OPTIMUM PN SEQUENCES FOR CDMA SYSTEMS

DILIP V. SARWATE
Coordinated Science Laboratory
and the Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801 USA

Abstract — Most known methods for the design of hopping patterns for frequency-hopped code-division multiple-access (CDMA) systems and for the design of signature sequences for direct-sequence CDMA systems provide sequences that can be viewed as codewords (or the images of codewords) from low-rate Reed-Solomon codes. This paper surveys sequence designs for CDMA systems from this viewpoint.

I. Introduction

Code-division multiple-access (CDMA) systems can be classified as frequency-hopped CDMA systems (FH/CDMA) or direct-sequence (DS/CDMA) systems [3, 27, 33]. As the adjective code-division implies, a CDMA system allows several transmitters to share the available bandwidth by the use of different codes which are used to distinguish the signals at the receiver. In an FH/CDMA system, a transmitter changes (hops) its RF carrier frequency at regular intervals as prescribed by a frequency-hopping pattern. Careful choice of the frequency-hopping patterns assigned to the transmitters allows the system designer to arrange matters so that the signals from two different transmitters hop to the same frequency only very infrequently. In contrast, a DS/CDMA transmitter phase-shift-keys its RF carrier with a signature sequence with very high pulse rate. Careful choice of the signature sequences assigned to the transmitters allows the system designer to arrange matters so that the signals from different transmitters interfere very little with each other in the receiver. The hopping patterns or signature sequences for CDMA systems are often referred to as pseudonoise (PN) sequences. This paper is a brief survey of various designs for such PN sequences from the viewpoint that most known design methods result in sequences that are codewords from low-rate Reed-Solomon codes, or the images of such codewords under some suitable linear mapping. Section II contains a brief survey of design methods for hopping patterns for FH/CDMA communication systems. Some of those methods explicitly use Reed-Solomon codes and the resulting frequency-hopping patterns are codewords from low-rate Reed-Solomon codes. Other methods were originally described using different terminology but the resulting frequency-hopping patterns also can be viewed as codewords from low-rate Reed-Solomon codes. Section III shows that several well-known signature sequence sets for DS/CDMA communications (such as the Gold sequences and Kasami sequences [23]) also can be viewed in terms of codewords from low-rate Reed-Solomon codes. However, there seems to be no apparent connection between the properties of the Reed-Solomon codes and the resulting signature sequences, and viewing the signature sequences as Reed-Solomon codewords provides no new insights into possible new or improved designs.

II. Frequency-Hopped Spread-Spectrum Systems

IIA. Properties of Frequency-Hopping Patterns

Let $q$ denote the number of frequency slots in a FH/CDMA system, and let $f_i$ denote the center frequency of the $i$-th slot,
frequency-hopping patterns for FH/CDMA systems operating in jamming or fading environments. If a signal visits one slot more often than others, then it is more vulnerable to jamming or fading in that slot. Of course, such a signal is less vulnerable in those slots that it visits less frequently, but clearly the maximum vulnerability is minimized if the slots are utilized as uniformly as possible. Uniform usage of slots also minimizes the average multiple-access interference from other transmitters.

When several FH/CDMA transmitters are simultaneously active, it often happens that two or more transmitters hop to the same frequency slot at the same time. This event is called a collision or hit and it usually causes such severe signal degradation that it is hard to detect collisions whenever possible, to delete the most severely degraded symbols, and then to reconstruct those deleted symbols by use of an erasure-and-error correcting channel code [1]. Collisions sometimes are be less of a problem in a fast FH/CDMA system in which a data symbol is transmitted over several dwell, than in a slow FH/CDMA system in which one or more data symbols is transmitted during a dwell. Note also that most FH/CDMA systems are not dwell-synchronous, that is, the relative delay between two signals need not be an integer multiple of the dwell duration. Thus, when the desired signal hops into a slot, a receiver tracking the signal may find that an interfering signal is already present in that slot, but that this interfering signal disappears before the end of the dwell interval. On the other hand, an interfering signal may suddenly appear during a dwell and last until the end of the dwell interval. Such partial hits can be accounted for quite easily if one knows the number of (full) collisions that occur for each given delay between the two patterns in a dwell-synchronous system. Full collisions are counted by the Hamming correlation function which is considered next.

II.B The Hamming Correlation Functions

Let $x$ and $y$ denote two frequency-hopping patterns with common period $N$. The number of hits that occur in one period of $x$ due to interference from $y$ is counted by the Hamming correlation function which was defined by Leupolz and Gehringer [10] as

$$ H_{x,y}(z) = \sum_{r \in Z} h(r, z) $$

where $h(r, z)$ is the relative delay between the two frequency-hopping patterns, the sum $r + j$ is taken modulo $N$, and

$$ h(r, z) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases} $$

Equivalently,

$$ H_{x,y}(z) = \sum_{r \in Z} h(r, z) $$

where $d(x, y)$ denotes the Hamming distance between the sequences $x$ and $y$. Naturally, one would like to have $x$ and $y$ such that $H_{x,y}(z)$ is as small as possible for all $z, 0 \leq z \leq N-1$. The Hamming autocorrelation function $H_{x}(z)$ for the hopping pattern $x$ is just $H_{x,x}(z)$ and has the obvious property that $H_{x}(z) = N$. One would like to choose $x$ such that the out-of-phase autocorrelation values $H_{x}(z), 0 \leq z < N$ are as small as possible. Such replicas may be received because of specular multipath propagation or because a repeat jammer is re-broadcasting the signal. The out-of-phase autocorrelation can also be used to estimate the likelihood of false lock in the initial acquisition and synchronization process that aligns the hopping pattern of the receiver's local oscillator with the received signal.

How small can the Hamming crosscorrelation and out-of-phase Hamming autocorrelation be? First, note that $0 \leq H_{x,y}(z) \leq N$ for all $z$. Let $H_{x,y}$ denote the average Hamming crosscorrelation value and $(, )$ denote the usual inner product of two vectors. Then,

$$ H_{x,y} = \sum_{z=0}^{N-1} H_{x,y}(z) = \sum_{r \in Z} N(z)N(y) = (N(x), N(y)) $$

Similarly, $H_{x}$, the average out-of-phase Hamming autocorrelation for the sequence $x$, is given by

$$ H_{x} = \sum_{z=0}^{N-1} H_{x}(z) = (N(x), N(x)) - N = N\langle x \rangle^{2} - N $$

If $N \leq q$, then (2), (4), and (9) lead to the trivial obvious conclusion that $H_{x} \geq 0$. Furthermore, $H_{x} = 0$ if and only if the hopping pattern satisfies (3), that is, if and only if each $N(x)$ is either 0 or 1. Such sequences are called nonrepeating hopping patterns because each frequency is used at most once in each period [28], and they are of interest for the purposes of initial acquisition and synchronization. Note that $H_{x} = 0$ implies that $H_{x,y} = 0$ for all $y$. More generally, (2) and (5) show that the right side of (9) is at least $N^{2}(q - N)$, and hence, for any sequence $x$,

$$ H_{x} \geq \frac{N}{N-1} \left( \frac{N}{q} - 1 \right) $$

The right side of (10) is nonpositive for $N \leq q$, and in this case, $H_{x} \geq 0$ as discussed above. On the other hand, if $N > q$, the right side of (10) exceeds $N/q - 1$. Since the Hamming correlation functions are integer-valued, it follows that for any sequence $x$,

$$ \max_{0 \leq z \leq N-1} H_{x}(z) \geq \frac{N}{q} - 1 $$

In comparison, for any $x$, $0 < j < N$, the expected value of $H_{x}(z)$, averaged over all possible $q^{N}$-N-tuples in the set $\{0, 1, \ldots, q-1\}^{N}$, is $N/q$. In other words, it is not possible to design hopping patterns whose autocorrelation values are significantly smaller than the average value for a randomly chosen hopping pattern.

Next, suppose that $x$ and $y$ are chosen randomly and independently from the set of $q^{N}$-N-tuples in the set $\{0, 1, \ldots, q-1\}^{N}$. Then, for all $x, 0 \leq z < N$, the expected value of $H_{x,y}(z)$ is $N/q$. Once again, it is not possible to do much better than this with nonrepeating designs except in a few special cases which essentially correspond to frequency-division multiple-access (FDMA) schemes. For applications to FH/CDMA systems, consider $x$, a set of $N$ hopping patterns of period $N$. From (8) it follows that

$$ \sum_{x \in X} \sum_{e \in X} \sum_{x' \in X} H_{x,e}(z) = \sum_{x \in X} \sum_{e \in X} \sum_{x' \in X} N(x')^{2} $$

Since

$$ \sum_{x \in X} N(x) \geq 0 \text{ for all } i, \text{ and } \sum_{x \in X} N(x) = KN $$

1 A more careful analysis leads to a more precise estimate for the right side of (10) but these results generally do not improve on the right side of (11). It is also worth noting that all these results can also be deduced by applying the well-known Plotkin upper bound on the average minimum distance of a block code [11] to a length $N$ $q$-ary block code whose codewords are $(e, T_{1}, \ldots, T_{N-1})$.  

\text{Since}
which is analogous to (1), it follows that the right side of (12) is smallest when

\[
\sum_{x \in X} N(x) = \left\lfloor \frac{KN}{q} \right\rfloor \quad \text{for } (KN \mod q) \text{ values of } i, \quad (13a)
\]

\[
\sum_{x \in X} N(x) = \left\lfloor \frac{KN}{q} \right\rfloor \quad \text{for } q - (KN \mod q) \text{ values of } i \quad (13b)
\]

Let \( R_i(x) \) and \( H_i(x) \) respectively denote the average and maximum values of \( H_i(x) \) over all \( K(K-1) \) pairs of distinct hopping patterns \( x \) and \( y \) in \( X \) and all \( j, 0 \leq j < N \). Similarly, let \( H_i(x) \) and \( H_i(x) \) respectively denote the average and maximum values of \( H_i(x) \) over all \( K \) patterns \( x \in X \) and all \( j, 0 \leq j < N \). Let \( \bar{R}_i(x) = \max(R_i(x), R_i(x)) \) and \( \bar{H}_i(x) = \max(H_i(x), H_i(x)) \). Then, it follows from (5) and (12) that

\[
\begin{align*}
K(K-1)N & H_i(x) + K(N-1)H_i(x) \\
& \geq K(K-1)N \bar{R}_i(x) + K(N-1)\bar{R}_i(x) \\
& = \sum_{x \in X} N(x)^2 - KN \geq \frac{KN^2}{q} - KN,
\end{align*}
\]

and hence, if \( KN > q \),

\[
\bar{H}_i(x) \geq \bar{R}_i(x) > \frac{N}{q} - \frac{1}{K},
\]

(15)

Thus, one or both of the maximum (and average) correlation values are bounded from below by a quantity which is almost the same as the expected value when random patterns are used.

The bound (15) on \( \bar{H}_i(x) \) is useful if \( N > q \). However, if \( N \) is no larger than \( q \), the bound is not only small but it hardly increases at all as \( K \) increases. In such instances, a large lower bound on \( \bar{H}_i(x) \) can be obtained as follows. Consider all the \( KN \) cyclic shifts of the hopping patterns in \( X \) as a q-ary nonlinear cyclic code of length \( N \). The Singleton bound on the minimum distance of this code [11] together with (7) implies that

\[
\bar{H}_i(x) \geq \log_q(KN) - 1.
\]

(16)

For example, according to (16), for a set of \( q^x \) hopping patterns of length \( N \leq q \), the maximum Hamming correlation value is at least \( q \). However, bound (16) increases only logarithmically with \( N \) whereas bound (15) increases linearly with \( N \), and thus the latter is tighter when applied to small sets of long hopping patterns.

Returning to (14), note that this can be written as

\[
\begin{align*}
H_i(x) & + \frac{1}{K-1}H_i(x) \\
& \geq \bar{R}_i(x) + \frac{1}{K-1}\bar{R}_i(x) \\
& \geq \frac{1}{K-1} \left( \frac{KN}{q} - 1 \right)
\end{align*}
\]

(17)

showing that there is a tradeoff between the maximum (or average) crosscorrelation and maximum (or average) autocorrelation values — if careful design of hopping patterns reduces one maximum (or average) correlation value substantially below \( N/q \), then the other maximum (or average) correlation value will be larger than \( N/q \). However, since different weights are attached to the quantities in (17), a set of patterns with very small maximum (or average) crosscorrelation will necessarily have large maximum (or average) autocorrelation but a set of patterns with very small maximum (or average) autocorrelation need not necessarily have very large maximum (or average) crosscorrelation value. As an example, it was shown above that if \( R_i(x) = 0 \) (which implies that \( H_i(x) = 0 \)), then \( H_i(x) \geq R_i(x) > KN/q - 1 \). In contrast, if \( H_i(x) = 0 \) (which implies that \( H_i(x) = 0 \) and all the patterns are nonrepeating), (17) shows that

\[
H_i(x) \geq \bar{R}_i(x) \geq \frac{N}{q} - \frac{1}{K-1} - 1
\]

where the right side is only slightly larger than the right side of (15).

1.2. Rules and Bursts

A hopping pattern of length \( N \) is said to contain a run of length \( r \) of the frequency \( f \) beginning at position \( j \), if

\[
(0, 0, 0, \ldots, f_{j-1}, f_j, f_{j+1}, \ldots, f_{j+r-1}, 0, 0, 0, \ldots) = (f_0, f_1, f_2, \ldots, f_L)
\]

where \( f_k \neq f \) and \( f_i \neq f \), and the subscribers on \( x \) are taken modulo \( N \). Long runs are undesirable for several reasons. First, the signal stays in the same slot for \( r \) successive dwells and thus is more vulnerable to that slot being jammed or in a deep fade. Second, long occupancy of a slot also makes the signal more vulnerable to interception by an unauthorized receiver. Finally, if long runs of the same frequency occur in two different patterns, then long bursts of full hits will occur whenever the relative delay is such that the runs arrive at the same time at a receiver. Although hits often can be detected and the corresponding symbols erased (and later restored by an error-and-erase correcting code), a burst of hits causes a large number of erasures in a short period of time, and this may well lead to a decoding failure in the error-control system. This is because the block length of the error-control code is usually much smaller than the length of the hopping patterns, and thus a code that can handle \( H \) hits scattered over \( N \) dwells may well fail if many of these \( H \) hits occur in a burst and affect symbols belonging to the same codeword.

Bursts of hits are caused not only by runs of the same frequency, but also by the occurrence of identical subsequences in two hopping patterns, that is, if \( (x_0, x_1, \ldots, x_{i-1}) = (y_0, y_1, \ldots, y_{i-1}) \), where, as before, the subscripts are taken modulo \( N \), then a burst of \( i \) hits occurs for a relative delay of \( (j-i) \) dwells. Generally, these hits become partial hits if the relative delay is \( (j-i+s) \) dwells unless the subsequences contain repetitions of the same frequency. Now, let \( B(X) \) denote the length of the longest burst of hits between any two hopping patterns in \( X \) and note that \( H(X) \geq B(X) \). The \( KN \) subsequences of the form \( (x_0, x_1, \ldots, x_{i+1}) \), \( x \in X \) cannot be all distinct if \( q < N \), and therefore bursts of length \( L \) must occur for all \( r \) satisfying this inequality. It follows that

\[
H_i(x) \geq B_i(x) \geq 2 \log_q(KN) - 1
\]

(18)

which not only provides a direct proof of (16) but also shows that one or more bursts of hits of length at least \( \log_q(KN) - 1 \) must occur.

1.2.2 The Design of Hopping Patterns using Reed-Solomon Codes

Hopping patterns were defined earlier as sequences of elements from the set \( \{f_0, f_1, \ldots, f_L-1\} \). However, it is not necessary that the elements of the set be the center frequencies of the slots. All the various properties of hopping patterns discussed above hold provided only that the set contains \( q \) distinct elements. In short, one can also regard a hopping pattern as a sequence of elements from some arbitrary set of \( q \) distinct elements, and the pattern can always be transformed into a sequence of frequencies by a suitable
one-to-one mapping from this set to \( \{f_0, f_1, \ldots, f_{q-1}\} \). This is the viewpoint that will be taken in the remainder of this section. In particular, hopping patterns will be viewed as sequences of elements from the finite field \( GF(q) = GF(p^d) \), where \( p \) denotes a prime. Thus, it should not be too surprising that Reed-Solomon codes over \( GF(q) \) are a source of excellent designs of hopping patterns. The concept is as follows.

Let \( N \) be a divisor of \( q - 1 \), and let \( \alpha \) denote a primitive \( N \)-th root of unity in \( GF(q) \). Let \( C(N,i+1:t) \) denote the cyclic \( (N,i+1) \) Reed-Solomon code over \( GF(q) \) with parity-check polynomial

\[
h(x) = \prod_{j=0}^{i} (x - \alpha^j),
\]

generator matrix

\[
G = \begin{bmatrix}
\alpha^0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{N-1} \\
\alpha^1 & \alpha^2 & \alpha^3 & \cdots & \alpha^{(N-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha^i & \alpha^{i+1} & \alpha^{i+2} & \cdots & \alpha^{i+(N-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha^{(q-1)} & \alpha^{(q-1)+1} & \cdots & \alpha^{(q-1)+(N-1)} \\
\end{bmatrix}, \tag{19}
\]

and minimum distance \( N - i \). Suppose that two cyclically inequivalent codewords \( x \) and \( y \) are chosen to be hopping patterns. Since the code is cyclic, \( T^y \) is a codeword for any \( j \). Furthermore, since the sequences are cyclically inequivalent, \( T^y \neq x \) for any \( j \). Hence, \( H_{\alpha}(y) = N - d(x,T^y) \leq t \). Similarly, if \( x \) is of period \( M \) where \( M \) is a divisor of \( N \), then \( H_{\alpha}(y) = N - d(x,T^y) \leq t \) for \( j \neq 0 \) and \( M \). Thus, hopping patterns can be constructed by choosing one codeword from each cyclic equivalence class. However, for reasons noted earlier, it is usually desirable to use only those patterns that have full period \( N \). Furthermore, since a pattern of period \( N \) may leave as many as \( q - N \) slots unused, this construction is usually applied only to Reed-Solomon codes of length \( q - 1 \). Interestingly, in the early seventies, the above idea was discussed by both Reed [20] and Solomon [28] in separate papers. Their solutions to the problems were somewhat different and these solutions are considered next.

II.E Reed's construction

In [20], Reed described a hopping patterns obtained by choosing one codeword from each cyclic equivalence class of the codewords belonging to the code \( C(q; 1, i+1; 0) \) with generator matrix

\[
G = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \alpha & \alpha^2 & \cdots & \alpha^{i-1} \\
1 & \alpha^2 & \alpha^3 & \cdots & \alpha^{i} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^{i-1} & \alpha^{i} & \cdots & \alpha^{(q-2)} \\
\end{bmatrix}, \tag{20}
\]

Note that \( \alpha \) is a primitive element of the field \( GF(q) \). The number of cyclic equivalence classes (i.e., the number of different hopping patterns) is given by \[ q - 1 \sum_{d \mid (q-1)} \phi(d)q^{1/d} \]

where \( \phi(d) \) is Euler's totient function. Of course, many of these equivalence classes contain codewords of periods less than \( q - 1 \) (referred to as nonprimitive codewords henceforth) and thus are usually not of interest. Reed also gave a lower bound on the number of hopping patterns of period \( q - 1 \) (these are primitive codewords) that can be obtained from this code. This bound is based on the following simple argument. If \( \alpha^i \) is a nonprimitive element of \( GF(q) \), then the \( i \)-th row \( (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(q-2)i}) \) of the generator matrix in (20) is a nonprimitive codeword. Suppose that \( q \) rows of \( G \) are nonprimitive codewords. The \( q' \)-linear combinations of these rows usually are nonprimitive codewords, but can be primitive codewords in some cases. On the other hand, nonzero linear combinations of the other \( q + 1 - q' \) rows are always primitive codewords. Since the sum of a primitive codeword and a nonprimitive codeword is a primitive codeword, it follows that there are at least \( q'^2 \) \( q' \)-primitive codewords in the code. Hence, the \( q' \)-th row of hopping patterns of period \( q - 1 \) obtained from \( C(q; 1, i+1; 0) \) contains at least \( q'^2 \) \( q' \)-primitive codewords. Furthermore, \( H_{\max}(x) = t \), and since \( KN = K(q - 1) < q'^4 \) (which implies that \( \log_q[KN] - 1 = t \), it follows that both (18) and (19) are satisfied with equality. In other words, these hopping patterns are optimal with respect to these bounds.

A detailed description of the construction of these hopping patterns has been published recently [20]. As a specific example of this construction process, consider \( C(q - 1, 1, 2; 0) \) whose generator matrix has rows \( (1, \alpha, \alpha^2, \ldots, \alpha^{q-2}) \) of period \( q - 1 \) and \( q - 1 \) respectively. Then, the \( q' \) hopping patterns are given by \( (B_1) \) when \( \beta \in GF(q) \). Put another way, let \( \beta_j, 0 \leq j \leq q - 1 \) denote the elements of \( GF(q) \). Then, the \( q' \) sequences obtained via Reed's construction can be expressed as

\[
x^{(j)} = (\beta_0, \beta_1, \ldots, \beta_j) + (1, \alpha, \alpha^2, \ldots, \alpha^{q-2}), \quad 0 \leq j \leq q - 1. \tag{21}
\]

Since the \( i \)-th element of the \( j \)-th sequence is

\[
x^{(j)}_i = \beta_j + \alpha^i, \quad 0 \leq i \leq q - 1, \quad 0 \leq j \leq q - 1, \tag{22}
\]

and since \( \alpha^i \neq 0 \), the element \( \beta_j \) does not occur in \( z^{(j)}_i \) while any other \( \beta_j \) occurs exactly once. Thus, these hopping patterns are nonrepeating and they also satisfy (13) with each element of \( GF(q) \) occurring a total of \( q - 1 \) times in the \( q' \) hopping patterns. Note also that for \( i \neq j \), \( \langle (x^{(j)}), (x^{(j')}) \rangle \approx q - 2 \) and that \( H_{\max}(x^{(j)}) \) has value 0 if \( i = 0 \) and value 1 otherwise.

Applying Reed's construction to \( C(q; 1, i+1, 1) \) where \( i \neq 0 \) sometimes provides minor improvements on the above results. If \( q = 2^3 \), Reed's construction applied to \( C(2^3, 1, 2; 0) \) provides \( 2^4 \) hopping patterns with \( H_{\max} = 1 \) as described by (21). In comparison, the construction provides \( 2^4 + 1 \) hopping patterns with \( H_{\max} = 2 \) when it is applied to \( C(2^4, 1, 2; 1) \). This is because both \( \alpha \) and \( \alpha^2 \) are primitive elements, and hence the codewords of the form \( (1,0) \) and \( (1,1) \) are cyclically inequivalent primitive codewords. Letting \( x \) and \( y \) denote the two rows of \( G \) and noting that \( T^x = \alpha^x \), this set of \( 2^4 + 1 \) hopping patterns can be expressed as

\[
\{x, y, x + y, T^x + y, T^x x + y, 2T^3 x + y, \ldots, 2^{2^3} x + y\}
\]

which is very similar to the representation of Gold sequences in Eq. (4.6) of [20]. Similarly, applying Reed's construction to \( C(2^9, 1, 3; 0) \) provides \( 2^{26} + 2^9 \) hopping patterns with \( H_{\max} = 2 \), whereas it provides \( 2^{26} + 2^9 + 1 \) hopping patterns with \( H_{\max} = 2 \) when it is applied to \( C(2^{10}, 1, 3, 1) \), where \( k \) is odd. More generally, if \( 2^k - 1 \) is a Mersenne prime, then all the rows of the generator matrix of \( C(2^k - 1, i+1; 1) \) are primitive codewords, and hence Reed's construction provides \( (2^{2k+1} - 1)/(2^k - 1) \) hopping patterns of period \( 2^k - 1 \) with \( H_{\max} = t \).

Although the hopping patterns obtained via Reed's construction are optimal with respect to the bounds (16) and (18), they
can have some undesirable properties when \( t > 1 \). For example, consider the \( q^t \) hopping patterns with \( H_{max} = 2 \) obtained from \( C(q - 1; 1,0) \) where \( q \) is assumed to be odd. It can be shown that some of the hopping patterns use only half of the available frequency slots, which is usually undesirable.

### II.F Solomon's Construction

In [28], Solomon considered the construction of hopping patterns based on cosets of Reed-Solomon codes. The code \( C(q-1;1,0) \) is a subcode of \( C(q-1;1,1;0) \), and hence the latter can be partitioned into \( q \) cosets of \( C(q-1;1,0) \). The coset representatives can be taken to be multiples of the last row of \( G \) in (20), i.e. \( \beta(1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(q-1)t}) \) where \( \beta \) is an element of \( GF(p) \). Now, cyclically shifting all the codewords in one such coset results in another such coset (usually distinct from the first.) Solomon suggested using the coset with representative \( (1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(q-1)t}) \) as a set of hopping patterns. Each coset contains \( q^t \) hopping patterns, and since these are all codewords in \( C(q-1;1,1;0) \), \( H_{max} = 1 \) for this set. In comparison, recall that Reed's set of hopping patterns also has \( H_{max} = 1 \) but contains at least \( q^t \) hopping patterns.

As an example of Solomon's construction technique, consider the repetition code \( C(q-1;1,0) \) which is a subcode of \( C(q-1,2,0) \). The codewords in the coset are all of the form

\[
(1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(q-1)t}) + (\beta,\beta,\ldots,\beta), \beta \in GF(q)
\]

and these are identical to the hopping patterns exhibited in (21).

On the other hand, Reed's construction can provide \( 2^t-1 \) hopping patterns with \( H_{max} = 1 \) when it is applied to \( C(2^t-1,2,1) \) over \( GF(2^t) \), while Solomon's construction provides only \( 2^t \) hopping patterns.

There is a minor problem (that did not show up in the above simple examples) with the general version of Solomon's construction. If \( \alpha^t \) is not a primitive element, then the coset representative \((1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(q-1)t}) \) is not a primitive codeword, and hence the hopping patterns do not all have period \( q-1 \) (even though \( H_{max} = t \) for the set.) Fortunately, there is a simple way around this difficulty. The code \( C(q-1;1,1;0) \) is also a subcode of \( C(q-1;1,1;0) \), and Solomon's set can be taken to be the coset with representative \((1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(q-1)t}) \). As noted previously, \( \alpha^{tq} = 1 \) is a primitive element. Hence all the hopping patterns in the coset are of period \( q-1 \), and the problem is thus eliminated.

### II.G Titebaum's Construction

Let \( k = 1 \) so that \( GF(q) = GF(p) \), and consider the code generated by the matrix

\[
G = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 0 & 1 & \ldots & p-1 \end{bmatrix}
\]

It was shown by Roth and Seroussi [21] that this code is a maximum-distance-separable (MDS) cyclic code, and that the code is equivalent under column permutations to an extended cyclic Reed-Solomon code over \( GF(p) \). The minimum distance of this code is \( p-1 \), and hence the representatives of the \( p-1 \) equivalence classes of period \( p \) form a set of nonrepeating hopping patterns with \( H_{max} = 0 \) and \( H_{max} = 1 \). The hopping patterns thus satisfy (3) and (13) with equality and are optimal with respect to the bounds of Section II.B. It is easily shown that the representatives of these equivalence classes may be taken to be

\[
(0,1,2,\ldots,(p-1)i), \quad 1 \leq i \leq p-1.
\]

This form of the construction is due to Titebaum [30] and Shaar and Davies [24]. Extensions to larger sets of hopping patterns can be found in [14] and [31].

A related construction, due to Shaar and Davies [25], is as follows. Suppose that \( 2^t - 1 \) is a Mersenne prime, and consider the generator matrix of the Reed-Solomon code \( C(2^t - 1,2^t - 1;1) \) over \( GF(2^t) \). The all rows of this generator matrix are primitive codewords of the form \((1,\alpha^t,\alpha^{2t},\ldots,\alpha^{(2^t-1)t}) \). Shaar and Davies proposed that these rows be considered as hopping patterns of period \( 2^t - 1 \) over the alphabet \( GF(2^t) \). Note that the \( i \)-th and the \( j \)-th sequence collide in the \( m \)-th and the \( n \)-th dwells when the relative time delay \( i \) dwells, then it must be that \( \alpha^m = \alpha^{(i+j)m} \) and \( \alpha^n = \alpha^{(i+j)n} \). However, these two equations cannot be satisfied simultaneously when \( i \neq j \).

Note that the Shaar-Davies construction cannot be used with fields of characteristic greater than 2 because \( p^2 - 1 \) is always composite when \( p > 2 \) (except in the trivial case \( p = 3 \), \( k = 1 \)). Another construction which also requires an alphabet of prime cardinality is given in [4]. However, this is not directly related to Reed-Solomon codes and will not be discussed further here.

### II.H The Lempel-Greenberger Construction

The Reed and Solomon constructions use codewords from cyclic Reed-Solomon codes and hence the hopping patterns have period at most \( q-1 \). However, the constructions can be used to create large sets of hopping patterns of these relatively short periods. In contrast, in their seminal paper [10], Lempel and Greenberger showed how to create small sets of hopping patterns of very large period. In hindsight, the Lempel-Greenberger construction can also be viewed as a construction based on Reed-Solomon codes, and thus it fits perfectly with the theme of this paper.

Let \( X \) denote an \( m \)-sequence (that is, a maximal-length linear feedback shift register sequence) of period \( N = p^{m-1} \) over \( GF(p) \). Two important properties of \( X \) are as follows:

1. For any \( i \), \( 0 < i < N \), there is a \( j \), \( 0 < j < N \), such that \( X = T^jX \) and \( X = T^jX \).

2. With subscript on \( X \) being taken modulo \( N \), the \( m \)-tuples \((X_0,X_1,\ldots,X_{m-1},0) \), \( 0 \leq i < N \), are distinct and nonzero, that is, each of the \( p^m-1 \) nonzero \( m \)-tuples occurs exactly once in a period of \( X \).

Suppose that \( k \leq n \). Then, since each nonzero \( k \)-tuple can be extended into \( p^{m-k} \) different nonzero \( m \)-tuples, the nonzero \( k \)-tuples all occur \( p^{m-k} \) times in a period of \( X \). Similarly, since the zero \( k \)-tuple can be extended into \( p^{m-k} - 1 \) different nonzero \( m \)-tuples, it occurs \( p^{m-k} - 1 \) times in a period of \( X \).

Sequences of \( k \)-tuples are the basis of the Lempel-Greenberger construction. Let \( X \) denote a sequence whose elements are consecutive overlapping \( k \)-tuples from \( X \). Thus,

\[
x_i = (X_i, X_{i+k}, X_{i+2k},\ldots,X_{i+kn}), \quad 0 \leq i < N.
\]

Since \( GF(q) = GF(p^m) \) can be regarded as a \( k \)-dimensional vector space over \( GF(p) \), one can also think of the \( k \) as elements of \( GF(q) \). Property 2 of \( X \) above thus implies that each nonzero element of \( GF(q) \) occurs \( p^{m-k} \) times in a period of \( X \) while 0 occurs \( p^{m-k} - 1 \) times, and thus satisfies (3). The Lempel-Greenberger set of hopping patterns can then be defined as the set of \( q \)-sequences \( \{x^{(j)} \} : 0 \leq j \leq q-1 \} \) where

\[
x_i^{(j)} = \beta_j + x_i, \quad 0 \leq i < N, \quad \beta_j \in GF(q).
\]
Note that $x$ itself is one of the members of this set of hopping patterns. Note also that each $z_{i}^{(j)}$ satisfies (3) with the element $\beta_{i}$ occurring $q^{n+k} - 1$ times and all the other elements occurring $p^{n+k} - 1$ times. Thus, the Lempel-Greenberger set also satisfies (3) with each element of $GF(q)$ occurring a total of $N$ times in the $q$ hopping patterns.

It was shown in [10] that for $1 < \ell < N$,

$$H_{d}(0) = p^{n+k} - 1 = \left\lfloor \frac{N}{q} \right\rfloor - 1 \quad (25)$$

and that if $i \neq j$, then $H_{d}(a_{i}, a_{j}) = 0$ and

$$H_{d}(a_{i}, a_{i}) = p^{n+k} = \left\lfloor \frac{N}{q} \right\rfloor > N \frac{1}{q} q \quad (26)$$

for $1 < \ell < N$. Thus, the hopping patterns are optimal with respect to the bounds (11) and (15). These properties can be proved straightforwardly using the properties of $X$. These properties can also be deduced from the fact that the Lempel-Greenberger hopping patterns can be obtained by mapping a set of Reed and Solomon sequences over $GF(p)$ of the form exhibited in (21) to $GF(q)$. This idea is considered next.

Suppose without loss of generality that the $m$-sequence $X$ is in its characteristic phase so that there is a primitive element $\xi \in GF(p^{n})$ such that $X_{i} = Tr(\xi^{i})$, $0 \leq i < N$ where $Tr(x) = x + x^{q} + \cdots + x^{q^{n-1}}$ is the trace function from $GF(p^{n})$ to $GF(p)$ [16]. Now, a standard polynomial for $GF(p^{n})$ over $GF(p)$ is $(1, \xi, \xi^{2}, \ldots, \xi^{n-1})$. The $m$-tuple $(a_{0}, a_{1}, \ldots, a_{n-1})$ represents the element $\sum a_{i} \xi^{i} \in GF(p^{n})$ with respect to this standard polynomial basis. Let $(g_{0}, g_{1}, \ldots, g_{n-1})$ denote the dual basis of the standard polynomial basis. With this dual basis, the $m$-tuple $(b_{0}, b_{1}, \ldots, b_{n-1})$ represents the element $\sum b_{i} g_{i} \in GF(p^{n})$. But, according to the properties of dual bases, the $b_{i}$ are given by $b_{i} = Tr(Y \cdot \xi^{i})$ for $0 \leq i \leq n - 1$ [16]. Thus the $m$-tuple

$$(X_{0}, X_{1}, \ldots, X_{n-1})$$

$$(\xi^{0}, \xi^{1}, \ldots, \xi^{n-1})$$

$$= (Tr(\xi^{0}), Tr(\xi^{1}), \ldots, Tr(\xi^{n-1}))$$

$$(\xi^{0}, \xi^{1}, \ldots, \xi^{n-1})$$

is just the representation of $\xi^{i}$ with respect to the dual of the standard polynomial basis. Hence, the sequence $X$ of successive overlapping $m$-tuples from $X$ with $i$-th element given by

$$X_{i} = (X_{0}, X_{1}, \ldots, X_{i-1})$$

is the sequence $(1, \xi, \xi^{2}, \ldots, \xi^{n-1})$ over $GF(p^{n})$ with respect to the dual of the standard polynomial basis.

Consider the Reed and Solomon set of sequences from the Reed-Solomon code $C(p^{n} - 1, 2, 0)$ over $GF(p^{n})$. Denoting the elements of $GF(p^{n})$ as $\gamma_{i}$, $0 \leq i \leq N$, the $i$-th sequence is just

$$X_{i}^{(0)} = (1, \xi, \xi^{2}, \ldots, \xi^{n-1}) + (\gamma_{0}, \gamma_{1}, \ldots, \gamma_{n}) \quad (28)$$

which is exactly of the form given in (21). Note that $\gamma_{i}$ does not occur in $X_{i}^{(0)}$ while all the other elements of $GF(p^{n})$ occur exactly once. Now, suppose that the elements in the vectors in (28) are represented in the dual-polynomial basis of (27). View the first $k$ entries of the representation of $\gamma_{i}$ as an element of $GF(q)$, and note that $\gamma^{n+k}$ different $\gamma$ give rise to the same element $\beta_{i}$ (say) of $GF(q)$. Of course, the representation of $\gamma^{i}$ is just the right side of (27) and the first $k$ entries are just $x_{i}$ as defined in (23). It follows that the sequence $z_{i}^{(0)}$ defined in (24) is the image of $p^{n+k}$ Reed-Solomon codewords $X_{i}^{(0)}$ under the projection mapping which maps an element of $GF(p^{n})$ onto its first $k$ coordinates in the dual-polynomial basis. Note also that only $q$ different sequences over $GF(q)$ are obtained from this mapping. As a special case, the Lempel-Greenberger hopping patterns are identical to the Reed and Solomon patterns when $n = k$ and all field elements are represented with respect to the dual of the standard polynomial basis.

As shown above, the Lempel-Greenberger hopping patterns are a special case of a more general sequence design based on the idea of mapping Reed and Solomon hopping patterns over $GF(p)$ onto $GF(q)$. All the Hamming correlation properties discussed above for the Lempel-Greenberger hopping patterns also apply to the more general set. To see this, note that $X^{(0)}$ and $X^{(1)}$ are both codewords in a linear cyclic code and hence $R^{(0)} = R^{(1)} = R^{(2)}$ in the same code. Furthermore, if $i = 0$, this codeword consists of $\gamma_{i} - \gamma_{i}$ repeated $N$ times, whereas if $0 < i < N$, then every element of $GF(p)$ except $\gamma_{i} - \gamma_{j}$ appears exactly once in this codeword. Now, for a relative time delay of $\ell$, the Hamming correlation between $L(X^{(0)})$ and $L(X^{(0)})$ is just the number of times that 0 appears in the sequence $L(X^{(0)}) - T L(X^{(0)})$. But this sequence is just the image of $X^{(0)} - \ell X^{(0)}$ under $L$. Thus, if $\gamma_{i} - \gamma_{i} \in ker(L)$, then $L(X^{(0)}) = L(X^{(0)})$, the correlation under consideration is an autocorrelation, and 0 appears $p^{n+k} - 1$ times for any $i$, $0 < i < N$. On the other hand, if $\gamma_{i} - \gamma_{i} \not\in ker(L)$, then $L(X^{(0)}) \neq L(X^{(0)})$, the correlation under consideration is a crosscorrelation, and 0 appears $p^{n+k} - 1$ times if $i \neq 0$ and never appears if $i = 0$. Thus, the Hamming correlation properties (25) and (26) of the Lempel-Greenberger hopping patterns also hold in the more general case.

Another interesting property of the Lempel-Greenberger hopping patterns arises from the fact that the underlying sequence $X$ is an $m$-sequence of period $p^{n} - 1$. According to Property 2 above, $X$ contains a run of length $n$ of each nonzero element of $GF(p)$. It follows that the sequence $s$ defined in (23) has a run of length $n - k + 1$ corresponding to each nonzero element of $GF(p)$. Thus, at some time during each period, the signal will hop to the frequency slot corresponding to $(i, 1, \ldots, 1) \in GF(q)$ and stay there for $n - k + 1$ successive dwells. Since $X$ also contains runs of lengths $n - 1, n - 2, \ldots$, the signal will return to the same slot many more times in each period though it will stay there for fewer successive dwells. Since $s^{(0)} = s \cdot \xi_{0}$, the other Lempel-Greenberger hopping patterns hop to slots corresponding to $\beta_{j} + (i, \xi, \ldots, \xi^{k-1})$ and stay there for $n - k + 1$ successive dwells. In fact, given any frequency slot, there are $p - 1$ Lempel-Greenberger patterns that will hop to that slot and stay there for $n - k + 1$ successive dwells. All this is clearly undesirable for the reasons discussed in Section II. Note that the maximum length of a burst of this for Lempel-Greenberger hopping patterns is at least $n - k + 1$ which is approximately $k$ times larger than the lower bound of (18). These properties also hold for the more general version of the Lempel-Greenberger sequence discussed above. The proof is a straightforward but not particularly interesting exercise in linear algebra and the theory of equivalent matrices.

III. Generalizations of the Lempel-Greenberger Construction

The Lempel-Greenberger construction is optimal with respect to various correlation bounds but has the defect that long runs occur in the sequences and these runs are undesirable for the reasons outlined in Section II. C. Various generalizations of this construction are possible. For example, one can use the extension field $GF(p^{n})$ instead of the prime field $GF(p)$. Thus, $X$ is an $m$-sequence of period $(p^{n})^{m} - 1$ over $GF(p^{n})$ and these general-
ized Lempel-Greenberger hopping patterns are formed by considering the sequence $x$ of successive overlapping $k$-tuples from $X$ and adding a fixed $k$-tuple over $GF(p')$ to each element of $x$. The hopping patterns are elements of $GF(p')^k$. None of the proofs in [10] really require the base field $GF(p)$ to be a prime field; they all hold mutatis mutandis if the base field is the extension field $GF(p^r)$ instead. Unfortunately, this also means that all the results asserted in the previous subsection also hold.

In particular, these generalized Lempel-Greenberger hopping patterns also have runs of the same frequency, and produce bursts of hits for certain relative time delays, etc.

Recently, a different solution to the runs problem, based on a combination of the Lempel-Greenberger and Reed-Solomon approaches, has been proposed by Burger [2]. This method can be viewed as a product code construction in which one code is a Lempel-Greenberger hopping pattern and the other code is a Reed-Solomon hopping pattern. The method begins by constructing a set of $q$ Lempel-Greenberger hopping patterns of period $p^r - 1$ over $GF(q)$ as usual. Each transmitter uses a different ($q-1,1$) Reed-Solomon code (actually a code of a $(q-1,1)$ Reed-Solomon code) over $GF(q)$ to encode each symbol in its Lempel-Greenberger pattern. In other words, each symbol in the Lempel-Greenberger pattern is replaced by a codeword of length $q - 1$ from the Reed-Solomon coset. This creates a hopping pattern of length $(p^r - 1)(q - 1) = p^{r+1} - p^r - 1$ over $GF(q)$. Now, the Reed-Solomon coset is a coset of $C(1, t, 1, 0)$, and the $q$ different cosets assigned to the $q$ transmitters are all subsets of $C(q - 1, 1, 0, 2)$. Hence, any two codewords in the coset assigned to a transmitter collide in at most one position, while codewords from the cosets assigned to different transmitters collide in at most two positions. The Hamming correlations of these patterns are not quite optimal but are nonetheless very good. More important however, is the fact that the runs of the same frequency that occur in the Lempel-Greenberger patterns have been broken up. It is also easy to show that at most $q$ successive collisions can occur between two patterns which alleviates the burden on the error correction system as well. Further details of this construction can be found in [2].

II.II Vajda's Construction

The use of a product code construction of hopping patterns has also been explored by Vajda [22] who took a cyclic product of two codes. The first code is obtained from $C(N, t + 1, 0)$ over $GF(q)$ where $N$ is a prime. As described in Section II.E, $q'$ hopping patterns of period $N$ can be obtained from this code. Let $r$ denote the largest integer such that $N^{-1} \leq q'$. This code is a (nonlinear) cyclic code consisting of a set of $N^{2-1}$ hopping patterns of period $N$ and all their cyclic shifts. Note that the minimum distance of this nonlinear cyclic code is $N - r$. The other code is a coset of $C(M, K - 1, 0)$ over $GF(q')$ that is a subcode of $C(M, K + 1, 0)$ over $GF(q')$. Note that $M$ is a divisor of $N^{2-1}$. Thus, this code has $N^{2-1}$ codewords over an alphabet of size $N^{2-1}$ and since the codewords belong to $C(M, K + 1, 0)$, the minimum distance between two codewords is at least $M - K$. Vajda has proposed using the cyclic product of these codes instead of the direct product discussed in the previous subsection. Thus, each of the $M N^{2-1}$ codewords in a codeword of the second code is replaced by a column vector of length $N$ consisting of a codeword of the first code. This creates a $N \times M$ matrix $Q = Q_{ij}$. Now, $M$ and $N$ are relatively prime, and hence the entries in $Q$ can be read off in cyclic fashion to form a hopping pattern of length $M$ whose $s$th symbol is $Q_{i,s}$ and $i = 1, \ldots, M$. Since the cyclic product of a $(t_1, k_1, d_1)$ cyclic code with a $(t_2, k_2, d_2)$ cyclic code is a $(t_1, k_1, k_2, d_2d_1)$ cyclic code [13], this hopping pattern is actually a codeword in a $(MN, k + 1)(K + 1, M - K)(N - 1)$ cyclic code over $GF(q)$. There are $N^{2-1}$ such hopping patterns, and it follows from (7) that, as shown in [32],

$$H_{max} \leq MN - (M - K)(N - 1) = M + KN - Kt.$$  

As an example of this construction, let $q = 32, N = 31, t = 2, r = 3$, and $M = (31^3 - 1)/(31 - 1) = 993$. Let $K = 4$. Then, a set of $31^2 = 967, 303, 661$ hopping patterns of period $31$ - $963 = 36,783$ over $GF(32)$ is obtained. The maximum Hamming correlation is $2,102$, so that there is, on the average, one hit every $14.64$ symbols.

In contrast, the Reed and Solomon sets of hopping patterns from $C(31, 3, 0)$ over $GF(32)$ provide 1,034 hopping patterns of period 31 with a maximum Hamming correlation of 3, that is, one hit every 15.5 symbols, which is very slightly better.

II.II Einarsson's Construction

Because of technological limits per the frequency synthesizers used to produce the frequency-hopped signals, the hopping rate in a FH/CDMA system is limited to a few thousand dwells per second. In a fast FH/CDMA system, the transmission of a symbol occurs over several hops, and it is necessary to use $M$-ary signaling in order to achieve a reasonably large data rate. Einarsson [5] proposed a combined design of hopping patterns and $M$-ary modulation for use in such systems. In systems using this design, each transmitter is assigned a collection of $M$ hopping patterns of length $N$, and transmits one $M$-ary data symbol per $N$ dwells by choosing and transmitting one of the hopping patterns. The data rate is thus $\log_2(M)/N$ bits per dwell. Note however, that the receiver is now more complicated since it must track all $M$ possible hopping patterns in order to determine which one is being transmitted. Thus, $M$ different frequency synthesizers might be needed in each receiver.

The Einarsson design uses all the nonzero codewords in the Reed-Solomon code $C(q - 1, 2, 0)$. Each transmitter is assigned all the codewords in a cyclic equivalence class. Thus, $M = N - q - 1$, and the hopping patterns assigned to $j$th transmitter are of the form

$$\beta_j \beta_j \ldots \beta_j \beta_j + \alpha \beta_j \beta_j \ldots \beta_j \beta_j, \quad 0 \leq j \leq N - 1.$$

Since all these sequences are from $C(q - 1, 2, 0)$, the number of hits between two patterns assigned to different transmitters is at most 1 regardless of the relative time delay between the two patterns.

However, the number of hits per period can be guaranteed to be 1 only if the two transmitters are frame-synchronous. If the transmitters are only dwell-synchronous, then the tail end and the front end of two possibly different hopping patterns from an interfering transmitter can cause collisions, and thus the number of hits per period can be 2 in some cases. There is also the question of the initial acquisition of synchronization in the receivers in such systems since the hopping patterns assigned to a transmitter are not cyclically inequivalent. In fact, the Hamming crosscorrelation between two hopping patterns assigned to the same transmitter can have values as large as $N - 1$.

III. Direct-Sequence Spread-Spectrum Systems

The desirable properties of signature sequences for DS/CDMA systems and a detailed tutorial survey of various constructions for these signature sequences can be found in [23]. Here, it is shown that most of these sequences can be viewed as images of codewords from Reed-Solomon codes.

2 A similar phenomenon in DS/CDMA systems gives rise to the odd crosscorrelation function of binary sequences (cf. [23]).
III.A. Binary m-sequences and their decimations

Let \( N = 2^k - 1 \) and let \( x^{(i)} \) denote a binary m-sequence of period \( N \). Suppose that \( x^{(i)} \) is in its characteristic phase, that is, \( x^{(i)}(0) = x_0^{(i)} \). Then there is a primitive element \( \alpha \) of \( GF(2^k) \) such that \( x_0^{(i)} = Tr(\alpha^i) = 0 \leq i < N \), where, as in Section II.B, \( Tr(\cdot) = x + x^2 + x^4 + \ldots + x^{2^{k-1}} \) is the trace function which maps \( GF(2^k) \) to \( GF(2) \). Thus, \( x^{(i)} \) is the image of the sequence \( \{x(0), x(1), \ldots, x(N-1)\} \) over \( GF(2) \). But \( x^{(i)} \) is a primitive codeword in the cyclic Reed-Solomon code \( C(N, 1, 1) \) with parity-check polynomial \( h(x) = (x - \alpha^{-i}) \) and thus, the binary m-sequence \( x^{(i)} \) can be obtained by mapping the Reed-Solomon codeword \( X^{(i)} \) to \( GF(2) \).

Moreover, for \( 0 \leq s < N \), the \( s \)-th decimation of \( x^{(i)} \) is the sequence \( x^{(i,s)} \) defined by \( x^{(i,s)}(t) = x^{(i+st)} \) where the subscripts are taken modulo \( N \). Thus, \( x^{(i,s)} = Tr(\alpha^{is}) = Tr(\alpha^s \alpha^i) \) so that \( x^{(i,s)} \) is the image of \( X^{(i)} = \{x(0), x(1), \ldots, x(N-1)\} \) which is a codeword in \( C(N, 1, s) \). Thus, the decimations of \( x^{(i)} \) are also images of Reed-Solomon codewords. If \( g_1(x) = N \), the element \( \alpha^i \) is primitive, and hence \( X^{(i)} \) is a primitive codeword and \( x^{(i,s)} \) is an m-sequence. Otherwise, \( X^{(i)} \) is nonprimitive and both \( X^{(i)} \) and \( x^{(i,s)} \) have period \( N \) if \( g_1(x) < N \). Note that since \( x^{(i)} \) is in its characteristic phase, that is, \( x^{(0)} = x^{(N-1)} \), that is, \( x^{(i,s)}(t) = x^{(i+st)} = x^{(i,s+st)} \).

It follows that \( x^{(i,s)} = x^{(i,s')} \) for all \( x \), \( 0 \leq s < N \), and all \( s, 0 \leq s < N \). Furthermore, \( X^{(i,s)} \) is not the only Reed-Solomon codeword that is mapped to \( X^{(i)} \) by the trace function \( X^{(i,s)} \) is also mapped to \( x^{(i,s)} \) by \( \beta \). Note that \( X^{(i,s)} \) is a codeword in the cyclic Reed-Solomon code \( C(N, 1, s) \) with parity-check polynomial \( h(x) = (x - \alpha^{-s}) \). This idea is used repeatedly in the remainder of this section.

III.B. Dual BCH sequences

Consider the Reed-Solomon code \( C(N, 2, 2) \) over \( GF(2^k) \) whose generator matrix \( G \) has two rows \( X^{(0)} \) and \( X^{(1)} \). Both rows are primitive codewords if \( n \) is odd, while if \( n \) is even, \( X^{(0)} \) has period \( N/3 \). Thus, this Reed-Solomon code has period \( 2^k + 1 \) or \( 2^k \) cyclically inequivalent codewords of period \( N \) according as \( n \) is odd or even. A typical primitive codeword of the form \( X^{(i)} = \beta X^{(0)} \) where \( \beta \) is a \( GF(2^k) \). Now, suppose that \( \beta = \alpha \) and that \( \beta \neq 0 \). Then \( S X^{(i)} = \alpha X^{(i)} \) is a cyclic shift of \( X^{(i)} \), and hence the trace function (which is a linear function from \( GF(2^k) \) to \( GF(2) \)) maps \( X^{(i)} = \beta X^{(0)} \) to the binary sequence \( x^{(i)} + X^{(i,s)} = x^{(i)} + T X^{(i,s)} \) for some \( s \), \( 0 \leq s < N \). If \( \beta = 0 \), the sequence is just \( x^{(i)} \). One other sequence that can be added to the list of binary sequences obtained from \( C(N, 2, 2) \) is \( X^{(i)} \) itself. Thus, the collection of \( 2^k + 1 \) sequences can be written as \( \{x^{(i)}(0), x^{(i,s)} | 0 \leq i < N \} \).

IV. Conclusions

This paper has discussed how Reed-Solomon codes can be used in the design of frequency-hopping patterns for FH/CDMA systems and signature sequences for DS/CDMA systems. Although signature sequences for DS/CDMA systems can be viewed as the images of Reed-Solomon codewords, there seems to be no obvious connection between the properties of the Reed-Solomon code and the correlation properties of the resulting signature sequences. Thus, the primary application of Reed-Solomon codes in sequence design for CDMA systems remains the design of hopping patterns for FH/CDMA systems.
in Section III is drawn from [23]. The author wishes to thank Professor Michael B. Pursley, his co-author on those papers, for many helpful discussions on this topic. The author also wishes to thank Professor Pentti Leppänen and Savo Glasic for the invitation to present this paper.

References and Selected Bibliography

1. C. A. Baum and M. B. Pursley, "Bayesian methods for error-


14. J. V. Mark and E. T. Titlebaum, "Frequency hopp... - Downloadable copy.


