User Unsuppressible Protocol Sequences for Collision Channel without Feedback

Chung Shue Chen[†], Kenneth W. Shum[‡], Chi Wan Sung[††], Wing Shing Wong[‡], Geir E. Øien[†]

[†] Dept of Electronics & Telecommunications
Norwegian University of Science and Technology
7491 Trondheim, Norway
E-mail: {cschen, oien}@iet.ntnu.no

[‡] Dept of Information Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
E-mail: kshum2008@gmail.com, wswong@ie.cuhk.edu.hk

[††] Dept of Electronic Engineering
City University of Hong Kong, Tat Chee Ave, Kowloon, Hong Kong
E-mail: albert.sung@cityu.edu.hk

Abstract

A revisit of the model of collision channel without feedback (CCw/oFD) has motivated some interesting designs on periodic binary sequences. The protocol and system simplicity is particularly favorable for applications in certain wireless sensor and ad hoc networks. User unsuppressibility for individual service guarantee is desirable and emphasized here. We review some protocol sequences that are user unsuppressible (UU). Lower bounds of sequence length are obtained. Some corresponding sequence sets are identified.

1. INTRODUCTION

In multi-access communications, random accessing has played an important role since early works [1, 2, 3] due to its simplicity and effectiveness in many different systems [4, 5, 6]. Slotted ALOHA [1] is one of the well-known examples. In the shared random access channel, if users transmit without coordination, packet collisions are natural and inevitable. For collision-free transmission, one may consider a rigid scheme such as TDMA. However, sometimes it may not be practical due to the stringent time synchronization requirement. Contention based random access protocols such as IEEE 802.11 CSMA/CA [5] could provide a more flexible scheme. However, it should be noted that they usually require some complicated processing such as backoff algorithms and random number generation.

In this paper, we consider a slotted multiple access channel model called the *collision channel without feedback* (CCw/oFD) [7]. It is assumed that senders cannot synchronize transmissions between one another as their relative time offsets are unknown to each other due to a lack of feedback links. Periodic binary *protocol sequences* are used to define channel access permission. A user will simply transmit a packet when its protocol sequence refers to '1'. Otherwise, it keeps silent. When more than one user transmit at a time slot, a collision occurs and it is considered that the information in the packet cannot be recovered. Fundamentally, it is shown in [3] that a reliable multi-access communication under CCw/oFD is achievable with carefully designed protocol sequences. Meanwhile, the zero error capacity region is derived.

The system simplicity is particularly interesting and attractive for applications in certain communication systems such as wireless sensor, RFID, and impulse radio systems in which sharing a radio channel with the requirement of well-coordinated transmissions and time offsets is often hard to thin devices. It does not require strict user synchronization, frequent channel monitoring and backoff algorithms, and can provide alternative options of distributed multiple access control.

For protocol sequences, some common design criteria include the maximum number of allowable sequences, their cross-correlation property, and required sequence length. In this paper, we focus on *user unsuppressibility* [8], which is a condition guaranteeing that each user can transmit at least one packet successfully within a certain period, no matter what the relative delay offsets of the other users are. The individual throughput may be low. However, it is important to ensure that each user can successfully transmit without collision to a certain amount in every deterministic time period. Traditional designs often focus on system throughput but little on individual guarantees. Note that the unsuppressibility property under CCw/oFD also fits well in defining delay-bounded MAC for unidirectional wireless links [9]. In general, short sequences

are more favorable. Given M users, we want to find a set of M user unsuppressible (UU) protocol sequences. The goal is to minimize the length, N, of the protocol sequences. We will review some sequence designs in the literature that are user unsuppressible. Lower bounds of N are derived and used to evaluate the performance of those designs.

The rest of the paper is organized as follows. Section 2 describes the system model. Constructions of protocol sequences for user unsuppressibility and shorter length are investigated and suggested in Section 3. Section 4 provides the comparison and a fundamental study of the design possibility. Finally, Section 5 contains some concluding remarks.

2. SYSTEM MODEL

The model of CCw/oFD is employed [3]. Consider a communication channel that is shared by M active users. It is divided into time slots of equal duration. Each user follows a periodic binary (0/1) sequence, $W = \{W(t), t = 0, 1, 2, \ldots\}$, and will transmit a packet at time slot t if and only if $W(t) = 1$. Here, we restrict our attention to the slot-synchronized model in which users transmit packets aligned to the slot boundaries. However, users do not know the time offsets between one another and cannot synchronize their transmissions. They may have different transmission starting time and relative delay offsets. At any t, if more than one user transmits at the same time, all the transmitted packets during the collision are considered lost. Otherwise, a receiver can receive the packet correctly and decode the content.

For a binary sequence W with period N, its *duty factor* [3] or transmission rate is defined as:

$$r \triangleq \frac{1}{N} \sum_{t=0}^{N-1} W(t), \qquad (1)$$

while its *weight*, w, is defined by the number of 1's, i.e., $w \triangleq rN$. The throughput of a user is defined by the fraction of packets it can send without suffering any collisions.

Let W_1 and W_2 be two binary sequences with common period N. For any relative time shift s, their Hamming cross-correlation is defined as:

$$H_{W_1, W_2}(s) \triangleq \sum_{t=0}^{N-1} W_1(t) W_2(t+s). \qquad (2)$$

3. PROTOCOL SEQUENCES WITH USER UNSUPPRESSIBILITY

Without loss of generality, we can have many different sequence designs which offer user unsuppressibility. However, the allowable number of active users, M, and their sequence common period, N, can be quite different [8]. The primary objective here is to have N as small as possible for general M, while user unsuppressibility holds. Some interesting designs and their characteristics are investigated below.

3.1. Wobbling Sequences

To support user unsuppressibility, one may employ wobbling sequences, $W_{b,l,d}$. The detailed definition can be found in [8]. We only briefly outline below. Let l be the square of a prime p, which will generate the shortest sequence set. For $b = 0, 1, \ldots, p-1$, the *linear congruence sequence* [10], $S_{b,l}$, is the binary sequence defined by specifying the 1's appearing at index set:

$$\{nl + nb - \lfloor nb/l \rfloor l : n = 0, 1, 2, \ldots\}. \qquad (3)$$

$S_{b,l}$ is of period p^4. For $d = 1, 2, \ldots, p$, the wobbling sequence is defined by:

$$W_{b,l,d}(t) = S_{b,l}(t) \vee \mathbf{L}^l S_{b,l}(t) \vee \cdots \vee \mathbf{L}^{(d-1)l} S_{b,l}(t) \qquad (4)$$

where $\mathbf{L}$ denotes the cyclic shift operator and $\vee$ refers to the logical OR operator.

Wobbling sequences support user unsuppressibility. However, it should be noted that they are designed mainly for high throughput but not just for user unsuppressibility. So, the duty factors for wobbling sequences are high.

Let $d = p$, by (4), there exists p wobbling sequences with $r = d/l = 1/p$ and $N = p^4$. Note that the construction is limited to prime p. Throughout this paper, we will use p to denote prime number. By the sum of the sequence cross-correlations, even when all these p sequences are used at the same time, unsuppressibility holds for every user. Therefore, it provides a solution of protocol sequences to support p active users with unsuppressibility. We denote its characteristics by the following triplet:

$$\left(M = p, N = p^4, r = 1/p \right). \qquad (5)$$

3.2. Subset of Prime Sequences

A *prime sequence* [4], $S_{b,p}$, can be represented by indexing the positions where its n-th entry of 1's appears, denoted by $I_S(n)$:

$$I_S(n) = np + nb - \lfloor nb/p \rfloor p \qquad (6)$$

where $b = 0, 1, \ldots, p-1$. They have $r = 1/p$ and $N = p^2$. For example, given $p = 3$, we have three

distinct sequences: {100100100}, {100010001}, and {100001010}.

It is known that $0 \le H_{S_{b,p}, S_{j \ne b, p}}(s) \le 2$, for any $0 \le s \le p^2 - 1$. For $b > 0$, the upper bound is tight. When $b = 0$, $H_{S_{0,p}, S_{j \ne 0, p}}(s) = 1$.

By the above cross-correlation properties, one can support a system of active users with unsuppressibility by a subset of the prime sequences $\{S_{b,p}\}$ as long as the sum of their duty factors does not exceed a certain threshold. To begin with, $S_{0,p}$ is included for usage because of its lower cross-correlation maximum, i.e., 1. Then, we will find out what is the maximum number of sequences allowed from the sequence set $\{S_{b \ne 0, p}\}$.

Clearly, if the total number of potential collisions is strictly less than p for each sequence period, user unsuppressibility holds. After taking into account $S_{0,p}$ and a sequence oneself, due to the tight upper bound 2, the maximum number of allowable sequences in the system is thus given by:

$$\lfloor ((p-1) - 1)/2 \rfloor + 1 + 1 = \lfloor p/2 \rfloor + 1. \tag{7}$$

So, we can have a solution of protocol sequences with user unsuppressibility and characteristics:

$$\left(\lfloor p/2 \rfloor + 1, p^2, 1/p \right). \tag{8}$$

Comparing (8) and (5), for same M, by substituting $M = \lfloor p/2 \rfloor + 1$, (8) requires $N < 4M^2$, i.e., generally, a shorter sequence period is required. A detailed comparison will be given in Section 4.

3.3. Extended Prime Code

It is observable that the cross-correlation between sequences has a significant impact on the number of potential collisions and thus M, which can be increased if the maximum cross-correlation is reduced.

Extended prime code (EPC) was introduced in [11]. A number of $(p-1)$ extra zeros are padded after every p elements in a prime sequence. Thus, $N = p(2p-1)$, while $r = 1/(2p-1)$. For example, given $p = 3$, we have {100*00* 100*00* 100*00*}, {100*00* 010*00* 001*00*} and {100*00* 001*00* 010*00*}, where "*00*" are the extra zeros padded. They can help to reduce the maximum cross-correlation from two to one such that $0 \le H_{W_i, W_{j \ne i}}(s) \le 1$, for any $0 \le s < p(2p-1)$. It is observable that EPC gives a solution of protocol sequences for user unsuppressibility in characteristics:

$$\left(p, 2p^2 - p, 1/(2p-1) \right). \tag{9}$$

3.4. Shift Invariant Sequences

The class of shift invariant (SI) sequences [12] inherently hold user unsuppressibility as they always have positive individual throughput in each sequence period no matter what the relative time offsets are. Besides, there always exists the corresponding sequences. For a number of M symmetric rate users with $r = 1/k$, where k is a positive integer greater than 1, it can be shown that $N \ge k^M$.

To support user unsuppressibility, if there is no constraint on the duty factor, a good choice for the purpose of least common period is to set $r = 1/2$, since N will thus be 2^M. It is the least among all the possible choices. This can be shown by the fact that here, $N = k^M$.

For example, given $r = 1/2$ and $M = 3$, we have $N = 2^3 = 8$ and the corresponding SI sequences:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} 11110000 \\ 11001100 \\ 10101010 \end{bmatrix}. \tag{10}$$

Built on SI sequences, for any positive M, one can have protocol sequences with user unsuppressibility in the characteristic triplet:

$$\left(M, 2^M, 1/2 \right). \tag{11}$$

4. COMPARISON AND ANALYSIS

In the following, a detailed comparison of the sequence period required in the above four potential protocol sequences is presented. Furthermore, explorations on some fundamental limits are reported.

4.1. Sequence Length and the Lower Bound

As shown in Fig. 1, SI sequences $(M, 2^M, 1/2)$ have the smallest N among the four solutions for $M \le 6$, although inherently 2^M grows exponentially. Generally speaking, for $M \ge 7$, EPC has the smallest N. However, note that it requires prime p in sequence construction. Besides, when compared to wobbling sequence and prime sequence subset, EPC has smaller N since $M \ge 3$. When $M = 2$, prime sequence subset has the smallest N same as that in SI sequence. It should be noted that the current comparison is just on the requirement of N, while here we do not care much about their duty factor and actual throughput.

Furthermore, we are interested to know what the lower bound of N required for user unsuppressibility with respect to M is. One may guess M^2 (even if limited to prime p such that, p^2) is a valid lower bound in general. Clearly, the answer is no, by the counter-example observed when $M = 3$, in which we do have a solution from SI sequences that only requires $N = 2^3 = 8$, which is strictly less than M^2. Some valid lower bounds are given below.
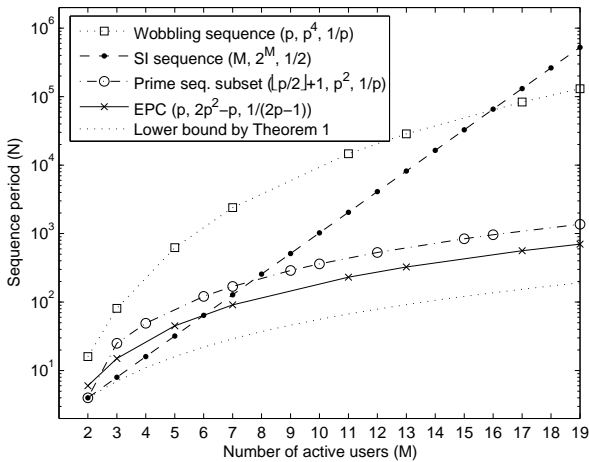
Figure 1: Sequence period is plotted against the number of active users supported. For those whose construction is limited to prime p, only the corresponding sets are shown. Their (M, N, r) is also indicated.

Theorem 1 *For any M protocol sequences that satisfy user unsuppressibility, N is at least $M(M+1)/2+1$.*

Proof: The proof proceeds by adding the users one by one. First, suppose that user 1 is transmitting while the rest are silent. It must occupy at least M time slots. Otherwise, if it occupies less than or equal to $M-1$ time slots, then we can properly choose a set of delay offsets for users $2, 3, \ldots, M$, such that user 1 is completely blocked by the others.

Next, fix the relative offset of user 1 and consider user 2. If users $3, 4, \ldots, M$ are silent, user 2 must be able to transmit at least $M-1$ packets successfully. Otherwise, by picking some delay offsets of users $3, 4, \ldots, M$, user 2 can be completely blocked. Now, user 1 and 2 together occupy at least $M + (M-1)$ time slots.

By similar argument, one can find that users $1, 2, \ldots, M-1$ must together occupy at least $M + (M-1) + \ldots + 2$ slots.

In order to accommodate the last user, we need at least two more empty slots. Otherwise, if the period is $M + (M-1) + \ldots + 2 + 1$ only, then there is at most one empty slot for the last user when users $1, 2 \ldots, M-1$ are active. We can pick a relative offset of user M so that user M does not transmit in this empty slot. Then, user M is suppressed by other users. This implies that

$$N \geq 1 + \sum_{k=1}^{M} k = 1 + M(M+1)/2. \qquad (12)$$

$\square$

There is another simple bound for the special case when each sequence contains exactly M ones in each period, i.e., $w = M$.

Theorem 2 *A user unsuppressible (UU) sequence set with characteristic triplet $(M, N, M/N)$ must satisfy $N \geq M^2$.*

Proof: A proof can be established similarly to that in [13, Proof of Theorem 1]. For any two sequences W_1 and W_2 in an $(M, N, M/N)$ sequence set, $\sum_{s=0}^{N-1} H_{W_1, W_2}(s) = M^2$. On the other hand, for UU to hold, the Hamming cross-correlation for each pair of sequences cannot be greater than 1 for any s, i.e., $H_{W_1, W_2}(s) \leq 1$. Therefore, $\sum_{s=0}^{N-1} H_{W_1, W_2}(s) \leq N$. Combining the above two, we get $N \geq M^2$. $\square$

Clearly, since EPC has $r = p/(2p^2 - p)$, i.e., M/N, Theorem 2 is applicable to. Comparing the required N with the lower bound $N \geq M^2$, one can see that roughly speaking, EPC has a quite good N, especially in large M, as it is on the same order of M^2.

4.2. Tight Bound and the Available Sequence Sets

In addition, we conduct an exhaustive search of UU sequence sets in symmetric rate case. In other words, they have constant weight. Table 1 reports the result and tight bounds obtained. Some related and interesting sequence sets found are listed as well. Note that since the computation time required is exponentially increasing in M and the sequence length, the searching is hard for large M.

When $M = 2$, $N = 4$ is optimal, i.e., it is the minimum necessary sequence length for user unsuppressibility to hold. It also attains the bounds in both Theorem 1 and 2. Corresponding sequences are given by SI sequences in $(2, \mathbf{4}, 1/2)$, i.e.,

$$\begin{bmatrix} S_0 \\ S_1 \end{bmatrix} = \begin{bmatrix} 1010 \\ 0110 \end{bmatrix}. \qquad (13)$$

When $M = 3$, $N = 8$ is optimal. The corresponding sequences are given by SI: $(3, \mathbf{8}, 1/2)$, as shown in (10). By Theorem 1, the minimum period is at least 7. We will show in the Appendix that a period of 7 is impossible. Hence, the minimum period is equal to 8. The lower bound is thus improved.

For $M = 3$, it is also possible to have sets of UU protocol sequences in $N = 12$ and $r = 1/3$. One of the feasible constructions is given below:

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \end{bmatrix} = \begin{bmatrix} 111100000000 \\ 110011000000 \\ 101010100000 \end{bmatrix}. \qquad (14)$$

When $M = 4$, $N = 16$ is optimal. It is given by SI sequences in $(4, \mathbf{16}, 1/2)$. We can have

$$\begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} 1111111100000000 \\ 1111000011110000 \\ 1100110011001100 \\ 1010101010101010 \end{bmatrix}. \qquad (15)$$

Theorem 1 says that the minimum period is at least 11. An exhaustive search is conducted for $N = 11$, 12, 13, 14 and 15, showing that no UU sequence set exists for N less than or equal to 15. Hence, $N = 16$ is the optimal period for 4 users.

Table 1: Results from exhaustive search. Labels: SI sequence, EPC, PS: prime sequence subset, WS: wobbling sequence. Characteristic triplet: (M, N, r).

M	Tight bound on N, available seq. set	Some other interesting UU sequence sets
2	$N = 4$, SI: $(2, \mathbf{4}, 1/2)$ $\equiv$ PS: $(2, 4, 1/2)$	EPC: $(2, 6, 1/3)$ WS: $(2, 16, 1/2)$
3	$N = 8$, SI: $(3, \mathbf{8}, 1/2)$	$9 \leq N \leq 11$: impossible to have UU sequence set under these N-values. Some UU sets available: $(3, 12, 1/4), (3, 12, 1/3),$ $(3, 12, 5/12), (3, 12, 1/2),$ EPC: $(3, 15, 1/5),$ PS: $(3, 25, 1/5),$ WS: $(3, 81, 1/3)$
4	$N = 16$, SI: $(4, \mathbf{16}, 1/2)$	PS: $(4, 49, 1/7)$
5	(unknown)	SI: $(5, \mathbf{32}, 1/2),$ EPC: $(5, 45, 1/9),$ WS: $(5, 625, 1/5)$
6	(unknown)	SI: $(6, \mathbf{64}, 1/2),$ PS: $(6, 121, 1/11)$
7	(unknown)	EPC: $(7, \mathbf{91}, 1/13),$ SI: $(7, 128, 1/2),$ PS: $(7, 169, 1/13),$ WS: $(7, 2401, 1/7)$
$\vdots$	$\vdots$	$\vdots$

5. CONCLUDING REMARKS

An exploratory investigation of multiple access control by protocol sequences in CCw/oFD with particular interests in the assurance of user unsuppressibility is reported. It aims to ensure individual service guarantee for every user and over each sequence period, even without backoff mechanisms and strict user synchronization. Four classes of periodic binary sequences are investigated and tailored for the unsuppressibility property. Meanwhile, sequences in minimum length are emphasized. A detailed comparison of their required sequence period is conducted. Besides, theoretical results of the lower bound are established. By an exhaustive search, some shortest and related sequence sets are identified. Results reported can provide interesting alternative design options of distributed multi-access protocols, and may also lead to a new stimulating and challenging research area.

Appendix

In this appendix, we will show that there does not exist an UU protocol sequence set for 3 users with period 7. The proof relies on the Cauchy-Davenport theorem from additive number theory (see e.g., [14]). Let $\mathbb{Z}_p$ denote the set of residues modulo p, where p is a prime number p. For two subsets A and B in $\mathbb{Z}_p$, the *sum set* $A + B$ is defined as:

$$\{a + b \in \mathbb{Z}_p : a \in A, b \in B\}. \qquad (16)$$

The Cauchy-Davenport theorem says that for any two subsets A and B of $\mathbb{Z}_p$, with p prime, if $A + B \neq \mathbb{Z}_p$, then

$$|A + B| \geq |A| + |B| - 1 \qquad (17)$$

where $|\cdot|$ denotes the cardinality of a set.

Let $-A$ denote the set $\{-a \in \mathbb{Z}_p : a \in A\}$. Then $A + (-A)$ is the set of differences between pairs of elements in A. We will use the special case of Cauchy-Davenport theorem when $p = 7$, $B = -A$, and $|A| \geq 4$. We state it explicitly below:

Proposition 3 *If we pick a subset A of $\mathbb{Z}_7$ with cardinality greater than or equal to 4, then $A + (-A) = \mathbb{Z}_7$, i.e., if we compute the differences between all pairs of elements in A, we will see $0, 1, 2, \ldots, 6$.*

We will apply the above result with A consisting of the locations of ones in a period. For example, consider the sequence $\{1111000\}$ of period 7. The ones are located at $A = \{0, 1, 2, 3\} \subset \mathbb{Z}_7$. Then, $-A = \{0, 6, 5, 4\}$, and $A + (-A) = \{0, 1, 2, \ldots, 6\} = \mathbb{Z}_7$.

The proof proceeds by contradiction. Suppose that we have a set of three UU protocol sequences with period 7. Denote the three sequences by S_A, S_B, and S_C. If the weight of each sequence is exactly 3, i.e., there are exactly 3 ones in each sequence, then we know that the period is at least 9 by Theorem 2. So, there is at least one sequence with at least 4 ones in a period.

Suppose S_A has 4 or more ones, and one of the other sequences, say S_C, has 3 ones in a period. By Proposition 3, for any difference $d = 1, 2, \ldots, 6$, we can always find a pair of ones in S_A with difference d. So, the first two ones in S_C can be blocked by S_A after picking a suitable offset. The remaining one in S_C can be blocked by S_B. Therefor, S_C is completely blocked. This contradicts the unsuppressibility assumption. Hence, all the three sequences have at least 4 ones in a period.

Suppose S_C has exactly 4 ones in a period. By the same argument, the first two ones of S_C can be blocked by S_A, and the last two ones can be blocked by S_B. Again, S_C can be completely blocked, and user unsuppressibility is not satisfied.

Therefore, we can conclude that one of the sequences must have at least 5 ones in a period. Suppose S_A has 5 ones and occupies 5 slots in a period. Then, there is only two slots left for the other two users, one slot for each of them. S_B and S_C must be all ones in order to transmit one packet for any shift. However, it is clear that we cannot have all-one sequence in a UU sequence set.

Now, we have eliminated all the possible cases for UU sequence set of period 7 for three users. Hence, it is concluded that such a protocol sequence set does not exist. □

Acknowledgments

References

[1] N. Abramson, "Packet switching with satellites," in *AFIPS Conf. Proc., Nat. Computer Conf.*, vol. 42, Jun. 1973, pp. 695–702.

[2] R. G. Gallager, "A perspective on multiaccess channels," *IEEE Trans. Inform. Theory*, vol. 31, no. 2, pp. 124–142, Mar. 1985.

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

[4] A. A. Shaar and P. A. Davies, "Prime sequences: quasi-optimal sequences for OR channel code division multiplexing," *IEE Electron. Lett.*, vol. 19, no. 21, pp. 888–890, Oct. 1983.

[5] IEEE Std 802.11, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," IEEE-SA Standards Board, 1999.

[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. Veh. Technol.*, vol. 57, no. 5, Sep. 2008.

[7] J. L. Massey, "The capacity of the collision channel without feedback," in *IEEE Int. Symp. Inform. Theory*, Jun. 1982, p. 101.

[8] W. S. Wong, "New protocol sequences for random access channels without feedback," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2060–2071, Jun. 2007.

[9] B. Andersson, N. Pereira, and E. Tovar, "Delay-bounded medium access for unidirectional wireless links," in *15th Intl. Conf. Real-Time Network and Syst.*, Nancy, France, Mar. 2007, pp. 1–10.

[10] E. L. Titlebaum, "Time-frequency hop signals, part I: coding based upon the theory of linear congruences," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-17, no. 4, pp. 490–493, Jul. 1981.

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

[12] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invaraint protocol sequences for collision channel without feedback," submitted.

[13] H. Chung and P. V. Kumar, "Optical orthogonal codes – new bounds and an optimal construction," *IEEE Trans. Inform. Theory*, vol. 36, no. 4, pp. 866–873, Jul. 1990.

[14] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. Springer-Verlag, 1996.