New Protocol Sequences for Random-Access Channels Without Feedback

Wing Shing Wong, *Fellow, IEEE*

***Abstract*—With recent developments in *ad hoc* networks and sensor networks, random-access protocol without feedback is a technique that deserves a closer look. This paper is based on Massey's model on random-access channel without feedback. A central concept of this model is the idea of protocol sequences. For these sequences, it is desirable that their cross correlation should be as low as possible and that the length of their period should not be too long, even if there is a large number of active users. Another useful feature is to be able to support multirate communication. Based on these considerations, a new family of protocol sequences is proposed in this paper. These new protocol sequences are built on the concept of prime sequences. It is shown that these sequences possess properties that make them suitable candidates for designing random access protocols for certain *ad hoc* or sensor networks.**

***Index Terms*—Hamming cross-correlation function, linear congruence sequence, prime sequence, protocol sequence, random-access channel without feedback, wobbling sequence.**

I. Introduction

THE idea of using deterministic coding sequences to define random-access protocol without feedback can be traced back to the seminal work of Massey and Mathys [1], [2]. Nguyen, László, and Massey [3] made a subsequent key contribution by applying constant-weight cyclically permutable codes to this problem. Other related works were reported in [4]–[7]. With recent developments in *ad hoc* networks, sensor networks, and radio-frequency identification (RFID), the issue of designing simple and efficient multiple-access algorithms for these systems calls for a revisit of this approach. Sensor networks (see, for example, [8]–[11]) pose an interesting challenge in particular. In addition to having a large number of devices distributed over a dynamically changing network topology, the sensors typically have very stringent size and power consumption requirements. Hence, it is desirable to implement simple random-access protocols that do not require frequent monitoring of the channel for feedback information and can avoid complicated processing such as back-off algorithm or random number generation.

A central concept in Massey's approach is the protocol sequence. A protocol sequence is a periodic binary sequence assigned to each user, which succinctly captures the information of when a user can transmit (sequence values equal to 1) and when to remain silent (sequence value equal to 0). Evaluating the performance of protocol sequences is a complicated issue and the outcome is dependent to some degree on the nature of the intended application. Nevertheless, the following criteria are 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 common period.
3. The length of the shortest common period for all active users. A shorter period tends to ensure less variability in performance.
4. The maximum number of distinct sequences that can be defined.
5. Support for *multirate* users. To do so, a scheme should include protocol sequences with a variety of duty factors. This is desirable since different sensors or communication nodes may have different data rate requirements.
6. Overhead issues. One example is the overhead for addressing the *identification problem* which deals with the issue of identifying the sender of a successfully received packet [2], [3].

Protocol sequences proposed in the literature provide different performance guarantees with regard to these criteria. It this paper, we propose a new family of protocol sequences, called the *wobbling sequences*, and discuss their performance characteristics with respect to the criteria described.

The construction of these sequences is based on the concept of *prime sequences*. Prime sequences were proposed by Shaar and Davies [12] and independently by Prucnal and his coworkers [13], around the same time when [1] was published. It was observed by Shaar that prime sequences are closely related to the frequency-hopping sequences introduced by Titlebaum [14] in 1981. The concept of a prime sequence has been further extended, such as in [15]–[18], with a particular view towards optical communication applications.

Wobbling sequences are periodic binary sequences. They have cross-correlation properties making them suitable for defining random-access protocols without feedback. It will be shown that these sequences are easy to generate and to decode. Protocols based on these sequences can accommodate a large number of active users and enjoy good sum rate. The period of these sequences does not grow exponentially as a function of the number of active users. For example, for the symmetric case where all users have equal rates, the minimum period of these sequences can be set to be the fourth power of the number

Manuscript received October 24, 2005; revised October 3, 2006. This work was supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region under Project 416906.

The author is with the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T. Hong Kong (e-mail: wswong@ie.cuhk.edu.hk).

Communicated by E. Modiano, Associate Editor for Communication Networks.

Digital Object Identifier 10.1109/TIT.2007.896867

of active users. The proposed protocol sequences can also accommodate multirate channels. However, a drawback of the scheme is that additional overhead bits are required in order to identify the packets, although such overheads are not unusual in multiple-access channel (MAC) protocols. (As an example, one can consider the MAC frame format specified in IEEE 802.11 [19].) Moreover, throughput lost due to such overheads can be made small if the amount of user data sent per transmission session is sufficiently large. For sensor network applications, the required data rate may be low, but the total amount of data to be transmitted over a session may be large. For example, each measurement from a sensor may be contained in a small-sized packet, but the measurements need to be repeated many times over a session. For such applications, initialization packets can be sent at the beginning of a transmission session, but overhead bits in subsequent packets in the same session can be avoided as explained in Section VI.

The organization of the rest of the paper is as follows. In Section II, we recall the basic communication model used by Massey to describe the random-access channel without feedback. This is the basic model assumed in this paper. Notations and definitions used in the later sections are also introduced. In Section III, we introduce the linear congruence sequences, which are a simple generalization of the prime sequences. These sequences are then used to construct the wobbling sequences introduced in this paper. Basic correlation properties of linear congruence sequences are presented in Section IV. The wobbling sequences are introduced in Section V along with descriptions of their fundamental correlation properties. In Section VI, we present the performance characteristics of a random-accessing scheme based on the wobbling sequences. Concluding remarks are provided in Section VII.

II. A Random Access Channel Model Without Feedback

A model for a collision channel without feedback has been considered previously in [1], [2]. We adopt this model here. Consider a communication channel that is shared by M active users. It is assumed that each of these users has an infinite backlog of packets to send. The channel is divided into time slots of equal duration. The users know the slot boundaries but are otherwise unsynchronized. Following [1], [2] we define a *protocol sequence*, $S = \{S(0), S(1), \ldots\}$, to be a binary sequence. An *active* user is said to transmit according to a protocol sequence S if the user transmits a packet at time slot i if and only if $S(i) = 1$. A receiver in the system listens to all time slots. (This assumption can be relaxed but it will not be considered here.) At any time slot, if only a single user transmits, the intended receiver can receive the packet correctly. The receiver then identifies who the sender of the packet is and decodes its content. If more than one user transmits, a collision occurs and all transmitted packets in that time slot are lost. It is further assumed that users employ coding across packets to recover data lost due to collisions. 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 completely unsynchronized. However, this more general scenario is not considered in this paper.

For a periodic binary sequence S with a minimum period N, following [2], define its *duty factor* by

$$r = \sum_{i=0}^{N-1} S(i)/N. \tag{2.0}$$

Users employing different duty factors transmit at different data rates. Given a protocol sequence set, denote the total number of distinct sequences that are defined by T. Denote the shortest common period of a sequence by N. If M users are active, let σ represent the minimum number of packets that can be sent by any user without suffering any collision within one period. For a protocol sequence set in which all sequences have the same duty factor, for example, when binary constant-weight cyclically permutable codes are used [3], [5], the ordered set (T, M, N, σ) is an important characteristic of the protocol sequence set.

Define the *rate* of a sequence as the ratio σ/N. The sum of the rates of all active users is referred to as the sum rate. For the case where the rates of all the users are symmetric, it has been shown in [2] that there exist protocol sequences with sum rate approaches $1/e$ as the number of active users tends to infinity. However, the period of these protocol sequences grows exponentially in M.

Sum rate is one way to measure the throughput performance of a protocol sequence set. For some sensor network or RFID applications, the required transmission data rate may be low, however, it is important to ensure that all transmitters can successfully transmit information at least once in a given time period, say in N time slots. We call such a property *un-suppressibility*. All protocol sequences reported in [1]–[7] can guarantee un-suppressibility, however the condition under which un-suppressibility can be guaranteed varies. These conditions include the maximum number of active users allowed and the length of the guarantee period N.

In some applications, transmitters are required to transmit at different data rate. However, not all protocol sequence sets proposed in the literature can support multirate sequences. For example, protocol sequences defined by using constant-weight cyclically permutable codes all have the same duty factor. The approach taken in [2], [7] allows simultaneous users with different duty factors. However, construction of the protocol sequences depends explicitly on the combination of the duty factors; different combinations may lead to different protocol sequences. In the approach proposed in this paper, multirate sequences are supported, although not all rates are permissible. The formulation of a sequence depends on its duty factor but is otherwise independent of other sequences. Hence, users requiring different duty factors can join or leave the system dynamically without affecting the protocol sequences of other users.

The protocol sequence set proposed in this paper is defined by means of a family of binary sequences called the *wobbling sequences*. It will be shown that such a protocol sequence set has good sum rate performance, allows for multirate transmissions, and can guarantee un-suppressibility for a large number of active users.

For construction of the proposed sequences, we need to employ some elementary number-theoretic concepts and notation. To fix ideas for subsequent discussions, recall that a *prime* is a positive integer that has no factor other than 1 and itself. Two distinct positive integers are *relatively prime* to each other if they have no common factors other than 1. Note that 1 is always relatively prime to any number. We represent the highest common factor of two integers a and b by $\mathrm{HCF}(a,b)$. If x is a real number, the notation $\lfloor x \rfloor$ represents the largest integer less than or equal to x and $\lceil x \rceil$ represents the smallest integer greater than or equal to x. Given two real numbers a and b, let $a \vee b$ denote the maximum number; hence, $0 \vee 0 = 0,\ 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$. Given three (possibly negative) integers a, b, and c, the equation

$$a = b \pmod{c} \tag{2.1}$$

holds if and only if there exists an integer l (possibly negative) such that

$$a = b + lc. \tag{2.2}$$

III. Linear Congruence Sequences

Let $S = \{S(i),\ i = 0,\ 1,\ \ldots\}$ be a binary sequence. Such a sequence can also be represented by indexing the positions at which it assumes the value of 1. That is, one can represent S by $\{I_S(i),\ i = 1,\ 2,\ \ldots\}$, where $I_S(i)$ denotes the position at which the ith entry of "1" in S appears. The following lemma relates the duty factor with the period of a sequence.

Lemma 1: If the sequence S is periodic with period N then for all nonnegative integers t

$$I_S(t + rN) = I_S(t) + N \tag{3.0}$$

where r is the duty factor of the sequence. Conversely, if for all nonnegative integers t

$$I_S(t + M) = I_S(t) + N \tag{3.1}$$

then S is periodic with period N and the duty factor of S is M/N.

The proof of this result is straightforward and is omitted.

The concept of prime sequences was introduced in [12]–[14]; it can be generalized to nonprimes. Let l be a positive integer and b be a nonnegative integer such that $b < l$. Define the linear congruence sequence generated by $(b,\ l)$ as follows.

Definition 1: Let $S = \{S(i),\ i = 0, 1, \ldots\}$ represent the linear congruence sequence generated by (b, l), then

$$I_S(i) = il + ib - \left\lfloor \frac{ib}{l} \right\rfloor l. \tag{3.2}$$

The integer b is known as the *key generator* of the sequence. When l is a prime, the sequence defined in (3.2) is simply a prime sequence ([12], [13]). The following result for linear congruence sequences is well known for prime sequences; it is included here for the sake of completeness.

Proposition 1: The minimum period of the linear congruence sequence generated by $(b,\ l)$ divides l^2 and has a duty factor of $1/l$. If b and l are relatively prime, then l^2 is the minimum period.

The proof of this result, which is based directly on the representation (3.2), is provided in Appendix A. As an illustrative example, the sequence generated by $(3, 9)$ has an I_S representation $(0, 12, 24, 27, 39, 51, 54, 66, 78, 81, \ldots)$ and a period of 27, which divides 81. On the other hand, the sequence generated by $(2, 9)$ has a period of 81.

If one considers the difference between two neighboring elements in a linear congruence sequence, one can see that

$$I_S(i+1) - I_S(i) = l + b - \left(\left\lfloor \frac{(i+1)b}{l} \right\rfloor - \left\lfloor \frac{ib}{l} \right\rfloor \right) l. \tag{3.3}$$

The sequence defined by

$$\left\{ \left\lfloor \frac{(i+1)b}{l} \right\rfloor - \left\lfloor \frac{ib}{l} \right\rfloor, \quad i = 0, 1, \ldots \right\}$$

is well known as a most regular binary sequence. (See, for example, [20] and also [21].)

IV. Correlation Properties of Linear Congruence Sequences

Definition 2: Let $S_1 = \{S_1(i)\}$ and $S_2 = \{S_2(i)\}$ be two periodic binary sequences with a common period N. As in [22], define the Hamming cross-correlation function between $\{S_1(i)\}$ and $\{S_2(i)\}$ for a shift s by

$$H_{S_1 S_2}(s) = \sum_{i=0}^{N-1} S_1(i) S_2(i+s). \tag{4.0}$$

In this paper, we prefer to use a normalized form of the Hamming cross-correlation function

$$\overline{H}_{S_1 S_2}(s) = \sum_{i=0}^{N-1} S_1(i) S_2(i+s)/N. \tag{4.1}$$

A nice property of the normalized form is that it always yields the same value no matter what common period is used. If $b_1 = b_2$, then the function in (4.1) is a normalized Hamming autocorrelation function. Note that for any integer j

$$\overline{H}_{S_1 S_2}(s) = \sum_{i=j}^{j+N-1} S_1(i) S_2(i+s)/N. \tag{4.2}$$

If one averages the normalized cross-correlation function over all shifts, the average value is simply the product of the duty factors of the sequences. This is a well-known fundamental result [23].

Lemma 2 [23]: Let S_1 and S_2 be periodic sequences with period N and duty factors r_1 and r_2 respectively. Then

$$\sum_{s=0}^{N-1} \overline{H}_{S_1S_2}(s) = r_1 r_2 N. \tag{4.3}$$

It is known that the cross-correlation function for prime sequences has a maximum value of 2. This is not true for linear congruence sequences in general. However, the following result holds.

Theorem 1: Let l, b_1, and b_2 be integers satisfying $0 \le b_1 < l$, $0 \le b_2 < l,\ b_1 \ne b_2$, and $\mathrm{HCF}(|b_2 - b_1|,\ l) = 1$. Let S_1 and S_2 be the linear congruence sequences generated by $(b_1,\ l)$ and $(b_2,\ l)$, respectively. For any shift $s,\ 0 \le s < l^2$, the normalized Hamming cross-correlation function satisfies

$$\overline{H}_{S_1S_2}(s) \le 2/l^2 = 2r^2 \tag{4.4}$$

where $r = 1/l$ is the duty factor of the sequence. Moreover, for if $b_1 = 0$ or $b_1 = 0$, then

$$\overline{H}_{S_1S_2}(s) = r^2. \tag{4.5}$$

The proof of this theorem is provided in Appendix B.

If l is a prime number, the relative prime condition of Theorem 1 is automatically satisfied. Hence, Theorem 1 is a generalization of the result in [12]. In subsequent discussions, we also need to investigate the autocorrelation property of these sequences. In particular, the following basic property of linear congruence sequences is needed for the construction of wobbling sequences.

Proposition 2: Let l and b satisfy $0 \le b < l$, and let S be a linear congruence sequence generated by $(b,\ l)$. If $b = 0$

$$\begin{aligned} &\overline{H}_{SS}(il) = 1/l \\ &\overline{H}_{SS}(s) = 0, \qquad \text{if } s \ne il. \end{aligned} \tag{4.6}$$

For the case $0 < b < l$ with l and b relatively prime

$$\begin{aligned} &\overline{H}_{SS}(0) = 1/l \\ &\overline{H}_{SS}(il) = 0, \qquad \text{for } i = 1, \ldots, l-1. \end{aligned} \tag{4.7}$$

Moreover, given any integer c_0 with $0 < c_0 < l$, let c_1 be the unique solution that satisfies $0 < c_1 < l$, and

$$c_1 b \equiv c_0 \pmod{l}. \tag{4.8}$$

Then $\overline{H}_{SS}(c_0 + c_1 l)$ and $\overline{H}_{SS}(c_0 + (c_1 - 1)l)$ are the only nonzero terms for shifts of the form $c_0 + il$. $l^2 \overline{H}_{SS}(c_0 + c_1 l)$ is equal to the number of integers n satisfying $0 \le n < l$, and

$$c_0 + nb - \left\lfloor \frac{nb}{l} \right\rfloor l < l; \tag{4.9}$$

$l^2 \overline{H}_{SS}(c_0 + (c_1 - 1)l)$ is equal to the number of integers n satisfying $0 \le n < l$ and

$$c_0 + nb - \left\lfloor \frac{nb}{l} \right\rfloor l \ge l. \tag{4.10}$$

Proof: Equations (4.6) and (4.7) are straightforward. The proof of the rest of the proposition mimics the proof of Theorem 1. In particular, the inequalities (4.9) and (4.10) are the corresponding versions of (B9) and (B15). Details are omitted. □

Note that (4.9) and (4.10) imply that

$$\overline{H}_{SS}(c_0 + c_1 l) + \overline{H}_{SS}(c_0 + (c_1 - 1)l) = 1/l. \tag{4.11}$$

It is also clear that $\overline{H}_{SS}(s)$ is strictly less than $1/l$ if both the generator of the sequence and the shift are positive. However, it can achieve values of up to $1/l - 1/l^2$. In other words, it is possible to resolve the relative shifts of S by means of autocorrelation. However, the resolution is not robust to error and interference.

The following cross-correlation property of linear congruence sequences is crucial to the construction of wobbling sequences.

Proposition 3: Let l, b_1, and b_2 be integers satisfying the conditions stated in Theorem 1. For $i = 1, 2$, let S_i be a linear congruence sequence generated by $(b_i,\ l)$, respectively. Then for any integers $c_0,\ d$, with $0 \le c_0 < l - 1$ and $1 \le d < l - 1$, the following holds:

$$\frac{d-1}{l^2} \le \sum_{i=0}^{d-1} \overline{H}_{S_1S_2}(c_0 + il) \le \frac{d+1}{l^2} \tag{4.12a}$$

and

$$\sum_{i=0}^{l-1} \overline{H}_{S_1S_2}(c_0 + il) = 1/l. \tag{4.12b}$$

The proof of this proposition is provided in Appendix C.

When the period of a linear congruence sequence is a power of a prime number, the following theorem explicitly describes the distribution of the cross-correlation values as a function of the shift value.

Theorem 2: Let $l = p^i$ be the power of a prime number and let integers b_1 and b_2 satisfy the conditions: $0 \le b_1 < l,\ 0 \le b_2 < l$, $b_1 \ne b_2$, and $\mathrm{HCF}(|b_2 - b_1|, p) = 1$. Denote by S_1 and S_2 the linear congruence sequences generated by (b_1, l) and (b_2, l), respectively. Let k, satisfying, $0 \le k < l - 1$, be the unique solution to

$$k(b_2 - b_1) \equiv b_1 b_2 \pmod{l}. \tag{4.13}$$

Then, for shifts varying between 0 and $l^2 - 1$, $(l - k)k$ of them satisfy the cross-correlation value

$$\overline{H}_{S_1S_2}(s) = 2/l^2, \tag{4.14}$$

$(l - k)k$ of them satisfy

$$\overline{H}_{S_1S_2}(s) = 0, \tag{4.15}$$

and $l^2 + 2k^2 - 2kl$ of them satisfy

$$\overline{H}_{S_1S_2}(s) = 1/l^2. \tag{4.16}$$

Proof of this theorem is provided in Appendix D.

TABLE I
$H_{S_1S_2}(c_0 + 8c_1) = 64\overline{H}_{S_1S_2}(c_0 + 8c_1)$

		Value of c_0							
		0	1	2	3	4	5	6	7
Value of c_1	0	**1**	**2**	**0**	**2**	**0**	**1**	**1**	**1**
	1	**1**	**0**	**2**	**0**	**2**	**1**	**1**	**1**
	2	**1**	**2**	**0**	**2**	**0**	**1**	**1**	**1**
	3	**1**	**0**	**2**	**0**	**2**	**1**	**1**	**1**
	4	**1**	**2**	**0**	**2**	**0**	**1**	**1**	**1**
	5	**1**	**0**	**2**	**0**	**2**	**1**	**1**	**1**
	6	**1**	**2**	**0**	**2**	**0**	**1**	**1**	**1**
	7	**1**	**0**	**2**	**0**	**2**	**1**	**1**	**1**

For example, if S_1 is the linear congruence sequence generated by $(1, 8)$ and S_2 by $(4, 8)$, then k in (4.13) is equal to 4. As shown in Table I, there are 16 shifts with a cross-correlation value of 2 (that is, a normalized value of $2/64$) and 16 shifts with value of 0.

Theorem 2 shows that in general the normalized cross-correlation function between two linear congruence sequences is $2/l^2$ for some shifts. So the bound in Theorem 1 is tight. On the other hand, one can show that for any two linear congruence sequences with period l^2 and duty factor $1/l$, the normalized cross-correlation function between them must be equal to or bigger than $1/l^2$ for some shifts. Hence, a natural question is whether there are families of periodic sequences with period l^2 and duty factor $1/l$ such that the normalized cross-correlation function between any two sequences is exactly $1/l^2$ for any shift.

In [24] (see also [18]), the concept of an extended prime sequence was introduced by padding extra zeroes in the prime sequences. It was shown that the maximum cross correlation for these sequences is 1. However, there are only p distinct sequences, with a duty factor of $1/p$ before padding and a common period of $p(2p-1)$. So after padding, the duty factor of these sequences is roughly $1/(2p)$ with at most p active users. In [25], a different approach to this question was presented. In that case, the system can support p distinct sequences each with a duty factor of $1/p$. However, a drawback of that approach is that the period of the sequences is exponential in p. We address this problem here by means of the wobbling sequences to be introduced in Section V.

Theorem 1 describes the Hamming cross-correlation function for linear congruence sequences with the same duty factor. To support multirate channels, sequences with different duty factors are needed. We present below a cross-correlation relation result for linear congruence sequences with different duty factors. First, the following lemma holds.

Lemma 3: Let l_1 and l_2 be positive integers, such that $l_1 = ql_2$ for some q that is a power of l_2. Let b_1 and b_2 be positive integers relatively prime to l_1. For any $0 \le s < l_1$, the equation

$$n_2 l_2 + n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l_2} \right\rfloor l_2 = n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + s \tag{4.17}$$

has at least q distinct solutions with $0 \le n_1 < l_1$.

Proof of this result is presented in Appendix E.

Remark: One can check directly that this result still holds if we let $b_2 = 0$ while keeping b_1 relatively prime to l_1. However, the result does not hold for $b_1 = 0$.

Let l_1 and l_2 be positive integers, such that $l_1 = ql_2$ for some q that is a power of l_2 and let b_1 be a positive integer and b_2 be a nonnegative integer. It is further assumed that b_1 and b_2 (if it is nonzero) are relatively prime to l_1. Let S_1 and S_2 be the linear congruence sequence generated by $(b_1,\ l_1)$ and $(b_2,\ l_2)$, respectively. S_1 and S_2 have a period l_1^2 with duty factors $r_1 = 1/l_1$ and $r_2 = 1/l_2$, respectively. Hence, the cross-correlation function between the two sequences is well defined.

Theorem 3: For the linear congruence sequences S_1 and S_2 previously defined

$$\overline{H}_{S_1S_2}(s) = q/l_1^2 = r_1 r_2 \tag{4.18}$$

for all nonnegative s.

Proof: For any s, with $0 \le s < l_1$, $l_1^2\overline{H}_{S_1S_2}(s)$ is equal to the number of solutions, $(n_1,\ n_2)$ to (4.17) with $0 \le n_1 < l_1$. By Lemma 3

$$l_1^2\overline{H}_{S_1S_2}(s) \ge q. \tag{4.19}$$

By Lemma 2

$$\sum_{t=0}^{l_1^2-1} \overline{H}_{S_1S_2}(t) = r_1 r_2 l_1^2 = \frac{l_1^2}{l_1 l_2} = q. \tag{4.20}$$

It follows that the inequality in (4.19) must in fact be an equality. □

Corollary: Let l_1 and l_2 be positive integers, such that $l_1 = ql_2$ for some q that is a power of l_2. Let b_1 and b_2 be positive integers relatively prime to l_1. For any $0 \le s$, the equation

$$n_2 l_2 + n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l_2} \right\rfloor l_2 = n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + s \tag{4.21}$$

has exactly q distinct solutions over any time period starting from i, $0 \le i \le n_1 < i + l_1$.

V. Wobbling Sequences and Their Correlation Properties

In subsequent discussions, we consider l to be a power of a prime number. That is

$$l = p^i \tag{5.0}$$

for some prime number p and positive integer i. We call the corresponding linear congruence sequence, a prime power sequence. For $0 \le b < l$, denote by $S_{b,\,l}$ the prime power sequence generated by $(b,\ l)$. Let $\boldsymbol{L}$ represent the operator that shifts a sequence by one element to the left. That is

$$\boldsymbol{L}S(i) = S(i+1). \tag{5.1}$$

Definition 3: Let $l = p^i$, with $i \ge 2$, be a prime power. Let b be an integer satisfying $0 < b < p$. For $1 \le d \le p$, the wobbling sequence generated by $(b,\ l,\ d)$, $W_{b,\,l,\,d}$, is defined by

$$W_{b,l,d}(i) = S_{b,l}(i) \vee \boldsymbol{L}^l S_{b,l}(i) \vee \boldsymbol{L}^{2l} S_{b,l}(i) \vee \cdots \vee \boldsymbol{L}^{(d-1)l} S_{b,l}(i). \tag{5.2}$$

For $b = 0$ and $1 \le d \le p$, $W_{0,\,l,\,d}$ is defined by

$$W_{0,l,d}(i) = S_{0,l}(i) \vee \boldsymbol{L}S_{0,l}(i) \vee \boldsymbol{L}^2 S_{0,l}(i) \vee \cdots \vee \boldsymbol{L}^{d-1} S_{0,l}(i). \tag{5.3}$$

Proposition 4: For $l = p^i$ with $i \ge 2$, $1 \le d \le p$, and $0 \le b < p$, the wobbling sequence $W_{b,\,l,\,d}$, has a duty factor equal to d/l.

Proof: For the case $0 < b < p$, b and l are relatively prime. By (4.7), the cross correlation between $\boldsymbol{L}^{jl}S_{b,l}$ and $\boldsymbol{L}^{kl}S_{b,l}$ for any pair of distinct, nonnegative integers j and k is zero. Similarly, (4.6) ensures that the cross correlation between $\boldsymbol{L}^{j}S_{0,l}$ and $\boldsymbol{L}^{k}S_{0,l}$ for any pair of distinct, nonnegative integers $0 \le j < p$ and $0 \le k < p$ is zero. Hence, in both cases, the number of the occurrences of "1" in $W_{b,\,l,\,d}$ is d times the number of the occurrences of "1" in $S_{b,\,l}$, and the duty factor of $W_{b,\,l,\,d}$ is d/l as claimed. □

The same arguments also show that for $0 < b < p$, $W_{b,\,l,\,d}$ is a binary sequence that can be represented as

$$\begin{aligned} W_{b,l,d}(i) &= S_{b,l}(i) + \boldsymbol{L}^{l}S_{b,l}(i) + \boldsymbol{L}^{2l}S_{b,l}(i) + \cdots + \boldsymbol{L}^{(d-1)l}S_{b,l}(i) \\ &= \sum_{j=0}^{d-1} S_{b,l}(i+jl). \end{aligned} \tag{5.4}$$

For $b = 0$, $W_{0,\,l,\,d}$ is a binary sequence that can be represented as

$$\begin{aligned} W_{0,l,d}(i) &= S_{0,l}(i) + \boldsymbol{L}S_{0,l}(i) + \boldsymbol{L}^{2}S_{0,l}(i) + \cdots + \boldsymbol{L}^{d-1}S_{0,l}(i) \\ &= \sum_{j=0}^{d-1} S_{0,l}(i+j). \end{aligned} \tag{5.5}$$

For illustration, consider the case $p = 3$, $l = p^2 = 9$. The linear congruence sequence $S_{1,9}$ has an I_S representation $(0, 10, 20, 30, 40, 50, 60, 70, 80, \ldots)$. $\boldsymbol{L}^9 S_{1,9}$ and $\boldsymbol{L}^{18} S_{1,9}$ can be represented by $(1, 11, 21, 31, 41, 51, 61, 71, 72, \ldots)$ and $(2, 12, 22, 32, 42, 52, 62, 63, 73, \ldots)$, respectively. The wobbling sequence $W_{1,9,3}$ is then defined to be

$$(0, 1, 2, 10, 11, 12, 20, 21, 22, 30, 31, 32, 40, 41, 42, 50, 51, 52, 60, 61, 62, 63, 70, 71, 72, 73, 80, \ldots).$$

The duty factor of this sequence is $1/3$ and its period is 81.

Theorem 4: Let $W_1 = W_{b_1,\,l,\,d_1}$ and $W_2 = W_{b_2,\,l,\,d_2}$ where $0 \le b_1 < p$, $0 \le b_2 < p$, $b_1 \ne b_2$, $1 \le d_1 \le p$, $1 \le d_2 \le p$. If $b_1 b_2 > 0$, then for all shift s

$$\overline{H}_{W_1W_2}(s) \le \frac{d_1(d_2+1)}{l^2} = \frac{d_2+1}{d_2} r_1 r_2 \tag{5.6}$$

where $r_1 = d_1/l$, $r_2 = d_2/l$ are the duty factors of the respective sequences. If $b_1 b_2 = 0$, then

$$\overline{H}_{W_1W_2}(s) = r_1 r_2. \tag{5.7}$$

Proof: From (5.4) and (5.5) it follows that if $b_1 b_2 > 0$, then

$$\overline{H}_{W_1W_2}(s) = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} \overline{H}_{S_1,S_2}(s + il + jl). \tag{5.8}$$

By Proposition 3, (5.8) can be reduced to the inequality

$$\overline{H}_{W_1W_2}(s) \le \sum_{i=0}^{d_1-1} \frac{d_2+1}{l^2} = \frac{d_1(d_2+1)}{l^2}. \tag{5.9}$$

If $b_1 = 0$

$$\overline{H}_{W_1W_2}(s) = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} \overline{H}_{S_1,S_2}(s + i + jl). \tag{5.10}$$

Equation (5.7) follows from Theorem 1. The case $b_2 = 0$ can be proven similarly. □

Theorem 5: Let p be a prime number and $l_2 = p^i$ for some positive integer i with $i \ge 2$. Let $l_1 = q l_2$ for some q that is a power of l_2. Let b_1 and b_2 be integers satisfying $0 \le b_2 < p$, $0 < b_1 < p$. For $1 \le d_1 \le p$, $1 \le d_2 \le p$, let $W_1 = W_{b_1,\,l_1,\,d_1}$ and $W_2 = W_{b_2,\,l_2\,d_2}$ with respective duty factor $r_1 = d_1/l_1$ and $r_2 = d_2/l_2$. Then

$$\overline{H}_{W_1W_2}(s) = r_1 r_2 \tag{5.11}$$

for all nonnegative s.

Proof: This proof is similar to Theorem 4. It follows from (5.4) and (5.5) together with Theorem 3. □

Definition 4: For any prime p and integer d with $1 \le d \le p$, construct a family of binary sequences $\boldsymbol{F}_p(d)$ as follows.

1. The wobbling sequence $W_{0,p^2,d}$ is in $\boldsymbol{F}_p(d)$.
2. For $i = 1,\ 2,\ \ldots$, let $j = 2^i$. For all such j and for all b satisfying $0 < b < p$, the wobbling sequences $W_{b,p^j,d}$ are in $\boldsymbol{F}_p(d)$.

Remark: There are infinite number of sequences in $\boldsymbol{F}_p(d)$ with different duty factors and periods. The periods of sequences in $\boldsymbol{F}_p(d)$ are of the form, $p^4,\ p^8, p^{16}, \ldots$ with duty factors $d/p^2, d/p^4, d/p^8,\ \ldots$, respectively.

VI. Basic Performance of Wobbling Sequences

Theorem 6: Consider the case $\boldsymbol{W} = \{ W_i,\ i = 1, \ldots, K \}$ consisting of elements in $\boldsymbol{F}_p(p)$ (note that $d = p$) with a common period N. Let r_j represent the duty factor of W_j. Assume that $\boldsymbol{W}$ satisfies the condition

$$\sum_{j=1}^{K} r_j \le 1. \tag{6.0}$$

Then for any W_i and any combinations of shifts, $s_1, \ldots, s_{i-1}$, $s_{i+1}, \ldots, s_K$, the following inequality holds:

$$\sum_{\substack{j=1 \\ j \ne i}}^{K} \overline{H}_{W_iW_j}(s_j) < r_i(1 - r_i/p). \tag{6.1}$$

Proof: Let the duty factor of W_i be r_i. Let v be the total number of sequences in the set $\boldsymbol{W}$ with duty factors equal to r_i. By definition of $\boldsymbol{F}_p(d)$, all these sequences are of the form $W_{b,l,p}$ with the same l and d but different generators, b. Since there are at most p such generators

$$v \le p. \tag{6.2}$$

By Theorem 4 and 5

$$\begin{aligned}&\sum_{\substack{j=1\\ j\neq i}}^{K}\overline{H}_{W_iW_j}(s_j)\\ &\quad\le r_i\sum_{r_j\neq r_i} r_j+\frac{p+1}{p}(v-1)r_i^2\\ &\quad\le r_i[(1-vr_i)+(1+1/p)(v-1)r_i]\\ &\quad= r_i[1-(1+1/p)r_i+vr_i/p]\\ &\quad= r_i[1-r_i+(v-1)r_i/p)]<r_i(1-r_i/p)\end{aligned}\tag{6.3}$$

□

Proposition 5: For a system of wobbling sequences of the form $W_{b,p^2,d}$ for a fixed d satisfying $1\le d\le p$, and all generators b satisfying $0<b<p$, the sum rate $R_{\rm sum}$ has a lower bound

$$R_{\rm sum}\ge\frac{dp^3-d(p-1)(dp+p-2)}{p^4}.\tag{6.4}$$

Proof: There are a total of p users in the system with a common period of p^4. For a user using a nonzero generator, the number of collisions in a period of p^4 slots with another user who is also using a nonzero generator, is bounded above by $d(d+1)$ according to Theorem 4. There are $(p-2)$ such other users. On the other hand, there is one user using the generator zero. The number of collisions with this user is d^2. Hence, the number of successful transmission for one of the $p-1$ users using a nonzero generator is bounded below by

$$dp^2-d(d+1)(p-2)-d^2.\tag{6.5}$$

For a user using the generator zero, the number of successful transmission is bounded below by

$$dp^2-d^2(p-1).\tag{6.6}$$

The proposition then follows from combining these lower bounds. □

We can now compare the performance of the wobbling sequences with the protocol sequences proposed in [2], [3], [5] with regard to the criterions stated previously.

Given any number of active users M with duty factors $p_i=q_i/q, \sum_{i=1}^{M}p_i=1$, the protocol sequences proposed by Massey and Mathys have a common period of $N=q^M$, which is of exponential growth in M. The sum rate is given by

$$\sum_{i=1}^{M}p_i\prod_{j\neq i}(1-p_j).\tag{6.7}$$

If $p_i=1/M$ and M tends to infinity, then the sum rate tends to $1/e$. The un-suppressibility property holds for this scheme and multirate protocols can be supported. However, the protocol sequences are dependent on the duty factor vector $(p_1,\ldots,p_M)$. The sequences can solve the identification problem without extra overhead; however, to find the packet location, a user has to send out initialization packets in the initial transmission periods [2].

Constant-weight cyclically permutable codes are used in [3], [5] which are constructed by means of linear cyclic codes over GF(p) (with p a prime) and a clever application of the Chinese Remainder Theorem correspondence. Performance of such sequences depends on the linear cyclic codes used and is complicated to analyze. However, some estimates based on Reed–Solomon (RS) or Bose–Chaudhuri–Hocquenghem (BCH) codes are presented in [5]. Recall that the quadruple (T,M,N,σ) captures the key performance characteristics of such protocol sequences. For the B* code constructed in [5]

$$\begin{aligned}T&=p^{(k-2)s}\\ N&=p(p^s-1)\\ w&=p^s-1\\ M&=\min\left\{T,\left\lfloor\frac{w-1}{w-d_c/2}\right\rfloor,\left\lfloor\frac{w-\sigma}{w-d_c/2}\right\rfloor+1\right\}\\ d_c&\ge 2(p^s-1-(k-1)p^{s-1}).\end{aligned}\tag{6.8}$$

Here, $1\le s,\ 3\le k<p-1$ are code parameters, w is the Hamming weight, and d_c is the cyclic minimum distance, which is defined to be the minimum Hamming distance from a codeword to its cyclic shifts or to cyclic shifts of another codeword [5]. To guarantee un-suppressibility, it follows from (6.8) that the number of active users that can be supported is

$$M=\left\lfloor\frac{w-1}{w-d_c/2}\right\rfloor+1\ge\left\lfloor\frac{p^s-2}{(k-1)p^{s-1}}\right\rfloor+1.\tag{6.9}$$

For large p, the lower bound is roughly equal to $\lceil p/(k-1)\rceil$. If one uses this as an estimate of the number of active users, then at most $\lceil p/2\rceil$ users can be supported, since $k\ge 3$. In this case, the sum of the duty factors of all the active users roughly equals $1/2$ only. Moreover, according to [5], for large p, the lower bound for the sum rate is

$$R_{\rm sum}\approx\frac{1}{4(k-1)}.\tag{6.10}$$

Multirate sequence is not supported by this approach. However, there is no additional overhead for handling the identification problem or the packet location problem.

For wobbling sequences, there are p sequences with a period p^4 and a duty factor d/p^2, $p-1$ sequences with a period p^8 and a duty factor d/p^4. For the case $d=p$, that is, if $\boldsymbol{F}_p(p)$ is used as the protocol sequence set, then as long as the total sum of duty factors does not exceed 1, then over a common period, say N slots, Theorem 6 guarantees that for any user with duty factor r_i, the user can transmit at least

$$Nr_i^2/p\tag{6.11}$$

packets that will not be blocked by other users. Hence, the un-suppressibility property can be guaranteed as long as (6.0) holds. In particular, if one uses only wobbling sequences of the form $W_{b,p^2,p}$, then there are p distinct sequences to support p active users, so that $M=p$ and the period $N=p^4$ is polynomial in M unlike the sequences of Massey and Mathys. Moreover, p unblocked slots can be guaranteed once every cycle of p^4 slots. Unlike the constant-weight cyclically permutable code approach, multirate users can be supported by

using wobbling sequences and the sequence formulations are independent of the duty factors of other users.

On the other hand, a drawback of the wobbling sequences is that overheads are needed for solving the identification problem and the packet location problem. One can deduce from Proposition 2 that the autocorrelation function for linear congruence sequences is not strong enough to uniquely identifying a sequence when other users are also transmitting. This holds true for wobbling sequences. One simple approach to address the identification and the packet location problem is to require a user to precede the payload data transmission with initialization packets at the first transmission period. This approach is similar to the approach taken in [2] to solve the packet location problem. Each initialization packet in the first transmission period for that user should contain a user identity, a key generator, a packet sequence number, and duty factor information. This information packet is sent repeatedly during the first transmission period according to the protocol sequence assigned to the user. With the un-suppressibility condition being satisfied, a receiver is guaranteed to receive at least one uncorrupted initialization packet from this user. The duty factor information then enables the receiver to identify the period of the sequence used by this particular user. With the other information provided, the receiver is able to uniquely identify transmissions in subsequent periods from this user even if those packets no longer contain any identity information. (If other users start to transmit at subsequent periods, more packets may become corrupted, but these events are detectable by the receiver.) To decode the payload information, packets from each period are grouped together; corrupted packets from a user in the same period can be treated as "erasures." Coding and decoding can then follow the approach described in [2] provided a minimum number of uncorrupted packets from a user can be guaranteed.

If the transmissions from users are sporadic and do not last over many sequence periods, then a second approach is to require the identity information be contained in each packet. This is suitable if the maximum number of active users and the maximum sequence numbers are relatively small in comparison to the data payload. As radio transmission technology improves, even for RFID systems, which are considered to be extremely low data rate, the popular EPC Class-1 Generation-2 standard specifies that the number of bits in a burst can range from 32 to 528 bits, with 16 protocol control bits [27]. If the identity overhead requires only a few additional bits, this second approach may not cause a heavy burden on system performance.

To obtain a protocol sequence with good sum rate performance, one can consider a system consisting of all wobbling sequences of the form $W_{b,p^2,d}$ for a fixed d. If $p>2$ is a prime then it follows that for $d=(p+1)/2$, a lower bound of the sum rate is

$$R_{\text{sum}} \geq \frac{(p+1)(p^3-2p^2+7p-4)}{4p^4}. \tag{6.12}$$

As p approaches infinity, the lower bound approaches $1/4$. This is lower than the theoretical limit of $1/e$ that can be achieved by the sequences of Massey and Mathys. However, it is higher than the lower bound in (6.10). Note that this is a lower bound only; the actual throughput could be higher.

For illustration, consider the case $p=3$ and $d=2$, the maximum cross correlation between $W_{0,9,2}$ and $W_{1,9,2}$ is 4. The maximum cross correlation between $W_{0,9,2}$ and $W_{2,9,2}$ is 4. The maximum cross correlation between $W_{1,9,2}$ and $W_{2,9,2}$ is 6. Hence, there are at least 26 successful transmissions, yielding a lower sum rate bound of $26/81$ as predicted by (6.12). By simulation, the actual minimum throughput of the system is indeed 26.

If one increases d to 3, then according to the lower bound (6.4), there sum rate is at least 7/27, which is lower than the $d=2$ case. Simulation shows that the actual minimum throughput is $29/81$ and is higher than the $d=2$ case. In comparison, according to [3] and [5], the minimum sum rate achieved using RS or BCH is $3/26$. Of course, in these cases, there are no identity overheads.

VII. Conclusion

Building on the idea of prime sequences, a new class of binary sequences with desirable cross-correlation properties is introduced. The wobbling sequences are shown to be suitable candidates for serving as protocol sequences. The performance characteristics of wobbling sequence are quite different from other traditional protocol sequences. Hence, they can offer alternative design options for MAC protocols, in particular for applications to sensor networks or RFID systems. The approach introduced here may also lead to constructions of other binary sequence families with interesting cross-correlation properties.

Appendix A

Proof of Proposition 1: It is easy to check that for all t

$$\begin{aligned} I_S(t+l) &= (t+l)l+(t+l)b-\left\lfloor\frac{(t+l)b}{l}\right\rfloor l \\ &= tl+tb-\left\lfloor\frac{tb}{l}\right\rfloor l+l^2 \\ &= I_S(t)+l^2. \end{aligned} \tag{A0}$$

Hence, l^2 is a period of the $(b,\ l)$ sequence and its minimum period N divides l^2. It also follows that the duty factor of the sequence is $1/l$. Now assume that b and l are relatively prime. Suppose that M is a solution to (3.1) for the minimum period N. From Lemma 1, it follows that

$$N=Ml. \tag{A1}$$

Moreover, for all nonnegative integers t

$$\begin{aligned} &(t+M)l+(t+M)b-\left\lfloor\frac{(t+M)b}{l}\right\rfloor l \\ &\qquad = tl+tb-\left\lfloor\frac{tb}{l}\right\rfloor l+N. \end{aligned} \tag{A2}$$

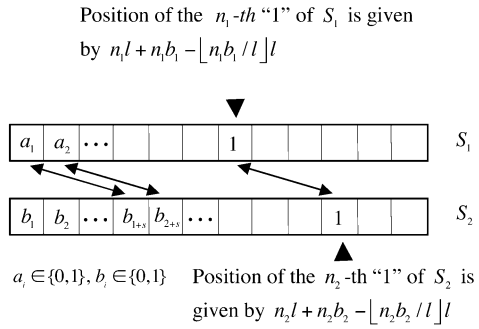

Fig. 1. Computation of $l^2 \bar{H}_{S_1 S_2}(s)$.

Hence, by choosing t to be l, it follows that

$$Mb - \left\lfloor \frac{Mb}{l} \right\rfloor l = N - Ml = 0. \tag{A3}$$

This equality holds only if l divides Mb. Since b and l are relatively prime, it follows that M is a multiple of l. In particular, it is easy to check that $M = l$ indeed provides a solution to (3.1) with

$$N = l^2. \tag{A4}$$

Hence, l^2 is the minimum period. □

Appendix B

Proof of Theorem 1: One can show that $l^2 \overline{H}_{S_1 S_2}(s)$ is equal to the number of distinct solutions of the form (n_1, n_2), with $0 \le n_1 < l$, to the equation

$$n_2 l + n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l} \right\rfloor l = n_1 l + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l} \right\rfloor l + s. \tag{B0}$$

It also follows from (B0) or from Fig. 1 that if there is a solution to (B0) of the form (n_1, n_2), with $n_1 \ge 0$, then $n_2 \ge 0$. Represent s in the form $c_1 l + c_0$ with $0 \le c_0 < l, 0 \le c_1 < l$. Then one can rewrite (B0) as

$$(n_2 - n_1 - c_1) l = n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l} \right\rfloor l + c_0 - n_2 b_2 + \left\lfloor \frac{n_2 b_2}{l} \right\rfloor l. \tag{B1}$$

By the definition of c_0 and the definition of $\lfloor \cdot \rfloor$, the following inequality holds:

$$-l + 1 \le n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l} \right\rfloor l + c_0 - n_2 b_2 + \left\lfloor \frac{n_2 b_2}{l} \right\rfloor l < 2l - 1. \tag{B2}$$

Hence, a solution to (B1) must satisfy

$$n_2 = \begin{cases} n_1 + c_1 & \text{or} \\ n_1 + c_1 + 1. \end{cases} \tag{B3}$$

Assume the first case and set

$$\begin{cases} n_1 = n \\ n_2 = n + c_1 \end{cases} \tag{B4}$$

with $0 \le n < l$. Then (B1) is reduced to

$$n(b_1 - b_2) \equiv -c_0 + c_1 b_2 \pmod{l}. \tag{B5}$$

Since $\mathrm{HCF}(|b_2 - b_1|, l) = 1$ and $b_1 \ne b_2$, there is one and only one solution to (B5), n^*, with $0 \le n^* < l$. (See, for example, [26].) Let

$$\begin{aligned} r_1 &\equiv n^* b_1 \pmod{l} \\ r_2 &\equiv n^* b_2 + c_1 b_2 \pmod{l} \end{aligned} \tag{B6}$$

with $0 \le r_1 < l,\ 0 \le r_2 < l$. From (B5) it follows that

$$r_2 \equiv c_0 + r_1 \pmod{l}. \tag{B7}$$

However, for a solution to (B1), the following equality must hold:

$$r_2 = c_0 + r_1. \tag{B8}$$

So, (B8) is satisfied by n^* if and only if

$$c_0 + r_1 < l. \tag{B9}$$

Now consider the second case of (B3) holds. It follows that a solution to (B1) satisfies

$$n_2 = n_1 + c_1 + 1. \tag{B10}$$

For clarity in argument, denote n_1 by m, $0 \le m < l$. Then, (B1) becomes

$$l = m b_1 - \left\lfloor \frac{m b_1}{l} \right\rfloor l + c_0 - (m + c_1 + 1) b_2 + \left\lfloor \frac{(m + c_1 + 1) b_2}{l} \right\rfloor l. \tag{B11}$$

Hence

$$m(b_1 - b_2) \equiv -c_0 + (c_1 + 1) b_2 \pmod{l}. \tag{B12}$$

Since $\mathrm{HCF}(|b_2 - b_1|, l) = 1$ and $b_1 \ne b_2$, there is one and only one solution to (B12), m^*, with $0 \le m^* < l$. Let

$$\begin{aligned} q_1 &\equiv m^* b_1 \pmod{l} \\ q_2 &\equiv m^* b_2 + (c_1 + 1) b_2 \pmod{l}. \end{aligned} \tag{B.13}$$

with $0 \le q_1, q_2 < l$. Then, m^* is a solution to (B11) if and only if

$$l = q_1 + c_0 - q_2 \tag{B14}$$

and the latter equation holds if and only if

$$c_0 + q_1 \ge l. \tag{B15}$$

In summary, (B0) has two solutions (n_1, n_2) with $0 \le n_1 < l$ if both of the following inequalities hold:

$$\begin{cases} c_0 + r_1 < l \\ c_0 + q_1 \ge l \end{cases} \tag{B16}$$

where

$$\begin{cases} r_1 \equiv n^* b_1 \pmod{l} \\ n^*(b_1 - b_2) \equiv -c_0 + c_1 b_2 \pmod{l}, \quad 0 \le n^* < l; \end{cases} \tag{B17}$$

and

$$\begin{cases} q_1 \equiv m^* b_1 \pmod{l} \\ m^*(b_1 - b_2) \equiv -c_0 + (c_1 + 1) b_2 \pmod{l}, \quad 0 \le m^* < l. \end{cases} \tag{B18}$$

There is only one solution if only one of the two inequalities in (B16) holds. There is no solution if none of the two inequalities holds. Hence

$$\overline{H}_{S_1S_2}(s) \le 2/l^2. \tag{B19}$$

To complete the proof of the theorem note that if $b_1 = 0$ or $b_2 = 0$, then

$$r_1 = q_1. \tag{B20}$$

Therefore, exactly one equation in (B16) holds. □

Appendix C

Proof of Proposition 3: Let $n(c_0, i)$, for $0 \le i < l$, be the solution satisfying $0 \le n(c_0, i) < l - 1$ and

$$n(c_0, i)(b_1 - b_2) \equiv -c_0 + ib_2 \pmod{l}. \tag{C0}$$

Similarly, define $m(c_0, i)$ to be the solution satisfying $0 \le m(c_0, i) < l - 1$ and

$$m(c_0, i)(b_1 - b_2) \equiv -c_0 + (i+1)b_2 \pmod{l}. \tag{C1}$$

Hence

$$\begin{aligned} m(c_0,0) &= n(c_0,1),\ m(c_0,1) \\ &= n(c_0,2),\ \ldots,\ m(c_0,l-1) = n(c_0,0). \end{aligned} \tag{C2}$$

Let $r_1(c_0, i)$ and $q_1(c_0, i)$ be nonnegative integers less than l satisfying

$$\begin{aligned} r_1(c_0,i) &\equiv n(c_0,i)b_1 \pmod{l}, \quad q_1(c_0,i) \\ &\equiv m(c_0,i)b_1 \pmod{l}. \end{aligned} \tag{C3}$$

Then

$$\begin{aligned} q_1(c_0,0) &= r_1(c_0,1),\ q_1(c_0,1) \\ &= r_1(c_0,2),\ \ldots,\ q_1(c_0,l-1) = r_1(c_0,0). \end{aligned} \tag{C4}$$

If $N(c_0, c_1)$ represents the total number of distinct solutions to (B16)–(B18) for the shift $s = c_0 + c_1 l$, then for $1 \le d < l - 1$, $\sum_{i=0}^{d-1} N(c_0, i)$ is equal to the number of inequalities that are satisfied in the following system:

$$\begin{aligned} &r_1(c_0,0) + c_0 < l, \quad q_1(c_0,0) + c_0 \ge l; \\ &r_1(c_0,1) + c_0 < l, \quad q_1(c_0,1) + c_0 \ge l; \\ &\qquad\vdots \\ &r_1(c_0,d-1) + c_0 < l, \quad q_1(c_0,d-1) + c_0 \ge l. \end{aligned} \tag{C5}$$

Due to (C4), $\sum_{i=0}^{d-1} N(c_0, i)$ is at least equal to $d-1$ with the possibility of upward adjustments from the "boundary terms": $r_1(c_0, 0)$ (adding 1 if the corresponding inequality holds) and $q_1(c_0, d-1)$ (adding 1 if the corresponding inequality holds.) Hence

$$d - 1 \le \sum_{i=0}^{d-1} N(c_0, i) \le d + 1. \tag{C6}$$

For $d = l$, $r_1(c_0, 0) = q_1(c_0, l-1)$ so exactly one of the two corresponding inequalities is valid, so

$$\sum_{i=0}^{l-1} N(c_0, i) = l. \tag{C7}$$

□

Appendix D

Proof of Theorem 2: If $b_1 = 0$ or $b_2 = 0$ then $k = 0$ and the result follows from Theorem 1. So assume $b_1 > 0$ and $b_2 > 0$. Let $b_1 = a_1 p^{j_1} < l = p^i$, $b_2 = a_2 p^{j_2} < p^i$, so that $\mathrm{HCF}(a_1, p) = 1$ and $\mathrm{HCF}(a_2, p) = 1$. Since $\mathrm{HCF}(b_2 - b_1, p) = 1$, it follows that $j_1 j_2 = 0$ and

$$j_1 + j_2 < i. \tag{D0}$$

Define $j = j_1 + j_2$. To prove (4.14), let α, satisfying the condition $0 \le \alpha < l - 1$, be the solution to

$$\alpha(b_1 - b_2) \equiv b_2 \pmod{l}. \tag{D1}$$

One can show that α is of the form $\alpha = \alpha_0 p^{j_2}$, with $(\alpha_0, p) = 1$, so that

$$\alpha_0(b_1 - b_2) \equiv a_2 \pmod{p^{i-j_2}}. \tag{D2}$$

It follows that $0 \le \alpha_0 < p^{i-j_2}$. Let $n(c_0, i)$, for $0 \le c_1 < l$, be the solution satisfying $0 \le n(c_0, c_1) < l - 1$ and

$$n(c_0, c_1)(b_1 - b_2) \equiv -c_0 + c_1 b_2 \pmod{l}. \tag{D3}$$

Let $r_1(c_0, c_1)$ be a nonnegative integer less than l satisfying

$$r_1(c_0, c_1) \equiv n(c_0, c_1)b_1 \pmod{l}. \tag{D4}$$

Denote $n(c_0, 0)$ by n_0, then

$$\begin{aligned} (n_0 + c_1\alpha)(b_1 - b_2) &\equiv -c_0 + c_1\alpha(b_1 - b_2) \\ &\equiv -c_0 + c_1 b_2 \pmod{l}. \end{aligned} \tag{D5}$$

Hence

$$(n_0 + c_1\alpha - n(c_0, c_1))(b_1 - b_2) \equiv 0 \pmod{l}. \tag{D6}$$

Since $|b_1 - b_2|$ and p are relatively prime, this implies

$$\begin{aligned} n(c_0, c_1) &\equiv n_0 + c_1\alpha \equiv n_0 + c_1\alpha_0 p^{j_2} \pmod{l} \\ r_1(c_0, c_1) &\equiv a_1 n_0 p^{j_1} + c_1 a_1 \alpha_0 p^{j} \pmod{l}. \end{aligned} \tag{D7}$$

Since $(a_1\alpha_0, p) = 1$, as c_1 cycles from 0 to $l-1$, $r_1(c_0, c_1)$ cycles through p^{i-j} distinct modulus l equivalent classes. One can view this as a sequence of state transitions. Call this the transition sequence for c_0. Moreover, at each step c_1, whenever $r_1(c_0, c_1)$ crosses $l-c_0$, that is, whenever the following inequalities hold simultaneously:

$$\begin{aligned} r_1(c_0, c_1) &< l - c_0 \\ r_1(c_0, c_1 + 1) &\geq l - c_0 \end{aligned} \tag{D.8}$$

the cross-correlation function at the corresponding shift $c_1 l + c_0$ is equal to $2/l^2$. Label such a transition a 2-transition. We want to count the number of 2-transitions as c_0 and c_1 cycle, respectively, from 0 to $l-1$, because this yields the total number of instances where the cross-correlation function is equal to $2/l^2$.

Since $j_1 j_2 = 0$, consider first the case $j_2 = 0$. In this case

$$r_1(c_0, c_1) \equiv (a_1 n_0 + c_1 a_1 \alpha_0) p^{j_1} \pmod{l}. \tag{D9}$$

For any fixed c_0 as c_1 cycles from 0 to $l-1$, the state sequence cycles through values from 0 to $(p^{i-j_1} - 1)p^{j_1}$ in some order, repeating p^{j_1} times. Note that changing the value of c_0 only affects the starting point of the cycle sequence. Note also that at a 2-transition

$$r_1(c_0, c_1 + 1) > r_1(c_0, c_1). \tag{D10}$$

This implies that

$$\begin{aligned} r_1(c_0, c_1 + 1) &= r_1(c_0, c_1) + \left[a_1 \alpha_0 p^{j_1}\right]_l \\ &= r_1(c_0, c_1) + [b_1 \alpha]_l. \end{aligned} \tag{D11}$$

Here, the notation $[x]_l$ represents the value between 0 and $l-1$ that is $(\mathrm{mod}\ l)$-equivalent to x. Note that from (D1)

$$b_1 \alpha (b_1 - b_2) \equiv b_1 b_2 \pmod{l}. \tag{D12}$$

Hence

$$[b_2 \alpha]_l = k. \tag{D13}$$

It follows from (D11) that there is no 2-transition if

$$r_1(c_0, c_1) \geq l - k. \tag{D14}$$

Consider now transition states satisfying $r_1(c_0, c_1) < l - k$. Represent such a state as x. There are totally $(l-k)/p^{j_1}$ such states, each being visited p^{j_1} times as c_1 cycles from 0 to $l-1$. Consider a transition jumping from x to $x+k$. For different c_0, such a transition occurs at different value of c_1, but nevertheless it will occur. It is not easy to characterize exactly at what value of c_0 and c_1 that such a transition is a 2-transition. It is, however, relatively easy to count the number of 2-transitions as c_0 ranges from 0 to $l-1$. To do so, we want to count the number of cases where such a transition from x to $x+k$ crosses the threshold $l - c_0$ in the sense defined by (D8) as c_0 varies. To satisfy (D8), the threshold value must lie in the interval $[x+1,\ x+k]$. So the number of 2-transitions affiliated with x as c_0 varies is equal to the length of the jump, that is, k. Summing over all the possible states of x, $((l-k)/p^{j_1})$ and counting their multiplicity of occurrences (p^{j_1}), one obtains the total number of 2-tranisions as

$$\frac{(l-k)}{p^{j_1}} p^{j_1} k = (l-k)k. \tag{D15}$$

One can show that the same result occurs for the case $j_1 = 0$ by using similar but slightly modified arguments. Hence, the number of shifts such that $\overline{H}_{S_1 S_2}(s) = 2/l^2$ is $(l-k)k$. By Lemma 2

$$\sum_{s=0}^{l^2-1} \overline{H}_{S_1 S_2}(s) = 1. \tag{D16}$$

So the number of shifts with $\bar{H}_{S_1 S_2}(s) = 1/l^2$ is equal to

$$\left(1 - \frac{2(l-k)k}{l^2}\right) l^2 = l^2 + 2k^2 - 2kl. \tag{D17}$$

The rest of the theorem then follows. □

Appendix E

Proof of Lemma 3: Consider a fixed shift value s which can be represented as

$$tl_2 + u \tag{E0}$$

with $0 \leq u < l_2,\ 0 \leq t < q$. For any fixed integer p_1, satisfying $0 \leq p_1 < l_2$, and any integer p_2, satisfying $0 \leq p_2 < q/l_2$, we want to construct an explicit solution to (4.17) parameterized by $(p_1,\ p_2)$.

Let k denote the unique integer satisfying $0 \leq p_1 < l_2$ and the equation

$$k b_2 \equiv \begin{cases} p_1 - t b_2 & (\mathrm{mod}\ l_2) \quad \text{if } p_1 \geq u, \\ p_1 - (t+1) b_2 & (\mathrm{mod}\ l_2) \quad \text{otherwise.} \end{cases} \tag{E1}$$

Define an integer j by

$$j = \begin{cases} p_1 - u, & \text{if } p_1 \geq u \\ p_1 - u + l_2, & \text{otherwise.} \end{cases} \tag{E2}$$

Note that $0 \leq j < l_2$. Since b_1 is relatively prime to l_1, there exists a unique integer n_1 such that $0 \leq n_1 < l_1$ and

$$n_1 b_1 = j + k l_2 + p_2 l_2^2 \pmod{l_1}. \tag{E3}$$

Since

$$\begin{aligned} j + k l_2 + p_2 l_2^2 &\leq l_2 - 1 + (l_2 - 1) l_2 + (q/l_2 - 1) l_2^2 \\ &= l_2 - 1 + (l_2 - 1) l_2 - l_2^2 + q l_2 = l_1 - 1 \end{aligned} \tag{E4}$$

it follows that

$$n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 = j + k l_2 + p_2 l_2^2. \tag{E5}$$

Let

$$n_2 = \begin{cases} n_1 q + k + t + p_2 l_2, & \text{if } p_1 \geq u \\ n_1 q + k + t + 1 + p_2 l_2, & \text{otherwise.} \end{cases} \tag{E6}$$

If $p_1 \geq u$, then by combining (E6) with (E1), one can show that

$$n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l_2} \right\rfloor l_2 = (k+t)b_2 - \left\lfloor \frac{(k+t)b_2}{l_2} \right\rfloor l_2 = p_1 - \left\lfloor \frac{p_1}{l_2} \right\rfloor l_2 = p_1. \tag{E7}$$

Hence

$$\begin{aligned} & n_2 l_2 + n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l_2} \right\rfloor l_2 \\ &= (n_1 q + k + t + p_2 l_2) l_2 + p_1 \\ &= n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + t l_2 + p_1 - j \\ &= n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + s. \end{aligned} \tag{E8}$$

This provides a solution to (4.17). Similarly, if $p_1 < u$, one can show that

$$n_2 b_2 = p_1. \tag{E.9}$$

Moreover

$$\begin{aligned} & n_2 l_2 + n_2 b_2 - \left\lfloor \frac{n_2 b_2}{l_2} \right\rfloor l_2 \\ &= (n_1 q + k + t + 1 + p_2 l_2) l_2 + p_1 \\ &= n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + t l_2 + p_1 - j + l_2 \\ &= n_1 l_1 + n_1 b_1 - \left\lfloor \frac{n_1 b_1}{l_1} \right\rfloor l_1 + s. \end{aligned} \tag{E10}$$

Therefore, this also provides a solution to (4.17).

Note that there are l_2 possible values for p_1 (and hence, l_2 possible values for k) and q/l_2 possible values for p_2. For each distinct (p_1, p_2) pair, the corresponding (n_1, n_2) solutions are distinct. Hence, for any fixed s, there are at least q solutions to (4.17) with $0 \leq n_1 < l_1$. □

ACKNOWLEDGMENT

The author would like to thank Chung Shue Chen for his help in performing the numerical simulations reported in this paper and the reviewers for their detailed and insightful comments.

REFERENCES

[1] J. L. Massey, "The capacity of the collision channel without feedback," in *Abstracts of Papers, IEEE Int. Symp. Information Theory*, 1982, p. 101.

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

[3] Q. A. Nguyen, L. Györfi, and J. L. Massey, "Constructions of binary constant-weight cyclic codes and cyclically permutable codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 940–949, May 1992.

[4] J. Y. N. Hui, "Multiple accessing for the collision channel without feedback," *IEEE J. Sel. Aareas Commun.*, vol. SAC-2, no. 4, pp. 575–582, Jul. 1984.

[5] L. Györfi and I. Vajda, "Construction of protocol sequences for multiple-access collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1762–1765, Sep. 1992.

[6] G. Thomas, "Capacity of the wireless packet collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 1141–1144, May 2000.

[7] V. C. da Rocha, Jr., "Protocol sequences for collision channel without feedback," *IEE Electron. Lett.*, vol. 36, no. 24, pp. 2010–2012, 2000.

[8] J. M. Rabaey, M. J. Ammer, J. L. de Silva, Jr., D. Patel, and S. Roundy, "Pico radio supports ad hoc ultra-low power wireless networking," in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mobile Computing and Networking*, Seattle, WA, 1999, pp. 271–278.

[9] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Pers. Commun.*, vol. 7, no. 5, pp. 16–27, Oct. 2000.

[10] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *Proc. ASPLOS 2000*, Cambridge, MA, 2000, pp. 93–104.

[11] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *Mobile Comp. Commun. Rev.*, vol. 6, no. 2, pp. 28–36, 2002.

[12] 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, 1983.

[13] P. R. Prucnal, M. A. Santoro, and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing," *IEEE/OSA J. Lightwave Technol.*, vol. 4, no. 5, pp. 547–554, May 1986.

[14] 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.

[15] W. C. Kwong, P. A. Perrier, and P. R. Prucnal, "Performance comparison of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area networks," *IEEE Trans. Commun.*, vol. 39, no. 11, pp. 1625–1634, Nov. 1991.

[16] S. V. Maric, Z. I. Kostić, and E. L. Titlebaum, "A new family of optical code sequences for use in spread-spectrum fiber-optic local area networks," *IEEE Trans. Commun.*, vol. 41, no. 8, pp. 1217–1221, Aug. 1993.

[17] A. A. Shaar, M. Gharib, and P. A. Davies, "Collision resolution in contention access local area networks using concatenated prime sequences," *IEE Proc.—Commun.*, vol. 149, no. 5, pp. 249–256, 2002.

[18] G.-C. Yang and W. C. Kwong, *Prime Codes with Applications to CDMA Optical and Wireless Networks*. Boston, MA: Artech House, 2002.

[19] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Std. 802.11, IEEE, 1999.

[20] B. Hajek, "Extremal splitting of point process," *Math. Oper. Res.*, vol. 10, no. 4, 1985.

[21] C. S. Chen and W. S. Wong, "Bandwidth allocation for wireless multimedia systems with most regular sequences," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 635–645, Mar. 2005.

[22] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. New York: Research Studies /Wiley, 1996.

[23] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.

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

[25] C. S. Chen, "Resource Management in Wireless Multimedia Systems," Ph.D. dissertation, Chinese University of Hong Kong, Shatin, 2005.

[26] M. B. Nathanson, *Elementary Methods in Number Theory*. New York: Springer, 2000.

[27] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9 EPCGlobal Inc., Jan. 2005 [Online]. Available: http://www.epcglobalinc.org/standards/