New user-irrepressible sequences for a collision channel without feedback

Yijin Zhang · Yuan-Hsun Lo · Kenneth W. Shum · Wing Shing Wong

Received: date / Accepted: date

Abstract Protocol sequences are binary and periodic sequences used for deterministic multiple access in a collision channel without feedback. In this paper, we focus on user-irrepressible (UI) protocol sequences that can guarantee a positive individual throughput per sequence period with probability one for a slot-synchronous channel, regardless of the delay offsets among the users. As the sequence period has a fundamental impact on the worst-case channel access delay, a common objective of designing UI sequences is to make the sequence period as short as possible. Consider a communication channel that is shared by $M$ active users, and assume that each protocol sequence has a constant Hamming weight $w$. To attain a better delay performance than previously known UI sequences, this paper presents a CRTm construction of UI sequences with $w = M + 1$. For all non-prime $M \geq 8$, our construction produces the shortest known sequence period and the shortest known worst-case delay of UI sequences. It is further shown that the new construction not
only enjoys a better average delay performance, but also has a higher average system throughput than other constructions which have the same sequence period. In addition, we derive an asymptotic lower bound on the minimum sequence period for $w = M + 1$ if the sequence structure satisfies some technical conditions, called equi-difference, and prove the tightness of this lower bound by using the CRT$m$ construction.

**Keywords** collision channel without feedback · protocol sequences · user-irrepressible sequences · conflict-avoiding codes

### 1 Introduction

#### 1.1 Background

Protocol sequences are periodic deterministic binary sequences that are used to provide reliable medium access control (MAC) protocol for a collision channel without feedback [1]. Compared with time division multiple access (TDMA), ALOHA and carrier sense multiple access (CSMA), a protocol sequence-based scheme does not require stringent time synchronization, channel monitoring, backoff algorithm or packet retransmission. Such simplicity is particularly desirable in wireless sensor networks (WSNs) and vehicular ad hoc networks (VANETs) [2,5,6,7,9,10,11], where well-coordinated transmission and time synchronization may be difficult to achieve due to user mobility, time-varying propagation delays or energy constraints. In addition to the guaranteed performance, such as worst-case delay or minimum throughput, which is a natural interest of the usage of protocol sequence-based scheme, some further performance metrics, such as average group/individual delay or average throughput, are investigated in [9,10,11]. Related approaches for sequence allocation can be found in [5,6].

In this paper, our focus is on user-irrepressible (UI) protocol sequences that can guarantee a positive individual throughput per sequence period with probability one for a slot-synchronous channel. UI property is a fundamental requirement in a protocol sequence-based scheme for delay-constrained services with small amounts of user data. The design goal of UI sequences is to minimize the sequence period, which indicates how long the receiver has to wait between two successfully transmitted packets in the worst-case, when the number of active users are given. Some constructions of UI sequences can be found in [1, 2, 3, 9, 10, 14, 16, 17, 18].

We remark that deterministic MAC protocols can also be referred to in the literature as conflict-avoiding codes (CACs) [10,20,21,22,23], optical orthogonal codes (OOCs) [24,25], or topological transparent scheduling [26,27,28] with different design goals. In particular, UI sequences aim to minimize the sequence period by assuming all users are active, whereas CACs aim to maximize the number of potential users when the sequence period and the number of maximum active users are both given.
1.2 System Model

We consider a feedback-free multiple-access channel shared by $M$ users transmitting to a single receiver. Channel time is assumed to be divided into time slots of equal duration. Each user reads out the 0’s and 1’s of the assigned (binary) protocol sequence periodically and transmits a packet in a time slot if and only if the sequence value is equal to 1. Here, for simplicity, we restrict our attention to the slot-synchronized model in which users transmit packets aligned to the slot boundaries. It is assumed that users know the slot boundaries. However, there are relative time offsets $\tau_i$ of user $i$ for $i = 1, 2, \ldots, M$, such that a packet from user $i$, received at slot $t$ on the receiver’s clock, was actually sent at slot $t - \tau_i$ on user $i$’s clock. These relative time offsets are random, always unknown to the users, but unchanged in a communication session.

If exactly one user transmits a packet within a slot, the packet can be received correctly. A collision occurs if two or more than two users transmit simultaneously, and all time-overlapping packets are assumed unrecoverable.

For $i = 1, 2, \ldots, M$, let $s_i := [s_i(0) s_i(1) \ldots s_i(L-1)]$ be a binary protocol sequence with sequence period (or length) $L$ assigned to user $i$. Let $Z_L = \{0, 1, 2, \ldots, L - 1\}$ denote the ring of residues modulo $L$. Given $s_i$, we define the characteristic set of $s_i$ by $I_i := \{t \in Z_L : s_i(t) = 1\}$. We also call $I_i$ as a “sequence”, although it is actually represented as a subset of $Z_L$. The cardinality of $I_i$, $|I_i|$, is called the Hamming weight of $I_i$ or $s_i$. Let $I_i + \tau_i := \{k + \tau_i : k \in I_i\}$, where the addition is performed in $Z_L$, be the shifted version of $I_i$ by a relative shift $\tau_i$. If the relative time offset of user $i$ is $\tau_i$, he or she transmits a packet at time slot $t$ if and only if $t \in I_i + \tau_i$ in modulo $L$. This paper assumes all sequences have the same Hamming weight $w$ (called constant-weight) and share the same period $L$.

For the sake of convenience, for any positive integer $M$, let $[M] := \{1, 2, \ldots, M\}$ and $[M]_i := [M] \setminus \{i\}$. Obviously, $[M] = [M]_i$ whenever $i \notin [M]$. Let $C = \{I_1, I_2, \ldots, I_M\}$ be a collection of $M$ subsets in $Z_L$. $I_i$ is said to be unblocked in $C$ if for any integer pattern $(\tau_j \in Z_L : j \in [M]_i)$, one has

$$I_i \not\subseteq \bigcup_{j \in [M]_i} (I_j + \tau_j).$$

We say $C$ is user-irrepressible (UI) if $I_i$ is unblocked for all $i \in [M]$.

Example 1 One can check that the following $C = \{I_1, I_2, I_3, I_4\}$ is a UI sequence set of period $L = 35$ by (1).

$$I_1 = \{0, 10, 15, 25, 30\}; \quad I_2 = \{0, 4, 13, 17, 26\};$$
$$I_3 = \{0, 8, 16, 24, 32\}; \quad I_4 = \{0, 6, 12, 18, 24\}.$$
Given two characteristic sets $I_1, I_2$ and a relative shift $\tau \in \mathbb{Z}_L$ between them. Let $H_{I_1, I_2}(\tau)$ denote the Hamming cross-correlation between $I_1$ and $I_2$ with respect to $\tau$ by giving

$$H_{I_1, I_2}(\tau) := |I_1 \cap (I_2 + \tau)|.$$  

The maximum Hamming cross-correlation between $I_1$ and $I_2$ is defined as

$$H_{I_1, I_2} := \max_{\tau \in \mathbb{Z}_L} H_{I_1, I_2}(\tau).$$

By symmetry, one can see that $H_{I_1, I_2} = H_{I_2, I_1}$. Let $\lambda_c$ be the maximum Hamming cross-correlation for any pair of distinct characteristic sets in $C$. We note that $\lambda_c$ measures the maximal mutual interference between any pair of the users in a slot-synchronous channel. In Example 1 one can check that $H_{I_1, I_2} = H_{I_1, I_3} = H_{I_2, I_3} = 1$, and $H_{I_2, I_4} = H_{I_3, I_4} = 2$. Hence we have $\lambda_c = 2$.

### 1.3 Related Works and Motivation

There are various known UI sequences in literature: *Shift-invariant Sequences (SI)* [1,3,9], *Wobbling Sequences (WS)* [2], *Extended Prime Sequences (EPS)* [14], *the Chinese Reminder Theorem Sequences (CRT)* [15,16] and *CRT Sequences in Prime Users (CRTp)* [17]. Table 1 lists the major parameters of these UI sequences.

| Construction | Applicable User Number | Constant-Weight? | Hamming Weight | Sequence Period | $\lambda_c$ |
|--------------|------------------------|------------------|---------------|-----------------|-----------|
| SI [1,3,9]   | positive integer $M$   | Yes              | $2^M-1$       | $2^M-1$         | $2^M-2$   |
| WS [2]       | odd prime $p$          | Yes              | $p^3$         | $p^4$           | $p^2$     |
| EPS [14]     | odd prime $p$          | Yes              | $p$           | $p(2p-1)$       | 1         |
| CRT [15]     | positive integer $M$   | Yes              | $M$           | $u_M(2M-1)$     | 1         |
| CRTp [17]    | odd prime $p$          | No               | one for $p$, and others for $p+1$ | $2p(p-1)$ | 2         |
| CRTm [17]    | positive integer $M$   | Yes              | $M + 1$       | $p_M(2M-1)$     | 2         |

The primary design objective of UI sequences is to minimize the sequence period $L$ when $M$ is given, as $L$ has a fundamental impact on the worst-case channel access delay, i.e., the maximum waiting time that a message can be successfully received. Let $L_{\text{min}}(M)$ be the smallest $L$ such that a set of $M$ UI sequences of common period $L$ exists. The work in [17] shows that $L_{\text{min}}(M)$ is lower bounded by $8M^2/9$. One can see from Table 1 that SI sequences are the shortest known UI sequences for $M \leq 6$, CRTp sequences are the shortest for all prime $M \geq 7$, and CRT sequences are the shortest for all non-prime $M \geq 8$. Moreover, the work in [15] improves the lower bound on the sequence period.
from $8M^2/9$ to $2M^2$ for the case with constant Hamming weight $w = M$, and shows that the CRT sequences achieve this lower bound asymptotically.

We now know that CRT sequences are the shortest known UI sequences for all non-prime $M \geq 8$, however, their small Hamming weight would possibly yield larger average delay \cite{15}, which is also an important considered metric in the evaluation of channel access schemes. This observation motivates us to investigate short UI sequences with $w > M$. In this paper, we propose a CRTm construction of UI sequences, which is also based on the Chinese Remainder Theorem \cite{29}.

1.4 Contribution

Our proposed CRTm sequences are with period $p_M(2M - 1)$, constant Hamming weight $M + 1$ and $\lambda_c = 2$, where $p_M$ is the smallest prime that is larger than $M$, for any positive integer $M$. Obviously, $p_M = u_M$ when $M$ is a non-prime. Both CRT sequences and CRTm sequences are the shortest known UI sequences for all non-prime $M \geq 8$, but CRTm sequences have a larger Hamming weight. It will be shown that this larger Hamming weight would bring better average delay and throughput performance. In addition, similar to the improvement of minimum sequence period for $w = M$ in \cite{15}, we derive an asymptotic lower bound of $2M^2$ for $w = M + 1$ if the sequence structure satisfies some technical conditions, called equi-difference, and hence prove the CRTm construction is optimal in the sense that it can achieve this lower bound. Our method can be viewed as a generalization of that in \cite{15} for $w = M$.

It is worth pointing out that our proposed CRTm construction allows $w \leq (M - 1)\lambda_c$, whereas all other known constant-weight UI sequences except SI in Table 1 strictly require $w > (M - 1)\lambda_c$. This latter condition clearly implies the UI property. The difference on the relation between $w$ and $\lambda_c$ makes the proof for the UI property of the CRTm construction very different and more complicated.

The rest of this paper is organized as follows. We set up some definitions and notation in Section 2. Section 3 presents the CRTm construction of UI sequences with constant weight $w = M + 1$, and demonstrates its delay and throughput performance through analytical and numerical study. Section 4 establishes an asymptotic lower bound on the minimum sequence period with $w = M + 1$, and proves that the CRTm construction can achieve this lower bound if the sequences are constant-weight and equi-difference. A conclusion is given in Section 5.

2 Definitions and Notation

Given a sequence set $\mathcal{C} = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_M\}$. For $i = 1, 2, \ldots, M$, let $\mathcal{B}_i$ be a collection of all indices $k$ ($k \neq i$) such that the $H_{\mathcal{I}_i, \mathcal{I}_k} = \max_{j \in [M]}, H_{\mathcal{I}_i, \mathcal{I}_j}$, that
is,
\[ B_i := \{ k \in [M]_i : H_{I_i,I_k} \geq H_{I_i,I_j}, \forall j \in [M]_i \} . \]

Let \( T_{i,k} \) be a collection of all relative shifts such that
\[ T_{i,k} = \{ \tau_k \in \mathbb{Z}_L : H_{I_i,I_k}(\tau_k) = H_{I_i,I_k} \} . \]

For \( \tau_k \) in \( T_{i,k} \), we define
\[ I_{i,k,\tau_k} := I_i \setminus (I_k + \tau_k) . \]

In Example 1, since \( H_{I_1,I_2} = H_{I_1,I_3} = H_{I_1,I_4} = H_{I_1,I_5} = 1 \), and \( H_{I_2,I_4} = H_{I_2,I_5} = 2 \), we have \( B_1 = \{2,3,4\} \), \( B_2 = B_3 = \{4\} \) and \( B_4 = \{2,3\} \). Meanwhile, \( T_{3,4} = \{0,8\} \), \( T_{3,4,0} = \{8,16,32\} \), and \( T_{3,4,8} = \{0,16,24\} \).

Let \( I \) be a sequence of period \( L \) and Hamming weight \( w \). We use \( d^*(I) \) to denote the set of non-zero differences between pairs of distinct elements in \( I \), i.e.,
\[ d^*(I) := \{ a - b \ (\text{mod} \ L ) : a,b \in I, a \neq b \} . \]

Obviously, \( |d^*(I)| \geq |I| - 1 \). \( I \) is said to be exceptional if \( |d^*(I)| < 2|I| - 2 \). \( I \) is called equi-difference if the elements in \( I \) form an arithmetic progression in \( \mathbb{Z}_L \), i.e.,
\[ I = \{0,g,2g,\ldots,(w-1)g\} \quad \text{for some} \ g \in \mathbb{Z}_L , \]
where the product is performed in \( \mathbb{Z}_L \). The element \( g \) is called a generator of \( I \). If all \( I \)s in \( C \) are equi-difference, then we say \( C \) is equi-difference.

In Example 2, \( I_1 \), \( I_2 \), \( I_3 \) and \( I_4 \) are equi-difference with Hamming weight \( w = 5 \) and generators \( g_1 = 15 \), \( g_2 = 13 \), \( g_3 = 8 \) and \( g_4 = 6 \), respectively. One can further check that \( d^*(I_1) = \{5,10,15,20,25,30\} \) and thus \( I_1 \) is exceptional.

3 A New Construction of UI Sequences

We start this section with a necessary and sufficient condition for a sequence set to be UI.

**Lemma 1** Let \( C = \{I_1, I_2, \ldots, I_M\} \) be a sequence set. \( C \) is UI if and only if, for \( i \in [M] \), \( A \subseteq [M] \), and arbitrary relative shifts \( \tau_j, j \in A \), one has
\[ \left| I_i \setminus \bigcup_{j \in A} (I_j + \tau_j) \right| \geq M - |A| . \]
Proof: We only consider the necessary part as the sufficient part is simply obtained by letting $A = [M]$. Assume to the contradiction that there exist $i \in [M], A \subseteq [M], \text{ and } \tau_j, j \in A$ such that the cardinality of $I_i \setminus \bigcup_{j \in A}(I_j + \tau_j)$ is at most $M - |A| - 1$. Then we always can choose some relative shifts $\tau_k$ for all $k \in [M]\setminus A$ such that

$$I_i \setminus \bigcup_{j \in A}(I_j + \tau_j) \subseteq \bigcup_{k \in [M]\setminus A}(I_k + \tau_k).$$

(3)

More precisely, one can iteratively cover one element in the left hand side of (3) by a sequence $I_k$ or its shifted version by $\tau_k$ for some $k \in [M]\setminus A$. This contradicts to (1). 

Now, we present a new construction of constant-weight UI sequences, called the CRTm construction, which is a variation of the CRT construction [15]. Even though the two constructions look similar, the proof of the UI property is very different as the CRTm construction allows $w \leq (M - 1)\lambda_c$.

Let $p$ and $q$ be relatively prime integers. Let $\mathbb{Z}_p \otimes \mathbb{Z}_q$, consisting of all ordered pairs $(a, b)$ with $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_q$, be the direct product of the rings $\mathbb{Z}_p$ and $\mathbb{Z}_q$. There is a natural bijection (ring isomorphism) $f : \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_p \otimes \mathbb{Z}_q$ by defining

$$f(x) := (x \mod p, x \mod q),$$

that is, $f$ preserves addition and multiplication on both sides. If there is no danger of confusion, operations under $\mathbb{Z}_p \otimes \mathbb{Z}_q$ are componentwise taken modulo $p$ and $q$. We will construct sequences by specifying characteristic sets in $\mathbb{Z}_p \otimes \mathbb{Z}_q$.

**CRTm Construction:** Given $M \geq 4$, we set $p_M$ to be the smallest prime larger than $M$. Let

$$\hat{I}_j := \begin{cases} \{ (jy, y) \in \mathbb{Z}_{p_M} \otimes \mathbb{Z}_{2M-1} : y = 0, 1, \ldots, M \}, & j = 0, 1, \ldots, p_M - 1; \\ \{ (y, 0) \in \mathbb{Z}_{p_M} \otimes \mathbb{Z}_{2M-1} : y = 0, 1, \ldots, M \}, & j = p_M. \end{cases}$$

Notice that $p_M$ is relatively prime to $2M - 1$ due to $M \geq 4$ and the Bertrand’s postulate, which states that there is always a prime strictly between $M$ and $2M - 2$ for any integer $M \geq 4$. Then we obtain the characteristic sets of the sequences, $I_j$, by taking the inverse image $f^{-1}(\hat{I}_j)$ for $j = 0, \ldots, p_M$. The CRTm construction produces $p_M + 1$ sequences of length $p_M(2M - 1)$ and constant-weight $M + 1$.

**Example 2** Given $M = 6$, the CRTm construction produces 8 sequences of period 77 and constant-weight 7. The characteristic sets are:

- $I_0 = \{0, 56, 35, 14, 70, 49, 28\}$; $I_1 = \{0, 1, 2, 3, 4, 5, 6\}$;
- $I_2 = \{0, 23, 46, 69, 15, 38, 61\}$; $I_3 = \{0, 45, 13, 58, 26, 71, 39\}$;
- $I_4 = \{0, 67, 57, 47, 37, 27, 17\}$; $I_5 = \{0, 12, 24, 36, 48, 60, 72\}$;
- $I_6 = \{0, 34, 68, 25, 59, 16, 50\}$; $I_7 = \{0, 11, 22, 33, 44, 55, 66\}$.
We now aim to show that any $M$ sequences obtained by the CRT$^m$ construction form a UI sequence set. We start with the following lemma that gives an equivalent condition for the existence of UI sequences with constant-weight $w = M + 1$.

**Lemma 2** A sequence set $C = \{I_1, I_2, \ldots, I_M\}$ of constant-weight $M + 1$ is UI if and only if, for $i \in [M]$, one has

(i) $H_{I_i, I_j} \leq 2$ for any $j \in [M]$, and

(ii) $H_{I_i, k, r_n I_j} \leq 1$, i.e., $d^*(I_{i,k}, r_n I_j) \cap d^*(I_j) = \emptyset$, for any distinct integers $j, k \in [M]$ such that $k \in B_i$ and any $r_n \in T_{i,k}$.

**Proof** First, we prove the necessary part by contradiction.

(i) Suppose $H_{I_i, I_j} \geq 3$ for some $j \in [M]$. Then $|I_i \setminus (I_j + \tau_j)| \leq M - 2 < M - 1$ for some $\tau_j \in T_{i,j}$, which contradicts to (2) by setting $A = \{j\}$.

(ii) Suppose $H_{I_{i,k}, r_n I_j} \geq 2$ for some distinct integers $j, k \in [M]$ such that $k \in B_i$ and some $r_n \in T_{i,k}$. By the defining property of $I_{i,k}, r_n I_j\), we have $I_{i,k}, r_n I_j \subset I_i$. It is easy to see $H_{I_i, I_j} \geq H_{I_{i,k}, r_n I_j} \geq 2$. Since $k \in B_i$, it further implies that $H_{I_i, I_j} \geq H_{I_{i,k}, r_n I_j} \geq 2$. Let $\tau_j$ be the relative shift so that $H_{I_{i,k}, r_n I_j}(\tau_j) = H_{I_{i,k}, r_n I_j}$. Then,

$$|I_i \setminus (I_k + \tau_k) \cup (I_j + \tau_j)| = |I_i \setminus (I_k + \tau_k) \setminus (I_j + \tau_j)| \leq |I_i \setminus (I_k + \tau_k)| - 2 \leq (M + 1) - 2 - 2 < M - 2,$$

which contradicts to (2) by setting $A = \{j, k\}$.

For the sufficient part, with condition (i) and (ii), as $w = M + 1$, it is easy to see that $I_i \not\subset \cup_{j \in [M]} (I_j + \tau_j)$ for any $i$ and any relative shifts $\tau_j$. It implies that $C$ is UI. \qed

We are ready to prove the UI property of the CRT$^m$ construction.

**Theorem 1** Any $M$ sequences from the CRT$^m$ construction form an equi-difference UI sequence set of length $p_M(2M - 1)$ and constant-weight $M + 1$.

**Proof** Observe that $\tilde{I}_j$ has the generator $(j, 1)$ for $j = 0, 1, \ldots, p_M - 1$ and generator $(1, 0)$ when $j = p_M$. Thus, the CRT$^m$ construction produces $p_M + 1$ equi-difference sequences of length $p_M(2M - 1)$. We define $d^*(\tilde{I}_j)$ in the same way as $d^*(I_j)$, but with the addition and subtraction done in $\mathbb{Z}_{p_M} \otimes \mathbb{Z}_{2M - 1}$ instead of $\mathbb{Z}_{p_M(2M - 1)}$. It is sufficient to show that each obtained sequence $\tilde{I}_i$, $i \in \{0, 1, \ldots, p_M\}$, satisfies the two conditions in Lemma 2. Note that, if $H_{\tilde{I}_i, \tilde{I}_j} = 1$ for any $j \neq i$, then both the two conditions of Lemma 2 hold for $i$.

First, consider $i = p_M$. We claim that $H_{\tilde{I}_{p_M}, \tilde{I}_j} = 1$. Suppose to the contradiction that $H_{\tilde{I}_{p_M}, \tilde{I}_j} \geq 1$, that is, $d^*(\tilde{I}_{p_M}) \cap d^*(\tilde{I}_j) \neq \emptyset$, for some $j \in \mathbb{Z}_{p_M}$. Then

$$(y_1, 0) - (y'_1, 0) \equiv (jy_2, y_2) - (jy'_2, y'_2) \in \mathbb{Z}_{p_M} \otimes \mathbb{Z}_{2M - 1},$$
for \( y_1, y'_1, y_2, y'_2 \in \{0, 1, \ldots, M\} \) with \( y_1 \neq y'_1 \) and \( y_2 \neq y'_2 \). By equating the second components on both sides, we have \( y_2 = y'_2 \), a contradiction to \( y_2 \neq y'_2 \). Hence \( \mathcal{I}_{pM} \) possesses the two conditions in Lemma 2.

Second, consider \( i \in \mathbb{Z}_{pM} \). If \( H_{\tilde{\mathcal{I}}_j, \tilde{\mathcal{I}}_i} = 1 \) for any \( j \neq i \), then we are done; otherwise, \( H_{\tilde{\mathcal{I}}_j, \tilde{\mathcal{I}}_i} \geq 2 \) for some \( j \in \mathbb{Z}_{pM} \setminus \{i\} \), i.e., \( d^*(\tilde{\mathcal{I}}_i) \cap d^*(\tilde{\mathcal{I}}_j) \neq \emptyset \). Note that \( p_M \) is not a candidate for \( j \) due to the first part. \( d^*(\tilde{\mathcal{I}}_i) \cap d^*(\tilde{\mathcal{I}}_j) \neq \emptyset \) implies that

\[
(iy_1, y_1) - (iy'_1, y'_1) \equiv (jy_2, y_2) - (jy'_2, y'_2) \quad \text{in } \mathbb{Z}_{pM} \otimes \mathbb{Z}_{2M-1},
\]

for some \( y_1, y'_1, y_2, y'_2 \in \{0, 1, \ldots, M\} \) with \( y_1 \neq y'_1 \) and \( y_2 \neq y'_2 \). By equating the second components on both sides, we have \( y_1 - y'_1 \equiv y_2 - y'_2 \pmod{2M-1} \).

Since \( 0 \leq y_1, y'_1, y_2, y'_2 \leq M \), there are only five possible solutions to \( y_1 - y'_1 \) and \( y_2 - y'_2 \), as follows.

\[
\begin{align*}
    y_1 - y'_1 &= y_2 - y'_2; \quad (4) \\
    y_1 - y'_1 &= M, \quad y_2 - y'_2 = -(M-1); \quad (5) \\
    y_1 - y'_1 &= -M, \quad y_2 - y'_2 = M-1; \quad (6) \\
    y_1 - y'_1 &= -(M-1), \quad y_2 - y'_2 = M; \quad (7) \\
    y_1 - y'_1 &= M-1, \quad y_2 - y'_2 = -M. \quad (8)
\end{align*}
\]

If \( y_1 - y'_1 = y_2 - y'_2 \), from the first component, we have \( (i-j)(y_1 - y'_1) \equiv 0 \pmod{p_M} \), which implies that \( i = j \) or \( y_1 = y'_1 \) due to \( i, j \in \mathbb{Z}_{pM} \) and \( 0 \leq y_1, y'_1 \leq M \). This contradicts the assumption that \( i \neq j \) and \( y_1 \neq y'_1 \). Hence (4) can be excluded. The remaining four possible solutions (5)–(12) imply respectively (9)–(12).

\[
\begin{align*}
    (y_1, y'_1) &= (M, 0) \quad \text{and} \quad (y_2, y'_2) = (0, M-1) \text{ or } (1, M); \quad (9) \\
    (y_1, y'_1) &= (0, M) \quad \text{and} \quad (y_2, y'_2) = (M-1, 0) \text{ or } (M, 1); \quad (10) \\
    (y_1, y'_1) &= (0, M-1) \text{ or } (1, M) \quad \text{and} \quad (y_2, y'_2) = (M, 0); \quad (11) \\
    (y_1, y'_1) &= (M-1, 0) \text{ or } (M, 1) \quad \text{and} \quad (y_2, y'_2) = (0, M). \quad (12)
\end{align*}
\]

Intuitively speaking, from the construction of

\[
\tilde{\mathcal{I}}_j = \left\{ (0, 0), (j, 1), (2j, 2), \ldots, (j(M-1), M-1), (jM, M) \right\},
\]

we call elements \((0, 0), (j, 1), (j(M-1), M-1)\) and \((jM, M)\) the head, second-head, second-tail and tail, respectively. The above arguments conclude the following property, say collided property.

If there is a pair of repeated elements between two sequences under some relative shift, the two elements must be \{head, tail\} of one sequence, and \{head, second-tail\} or \{second-head, tail\} of another.
Back to $\overset{\sim}{\mathcal{I}}_i$, the collided property immediately implies $H_{\overset{\sim}{\mathcal{I}}_i, \overset{\sim}{\mathcal{I}}_j} \leq 2$ for any $j \neq i$, i.e., Lemma 2(i). Now, it remains to show that Lemma 2(ii) holds as well. Consider $k \in B_i$. If $H_{\overset{\sim}{\mathcal{I}}_i, \overset{\sim}{\mathcal{I}}_k} = 1$, then the result follows. If $H_{\overset{\sim}{\mathcal{I}}_i, \overset{\sim}{\mathcal{I}}_k} \geq 2$ and $H_{\overset{\sim}{\mathcal{I}}_i, \tau_k \overset{\sim}{\mathcal{I}}_j} \geq 2$, by the definition of $\overset{\sim}{\mathcal{I}}_{i,k,\tau_k}$ and condition (i), we have $H_{\overset{\sim}{\mathcal{I}}_i, \overset{\sim}{\mathcal{I}}_k} = 2$, $H_{\overset{\sim}{\mathcal{I}}_i, \overset{\sim}{\mathcal{I}}_j} = 2$ and $H_{\overset{\sim}{\mathcal{I}}_{i,k,\tau_k}, \overset{\sim}{\mathcal{I}}_j} = 2$. By the collided property, both the repeated elements of $\mathcal{I}_k$ and $\mathcal{I}_j$ are in the form \{head, tail\}, while the repeated elements of $\mathcal{I}_i$ with respect to $\mathcal{I}_k$ and $\mathcal{I}_j$ are in the form \{head, second-tail\} (or \{second-head, tail\}) and \{second-head, tail\} (or \{head, second-tail\}). Since in a single sequence \{second-head, tail\} is a shifted version of \{head, second-tail\}, the two \{head, tail\} pairs of $\mathcal{I}_k$ and $\mathcal{I}_j$ are repeated under some relative shift, which contradicts to the collided property. Hence we complete the proof. \hfill $\Box$

To our best knowledge, for all non-prime $M \geq 8$, CRT$m$ and CRT sequences both have the shortest known sequence length for the UI property, but the Hamming weight of CRT$m$ sequences is larger by one. To show that CRT$m$ sequences are of more practical interests, we present a performance comparison between CRT$m$ sequences and CRT sequences through analytical and numerical study. We consider three performance metrics: the maximum individual-delay, average individual-delay and average group-delay. Starting from a random time instant, the individual-delay of a user measures how long a user has to wait until he or she can send one packet successfully. The group-delay is the time duration we should wait until every user has sent successfully at least one packet. For each $M$, we run 500000 samples to generate uniformly distributed random delay offsets. Table 2 shows that CRT$m$ sequences enjoy better average delay performance than CRT sequences for all examined cases. This phenomena can be attributed to the fact that CRT$m$ sequences produce one more transmitting opportunity for each user in every sequence period. Meanwhile, as expected, CRT$m$ sequences and CRT sequences enjoy the same maximum individual-delay, as they have the same sequence period for all non-prime $M \geq 8$.

\begin{table}[h]
\centering
\caption{Delay performance of CRT sequences and CRT$m$ sequences.}
\begin{tabular}{|c|c|c|c|c|c|c|}
\hline
\textbf{M} & 8 & 9 & 10 & 12 & 14 & 15 \\
\hline
\textbf{Maximum} & CRT & 165 & 209 & 299 & 459 & 493 \\
individual-delay & CRT$m$ & 165 & 209 & 299 & 459 & 493 \\
\hline
\textbf{Average} & CRT & 20.1 & 21.6 & 26.5 & 34.5 & 35.1 \\
individual-delay & CRT$m$ & 18.3 & 20.5 & 25.1 & 32.6 & 33.5 \\
\hline
\textbf{Average} & CRT & 51.1 & 54.2 & 58.2 & 74.8 & 104.1 \\
group-delay & CRT$m$ & 45.8 & 49.9 & 54.0 & 70.5 & 97.2 \\
\hline
\end{tabular}
\end{table}

\begin{table}[h]
\centering
\caption{Delay performance of CRT sequences and CRT$m$ sequences.}
\begin{tabular}{|c|c|c|c|c|c|c|}
\hline
\textbf{M} & 16 & 18 & 20 & 25 & 30 & 40 \\
\hline
\textbf{Maximum} & CRT & 527 & 665 & 897 & 1421 & 1829 \\
individual-delay & CRT$m$ & 527 & 665 & 897 & 1421 & 1829 \\
\hline
\textbf{Average} & CRT & 35.9 & 40.5 & 48.5 & 62.0 & 68.5 \\
individual-delay & CRT$m$ & 34.4 & 39.0 & 46.6 & 60.1 & 66.9 \\
\hline
\textbf{Average} & CRT & 110.8 & 129.4 & 161.5 & 221.2 & 251.8 \\
group-delay & CRT$m$ & 105.7 & 124.1 & 153.9 & 212.4 & 245.1 \\
\hline
\end{tabular}
\end{table}
In addition to delay, throughput is another common performance metric in the evaluation of multiple-access channel protocols. We conclude this section by showing that CRTm sequences have a higher average system throughput than CRT sequences, see Table 3. The average system throughput \( R(C) \) of a sequence set \( C \) is defined as the fraction of time slots in which the users send out contention-free packets averaged over all possible offsets, and [19] have shown its value can be computed by:

\[
R(C) := \sum_{i \in [M]} \left( \frac{|I_i|}{L} \prod_{j \in [M], i} \left( 1 - \frac{|I_j|}{L} \right) \right),
\]

where \( C = \{I_1, I_2, \ldots, I_M\} \) with sequence length \( L \). Note that both CRT and CRTm are of constant-weight, so the average system throughput is simply put as

\[
M \times \frac{w}{L} (1 - \frac{w}{L})^{M-1}.
\]

**Table 3** Average system throughput of CRT sequences and CRTm sequences.

| \( M \) | 8   | 9   | 10  | 12  | 14  | 15  |
|--------|-----|-----|-----|-----|-----|-----|
| CRT    | 0.274 | 0.292 | 0.308 | 0.307 | 0.285 | 0.296 |
| CRTm   | 0.295 | 0.310 | 0.324 | 0.320 | 0.297 | 0.307 |

\[
M = 16 \quad 18 \quad 20 \quad 25 \quad 30 \quad 40
\]

| \( M \) | 16  | 18  | 20  | 25  | 30  | 40  |
|--------|-----|-----|-----|-----|-----|-----|
| CRT    | 0.306 | 0.306 | 0.291 | 0.287 | 0.305 | 0.304 |
| CRTm   | 0.316 | 0.314 | 0.299 | 0.294 | 0.310 | 0.308 |

### 4 A Tight Asymptotic Lower Bound on Sequence Period

In this section, we derive an asymptotic lower bound on sequence period for the equi-difference structure and \( w = M + 1 \), and then show this lower bound is tight by using the CRTm construction.

#### 4.1 Preliminaries

We start with three basic results which will be useful to derive a lower bound on sequence period.

The following necessary condition for \( C = \{I_1, I_2, \ldots, I_M\} \) of constant-weight \( M + 1 \) to be UI directly follows from Lemma 2(ii), and thus its proof is omitted here.

**Proposition 1** Let \( C = \{I_1, I_2, \ldots, I_M\} \) be a UI sequence set of constant-weight \( M + 1 \). Then for \( i \neq j \in [M] \), one has

\[
H_{I_{i,k\tau_k}I_{j,l\tau_l}} \leq 1, \text{ i.e., } d^*(I_{i,k\tau_k}) \cap d^*(I_{j,l\tau_l}) = \emptyset
\]
for \( k \in B_i \), \( \tau_k \in T_{i,k} \), \( l \in B_j \), \( \tau_l \in T_{j,l} \) and \( \{ i, k \} \neq \{ j, l \} \).

The following result provides an upper bound on \(|d^*(I_i) \cap d^*(I_j)|\) for \( i \neq j \).

**Lemma 3** Let \( I_1 \) and \( I_2 \) be two equi-difference sequences of the same period. If \( H_{I_1, I_2} \leq 2 \), then

\[
|d^*(I_1) \cap d^*(I_2)| \leq 4.
\]

**Proof** Let \( g_1 \) and \( g_2 \) are the generators of \( I_1 \) and \( I_2 \), respectively. Then \( I_1 \) and \( I_2 \) are of the form:

\[
I_1 = \{0, g_1, 2g_1, \ldots, (w-1)g_1\}; \quad I_2 = \{0, g_2, 2g_2, \ldots, (w-1)g_2\}.
\]

Consider the following four sets:

\[
d^*_a(I_1) = \{g_1, 2g_1, \ldots, (w-1)g_1\}; \\
d^*_b(I_1) = \{-g_1, -2g_1, \ldots, -(w-1)g_1\}; \\
d^*_a(I_2) = \{g_2, 2g_2, \ldots, (w-1)g_2\}; \\
d^*_b(I_2) = \{-g_2, -2g_2, \ldots, -(w-1)g_2\}.
\]

Obviously, \( d^*_a(I_1) \cup d^*_b(I_1) = d^*(I_1) \) and \( d^*_a(I_2) \cup d^*_b(I_2) = d^*(I_2) \).

Now we prove this lemma by contradiction. Suppose \(|d^*(I_1) \cap d^*(I_2)| \geq 5\).

Then we have

\[
5 \leq |d^*(I_1) \cap d^*(I_2)| = \left| \left( d^*_a(I_1) \cup d^*_b(I_1) \right) \cap \left( d^*_a(I_2) \cup d^*_b(I_2) \right) \right|
\]

which implies that at least one of the four sets \( d^*_a(I_1) \cap d^*_b(I_2) \), \( d^*_a(I_1) \cap d^*_b(I_2) \), \( d^*_a(I_1) \cap d^*_b(I_2) \) and \( d^*_a(I_1) \cap d^*_b(I_2) \) has cardinality at least 2. There are four cases as follows.

**C1se 1.** If \(|d^*_a(I_1) \cap d^*_b(I_2)| \geq 2\), then \( H_{I_1, I_2}(0) \geq 3 \).

**C2se 2.** If \(|d^*_a(I_1) \cap d^*_b(I_2)| \geq 2\), then \( H_{I_1, I_2}(-(w-1)g_2) \geq 3 \).

**C3se 3.** If \(|d^*_a(I_1) \cap d^*_b(I_2)| \geq 2\), then \( H_{I_1, I_2}((w-1)g_1) \geq 3 \).

**C4se 4.** If \(|d^*_a(I_1) \cap d^*_b(I_2)| \geq 2\), then \( H_{I_1, I_2}(0) \geq 3 \).

Each of the four cases implies that \( H_{I_1, I_2} \geq 3 \), which contradicts to the assumption that \( H_{I_1, I_2} \leq 2 \). This completes the proof. \( \square \)

We illustrate Lemma 3 with the following example.

**Example 3** Consider the following equi-difference sequences \( I_1 \), \( I_2 \) and \( I_3 \) of period 40 with generators \( g_1 = 7 \), \( g_2 = 9 \), \( g_3 = 17 \) and Hamming weight 6:

\[
I_1 = \{0, 7, 14, 21, 28, 35\}, \\
I_2 = \{0, 9, 18, 27, 36, 5\}, \\
I_3 = \{0, 17, 34, 11, 28, 5\}.
\]

We have \( H_{I_1, I_2} = H_{I_1, I_3} = H_{I_2, I_3} = 2 \) while \(|d^*(I_1) \cap d^*(I_2)| = |d^*(I_2) \cap d^*(I_3)| = |\{5, 35\}| = 2\) and \(|d^*(I_1) \cap d^*(I_3)| = |\{5, 12, 28, 35\}| = 4\).
We also need the following previously known result to quantify the maximum number of exceptional sequences if their non-zero difference sets are mutually disjoint.

**Lemma 4** ([21]) Consider \( I \)s in \( \mathbb{Z}_L \) whose Hamming weights are all equal to \( u \). Let \( \pi(L, 2u - 2) \) be the number of distinct relatively prime divisors of \( L \) between 2 and \( 2u - 2 \). There are at most \( \pi(L, 2u - 2) \) exceptional \( I \)s such that their non-zero difference sets are mutually disjoint.

4.2 A lower bound on sequence period

In order to obtain the minimal number of mutually disjoint non-zero difference sets in a UI sequence set, we set up the following definitions.

For \( i \in [M] \), let \( r_i \) be the smallest integer in \( B_i \). Define

\[ F := \{ i \in [M] : i = r_i \}. \]

\( F \) can be further divided into the following two disjoint subsets:

\[ F_1 := \{ i \in [M] : i = r_i, i > r_1 \}, \]

\[ F_2 := \{ i \in [M] : i = r_i, i < r_1 \}. \]

Obviously, \( |F_1| = |F_2| = |F|/2 \). In Example 1, \( F = \{2, 4\} \) and \( F_1 = \{4\}, F_2 = \{2\} \). The motivation of these definitions will be clear after Theorem 2.

Given a positive integer \( M \), let \( L_{\text{min}}(M) \) be the smallest period \( L \) such that an equi-difference UI sequence set with constant-weight \( M + 1 \) exists. We are ready for our main result in this section.

**Theorem 2**

\[ \liminf_{M \to \infty} \frac{L_{\text{min}}^e(M)}{2M^2} \geq 1. \]

**Proof** Consider an equi-difference sequence set \( C = \{I_1, I_2, \ldots, I_M\} \) of constant-weight \( M + 1 \). For \( i = 1, 2, \ldots, M \), let \( I_{r_i}^* \) be a subset of \( I_{r_i, \tau_i^*} \) such that \( |I_{r_i}^*| = M - 1 \), where \( \tau_i^* \) is the smallest element in \( I_{r_i, \tau_i} \).

By Proposition 1, the non-zero difference sets of the following distinct \( M - |F| + |F_1| \) sequences are mutually disjoint:

\[ \{I_{r_i}^* : i \in ([M] \setminus F) \cup F_1\}. \] (15)

Similarly, the non-zero difference sets of the following distinct \( M - |F| + |F_2| \) sequences are mutually disjoint:

\[ \{I_{r_i}^* : i \in ([M] \setminus F) \cup F_2\}. \] (16)

By Lemma 1, plugging \( u = M - 1 \) implies that there are at most \( \pi(L, 2M - 4) \) exceptional sequences in each of (15) and (16). By Proposition 1 we further have

\[ \left( d^*(I_{r_{i_1}}^*) \cup d^*(I_{r_{i_2}}^*) \right) \cap \left( d^*(I_{r_{i_1}}^*) \cup d^*(I_{r_{i_2}}^*) \right) = \emptyset \]
for any distinct $i_1, i_2 \in F_1$ or any distinct $i_1, i_2 \in F_2$.

Since the total number of distinct nonzero differences cannot be larger than the number of nonzeros in $\mathbb{Z}_L$, we have:

$$L - 1 \geq \sum_{i \in [M] \setminus F} |d^*(I_{i,r_i})| + \sum_{i \in F_1} |d^*(I_{i,r_i}) \cup d^*(I_{r_i,i})|$$

$$= \sum_{i \in [M]} |d^*(I_{i,r_i})| - \sum_{i \in F_1} |d^*(I_{r_i,i}) \cap d^*(I_{r_i,i})|. \quad (17)$$

By Lemma 3 and the condition that $H_{I_{r_i}} \leq 2$ for all $i$, we have

$$|d^*(I_{i,r_i}) \cap d^*(I_{r_i,i})| \leq |d^*(I_{i}) \cap d^*(I_{r_i})| \leq 4. \quad (18)$$

Combining (17) and (18) derives

$$L \geq \sum_{i \in [M]} |d^*(I_{i,r_i})| - 4|F_1| + 1$$

$$\geq (M - 2\pi(L, 2M - 4))(2(M - 4) + 2\pi(L, 2M - 4)(M - 2) - 4|F_1| + 1$$

$$\geq (M - 2\pi(L, 2M - 4))(M - 2) - 2M + 1. \quad (19)$$

The second “$\geq$” of the above is due to the fact that there are at most $2\pi(L, 2M - 4)$ exceptional sequences in total $M$ sequences, while the last one follows from $|F_1| = |F|/2 \leq M/2$. Taking lim sup on both sides of (19) leads to

$$\liminf_{M \to \infty} \frac{L}{2M^2} \geq \liminf_{M \to \infty} \frac{(2M - 4)M}{2M^2} - \frac{2\pi(L, 2M - 4)(M - 2) - 2M - 1}{2M^2}$$

$$= 1 - \liminf_{M \to \infty} \frac{\pi(L, 2M - 4)}{M} \leq 1.$$

The last identity above is due to

$$\liminf_{M \to \infty} \frac{\pi(L, 2M - 4)}{(2M - 4)/ \ln(2M - 4)} \leq 1,$$

which can be obtained by the prime number theorem. Hence we complete the proof. \qed

By the CRTm construction, we show that the asymptotic lower bound in Theorem 2 can be achieved.

**Theorem 3**

$$\liminf_{M \to \infty} \frac{L^e_{\min}(M)}{2M^2} = 1.$$
Proof Consider $M \geq 4$ is not a prime number. By the CRTm construction, we can obtain equi-difference UI sequences of constant-weight $M + 1$ and period $p(2M - 1)$. Since there are infinitely many primes $p$ and we can always set $M = p - 1$, we have $\lim \inf_{M \to \infty} p/M = 1$. Therefore, we have

$$\lim \inf_{M \to \infty} \frac{p(2M - 1)}{2M^2} = 1.$$ 

This shows that the asymptotic lower bound in Theorem 2 is tight and hence the result follows.

\[\Box\]

5 Conclusion

This paper studies UI sequences for bounded-delay data service in wireless multiple-access networks without stringent time synchronization. To achieve a better delay performance than that of previously known constructions, a new construction of UI sequences with constant-weight $M + 1$ is devised for a system with $M$ active users. The new construction and the previously known CRT construction in [15] both produce the shortest known sequence period for all non-prime $M \geq 8$. Moreover, it is shown that the new construction not only enjoys a better average delay performance, but also has a higher average system throughput than the CRT construction, and thus is of more practical interests. On the other hand, an asymptotic lower bound on the sequence period is derived for equi-difference UI sequences with constant-weight $M + 1$, and is achieved by using the proposed new construction.

Our follow-up work seeks to investigate shorter UI sequences by using the methods presented in this paper. In addition, our approaches can also be applied to study more general CACs, without requiring that the Hamming weight is equal to the number of active users.

Acknowledgements This work was supported by the National Natural Science Foundation of China under grant number 61301107 and 11601454, the open research fund of National Mobile Communications Research Laboratory, Southeast University, under grant number 2017D09, and the Natural Science Foundation of Fujian Province of China under grant number 2016J05021.

References

1. J. L. Massey, P. Mathys, “The collision channel without feedback,” IEEE Trans. Inf. Theory, vol. IT-31, no. 2, pp. 192–204, Mar. 1985.
2. W. S. Wong, “New protocol sequences for random access channels without feedback,” IEEE Trans. Inf. Theory, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.
3. C. S. Chen, W. S. Wong and Y. Q. Song, “Constructions of robust protocol sequences for wireless sensor and ad hoc networks,” IEEE Trans. Veh. Tech., vol. 57, no. 5, pp. 3053–3063, Sep. 2008.
4. Y. Wu, K. W. Shum, Z. Lin, W. S. Wong and L. Shen, “Protocol sequences for mobile ad hoc networks,” in Proc. IEEE Int. Conf. on Comm., Budapest, Jun. 2013, pp. 1730–1735.
5. Y. Wu, K. W. Shum, W. S. Wong and L. Shen, “Safety messages broadcast in vehicular ad hoc networks based on protocol sequences,” IEEE Trans. Veh. Tech., vol. 63, no. 3, pp. 1467–1479, Mar. 2014.
6. W. S. Wong, “Transmission sequence design and allocation for wide area ad hoc networks,” IEEE Trans. Veh. Technol., vol. 63, no. 2, pp. 869–878, Feb. 2014.
7. Y. Mao and L. Shen, “A framework for protocol sequence allocation in vehicular ad hoc networks,” Proc. IEEE Veh. Tech. Conf., Nanjing, China, May 2016.
8. C.-C. Chen, G.-C. Yang, M.-K. Chang, J.-S. Lin, W. S. Wong and W. C. Kwong, “Constructions and throughput analyses of protocol channels with adjustable duty factor for collision channels without Feedback,” IEEE Trans. Commun., vol. 65, no. 10, pp. 4736–4748, Nov. 2016.
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. Inf. Theory, vol. 55, no. 7, pp. 3312–3322, Jul. 2009.
10. Y. Zhang, Y.H. Lo, W. S. Wong and F. Shu, “Protocol sequences for the multiple-packet reception channel without feedback,” IEEE Trans. Veh. Tech., vol. 64, no. 4, pp. 1687–1698, Apr. 2016.
11. L. Salaun, C. S. Chen, Y. Chen and W. S. Wong, “Constant delivery delay protocol sequences for the collision channel without feedback,” to appear in Proc. Int. Symp. Wire. Pers. Multimed. Commun., Shenzhen, China, Nov. 2016.
12. Q. A. Nguyen, L. Györfi and J. L. Massey, “Constructions of binary constant-weight cyclic codes and cyclically permutable codes,” IEEE Trans. Inf. Theory, vol. 38, no. 3, pp. 940–949, May 1992.
13. L. Györfi and I. Vajda, “Construction of protocol sequences for multiple-access collision channel without feedback,” IEEE Trans. Inf. Theory, vol. 39, no. 5, pp. 1762–1765, Sep. 1993.
14. G. C. Yang and W. C. Kwong, “Performance analysis of optical CDMA with prime codes,” IEEE Electron. Lett., vol. 31, no. 7, pp. 569–570, 1995.
15. 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 Proc. IEEE Int. Symp. Inf. Theory, Seoul, Korea, Jun. 2009, pp. 1368–1372.
16. K. W. Shum and W. S. Wong, “Construction and applications of CRT sequences,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5780–5795, Nov. 2010.
17. K. W. Shum, Y. Zhang and W. S. Wong, “User-irrepressible sequences,” in Proc. Conf. SETA, Paris, Sept. 2010, pp. 88–101.
18. Y. Chen, K. W. Shum and W. S. Wong, “Generalized CRT sequence and its applications,” to appear in Proc. Conf. SETA, Chengdu, Oct. 2016.
19. V. I. Levenshtein and V. D. Tonchev, “Optimal conflict-avoiding codes for three active users,” in Proc. IEEE Int. Symp. Inf. Theory, Adelaide, Sept. 2005, pp. 535–537.
20. H.-L. Fu, Y.-H. Lin and M. Mishima, “Optimal conflict-avoiding codes of even length and weight 3,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5747–5756, Nov. 2010.
21. Shum K.W., Wong W.S., Chen C.S.: A general upper bound on the size of constant-weight conflict-avoiding codes. IEEE Trans. Inform. Theory 56(7), 3265–3276 (2010).
22. Y.-H. Lo, H.-L. Fu and Y.-H. Lin, “Weighted maximum matchings and optimal equi-difference conflict-avoiding codes,” Des. Codes Cryptogr., vol. 76, no. 2, pp. 361–372, 2015.
23. Y. Lin, M. Mishima and M. Jimbo, “Optimal equi-difference conflict-avoiding codes of weight four,” Des. Codes Cryptogr., vol. 78, no. 3, pp. 747–776, 2016.
24. F. R. K. Chung, J. A. Salehi and V. K. Wei, “Optimal optical orthogonal codes: Design, analysis, and applications,” IEEE Trans. Inf. Theory, vol. 35, no. 3, pp. 595–604, May 1989.
25. J. Wang and J. Yin, “Two-dimensional optical orthogonal codes and semicyclic group divisible designs,” IEEE Trans. Inf. Theory, vol. 56, no. 5, pp. 2177–2187, May 2010.
26. W. Chu, C. J. Colbourn and V. R. Syrotiuk, “The effects of synchronization on topology-transparent scheduling,” Wire. Netw., vol. 12, no. 6, pp. 681–690, Nov. 2006.
27. W. Chu, C. J. Colbourn and V.R. Syrotiuk, “Slot synchronized topology-transparent scheduling for sensor networks,” Comput. Commun., vol. 29, no. 4, pp. 421–428, Feb. 2006.
28. Y. Liu, V. O. K. Li, K.-C. Leung, and L. Zhang, “Topology-transparent scheduling in mobile ad hoc networks with multiple packet reception capability,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 5940–5953, Nov. 2014.

29. K. Ireland and M. Rosen, “A Classical Introduction to Modern Number Theory”, New York: Springer-Verlag, 1990.