Protocol Sequences for the Collision Channel without Feedback

ZHANG, Yijin

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of
Doctor of Philosophy
in
Information Engineering

The Chinese University of Hong Kong
September 2010

Abstract of thesis entitled:

Protocol Sequences for the Collision Channel without Feedback

Submitted by ZHANG, Yijin

for the degree of Doctor of Philosophy

at The Chinese University of Hong Kong in September 2010

This thesis is based on Massey's model on collision channels without feedback, in which collided packets are considered unrecoverable. A collision occurs if two or more packets are partially or totally overlapped. Each potential user is assigned a deterministic zero-one pattern, called the protocol sequence, and sends a packet if and only if it is active and the value of the sequence is equal to one. Due to lack of feedback, the beginning of the protocol sequences cannot be synchronized and variation in relative offsets is inevitable. It further yields variation in throughput.

We study the design of protocol sequences from three different perspectives.

First of all, in order to minimize variation of throughput due to delay offsets, we investigate protocol sequences whose pairwise Hamming cross-correlation is a constant for all possible relative offsets. It can be viewed as a generalization of completely shift-invariant sequences, which can achieve the zero-variation in throughput over a slot-synchronized channel.

The second one is a non-blocking property which ensures that each active user can successfully transmit information at least once

in its each active period. With the assumption that all potential users may be active simultaneously, user-irrepressible sequences and completely irrepressible sequences are studied respectively for different level of synchronization, to support the non-blocking property.

Provided that the number of active users is smaller than the number of potential users, strongly conflict-avoiding codes are introduced with the non-blocking property in the asynchronous channel. It can be viewed as an extension of completely irrepressible sequences.

At last, we focus on the detection problem in the protocol sequence design. The objective is to construct user-detectable 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.

摘要

本論文主要基於Massey創立的無反饋衝突信道模型。在此模型中如果多餘一個的數據包部份或全部地在信道上重合，我們視之為衝突產生并無法恢復。每一個潛在用戶被分配一個被稱之為協議序列的確定性二進制數列，當且僅當自身處於激活狀態并且序列值為一時進行數據包的發送。由於缺少信道信息的反饋，每個用戶的協議序列不能同步而且用戶之間相對延遲的變化也無法避免，並且進一步造成吞吐率的變化。

本論文將從以下三個方面對協議序列的設計進行研究。

首先，以最小化吞吐率的變化為目標，我們對具有成對漢明跨相關函數為常數特性的協議序列進行了探討。它可被視之為completely shift-invariant協議序列的擴展。

其次我們著眼于協議序列的非阻塞性質，它確保了每個激活用戶可以在其每一激活週期內成功發送數據包一次。以非阻塞性為前提，我們基於不同的信道同步層次，分別對user-irrepressible序列，completely irrepressible序列，和strongly conflict-avoiding codes進行了研究。

最後我們構造了user-detectable序列以確保用戶在一定的延遲內被檢測到當且僅當它處於激活狀態。

Acknowledgement

First of all, I would like to express my deepest appreciation to my advisor Professor Wing Shing Wong. His continuous encouragement, insightful suggestions, and excellent guidance had led me to successfully complete this thesis. I am most grateful to his trust and patience during these three years.

I am especially indebted to Dr. Kenneth W. Shum for helping me to study combinatorics, number theory, and their applications to protocol sequences. I have learned a lot through discussions and joint works with him.

With this opportunity, I am grateful to Professor Pingping Xu, who introduced and helped me to start my graduate study.

Many thanks go to my labmates. Some of them are Yi Chen, Shenghao Yang, Fan Chen, Yanlin Geng and Silas Fong.

Finally, with a deep sense of gratitude, I would like to thank my parents, my wife and her parents for their endless support and love.

To my wife, Xi Sheng

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 The Collision Channel without Feedback

Massey and Mathys [20, 21] introduced the model of the collision channel without feedback for multiple access communication. Consider a time-slotted system, consisting of M potential users and one sink, but at most K users are active at the same time. The channel is divided into time slots of equal duration. Since there is no central coordination and no feedback from the data sink, we cannot do packet scheduling for media access control. An alternative is to use a random transmission scheme such as ALOHA [2, 3], where each user sends a packet in a time slot with a defined probability, independent of what it has done in previous time slots and other users. However, implementing a random number generator is sometimes too costly for users, which are both power and computational complexity limited. As we do not assume the users are equipped with any receiver, contention based protocols, which require listening to the channel, is not feasible. We also note that for both random transmission and contention based protocol, there is no guarantee on transmission delay in the worst case.

In this thesis, we will follow the approach in [21], and specify the

transmission pattern by a deterministic sequence, called a *protocol sequence*. The components of a protocol sequence are either zero or one. Each potential user is assigned a protocol sequence with the same length, and reads off the protocol sequence periodically if it is active. It transmits a packet within one time slot duration if the sequence value is one, and keeps silent for one time slot if it is zero. Suppose the sequence length is L time slots. For $i = 1, 2, \ldots, M$, the protocol sequence associated with user i is specified by a L-dimensional row vector $s_i := [s_i(0)\ s_i(1)\ \ldots\ s_i(L-1)]$. Without loss of generality, $s_i(0)$ here is assumed to be 1 for all i. 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 L time slots before becoming active again. We use the word sequence "period" and sequence "length" interchangeably in this thesis.

As there is no feedback from the receiver and no cooperation among the users, the channel is not synchronized, i.e., there is no guarantee that the protocol sequence will start at the same time. Each user has a delay offset, which is random but remains fixed throughout the communication session. Let δ_i be the time offset of user i for $i = 1, 2, \ldots, M$, measured in time slot duration units. It is a real-valued number which can be interpreted as the difference between the time shown on the receiver's clock and the time shown on user i's clock. In this thesis, all time indices and time intervals referred are understood to be at the receiver's clock and in the units of time slot duration. Furthermore, we distinguish between two different levels of synchronization:

1) The channel is slot-synchronized if all users know the slot boundaries of the channel, i.e., the time offsets $\delta_1, \delta_2, \ldots, \delta_M$ are arbitrary integers.

2) The channel is asynchronous if it is not slot-synchronized. In this model, all users do not know the slot boundaries of the channel. It implies the time offsets $\delta_1, \delta_2, \ldots, \delta_M$ are arbitrary real numbers.

Thus, if all users start their packet transmissions at an integral time epoch, collisions will result only when received packets completely overlap. In the asynchronous case, however, collisions can occur due to partial overlapping of packets. We further assume a packet in the asynchronous channel is received correctly if it is not subject to any collision and is unrecoverable otherwise. In other words, a packet is assumed to be successful if and only if it is not completely or partially overlapped by any other packet. In [12, 38], some studies were carried out for the asynchronous channel by using error correction techniques for recovery from some partially overlapped collisions. However, this scenario is not considered in this thesis.

In multiple access transmission without packet header, one necessary task [1,10,21] of the receiver is addressing the decoding problem which deals with the issue of determining the sender of each successfully received packet by merely observing the channel activity. In other words, the protocol sequences may have some structures that allow the receiver to determine from whom a packet is sent, even without header information. Discussions on sender and packet decoding issues can be found in [41] for practical considerations. One can consider the simple approach of requiring each packet to include a header, which contains the user identity and data index. If the payload of a packet is large enough, the cost of this overhead could be quite small.

Evaluating the performance of protocol sequences is a compli-

cated issue. Nevertheless, the following criteria [41] is commonly considered.

1) The number of active users that can be supported simultaneously.

2) Throughput performance, measured for example by the amount of successful transmissions that can be guaranteed in a sequence period.

3) The length of the sequence period for all active users with some guaranteed throughput in each active period. A shorter length tends to ensure less variability in performance.

Protocol sequences proposed in the literature provide different performance guarantees with regard to these criteria. We will make a survey of them in the next section.

1.2 Existing Results on Protocol Sequences

1.2.1 The Slot-Synchronized Case

All protocol sequences mentioned in this subsection are designed for the slot-synchronized collision channel. The throughput of a user is defined as the fraction of slots it can send a packet without suffering any collision. The sum or system throughput can be found as the throughput of all active users.

The capacity of the collision channel without feedback is explored by Massey and Mathys in [21]. It is shown that the theoretical zero-error sum-capacity is $1/e$ for the slot-synchronized channel. In order to achieve the theoretical capacity of the slot-synchronized channel, protocol sequences with the special property that the variation of throughput due to integer-delay offsets is zero, are proposed

in [21]. Protocol sequences with this property are called *completely shift-invariant* or *shift-invariant* sequences [31]. Such protocol sequences have the advantage that there is no fluctuation in throughput no matter what the integer-delay offsets are, and hence can guarantee the largest sum throughput in the worst case. Constructions of complectly shift-invariant protocol sequences are reported in [6,21,31]. Nevertheless, such sequences have a drawback that the period grows exponentially in M, for $M = K$. In fact, it will be further proved in this thesis that the period grows exponentially in M for all $K \leq M$.

After the seminar work of [20], more general constructions under the name of *constant-weight cyclically permutable codes* are reported in [1, 4, 10, 25]. In the context of optical communications, these protocol sequences can also be viewed as *optical orthogonal codes* (OOC) [8], which have quite different design criteria compared with protocol sequences. The main difference is that the Hamming auto-correlation is inessential in the design of protocol sequences for a system with packet header, but important for optical orthogonal codes. For a system without packet header, the Hamming auto-correlation is considered in protocol sequences [1,10] to address the decoding problem.

Another class of protocol sequences, called *linear congruence sequences* [39], is originally designed for frequency-hopping signals. Furthermore, *prime sequences*, a subset of linear congruence sequences, were proposed by Shaar and Davies [30] and independently by Prucnal and his coworkers [27], around the same time when [20] was published. It also finds applications in optical spread spectrum systems. In [42,43], the concept of an *extended prime sequence* was introduced by padding extra zeroes in the prime sequences, with a

particular view towards optical CDMA applications.

Built on the concept of linear congruence sequences, a family of protocol sequences, called *wobbling sequences* [41], was designed to support multi-rate service and a large number of active users. It has a common period which is equal to M^4 for the case $K = M$ and worst-case system throughput provably larger than a positive constant that is approximately equal to 0.25 when M is large. One can check the asymptotic throughput performance of wobbling sequences is close to that of completely shift-invariant sequences, say $1/e$, but the period is much smaller. Recently, [32] improved upon the wobbling sequences by constructing protocol sequences with period of order $O(M^2)$ for $M = K$ and $O(M^3)$ for $M \geq 2K$, while the guarantee of the worst-case sum throughput remains the same. The *Chinese remainder theorem* (CRT) [9] is employed in [32]. Applications of CRT can also be found in [1, 10, 25, 35].

Considering the case $K = M$, the concept of *user-irrepressible* (UI) sequences is proposed in [5, 35, 41]. It ensures that each active user can successfully transmit information at least once in a sequence period over the slot-synchronized channel. All protocol sequences reported in [1, 4, 10, 21, 25, 32, 35, 41–43] can be viewed as UI sequences. The shortest UI sequences called *CRT sequences* can be found in [35]. Its period is equal to $p_M(2M - 1)$ with p_M is the smallest prime not less than M.

For the case that $K \leq M$, a set of M binary sequences is called (M, K)-*conflict-avoiding* [40] if every subset of K sequences out of these M sequences is UI. Given the code length L, the objective in the construction of conflict-avoiding sequence set (see e.g [14,24] and the references therein) is to maximize the number of potential users M, with the guarantee of at least one packet received successfully

from each active user in L time slots, provided that the number of active users is no more than K.

1.2.2 The Asynchronous Case

It is shown in [21] that the zero-error sum-capacity is $1/e$ for the asynchronous channel. The capacity is achieved by applying coding and interleaving on the completely shift-invariant sequences, but with an infinite period. More general, the following was proved in [21].

Lemma 1.1 ([21] Lemma 5). *Let m be any integer larger than 1. Given a protocol sequence set of period L with worst-case system throughput larger than T in the slot-synchronized channel, then there exists a protocol sequence set of period mL with worst-case system throughput larger than $(m-1)T/m$ in the asynchronous channel.*

1.3 Notations and Definitions

For the clarity of our presentation and convenience of the readers, some basic notations and definitions used in protocol sequences are defined in this section.

Definition 1.1. Given a binary sequence of length L,

$$s := [s(0)\ s(1)\ \ldots\ s(L-1)],$$

we define its *Hamming weight* as

$$w_H(s) := \sum_{t=0}^{L-1} s(t). \tag{1.1}$$

For example, the Hamming weight of [11001100] is 4.

Definition 1.2. The *cyclic shift* of s with length L by an integer τ is denoted by

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

The subtraction $t-\tau$ is performed modulo L for $t = 0, 1, \ldots, L-1$. For example, given $s = [11001100]$, we have $s^{(2)} = [00110011]$.

Definition 1.3. Given two sequences $s_1(t)$ and $s_2(t)$ both of length L, we define the *pairwise Hamming cross-correlation* function of $s_1(t)$ and $s_2(t)$ by

$$H_{s_1 s_2}(\tau) := \sum_{t=0}^{L-1} s_1(t) s_2(t-\tau). \tag{1.2}$$

The *Hamming auto-correlation* of s_1 is defined by

$$H_{s_1 s_1}(\tau) := \sum_{t=0}^{L-1} s_1(t) s_1(t-\tau). \tag{1.3}$$

For example, given $s_1 = [11001100]$ and $s_2 = [10101010]$, we have $H_{s_1 s_2}(2) = 2$ and $H_{s_1 s_1}(2) = 0$.

Definition 1.4. For two binary sequences $s_1(t)$ and $s_2(t)$, their *logical OR* is defined as

$$(s_1 \vee s_2)(t) := \begin{cases} 1 & \text{if } s_1(t) = 1 \text{ or } s_2(t) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{1.4}$$

Definition 1.5. For each t, we say that the t-th component of sequence s_1 is *covered* by sequence s_2 if $s_2(t) = 1$. Sequence s_1 is *covered* by s_2 if each "1" in s_1 is covered by s_2, i.e., $s_1(t) = 1$ implies $s_2(t) = 1$ for all t. We write $s_1 \preceq s_2$ if s_1 is covered by s_2.

Consider u sequences $s_i(t)$, for $i = 1, 2, \ldots, u$. Sequence $s_i(t)$ is *blocked* by other $u-1$ sequences if we can find delay offsets τ_j, for $j \in \{1, 2, \ldots, u\} \setminus \{i\}$, such that

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

Otherwise, it is not blocked by other $u-1$ sequences.
As an example, in the following three sequences:

$$s_1 = [11001100]$$
$$s_2 = [10101010]$$
$$s_3 = [00011100]$$

we have s_3 is blocked by s_1 and s_2 as

$$s_3 \preceq (s_1^{(0)} \vee s_2^{(1)}) = [11011101].$$

When the Hamming weight of a sequence is small in comparison with the length L, the sequence can be compactly represented by specifying the locations of ones. Let $\mathbb{Z}_L$ be the additive group of residues modulo L. We use $|\cdot|$ to denote the cardinality of a set.

Definition 1.6. Given a sequence $s(t)$ of length L, let the *characteristic set* of $s(t)$, denoted by $\mathcal{I}_s$, be the subset of $\mathbb{Z}_L$ such that $t \in \mathcal{I}_s$ if and only if $s(t) = 1$.

Shifting a sequence cyclically by τ is equivalent to translating its characteristic set by τ, with addition performed modulo L. Given a subset $\mathcal{I}$ in $\mathbb{Z}_L$, and $\tau \in \mathbb{Z}_L$, we denote the translation of $\mathcal{I}$ by τ as

$$\mathcal{I} + \tau := x + \tau \in \mathbb{Z}_L : x \in \mathcal{I}. \tag{1.5}$$

Expressed in terms of the characteristic set, the pairwise Hamming cross-correlation of sequences $s_1(t)$ and $s_2(t)$ equals

$$H_{s_1 s_2}(\tau) = |\mathcal{I}_{s_1} \cap (\mathcal{I}_{s_2} + \tau)| \tag{1.6}$$

for all $\tau = 0, 1, \ldots, L$.
As an example, given $s_1 = [11001100]$ and $s_2 = [10101010]$, we have $\mathcal{I}_{s_1} = \{0, 1, 4, 5\}$ and $\mathcal{I}_{s_2} = \{0, 2, 4, 6\}$. Furthermore, we find

$$|\{0, 1, 4, 5\} \cap (\{0, 2, 4, 6\} + 2)| = 2$$

which equals the value of $H_{s_1 s_2}(2)$.

Definition 1.7. For a subset $\mathcal{I}$ of $\mathbb{Z}_L$, we let

$$d(\mathcal{I}) := \{a_i - a_j : a_i, a_j \in \mathcal{I}\}, \tag{1.7}$$

and call it the *set of differences* in $\mathcal{I}$. Since zero is always in $d(\mathcal{I})$ for any subset $\mathcal{I}$, we also define

$$d^*(\mathcal{I}) := d(\mathcal{I}) \setminus \{0\}, \tag{1.8}$$

the differences between pairs of distinct elements in $\mathcal{I}$.
As an example, for $s = [100100100]$, we have $d(\mathcal{I}_s) = \{0, 3, 6\}$ and $d^*(\mathcal{I}_{s_1}) = \{3, 6\}$.

Definition 1.8. A sequence s is called *equi-difference* if the elements in $\mathcal{I}_s$ form an arithmetic progression in $\mathbb{Z}_L$, i.e.,

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

for some $g \in \mathbb{Z}_L$. In the above equation, the product jg is reduced mod L, for $j = 1, 2, \ldots, w_H(s) - 1$. The element g or $L - g$ is called the *generator* or *common difference* of this sequence.

For an equi-difference sequence generated by g or $L - g$, the set of differences is equal to

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

If each sequence in a sequence set is equi-difference, this sequence set is said to be *equi-difference*.

Given two equi-difference sequences s_1 and s_2 with $w_H(s_1)g_1 \neq 0 \mod L$ and $w_H(s_2)g_2 \neq 0 \mod L$, we say they are *distinct* if we have

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

For example, $s_1 = [10101000]$ and $s_2 = [10010010]$ are both equi-difference with the generator 2 and 3 respectively. They are also distinct.

1.4 Thesis Outline

In the remainder of this thesis, we discuss existence problems and constructions of several kinds of protocol sequences in the following five chapters. In particular, the slot-synchronized collision channel is assumed in Chapter 2, 3, 6 and the asynchronous collision channel is studied in Chapter 4, 5. Also we assume all potential users may be active at the same time, i.e., $M = K$ in Chapter 2, 3 ,4 and 6. In Chapter 5, a more general scenario with $M \geq K$ is considered.

In Chapter 2, we introduce pairwise shift-invariant protocol sequences which is a generalization of completely shift-invariant sequences. Basic properties are investigated including minimum period and bit structures. Furthermore, the sequence set is shown to be completely shift-invariant, if the sequences satisfy some technical conditions. The results presented in this chapter supplement well the existing results in the literature [6, 31].

In Chapter 3, 4 and 5, we consider the non-blocking property which ensures that each active user can successfully transmit information at least once in its each active period.

In Chapter 3, with the assumption $M = K$, we focus on user-irrepressible protocol sequences with the non-blocking property in the slot-synchronized channel. A blocking algorithm is introduced to provide a necessary condition of such sequences. We further show that some user-irrepressible sequence sets must be pairwise shift-invariant with some special period and number of users. The work of this chapter is a continuation of results presented in [5].

The non-blocking property in the asynchronous channel is studied in Chapter 4. For $M = K$, sequence sets with this property are said to be completely irrepressible. We analyze the class of completely irrepressible sequences with the minimum number of ones in each period, and derive a lower bound on the minimum period. Moreover, for equi-difference sequence sets, we improve the lower bound and present a construction method that meets this lower bound asymptotically.

A generalization of Chapter 4 is carried out in Chapter 5 for the case $M \geq K$. We investigate strongly conflict-avoiding codes (SCAC) which is a set of M binary sequences in which every subset of K sequences out of these M sequences is completely irrepressible. It guarantees the non-blocking property in the asynchronous channel for $M \geq K$. Under a different objective compared with Chapter 4, given code length L, we present upper bounds on the size of SCAC and equi-difference SCAC, which hold for all K in general. The code size is the number of potential users that can be supported.

Chapter 6 is dedicated to user-detectable sequences with the property that each active user can be detected by looking at the channel activity only for the system without packet header, within some bounded delay. Some lower and upper bounds of its mini-

mum period are presented. We further display some interconnections between user-detectable sequences and other research areas in sequence design.

In Chapter 7, we provide concluding remarks and open problems in this thesis.

Various parts of this thesis have appeared in [36, 44–47].

□ **End of chapter.**

Chapter 2

Pairwise Shift-Invariant Sequences

Summary

For protocol sequences in the slot-synchronized channel, it is desirable that their Hamming cross-correlation should be as low as possible and that the length of their period should not be long. Completely shift-invariant sequences form an important class of protocol sequences which have perfect cross-correlation property but exponential growth period as a function of the number of users. We investigate in this chapter a broader class of protocol sequences which are only pairwise shift-invariant. Results on minimum period and bit-pattern structure are presented.

2.1 System Model

In this chapter, we focus on the collision channel without feedback described in Section 1.1, and consider a time-slotted system, consisting of M potential users and one sink, with all users may be active at the same time. It is assumed that the collision channel is slot-synchronized, i.e., the users know and align to the slot boundaries. However, they are not required to synchronize to each other and have different start time.

Guaranteed throughput and least common period are two common performance measures for protocol sequences. As users may join and depart at different times, sequences with long period are undesirable even if they can ensure high throughput. Since these performance measures are closely tied to the periodic Hamming cross-correlation function, the latter is the main object of study in this chapter. Ideally, the cross-correlation function should be invariant to relative shift delays among the sequences, as they cannot be assumed to be synchronized due to lack of feedback. More specifically, pairwise shift-invariant sequences are considered here.

2.2 Hamming Cross-Correlation

Definition 2.1. Let $s_1, \ldots, s_k$ be k periodic binary sequences with a common period L. Define the *k-wise Hamming cross-correlation* function among these k sequences for relative shifts $\tau_1, \ldots, \tau_{k-1}$ by

$$H_{s_1 \ldots s_k}(\tau_1, \ldots, \tau_{k-1}) := \sum_{t=0}^{L-1} s_1(t) s_2(t-\tau_1) \cdots s_k(t-\tau_{k-1}). \quad (2.1)$$

The subtraction $t - \tau_i$ is performed modulo L for all i.

The normalized version is defined to be

$$\bar{H}_{s_1 \ldots s_k}(\tau_1, \ldots, \tau_{k-1}) := H_{s_1 \ldots s_k}(\tau_1, \ldots, \tau_{k-1})/L.$$

The pairwise case $H_{s_1 s_2}$ defined in (1.2) is simply the Hamming cross-correlation function for a pair of sequences, i.e., $k = 2$.

Definition 2.2. The k-wise Hamming cross-correlation is said to be *shift-invariant* (SI) if $\bar{H}_{s_1 \ldots s_k}$ is identically equal to a constant. A set of protocol sequences is called *completely SI* if the k-wise Hamming cross-correlation is SI for all choices of k distinct sequences and for all k. A set of protocol sequences is called *pairwise SI* if the pairwise Hamming cross-correlation is SI for all pairs of distinct protocol sequences.

For a periodic binary sequence s with a period L, following [21], we define its *duty factor* by

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

The following is a basic result on Hamming cross-correlation [29]:

$$\frac{1}{L^{k-1}} \sum_{\tau_1=0}^{L-1} \cdots \sum_{\tau_{k-1}=0}^{L-1} \bar{H}_{s_1 \ldots s_k}(\tau_1, \ldots, \tau_{k-1}) = R_1 \cdots R_k, \tag{2.2}$$

where R_i denotes the duty factor of s_i, for $i = 1, \ldots, k$. If the k-wise Hamming cross-correlation is SI, then it follows from (2.2) that $\bar{H}_{s_1 \ldots s_k}$ is identically equal to $R_1 R_2 \cdots R_k$. In particular, $\bar{H}_{s_1 s_2}$ is identically equal to $R_1 R_2$ if it is SI.

Completely SI sequences enjoy a constant individual throughput property that is independent of any relative shift delays, and

are used as a building block in achieving the capacity of the collision channel without feedback [21]. Unfortunately, it is proved that completely SI sequences have long common periods [31]. This motivates the relaxation of the completely SI assumption to pairwise SI. Obviously, the collection of all completely SI sequence sets is a subset of the collection of pairwise SI sequences. However, pairwise SI sequences in general are not completely SI, which can be seen from the following example.

Example 2.1: Consider a set of 3 protocol sequences with duty factors 1/2, 1/3, and 1/5. One can check that the following sequence set is pairwise SI, but not completely SI:

$$s_1 = [11100011100011100011100011000]$$
$$s_2 = [11111000000000011111000000000]$$
$$s_3 = [11000000001100000000110000000]$$

For zero shift-delay, the 3-wise cross-correlation value is 2. However, the 3-wise cross-correlation value cannot be 2 for all shift-delays as the averaged 3-wise cross-correlation value should be 1 by (2.2).

From simulation studies, one can show that some pairwise SI sequences enjoy throughput performance close to SI sequences. It is of interest to understand whether short pairwise SI sequences can be constructed. A surprising result proven in this chapter is that for some combinations of duty factors, pairwise SI sequences are indeed completely SI. Moreover, we will show that for pairwise SI sequences the minimum period is exponential in the number of distinct sequences.

2.3 Discrete Fourier Analysis

Definition 2.3. A periodic sequence s can be represented by a polynomial with binary coefficients, denoted by $s(x)$,

$$s(x) := \sum_{t=0}^{L-1} s(t)x^t. \tag{2.3}$$

A complex number ω is called a *primitive* L-th root of unity if $\omega^L = 1$ but $\omega^n \neq 1$ for all $1 \leq n < L$. In this chapter, we will choose and fix a complex primitive L-th root of unity and denote it by ω. The discrete Fourier transform of sequence s is defined as $s(\omega^n)$ with n varying from 0 to $L-1$. A complex L-th root of unity ψ is called a *spectral null* of the sequence s if $s(\psi) = 0$.
A cyclic shift of a sequence s by τ corresponds to multiplying $s(x)$ by x^τ modulo $x^L - 1$. Therefore cyclically shifting a sequence does not alter the spectral nulls.

The next lemma is the discrete analog of Plancherel's identity [37].

Lemma 2.1. *Two sequences a and b with period L is pairwise SI if and only if $a(x)b(x)$ is divisible by $(x^L - 1)/(x - 1)$.*

Proof. Let $H_{ab}(\tau)$ be the pairwise Hamming cross-correlation function corresponding to a and b. We have

$$\begin{aligned}\sum_{\tau=0}^{L-1} H_{ab}(\tau)x^\tau &\equiv \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} a(t)b(t-\tau)x^\tau \\ &\equiv \sum_{t=0}^{L-1} a(t)x^{-t}\sum_{\tau=0}^{L-1} b(t-\tau)x^{t-\tau} \\ &\equiv a(x^{-1})b(x) \pmod{x^L - 1}. \end{aligned}\tag{2.4}$$

Hence $H_{ab}(\tau)$ is SI if and only if

$$a(x^{-1})b(x) \equiv h_0 \sum_{\tau=0}^{L-1} x^{\tau} \pmod{x^L - 1},$$

where h_0 denotes the common pairwise Hamming cross-correlation value. As the coefficients of $a(x)$ are real numbers, the spectral nulls of $a(x^{-1})$ are closed under taking reciprocal. Thus, spectral nulls of $a(x)$ and $b(x)$ contains all spectral nulls of $\sum_{\tau=0}^{L-1} x^{\tau} = (x^L - 1)/(x - 1)$. It follows that sequences a and b is pairwise SI if and only if $a(x)b(x)$ is divisible by $(x^L - 1)/(x - 1)$. □

In Example 2.1, the three polynomials $s_1(x)$, $s_2(x)$ and $s_3(x)$ are respectively

$$(x^2 + x + 1)\frac{x^{30} - 1}{x^6 - 1}, \quad \frac{x^5 - 1}{x - 1}\frac{x^{30} - 1}{x^{15} - 1}, \quad (x + 1)\frac{x^{30} - 1}{x^{10} - 1}.$$

It can be verified that $s_1(x)s_2(x)$, $s_2(x)s_3(x)$ and $s_3(x)s_1(x)$ are all divisible by $(x^{30} - 1)/(x - 1)$. Hence $\{s_1, s_2, s_3\}$ is a pairwise SI protocol set by Lemma 2.1.

2.4 Minimum Period

In subsequent discussions, we consider a set of M pairwise SI sequences, $s_1, \ldots, s_M$, with associated polynomial $s_1(x), \ldots, s_M(x)$. Let the duty factors be n_i/d_i, for $i = 1, 2, \ldots, M$, with n_i and d_i being relatively prime. Denote the common period of this sequence set by L. Let $p_1, \ldots, p_m$ be the prime factors of L, and $L = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$. Since L must be a multiple of the denominator d_i of each duty factor, the prime factorization of d_i can be written as $p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_m^{e_{im}}$ with $e_{i1} \leq r_1$, $e_{i2} \leq r_2, \ldots, e_{im} \leq r_m$.

Definition 2.4. For $n \geq 1$, the n-th *cyclotomic polynomial*, $f_n(x)$, is the monic polynomial whose zeros are precisely the complex primitive n-th roots of unity, each with multiplicity 1 [13, p.194].
For example, the 6th cyclotomic polynomial is

$$f_6(x) = (x - e^{2\pi\sqrt{-1}/6})(x - e^{-2\pi\sqrt{-1}/6}) = x^2 - x + 1.$$

We summarize below some results about cyclotomic polynomials that we will need in this chapter.

Lemma 2.2 ([13] Chapter 13).

(i) Cyclotomic polynomials are monic polynomials with integral coefficients.

(ii) $f_n(x)$ is a factor of $x^L - 1$ if and only if n divides L.

(iii) For all n, $f_n(x)$ is irreducible in the ring of polynomials with integral coefficients, i.e., if $f_n(x)$ divides $a(x)b(x)$, where $a(x)$ and $b(x)$ are polynomials with integral coefficients, then $f_n(x)$ divides $a(x)$ or $b(x)$, or both.

(iv) For a prime number p and positive integer m, the cyclotomic polynomial $f_{p^m}(x)$ equals $(x^{p^m} - 1)/(x^{p^{m-1}} - 1)$. Hence $f_{p^m}(1) = p$.

Definition 2.5. For $j = 1, 2, \ldots, m$, let

$$\mathcal{N}_j := \{f_{p_j^k}(x) : k = 1, 2, \ldots, r_j\}, \tag{2.5}$$

where r_j is the exponent of p_j in the factorization of L.

By part (ii) in Lemma 2.2, every cyclotomic polynomial $f(x)$ in $\mathcal{N}_j$ divides $(x^L - 1)/(x - 1)$, and by part (iv) in Lemma 2.2, we have $f(1) = p_j$ for all $f(x) \in \mathcal{N}_j$. It is noted that elements in $\mathcal{N}_j$ do not have common factors.

Lemma 2.3.

(i) For $i = 1, \ldots, M$ and $j = 1, \ldots, m$, at least e_{ij} cyclotomic polynomials in $\mathcal{N}_j$ does not divide $s_i(x)$.

(ii) If $\Phi_1(x)$ and $\Phi_2(x)$ are polynomials in $\mathcal{N}_j$ such that $\Phi_1(x)$ does not divide $s_i(x)$ and $\Phi_2(x)$ does not divide $s_k(x)$, for $i \neq k$, then $\Phi_1(x)$ and $\Phi_2(x)$ must be distinct.

Proof. (i) Suppose there are c_{ij} polynomials in $\mathcal{N}_j$ that divides $s_i(x)$, say $g_1(x), \ldots, g_{c_{ij}}(x)$. As they are monic polynomials with integral coefficents, we can write $s_i(x) = g_k(x)h_k(x)$ for each $k = 1, 2, \ldots, c_{ij}$, where $h_k(x)$ is a polynomial with integral coefficients. Let $g(x)$ be the product $g_1(x) \cdots g_{c_{ij}}(x)$. Because each factor $g_k(x)$ is irreducible, $s_i(x)$ is divisible by $g(x)$, i.e., $s_i(x) = g(x)h(x)$, for some polynomial $h(x)$ with integral coefficients. Then, by putting $x = 1$, and using the property that $g(1) = p_j^{c_{ij}}$ by part (iv) of Lemma 2.2, we see that $p_j^{c_{ij}}$ divides $s_i(1)$. On the other hand, $s_i(1) = n_i L/d_i$ by (2.3) and the definition of duty factor. Since n_i is relatively prime to d_i, $s_i(1)$ contains exactly $r_j - e_{ij}$ factors of p_j. Thus, $c_{ij} \leq r_j - e_{ij}$. It follows that e_{ij} is less than or equal to $r_j - c_{ij}$, which is exactly the number of polynomials in $\mathcal{N}_j$ that does not divide $s_i(x)$.

(ii) Suppose on the contrary that we can find $\Phi(x) \in \mathcal{N}_j$ such that $\Phi(x)$ does not divide $s_i(x)$ and $s_k(x)$, for $i \neq k$. Then by part (iii) of Lemma 2.2, $\Phi(x)$ does not divide $s_i(x)s_k(x)$. As $\Phi(x)$ is a factor of $(x^L - 1)/(x - 1)$ by part (ii) of Lemma 2.2, this contradicts the fact that $s_i(x)s_k(x)$ is divisible by $(x^L - 1)/(x - 1)$. □

Theorem 2.4. *The common period of any set of M pairwise SI sequences with duty factors n_i/d_i, for $i = 1, 2, \ldots, M$, (with n_i and d_i relatively prime) is divisible by $d_1 d_2 \cdots d_M$. In particular, the minimum common period is at least $d_1 d_2 \cdots d_M$.*

Proof. From Lemma 2.3, we conclude that $\mathcal{N}_j$ must contain at least $b_j := e_{1j} + e_{2j} + \ldots + e_{Mj}$ cyclotomic polynomials. Hence, $r_j \geq b_j$. Since the above inequality holds for all j, it follows that $\prod_{j=1}^{m} p_j^{b_j}$ divides L. But $d_1 d_2 \cdots d_M = \prod_{j=1}^{m} p_j^{b_j}$ by the definition of b_j. Therefore $d_1 d_2 \cdots d_M$ divides L. □

It is shown in [31] that the minimum common period of a set of M *completely* SI sequences, with duty factors as in Theorem 2.4, is at least $d_1 d_2 \cdots d_M$. We conclude from Theorem 2.4 that relaxing the completely SI requirement to pairwise SI *cannot* shorten the common period.

2.5 Structural Theorem

Theorem 11 in [31], although stated for completely SI sequences, depends only on the pairwise SI property. These results imply interesting structures for pairwise SI sequences.

Theorem 2.5 ([31]). *Suppose that the duty factors of a set of M pairwise SI sequences are n_i/p, for $i = 1, \ldots, M$, and p is a prime number. If the common period meets the lower bound in Theorem 2.4, i.e., the common period is p^M, then the least periods of the sequences are p, $p^2, \ldots, p^M$. Moreover, suppose that the sequence with least period p^i has duty factor n_i/p. For each r with $0 \leq r \leq p^{i-1} - 1$, there are exactly n_i ones located among positions*

$$r, r + p^{i-1}, r + 2p^{i-1}, \ldots, r + (p-1)p^{i-1}. \tag{2.6}$$

Theorem 2.6. *Let p be a prime. If M pairwise SI protocol sequences with duty factors n_i/p, for $i = 1, 2, \ldots, M$, have a common minimum period p^M, then they are completely SI.*

Proof. Theorem 2.5 implies that such pairwise SI sequences possess the structure described by (2.6). Theorem 8 in [31] established that such sequences are completely SI. □

Example 2.2: Consider the case that $M = 3$, $L = 27$ and the duty factors are all 2/3. We can verify that the following sequence set is pairwise SI by Lemma 2.1. It follows from Theorem 2.6 that it must be also completely SI.

$$s_1 = [110110110110110110110110110]$$
$$s_2 = [111111000111111000111111000]$$
$$s_3 = [111111111111111111000000000]$$

Remark: Theorem 2.6 explains why the construction in [6], which is targeted for pairwise SI sequences actually leads completely SI sequences.

2.6 Numerical Studies

Consider p pairwise SI sequences, each with duty factor R and period L. The sum throughput has a lower bound:

$$\sum_{i=1}^{p} \left[R - \sum_{j \neq i} \bar{H}_{s_i s_j}(0) \right] = p[R - R^2(p-1)] \tag{2.7}$$

For prime p, we can take $R = (p+1)/(2p^2)$ in the construction of wobbling sequences to obtain a lower bound on the sum throughput that approaches 1/4 as p approaches infinity [41]. Under the same condition, the sum throughput of pairwise SI sequences also

approaches 1/4 from (2.7).

Protocol sequences	Max. pairwise cross-correlation	L	Asymp. throughput lower bound
Pairwise SI	R^2	p^p	1/4
Wobbling	$\frac{(p+3)R^2}{p+1}$	p^4	1/4

If the pairwise cross-correlation function can vary slightly, as in wobbling sequences, the minimum period can be reduced. The two families of sequence sets achieve roughly the same throughput performance when p is large.

2.7 A Result on Completely Shift-Invariant Sequences

In this section, we consider a more general case of M potential users but at most K users are active at the same time. K can be any integer such that $2 \leq K \leq M$. We are interested in the sequence set of M sequences with any subset of K sequences is completely SI. The minimum common period of such sequence set is presented in [31] for $M = K$, which is a special case of the following result.

Theorem 2.7. *The minimum common period of any set of M sequences with duty factors n_i/d_i, for $i = 1, 2, \ldots, M$, (with n_i and d_i relatively prime), in which any K sequences with $2 \leq K \leq M$ are completely SI, is at least $d_1 d_2 \cdots d_M$.*

Proof. It is easy to see the sequence set described in the condition of Theorem 2.7 must be pairwise SI for any $K \geq 2$. Thus from Theorem 2.4, we know the minimum common period is at least $d_1 d_2 \cdots d_M$. □

2.8 Conclusion

In this chapter, pairwise SI protocol sequences are introduced. We have explored basic properties of its minimum period. Furthermore, if duty factors of the sequences satisfy some technical conditions, the sequence set is completely SI.

□ **End of chapter.**

Chapter 3

User-Irrepressible Sequences

Summary

In this chapter, we assume all potential users may be active simultaneously and consider user-irrepressible protocol sequences with the property that each active user is able to send at least one packet successfully in each sequence period in the slot-synchronized channel without feedback. A blocking algorithm is introduced to provide a necessary condition of user-irrepressible sequences. We further show that some user-irrepressible sequence sets must be pairwise shift-invariant with some special period and number of users.

3.1 Introduction

In this chapter, we continue to focus on the slot-synchronized collision channel without feedback described in Section 1.1, and consider a time-slotted system, consisting of M potential users and one sink, with all users may be active at the same time.

The protocol sequence set with the non-blocking property in the slot-synchronized channel is investigated in this chapter. We say that a protocol sequence set with M elements is *user-irrepressible* (UI) [35, 41] if M users (each of them assigned a unique protocol sequence from the set and transmit packets according to the protocol sequence when active) can all send out at least one packet successfully in each active period, no matter what the integer-delay offsets are.

We can make the following formal definition of UI sequence set.

Definition 3.1. Consider a protocol sequence set $\mathcal{S}$ of period L, consisting of M sequences $s_i(t)$, for $i = 1, 2, \ldots, M$. If there is a sequence in $\mathcal{S}$ that is blocked by the other sequences in $\mathcal{S}$, we say that $\mathcal{S}$ is *user-repressible*. Otherwise, $\mathcal{S}$ is said to be UI.

As an example, one can check the following four sequences are UI. It can also be viewed as a completely or pairwise shift-invariant sequence set introduced in Chapter 2.

$$s_1 = [1010101010101010]$$
$$s_2 = [1100110011001100]$$
$$s_3 = [1111000011110000]$$
$$s_4 = [1111111100000000].$$

We note that this is a guarantee with probability one that each

user has at least one successfully sent packet in a fixed time length, in contrast to random access scheme, like slotted ALOHA [2, 3], where it is only guaranteed that with some probability strictly less than one. Application of the strict guarantee can be found in [28] for medical systems.

This chapter is organized as follows. We present some preliminary results in Section 3.2. A blocking algorithm and a necessary condition for the existence of UI sequences are given in Section 3.3. In Section 3.4, we show that in some special cases where the lower bound on period is met with equality, UI sequences possess some special structures. Finally, we close this chapter with some concluding remarks in Section 3.5.

3.2 Preliminaries

We state two simple propositions which will be useful in this chapter.

Proposition 3.1. *Suppose sequence s_1 is blocked by s'_2, $s'_3, \ldots s'_M$, and $s'_i \preceq s_i$ for $i = 2, 3, \ldots, M$. Then s_1 is blocked by s_2, $s_3, \ldots, s_M$.*

Proof. It follows immediately from

$$\begin{aligned} s_1 &\preceq (s_2^{\prime(\tau_2)} \vee s_3^{\prime(\tau_3)} \vee \ldots \vee s_M^{\prime(\tau_M)}) \\ &\preceq (s_2^{(\tau_2)} \vee s_3^{(\tau_3)} \vee \ldots \vee s_M^{(\tau_M)}). \end{aligned}$$

□

The following elementary property for pairwise Hamming cross-correlation is a special case of (2.2) due to [29]. We include the short proof here for the sake of completeness.

Proposition 3.2 ([29]). *Given two binary sequences $s_1(t)$ and $s_2(t)$, we have*

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

Proof.

$$\begin{aligned}\sum_{\tau=0}^{L-1} H_{s_1 s_2}(\tau) &= \sum_{\tau=0}^{L-1}\sum_{t=0}^{L-1} s_1(t) s_2(t+\tau) \\ &= \sum_{t=0}^{L-1} s_1(t) \sum_{\tau=0}^{L-1} s_2(t+\tau) \\ &= \sum_{t=0}^{L-1} s_1(t) \sum_{\tau=0}^{L-1} s_2(\tau) = w_H(s_1) w_H(s_2).\end{aligned}$$

□

3.3 Blocking Algorithm

Let $\mathcal{S} = \{s_1, s_2, \ldots, s_M\}$ be a set of M protocol sequences of period L. We describe below a generic blocking algorithm whose objective is to cyclically shift $s_2, s_3, \ldots, s_M$, so that the first sequence s_1 is blocked by $\bigvee_{k=2}^{M} s_k^{(\tau_k)}$.

1. Fix the delay offset of s_1 to zero.
2. Cyclically shift s_2 so that maximal number of "1"s in s_1 is overlapped by $s_2^{(\tau_2)}$.
3. Cyclically shift s_3 in such a way that most of the remaining "1"s in s_1 are overlapped by $s_3^{(\tau_3)}$.
4. Cyclically shift s_4 in order to cover most of the remaining "1"s in s_1 that are not overlapped by $s_2^{(\tau_2)}$ and $s_3^{(\tau_3)}$.

5. Continue for s_5, $s_6, \ldots, s_M$.

In Theorem 3.3, we will specify how to choose the delay offsets τ_2 and τ_3 etc., and give a condition under which s_1 is guaranteed to be blocked by the above procedure.

Theorem 3.3 ([36]). *Let $\mathcal{S} = \{s_1, s_2, \ldots, s_M\}$ be a set of M protocol sequences of period L. Suppose that s_1 has the smallest Hamming weight, i.e., $w_H(s_1) = w$ and $w_H(s_i) \geq w$ for $i = 2, \ldots, M$. Define an integer sequence $(r_k(w, L))_{k=0}^{\infty}$ recursively by*

$$r_0(w, L) := w \tag{3.1}$$

$$r_k(w, L) := r_{k-1}(w, L) - \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil, \quad \text{for } k \geq 1. \tag{3.2}$$

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

Proof. Let $x_1(t)$ be the sequence $s_1(t)$. In this proof, we will recursively define $M - 1$ sequences $x_2(t), x_3(t), \ldots, x_M(t)$, with the property that $w_H(x_k) = r_{k-1}(w, L)$, for $k = 2, 3, \ldots, M$. We first note that the Hamming weight of $x_1(t)$ is equal to $r_0(w, L) = w$.

Because $w_H(x_1) = w$ and $w_H(s_2) \geq w$, from Proposition 3.2, we obtain

$$\sum_{\tau=0}^{L-1} H_{x_1 s_2}(\tau) = w_H(x_1) w_H(s_2) \geq w^2. \tag{3.3}$$

We can interpret the above inequality as: the mean pairwise Hamming cross-correlation, averaged over all delay offsets, is at least w^2/L. Hence, we can find some delay offset τ such that $H_{x_1 s_2}(\tau) \geq w^2/L$. If on the contrary we have $H_{x_1 s_2}(\tau) < w^2/L$ for all $\tau = 0, 1, \ldots, L - 1$, then

$$\sum_{\tau=0}^{L-1} H_{x_1 s_2}(\tau) < L(w^2/L) = w^2,$$

contradicting (3.3). We pick a delay offset, say τ_2, so that

$$H_{x_1 s_2}(\tau_2) \geq \lceil w^2/L \rceil.$$

By removing some "1"s in s_2 if necessary, we define another binary sequence $s_2' \preceq s_2$ such that

$$H_{x_1 s_2'}(\tau_2) = \lceil w^2/L \rceil.$$

Let the sequence obtained from x_1 by removing the "1"s that are overlapped by $s_2^{\prime(\tau_2)}$ be x_2. We note that $x_2 \preceq x_1$, and

$$w_H(x_2) = w - \lceil w^2/L \rceil = r_1(w, L).$$

Given $x_{k-1}(t)$, we recursively define $x_k(t)$ in a similar fashion. In the kth step, by Prop. 3.2, we have

$$\sum_{\tau=0}^{L-1} H_{x_k s_{k+1}}(\tau) = w_H(x_k) w_H(s_{k+1}) \geq w r_{k-1}(w, L).$$

We can find a delay offset τ_{k+1} for s_{k+1} such that

$$H_{x_k s_{k+1}}(\tau_{k+1}) \geq \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil.$$

Let $s_{k+1}' \preceq s_{k+1}$ be obtained by removing some "1"s from s_{k+1} so that

$$H_{x_k s_{k+1}'}(\tau_{k+1}) = \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil.$$

Let the sequence obtained from x_k by removing the "1"s that are overlapped by $s_{k+1}^{\prime(\tau_{k+1})}$ be x_{k+1}.

Since by construction, the Hamming cross-correlation between x_k and s_{k+1}' is exactly $\left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil$, the Hamming weight of x_{k+1} is

$$\begin{aligned} w_H(x_{k+1}) &= w_H(x_k) - \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil \\ &= r_{k-1}(w, L) - \left\lceil \frac{w}{L} r_{k-1}(w, L) \right\rceil \\ &= r_k(w, L). \end{aligned}$$

We repeat the above process until we get x_M. By induction, the Hamming weight of x_M is equal to

$$w_H(x_M) = r_{M-1}(M, L).$$

If $r_{M-1}(M, L) = 0$ holds, then the Hamming weight of x_M is zero. In other words, s_1 is blocked by $s_2^{\prime(\tau_2)} \vee s_3^{\prime(\tau_3)} \vee \ldots \vee s_M^{\prime(\tau_M)}$. By Proposition 3.1, we conclude that s_1 is also blocked by $s_2, s_3, \ldots, s_M$. □

3.4 Special Structures

In [36], a more detailed analysis of the integer sequence $r_k(w, L)$, shows that Theorem 3.3 gives a lower bound of $(8/9)M^2$ on the period of UI sequence set of M sequences for all M. It improves upon the previous lower bound $1 + M(M-1)/2$ from [5]. As a special case, we have the lower bound $8k^2$, for the case $M = 3k$.

We use $\mathsf{UIS}(L, M)$ to denote a set of M UI sequences with period L.

Theorem 3.4. *If there exists a $\mathsf{UIS}(8k^2, 3k)$ for $k \geq 1$, then the smallest Hamming weight of the sequences is $w = 4k$.*

Proof. It is shown in [36] that $M \leq \sqrt{L}(3/\sqrt{8})$ and the equality holds only if $w = \sqrt{2L}$. Then for the case $L = 8k^2$, we know $M = 3k$ and $w = 4k$. This completes the proof. □

We next show that $\mathsf{UIS}(L, 3k)$ must be pairwise shift-invariant (SI) if the period meets the lower bound $8k^2$.

Theorem 3.5. *For $k \geq 1$, any $\mathsf{UIS}(8k^2, 3k)$ is pairwise SI.*

Proof. Suppose that $\mathcal{S}$ is a set of $M = 3k$ UI protocol sequences with period $L = 8k^2$. From Theorem 3.4, we can support $M = 3k$

users with period $L = 8k^2$ only if the smallest Hamming weight of the sequences is $w = 4k$. We want to show that (a) the Hamming weight of each sequence is equal to $4k$ and (b) the Hamming cross-correlation between *every* pair of distinct sequences equals 2.

Suppose that $s_1(t)$ is a sequence with Hamming weight $4k$, and suppose that there is another sequence in $\mathcal{S}$, say $s_2(t)$, whose Hamming weight is strictly larger than $4k$. From Proposition 3.2, the average pairwise Hamming cross-correlation over all delay offsets is equal to

$$\frac{w_H(s_1)w_H(s_2)}{L} > \frac{(4k)(4k)}{8k^2} = 2.$$

We can hence find a delay offsets τ_2 such that $H_{s_1 s_2}(\tau_2) \geq 3$. By removing some "1"'s in s_2, we replace s_2 by a new sequence s_2' with the property that

$$H_{s_1 s_2'}(\tau_2) = 3.$$

We now continue the blocking algorithm described in Section 3.3, and compute the sequence of integers $r_k(w, L)$ for $k = 2, 3, \ldots$, which equal

$$\underbrace{4k-3,\ 4k-5,\ \ldots, 2k+1}_{k-1},\ \underbrace{2k-1,\ 2k-2,\ \ldots, 1}_{2k-1}, 0,\ \ldots.$$

There are $3k - 2$ integers in the above integer sequence. The algorithm stops after we introduce $3k - 2$ more protocol sequences after s_2', and hence s_1 is blocked by s_2', s_3, $s_4, \ldots, s_{3k}$. Therefore, by Proposition 3.1, s_1 can be blocked by s_2, $s_3, \ldots, s_{3k}$. This contradicts Definition 3.1, and proves that every sequence in $\mathcal{S}$ has Hamming weight $4k$. This proves (a).

Having proved that the Hamming weight of each sequence in $\mathcal{S}$ is equal to $4k$, we calculate the average Hamming cross-correlation between two distinct sequences, say s_1 and s_2. By Proposition 3.2

again,

$$\frac{w_H(s_1)w_H(s_2)}{L} = \frac{(4k)(4k)}{8k^2} = 2.$$

If the Hamming cross-correlation between s_1 and s_2 is equal to 3 or larger for some delay offset τ, then the same procedure described in the previous paragraph applies verbatim, and leads to a contradiction with user-irrepressibility. So, the pairwise Hamming cross-correlation is less than or equal to 2 for all delay offsets. However, the average value is also equal to 2. This implies that it must be identically equal to 2 for all delay offsets. Thus $\mathcal{S}$ is pairwise SI. □

Example 3.1: The following three sequences form a $\mathsf{UIS}(8,3)$ which is pairwise SI. This verifies Theorem 3.5 for $k = 1$. However, this is the only example possible.

$$s_1 = [10101010]$$
$$s_2 = [11001100]$$
$$s_3 = [11110000]$$

Corollary 3.6. *For $k \geq 2$, there is no $\mathsf{UIS}(8k^2, 3k)$.*

Proof. In Theorem 2.4 of previous chapter, it is shown that the period of pairwise SI sequences grows exponentially as a function of the number of users; the period of pairwise SI sequences for M users is at least 2^M. Any $\mathsf{UIS}(8k^2, 3k)$ must be pairwise SI by Theorem 3.5. If a $\mathsf{UIS}(8k^2, 3k)$ exists, the period $8k^2$ must be larger than 2^{3k}, which cannot hold for $k \geq 2$. □

An implication of Corollary 3.6 is that for $k \geq 2$, the lower bound $8k^2$ on minimal period cannot be attained. So, for $k \geq 2$, the minimum period of UI sequences for $3k$ users is at least $8k^2 + 1$.

3.5 Conclusion

A blocking algorithm is introduced in this chapter to provide a necessary condition of non-blocking property in the slot-synchronized channel. We further present some special properties in UI sequence set with some special period and number of users.

□ **End of chapter.**

Chapter 4

Completely Irrepressible Sequences

Summary

In this chapter we assume all potential users are active all the time and consider protocol sequence sets with the property that each active user is able to send at least one packet successfully in its each active period for the asynchronous channel without feedback. Such sequence sets are said to be completely irrepressible. We analyze the class of completely irrepressible sequence set with the minimum number of ones in each period, and derive the lower bound on its minimum period. Moreover, for equi-difference sets, we improve the lower bound and present a construction method that meets this lower bound asymptotically.

4.1 Introduction

4.1.1 Background and Motivation

In this chapter, we follow the asynchronous model described in Section 1.1 to define a time-slotted system, consisting of M potential users and one sink, with all users are active all the time. Let δ_i be the time offset of user i for $i = 1, 2, \ldots, M$. All δ_i are arbitrary real numbers. Thus user i would start its transmission scheme at the time index δ_i. If for some non-negative integer n_0, user i is active in its n_0-th slot and the sequence value is equal to one, then user i will transmit its packet at time interval $[n_0 + \delta_i, n_0 + \delta_i + 1)$. This packet is assumed to be successful if and only if it is not completely or partially overlapped by any other packet.

UI [5,35,41] sequence sets provide the non-blocking property in the slot-synchronized channel. However, all UI sequence sets known so far cannot guarantee the non-blocking property if the channel is asynchronous. An example is the following.

Example 4.1: s_1, s_2 and s_3 form a UI sequence set:

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

In the asynchronous channel, for $\delta_1 = 0$, $\delta_2 = 0.5$ and $\delta_3 = 2$, all packets from user 1 are lost due to two partially overlapping collisions and one completely overlapping collision, as illustrated in Fig. 4.1.

In this chapter, we consider the non-blocking property in the asynchronous channel. More strictly speaking, a protocol sequence set of M elements is said to be *completely irrepressible* (CI) if each

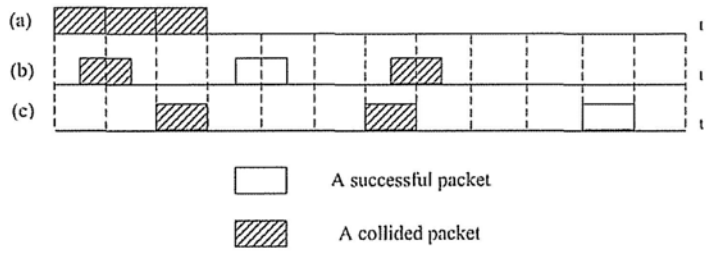

Figure 4.1: (a) Packets from user 1, (b) packets from user 2, (c) packets from user 3.

of M users can send out at least one packet successfully in its each active period, for any real numbers $\delta_1, \delta_2, \ldots, \delta_M$. Obviously, a CI sequence set must be UI since the collection of all possible time offsets in the slot-synchronized channel is just a subset of that in the asynchronous channel.

4.1.2 Notations and Preliminaries

If x is a real number, the notation $\lfloor x \rfloor$ represents the largest integer less than or equal to x. The smallest integer larger than or equal to x is denoted by $\lceil x \rceil$.

Definition 4.1. For all $t \in [0, L)$, define $f_s(t)$ as the *protocol signal* generated by s at $\lfloor t \rfloor$. That is,

$$f_s(t) := s(\lfloor t \rfloor).$$

Given two sequences s_1 and s_2, define the *asynchronous pairwise Hamming cross-correlation* of f_{s_1} and f_{s_2} by

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

The subtraction $t - \delta$ is performed modulo L. When δ is an integral number τ, it reduces to the usual notion of *pairwise Hamming*

cross-correlation.

For all $\delta \in [0, L)$, the following property holds for the asynchronous pairwise Hamming cross-correlation function.

Proposition 4.1. *Given two binary sequences s_1 and s_2, both with period L, we have*

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

Proof.

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

□

When restricted to an integer δ, the result in Proposition 4.1 reduces to the well-known elementary property of pairwise Hamming cross-correlation presented in Proposition 3.2 due to [29].

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

Proposition 4.2. *If a sequence set $\{s_1, s_2, \ldots, s_M\}$ is CI, then we have $w_H(s_i) \geq M$ for $i = 1, 2, \ldots, M$.*

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

From the construction presented in Section 4.4, for any M, we can see there exists a CI sequence set of M sequences, each with Hamming weight M. Thus we find the lower bound in Proposition 4.2 can be achieved for any M. In order to enhance battery life of a sensor network, we want to design CI protocol sequence set with the number of packets sent in each period as small as possible. Thus we say a CI sequence set of M sequences is *minimal energy CI* (MCI) if the Hamming weight of each sequence is M. We use $\mathsf{MCIS}(L, M)$ to denote a MCI sequence set of M sequences with period L. Specially we denote an equi-difference $\mathsf{MCIS}(L, M)$ by $\mathsf{MCIS}^e(L, M)$.

4.1.3 Main Results

The objective in this chapter is to construct MCI protocol sequence sets with period as small as possible in order to minimize the transmission delay in the worst case scenario. Furthermore, to investigate the shortest latency that can be achieved, we want to determine $L_{\min}(M)$, the smallest period L such that a $\mathsf{MCIS}(L, M)$ exists.

Equi-difference sequence set is an important class of protocol sequence sets with non-blocking property. Some bounds and constructions of equi-difference UI sequence set have been investigated

in [23] and [34]. Moreover, it was shown that almost all known shortest UI sequence sets with least ones in a period enjoy the equi-difference structure. Thus we also focus on $L^e_{\min}(M)$, the smallest period L such that a $\mathsf{MCIS}^e(L, M)$ exists.

This chapter is organized as follows. After proving several important properties of CI sequence set in Section 4.2, we establish a lower bound on $L_{\min}(M)$ and an asymptotic lower bound on $L^e_{\min}(M)$ in Section 4.3. Then a construction that meets the asymptotic bound on $L^e_{\min}(M)$ is presented in Section 4.4. Section 4.5 gives a comparison with random access scheme in terms of blocking probability and time length. Finally, we make a conclusion in Section 4.6.

4.2 Properties of Completely Irrepressible Sequence Set

In our channel model, if user i starts its packet transmission at time index $k_0 + \delta_i$ for some non-negative integer k_0, this packet is successfully received if and only if no any other user would start or end its transmission at interval $[k_0 + \delta_i, k_0 + \delta_i + 1)$. For studying the individual successful transmission amount in the asynchronous channel to see whether a protocol sequence set is CI or not, we present the following result by generalizing the observation in [21]. δ_{max} is used to denote the maximum value of δ_i for $i = 1, 2, \ldots, M$. Given a sequence s, we construct s' as:

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

Given $s_1, s_2, \ldots, s_M$ and $\delta_1, \delta_2, \ldots, \delta_M$, the sequence set $T_i =$

$\{s_{i\_1}, s_{i\_2}, \ldots, s_{i\_M}\}$ for $i = 1, 2, \ldots, M$, is constructed as the following rule:

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

Proposition 4.3. *For $i = 1, 2, \ldots, M$, we have*

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

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

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

$$\bigvee_{j=1, j\neq i}^{M} f_{s_j}(t - \delta_j) = 0 \tag{4.1}$$

for any $t \in [k_0 + \delta_i, k_0 + \delta_i + 1)$. Let ξ_1 be the collection of all $j \in \{1, 2, \ldots, M\} \setminus \{i\}$ such that $\lfloor \delta_j - \delta_i \rfloor \neq \delta_j - \delta_i$. Let ξ_2 be $\{1, 2, \ldots, M\} \setminus \{i, \xi_1\}$. Then from (4.1) we have the following formula

to find this packet is not successful if it is equal to one.

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

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

integral number k such that $k + \delta_i \geq \delta_{max}$ can be found as:

$$\begin{aligned}
&\sum_{k_0=k}^{k+L-1} \left\lceil \int_{k_0+\delta_i}^{(k_0+1+\delta_i)^-} f_{s_i}(t-\delta_i) \bigvee_{j=1,j\neq i}^{M} f_{s_j}(t-\delta_j)\, dt \right\rceil \\
&= \sum_{k_0=k}^{k+L-1} s_i(k_0) \bigvee_{j=1,j\neq i}^{M} s_{i_j}(k_0) \\
&= \sum_{k_0=0}^{L-1} s_{i_i}(k_0) \bigvee_{j=1,j\neq i}^{M} s_{i_j}(k_0),
\end{aligned}$$

which implies the number of covered ones of s_{i_i} in T_i. Thus the claim (i) of Proposition 4.3 is proved.

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

The following equivalent condition for the non-blocking property in the asynchronous channel directly follows Proposition 4.3.

Theorem 4.4. *A sequence set $\{s_1, s_2, \ldots, s_M\}$ is CI iff s_{i_i} is unblocked in T_i for any $\delta_1, \delta_2, \ldots, \delta_M$ and any $i \in \{1, 2, \ldots, M\}$.*

As an example, consider the protocol sequence set in Example 4.1 with the time offset $(\delta_1 = 0.5, \delta_2 = 1, \delta_3 = 2.5)$ in the asynchronous channel. To obtain the number of successful slots from user 1, we find T_1 as

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

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

Following Proposition 4.3, we know that T_i is determined by i and δ_j for $j = 1, 2, \ldots, M$. Thus for every distinct user, we have T_i may be different from T_j if $i \neq j$. For example, T_3 can be found as

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

Then we have the following equivalent condition for minimal energy non-blocking property in the asynchronous channel.

Theorem 4.5. *A sequence set $\{s_1, s_2, \ldots, s_M\}$ with $w_H(s_i) = M$ for $i = 1, 2, \ldots, M$ is MCI iff we have $H_{s_i s'_j}(\tau) \leq 1$ for any integer τ and any pair of distinct i and j.*

Proof. We first prove the "only if" part by contradiction. Suppose $H_{s_i s'_j}(\tau_0) > 1$ for some integer τ_0 and some j with $j \neq i$. Then by letting $\tau_0 < \delta_j - \delta_i < \tau_0 + 1$, we have $s_{i\_i} = s_i$ and $s_{i\_j} = s_j^{\prime(\tau_0)}$ in T_i. Thus we have at least two ones of s_{i_i} are covered by s_{i_j}. Then from $w_H(s_{i\_i}) = w_H(s_i) = M$, we know there are at most $M - 2$ remaining ones in s_{i_i}. We can choose some delay offsets of other $M - 2$ sequences such that the remaining $M - 2$ ones are totally covered in T_i. Thus we find s_{i_i} is covered in T_i. Following Theorem 4.4, we further have $\{s_1, s_2, \ldots, s_M\}$ is not CI, which contradicts the condition.

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

$$H_{s_i s_j}(\lfloor \delta_j - \delta_i \rfloor) \leq H_{s_i s'_j}(\lfloor \delta_j - \delta_i \rfloor).$$

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

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

Thus we can conclude s_{i_i} is unblocked in T_i for any i and any $\{\delta_1, \delta_2, \ldots, \delta_M\}$. It implies $\{s_1, s_2, \ldots, s_M\}$ is thus CI following Theorem 4.4. It is also MCI as each sequence has Hamming weight M. □

In the view of the difference sets, we have the following version of Theorem 4.5.

Theorem 4.6. *Let $\mathcal{I}_{s_j}$, $j = 1, 2, \ldots, M$, be the characteristic sets of M sequences of period L, such that $\mathcal{I}_{s_j}$ contains exactly M elements in $\mathbb{Z}_L$ for all j. Let α_j be any element in $d^*(\mathcal{I}_{s_j})$ for $j = 1, 2, \ldots, M$. The corresponding sequence set is MCI iff*

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

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

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

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

(i) Suppose $1, L-1 \in d^*(\mathcal{I}_{s_i})$. We also have $1 \in d^*(\mathcal{I}_{s'_j})$ following the construction of s'_j. Then we can find some integer τ_0 such that $H_{s_i s'_j}(\tau_0) = 2$ as there is a common element 1 between $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s'_j})$. From Theorem 4.5, we know the sequence set is not CI contradicting the condition. We thus have $1, L-1 \notin d^*(\mathcal{I}_{s_j})$ for $j = 1, 2, \ldots, M$.

(ii) Suppose $\alpha_i = \alpha_j$ for some distinct i and j. Then we have $H_{s_i s_j}(\tau_0) = 2$ for some integer τ_0. It implies $H_{s_i s'_j}(\tau_0) \geq 2$ which contradicts Theorem 4.5. Thus we have $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s_j})$ are disjoint for all pairs of distinct i and j.

(iii) If $\alpha_j \in d^*(\mathcal{I}_{s_j})$, we can find $\alpha_j \pm 1 \in d^*(\mathcal{I}_{s'_j})$ from the construction of s'_j. Suppose $\alpha_i - \alpha_j = 1$. Then we can find some integer-delay τ_0 such that $H_{s_i s'_j}(\tau_0) = 2$ as there is a common element $(\alpha_j + 1)$ between $d^*(\mathcal{I}_{s_i})$ and $d^*(\mathcal{I}_{s'_j})$. Thus from Theorem 4.5 we know the sequence set is not CI contradicting the condition. By the same argument, $\alpha_i - \alpha_j = -1$ would also make the contradiction. Therefore, $\alpha_i - \alpha_j \neq \pm 1$ is a necessary condition here.

Next we will prove the "if" part.

With the conditions and the construction of s'_j, we must have $H_{s_i s'_j}(\tau) \leq 1$ for any integer τ and any pair of distinct i and j. Following Theorem 4.5, it suffices to show that the entire sequence set is MCI. □

Remark: For the slot-synchronous channel, i.e., δ_i is an integer for all i, we have $s'_j = s_j$ for $j = 1, 2, \ldots, M$. Thus the equivalent condition in Theorem 4.5 is reduced to $H_{s_i s_j}(\tau) \leq 1$ for any integer τ and any pair of distinct i and j. Furthermore, we have (ii) of Theorem 4.6 is an equivalent condition here.

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

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

The following lower bound on $L_{\min}(M)$ hinges on elementary property of pairwise Hamming cross-correlation in Proposition 3.2.

Theorem 4.7. *For $M \geq 2$, we have*

$$L_{\min}(M) \geq 2M^2. \tag{4.2}$$

Proof. For distinct i and j, the Hamming weight of s_i and s_j are both known as M. With (i) of Theorem 4.6 we know there is no adjacent ones in s_j. Then by the construction of s'_j, we find the Hamming weight of s'_j is equal to $2M$. Thus from Proposition 3.2, we know $H_{s_i s'_j}(\tau)$ averaged over all integer τ, is equal to $2M^2/L$. Then if $2M^2/L > 1$, we can find some τ_0 such that $H_{s_i s'_j}(\tau_0) \geq 2$, which contradicts Theorem 4.5. Therefore, we can conclude that $2M^2/L \leq 1$ or equivalently $L \geq 2M^2$. □

Example 4.2: s_1 and s_2 form a MCIS$(8, 2)$:

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

It is easy to see that the bit structure is in accordance with Theorem 4.6 from the following:

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

From Theorem 4.7, we know the above is the shortest MCI sequence set for $M = 2$.

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

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

For the slot-synchronized channel, one can check the difference sets below are just in accordance with (ii) of Theorem 4.6.

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

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

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

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

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

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

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

Theorem 4.8. *For any $\mathsf{MCIS}^e(L, M)$, we have*

$$|\Gamma_M| \geq M - \pi(2M - 2). \tag{4.3}$$

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

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

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

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

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

case 1: $m_1 g_1 - (-m_2 g_1) = 1 \bmod L$;

case 2: $(-m_4 g_1) - m_3 g_1 = 1 \bmod L$;

case 3: $m_5 g_1 - m_6 g_1 = 1 \bmod L$.

It is easy to see that case 3 implies there exists two consecutive ones in s_1. It contradicts (i) of Theorem 4.6. Thus we can rule out the case 3 and just need to consider the first two cases. The case that $m_1 + m_2 < M$ or $m_3 + m_4 < M$ can also be ruled out due to it also implies that there exists a consecutive two ones' run in s_1 contradicting (i) of Theorem 4.6. By letting $n_1 = (m_1 + m_2)$ and $n_2 = (m_3 + m_4)$, both ranged from M to $2M - 2$, we can further simplify the two cases into

$$n_1 g_1 = 1 \bmod L; \tag{4.4}$$

$$n_2 g_1 = -1 \bmod L. \tag{4.5}$$

Also, we can find n_1 is relatively prime to L. Otherwise over $\mathbb{Z}_L$, the result of $n_1 g_1$ should be located in $[2, L-2]$, which contradicts (4.4). The same result can also be found for n_2 and L.

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

$$r_1 g_2 = 1 \bmod L; \tag{4.6}$$

$$r_2 g_2 = -1 \bmod L. \tag{4.7}$$

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

Consider (4.4) and (4.6) first. Combining them we have

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

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

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

If $v_1 > 1$, we can find (n_1/v_1) and (r_1/v_1) are both smaller than M from $n_1, r_1 \leq 2M - 2$. It further implies that there is a common element between $d^*(\mathcal{I}_{s_1})$ and $d^*(\mathcal{I}_{s_2})$, which contradicts (ii) of Theorem 4.6. Therefore we find that $v_1 = 1$, i.e., n_1 and r_1 are relatively prime.

Then consider (4.4) and (4.7). Combining them we have

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

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

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

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

For (4.5) and (4.6), similarly we also can get that n_2 and r_1 are relatively prime. The result is also true for n_2 and r_2 considering (4.5) and (4.7). Therefore, by the above argument we can conclude that the four pairs (n_1, r_1), (n_1, r_2), (n_2, r_1), (n_2, r_2) are all relatively prime respectively. In other words, if there are two sequences not in Γ_M, at least one case of the above would occur, then there are at least two proper integral numbers, ranged from M to $2M - 2$, such that they are relatively prime.

The above claim can be easily generalized to that there are $M - |\Gamma_M|$ sequences not in Γ_M. Then there are $M - |\Gamma_M|$ proper integral

numbers, ranged from M to $2M-2$, namely $\beta_1, \beta_2, \ldots, \beta_{M-|\Gamma_M|}$, such that they are mutually relatively prime. The number of these integers is less than or equal to the maximal number of relatively prime integers between 2 and $2M-2$. We thus have $M-|\Gamma_M|$ less than or equal to $\pi(2M-2)$. □

We state a version of Kneser's theorem, which is tailored to what we need here. It will be useful to derive the asymptotic lower bound on $L^e_{\min}(M)$. A proof of Kneser's theorem can be found in [19].

Theorem 4.9 (Kneser [16]). *If a subset $\mathcal{I}$ in $\mathbb{Z}_L$ satisfies*

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

then there exists a proper divisor α of L such that

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

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

Furthermore, in view of Kneser's theorem, we classify M sequences in a given $\mathsf{MCIS}^e(L, M)$ into two types. We say that a sequence is in *class 1* if the associated set of differences contains the multiples of a proper divisor of L, otherwise, we say that it is in *class 2*. Denote the set of sequences in class 2 as Υ_M. As proved in [35], we have the following asymptotic result:

$$\liminf_{M\to\infty} \frac{|\Upsilon_M|}{M} = 1. \tag{4.8}$$

Theorem 4.10.

$$\liminf_{M\to\infty} \frac{L^e_{\min}(M)}{4M^2} \geq 1. \tag{4.9}$$

Proof. By the prime number theorem, we know $\pi(x)$ is close to $x/\ln x$ for large M. Thus following (4.3) we have

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

which implies

$$\liminf_{M\to\infty} \frac{|\Gamma_M|}{M} = 1, \tag{4.10}$$

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

Given a $\mathsf{MCIS}^e(L,M)$, let Ω_M be $\Gamma_M \cap \Upsilon_M$. With Theorem 4.9 and $\Omega_M \subseteq \Upsilon_M$, we see the total number of distinct elements in all $d^*(\mathcal{I}_{s_j})$ for $s_j \in \Omega_M$ is at least

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

Following Theorem 4.6, the definition of Γ_M and $\Omega_M \subseteq \Gamma_M$, we know the difference of any pair elements in all $d^*(\mathcal{I}_{s_j})$, $s_j \in \Omega_M$, is at least two. Thus, the nonzeros in $\mathbb{Z}_L$ should contain at least $|\Omega_M|(2M-2)$ distinct elements whose mutual difference is at least two. Also we have 1 and $L-1$ are not contained in these elements from (i) of Theorem 4.6. Then we have

$$L-1 \geq 1+2|\Omega_M|(2M-2). \tag{4.11}$$

We define ε_1 and ε_2 as the following respectively:

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

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

Combining them, we have

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

which implies

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

Then following (4.8), (4.10) and the above, we have

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

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

$$\liminf_{M\to\infty} \frac{|\Omega_M|}{M} = 1. \tag{4.12}$$

Hence the following result can be found from (4.11) and (4.12):

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

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

□

4.4 An Asymptotically Optimal Construction

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

Theorem 4.11. *Given a $\mathsf{MUIS}(L, M)$, then a $\mathsf{MCIS}(2L, M)$ can be constructed by doubling all elements in the characteristic set of each sequence.*

Proof. In the slot-synchronized channel, following the construction of s'_j, Theorem 4.5 can be found reduced to $H_{s_i s_j}[\tau] \leq 1$ for any integer τ and any pair of distinct i and j, for any $\mathsf{MUIS}(L, M)$. Thus we find (ii) of Theorem 4.6 holds. By doubling all elements in the characteristic set of each sequence and period, we further find (i) and (iii) of Theorem 4.6 hold since the difference of any two distinct even numbers is even. Therefore, from Theorem 4.6 we can conclude this new sequence set is a $\mathsf{MCIS}(2L, M)$. □

Remark: The variation is found as a special case of Lemma 1.1 due to [21] which is targeted for achieving the capacity of the asynchronous collision channel without feedback.

Theorem 4.10 asserts that $L^e_{\min}(M)$ is lower bounded by $4M^2$ approximately when M is large. In order to design a $\mathsf{MCIS}^e(L, M)$ with period achieving $4M^2$ asymptotically, the following construction for UI sequence set is introduced.

CRT Construction: The construction is based on Chinese remainder theorem (CRT). The mapping $f : \mathbb{Z}_{pq} \to \mathbb{Z}_p \oplus \mathbb{Z}_q$ defined by $f(a) := (a \bmod p, a \bmod q)$ is a bijection from $\mathbb{Z}_{pq}$ to $\mathbb{Z}_p \oplus \mathbb{Z}_q$ when p and q are relatively prime [13], and preserves addition and multiplication by integers. Given M, we set q to be $2M - 1$, and p any prime larger than or equal to M and relatively prime to $2M - 1$. Let u be any integer ranged from 1 to $M - 1$, relatively prime to $2M - 1$. For $j = 0, 1, \ldots, M - 1$, we let

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

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

Remark: The construction above is similar to [32] which also employs Chinese remainder theorem. When $u = 1$, it is the same

as the original construction in [35].

Let h be the number of integers ranged from 1 to $M-1$ and relatively prime to $2M-1$. The following is a generalization of that in [35].

Theorem 4.12. *For all M, the sequences by CRT construction form h distinct $\mathsf{MUIS}^e(p(2M-1), M)$s consisting of hM distinct sequences.*

Proof. First we know that all sequences formed by CRT construction are equi-difference. For $s_{j,u}$, its common difference can be found as (j, u) or $(p-j, 2M-1-u)$. Then we will show $s_{j,u}$ for $j = 0, 1, \ldots, M-1$ form a $\mathsf{MUIS}^e(p(2M-1), M)$. Suppose for the sake of contradiction that, we can find two distinct i and j in $\{0, 1, \ldots, M-1\}$ such that $d^*(\mathcal{I}'_{s_{i,u}})$ and $d^*(\mathcal{I}'_{s_{j,u}})$ share a common element. Then

$$(iy'_1, y'_1u) - (iy_1, y_1u) = (jy'_2, y'_2u) - (jy_2, y_2u)$$

for some $y'_1 \neq y_1$ and $y'_2 \neq y_2$. By equating the second components on both sides, we see that $u(y'_1 - y_1) = u(y'_2 - y_2) \bmod 2M-1$. Since the range of y_1, y'_1, y_2 and y'_2 is between 0 and $M-1$, we must have $y'_1 - y_1 = y'_2 - y_2$ due to u is prime to $2M-1$. From the first component, we obtain $(i-j)(y'_1 - y_1) \equiv 0 \bmod p$, which implies that $y'_1 = y_1$. This contradicts the assumption that $y'_1 \neq y_1$. It implies the condition in (ii) of Theorem 4.6 holds for $\mathcal{I}_{s_{j,u}}$ here for $j = 0, \ldots, M-1$. Therefore, following Theorem 4.6 we can conclude that the sequences formed by the CRT construction with the same value of u form a $\mathsf{MUIS}^e(p(2M-1), M)$.

Now we know there are total h sequence set formed by CRT construction with different value of u. Then we will show that all hM sequences here are distinct. For sequences constructed by the

same value of u, we can easily find that these M sequences are distinct, otherwise any two non-distinct sequences would be totally blocked each other for some relative integer-shift which contradicts the definition of UI sequence set.

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

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

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

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

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

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

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

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

We modify the CRT construction via the method stated in Theorem 4.11. We call it *mCRT construction.*

Theorem 4.13. *For all M, the sequences by mCRT construction form h distinct $\mathsf{MCIS}^e(2p(2M-1), M)$s consisting of hM distinct sequences.*

Proof. It directly follows Theorem 4.11 and 4.12. □

Example 4.3: By mCRT construction for $p = M = 3$, we can design the following two distinct $\mathsf{MCIS}^e(30, 3)$s including six distinct sequences.

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

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

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

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

By mCRT construction, we will show the asymptotic lower bound in Theorem 4.10 can be achieved.

Theorem 4.14.

$$\liminf_{M\to\infty} \frac{L^e_{\min}(M)}{4M^2} = 1. \tag{4.13}$$

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

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

Table 4.1: The shortest known periods of MCI sequence set with M sequences for $M = 2, 3, 4, 5$.

Also we have the following fact:

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

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

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

This shows that the asymptotic lower bound in Theorem 4.10 is tight and proves Theorem 4.14. □

Remark: For $M = 2, 3, 4, 5$, the shortest known period of MCI sequence set with M sequences is listed in Table 4.1. We note the sequence set for $M = 2, 3$ is equi-difference, but not for $M = 4, 5$. However, these sequence sets are all constructed from UI sequence set following Theorem 4.11. For example, when $M = 4$, it is constructed from

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

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

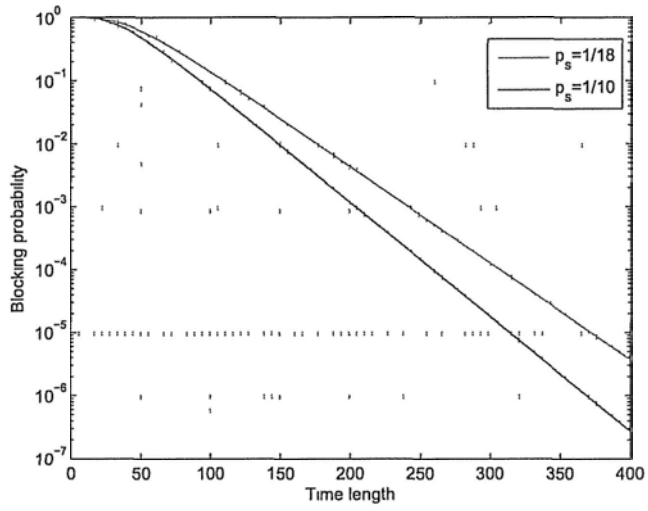

Figure 4.2: The blocking probability for 5 users in a random access scheme with $p_s = 1/18$ and $1/10$.

4.5 Discussion on Blocking Probability

In multiple access scheme for the asynchronous collision channel without feedback, we can compute the probability of at least one of the users cannot send any packet successfully in a given time length of N slots. We call this the *blocking probability*. The blocking probability is zero for MCI sequences if N is not less than the sequence period.

Consider a random access scheme in which each user sends a packet in each slot with a fixed probability p_s. Its blocking probability of M users in N time slots can be found by

$$1 - \left(1 - (1 - p_s(1 - 2p_s)^{M-1})^N\right)^M. \tag{4.14}$$

It is obvious the blocking probability of the random scheme is always nonzero. In other words, non-blocking property for the asynchronous channel does not hold here.

The fraction of ones of the MCI sequences formed by mCRT construction for 5 users is 1/18; and the sequence period is 90 time slots. The blocking probability is zero for the MCI sequence set if $N \geq 90$. In order to make a fair comparison with MCI sequence set considering power consumption, we set $p_s = 1/18$ to generate the same expected fraction of ones in the random access scheme. We plot its blocking probability for 5 users in Fig. 4.2. We see that when $N = 90$, the blocking probability of random access is about 0.2; and if we want it less than, say 10^{-4}, in a time length of N time slots, we must have $N \geq 306$ for random scheme.

In fact, the random scheme would enjoy better blocking probability if we relax the requirement of expected fraction of ones. Given M, we find the minimal value of (4.14) is achieved by $p_s = 1/(2M)$. Then the blocking probability of the random scheme for 5 users with $p_s = 1/10$ is also plotted in Fig. 4.2. For $N = 90$, the blocking probability is about 0.11. The expected power consumption is approximately double of that in the MCI sequences formed by mCRT construction.

In addition, we plot in Fig. 4.3 the blocking probability for different number of users, with the condition that the time length and p_s are equal to the period and duty factor of mCRT sequences respectively. The blocking probability reduces rapidly when the user number grows. It is caused by the period of mCRT sequences is of order $O(M^2)$.

4.6 Conclusion

MCI sequence sets are minimal energy sequence sets which provide the non-blocking property for the asynchronous collision chan-

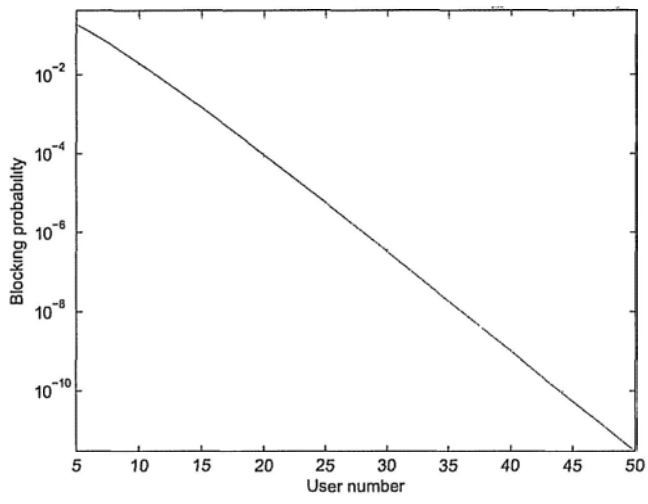

Figure 4.3: The blocking probability for different user numbers in a random access scheme under the condition $p_s = M/2p_M(2M-1)$ and $N = 2p_M(2M-1)$.

nel without feedback. The lower bound on the minimum period of such sequence set is shown as $2M^2$ for M users in this chapter. Furthermore, for equi-difference set, we improve the asymptotic lower bound to $4M^2$. A construction that meets this bound asymptotically is also given.

In addition, we have the following:

Conjecture 4.15. *Given M, then we have*

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

Furthermore, for all $M \geq 2$, we have the following improvements upon the asymptotic bounds in Conjecture 4.15.

Conjecture 4.16. *Let Φ_M be the shortest period among all sets of M UI sequences, each with Hamming weight M. Then for $M \geq 2$*

we have

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

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

□ **End of chapter.**

Chapter 5

Strongly Conflict-Avoiding Codes

Summary

Strongly conflict-avoiding codes are used in the asynchronous collision channel without feedback to guarantee each active user can send at least one packet successfully in its active period. The number of codewords in a strongly conflict-avoiding code is the number of potential users that can be supported. In this chapter, an upper bound on the size of strongly conflict-avoiding codes is derived for all Hamming weights. In addition, we provide an improved upper bound for equi-difference codes. This bound is further shown to be tight asymptotically.

5.1 Introduction

A set of M binary sequences is called (M, K)-*conflict-avoiding* [40] if every subset of K sequences out of these M sequences is user-irrepressible. Conflict-avoiding sequences find applications in the collision channel without feedback in which there are M potential users, but at most K of them are active at the same time. It guarantees the non-blocking property in the slot-synchronized case. In particular, considering the case where Hamming weight of each sequence equals K, an (M, K)-conflict-avoiding sequence set is called a *conflict-avoiding code* (CAC) [14, 17, 18, 22–24, 33, 34].

In this chapter, we consider a more general scenario in which the collision channel is asynchronous, as described in Section 1.1. A set of M binary sequences is called (M, K)-*strongly conflict-avoiding* if every subset of K sequences out of these M sequences is completely irrepressible (see Chapter 4). It guarantees the non-blocking property in the asynchronous channel with M potential users and at most K active users. Let the Hamming weight of each strongly conflict-avoiding sequence be w. Under the assumption of $w = K$, an (M, K)-strongly conflict-avoiding sequence set is called a *strongly conflict-avoiding code* (SCAC). Obviously, given M and K, the collection of all SCACs is a subset of the collection of all CACs, since the slot-synchronized channel is a special case of the asynchronous channel.

In this chapter, we are interested in SCAC and equi-difference SCAC with fixed codeword length and a given value of K. The aim of the study is to maximize the total number of potential users that can be supported. This viewpoint is also adopted for studying CAC and equi-difference CAC in [14, 17, 18, 22–24, 33, 34]. We remark that

some results in this chapter are motivated by [34] which provides a general upper bound for the size of CAC.

This chapter is organized as follows. We define SCAC and equi-difference SCAC by setting up some notations in Section 5.2. The first main result in this chapter is contained in Section 5.3, which provides an upper bound on the number of potential users that can be supported in an SCAC, given the length L and Hamming weight w. Furthermore, in Section 5.4 we present the second main result: an upper bound on the size of equi-difference SCAC. The asymptotic version of the upper bounds derived in previous sections is given respectively in Section 5.5. In Section 5.6, we show the upper bound in section 5.4 is asymptotically tight. Finally, we close in Section 5.7 with some concluding remarks.

5.2 Definitions and Notations

As defined in Section 1.3, we can represent a binary sequence by the characteristic set specifying the time indices where the sequence value is equal to one. In this chapter, subsets of $\mathbb{Z}_L$ with cardinality w are also called *codewords*. We sometime say that $\mathcal{I}$ is a codeword or sequence of weight w.

Given two non-empty subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{Z}_L$, the *sum set* and *difference set* of $\mathcal{A}$ and $\mathcal{B}$, are defined as

$$\mathcal{A}+\mathcal{B} := \{a+b:\ a\in\mathcal{A}, b\in\mathcal{B}\}$$
$$\mathcal{A}-\mathcal{B} := \{a-b:\ a\in\mathcal{A}, b\in\mathcal{B}\}$$

respectively. The negative of $\mathcal{A}$ is defined as

$$-\mathcal{A} := \{-a:\ a\in\mathcal{A}\}.$$

Given a codeword $\mathcal{I}$, we make the following definition, which is based on $d^*(\mathcal{I})$ defined in Section 1.3,

$$d^*(\mathcal{I})' := d^*(\mathcal{I}) \cup (d^*(\mathcal{I}) + 1) \cup (d^*(\mathcal{I}) - 1).$$

Obviously, we have $d^*(\mathcal{I})' \supseteq d^*(\mathcal{I})$.

Definition 5.1. A collection of M codewords

$$\mathscr{C} = \{\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_M\}$$

is called a CAC of length L and weight w if for all $j \neq k$,

$$d^*(\mathcal{I}_j) \cap d^*(\mathcal{I}_k) = \emptyset, \tag{5.1}$$

or equivalently, if

$$H_{s_j s_k}(\tau) \leq 1 \tag{5.2}$$

for all $j \neq k$ and τ.

Definition 5.2. Furthermore it is called an SCAC of length L and weight w if for all $j \neq k$,

$$d^*(\mathcal{I}_j)' \cap d(\mathcal{I}_k) = \emptyset, \tag{5.3}$$

or equivalently, if

$$H_{s_j(s_k \vee s_k^{(1)})}(\tau) \leq 1 \tag{5.4}$$

for all $j \neq k$ and τ. We use the notation $\mathsf{SCAC}(L, w)$ for an SCAC of length L and weight w. The symbol $\mathsf{SCAC}^e(L, w)$ is used for an equi-difference SCAC of length L and weight w.

Remark: From the property in (5.3), we know

$$\{1, L-1\} \cap d^*(\mathcal{I}_j) = \emptyset$$

as 0 is always included in $d(\mathcal{I}_k)$. One can check (5.3) also implies for all $j \neq k$,

$$\big(d^*(\mathcal{I}_j) + \{0,1\}\big) \cap \big(d^*(\mathcal{I}_k) + \{0,1\}\big) = \emptyset. \tag{5.5}$$

Example 5.1: $L = 30$, $w = 3$. The four codewords $\{0, 10, 20\}$, $\{0, 2, 4\}$, $\{0, 14, 22\}$ and $\{0, 12, 24\}$ constitute an $\mathsf{SCAC}^e(30, 3)$. We can verify that the following

$$\begin{aligned} d(\{0,10,20\}) &= \{0,10,20\} \\ d(\{0,2,4\}) &= \{0,2,4,26,28\} \\ d(\{0,14,22\}) &= \{0,8,14,16,22\} \\ d(\{0,12,24\}) &= \{0,6,12,18,24\} \end{aligned}$$

and

$$\begin{aligned} d^*(\{0,10,20\})' &= \{9,10,11,19,20,21\} \\ d^*(\{0,2,4\})' &= \{1,2,3,4,5,25,26,27,28,29\} \\ d^*(\{0,14,22\})' &= \{7,8,9,13,14,15,16,17,21,22,23\} \\ d^*(\{0,12,24\})' &= \{5,6,7,11,12,13,17,18,19,23,24,25\} \end{aligned}$$

satisfy the condition in (5.3). The SCAC is equi-difference, with generators 10, 2, 22 and 12.

Given positive integers L and w, consider respectively the class of all $\mathsf{SCAC}(L, w)$s and $\mathsf{SCAC}^e(L, w)$s. The maximal number of codewords in an $\mathsf{SCAC}(L, w)$ is denoted by $M(L, w)$. We also use $M^e(L, w)$ for the maximal number of codewords in an $\mathsf{SCAC}^e(L, w)$. The objective of this chapter is to derive upper bounds on $M(L, w)$ and $M^e(L, w)$ for all L and w.

5.3 Upper Bound on $M(L, w)$

5.3.1 The case of $L < 2w^2$

The result that $M(L, w) = 0$ for $L < w$ is obvious from the definition of Hamming weight. Now we will study the case for $w \leq L < 2w^2$.

Theorem 5.1. *For $w \leq L < 2w^2$,*

$$M(L, w) = 1. \tag{5.6}$$

Proof. Let $\mathcal{I}_j$ and $\mathcal{I}_k$ be two distinct codewords in an $\mathsf{SCAC}(L, w)$. We can find $1 \notin d(\mathcal{I}_k)$ otherwise the condition in (5.3) would be violated since 0 and 1 are always included in $d^*(\mathcal{I}_j)'$. Thus we conclude the Hamming weight of $(s_k \vee s_k^{(1)})$ is $2w$. From Proposition 3.2, we know

$$\sum_{\tau=0}^{L-1} H_{s_j(s_k \vee s_k^{(1)})}(\tau) = 2w^2.$$

Then with the condition $w \leq L < 2w^2$, we can find some τ_0 such that

$$H_{s_j(s_k \vee s_k^{(1)})}(\tau_0) > 1,$$

which contradicts (5.4). Therefore, we can conclude that $M(L, w) < 2$ for $L < 2w^2$. Since (5.3) always hold for an $\mathsf{SCAC}(L, w)$ with one codeword, we further have $M(L, w) = 1$ for $w \leq L < 2w^2$. □

5.3.2 The case of $L \geq 2w^2$

In this subsection we derive an upper bound on the size of SCAC for $L \geq 2w^2$ by applying Kneser's theorem [16], which is a

result about the sum of subsets in an abelian group G. As we only work with $\mathbb{Z}_L$, Kneser's theorem will be considered for $G = \mathbb{Z}_L$. First we introduce some more notations.

Given a non-empty subset $\mathcal{S} \subseteq \mathbb{Z}_L$, an element $h \in \mathbb{Z}_L$ is called a *period* of $\mathcal{S}$ if $h + \mathcal{S} = \mathcal{S}$. The *stabilizer* of $\mathcal{S}$, denoted by $H(\mathcal{S})$, is the set of all periods of $\mathcal{S}$,

$$H(\mathcal{S}) := \{h \in \mathbb{Z}_L : h + \mathcal{S} = \mathcal{S}\}.$$

It is obvious that $0 \in H(\mathcal{S})$ for every non-empty subset $\mathcal{S}$ of $\mathbb{Z}_L$, and $H(\mathcal{S})$ is a subgroup of $\mathbb{Z}_L$.

We use $\langle \alpha \rangle$ to denote the subgroup of $\mathbb{Z}_L$ generated by α, i.e.,

$$\langle \alpha \rangle := \{j\alpha \in \mathbb{Z}_L : j = 0, 1, 2, \ldots\}.$$

When α divides L, we have $\langle \alpha \rangle$ consists of L/α elements.

Note that an subset $\mathcal{S}$ of $\mathbb{Z}_L$ with $|H| > 1$ can be written as the union of cosets of H,

$$\mathcal{S} = \bigcup_{a \in \mathcal{S}} (H + a).$$

As an example, consider the subset $\mathcal{S} = \{0, 1, 4, 5\} \subset \mathbb{Z}_8$. The stabilizer of $\mathcal{S}$ is $H = \{0, 4\} = \langle 4 \rangle$ and $\mathcal{S}$ is a union of H and the coset $\{1, 5\}$.

First we have the following simple result:

Lemma 5.2. *For any subset $\mathcal{I} \in \mathbb{Z}_L$ with $0 \in \mathcal{I}$, we have $H(\mathcal{I}) \subseteq \mathcal{I}$.*

Proof. Let h be an element in $H(\mathcal{I})$. Because $0 \in \mathcal{I}$ and $h + \mathcal{I} \subseteq \mathcal{I}$, we have $h = h + 0 \in \mathcal{I}$. This proves that the stabilizer of $\mathcal{I}$ is a subset of $\mathcal{I}$ if $0 \in \mathcal{I}$. □

Theorem 5.3 (Kneser). *Let $\mathcal{A}$ and $\mathcal{B}$ be non-empty subsets of $\mathbb{Z}_L$, and let $H = H(\mathcal{A} + \mathcal{B})$ be the stabilizer of $\mathcal{A} + \mathcal{B}$. If $|\mathcal{A} + \mathcal{B}| <$*

$|\mathcal{A}| + |\mathcal{B}|$, *then*

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + H| + |\mathcal{B} + H| - |H|. \tag{5.7}$$

Proof of Theorem 5.3 can be found in [19] or [26]. We will apply Kneser's theorem through the following Corollary.

Corollary 5.4. *Let $\mathcal{I}$ be a codeword in an SCAC(L, w) such that $|d(\mathcal{I}) + \{0, 1\}| \leq 3w - 2$ and H be the stabilizer of $d(\mathcal{I}) + \{0, 1\}$, then we have $|H| > 1$ and*

$$|d(\mathcal{I}) + \{0, 1\}| = |\mathcal{I} + \{0, 1\} + H| + |\mathcal{I} + H| - |H|. \tag{5.8}$$

Proof. Suppose that $\mathcal{I}$ is a codeword in an SCAC(L, w) such that $|d(\mathcal{I}) + \{0, 1\}| \leq 3w - 2$ and let H be the stabilizer of $d(\mathcal{I}) + \{0, 1\}$. $|-\mathcal{I}|$ can be easily found as w. By the definition in (5.3), we know $1 \notin d^*(\mathcal{I})$. Thus we have $|\mathcal{I} + \{0, 1\}| = 2w$. The condition in Kneser's theorem is satisfied with $\mathcal{A} = \mathcal{I} + \{0, 1\}$ and $\mathcal{B} = -\mathcal{I}$, because

$$\begin{aligned} |\mathcal{I} + \{0, 1\} + (-\mathcal{I})| = |d(\mathcal{I}) + \{0, 1\}| &\leq 3w - 2 \\ &< |\mathcal{I} + \{0, 1\}| + |-\mathcal{I}| = 3w. \end{aligned}$$

From (5.7), we obtain

$$\begin{aligned} |d(\mathcal{I}) + \{0, 1\}| &= |\mathcal{I} + \{0, 1\} + H| + |-\mathcal{I} + H| - |H| \\ &= |\mathcal{I} + \{0, 1\} + H| + |\mathcal{I} + H| - |H|. \end{aligned}$$

In the last equality above, we have used the fact $-H = H$ since H is a subgroup of $\mathbb{Z}_L$. This proves (5.8). Since $|\mathcal{I} + H| \geq w$ and $|\mathcal{I} + \{0, 1\} + H| \geq 2w$, we obtain the following from (5.8).

$$|d(\mathcal{I}) + \{0, 1\}| \geq 3w - |H|.$$

Thus we have

$$3w - |H| \leq |d(\mathcal{I}) + \{0,1\}| \leq 3w - 2.$$

We conclude that $|H| \geq 2$. □

Definition 5.3. A codeword $\mathcal{I}$ of weight w is said to be *peculiar* if

$$|d(\mathcal{I}) + \{0,1\}| \leq 3w - 2. \tag{5.9}$$

One can check in Example 5.1 only the first codeword is peculiar.

In the next theorem we give a method for upper bounding the size of an SCAC.

Theorem 5.5. *Let $\mathscr{C}$ be an SCAC(L, w) in which P codewords are peculiar. For $j = 1, 2, \ldots, P$, denote the j-th peculiar codeword by $\mathcal{I}_j$, and let the stabilizer of $d(\mathcal{I}_j) + \{0,1\}$ be H_j. Define*

$$\Delta_j := |\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - 3w. \tag{5.10}$$

Then for $L \geq 2w^2$,

$$|\mathscr{C}| \leq \left\lfloor \frac{L - 2 + \sum_{j=1}^{P} (|H_j| - \Delta_j - 1)}{3w - 3} \right\rfloor. \tag{5.11}$$

Proof. By the definition in (5.3), we have the following

$$\big(d^*(\mathcal{I}_j) + \{0,1\}\big) \cap \big(d^*(\mathcal{I}_k) + \{0,1\}\big) = \emptyset$$

for all distinct j and k. It implies $\big(d^*(\mathcal{I}_j) + \{0,1\}\big)$ and $\big(d^*(\mathcal{I}_k) + \{0,1\}\big)$ are disjoint for any pair of distinct codewords $\mathcal{I}_j$ and $\mathcal{I}_k$ in $\mathscr{C}$.

By the definition in (5.3), we have $\{0, 1, L-1\} \cap d^*(\mathcal{I}_j) = \emptyset$. Furthermore, we have

$$\{0,1\} \cap (d^*(\mathcal{I}_j) + \{0,1\}) = \emptyset$$

for all j. We thus have the following basic inequality,

$$L - 2 \geq \sum_{\mathcal{I} \in \mathscr{C}} |d^*(\mathcal{I}) + \{0,1\}|. \tag{5.12}$$

We also know $\{0,1\} \cup (d^*(\mathcal{I}_j) + \{0,1\}) = d(\mathcal{I}_j) + \{0,1\}$ for all j, which implies

$$|d^*(\mathcal{I}_j) + \{0,1\}| = |d(\mathcal{I}_j) + \{0,1\}| - 2.$$

Thus the inequality in (5.12) becomes

$$L - 2 \geq \sum_{\mathcal{I} \in \mathscr{C}} (|d(\mathcal{I}) + \{0,1\}| - 2).$$

From Corollary 5.4 we get

$$\begin{aligned} L - 2 &\geq \sum_{j=1}^{P} (|\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - |H_j| - 2) \\ &\quad + (|\mathscr{C}| - P)(3w - 1 - 2) \\ &= \sum_{j=1}^{P} (\Delta_j - |H_j| + 3w - 2) + (|\mathscr{C}| - P)(3w - 3) \end{aligned}$$

After some rearrangement of terms, we get

$$|\mathscr{C}| \leq \frac{L - 2 + \sum_{j=1}^{P} (|H_j| - \Delta_j - 1)}{3w - 3}.$$

This finishes the proof of the theorem. □

We introduce a few more definitions which will be useful in Theorem 5.6.

Definition 5.4. Let

$$S(L,w) := \Big\{ x \in \{2,3,\ldots,3w-2\} : x \text{ divides } L, \tag{5.13}$$

$$\text{and } x(\lceil w/x \rceil + \lceil 2w/x \rceil) - x \leq 3w-2 \Big\}. \tag{5.14}$$

$S(L,w)$ may be empty, for example when L is prime. Let $\mathscr{S}(L,w)$ be the collection of subsets of $S(L,w)$, such that each pair of distinct elements in $\mathcal{S} \in \mathscr{S}(L,w)$ are relatively prime, i.e.,

$$\mathscr{S}(L,w) := \{\mathcal{S} \subseteq S(L,w) : \gcd(i,j) = 1, \forall i,j, \in \mathcal{S}, i \neq j\}.$$

Given an integer $L \geq w \geq 2$, if $\mathscr{S}(L,w)$ is non-empty, define

$$F(L,w) := \max_{\mathcal{S} \in \mathscr{S}(L,w)} \sum_{x \in \mathcal{S}} \Big(x - 1 - x(\lceil 2w/x \rceil + \lceil w/x \rceil) + 3w \Big) \tag{5.15}$$

with the maximum taken over all subsets $\mathcal{S}$ in $\mathscr{S}(L,w)$. We note that $F(L,w)$ is non-negative by the condition in (5.14). If $\mathscr{S}(L,w)$ is empty, we define $F(L,w)$ as zero.

Theorem 5.6. *For $L \geq 2w^2$ and $w \geq 2$,*

$$M(L,w) \leq \left\lfloor \frac{L-2+F(L,w)}{3w-3} \right\rfloor. \tag{5.16}$$

Proof. In an $\mathsf{SCAC}(L,w)$, suppose that there are P peculiar codewords, denoted by $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_P$. For $j = 1,2,\ldots,P$, let H_j be the stabilizer of $d(\mathcal{I}_j) + \{0,1\}$. Consider two distinct codewords $\mathcal{I}_i$ and $\mathcal{I}_j$ in these P codewords, we have $|H_i|$ and $|H_j|$ are both strictly larger than one by Corollary 5.4. As subgroups of $\mathbb{Z}_L$, H_i and H_j can be written as $\langle \alpha_i \rangle$ and $\langle \alpha_j \rangle$ respectively, for some proper divisors α_i and α_j of L, so that $|H_i| = L/\alpha_i$ and $|H_j| = L/\alpha_j$.

Suppose that $|H_i|$ and $|H_j|$ are not relatively prime, say, if $b > 1$ is a common divisor of $|H_i|$ and $|H_j|$, then

$$bx_i = \frac{L}{\alpha_i},\ bx_j = \frac{L}{\alpha_j},$$

for some integers x_i and x_j, and we get

$$b\alpha_i x_i = L = b\alpha_j x_j.$$

After dividing the above equation by b, we see that L/b is an integral multiple of both α_i and α_j, and hence is a common element in H_i and H_j. Moreover, L/b is non-zero mod L, because $b > 1$. The two stabilizers H_i and H_j thus contain a common non-zero element. By Lemma 5.2, we have $d(\mathcal{I}_i) + \{0,1\} \supseteq H_i$ and $d(\mathcal{I}_j) + \{0,1\} \supseteq H_j$, and so L/b is also a common non-zero element of $d(\mathcal{I}_i) + \{0,1\}$ and $d(\mathcal{I}_j) + \{0,1\}$. If $L/b = 1$, we have $\alpha_i = \alpha_j = 1$ and $|H_i| = |H_j| = L$. It implies $H_i = H_j = \{0, 1, \ldots, L-1\}$ and

$$d(\mathcal{I}_i) + \{0,1\} = d(\mathcal{I}_j) + \{0,1\} = \{0, 1, \ldots, L-1\},$$

which contradicts the defining property of (5.3). Hence non-zero L/b is not equal to one. We thus find L/b is also a common element of $d^*(\mathcal{I}_i) + \{0,1\}$ and $d^*(\mathcal{I}_j) + \{0,1\}$. This contradicts (5.5) which is necessary for (5.3). Thus we find that $|H_i|$ and $|H_j|$ are relatively prime.

For each j, $|\mathcal{I}_j + \{0,1\} + H_j|$ is an integral multiple of $|H_j|$ because $\mathcal{I}_j + \{0,1\} + H_j$ is a union of H_j and its cosets. Furthermore, we have $|\mathcal{I}_j + \{0,1\} + H_j|$ is larger than or equal to $2w$ because $|\mathcal{I}_j + \{0,1\} + H_j|$ contains $|\mathcal{I}_j + \{0,1\}|$ and $|\mathcal{I}_j + \{0,1\}| = 2w$ which has already been noted in the proof of Corollary 5.4. Similarly, we also have $|\mathcal{I}_j + H_j|$ is an integral multiple of $|H_j|$ and is not less than

w. We thus have the following inequality,

$$|\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| \geq |H_j|\Big(\left\lceil \frac{2w}{|H_j|} \right\rceil + \left\lceil \frac{w}{|H_j|} \right\rceil\Big).$$

The two parts of right hand side in the above inequality are the smallest integral multiples of $|H_j|$ which is not less than $2w$ and w respectively.

We next show that $|H_j| \in S(L,w)$, for $j = 1,2,\ldots,P$. For each j, the subgroup H_j cannot have size strictly larger than $3w-2$, otherwise by Corollary 5.4, we have

$$\begin{aligned} |d(\mathcal{I}_j) + \{0,1\}| &= |\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - |H_j| \\ &\geq 2|H_j| - |H_j| \\ &= |H_j| > 3w - 2, \end{aligned}$$

which is a contradiction to the definition of peculiar codeword in (5.9). In addition, we must have $|H_j| \geq 2$ by Corollary 5.4. This shows that $2 \leq |H_j| \leq 3w-2$.

As a subgroup of $\mathbb{Z}_L$, we see that $|H_j|$ is a divisor of L. Moreover, for $j = 1,2,\ldots,P$, $|H_j|$ satisfies

$$\begin{aligned} 3w - 2 &\geq |d(\mathcal{I}_j) + \{0,1\}| \\ &= |\mathcal{I}_j + \{0,1\} + H_j| + |\mathcal{I}_j + H_j| - |H_j| \\ &\geq |H_j|\Big(\left\lceil \frac{2w}{|H_j|} \right\rceil + \left\lceil \frac{w}{|H_j|} \right\rceil\Big) - |H_j|. \end{aligned}$$

Consequently, $|H_j|$ satisfies the conditions in (5.13) and (5.14), and hence belong to the set $S(L,w)$. We have already shown that $|H_i|$ and $|H_j|$ are relatively prime for $i \neq j$. Therefore

$$\{|H_1|, |H_2|, \ldots, |H_P|\} \in \mathscr{S}(L,w).$$

For $j = 1,2,\ldots,P$, let Δ_j be defined as in Theorem 5.5. We can upper bound $|H_j| - 1 - \Delta_j$, which appears in the summation in

p	q	r	S	F
0	0	0	$\emptyset$	0
1	0	0	$\{2\}$	1
≥ 2	0	0	$\{2,4\}$	3
0	≥ 1	0	$\{9\}$	2
1	≥ 1	0	$\{2,9\}$	3
≥ 2	≥ 1	0	$\{2,4,9\}$	5
0	0	≥ 1	$\{5\}$	1
1	0	≥ 1	$\{2,5\}$	2
≥ 2	0	≥ 1	$\{2,4,5\}$	4
0	≥ 1	≥ 1	$\{5,9\}$	3
1	≥ 1	≥ 1	$\{2,5,9\}$	4
≥ 2	≥ 1	≥ 1	$\{2,4,5,9\}$	6

Table 5.1: Values of $S(L,4)$ and $F(L,4)$

(5.11), by

$$|H_j| - 1 - \Delta_j \leq |H_j| - 1 - |H_j| \left\lceil \frac{w}{|H_j|} \right\rceil - |H_j| \left\lceil \frac{2w}{|H_j|} \right\rceil + 3w,$$

which equals the summand in (5.15) with x substituted by $|H_j|$. By exhausting all possible choices of $\mathcal{S}$ in $\mathscr{S}(L,w)$, we have the following upper bound

$$\sum_{j=1}^{P} (|H_j| - 1 - \Delta_j) \leq F(L,w).$$

Substituting it back to (5.11), we have

$$|\mathscr{C}| \leq \left\lfloor \frac{L - 2 + F(L,w)}{3w - 3} \right\rfloor.$$

This completes the proof of Theorem 5.6. □

We illustrate Theorem 5.6 with $w = 4$.

Corollary 5.7. *Let L be an integer factorized as $2^p 9^q 5^r \ell$, where ℓ is not divisible by 2, 9 or 5. Then for $L \geq 32$ we have*

$$M(L,4) \leq \begin{cases} \lfloor (L-2)/9 \rfloor & \text{if } p=q=r=0, \\ \lfloor (L-1)/9 \rfloor & \text{if } p=1, q=r=0, \text{or} \\ & \quad p=0, q=0, r \geq 1, \\ \lfloor L/9 \rfloor & \text{if } p=r=0, q \geq 1, \text{or} \\ & \quad p=1, q=0, r \geq 1, \\ \lfloor (L+1)/9 \rfloor & \text{if } p \geq 2, q=r=0, \text{or} \\ & \quad p=1, q \geq 1, r=0, \text{or} \\ & \quad p=0, q \geq 1, r \geq 1, \\ \lfloor (L+2)/9 \rfloor & \text{if } p \geq 2, q=0, r \geq 1, \text{or} \\ & \quad p=1, q \geq 1, r \geq 1, \\ \lfloor (L+3)/9 \rfloor & \text{if } p \geq 2, q \geq 1, r=0 \\ \lfloor (L+4)/9 \rfloor & \text{if } p \geq 2, q \geq 1, r \geq 1. \end{cases}$$

Proof. The value of $x - 1 - x(\lceil 2w/x \rceil + \lceil w/x \rceil) + 3w$ for $x \in \{2, 3, \ldots, 10\} \setminus \{3, 6, 7\}$ is shown in the following table:

x	2	4	5	8	9	10
$x - 1 - x(\lceil 2w/x \rceil + \lceil w/x \rceil) + 3w$	1	3	1	3	2	1

We note that 3, 6 and 7 are not shown in the above table, because they do not satisfy the condition in (5.14).

Since the value of $x - 1 - x(\lceil 2w/x \rceil + \lceil w/x \rceil) + 3w$ for $x = 2$ and $x = 10$ are the same, we can disregard the case $x = 10$ in the computation of $F(L, w)$ without impacting the result. By the same reason, we can ignore the case $x = 8$. We tabulate $S(L, 4)$ and

$F(L,4)$ in Table 5.1. By Theorem 5.6, we get

$$M(L,4) \leq \left\lfloor \frac{L-2+F(L,4)}{9} \right\rfloor .$$

The upper bound in Corollary 5.7 is obtained after gathering up the data in Table 5.1. □

5.4 Upper Bound on $M^e(L,w)$

The result in Theorem 5.1 also holds for the upper bound on $M^e(L,w)$ if $L < 2w^2$. This section will be devoted to establishing an upper bound on $M^e(L,w)$ for $L \geq 2w^2$.

Definition 5.5. We adopt the terminology in [24] and say that a codeword $\mathcal{I}$ of weight w is *exceptional* if

$$|d^*(\mathcal{I})| < 2w-2, \tag{5.17}$$

or equivalently, if

$$|d(\mathcal{I})| \leq 2w-2. \tag{5.18}$$

From the discussion above, we see that if a codeword $\mathcal{I}$ is equi-difference with generator g, then it is exceptional if and only if $\pm g$, $\pm 2g, \ldots, \pm(w-1)g$ are *not* distinct mod L.

Lemma 5.8. *Let $\mathcal{I}$ be an exceptional codeword in an $SCAC^e(L,w)$ and its generator be g, then we have*

(i) g is not relatively prime to L;

(ii) $d(\mathcal{I})$ is a subgroup of $\mathbb{Z}_L$.

Proof. If an equi-difference $\mathcal{I}$ is exceptional, i.e., $|d(\mathcal{I})| \leq 2w-2$, then there exists two distinct integers m_1 and m_2 ranged in $[-(w-$

$1), w-1]$ satisfying

$$m_1 g = m_2 g \mod L$$

which implies g is not relatively prime to L.

By the above equation, we further have

$$tg = 0 \mod L$$

for $t = |m_1 - m_2|$ and

$$d(\mathcal{I}) = \{0, g, \ldots, (t-1)g\}.$$

from which we find $d(\mathcal{I})$ is a subgroup of $\mathbb{Z}_L$. □

We illustrate Lemma 5.8 using Example 5.1.

Example 5.1 continued: The equi-difference codeword generated by 10 is exceptional, because

$$|d^*(\{0, 10, 20\})| = |\{10, 20\}| = 2 < 2 \cdot 3 - 2.$$

We can verify that $d(\{0, 10, 20\}) = \{0, 10, 20\}$ is a subgroup of $\mathbb{Z}_{30}$.

Lemma 5.9. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two distinct exceptional codewords in an $SCAC^e(L, w)$. Then $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are two relatively prime divisors of L between w and $2w-2$.*

Proof. First by Lemma 5.8 we know $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are both subgroups of $\mathbb{Z}_L$ and thus both divide L. If $|d(\mathcal{I}_1)|$ and $|d(\mathcal{I}_2)|$ are not relatively prime, as proved in Theorem 5.6, we find $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$ contain a common non-zero element. This contradicts the defining property in (5.3). Here, they can also be found in the range $[w, 2w-2]$ from the definition of exceptional codewords. This completes the proof of Lemma 5.9. □

Definition 5.6. A codeword $\mathcal{I}$ is said to be *dispersive* if any two distinct elements in $d(\mathcal{I})$ are not consecutive. Otherwise, it is *non-dispersive.*

Lemma 5.10. *Let $\mathcal{I}$ be a non-dispersive codeword in an $SCAC^e(L, w)$ and its generator be g. If there are k $(k > 0)$ pairs of consecutive elements in $d(\mathcal{I})$, then we have*

(i)

$$(2w - k - 1)g = 1 \text{ or } -1 \mod L \tag{5.19}$$

with $k \leq w - 1$;

(ii) g and $2w - k - 1$ are both relatively prime to L;

(iii) $\mathcal{I}$ is non-exceptional.

Proof. If there are k $(k > 0)$ pairs of consecutive elements in $d(\mathcal{I})$, then there exists at least one solution of m in $[-2w + 2, 2w - 2]$ for the following:

$$mg = 1 \mod L. \tag{5.20}$$

We first have g and m are both relatively prime to L, otherwise (5.20) does not hold. Then by the condition g is relatively prime to L, we find there exists at most one solution of m in $[-2w+2, 2w-2]$ for (5.20).

Furthermore, the solution range of $[-w+1, w-1]$ can be ruled out here, otherwise we can find $1 \in d(\mathcal{I})$ which violates the condition in (5.3). Hence we must have one unique solution of m in $[w, 2w - 2] \cup [-2w+2, -w]$. The value of m can be easily found as $2w-k-1$ or $-(2w - k - 1)$ from $d(\mathcal{I}) = \{0, g, \ldots, (w - 1)g\}$ with $1 \notin d(\mathcal{I})$. Then $2w - k - 1$ is also relatively prime to L. From the range of m, we prove $k \leq w - 1$.

In addition, we obtain $\mathcal{I}$ must be non-exceptional, otherwise g is not relative prime to L following (i) of Lemma 5.8, which contradicts the condition g is relatively prime to L for non-dispersive $\mathcal{I}$. □

We illustrate Lemma 5.10 by the following example.

Example 5.2: $L = 28$, $w = 3$. The three codewords $\{0, 2, 4\}$, $\{0, 7, 14\}$ and $\{0, 9, 18\}$ constitute an $\mathsf{SCAC}^e(28, 3)$. We can verify that the following holds for (5.3).

$$\begin{aligned} d(\{0, 2, 4\}) &= \{0, 2, 4, 24, 26\} \\ d(\{0, 7, 14\}) &= \{0, 7, 14, 21\} \\ d(\{0, 9, 18\}) &= \{0, 9, 10, 18, 19\}. \end{aligned}$$

The SCAC is equi-difference, with generators 2, 7 and 9. The codeword generated by 9 is non-dispersive, because $(9, 10)$ and $(18, 19)$ are two pairs of consecutive elements in $d(\{0, 9, 18\})$. Furthermore, one can check

$$(2 \cdot 3 - 2 - 1) \cdot 9 = -1 \mod 28$$

with $k = 2 \leq 3 - 1$, also 9 and $2 \cdot 3 - 2 - 1 = 3$ are both relatively prime to 28.

Lemma 5.11. *Let $\mathcal{I}_1$ and $\mathcal{I}_2$ be two distinct non-dispersive codewords in an $\mathsf{SCAC}^e(L, w)$. If there are k_1 and k_2 pairs of consecutive elements respectively in $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$, then $2w - k_1 - 1$ and $2w - k_2 - 1$ are two relatively prime integers between w and $2w - 2$ such they are both relatively prime to L.*

Proof. Let g_1 and g_2 be the generator of $\mathcal{I}_1$ and $\mathcal{I}_2$ respectively. By Lemma 5.10, if there are k_1 and k_2 pairs of consecutive elements

respectively in $d(\mathcal{I}_1)$ and $d(\mathcal{I}_2)$, then we have the following result for $\mathcal{I}_1$ and $\mathcal{I}_2$ respectively.

First, we know $2w - k_1 - 1$ and $2w - k_2 - 1$ are both relatively prime to L. By letting $r_1 = 2w - k_1 - 1$, we have the following two possible cases for $\mathcal{I}_1$.

$$r_1 g_1 = 1 \bmod L;$$

$$r_1 g_1 = -1 \bmod L.$$

By letting $r_2 = 2w - k_2 - 1$, we also have the following two possible cases for $\mathcal{I}_2$.

$$r_2 g_2 = 1 \bmod L;$$

$$r_2 g_2 = -1 \bmod L.$$

By the proof in Theorem 4.8, we can conclude that r_1 and r_2 must be relatively prime. We further obtain $2w - k_1 - 1$ and $2w - k_2 - 1$ are two relatively prime integers between w and $2w - 2$ such they are both relatively prime to L.

□

The next theorem establishes an upper bound on the size of an equi-difference SCAC.

Theorem 5.12. *Let $\mathscr{C}$ be an SCAC$^e(L, w)$ in which E_1 codewords are exceptional and E_2 codewords are non-dispersive. For $j = 1, 2, \ldots, E_1$, denote the j-th exceptional codeword by $\mathcal{I}_j$. For $j = 1, 2, \ldots, E_2$, denote the j-th non-dispersive codeword by $\mathcal{J}_j$, and let the number of pairs of consecutive elements in $d(\mathcal{J}_j)$ be k_j. Then for $L \geq 2w^2$,*

$$|\mathscr{C}| \leq \left\lfloor \frac{L - 2 + 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2} k_j}{4w - 4} \right\rfloor. \quad (5.21)$$

Proof. From (iii) of Lemma 5.10, we know in an $\mathsf{SCAC}^e(L, w)$, the set of exceptional codewords and the set of non-dispersive codewords are mutually exclusive.

Let the number of non-exceptional and dispersive codewords be N. Since any two elements in $d(\mathcal{I})$ are not consecutive and $d^*(\mathcal{I}) = 2w-2$ for each non-exceptional and dispersive equi-difference codeword $\mathcal{I}$, by definition we have the following inequality:

$$L - 2 \geq 2N(2w-2) + \sum_{j=1}^{E_1} 2|d^*(\mathcal{I}_j)| + \sum_{j=1}^{E_2}(4w - 4 - k_j).$$

By the fact that $|d^*(\mathcal{I}_j)| = |d(\mathcal{I}_j)|-1$, the above inequality becomes:

$$\begin{aligned} L - 2 &\geq 2N(2w-2) + \sum_{j=1}^{E_1} 2(|d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2}(4w - 4 - k_j) \\ &= 2(N + E_1 + E_2)(2w-2) \\ &\quad - 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) - \sum_{j=1}^{E_2} k_j \end{aligned}$$

After some rearrangement of terms, we get

$$\begin{aligned} |\mathscr{C}| &= N + E_1 + E_2 \\ &\leq \frac{L - 2 + 2\sum_{j=1}^{E_1}(2w - |d(\mathcal{I}_j)| - 1) + \sum_{j=1}^{E_2} k_j}{2(2w-2)}. \end{aligned}$$

This finishes the proof of the theorem. □

We make a few more definitions which will be useful in Theorem 5.13.

Definition 5.7. Let

$$S_1(L, w) := \Big\{ x \in \{w, w+1, \ldots, 2w-2\} : x \text{ divides } L \Big\}. \quad (5.22)$$

$S_1(L, w)$ may be empty, for example when L is prime.

Let

$$S_2(L, w) := \Big\{x \in \{w, w+1, \ldots, 2w-2\} : \gcd(x, L) = 1\Big\}. \quad (5.23)$$

Let $\mathscr{S}_1(L, w)$ be the collection of subsets of $S_1(L, w)$, such that each pair of distinct elements in $\mathcal{S}_1 \in \mathscr{S}_1(L, w)$ are relatively prime, i.e.,

$$\mathscr{S}_1(L, w) := \{\mathcal{S}_1 \subseteq S_1(L, w) : \gcd(i, j) = 1, \\ \forall i, j, \in \mathcal{S}_1, i \neq j\}.$$

Let $\mathscr{S}_2(L, w)$ be the collection of subsets of $S_2(L, w)$, such that each pair of distinct elements in $\mathcal{S}_2 \in \mathscr{S}_2(L, w)$ are relatively prime, i.e.,

$$\mathscr{S}_2(L, w) := \{\mathcal{S}_2 \subseteq S_2(L, w) : \gcd(i, j) = 1, \\ \forall i, j, \in \mathcal{S}_2, i \neq j\}.$$

Given an integer $L \geq w \geq 2$, if $\mathscr{S}_1(L, w)$ is non-empty, define

$$F_1(L, w) := \max_{\mathcal{S}_1 \in \mathscr{S}_1(L,w)} \sum_{x \in \mathcal{S}_1} (2w - x - 1) \quad (5.24)$$

with the maximum taken over all subsets $\mathcal{S}_1$ in $\mathscr{S}_1(L, w)$. If $\mathscr{S}_1(L, w)$ is empty, we define $F_1(L, w)$ as zero. We note that the summand in (5.24) is positive by the condition in (5.22). Hence, $F_1(L, w)$ is non-negative.

Similarly, we also define the following if $\mathscr{S}_2(L, w)$ is non-empty for a given integer $L \geq w \geq 2$,

$$F_2(L, w) := \max_{\mathcal{S}_2 \in \mathscr{S}_2(L,w)} \sum_{x \in \mathcal{S}_2} (2w - x - 1). \quad (5.25)$$

If $\mathscr{S}_2(L, w)$ is empty, we define $F_2(L, w)$ as zero.

Theorem 5.13. *For $L \geq 2w^2$ and $w \geq 2$,*

$$M^e(L,w) \leq \left\lfloor \frac{L-2+2F_1(L,w)+F_2(L,w)}{4w-4} \right\rfloor. \tag{5.26}$$

Proof. Following Lemma 5.9, we have

$$\sum_{j=1}^{E_1}(2w-|d(\mathcal{I}_j)|-1) \leq F_1(L,w).$$

Following Lemma 5.11, we have

$$\sum_{j=1}^{E_2} k_j \leq F_2(L,w).$$

Substituting them back to (5.21), we have

$$M^e(L,w) \leq \left\lfloor \frac{L-2+2F_1(L,w)+F_2(L,w)}{4w-4} \right\rfloor.$$

This completes the proof of Theorem 5.13. □

We illustrate Theorem 5.13 with $w = 4$.

Corollary 5.14. *Let L be an integer factorized as $2^p3^q5^r\ell$, where ℓ is not divisible by 2, 3 or 5. Then for $L \geq 32$ we have*

$$M^e(L,4) \leq \begin{cases} \lfloor L/12 \rfloor & \text{if } p=1, q=r=0, \\ \lfloor (L+2)/12 \rfloor & \text{if } p=1, q\geq 1, r=0, \text{or} \\ & \quad p=1, q=0, r\geq 1, \\ \lfloor (L+3)/12 \rfloor & \text{if } p=r=0, q\geq 0 \\ \lfloor (L+4)/12 \rfloor & \text{if } p=1, q\geq 1, r\geq 1, \\ \lfloor (L+5)/12 \rfloor & \text{if } p=0, q\geq 0, r\geq 1 \\ \lfloor (L+6)/12 \rfloor & \text{if } p\geq 2, q\geq 0, r=0 \\ \lfloor (L+8)/12 \rfloor & \text{if } p\geq 2, q\geq 0, r\geq 1. \end{cases}$$

p	q	r	S_1	S_2	F_1, F_2	$2F_1 + F_2$
0	0	0	$\emptyset$	$\{4,5,6\}$	0, 5	5
1	0	0	$\emptyset$	$\{5\}$	0, 2	2
≥ 2	0	0	$\{4\}$	$\{5\}$	3, 2	8
0	≥ 1	0	$\emptyset$	$\{4,5\}$	0, 5	5
1	≥ 1	0	$\{6\}$	$\{5\}$	1, 2	4
≥ 2	≥ 1	0	$\{4,6\}$	$\{5\}$	3, 2	8
0	0	≥ 1	$\{5\}$	$\{4,6\}$	2, 3	7
1	0	≥ 1	$\{5\}$	$\emptyset$	2, 0	4
≥ 2	0	≥ 1	$\{4,5\}$	$\emptyset$	5, 0	10
0	≥ 1	≥ 1	$\{5\}$	$\{4\}$	2, 3	7
1	≥ 1	≥ 1	$\{5,6\}$	$\emptyset$	3, 0	6
≥ 2	≥ 1	≥ 1	$\{4,5,6\}$	$\emptyset$	5, 0	10

Table 5.2: Values of $S_1(L,4), S_2(L,4), F_1(L,4)$ and $F_2(L,4)$

Proof. We tabulate $S_1(L,4)$, $S_2(L,4)$, $F_1(L,4)$ and $F_2(L,4)$ in Table 5.2. By Theorem 5.13, we get

$$M^e(L,4) \leq \left\lfloor \frac{L-2+2F_1(L,4)+F_2(L,4)}{12} \right\rfloor.$$

The upper bound in Corollary 5.14 is obtained after applying the data in Table 5.2 to the above inequality case by case. □

Example 5.3: $L = 74$, $w = 4$. The following six codewords constitute an $\mathsf{SCAC}^e(74,4)$:

$$\{0,2,4,6\}, \{0,16,32,48\},$$
$$\{0,20,40,60\}, \{0,12,24,36\},$$
$$\{0,22,44,66\}, \{0,28,56,10\}.$$

We find this SCAC enjoys maximum size of $\mathsf{SCAC}^e(74,4)$, since $M^e(74,4) \leq \lfloor 74/12 \rfloor = 6$ following Corollary 5.14.

5.5 Asymptotic Upper Bounds

The value of $F(L, w)$ in Theorem 5.6 can be computed by linear programming as follows. For each element i in $S(L, w)$, define a variable z_i. Let the objective function be $\sum_{i \in S(L,w)} c_i z_i$, with c_i defined by

$$c_i := i - 1 - i(\lceil w/i \rceil + \lceil 2w/i \rceil) + 3w.$$

For each prime number p between 2 and $3w-2$, impose a constraint

$$\sum_{p|i} z_i \leq 1, \tag{5.27}$$

where the summation is taken over all i that is divisible by p. Then $F(L, w)$ is the optimal value by maximizing $\sum_{i \in S(L,w)} c_i z_i$ subject to the constraint in (5.27) for p ranging over all prime numbers between 2 and $3w - 2$, and $0 \leq z_i \leq 1$ for all $i \in S(L, w)$. Using the linear programming, the upper bounds on $M(L, w)$ given by Theorem 5.6 for weight 4 and length between 32 and 400 are plotted in Fig. 5.1. The value for length smaller than 32 is found directly by Theorem 5.1. By similar linear programming, the value of $F_1(L, w)$ and $F_2(L, w)$ in Theorem 5.13 can both be obtained. For weight 4 and length between 32 and 400, the upper bound on $M^e(L, w)$ given by Theorem 5.13 is also contained in Fig. 5.1.

The upper bounds on size of CAC are due to [34]. We plot the value for weight 4 in Fig. 5.1 for the convenience of the readers to compare SCAC and equi-difference SCAC with CAC.

Furthermore, the next theorem gives upper bounds on the value of $F(L, w)$, $F_1(L, w)$ and $F_2(L, w)$ in closed-form expression, from which we can obtain the asymptotic growth rate of upper bounds on $M(L, w)$ and $M^e(L, w)$ respectively.

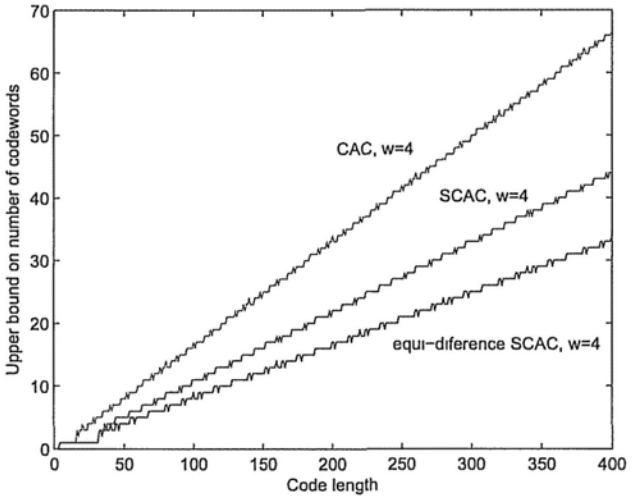

Figure 5.1: Upper bounds on size of CAC, SCAC and equi-difference SCAC for weight 4.

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

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

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

Theorem 5.15. *For $L \geq 2w^2$ and $w \geq 2$, we have*

$$M(L,w) \leq \left\lfloor \frac{L-2}{3w-3} + \frac{\pi(3w-2)}{3} \right\rfloor, \tag{5.28}$$

$$M^e(L,w) \leq \left\lfloor \frac{L-2}{4w-4} + \frac{3\pi(2w-2)}{4} \right\rfloor. \tag{5.29}$$

Proof. Recall that $F(L,w)$ is the maximum of

$$\sum_{x \in \mathcal{S}} (x - 1 - x(\lceil w/x \rceil + \lceil 2w/x \rceil) + 3w), \tag{5.30}$$

taken over all subsets $\mathcal{S}$ in $\mathscr{S}(L, w)$. For $x/2 < w \leq x$, we observe that

$$\begin{aligned} x - 1 - x(\lceil w/x \rceil + \lceil 2w/x \rceil) + 3w &= x - 1 - 3x + 3w \\ &= 3w - 2x - 1 \\ &\leq w - 1, \end{aligned}$$

and for $w > x$, we have

$$\begin{aligned} x - 1 - x(\lceil w/x \rceil + \lceil 2w/x \rceil) + 3w &\leq x - 1 - x(3w/x) + 3w \\ &= x - 1 < w - 1, \end{aligned}$$

and for $w \leq x/2$, we have

$$\begin{aligned} x - 1 - x(\lceil w/x \rceil + \lceil 2w/x \rceil) + 3w &\leq x - 1 - 2x + 3w \\ &= 3w - x - 1 \leq w - 1. \end{aligned}$$

In summary, we obtain

$$x - 1 - x(\lceil w/x \rceil + \lceil 2w/x \rceil) + 3w \leq w - 1$$

for all $x \in S(L, w)$.

The number of summands in (5.30) is less than or equal to the maximum number of relatively prime integers in $S(L, w)$. Since $S(L, w) \subseteq \{2, 3, \ldots, 3w - 2\}$, the number of summands in (5.30) is less than or equal to the maximal number of relatively prime integers between 2 and $3w - 2$, namely $\pi(3w - 2)$. The summation in (5.30) is thus less than or equal to $(w - 1)\pi(3w - 2)$, and hence

$$F(L, w) \leq (w - 1)\pi(3w - 2).$$

The result of (5.28) in Theorem 5.15 follows by replacing $F(L, w)$ by $(w - 1)\pi(3w - 2)$ in Theorem 5.6.

Now we will prove (5.29) in Theorem 5.15. From the definition of $S_1(L, w)$, we obtain

$$2w - x - 1 \leq w - 1$$

for all $x \in S_1(L, w)$.

The number of summands in (5.24) is less than or equal to the maximum number of relatively prime integers in $S_1(L, w)$. Since $S_1(L, w) \subseteq \{w, w+1, \ldots, 2w-2\}$, the number of summands in (5.24) is less than or equal to the maximal number of relatively prime integers between 2 and $2w - 2$, namely $\pi(2w - 2)$. The summation in (5.24) is thus less than or equal to $(w - 1)\pi(2w - 2)$, and hence

$$F_1(L, w) \leq (w - 1)\pi(2w - 2).$$

By the same argument, we also can find

$$F_2(L, w) \leq (w - 1)\pi(2w - 2).$$

Inequity (5.29) follows by replacing $F_1(L, w)$ and $F_2(L, w)$ by $(w - 1)\pi(2w - 2)$ in Theorem 5.13. □

The following is an asymptotical version of Theorem 5.15 which implies for each w, the growth of upper bounds on $M(L, w)$ and $M^e(L, w)$ are roughly linear in L, with slope $(3w - 3)^{-1}$ and $(4w - 4)^{-1}$ respectively.

Theorem 5.16. *For $w \geq 2$, we have*

$$\limsup_{L\to\infty} \frac{M(L, w)}{L} \leq \frac{1}{3w - 3}, \tag{5.31}$$

$$\limsup_{L\to\infty} \frac{M^e(L, w)}{L} \leq \frac{1}{4w - 4}. \tag{5.32}$$

Proof. The result in (5.31) follows from taking lim sup after dividing L on both sides in (5.28). We also can find (5.32) from (5.29). □

5.6 Tightness of Asymptotic Upper Bound on $M^e(L, w)$

In this section, we will show that there exists $\mathsf{SCAC}^e(L, w)$s, asymptotically achieving the upper bound in (5.32) of Theorem 5.16 for each w. First we introduce the following approach to construct $\mathsf{SCAC}(L, w)$ from existing CAC. It can be view as an application of Lemma 1.1 due to [21].

Theorem 5.17. *If there exists a CAC of M codewords, each with Hamming weight w and period l, then there exists an $\mathsf{SCAC}(2l, w)$ with M codewords.*

Proof. By doubling all elements in each $\mathcal{I}$ of a given CAC and period l, we can construct a new CAC with period $2l$. All elements in the set of differences of each codeword in this new CAC can be found as even. We thus have

$$d^*(\mathcal{I}_j)' \cap d(\mathcal{I}_k) = \emptyset$$

for all $j \neq k$. It implies the new CAC is an $\mathsf{SCAC}^e(2l, w)$ with M codewords. □

The following asymptotic result of CAC is due to [33]. It can be used to directly construct asymptotically optimal $\mathsf{SCAC}^e(L, w)$. Denote the maximal number of codewords in the class of all CACs with length L and weight w by $M^e_{\mathsf{CAC}}(L, w)$.

Theorem 5.18 ([33, Prop. 3]). *For all $w \geq 2$ we have*

$$\limsup_{L\to\infty} \frac{M^e_{\mathsf{CAC}}(L, w)}{L} \geq \frac{1}{2w - 2}.$$

For general w, we have the following

Theorem 5.19. *For all $w \geq 2$ we have*

$$\limsup_{L\to\infty} \frac{M^e(L,w)}{L} = \frac{1}{4w-4}.$$

Proof. Following Theorem 5.17 and Theorem 5.18, we have

$$\limsup_{L\to\infty} \frac{M^e(L,w)}{L} \geq \frac{1}{4w-4}.$$

This shows that the asymptotic lower bound in (5.32) is tight and proves Theorem 5.19. □

5.7 Conclusion

In this chapter, we introduce SCAC used in multiple access for the asynchronous collision channel without feedback. It is a special class of CAC, which is for the slot-synchronous channel. We present upper bounds on the size of SCAC and equi-difference SCAC, which hold for all weights in general.

For each w, we show the asymptotic upper bounds on $M(L,w)$ and $M^e(L,w)$ are linear in L, with slope $(3w-3)^{-1}$ and $(4w-4)^{-1}$ respectively. By constructing asymptotically optimal equi-difference SCAC with existing CAC, we prove that the asymptotic upper bound on $M^e(L,w)$ is tight. However, the tightness of upper bound on $M(L,w)$ is still unknown and would be a challenging direction for further studies.

□ **End of chapter.**

Chapter 6

User-Detectable Sequences

Summary

In this chapter 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 chapter. In addition, we display some interconnections with some other sequence designs.

6.1 Introduction

In this chapter, we focus on the collision channel without feedback described in Section 1.1. Consider a time-slotted system with slot synchronization, consisting of M potential users and one sink. All users may be active at the same time. For practical considerations, one would like to remove the assumption that the slot boundaries are synchronized. 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 [1, 10] 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.:

1) to detect each active user (detection),

2) to determine the sender of each successful received packet (decoding), and

3) to find their delay offsets (synchronization).

In this chapter we investigate only the detection problem, as task 2) and 3) 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* [11, 15] with the assumption all active users start its codeword

at the same time, which is applicable in signature codes, group testing, etc. It can be viewed as a special case of the concept discussed here (each active user can send its sequence at any time slot).

In this chapter, in order to explore the minimal delay in the worst case, we are interested in $L^D_{\min}(M)$, the smallest length L such that a UD sequence set exists for M users. The chapter is organized as follows. After setting up some notations and definitions in Section 6.2, we establish a lower bound on $L^D_{\min}(M)$ in Section 6.3. Then an upper bound and related constructions are presented in Section 6.4. Section 6.5 gives a proof to show the existence of UD sequence set different from that in Section 6.4. Finally, we close in Section 6.6 with some concluding remarks.

6.2 Channel Model

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

Definition 6.1. 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 6.2. 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 $\{1, 2, \ldots, M\}$. A sequence set of period L is said to be UD if the following conditions:

1. If user i becomes active or starts a new sequence at t, then $i \in D(t + L - 1)$;
2. 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 $i \in \{1, 2, \ldots, M\}$.

6.3 A Lower Bound on Minimum Period

In order to explore the minimal delay we can achieve, a lower bound on $L^D_{\min}(M)$ 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 $C^i_A(t_0)$ 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 6.1: Sequence periods are indicated by underbrace. For some time offsets and starting time of each user, we have the

following:

$$
\begin{aligned}
c_1(t) &: \underbrace{11000010000000011000010000000}0 \\
c_2(t) &: \underbrace{11100000000000}0000000000000 \\
c_3(t) &: 0\underbrace{10000100001000}000000000000 \\
c_4(t) &: 000\underbrace{10010010000000}0000000000 \\
c_5(t) &: \underbrace{10001000100000010001001000000}0 \\
c(t) &: **1110*01101000*10010101000000
\end{aligned}
$$

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.

Proposition 6.1. *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 6.1, we have the following:

Proposition 6.2. *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 6.1 we know this sequence set is not UD. □

Then from the necessary condition in Proposition 6.2, we have the following lower bound on $L^D_{\min}(M)$.

Theorem 6.3. *For any positive integer M,*

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

Proof. Following Proposition 6.2, 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 $\{s_2, s_3, \ldots, s_{\lceil M/2 \rceil}\}$. We use blocking algorithm described in Section 3.3 to block s_1 by cyclically shifting $s_2, s_3, \ldots, s_{\lceil M/2 \rceil}$.

1. Fix the delay offset of s_1 to zero.
2. Cyclically shift s_2 so that maximal "1"s in s_1 is overlapped by $s_2^{(\tau_2)}$.

3. Cyclically shift s_3 in such a way that most of the remaining "1"s in s_1 are overlapped by $s_3^{(\tau_3)}$.

4. Cyclically shift s_4 in order to overlap most of the remaining "1"s in s_1 that are not overlapped by $s_2^{(\tau_2)}$ and $s_3^{(\tau_3)}$.

5. Continue for $s_5, s_6, \ldots, s_{\lceil M/2 \rceil}$.

A more detailed analysis presented in [36] 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 $\{s_1, s_2, \ldots, s_{\lceil M/2 \rceil}\}$ 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 $(8/9)\lceil M/2 \rceil^2$. □

6.4 An Upper Bound on Minimum Period

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

Definition 6.3. We say that $c(t)$ is *matched* to s_i at time t_0 if $\forall t = 0, 1, \ldots, L-1$, $s_i(t) = 1 \Rightarrow c(t_0 + t) = 1$ 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 $s_i(t) = c(t + t_0) = 1$. 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*.

Remark: 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 $i = 1, 2, \ldots, M$, 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 there is a 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 6.1 below.

Algorithm 6.1 Detecting algorithm for UI sequence sets.

```
for i = 1, 2, ..., M do
  for t_0 = 0, 1, 2, ... do
    if c(t) is matched to s_i(t) at t_0 then
      active(i) ← TRUE
    else
      active(i) ← FALSE
    end if
  end for
end for
```

The following shows that the above algorithm can indeed make the user-detection under some conditions. The definition of UI sequence set can be found in Definition 3.1 of Section 3.3.

Theorem 6.4. *A sequence set is UD by Algorithm 6.1 if it is UI.*

Proof. Consider user g and its assigned sequence s_g here. By Algorithm 6.1, 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 blocked 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 6.1. □

Furthermore, the following upper bound just directly follows Theorem 6.4.

Theorem 6.5. *Let $\Psi(M)$ be the smallest period such that there exists a UI sequence set of M sequences. Then we have*

$$L^D_{\min}(M) \leq \Psi(M).$$

The following upper bound is guaranteed by CRT construction [35] and some improved results provided in Section 4.4, Chapter 4.

Theorem 6.6. *Let p_M be the smallest prime larger than or equal to M. Then we have*

$$L^D_{\min}(M) \leq p_M(2M-1).$$

Example 6.2: By the CRT construction, for $M = 3$ we can design the following UD sequence set with $L = 15$:

$$s_1 = [100000100000100]$$
$$s_2 = [111000000000000]$$
$$s_3 = [100010001000000].$$

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.

$$c_1(t) : \underbrace{100000100000100100000100000100}00000$$
$$c_2(t) : 00000\underbrace{111000000000000}00000000000000$$
$$c_3(t) : 00000\underbrace{100010001000000100010001000000}$$
$$c(t) : 100001*1110011010000\overline{11}00100110000000$$

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 overline. 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 has been proved in [36] 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 $8M^2/9$.

6.5 Existence of UD Sequence Set which is not UI

An *optical orthogonal code*(OOC)$(L, w, \lambda_a, \lambda_c)$ [8] is a family of binary sequences of length L and weight w that satisfy the following two properties:

1. the Hamming auto-correlation of any sequence is not bigger than λ_a for any non-zero τ performed modulo L;
2. the pairwise Hamming cross-correlation of any pair sequences is not bigger than λ_c for any τ.

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 6.7 ([7]). *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 6.7.

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 6.7, 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 covered by other $M - 1$ sequences for some time offsets. It's easy to see the pairwise cross-correlation property between s_M and any other sequence is still unchanged. The auto-correlation property of s_M is also the same.

We first introduce another detection method which is different from Algorithm 6.1. The receiver keeps track with the set of active users by maintaining M Boolean variables $active(i)$ for $i = 1, 2, \ldots, M$, with the values set to FALSE initially. We summarize the procedure in Algorithm 6.2.

Algorithm 6.2 Detecting algorithm for sequence sets formed by OOC construction.

```
for i = 1, 2, ..., M do
  for t_0 = 0, 1, 2, ... do
    if c(t) is matched to s_i(t) at t_0 then
      if i = M then
        if ζ_{t_0}^{M} = ζ'_{t_0}^{M} and |ζ'_{t_0}^{M} ∩ ζ'_{t_j}^{j}| = 1 for any j ∈ {1, 2, ..., M − 1} and
        some t_j then
          active(i) ← FALSE
        else
          active(i) ← TRUE
        end if
      else
        active(i) ← TRUE
      end if
    else
      active(i) ← FALSE
    end if
  end for
end for
```

By Algorithm 6.2, we can show the above sequence set is indeed UD.

Theorem 6.8. *The sequence set formed by OOC construction is UD by Algorithm 6.2.*

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 blocked 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 blocked by other $M-1$ active sequences and a shift-version of itself for some time offsets. It contradicts the condition $w = M+1 > (M-1)\lambda_c+\lambda_a = (M-1)\cdot 1+1$. Thus by Algorithm 6.2, we can find the exact starting time of user g. The result can be easily generalized to $s_1, s_2, \ldots, s_{M-1}$. It further implies that user j actually does transmission at t if $t \in \zeta_{t_0}^j$ for any $j \in \{1, 2, \ldots, M-1\}$.

Now we will prove user M can also be detected. Our task now is to show Algorithm 6.2 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 $j \in \{1, 2, \ldots, M-1\}$ 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 6.2, even if it would be blocked by other users sometimes.

□

Remark: (i) By Algorithm 6.1 and CRT construction, we cannot determine the exact starting time of any active user. However,

each active user can be detected within some bounded delay, from the UI property of the entire sequence set, as presented in Theorem 6.4.

(ii) By Algorithm 6.2 and OOC construction, we can find the exact starting time of all active users except user M. Then with the exact starting time of other users, user M can be detected if and only if it has been active, even though it may be totally blocked by other users.

(iii) Theorem 6.8 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 6.6. 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 6.3: A sequence set which is not UI is given below:

$$\mathbf{s}_1 = [1100]$$
$$\mathbf{s}_2 = [1010]$$
$$\mathbf{s}_3 = [1110].$$

One can check this sequence set is UD. The period is smaller compared with Example 6.2. However, we can find it is in accordance with Proposition 6.2.

6.6 Conclusion

In this chapter, 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

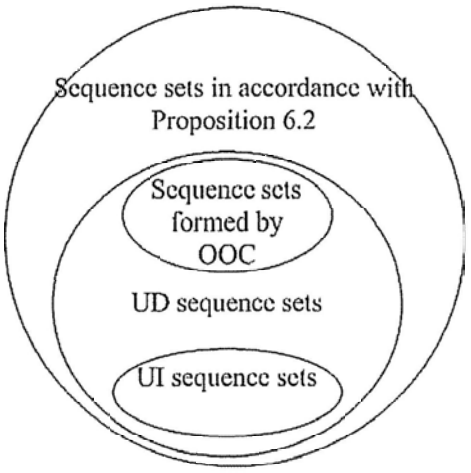

Figure 6.1: Relationships between UD sequences and other sequence designs.

M as the following:

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

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. 6.1, we displayed some interconnections between UD sequence set and other research areas in sequence design. This open up many interesting directions for further research.

□ **End of chapter.**

Chapter 7

Further Work and Open Problems

In Chapter 3, we have discussed bounds and special structures of UI sequence sets. It is further reported in [36] that the lower and upper bound on the minimum period are respectively $8M^2/9$ and $2M^2$ asymptotically. Thus we have the following open problem.

Problem 1. Close the gap asymptotically between the upper bound and lower bound on the minimum period of a UI sequence set of M sequences.

We are also interested in the case that in the slot-synchronized channel we can find at least one packet received successfully from each active user in L time slots, provided that the number of potential users is M and the number of active users is no more than K. The following is a question extending the results investigated in Chapter 3.

Problem 2. Establish the lower bound on minimum period of a sequence set of M sequences with the property that any sequence is not blocked by any other $K-1$ sequences.

For the asynchronous channel, CI sequence sets and SCAC are investigated in Chapter 4 and 5 respectively. The following are some interesting directions for further study.

Problem 3. Find the proof of Conjecture 4.15 and 4.16.

Problem 4. Provide the construction that asymptotically meets the upper bound in Theorem 5.6 or improve this upper bound.

In Chapter 6, we introduced UD sequence sets and presented lower and upper bounds on the minimum period. However, the following is still unsolved.

Problem 5. Improve the upper bound and lower bound on the minimum period of a UD sequence set of M sequences.

□ **End of chapter.**

Bibliography

[1] N. Q. A, L. Györfi, and J. L. Massey. Constructions of binary constant-weight cyclic codes and cyclically permutable codes. *IEEE Trans. Inform. Theory*, 38(3):940–949, May 1992.

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

[3] V. Anantharam. The stability region of the finite-user slotted ALOHA protocol. *IEEE Trans. Inform. Theory*, 37(3):535–540, May 1991.

[4] S. Bitan and T. Etzion. Constructions for optimal constant weight cyclically permutable codes and difference families. *IEEE Trans. Inform. Theory*, 41(1):77–87, Jan. 1995.

[5] 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, Dec. 2008.

[6] C. S. Chen, W. S. Wong, and Y.-Q. Song. Constructions of robust protocol sequences for wireless sensor and ad hoc networks. *IEEE Trans. Vehicular Tech.*, 57(5):3053–3063, 2008.

[7] W. Chu and S. W. Golomb. A new recursive construction for optical orthogonal codes. *IEEE Trans. Inform. Theory*, 49(11):3072–3076, Nov. 2003.

[8] F. R. K. Chung, J. A. Salehi, and V. K. Wei. Optical orthogonal codes: design, analysis and applications. *IEEE Trans. Inform. Theory*, 35(3):595–604, May 1989.

[9] C. Ding, D. Pei, and A. Salomaa. *Chinese Remainder Theorem – Applications in Computing, Coding, Cryptography.* World Scientific Publishing, Singapore, 1996.

[10] L. Gyöfi and I. Vajda. Construction of protocol sequences for multiple-access collision channel without feedback. *IEEE Trans. Inform. Theory*, 39(5):1762–1765, Sept. 1993.

[11] S. Györi. Coding for a multiple access OR channel: a survey. *Discrete Applied Mathematics*, (156):1407–1430, 2008.

[12] J. Y. N. Hui. Multiple accessing for the collision channel without feedback. *IEEE J. Sel. Aareas Commun.*, SAC-2(4):575–582, July 1984.

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

[14] 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, Aug. 2007.

[15] W. H. Kautz and R. C. Singleton. Nonrandom binary superimposed codes. *IEEE Trans. Inform. Theory*, 10:363–367, Oct. 1964.

[16] M. Kneser. Abschätzungen der asymptotischen dichte von summenmengen. *Math. Zeit.*, 58:459–484, 1953.

[17] V. I. Levenshtein. Conflict-avoiding codes and cyclic triple systems. *Problems of Information Transmission*, 43(3):199–212, 2007.

[18] V. I. Levenshtein and V. D. Tonchev. Optimal conflict-avoiding codes for three active users. In *IEEE Int. Symp. Inform. Theory*, pages 535–537, Adelaide, Australia, Sept. 2005.

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

[20] J. L. Massey. The capacity of the collision channel without feedback. In *IEEE Int. Symp. Inform. Theory*, page 101, June 1982.

[21] J. L. Massey and P. Mathys. The collision channel without feedback. *IEEE Trans. Inform. Theory*, 31(2):192–204, Mar. 1985.

[22] M. Mishima, H.-L. Fu, and S. Uruno. Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3. *Design, Codes and Cryptography*, 52:275–291, 2009.

[23] K. Momihara. Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. *Design, Codes and Cryptography*, 45(3):379–390, 2007.

[24] K. Momihara, M. Müller, J. Satoh, and M. Jimbo. Constant weight conflict-avoiding codes. *SIAM J. Discrete Math.*, 21(4):959–979, 2007.

[25] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Inform. Theory*, 41(2):448–455, Mar. 1995.

[26] M. B. Nathason. *Additive Number Theory – Inverse Problems and Geometry of Sumsets.* Number 165 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1996.

[27] P. R. Prucnal, M. A. Santoro, and T. R. Fan. Spread spectrum fiber-optic local area network using optical processing. *J. Lightwave Technol.*, 4(5):547–554, 1986.

[28] 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.

[29] D. V. Sarwate and M. B. Pursley. Crosscorrelation properties of pseudorandom and related sequences. *Proc. IEEE*, 68(5):593–619, 1980.

[30] A. A. Shaar and P. A. Davies. Prime sequences: quasi-optimal sequences for OR channel code division multiplexing. *IEE Electron. Lett.*, 19(21):888–890, Oct. 1983.

[31] 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(7):3312–3322, July 2009.

[32] K. W. Shum and W. S. Wong. Construction and applications of CRT sequences. *To appear in IEEE Trans. Inform. Theory*, 2010.

[33] K. W. Shum and W. S. Wong. A tight asymptotic bound on the size of constant-weight conflict-avoiding codes. *Des. Codes Cryptogr.*, 57(1):1–14, Oct. 2010.

[34] K. W. Shum, W. S. Wong, and C. S. Chen. A general upper bound on the size of constant-weight conflict-avoiding codes. *IEEE Trans. Inform. Theory*, 56(7):3265–3276, July 2010.

[35] 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.

[36] K. W. Shum, Y. Zhang, and W. S. Wong. User-irrepressible sequences. In *The 6th Conf. on Sequences and their Applications*, pages 88–101, Paris, Sept. 2010.

[37] E. M. Stein and R. Shakarchi. *Fourier Analysis: An Introduction.* Princeton University Press, Princeton, New Jersey, 2003.

[38] G. Thomas. Capacity of the wireless packet collision channel without feedback. *IEEE Trans. Inform. Theory*, 46(3):1141–1144, 2000.

[39] E. L. Titlebaum. Time-frequency hop signals, part I: coding based upon the theory of linear congruences. *IEEE Trans. Aerosp. Electron. Syst.*, AES-17(4):490–493, July 1981.

[40] B. S. Tsybakov and A. R. Rubinov. Some constructions of conflict-avoiding codes. *Problemy Peredachi Informatsii*,

38(4):268–279, 2002. [Problem of Inform. Trans. (English Transl.) pp.268–279].

[41] W. S. Wong. New protocol sequences for random access channels without feedback. *IEEE Trans. Inform. Theory*, 53(6):2060–2071, June 2007.

[42] G. Yang and W. C. Kwong. Performance analysis of optical CDMA with prime codes. *IEE Electron. Lett.*, 31(7):569–570, Mar. 1995.

[43] G. Yang and W. C. Kwong. *Prime Codes with Applications to CDMA Optical and Wireless Networks.* Artech House, Norwood, Massachuset, 2002.

[44] Y. Zhang, K. W. Shum, and W. S. Wong. On pairwise shift-invariant protocol sequences. *IEEE Commun. Lett.*, 13(6):453–455, June 2009.

[45] Y. Zhang, K. W. Shum, and W. S. Wong. Completely irrepressible sequences for the asynchronous collision channel without feedback. *submitted to IEEE Trans. Vehicular Tech.*, 2010.

[46] Y. Zhang, K. W. Shum, and W. S. Wong. Strongly conflict-avoiding codes. *submitted to SIAM J. Discrete Math.*, 2010.

[47] Y. Zhang, K. W. Shum, and W. S. Wong. User-detectable sequences for the collision channel without feedback. In *The 7th Int. Symp. on Wireless Commun. Systems*, York, Sept. 2010.