User-Irrepressible Sequences

Kenneth W. Shum, Yijin Zhang and Wing Shing Wong

Department of Information Engineering,
the Chinese University of Hong Kong,
Shatin, Hong Kong.
{wkshum, zyj007, wswong}@ie.cuhk.edu.hk

Abstract. Protocol sequences are binary and periodic sequences used in multiple-access scheme for collision channel without feedback. Each user reads out the bits from the assigned protocol sequence periodically, and sends a packet whenever the bit is equal to one. It is assumed that any two or more packets overlapping in time result in a collision, and the collided packets are unrecoverable. Due to the lack of feedback and cooperation, there are some relative delay offsets between protocol sequences. We consider protocol sequences with the property, called user-irrepressibility, that each user is guaranteed to send at least one packet in each sequence period without collision, no matter what the delay offsets are. The period length is hence a measure of delay; each user need to wait no more than a period time before a successful transmission can be made. Our objective is to construct user-irrepressible sequences with sequence period as short as possible. In this paper, we present a new construction for prime number of users. A lower bound on period which is applicable in general for any number of users is also derived.

Keywords: Protocol sequences, conflict-avoiding codes, collision channel without feedback.

1 Introduction

We consider packetized multiple-access transmission system in which time is divided into time slots, and assume slot synchronization. A user who wants to transmit a packet must send the packet within a time slot. If exactly one user transmits in a time slot, then the packet is received error-free. However, when two or more users send simultaneously in a time slot, we have a collision and the collided packets are assumed unrecoverable.

We assume that there is no communication among the transmitting nodes. The transmission scheme is thus fully distributed. Also, as argued in [5], information is transmitted via the content of the packets only, but not via the channel access times of the users. The decision of whether transmitting a packet or not

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

in a time slot is independent of the data to be sent. Without loss of generality, the scheduling of packets is done by assigning each user a deterministic binary sequence, call protocol sequence. Each user reads out the bits from the assigned protocol sequence periodically, and sends a packet if and only if the value is equal to one. The users may start their communication at different times. Since we do not assume any feedback from the receiver and cooperation among the users, this incurs relative delay offsets between protocol sequences. We assume that the relative delay offsets of the protocol sequences are arbitrary but fixed throughout the transmission session.

Our design objective, called *user-irrepressibility* [11], is to guarantee in the worst case that each user is able to send at least one packet successfully to the sink node in each period. In other words, no mater what the relative delay offsets are, there is at least one successful packet for each user in each period. This can be re-phrased in terms of the sequence matrix as follow. Given M binary sequences of length L, we cyclically shift each of them and stack them together in an $M \times L$ matrix, one row for each sequence. The sequences are user-irrepressible if no matter what the cyclic shifts are, the resulting $M \times L$ matrix always contains an $M \times M$ identity matrix as a submatrix. The common period of a set of user-irrepressible sequences measures the maximum waiting time until a packet can be sent successfully. This bounded-delay requirement finds application in medical systems [7] and body sensor networks [13] for instance. Let $L_{\min}(M)$ be the smallest L such that a set of M user-irrepressible sequences of common period L exists. Previous work in [2] shows that $L_{\min}(M)$ is lower bounded by $1 + M(M+1)/2$.

The notion of user-irrepressibility is addressed in another context, under the name of *conflict-avoiding codes* (CAC) (see e.g. [4] [6] and the references therein) with different perspective. In the study of CAC, there are T potential users, and at most M of them are active at the same time. Given the sequence period L, the objective in the construction of CAC is to maximize the number of potential users T, with the guarantee of at least one packet received successfully from each active user in a period time, provided that the number of active users is no more than M. In this paper, we consider the case where all users are active, and minimize the period for fixed number of users.

In this paper we assume slot synchronism. If frame synchronization, which is stronger than slot synchronization, is allowed, the problem has a trivial time-division multiple-access (TDMA) solution, namely, the sequence period is $L = M$ and the ith user sends a packet in the ith time slot. Collision can be totally avoided in this case. However, with slot synchronization, the relative delay offsets among sequences are nonzero and uncontrollable.

This paper is organized as follows. After setting up the notations in Section 2, we review some existing constructions of user-irrepressible sequences in Section 3. A new construction of user-irrepressible sequence is given in Section 4. A method for computing a lower bound for $L_{\min}(M)$ is presented in Section 5. The current status of our knowledge on $L_{\min}(M)$ is summarized at the end of this paper.

2 Notations and Preliminaries

We represent a periodic sequence with period L by a sequence of finite length L. We will use "period" and "length" interchangeably. The *Hamming weight* of a binary sequence $a(t)$, denoted by $w_H(a)$, is the number of 1's in a period. The *Hamming cross-correlation* between two sequences $a(t)$ and $b(t)$, denoted by $H_{ab}(\tau)$, is defined as

$$H_{ab}(\tau) := \sum_{t=0}^{L-1} a(t)b(t-\tau).$$

Let $\mathbb{Z}_L = \{0, 1, 2, \ldots, L-1\}$ denote the residues of integer modulo L. Given a binary sequence $s(t)$ of length L, we define the *characteristic set* of $s(t)$ by

$$\mathcal{I}_s := \{t \in \mathbb{Z}_L : s(t) = 1\}.$$

A cyclic shift of a sequence $s(t)$ by τ corresponds to a translation of $\mathcal{I}_s$ by τ in $\mathbb{Z}_L$. Given any subset $\mathcal{A}$ of $\mathbb{Z}_L$, we define the sum of $\mathcal{A}$ and an element x in $\mathbb{Z}_L$ by

$$\mathcal{A} + x := \{a + x \in \mathbb{Z}_L : a \in \mathcal{A}\}.$$

A cyclic shift of $s(t)$ by τ is thus represented by $\mathcal{I}_s + \tau$. The Hamming cross-correlation between two binary sequence s_1 and s_2, with delay offset τ, is equal to the cardinality of

$$\mathcal{I}_{s_1} \cap (\mathcal{I}_{s_2} + \tau).$$

Consider a collection of subsets $\mathscr{S} = \{\mathcal{I}_0, \mathcal{I}_1, \ldots, \mathcal{I}_{M-1}\}$ of $\mathbb{Z}_L$. This specifies a set of M binary sequences $\{s_0(t), s_1(t), \ldots, s_{M-1}(t)\}$ by letting the ith subset $\mathcal{I}_i$ in $\mathscr{S}$ be the characteristic set of $s_i(t)$. We say that $\mathcal{I}_i$ is *cyclically covered* by the other sets in $\mathscr{S}$ if we can find some integers τ_j, for $j \in \{1, 2, \ldots, M-1\} \setminus \{i\}$, such that

$$\mathcal{I}_i \subseteq \bigcup_{j \neq i} (\mathcal{I}_j + \tau_j)$$

The sequence $s_i(t)$ corresponding $\mathcal{I}_i$ is then said to be *blocked* by the other sequences. If there is a set in $\mathscr{S}$ which is cyclically covered by the others, or equivalently if there is a sequence which is blocked by the other sequences, we say that $\mathscr{S}$ is *user-repressible*. Otherwise, $\mathscr{S}$ is said to be *user-irrepressible* (UI). We use $\mathsf{UIS}(L, M)$ to denote a collection of M user-irrepressible subsets in $\mathbb{Z}_L$. We will abuse notation and use $\mathsf{UIS}(L, M)$ for the corresponding set of binary sequences as well.

UI sequences are related to another combinatorial structure called cover-free family [3]. A collection of sets $\mathscr{F}$ is called *r-cover-free* if $\mathcal{F}_0 \not\subset \mathcal{F}_1 \cup \mathcal{F}_2 \cup \ldots \cup \mathcal{F}_r$ for all $\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_r \in \mathscr{F}$ ($\mathcal{F}_i \neq \mathcal{F}_j$ if $i \neq j$). A collection of M binary sequences is UI if for all possible choices of delay offsets τ_i, the translated characteristic sets $\mathcal{I}_i + \tau_i$, for $i = 0, 1, \ldots, M-1$, form an $(M-1)$-cover-free family.

As a “non-example”, consider the following three sequences of length 7:

$$\begin{aligned} s_1(t) &: 1110000 \\ s_2(t) &: 1010100 \\ s_3(t) &: 1001001 \end{aligned}$$

The first sequence $s_1(t)$ can be blocked by $s_2(t)$ and $s_3(t)$, because $\mathcal{I}_1 = \{0, 1, 2\}$ is contained in

$$\mathcal{I}_2 \cup (\mathcal{I}_3 + 1) = \{0, 1, 2, 4\}.$$

These three binary sequences are hence not UI.

A sequence set is said to be *constant-weight* if all sequences have the same Hamming weight. A constant-weight UI sequence set with Hamming weight w is denoted by $\mathsf{UIS}(L, M, w)$. Several existing constructions of constant-weight UI sequences are reviewed in the next section. A new construction of non-constant-weight UI sequences will be described in Section 4.

3 Known Constructions of UI Sequences

Shift-Invariant Sequences (SIS). Shift-invariant sequences are studied in [5] as an essential ingredient for achieving the capacity of the collision channel without feedback. This class of protocol sequences has the property that all Hamming cross-correlation functions of order two or higher are constant. From the construction of SIS, we obtain constant-weight $\mathsf{UIS}(2^M, M, 2^{M-1})$ for $M \geq 2$. For example, the following are three constant-weight UI sequences which are shift-invariant:

$$\begin{aligned} s_0(t) &: 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0, \\ s_1(t) &: 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0, \\ s_2(t) &: 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0. \end{aligned}$$

However, it is proved in [9] that the period of SIS increases exponentially as a function of the number of users. Shift-invariant sequences are of practical interests only when the small number of users is small.

Extended Prime Sequences (EPS). For prime p, a construction of constant-weight $\mathsf{UIS}(p(2p-1), p, p)$ is given in [12]. Let $[x \bmod p]$ denote the unique integer between 0 and $p - 1$ such that

$$x = qp + [x \bmod p]$$

holds for some integer q. For $g = 1, 2, \dots, p$, the gth extended prime sequence is defined by setting the characteristic set of the gth sequence to

$$\mathcal{I}_g = \{j(2p - 1) + [gj \bmod p] : j = 0, 1, \dots, p - 1\}.$$

It can be shown that the Hamming cross-correlation between two distinct EPS is at most one. As the Hamming weight of each sequence is p, this implies that the extended prime sequences enjoy the UI property.

CRT Sequences. Given a positive integer M, let p be the smallest prime number which is larger than or equal to M. A constant-weight $\mathsf{UIS}(p(2M-1), M, M)$ can be constructed as follows. By Bertrand's postulate [1, Chapter 2], p can be chosen between M and $2M-2$, and hence p and $2M-1$ are relatively prime. We apply Chinese remainder theorem (CRT) and identify $\mathbb{Z}_{p(2M-1)}$ with the direct sum $\mathbb{Z}_p \oplus \mathbb{Z}_{2M-1}$; the bijection $\varphi : \mathbb{Z}_{p(2M-1)} \to \mathbb{Z}_p \oplus \mathbb{Z}_{2M-1}$ is given by

$$\varphi(x) := (x \bmod p, x \bmod 2M-1).$$

For $g = 1, 2, \ldots, p$, the gth sequence is defined by setting the corresponding characteristic set to

$$\mathcal{I}_g = \{t \in \mathbb{Z}_L : \varphi(t) = (jg \bmod p, j), j = 0, 1, \ldots, M-1\}.$$

It is shown in [10] that the Hamming cross-correlation between two distinct CRT sequences is at most one. This guarantees that the constructed sequences are UI.

4 A New Construction Based on CRT for Prime Number of Users

We present a variation of the CRT construction in this section. Even though the two constructions look similar, the proof of user-irrepressibility is very different. The new sequences are not constant-weight, and are shorter than the extended prime sequences with the same number of users.

Let p be an odd prime. Since p and $2p-2$ are relatively prime, by the Chinese remainder theorem, there is an isomorphism θ from $\mathbb{Z}_{p(2p-2)}$ to $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$, given by

$$\theta(t) := (t \bmod p, t \bmod 2p-2).$$

We will henceforth identify $\mathbb{Z}_{p(2p-2)}$ with $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. The new class of UI sequences is specified by the corresponding characteristic sets in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. For $g = 0$, let

$$\mathcal{I}_0 = \{(i, 0) : i = 0, 1, \ldots, p-1\}, \tag{1}$$

and for $g = 1, \ldots, p-1$, let

$$\mathcal{I}_g = \{(gj \bmod p, j) : j = 0, 1, 2, \ldots, p\}. \tag{2}$$

This produces p sequences of length $p(2p-2)$. The first sequence is of weight p, and the remaining sequences are of weight $p+1$. We call this construction CRT_p, and distinguish it from the previous CRT construction by subscript "$_p$".

A cyclic shift of a sequence by τ corresponds to adding $\theta(\tau)$ to the corresponding characteristic set. We will use the notation

$$\mathcal{I}_g + (a, b) := \{(x, y) + (a, b) : (x, y) \in \mathcal{I}_g\},$$

with the addition carried out in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. We note that the sets in (1) and (2) are arithmetic progressions in $\mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$. For $(x, y) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ and integers

$k_1 \leq k_2$, we will use $(x, y) \cdot [k_1, k_2]$ to represent an arithmetic progression with common difference (x, y),

$$\{(k_1x, k_1y), ((k_1 + 1)x, (k_1 + 1)y), \dots, (k_2x, k_2y)\}.$$

In this notation, the characteristic sets in (1) and (2) are $(1, 0) \cdot [0, p - 1]$ and $(g, 1) \cdot [0, p]$.

Lemma 1. *For each $(a, b) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ and $h = 1, 2, \dots, p-1$, $(1, 0) \cdot [0, p-1]$ and $(h, 1) \cdot [0, p] + (a, b)$ contains at most one common element.*

Proof. If $(i, 0) = (hj + a, j + b)$, for some $i = 0, 1, \dots, p - 1$ and $j = 0, 1, \dots, p$, then by equating the second components, the value of j is uniquely determined by $j = -b \bmod 2p-2$. The value of i is then uniquely determined as well by equating the first components. This shows that if $(1, 0) \cdot [0, p]$ and $(h, 1) \cdot [0, p - 1] + (a, b)$ have nonempty intersection, the intersection contains exactly one element. □

Lemma 2. *For each $(a, b) \in \mathbb{Z}_p \oplus \mathbb{Z}_{2p-2}$ and distinct g and h in $\{1, 2, \dots, p-1\}$, $(g, 1) \cdot [0, p]$ and $(h, 1) \cdot [0, p] + (a, b)$ contains at most two common elements.*

Proof. Suppose that there are two or more common elements in $(g, 1) \cdot [0, p]$ and $(h, 1) \cdot [0, p] + (a, b)$. Let A and B be two of them. We have

$$A = (gj_1, j_1) = (hj'_1 + a, j'_1 + b) \tag{3}$$
$$B = (gj_2, j_2) = (hj'_2 + a, j'_2 + b) \tag{4}$$

for some $j_1, j_2, j'_1, j'_2 \in \{0, 1, \dots, p\}$, $j_1 \neq j_2$ and $j'_1 \neq j'_2$.

Let $\delta := j_2 - j_1$ and $\delta' := j'_2 - j'_1$. Both δ and δ' assume value in the following range

$$\{-p, -(p - 1), \dots, -2, -1\} \cup \{1, 2, \dots, p - 1, p\}. \tag{5}$$

By interchanging the values of j_1 and j_2 if necessary, we consider only $\delta \in \{1, 2, \dots, p\}$ without loss of generality.

After subtracting (3) from (4) and equating the two components, we obtain the following system of modular equations

$$g\delta = h\delta' \bmod p, \tag{6}$$
$$\delta = \delta' \bmod 2p - 2. \tag{7}$$

For $\delta = 1, 2, \dots, p - 3$, (6) and (7) have no common solution. Indeed, the only δ' in the range of (5) which equals $\delta \bmod 2p - 2$ is $\delta' = \delta$, and from (6), we obtain $(g - h)\delta = 0 \bmod p$, which contradicts the assumption that $g \neq h$.

For $\delta = p - 2$, (6) and (7) also have no common solution. In this case, δ' is equal to either $p - 2$ and $-p$ by (7). The possibility of $\delta' = p - 2$ is forbidden because otherwise we would obtain the contradiction $g = h$ from (6). On the other hand, if $\delta' = -p$, we get $g(p - 2) = 0 \bmod p$ from (6), which implies that $g = 0 \bmod p$. Again, we arrive at a contradiction.

In the following, we consider the two remaining cases: $\delta = p$ and $\delta = p - 1$.

(i) Suppose $\delta = p$. The value of δ' is equal to either p or $-(p-2)$ by (7). The latter is not feasible, because after substituting $\delta = p$ and $\delta' = -(p-2)$ into (6), we obtain

$$0 = -h(p-2) \bmod p,$$

which contradicts the assumption that h is nonzero. Hence, we must have $\delta' = \delta = p$. Since the range of j_1, j_2, j_1' and j_2' is $\{0, 1, \dots, p\}$, we obtain $j_1 = j_1' = 0$, and $j_2 = j_2' = p$. By substituting $j_1 = j_1' = 0$ into (3), we thus get $a = b = 0$. This solution is tabulated in the first row of Table 1.

(ii) Suppose $\delta = p-1$. The values of δ' which satisfy (7) are $\pm(p-1)$. We cannot have $\delta' = p-1$, because it implies $g = h \bmod p$ by (6). The only choice of δ' is thus $\delta' = -(p-1)$. In this case, we have $\delta = -\delta'$ and $g = -h \bmod p$. Since $\delta = p-1$, the corresponding pairs of j_1 and j_2 are (a) $j_1 = 0$ and $j_2 = p-1$, and (b) $j_1 = 1$ and $j - 2 = p$. Likewise, since $\delta = -(p-1)$, the corresponding pairs of j_1' and j_2' are (a') $j_1' = p-1$ and $j_2' = 0$ and (b') $j_1' = p$ and $j_2' = 1$. The four different combinations are summarized in the last four rows of Table 1.

As h is between 1 and $p-1$, each pair of (a, b) in the last two columns of Table 1 are distinct. For fixed values of a and b, if $(gj, j) = (hj' + a, j' + b)$ has two solutions (j_1, j_1'), (j_2, j_2'), they must be associated with one of the rows in Table 1. Therefore, $(g, 1) \cdot [0, p]$ and $(h, 1) \cdot [0, p] + (a, b)$ contain exactly two common elements for precisely five different combinations of a and b listed in Table 1. This excludes the possibility of having three or more common elements. □

j_1	j_2	j_1'	j_2'	$a \bmod p$	$b \bmod 2p-2$
0	p	0	p	0	0
0	$p-1$	$p-1$	0	h	$p-1$
0	$p-1$	p	1	0	$p-2$
1	p	$p-1$	0	0	p
1	p	p	1	$-h$	$p-1$

Table 1. Solutions to (3) and (4)

Lemmas 1 and 2 show that the Hamming cross-correlation of two sequences from the CRT$_p$ is either 0, 1 or 2. In fact, if $h = -g \bmod p$, the number of occurrences of 2 as a cross-correlation value is exactly five. For distinct h and g in $\{1, 2, \dots, p-1\}$ such that $h \neq -g \bmod p$, only the first row in Table 1 is feasible, and the Hamming cross-correlation equals 2 when and only when the relative delay offset is zero.

Theorem 1. *For prime number p, the sequences from the CRT$_p$ construction form a UIS$(2p(p-1), p)$.*

Proof. Let $\mathcal{I}_i$, $i = 0, 1, \dots, p-1$, be the characteristic set from the CRT$_p$ construction, and τ_i be the relative delay offsets.

Consider the first sequence, which is represented by $\mathcal{I}_0$. By Lemma 1, $\mathcal{I}_0$ and $\mathcal{I}_h + \theta(\tau_h)$ have at most one common elements, for $h = 1, 2, \ldots, p-1$. Since $\mathcal{I}_0$ contains p elements and there are only $p-1$ other users, we can find an element in $\mathcal{I}_0$ which is not contained in $\bigcup_{h=1}^{p-1}(\mathcal{I}_h + \theta(\tau_h))$. Hence $\mathcal{I}_0$ cannot be cyclically covered no matter how the delay offsets are chosen.

Next, we show that for each $g \in \{1, 2, \ldots, p-1\}$, $\mathcal{I}_g$ cannot be cyclically covered by the others. Suppose without loss of generality that $\tau_g = 0$. Let $\bar{g}$ denote $-g \bmod p$. We have seen in the proof of Lemma 2 that $\mathcal{I}_{\bar{g}}$ is the only one whose translates can overlap $\mathcal{I}_g$ with intersection other than $(0, 0)$ and $(0, p)$.

Let $\mathscr{J}$ denote $\mathcal{I}_g \cap (\mathcal{I}_{\bar{g}} + (\theta(\tau_{\bar{g}})))$. We consider two cases.

(i) $|\mathscr{J}| = 0, 1$. Let

$$\mathscr{A} := \{h \in \{0, 1, \ldots, p-1\} \setminus \{g\} : \big|\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h))\big| = 2\},$$

and $\mathscr{B}$ be $\{0, 1, \ldots, p-1\} \setminus (\{g\} \cup \mathscr{A})$. In other words, $\mathscr{A}$ (resp. $\mathscr{B}$) corresponds to the set of sequences whose Hamming cross-correlation with s_g is equal to two (resp. one). By assumption, we have $\bar{g} \in \mathscr{B}$. For all $h \in \mathscr{A}$, we have

$$\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)) = \{(0, 0), (0, p)\}.$$

(the first row in Table 1). Then

$$\Big|\mathcal{I}_g \cap \bigcup_{h \neq g} (\mathcal{I}_h + \theta(\tau_h))\Big| \leq \Big| \bigcup_{h \in \mathscr{A}} (\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)))\Big| + \Big| \bigcup_{h \in \mathscr{B}} (\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h)))\Big|.$$

If $\mathscr{A}$ is empty, then the first term on the right hand side is zero, and the second term is no more than $p-1$. If $\mathscr{A}$ is not empty, then the first term is equal to two, and the second term is no more than $p-2$. In any case, the sum on the right hand side does not exceed p. Since $|\mathcal{I}_g| = p+1$, we see that $\mathcal{I}_g$ is not contained in $\bigcup_{h \neq g}(\mathcal{I}_h + \theta(\tau_h))$.

(ii) $|\mathscr{J}| = 2$. In this case, $\mathscr{J}$ equals either $\{(0, 0), ((p-1)g, p-1)\}$, or $\{(g, 1), (0, p)\}$ (the last four rows in Table 1). For $h \notin \{g, \bar{g}\}$, we claim that

$$|(\mathcal{I}_g \setminus \mathscr{J}) \cap (\mathcal{I}_h + \theta(\tau_h))| \leq 1. \tag{8}$$

If $|\mathcal{I}_g \cap (\mathcal{I}_h + \theta(\tau_h))| = 1$, then (8) follows immediately. Otherwise, if $\mathcal{I}_g$ and $\mathcal{I}_h + \theta(\tau_h)$ have two elements in common, then these two elements are $(0, 0)$ and $(0, p)$ (the first row in Table 1). Either $(0, 0)$ or $(0, p)$ is in common with $\mathscr{J}$. This implies

$$|(\mathcal{I}_g \setminus \mathscr{J}) \cap (\mathcal{I}_h + \theta(\tau_h))| = 1$$

and finishes the proof of the claim. Hence,

$$\Big|\mathcal{I}_g \cap \bigcup_{h \neq g} (\mathcal{I}_h + \theta(\tau_h))\Big| \leq |\mathscr{J}| + \Big| \bigcup_{h \neq \{g, \bar{g}\}} (\mathcal{I}_g \setminus \mathscr{J}) \cap (\mathcal{I}_h + \theta(\tau_h))\Big|.$$

As the second term on the right hand side is no more than $p-2$, we see that the sum is less than or equal to p. Since $|\mathcal{I}_g| = p+1$, this completes the proof that $\mathcal{I}_g$ cannot be cyclically covered. □

Example: Let $p = 7$. The CRT_p construction produces a set of seven UI sequences of period 84. The characteristic sets are:

$$\begin{aligned}
\mathcal{I}_0 &= \{0, 12, 24, 36, 48, 60, 72\}, & \mathcal{I}_1 &= \{0, 1, 2, 3, 4, 5, 6, 7\}, \\
\mathcal{I}_2 &= \{0, 7, 17, 27, 37, 54, 64, 74\}, & \mathcal{I}_3 &= \{0, 7, 18, 29, 40, 51, 62, 73\}, \\
\mathcal{I}_4 &= \{0, 7, 16, 25, 41, 50, 66, 75\}, & \mathcal{I}_5 &= \{0, 7, 15, 30, 38, 53, 61, 76\}, \\
\mathcal{I}_6 &= \{0, 7, 13, 26, 39, 52, 65, 78\}.
\end{aligned}$$

The period of UI sequences obtained by construction CRT_p is shorter than the period from EPS. The shortest known periods of UI sequences, for $M = 1, 2, \ldots, 12$, are shown in Table 2 in the next section.

Remark: We can generalize the construction in (2) by defining

$$\mathcal{I}_g := \{(gj \bmod p, fj \bmod q) : j = 0, 1, 2, \ldots, p\}$$

for some integer f which is relatively prime with q. It can be proved in a similar way that the resulting sequences are UI. The original construction is a special case with $f = 1$.

5 Lower bound on period

The property of user-irrepressibility can be interpreted as a two-person game. Player 1 writes down a set of M binary sequences of length L. Then Player 2 tries to adjust the delay offsets and block one of the sequences. If Player 2 succeeds in doing so, the binary sequences are not UI, otherwise, the Player 1 wins and the binary sequences are UI. In this section, we describe a greedy algorithm for Player 2, called *blocking algorithm*, and derive a sufficient condition under which Player 2 has a sure win, no matter what Player 1 writes down in the first place. Under this condition, one of the protocol sequence is blocked by the others, and hence the sequence set cannot be UI. This gives a lower bound on the period of UI sequences.

Blocking algorithm

Inputs: A set of M binary sequences of length L, $s_0(t)$, $s_1(t), \ldots, s_{M-1}(t)$.

(1) Re-label the sequences so that the Hamming weight of $s_0(t)$ is smallest among the M binary sequences. Set $k = 1$.

(2) Cyclically shift $s_k(t)$ so that the Hamming cross-correlation between $s_0(t)$ and $s_k(t)$ is maximal.

(3) Set the 1's in $s_0(t)$ which overlap with the shifted version of $s_k(t)$ to zero.

(4) If $k < M - 1$, increment k by one and go back to step (2).

If all of the 1's in $s_0(t)$ is removed after the termination of the blocking algorithm, then $s_0(t)$ is blocked and Player 2 wins.

Theorem 2. *Let $s_0(t), s_1(t), \ldots, s_{M-1}(t)$ be M binary sequences of length L. Suppose s_0 has the smallest Hamming weight, i.e., $w_H(s_0) = w$ and $w_H(s_i) \geq w$ for $i = 1, \ldots, M-1$. Define an integer sequence $(r_k(w,L))_{k=0}^{\infty}$ recursively by*

$$r_0(w,L) := w \tag{9}$$

$$r_k(w,L) := r_{k-1}(w,L) - \left\lceil \frac{w}{L} r_{k-1}(w,L) \right\rceil, \quad \textit{for } k \geq 1. \tag{10}$$

If $r_{M-1}(w,L) = 0$, then $s_0(t)$ is blocked by $s_1(t)$, $s_2(t), \ldots, s_{M-1}(t)$.

Proof. We will use the following fact: For two binary sequences $a(t)$ and $b(t)$ of period L and Hamming weight $w_H(a)$ and $w_H(b)$, we have

$$\sum_{\tau=0}^{L-1} H_{ab}(\tau) = w_H(a) w_H(b). \tag{11}$$

The proof of this fact is straightforward, and can be found in [8].

Let $x_0(t)$ be the sequence $s_0(t)$. We will recursively define $M-1$ sequences $x_1(t), x_2(t), \ldots, x_{M-1}(t)$, and prove by induction that $w_H(x_k) = r_k(w,L)$, for $k = 1, 2, \ldots, M-1$. The sequence $x_k(t)$ corresponds to what we get after step (3) in the blocking algorithm. Note that the Hamming weight of $x_0(t)$ is equal to $r_0(w,L) = w$. Because $w_H(x_0) = w$ and $w_H(s_1) \geq w$, from (11), we obtain

$$\frac{1}{L} \sum_{\tau=0}^{L-1} H_{x_0 s_1}(\tau) = \frac{w_H(x_0) w_H(s_1)}{L} \geq \frac{w^2}{L}.$$

The mean Hamming cross-correlation, averaged over all τ, is no less than w^2/L. We pick a delay offset for $s_1(t)$, say τ_1, so that $H_{x_0 s_1}(\tau_1) \geq \lceil w^2/L \rceil$, and define a binary sequence $x_1(t)$ by removing $\lceil w^2/L \rceil$ 1's from $x_0(t)$ which overlap with the 1's in the shifted version of $s_1(t)$. Here we slightly modify the blocking algorithm; in order to make the analysis more tractable, the number of 1's we take away from $x_0(t)$ is *exactly* $\lceil w^2/L \rceil$, instead of the maximal Hamming cross-correlation between $x_0(t)$ and $s_1(t)$. After the first step, we have $w_H(x_1) = w - \lceil w^2/L \rceil = r_1(w,L)$.

Given $x_{k-1}(t)$, we recursively define $x_k(t)$ in a similar fashion. In the kth step, we have

$$\frac{1}{L} \sum_{\tau=0}^{L-1} H_{x_{k-1} s_k}(\tau) = \frac{w_H(x_{k-1}) w_H(s_k)}{L} \geq \frac{r_{k-1}(w,L) \cdot w}{L}.$$

We can find a particular cyclic shift of $s_k(t)$ so that the Hamming cross-correlation between x_{k-1} and s_k is at least $\lceil \frac{w}{L} r_{k-1}(w,L) \rceil$. We remove exactly $\lceil \frac{w}{L} r_{k-1}(w,L) \rceil$ 1's in x_{k-1} which overlap with the shifted version of $s_k(t)$, and call the resulting sequence $x_k(t)$. Again, the total number of overlapping 1's may be more than $\lceil \frac{w}{L} r_{k-1}(w,L) \rceil$ but we only remove $\lceil \frac{w}{L} r_{k-1}(w,L) \rceil$ of them. After the kth step, we have $w_H(x_k) = r_k(w,L)$.

If $r_{M-1}(w,L)$ is zero, then there is no more 1 in $x_{M-1}(t)$. In this case, $s_0(t)$ is blocked by $s_1(t)$, $s_2(t), \ldots, s_{M-1}(t)$. □

We apply Theorem 2 several times, once for each $w \in \{1, 2, \dots, L\}$. If $r_{M-1}(w, L)$ is zero for all $w = 1, 2, \dots, L$, then for any M sequences of length L, the blocking algorithm can always succeed in blocking one of the sequences. We thus have the following necessary condition for the existence of UI sequences.

Theorem 3. *Let $r_k(w, L)$ be defined by* (9) *and* (10)*. If $r_{M-1}(w, L) = 0$ for $w = 1, 2, \dots, L$, and $L \leq L_0$, then $\mathsf{UIS}(L_0, M)$ does not exist, i.e., $L_{\min}(M)$ is strictly larger than L_0.*

As an example, we consider the case when $M = 3$. We tabulate $r_2(w, L)$ in the following table.

L	$r_2(1,L)$	$r_2(2,L)$	$r_2(3,L)$	$r_2(4,L)$	$r_2(5,L)$	$r_2(6,L)$	$r_2(7,L)$	$r_2(8,L)$
1	0							
2	0	0						
3	0	0	0					
$\vdots$	$\vdots$	$\vdots$	$\vdots$					
7	0	0	0	0	0	0	0	
8	0	0	0	1	0	0	0	0

The value of $r_2(w, L)$ is zero for all w when L is less than or equal to 7. The first non-zero entry occurs when $L = 8$ and $w = 4$, and $r_2(4, 8)$ is equal to one. By Theorem 3, we conclude that $L_{\min}(3) \geq 8$. In fact, a set of three UI sequences of length eight exists and is exhibited in Section 3. Therefore, $L_{\min}(3) = 8$. Furthermore, since $r_2(w, 8)$ is positive only when $w = 4$, the smallest Hamming weight in an $\mathsf{UIS}(8, 3)$ must be equal to four. The protocol sequences in the example in Section 3 indeed have Hamming weight equal to four.

We investigate the integer sequence $(r_k(w, L))_{k=0}^{\infty}$ defined in (9) and (10) in more details. We observe that for any fixed w and L, the value of $r_k(w, L)$ is monotonically decreasing as k increases, and stabilizes at 0 eventually. For instance, if $w \leq \sqrt{L}$, then $\lceil w r_k(w, L)/L \rceil = 1$ for $k = 0, 1, \dots, w-1$. The integer sequence $(r_k(w, L))_{k=0}^{\infty}$ in this case is

$$w,\ w-1,\ w-2, \dots, 3,\ 2,\ 1,\ 0,\ 0,\ \dots.$$

Suppose that w is in the range $\sqrt{L} < w \leq \sqrt{2L}$. The decrease of Hamming weight after a step in the blocking algorithm is equal to two whenever

$$r_{k-1}(w, L) - r_k(w, L) = \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil = 2.$$

This happens when $1 < (w/L) \cdot r_{k-1}(w, L) \leq 2$. The integer sequence $(r_k(w, L))_{k=0}^{\infty}$ for $\sqrt{L} < w \leq \sqrt{2L}$ is

$$\underbrace{w,\ w-2,\ \dots, n_1+2}_{n_2},\ \underbrace{n_1,\ n_1-1,\ \dots,\ 1}_{n_1},\ 0, \dots,$$

where n_1 and n_2 denote the number of terms with a step size of -1 and -2 respectively. We note that $n_1 + 2n_2 = w$.

In general, we have the following

Theorem 4. *Let $w \leq L$ be fixed integers, and α be $\lceil w^2/L \rceil$. Then*

$$r_{M-1}(w,L) > 0 \textit{ implies } M \leq \frac{w}{\alpha} + \frac{L}{w}\sum_{i=2}^{\alpha}\frac{1}{i}.$$

Proof. In this proof, we simplify notation and write r_k instead of $r_k(w,L)$. For $i = 1, 2, \ldots, \alpha$, let n_i be number of integers r_k in $(r_k)_{k=0}^{\infty}$ such that $r_k - r_{k+1} = i$. The integers n_1, $n_2, \ldots, n_\alpha$ satisfy the relation

$$n_1 + 2n_2 + 3n_3 + \ldots + \alpha n_\alpha = w. \tag{12}$$

Now, consider the terms r_k in $(r_k)_{k=0}^{\infty}$ which satisfy $r_k - r_{k+1} = i$, i.e.,

$$r_k - r_{k+1} = \lceil w r_k / L \rceil = i.$$

We obtain from the last equality that $wr_k/L > i - 1$. Therefore, the r_k's which satisfy $r_k - r_{k+1} = i$ must lie in the range

$$(i-1)\frac{L}{w} < r_k \leq w - \sum_{j=i+1}^{\alpha} jn_j. \tag{13}$$

Furthermore, if r_{k_i} is the smallest r_k in $(r_k)_{j=0}^{\infty}$ such that $r_{k_i} - r_{k_i+1} = i$, then $r_{k_i-1} \leq (i-1)L/w < r_{k_i}$.

The range in (13) may be empty, in which case there is no r_k which satisfies $r_k - r_{k+1} = i$ and $n_i = 0$. If it is not empty, then

$$n_i \geq \frac{1}{i}\Big(\big(w - \sum_{j=i+1}^{\alpha} jn_j\big) - (i-1)\frac{L}{w}\Big),$$

since the difference between two adjacent r_k's in this range is precisely i. We simplify the above inequality to

$$(i-1)\frac{L}{w} + \sum_{j=i}^{\alpha} jn_j \geq w. \tag{14}$$

Inequality (14) is valid for $i = 1, 2, \ldots, \alpha$, and reduces to (12) when $i = 1$.

For $i = 2, 3, \ldots, \alpha$, divide both sides of (14) by $i(i-1)$, and add the resulting inequalities,

$$\sum_{i=2}^{\alpha}\frac{L}{iw} + \sum_{i=2}^{\alpha}\sum_{j=i}^{\alpha}\frac{jn_j}{i(i-1)} \geq \sum_{i=2}^{\alpha}\frac{w}{i(i-1)}. \tag{15}$$

After exchanging the order of the double summation, we can rewrite (15) as

$$\sum_{i=2}^{\alpha}\frac{L}{iw} + \sum_{j=2}^{\alpha} n_j(j-1) \geq w\Big(1 - \frac{1}{\alpha}\Big)$$

$$w - \sum_{j=2}^{\alpha} n_j(j-1) \leq \frac{w}{\alpha} + \frac{L}{w}\sum_{i=2}^{\alpha}\frac{1}{i}.$$

We replace w on the left hand side by $\sum_{j=1}^{\alpha} jn_j$, and obtain

$$\sum_{j=1}^{\alpha} n_j \leq \frac{w}{\alpha} + \frac{L}{w}\sum_{i=2}^{\alpha}\frac{1}{i}. \tag{16}$$

The theorem follows by noting that $M \leq \sum_{j=1}^{\alpha} n_j$. □

For positive integer n, let the nth harmonic number be denoted by $H_n := \sum_{i=1}^{n} 1/i$, and let $F : \mathbb{R}_+ \to \mathbb{R}_+$ be a function defined as

$$F(x) := \frac{x}{k} + \frac{H_k - 1}{x} \quad \text{for } \sqrt{k-1} < x \leq \sqrt{k},\ k = 1, 2, 3, \ldots.$$

Although $F(x)$ is defined in a piece-wise manner, it can be shown that $F(x)$ is a continuous function, i.e., it is continuous at $x = \sqrt{k}$ for $k = 1, 2, 3, \ldots$

In terms of $F(x)$, Theorem 4 can be re-phrased as

$$r_{M-1}(w, L) > 0 \text{ implies } M \leq \sqrt{L}F(w/\sqrt{L}).$$

Indeed, as $\alpha - 1 < w^2/L \leq \alpha$, the right hand side of (16) can be written as

$$\sqrt{L}\Big(\frac{w}{\sqrt{L}\alpha} + \frac{\sqrt{L}}{w}\sum_{i=2}^{\alpha}\frac{1}{i}\Big) = \sqrt{L}\Big(\frac{w}{\sqrt{L}\alpha} + \frac{\sqrt{L}}{w}(H_\alpha - 1)\Big) = \sqrt{L}\cdot F(w/\sqrt{L}).$$

One can show by calculus that the function $F(x)$ attains global maximum at $x = \sqrt{2}$, with maximal value $F(\sqrt{2}) = 3/\sqrt{8}$. If a $\mathsf{UIS}(L, M)$ exists, then from Theorem 2 we know that $r_{M-1}(w, L)$ is positive for some w, and from Theorem 4, we have $M \leq \sqrt{L}F(w/\sqrt{L}) \leq \sqrt{L}(3/\sqrt{8})$. We have thus proved the following

Theorem 5. $L_{\min}(M) \geq \lceil 8M^2/9 \rceil$.

Theorem 5 improves upon the previous lower bound $1 + M(M-1)/2$ from [10].

The calculations as described in Theorem 3 have been automated by a computer program, and the resulting lower bounds on the period of UI sequences for $M = 2, 3, \ldots, 13$ are tabulated in the third column in Table 2. The value of $\lceil 8M^2/9 \rceil$ is shown in the second column. We can observe that the lower bounds obtained by Theorem 3 coincide with those by Theorem 5 very often. In fact, one can show by a more detailed analysis that the two lower bounds yield the same value when M is a multiple of 3. In the last column in Table 2, we list the shortest known period of UI sequences. The known periods in the first five entries come from the class of shift-invariant sequences. For seven or more users, CRT and CRT$_p$ give the shortest known period.

6 Conclusion

A new construction of UI sequences when the number of users is a prime integer is devised. The sequence length of the new construction increases asymptotically like $2M^2$. Also, a lower bound of $8M^2/9$ is proved in this paper. Closing the gap between the upper and lower bound for $L_{\min}(M)$ is an interesting direction for future work.

M	$\lceil 8M^2/9 \rceil$	$L_{\min}(M)$	Known period
2	4	4	4 (SIS)
3	8	8	8 (SIS)
4	15	≥ 15	16 (SIS)
5	23	≥ 24	32 (SIS)
6	32	≥ 32	64 (SIS)
7	44	≥ 44	84 (CRT_p)
8	57	≥ 60	165 (CRT)
9	72	≥ 72	187 (CRT)
10	89	≥ 90	209 (CRT)
11	108	≥ 108	220 (CRT_p)
12	128	≥ 128	299 (CRT)
13	151	≥ 152	312 (CRT_p)

Table 2. Lower bound on the minimum period of user-irrepressible sequences and periods of known user-irrepressible sequences. (It can be proved that there is no $\mathsf{UIS}(15, 4)$ by a separate argument and thus $L_{\min}(4) = 16$)

References

1. M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, New York, 3rd edition, 2004.
2. C. S. Chen, K. W. Shum, C. W. Sung, W. S. Wong, and G. E. Øien. User unsuppressible protocol sequences for collision channel without feedback. In *Proc. IEEE Int. Symp. Inform. Theory and its Applications*, pages 1213–1218, Auckland, December 2008.
3. P. Erdős, P. Frankl, and Z. Füredi. Family of finite sets in which no set is covered by the union of r others. *Israel J. of Math.*, 51(1-2):79–89, 1985.
4. 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*, 53:2732–2742, August 2007.
5. J. L. Massey and P. Mathys. The collision channel without feedback. *IEEE Trans. Inform. Theory*, 31(2):192–204, March 1985.
6. K. Momihara, M. Müller, J. Satoh, and M. Jimbo. Constant weight conflict-avoiding codes. *SIAM J. Discrete Math.*, 21(4):959–979, 2007.
7. U. Roedig, A. Barroso, and C. J. Sreenan. f-MAC: A deterministic media access control protocol without time synchronization. In K. Römer, H. Karl, and F. Mattern, editors, *3rd European Workshop on Wireless Sensor Networks*, number 3868 in Lecture Notes in Computer Science, pages 276–291, Berlin, 2006. Springer-Verlag.
8. D. V. Sarwate and M. B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proc. IEEE*, 68(5):593–619, 1980.
9. 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*, 55:3312–3322, July 2009.
10. 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*, pages 1368–1372, Seoul, June 2009.
11. W. S. Wong. New protocol sequences for random access channels without feedback. *IEEE Trans. Inform. Theory*, 53(6):2060–2071, June 2007.
12. G.-C. Yang and W. C. Kwong. Performance analysis of optical CDMA with prime codes. *IEE Electron. Lett.*, 31(7):569–570, March 1995.
13. G.-Z. Yang, editor. *Body Sensor Networks*. Springer-Verlag, London, 2006.