

13

a period of  $2^{10}-1=1023$  (or  $2^{15}-1=32767$ ). There are 33 (or 1057) 31-bit sequences transmitted per 1023-bit (32767-bit) period, assuming that the feedback in lower register 156 has degree 10 (15). Therefore, it is convenient if the block length of a modified Reed-Solomon code is (a small multiple of) 33. In this case, synchronization of the codeword coincides with synchronization of the Q-arm  $b(t)$ . This can be achieved by using a Reed-Solomon code of block length 33 over  $GF(2^{10})$  (1057 over  $GF(2^{15})$ ) and blocking 10 (15) bits (two (three) consecutive received symbols) as elements of a received 33-symbol (1057-symbol) word. Such a word spans two (three) periods of the 1023-bit (32767-bit) sequence. In one embodiment, to facilitate synchronization of the code blocks, the polarity of the transmitted sequences are inverted after two (three) consecutive sequence periods. A polarity inversion indicates the boundary of a codeword. Other modifications of this technique are also possible. For example, if a non-primitive degree-15 polynomial is used in the previous example, a sequence of period  $31 * 151=4681$  can be generated. In general any divisor of  $2^{kn}-1$  can be used, where  $k$  is a positive integer. The block length of the modified Reed-Solomon code over  $GF(2^{15})$  is then 151, and three periods of 4681 comprise a block.

The symbol-oriented coding/decoding approach of the present invention is superior to a bit-oriented approach for multiple-sequence spread spectrum systems. Symbol-oriented coding/decoding schemes have not been used in previously developed spread spectrum systems. The QUALCOMM system uses interleaving combined with convolutional codes, presumably because of the ready availability of convolutional coding/decoding hardware. For conventional, single-sequence systems, Reed-Solomon or other block-oriented codes offer no particular advantage over convolutional codes, especially if interleaving is employed.

The above description is included to illustrate the operation of the preferred embodiments and is not meant to limit the scope of the invention. The scope of the invention is limited only by the following claims. From the above discussion, many variations will be apparent to one skilled in the art that are yet encompassed by the spirit and scope of the invention.

APPENDIX A

All operations in the following (except for sums of subscripted indices) take place over  $GF(2)$ , the field of two elements. The cyclic correlations  $\{C_0, C_1, \dots, C_{2^n-2}\}$  at successive offsets between a  $(2^n-1)$ -long sequence  $\{Y_0, Y_1, \dots, Y_{2^n-2}\}$  of real or complex numbers and a binary sequence  $\{u_0, u_1, \dots, u_{2^n-2}\}$  of the same length are defined by the equations:

$$c_k = \sum_{i=0}^{2^n-1} y_i(-1)^{u_i+k}, 0 \leq k \leq 2^n - 2.$$

The Hadamard transform of a  $2^n$ -long sequence  $\{z_0, z_1, \dots, z_{2^n-1}\}$  is defined to be the set of transform coefficients  $\{Z_s\}$ , defined by

$$Z_s = \frac{1}{2^n} \sum_{k=0}^{2^n-1} z_k (-1)^{ks}$$

where  $\bar{k} \cdot \bar{s}$  denotes the dot product of the vectors  $\bar{k}$  and  $\bar{s}$  consisting of the  $n$ -long binary representation of the integers

14

$R$  and  $s$ , respectively (that is, if

$$k = \sum_{i=0}^{n-1} k_i 2^i, \text{ then } \bar{k} = (k_0, k_1, \dots, k_{n-1}).$$

The convolution coefficients  $\{c_k\}$  may be obtained as a permutation of the coefficients of a Hadamard transform applied to a padded and reordered version of the sequence  $\{y_k\}$ . To show this, it is necessary to discuss some concepts from the theory of finite fields.

Suppose that  $f(x)$  is a polynomial of degree  $n$  in  $GF(2)[x]$  (the set of polynomials in the variable  $x$  with coefficients in  $GF(2)$ ), given by

$$f(x) = x^n \oplus \sum_{i=0}^{n-1} f_i x^i$$

(Here,  $\Sigma$  denotes a sum in  $GF(2)[x]$ ). A linear recursive sequence satisfying  $f$  is a sequence  $\{u_k\}$  such that  $u_k = f_0 u_k \oplus f_1 u_{k-1} \oplus \dots \oplus f_{n-1} u_{k-n+1}$ , and  $f$  is said to "generate"  $\{u_k\}$ . If  $\{u_k\}$  is a maximal-length linear recursive sequence ("M-sequence", or MLLRS) of period  $2^n-1$ , then  $f$  is said to be "primitive." The "companion matrix" of  $f$  is defined to be

$$A = \begin{bmatrix} f_0 & f_1 & \dots & f_{n-2} & f_{n-1} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

If  $\{u_k\}$  is a linear recursive sequence over  $GF(2)$  satisfying  $f(x)$ , let  $\underline{u}_k$  denote the column vector

$$\underline{u}_k = \begin{bmatrix} u_{k+n-1} \\ \vdots \\ u_{k+1} \\ u_k \end{bmatrix}$$

Then,  $A \underline{u}_k = \underline{u}_{k+1}$ . That is, multiplication of a "fill"  $\underline{u}_k$  by  $A$  shifts a register "driven by  $f$ " to produce the next fill,  $\underline{u}_{k+1}$ . Thus,  $\underline{u}_k = A^k \underline{u}_0$ . If  $f$  is primitive of degree  $n$ , then a sequence of  $2^n-1$  successive fills of a register driven by  $f$  consists of a permutation of all of the non-zero binary  $n$ -tuples. Let

$$\underline{e} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 1 \end{bmatrix}$$

and suppose  $\underline{e}^T$  denotes the transpose of  $\underline{e}$ . Let  $\underline{e}_k = (A^T)^k \underline{e} = (\underline{e}_{ki})$ . Then,  $\underline{u}_k = \underline{e}^T \underline{u}_k = \underline{e}^T A^k \underline{u}_0 = \underline{e}_k^T \underline{u}_0$ .

Now suppose that  $f$  is primitive and define  $\{z_0, z_1, z_2, \dots, z_{2^n-1}\}$  by  $z_0=0$  and  $z_{e_i} = Y_i, 0 \leq i \leq 2^n-2$  (here,  $e_i$  is used as