V. Discussion

In this paper we have presented results which are useful in the study and selection of sequences with good correlation properties. We should point out that the following generalization of Proposition 1 and Corollary 2 can be established. For $T > 0$, let $\mathcal{L}_T$ be the space of all complex-valued functions of a real variable which satisfy $x(t+T), x(t)$ for each t and $\int_{[0,T)} |x(t)|^2 \mu\,(dt) < \infty$, where μ is a measure on the real line. If, for each $x \in \mathcal{L}_T$ and $y \in \mathcal{L}_T$, we define $C_{x,y}(T) = C_{x,y}(-T) = 0$ and

$$C_{x,y}(\tau) = \begin{cases} \displaystyle\int_{[0,T-\tau)} x(t) y^*(t+\tau) \mu\,(dt), & 0 \le \tau < T \\ \displaystyle\int_{[0,T+\tau)} x(t-\tau) y^*(t) \mu\,(dt), & -T < \tau < 0, \end{cases}$$

then

$$\int_{[-T,T)} |C_{x,y}(\tau)|^2 \mu\,(d\tau) = \int_{[-T,T)} C_{x,x}(\tau) C_{y,y}{}^*(\tau) \mu\,(d\tau)$$
$$\le \left[\int_{[-T,T)} |C_{x,x}(\tau)|^2 \mu(d\tau) \right]^{1/2} \left[\int_{[-T,T)} |C_{y,y}(\tau)|^2 \mu\,(d\tau) \right]^{1/2}.$$

This gives Proposition 1 and Corollary 2 as a special case when $\mu(\{i\}) = 1$, for each $i \in Z$ and $\mu(Z^C) = 0$.

We have also indicated how these results can be employed to reduce the amount of computation required to calculate the key correlation parameters. In addition to application of the analytical results of Section III to computational problems, Proposition 1 and its corollaries can be employed to investigate aperiodic cross-correlation properties of certain classes of sequences which have been studied from the point of view of their aperiodic autocorrelation properties [8]–[10]. Our brief discussion of Barker sequences in Section III gives an indication of what might result from such an investigation.

Acknowledgment

The authors wish to thank Mr. H. F. A. Roefs for pointing out that the approximation $r_{k,i} \approx \tilde{r}_{k,i}$ is exact for Barker sequences and for supplying numerical data on the magnitude of the error in this approximation for auto-optimal shifts of m-sequences of period 127.

References

[1] J. L. Massey and J. J. Uhran, "Sub-baud coding," *Proceedings of the Thirteenth Annual Allerton Conference on Circuit and System Theory,* Monticello, IL, pp. 539–547, October 1975 (see also "Final report for multipath study," Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, 1969).

[2] M. B. Pursley, "Evaluating performance of codes for spread spectrum multiple access communications," *Proceedings of the Twelfth Annual Allerton Conference on Circuit and System Theory,* Monticello, IL, pp. 765–774, October 1974 (see also "Tracking and data relay satellite system configuration and tradeoff study," Volume 4, Appendix D, Hughes Aircraft Company, Space and Communications Group, El Segundo, CA, Report 20642R, Sept. 1972).

[3] K. Yao, "Error probability of spread spectrum multiple access communication systems," *Proceedings of the 1976 Conference on Information Sciences and Systems,* Johns Hopkins University, Baltimore, MD, pp. 67–72, March 1976.

[4] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory,* vol. IT-13, pp. 619–621, Oct. 1967.

[5] K. Yao and R. M. Tobin, "Moment space upper and lower error bounds for digital systems with intersymbol interference," *IEEE Trans. Inform. Theory,* vol. IT-22, pp. 65–75, Jan. 1976.

[6] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 397–399, May 1974.

[7] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inform. Theory,* vol. IT-14, pp. 154–156, Jan. 1968.

[8] R. H. Barker, "Group synchronizing of binary digital systems," in *Communication Theory* (W. Jackson, editor). New York: Academic Press, 1953.

[9] R. Turyn and J. Storer, "On binary sequences," *Proc. Amer. Math. Soc.,* vol. 12, pp. 394–399, 1961.

[10] G. Seguin, "Binary sequences with specified correlation properties," Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, Technical Report No. 7103, Aug. 1971.

[11] M. R. Sywyk, "Sub-baud codes for code multiplexing," M. Eng. Thesis, Royal Military College of Canada, Kingston, ON, Canada, May 1975.

[12] T. G. Stockham, Jr., "High speed convolution and correlation," *Spring Joint Computer Conference, AFIPS Conference Proceedings,* Vol. 28, pp. 229–233, 1966.

[13] M. B. Pursley and D. V. Sarwate, "Correlation parameters for periodic sequences—Properties, bounds and efficient computational methods," Coordinated Science Laboratory, Technical Report R-725, University of Illinois, Urbana, IL, Apr. 1976.

Decoding of Alternant Codes

HERMANN J. HELGERT

***Abstract*—It is shown that the only modification of the Berlekamp algorithm required to decode the class of alternant codes consists of a linear transformation of the syndromes prior to the application of the algorithm. Since alternant codes include all Bose–Chaudhuri–Hocquenghem (BCH) and Goppa codes, the Chien-Choy generalized BCH codes, and the generalized Srivastava codes, all of these can be decoded with no increase in complexity over BCH decoding.**

I. Alternant Codes

The general class of alternant codes [1] may be defined as follows. Let

$$H_A = CXY$$
$$= \begin{bmatrix} C_{01} & C_{11} & \cdots & C_{t-1,1} \\ C_{02} & C_{12} & \cdots & C_{t-1,2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ C_{0t} & C_{1t} & \cdots & C_{t-1,t} \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & & x_n \\ x_1{}^2 & x_2{}^2 & & x_n{}^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_1{}^{t-1} & x_2{}^{t-1} & \cdots & x_n{}^{t-1} \end{bmatrix} \begin{bmatrix} y_1 & 0 & \cdots & 0 \\ 0 & y_2 & \cdots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & & \cdots & y_n \end{bmatrix} \quad (1)$$

where all quantities are elements of $GF(q^m)$ and, in addition, the y are nonzero and the x are distinct. Then if $mt < n$ and C is nonsingular, H_A is the parity check matrix of a linear alternant code of length n, minimum distance $d \ge t+1$, and at most mt parity check symbols.

It is easily shown that alternant codes include as special cases all Bose–Chaudhuri–Hocquenghem (BCH) and Goppa codes [2], Chien and Choy's generalized BCH codes [3], and the class of generalized Srivastava codes [1]. For example, the Goppa codes can be defined in terms of their parity check matrix which takes

Manuscript received October 24, 1975; revised May 21, 1976.
The author is with the Department of Electrical Engineering and Computer Science, George Washington University, Washington, DC 20006.

the form

$$H_G = \begin{bmatrix} b_t & 0 & 0 & \cdots & 0 \\ b_{t-1} & b_t & 0 & \cdots & 0 \\ b_{t-2} & b_{t-1} & b_t & \cdots & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ b_1 & b_2 & b_3 & & b_t \end{bmatrix} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_1^{t-1} & x_2^{t-1} & \cdots & x_n^{t-1} \end{bmatrix}$$

$$\begin{bmatrix} g^{-1}(x_1) & 0 & \cdots & 0 \\ 0 & g^{-1}(x_2) & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ 0 & 0 & \cdots & g^{-1}(x_1) \end{bmatrix} \quad (2)$$

where $g(z) = \Sigma_{i=0}^{t} b_i z^i$ is the Goppa polynomial of degree t with coefficients in $GF(q^m)$ and having no roots among the x_i.

In what follows, we show that Berlekamp's algorithm for decoding BCH codes also applies to alternant codes, the only required modification being a linear transformation of the syndromes prior to the application of the algorithm.

II. Decoding

Assume errors of values $z_1, z_2, \cdots, z_l$ at locations $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$, $l \le [t/2]$. Then, in matrix notation, the syndromes $R_1, R_2, \cdots, R_t$ for an alternant code are given by

$$\begin{bmatrix} R_1 \\ R_2 \\ \\ \\ \cdot \\ \cdot \\ R_t \end{bmatrix} = C \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_{i_1} & x_{i_2} & \cdots & x_{i_l} \\ x_{i_1}^2 & x_{i_2}^2 & \cdots & x_{i_l}^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{i_1}^{t-1} & x_{i_2}^{t-1} & \cdots & x_{i_l}^{t-1} \end{bmatrix} \begin{bmatrix} z_1 y_{i_1} \\ z_2 y_{i_2} \\ \\ \cdot \\ \cdot \\ \cdot \\ z_1 y_{i_l} \end{bmatrix}.$$

Let

$$\begin{bmatrix} S_1 \\ S_2 \\ \\ \cdot \\ \cdot \\ S_t \end{bmatrix} = C^{-1} \begin{bmatrix} R_1 \\ R_2 \\ \\ \cdot \\ \cdot \\ R_t \end{bmatrix}.$$

Then $S_j = \Sigma_{k=1}^{l} z_k y_{i_k} x_{i_k}^{j-1}$, $j = 1,2,\cdots,t$.

To relate these weighted power sum symmetric functions to the elementary symmetric functions of the error locations, we set

$$x^l + \sigma_1 x^{l-1} + \sigma_2 x^{l-2} + \cdots + \sigma_{l-1} x + \sigma_l = (x - x_{i_1})(x - x_{i_2}) \cdots (x - x_{i_l}).$$

Multiplying both sides by $z_k y_{i_k} x_{i_k}^{j-1}$ and evaluating at $x = x_{i_k}$ yields

$$z_k y_{i_k} x_{i_k}^{j+l-1} + \sigma_1 z_k y_{i_k} x_{i_k}^{j+l-2} + \sigma_2 z_k y_{i_k} x_{i_k}^{j+l-3} + \cdots + \sigma_{l-1} z_k y_{i_k} x_{i_k}^{j} + \sigma_l z_k y_{i_k} x_{i_k}^{j-1} = 0.$$

Finally, we sum over k from 1 to l and obtain

$$S_{j+l} + \sigma_1 S_{j+l-1} + \sigma_2 S_{j+l-2} + \cdots + \sigma_{l-1} S_{j+1} + \sigma_l S_j = 0, \quad (3)$$

where all S_j are known for $j = 1,2,\cdots,t$. These are a set of $t - l$ equations in the l unknown σ and, since we assumed $l \le [t/2]$, we have at least as many equations as unknowns. Thus the existence of a unique solution depends on the matrix

$$M = \begin{bmatrix} S_1 & S_2 & \cdots & S_l \\ S_2 & S_3 & \cdots & S_{l+1} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ S_l & S_{l+1} & \cdots & S_{2l-1} \end{bmatrix}.$$

Since M can be written as the triple product

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_{i_1} & x_{i_2} & \cdots & x_{i_l} \\ x_{i_1}^2 & x_{i_2}^2 & \cdots & x_{i_l}^2 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{i_1}^{l-1} & x_{i_2}^{l-1} & \cdots & x_{i_l}^{l-1} \end{bmatrix}$$

$$\begin{bmatrix} z_1 y_{i_1} & 0 & \cdots & 0 \\ 0 & z_2 y_{i_2} & \cdots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \cdots & z_l y_{i_l} \end{bmatrix} \begin{bmatrix} 1 & x_{i_1} & x_{i_1}^2 \cdots & x_{i_1}^{l-1} \\ 1 & x_{i_2} & x_{i_2}^2 \cdots & x_{i_2}^{l-1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & x_{i_l} & x_{i_l}^2 \cdots & x_{i_l}^{l-1} \end{bmatrix}$$

it is nonsingular if the S_j are weighted power sums of exactly l of the x_i and is singular if fewer than l of the x_i are involved. Therefore, a unique solution to (3) exists whenever $l \le [t/2]$.

It is now a simple matter to repeat the derivation in [5, section 9.5] to show that the Berlekamp algorithm applied to the sequence $S_1, S_2, \cdots, S_t$ produces the polynomial

$$\sigma^{(l)}(x) = \sigma_l x^l + \sigma_{l-1} x^{l-1} + \cdots \sigma_1 x + 1$$

whose roots are the inverses of the error locations $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$. The case where one of the x_i may equal zero, however, must be resolved separately, since no inverse exists for this element. A modification of the algorithm to produce the reciprocal of $\sigma^{(l)}(x)$ would eliminate the problem, but this hardly seems worth the trouble, since the condition can easily be detected by other means [4].

For binary codes with $y_i = x_i$ and t even, we have $S_{2j} = S_j^2$. Hence the same simplified Berlekamp algorithm as for binary BCH codes applies.

We also note that the parity check matrices XY and CXY define the same code, for any nonsingular C. Therefore, C may in principle always be taken as the unit matrix and this eliminates the need for transforming the syndromes. It is important to realize, however, that in certain cases a judicious choice of C, together with column permutations on XY, may significantly alter the complexity of implementation of the encoding operation.

Finally, we point out that certain subclasses of the alternant codes, such as the generalized BCH codes defined by Chien and Choy and the Goppa codes, have previously been shown to be decodable by the Berlekamp algorithm [3], [6].

References

[1] H. J. Helgert, "Alternant codes," *Inform. Cont.*, vol. 26, pp. 369–380, Dec. 1974.

[2] V. D. Goppa, "A new class of linear error-correcting codes," *Probl. Peredaci Informatii*, vol. 6, pp. 24–30, Sept. 1970.

[3] R. T. Chien and D. M. Choy, "Algebraic generalization of BCH-Goppa-Helgert codes," *IEEE Trans. Inform. Theory*, vol. IT-21, pp. 70–79, Jan. 1975.

[4] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[5] W. W. Peterson and E. J. Weldon, *Error Correcting Codes*. Cambridge, Mass., The MIT Press, 1972.

[6] C. T. Retter, "Decoding Goppa codes with a BCH decoder," *IEEE Trans. Inform. Theory*, vol. IT-21, p. 112, Jan. 1975.