

# User-Detectable Sequences for the Collision Channel Without Feedback

Yijin Zhang, Kenneth W. Shum, Wing Shing Wong

*Department of Information Engineering*

*The Chinese University of Hong Kong*

*Shatin, Hong Kong*

{zyj007, wswong}@ie.cuhk.edu.hk

wkshum@inc.cuhk.edu.hk

**Abstract**—Protocol sequences are used for distributed multiple accessing in the collision channel without feedback. In this paper we consider user-detectable sequences with the property that each active user can be detected by looking at the channel activity only, within some bounded delay. It is important in some applications such as ad hoc networks. Some lower and upper bounds of its minimum period are investigated in this paper. In addition, we display some interconnections with some other sequence designs.

**Index Terms**—Collision channel without feedback, protocol sequences, user-irrepressible sequences, CRT construction, optical orthogonal code.

## I. INTRODUCTION

Massey and Mathys [1], [2] introduced the model of the collision channel without feedback for multiple access communication. Consider a time-slotted system, consisting of  $M$  users and one sink. All  $M$  users may be active at the same time. Each user is assigned a binary deterministic sequence with length  $L$ , called a *protocol sequence*. For  $i = 1, 2, \dots, M$ , the protocol sequence associated with user  $i$  is specified by a row vector  $s_i := [s_i(0) s_i(1) \dots s_i(L-1)]$ . When a user changes from inactive to active, protocol sequence assigned are read slot by slot periodically. It transmits a packet within the boundaries of a time slot if and only if the value of the protocol sequence at that time slot equals one. If two or more users send simultaneously, we say that there is a collision and we assume that no information can be recovered. If one and only one user transmits, the packet can be received error-free. When a user changes from active to inactive, it is assumed that after the end of the sequence, the user must keep silent for at least one period before becoming active again.

There is some complication due to delay offsets. As there is no feedback from the receiver and no cooperation among the users, each user has a delay offset which is a random integer but remains fixed throughout the communication session. In other words, all protocol sequences sent by active users are not frame synchronized. Suppose user  $i$  starts a protocol sequence at the time index  $t_0$ . It will send a packet if  $s_i(t-t_0)$  equals 1. For practical considerations, one would like to remove the assumption that the slot boundaries are synchronized, i.e.,  $t_0$

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

here may be a non-integral number. It is, in fact, possible to do so and to allow the users to be totally asynchronous. Our result can also be extended to this more general scenario.

In multiple access transmission without packet header, three tasks [3], [4] should be solved by the receiver through observing the channel activity (whether a time slot is idle, containing a collision or a successful packet), viz.:

- (i) to detect each active user (detection),
- (ii) to determine the sender of each successful received packet (decoding), and
- (iii) to find their delay offsets (synchronization).

In this paper we investigate only the detection problem, as task (ii) and (iii) may be not necessary for some applications. We want to find protocol sequences that allow any active user be detected by the receiver via some algorithm within some bounded delay if and only if it has become active. Such protocol sequence set is said to be *user-detectable* (UD).

The notion of user-detectability is also addressed in another context for the OR channel, under the name *uniquely decipherable code* [5], [6] with the assumption all active users start its codeword at the same time, which can be viewed as a special case of the concept discussed here.

In this paper, in order to explore the minimal delay in the worst case, we are interesting in  $L_{\min}(M)$ , the smallest length  $L$  such that a UD sequence set exists for  $M$  users. The paper is organized as follows. After setting up some notations and definitions in Section II, we establish a lower bound on  $L_{\min}(M)$  in section III. Then an upper bound and related constructions are presented in section IV. Section V gives a proof to show the existence of UD sequence set different from that in section IV. Finally, we close in Section VI with some concluding remarks.

## II. NOTATIONS AND DEFINITIONS

We will use sequence “period” and sequence “length” interchangeably. Given a binary sequence  $s(t)$ ,  $t = 0, 1, \dots, L-1$ , of length  $L$ , we define its *Hamming weight* as

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

Let the *cyclic shift* of a sequence  $s$  by relative shift  $\tau$  be

denoted by  $s^{(\tau)}$ ,

$$s^{(\tau)}(t) := s(t - \tau).$$

The subtraction  $t - \tau$  is performed modulo  $L$ .

Given two sequences  $s_1(t)$  and  $s_2(t)$ , the Hamming cross-correlation function between  $s_1$  and  $s_2$  is defined by

$$H_{s_1 s_2}(\tau) := \sum_{t=0}^{L-1} s_1(t) s_2(t - \tau).$$

If  $s_1(t) = s_2(t)$ , the crosscorrelation is reduced to the autocorrelation of  $s_1$  or  $s_2$ .

In our channel model, detection of user activity is achieved by merely observing the channel activity. To this end, we make the following:

**Definition 1.** For each time index  $t$ , let

$$c(t) = \begin{cases} 0 & \text{if no user transmits at slot } t, \\ 1 & \text{if exactly one user transmits at slot } t, \\ * & \text{if more than one users transmit at slot } t. \end{cases}$$

We call  $c(t)$  the *channel-activity signal*. For each time index  $t$ , let  $c_i(t)$  be 1 if user  $i$  transmits at  $t$  or zero otherwise. We call  $c_i(t)$  the *signal of user  $i$* .

We also make the following formal definition of UD sequence set.

**Definition 2.** Let  $D(t)$  be the detection result of active users at the time index  $t$  by observing  $c(t)$  in  $[0, t]$ . The value of  $D(t)$  may be an empty set or a subset of  $\{1, 2, \dots, M\}$ . A sequence set of period  $L$  is said to be UD if the following conditions:

- (i) If user  $i$  becomes active or starts a new sequence at  $t$ , then  $i \in D(t + L - 1)$ ;
- (ii) If  $i \in D(t)$ , then user  $i$  actually becomes active or starts a new sequence in the time interval  $[t - 2L + 2, t]$ ;

are both satisfied for any non-negative  $t$  and any  $i \in \{1, 2, \dots, M\}$ .

### III. A LOWER BOUND ON $L_{\min}(M)$

In order to explore the minimal delay we can achieve, a lower bound on  $L_{\min}(M)$  will be presented in this section.

We first give an example of a protocol sequence set which is not UD. Given that user  $i$  becomes active or starts a new sequence at  $t_0$ , let  $C_A^i(t_0)$  be the channel activity vector of  $c(t)$  in  $[t_0, t_0 + L - 1]$ . Let  $C_I^i(t_0)$  be the channel activity vector of  $c(t)$  in  $[t_0, t_0 + L - 1]$  provided that user  $i$  is inactive in  $[t_0, t_0 + L - 1]$ .

**Example 1:** Sequence periods are indicated by underbrace. Given a sequence set, for some time offsets and starting time

of each user, we have the following:

$$\begin{aligned} c_1(t) &: \underbrace{1100001000000000}_{L=10} \underbrace{1100001000000000}_{L=10} \\ c_2(t) &: \underbrace{1110000000000000}_{L=10} \underbrace{0000000000000000}_{L=10} \\ c_3(t) &: \underbrace{0100001000010000}_{L=10} \underbrace{0000000000000000}_{L=10} \\ c_4(t) &: \underbrace{000100100100000000}_{L=10} \underbrace{0000000000000000}_{L=10} \\ c_5(t) &: \underbrace{1000100010000000}_{L=10} \underbrace{1000100010000000}_{L=10} \\ c(t) &: * \underbrace{1110} * \underbrace{01101000} * \underbrace{10010101000000} \end{aligned}$$

One can check  $C_A^1(0) = C_I^1(0)$  for this case. Then we cannot be sure user 1 is active or not in  $[0, 14]$  from the channel-activity signal. Thus the sequence set is not UD.

Inspired by the above example, we present one necessary condition for user-detectability after introducing the definitions below.

For two binary sequences  $s$  and  $s'$ , their *logical OR* is defined as

$$(s \vee s')(t) := \begin{cases} 1 & \text{if } s(t) = 1 \text{ or } s'(t) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

**Definition 3.** Consider a protocol sequence set of period  $L$ , consisting of  $u$  sequences  $s_i(t)$ , for  $i = 1, 2, \dots, u$ . Sequence  $s_i(t)$  is *blocked* by other  $u - 1$  sequences if we can find delay offsets  $\tau_j$ , for  $j \in \{1, 2, \dots, u\} \setminus \{i\}$ , such that

$$s_i \preceq (s_1^{(\tau_1)} \vee \dots \vee s_{i-1}^{(\tau_{i-1})} \vee s_{i+1}^{(\tau_{i+1})} \vee \dots \vee s_u^{(\tau_u)}).$$

Otherwise, it is not blocked by other  $u - 1$  sequences.

**Proposition 1.** *If a sequence set is UD, then each sequence in this sequence set cannot be blocked by two disjoint subsets of other sequences respectively.*

*Proof:* Consider  $s_g$  such that it can be blocked by two disjoint subsets of other sequences respectively. Suppose user  $g$  becomes active at  $t_0$ . Then we know for every time index in  $[t_0, t_0 + L - 1]$  such that user  $g$  has 1, at least other two users can also have one for some time offsets. Thus, even if user  $g$  is not active in  $[t_0, t_0 + L - 1]$ , we also can find  $c(t)$  equals  $*$  at these time indexes. On the other hand, for each time index in  $[t_0, t_0 + L - 1]$  such that user  $g$  has 0, it would not cause the change in  $c(t)$ . For this special case, we find  $C_A^g(t_0) = C_I^g(t_0)$  which implies the sequence set is not UD. Thus we can conclude that each sequence in a UD sequence set cannot be blocked by two disjoint subsets of other sequences respectively. ■

From Proposition 1, we have the following:

**Proposition 2.** *If a sequence set of  $M$  sequences is UD, then each sequence cannot be blocked by any other  $\lceil M/2 \rceil - 1$  sequences.*

*Proof:* We prove this claim by contradiction. Consider user  $g$  in a given sequence set such that it can be blocked by any other  $\lceil M/2 \rceil - 1$  sequences. Then we can partition the

other  $M - 1$  sequences into two disjoint subsets such that each subset contains at least  $\lceil M/2 \rceil - 1$  sequences as  $2(\lceil M/2 \rceil - 1) \leq M - 1$ . By the hypothesis, each subset can block user  $g$  respectively. Therefore, following Proposition 1 we know this sequence set is not UD. ■

Then from the necessary condition in Proposition 2, we have the following lower bound on  $L_{\min}(M)$ .

**Theorem 3.** For any positive integer  $M$ ,

$$L_{\min}(M) \geq \frac{8\lceil M/2 \rceil^2}{9}.$$

*Proof:* Following Proposition 2, we can pick some  $\lceil M/2 \rceil$  sequences in a UD sequence set and relabel them so that the Hamming weight of  $s_1$  is smallest and  $s_1$  cannot be blocked by  $\{s_2, s_3, \dots, s_{\lceil M/2 \rceil}\}$ . We further describe below a blocking algorithm whose objective is to block  $s_1$  by cyclically shifting  $s_2, s_3, \dots, s_{\lceil M/2 \rceil}$ .

- (i) Fix the delay offset of  $s_1$  to zero.
- (ii) Cyclically shift  $s_2$  so that some of the “1”s in  $s_1$  is blocked by  $s_2^{(\tau_2)}$ .
- (iii) Cyclically shift  $s_3$  in such a way that part of the remaining “1”s in  $s_1$  are blocked by  $s_3^{(\tau_3)}$ .
- (iv) Cyclically shift  $s_4$  in order to block part of the remaining “1”s in  $s_1$  that are not blocked by  $s_2^{(\tau_2)}$  and  $s_3^{(\tau_3)}$ .
- (v) Continue for  $s_5, s_6, \dots, s_{\lceil M/2 \rceil}$ .

A more detailed analysis presented in [7], which is not included here due to space limitation, shows that we can always block  $s_1$  by other  $\lceil M/2 \rceil - 1$  sequences if  $L < (8/9)\lceil M/2 \rceil^2$ . Thus the above algorithm gives a lower bound of  $(8/9)\lceil M/2 \rceil^2$  on the period of  $\{s_1, s_2, \dots, s_{\lceil M/2 \rceil}\}$  with the condition there must exist some ones remain in  $s_1$  after the blocking algorithm.

Furthermore, the period of a UD sequence set of  $M$  sequences can also be obtained at least  $(8/9)\lceil M/2 \rceil^2$ . ■

#### IV. AN UPPER BOUND ON $L_{\min}(M)$ AND CONSTRUCTIONS

In this section, we will show some special classes of sequence set must be UD by the following detection method.

**Definition 4.** We say that  $c(t)$  is *matched* to  $s_i$  at time  $t_0$  if  $\forall t = 0, 1, \dots, L - 1, s_i(t) = 1 \Rightarrow c(t_0 + t) = 1$  or  $*$ .

If  $c(t)$  is matched to  $s_i$  at  $t_0$ , let  $\zeta_{t_0}^i$  be the collection of  $t_0 + t$  such that  $s_i(t) = 1$ .  $\zeta_{t_0}^i$  is used to denote the collection of  $t_0 + t$  such that  $s_i(t) = c(t_0 + t) = 1$ . Obviously, we have  $\zeta_{t_0}^i \subseteq \zeta_{t_0}^i$ . If user  $i$  actually does not transmit at any time index included in  $\zeta_{t_0}^i$ , this matching is said to be a *false matching*.

*Remarks:* To know whether the channel activity signal  $c(t)$  is matched to a sequence at  $t_0$  or not, it is necessary for the receiver to know the all values of  $c(t)$  in  $[t_0, t_0 + L - 1]$ . In other words, the receiver would make the decision at  $t_0 + L - 1$ .

We now introduce the detecting algorithm used in this section. The channel activity signal is observed all the time. The receiver keeps track with the set of active users by maintaining  $M$  Boolean variables  $active(i)$  for  $i = 1, 2, \dots, M$ , with the

values set to FALSE initially. The receiver is required to check whether  $c(t)$  is matched to  $s_i$  or not for each time index. If they are matching at  $t_0$ , then  $active(i)$  is set to TRUE and we have  $i \in D(t_0 + L - 1)$ . Otherwise, we would set  $active(i)$  as FALSE which implies  $i \notin D(t_0 + L - 1)$ . We summarize the procedure in Algorithm 1 below.

**Algorithm 1** Detecting algorithm for UI sequence sets.

---

```

1: for  $i = 1, 2, \dots, M$  do
2:   for  $t_0 = 0, 1, 2, \dots$  do
3:     if  $c(t)$  is matched to  $s_i(t)$  at  $t_0$  then
4:        $active(i) \leftarrow \text{TRUE}$ 
5:     else
6:        $active(i) \leftarrow \text{FALSE}$ 
7:     end if
8:   end for
9: end for

```

---

Before showing that the above algorithm can indeed make the user-detection under some conditions, we introduce one more definition:

**Definition 5.** A sequence set is said to be *user-irrepressible* (UI) [8] if each sequence is not blocked by other sequences no matter what the relative offsets are.

**Theorem 4.** A sequence set is UD by Algorithm 1 if it is UI.

*Proof:* Consider user  $g$  and its assigned sequence  $s_g$  here. By Algorithm 1, we know the receiver can always find  $c(t)$  is matched to  $s_g(t)$  at  $t_1$  if user  $g$  becomes active at  $t_1$ . Then the receiver would be aware of this fact at  $t_1 + L - 1$ . Thus, the event that user  $g$  becomes active from inactive can be known by the receiver with  $L - 1$  slots delay in the worst case.

The only source of error is there exists a false matching of  $s_g$  at  $t_0$ . If this error occurs, then we can find  $s_g$  can be covered by other actually active  $M - 1$  users for some time shifts. This contradicts the definition of UI sequence set. Thus the error cannot occur. Indeed we can show user  $g$  must become active from inactive or start a new sequence period at  $t_0 + L - 1$  or at most  $2L - 2$  slots earlier. To make  $c(t)$  is matched to  $s_g(t)$  at  $t_0$ , we must have user  $g$  starts its sequence period at the time index which is located in  $[t_0 - L + 1, t_0 + L - 1]$ , otherwise there is no intersection slots between  $c(t)$  in  $[t_0, t_0 + L - 1]$  and user  $g$ 's actual transmissions.

Finally we can conclude that any UI sequence set is UD by Algorithm 1. ■

Furthermore, the following upper bound just directly follows Theorem 4.

**Theorem 5.** Let  $\Lambda(M)$  be the smallest period such that there exists a UI sequence set of  $M$  sequences. Then we have

$$L_{\min}(M) \leq \Lambda(M).$$

Following Theorem 4, some known constructions of UI sequence sets can be applied for UD sequence set. We show

the shortest known UI sequence set here. A detailed proof can be found in [9].

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

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

Cyclic shift of a sequence by integer  $\tau$  is equivalent to adding  $\tau$  modulo  $L$  to the corresponding characteristic set.

**CRT Construction [9]:** This construction is based on Chinese remainder theorem. The mapping  $f : \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_p \oplus \mathbb{Z}_q$  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 [10], 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  $2M - 1$ . For  $j = 0, 1, \dots, M - 1$ , we let

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

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

The following upper bound is guaranteed by the CRT construction.

**Theorem 6.** *Let  $p_M$  be the smallest prime larger than or equal to  $M$ . Then we have*

$$L_{\min}(M) \leq p_M(2M - 1).$$

**Example 2:** By the CRT construction, for  $M = 3$  we can design the following UD sequence set with  $L = 15$ :

$$\begin{aligned} s_1 &= [100000100000100] \\ s_2 &= [11100000000000] \\ s_3 &= [100010001000000]. \end{aligned}$$

For some time offsets and starting time of each user, we have the following case to make the user-detection. Sequence periods are indicated by underbrace.

$$\begin{aligned} c_1(t) &: \underbrace{100000100000100100000100000010000000}_{\text{underbrace}} \\ c_2(t) &: 000000\underbrace{11100000000000000000000000000000}_{\text{underbrace}} \\ c_3(t) &: 00000\underbrace{100010001000000100010001000000}_{\text{underbrace}} \\ c(t) &: 10000\underbrace{1*1110011010000110010011000000}_{\text{underbrace}} \end{aligned}$$

Then one can check  $c(t)$  is matched to  $s_2(t)$  at the time indexes which are indicated by underline. Thus the receiver would set  $active(2)$  as TRUE at the time indexes which are indicated by underline. The result of  $D(t)$  including 2 here can be found as  $D(19)$ ,  $D(20)$  and  $D(21)$ , while user 2 actually becomes

active at  $t = 6$ . However, we cannot know the exact starting time of user 2.

We have proved in this section that any UI sequence set is UD. However, it was proved in [7] that the period of UI sequence set with  $M$  sequences is at least  $8M^2/9$ . In the next section we will investigate the existence of UD sequence set which is not UI, with the period between  $(8/9)\lceil M/2 \rceil^2$  and  $8M^2/9$ .

## V. EXISTENCE OF UD SEQUENCE SET WHICH IS NOT UI

An *optical orthogonal code*(OOC)( $L, w, \lambda_a, \lambda_c$ ) [11] is a family of binary sequences of length  $L$  and weight  $w$  that satisfy the following two properties:

- (i) the Hamming autocorrelation is not bigger than  $\lambda_a$  for any non-zero  $\tau$  performed modulo  $L$ ;
- (ii) the Hamming crosscorrelation is not bigger than  $\lambda_c$  for any  $\tau$ .

The  $OOC(L, w, 1, 1)$  has been extensively studied. Here, we show one example to construct a UD sequence set which is not UI.

**Theorem 7** ([12]). *Let  $q$  be a prime power and  $p$  be a prime not less than  $q + 1$ . Then there exists an  $OOC(L, q + 1, 1, 1)$  with  $p$  codewords.*

Then the following construction can be easily found by Theorem 7.

**OOC Construction:** Let  $q$  be the smallest prime power not less than  $M$ , and  $p$  the smallest prime not less than  $q + 1$ . Then following Theorem 7, we can construct an  $OOC(L, M + 1, 1, 1)$  with  $M$  sequences. We further replace two of ones in the  $M$ -th sequence by two zeros to make its weight as  $M - 1$ .

The sequence set formed by OOC construction is not UI due to the fact that all  $M - 1$  ones of  $s_M$  can be totally blocked by other  $M - 1$  sequences for some time offsets. It's easy to see the crosscorrelation property between  $s_M$  and any other sequence is still unchanged. The autocorrelation property of  $s_M$  is also the same.

We first introduce another detection method which is different from Algorithm 1. The receiver keeps track with the set of active users by maintaining  $M$  Boolean variables  $active(i)$  for  $i = 1, 2, \dots, M$ , with the values set to FALSE initially. We summarize the procedure in Algorithm 2.

By Algorithm 2, we can show the above sequence set is indeed UD.

**Theorem 8.** *The sequence set formed by OOC construction is UD by Algorithm 2.*

*Proof:* Consider user  $g$ , but  $g \neq M$  first. The error source is that there exists a false matching for  $s_g$ . If this error does occur, we can find  $s_g$  can be covered by other  $M - 1$  actually active users. It contradicts the condition of  $w = M + 1 > (M - 1)\lambda_c = (M - 1) \cdot 1$ . Thus this error cannot occur. Then we want to show if  $c(t)$  is matched to  $s_g$  at  $t_0$ , then user  $g$  actually becomes active or start a new sequence at  $t_0$ . Otherwise, we have  $s_g$  can be covered by other  $M - 1$  active sequences and a shift-version of itself for some time offsets. It contradicts the

---

**Algorithm 2** Detecting algorithm for sequence sets formed by OOC construction.

---

```

1: for  $i = 1, 2, \dots, M$  do
2:   for  $t_0 = 0, 1, 2, \dots$  do
3:     if  $c(t)$  is matched to  $s_i(t)$  at  $t_0$  then
4:       if  $i = M$  then
5:         if  $\zeta_{t_0}^M = \zeta_{t_0}^{\prime M}$  and  $|\zeta_{t_0}^{\prime M} \cap \zeta_{t_j}^{\prime j}| = 1$  for any
            $j \in \{1, 2, \dots, M-1\}$  and some  $t_j$  then
6:            $active(i) \leftarrow FALSE$ 
7:         else
8:            $active(i) \leftarrow TRUE$ 
9:         end if
10:       else
11:          $active(i) \leftarrow TRUE$ 
12:       end if
13:     else
14:        $active(i) \leftarrow FALSE$ 
15:     end if
16:   end for
17: end for

```

---

condition  $w = M+1 > (M-1)\lambda_c + \lambda_a = (M-1) \cdot 1 + 1$ . Thus by Algorithm 2, we can find the exact starting time of user  $g$ . The result can be easily generalized to  $s_1, s_2, \dots, s_{M-1}$ . It further implies that user  $j$  actually does transmission at  $t$  if  $t \in \zeta_{t_0}^j$  for any  $j \in \{1, 2, \dots, M-1\}$ .

Now we will prove user  $M$  can also be detected. Our task now is to show Algorithm 2 can prevent any false matching of  $s_M$ . Suppose  $c(t)$  is found matched to  $s_M$  at  $t_0$ . Consider  $M-1$  nonzeros positioned in  $\zeta_{t_0}^M$ . First if we have  $\zeta_{t_0}^M \neq \zeta_{t_0}^{\prime M}$ , then we can find this matching is not false. It is due to the property that each other user can contribute at most a one for these  $M-1$  nonzeros from the condition  $\lambda_c = 1$ . Then if  $\zeta_{t_0}^M = \zeta_{t_0}^{\prime M}$ , the equivalent condition of the false matching is each other user contributes exactly a one in these  $M-1$  ones. It implies  $|\zeta_{t_0}^{\prime M} \cap \zeta_{t_j}^{\prime j}| = 1$  for any  $j \in \{1, 2, \dots, M-1\}$  and some  $t_j$  such that  $c(t_j)$  is matched to  $s_j$ . Then this matching can be checked false or not by seeing whether the above two conditions are satisfied.

Therefore, user  $M$  can also be detected by ruling out the false matching with Algorithm 2, even if it would be totally blocked by other users sometimes. ■

Theorem 8 asserts the existence of UD sequence set which is not UI for any  $M$ . The period is larger than the upper bound presented in Theorem 6. However, UD sequence sets which are not UI may be also a potential direction to make the period shorter. The general construction is still unknown, but some special examples can be found.

**Example 3:** A sequence set which is not UI is given below:

$$\begin{aligned}
s_1 &= [1100] \\
s_2 &= [1010] \\
s_3 &= [1110].
\end{aligned}$$

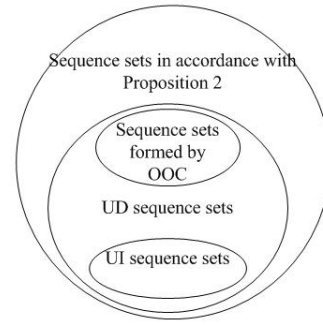


Fig. 1. Relationships between UD sequences and other sequence designs.

One can check this sequence set is UD. The period is smaller compare with Example 2. However, we can find it is in accordance with Proposition 1.

## VI. CONCLUSION

In this paper, we introduce the user-detectability in the design of protocol sequences. Some lower and upper bounds of its minimum period are presented. We also summarize them for large  $M$  as the following:

$$2M^2/9 \leq L_{\min}(M) \leq 2M^2,$$

so there is a gap between the upper and lower bounds. However, they are both of order  $O(M^2)$ .

Moreover, as illustrated in Fig. 1, we displayed some inter-connections between UD sequence set and other research areas in sequence design. This open up many interesting directions for further research.

## REFERENCES

- [1] J. L. Massey, "The capacity of the collision channel without feedback," in *IEEE Int. Symp. Inform. Theory*, Jun. 1982, p. 101.
- [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. 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.
- [4] L. Gyöfi and I. Vajda, "Construction of protocol sequences for multiple-access collision channel without feedback," *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 1762–1765, Sep. 1993.
- [5] W. H. Kautz and R. C. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inform. Theory*, vol. 10, pp. 363–367, Oct. 1964.
- [6] S. Györi, "Coding for a multiple access OR channel: a survey," *Discrete Applied Mathematics*, no. 156, pp. 1407–1430, 2008.
- [7] K. W. Shum, Y. Zhang, and W. S. Wong, "User-irrepressible sequences," in *The 6th Conf. on Sequences and their Applications*, Paris, Sep. 2010.
- [8] 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.
- [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, pp. 1368–1372.
- [10] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1990.
- [11] 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.
- [12] W. Chu and S. W. Golomb, "A new recursive construction for optical orthogonal codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 11, pp. 3072–3076, Nov. 2003.