative integer-shift which contradicts the definition of UI sequence set.

Since u is relative prime to $2M-1$, we have

$$g\neq 0\mod 2M-1$$

with $g=f^{-1}(j,u)$. Thus we find $Mg\neq 0\mod L$ with $L=p(2M-1)$. Let u_1 and u_2 be two distinct integers ranged from 1 to $M-1$ and relatively prime to $2M-1$ respectively. Consider two sequence formed by CRT construction letting $u=u_1$ and $u=u_2$ respectively. Suppose for the sake of contradiction that, for some j and j' we can find that

$$(j,u_1)=(j',u_2)\text{ or }(p-j',2M-1-u_2).$$

By equating the second components on both sides, we see that

$$u_1=u_2\text{ or }2M-1-u_2\bmod 2M-1.$$

Since that the range of u_1 and u_2 is between 1 and $M-1$, we must have $u_1=u_2$. This contradicts the assumption that $u_1\neq u_2$. Thus any two sequences constructed by different value of u can be found distinct.

Finally, we can conclude the CRT construction form h distinct $\mathsf{EUIS}^e(p(2M-1),M)$s including hM distinct sequences.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

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

[3] N. Abramson, “The aloha system: Another alternative for computer communications,” *In Proceedings of the Fall 1970 AFIPS Computer Conference*, pp. 281–285, Nov. 1970.

[4] V. Anantharam, “The stability region of the finite-user slotted ALOHA protocol,” *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 535–540, May 1991.

[5] J. Y. N. Hui, “Multiple accessing for the collision channel without feedback,” *IEEE J. Sel. Aareas Commun.*, vol. SAC-2, no. 4, pp. 575–582, Jul. 1984.

[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] G. Yang and W. C. Kwong, “Performance analysis of optical CDMA with prime codes,” *IEE Electron. Lett.*, vol. 31, no. 7, pp. 569–570, Mar. 1995.

[8] ——, *Prime Codes with Applications to CDMA Optical and Wireless Networks*. Norwood, Massachuset: Artech House, 2002.

[9] K. W. Shum, W. S. Wong, C. W. Sung, and C. S. Chen, “Design and construction of protocol sequences: Shift invariance and user irrepressibility,” in *IEEE Int. Symp. Inform. Theory*, Seoul, Jun. 2009.

[10] K. W. Shum, Y. Zhang, and W. S. Wong, “User-irrepressible sequences,” *to appear in SETA 2010*.

[11] 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.

[12] 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.

[13] K. Momihara, “Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three,” *SIAM J. Discrete Math.*, vol. 45, pp. 379–390, 2007.

[14] K. W. Shum, W. S. Wong, and C. S. Chen, “A general upper bound on the size of constant-weight conflict-avoiding codes,” *to appear in IEEE Trans. Inform. Theory*.

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

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

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

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