APPLICATION OF CIRCULANT MATRICES TO THE CONSTRUCTION AND DECODING OF LINEAR CODES

RON M. ROTH, MEMBER, IEEE AND ABRAHAM LEMPEL, FELLOW, IEEE

Department of Computer Science
Technion, Israel Institute of Technology
Haifa 32000 - Israel

ABSTRACT

An $r \times r$ matrix $A = [a_{ij}]$ over a field F is called circulant if $a_{ij} = a_{0,(j-i) \bmod r}$. An $[n = 2r, k = r]$ linear code over $F = GF(q)$ is called double-circulant if it is generated by a matrix of the form $[I \ A]$, where A is an $r \times r$ circulant matrix. In this work we first employ the Fourier transform technique to analyze and construct several families of double-circulant codes. The minimum distance of the resulting codes is lower-bounded by $2\sqrt{r}$ and can be decoded easily employing the standard BCH decoding algorithm or the majority-logic decoder of Reed-Muller codes. Second, we present a decoding procedure for Reed-Solomon codes, based on a representation of the parity-check matrix by circulant blocks. The decoding procedure inherits both the (relatively low) time complexity of the Berlekamp-Massey algorithm, and the hardware simplicity characteristic of Blahut's algorithm. The proposed decoding procedure makes use of the encoding circuit together with a reduced version of Blahut's decoder.

This work was presented in part at the Beijing International Workshop on Information Theory, July 1988, and in part at the IEEE International Symposium on Information Theory, San Diego, California, January 1990.

I. INTRODUCTION

An $r \times r$ matrix $A = [a_{ij}]_{0 \le i,j \le r-1}$ over a field F is called *circulant* if $a_{ij} = a_{0,j-i} \triangleq a_{j-i}$ for all $0 \le i, j \le r-1$, where indices are computed modulo r.

Let the notation $[n, k, d]$ stand for a k-dimensional linear code of length n and minimum distance d over F, and let $r = n - k$ denote the redundancy of the code. An $[n = 2r, k = r, d]$ linear code over F is called *double-circulant* if it is generated by a matrix $G = [I \ A]$, where A is an $r \times r$ circulant matrix over F [11, p. 497]. Double-circulant codes have been discussed extensively in the literature [3][7][8][9][11, Ch. 16, §7][13] and a subclass of double-circulant codes approaches the Gilbert-Varshamov bound [10]. Also, the circulant structure of their generator matrices and their parity-check matrices[1] $H = [-A' \ I]$ suggests fast techniques for encoding and syndrome evaluation of such codes. However, the best lower bound on the minimum distance of known families of double-circulant codes is $\sqrt{2r} + O(1)$ [6]. Furthermore, no easy decoding algorithm has been suggested for such code families.

In Section III we investigate several classes of double-circulant codes. As the Fourier transform has proved to be a useful tool in analyzing cyclic codes, especially the BCH codes [4, Chs. 7-9], it is therefore natural to try to apply this tool to double-circulant codes. We employ the Fourier transform to construct and examine some families of double-circulant codes and prove a lower bound of $2\sqrt{r}$ on their minimum distance. We also present an easy decoding algorithm for these codes, based on the Berlekamp-Massey decoding algorithm for BCH codes [2, §7.4][4, Ch. 9][12]. A special case of the given construction is a family of majority-logic decodable codes, resembling the Reed-Muller codes of rate one half [11, Ch. 13].

Next, we show that in many cases, we can transform the parity-check matrix of Reed-Solomon (RS) codes into $H = [(A^{t-1})' \ (A^{t-2})' \cdots A' \ I]$, forming a concatenation of several circulant matrices. This leads to a new decoding algorithm for such codes, based on Blahut's time

[1] A' stands for the transpose of A.

domain decoder [5].

For a RS code of length n and redundancy r, let $\hat{\mathbf{s}}$ denote the r-dimensional Fourier transform of the syndrome $\mathbf{s}$ obtained using the parity-check matrix H. We say that $\hat{\mathbf{s}}$ is the syndrome in the *frequency domain* while $\mathbf{s}$ is the *time domain* syndrome. Time domain decoding of RS codes has been discussed widely by Blahut in [5]. The time domain algorithm used by Blahut is the conventional Berlekamp-Massey decoding algorithm for RS codes after undergoing an inverse n-dimensional Fourier transform, thus avoiding the need to evaluate the syndrome. Still, the time-complexity of Blahut's algorithm in a pipeline scheme remains proportional to $r \cdot n$ (or n^2 in a simpler version of the algorithm), while the required memory is proportional to n.

The algorithm presented in Section IV makes use of the fact that H is a *systematic* parity-check matrix and, therefore, the r-dimensional time-domain syndrome can be calculated using the *encoding* circuit, thus avoiding the need for extra hardware. In this way we obtain a time-domain decoder whose time complexity is proportional to the encoding time plus r^2 in a pipeline configuration (see illustrations in [5]). Decoding time can be reduced at the expense of employing r replicas of multipliers and r-th order unit-root generators, whereby the encoding (and syndrome calculation) becomes the time complexity bottleneck. As encoding is carried out by a shift-register, its complexity is n, similar to that of any cyclic code. Since in our algorithm the Berlekamp-Massey decoding procedure undergoes an r-dimensional Fourier transform, the memory required is proportional to r.

Although we describe the proposed decoding algorithm as a sequential procedure, its advantages are manifest in hardware implementations (e.g. VLSI design). Our building blocks are Blahut's decoders, reduced in size. The reduction in size is compensated for by interpolation which, again, is performed using the encoding circuit only. Thus, all decoding tasks of the proposed algorithm need no hardware other than the encoding circuit and a reduced Blahut's decoder.

II. CIRCULANT MATRICES AND THE FOURIER TRANSFORM

Consider a circulant matrix $A = [a_{ij}] = [a_{j-i}]$, $0 \le i, j \le r-1$. The polynomial $a(x) = a_0 + a_1 x + \cdots + a_{r-1} x^{r-1}$ is called the *defining polynomial* of A. With every $\mathbf{u} = [u_0\ u_1 \cdots u_{r-1}] \in F^r$ we associate a polynomial $u(x) = u_0 + u_1 x + \cdots + u_{r-1} x^{r-1}$. It is easy to verify [11, p. 506] that $\mathbf{v} = \mathbf{u}\ A$ if and only if $v(x) = u(x) \cdot a(x) \pmod{x^r - 1}$ where $a(x)$ is the defining polynomial of A and $u(x)$, $v(x)$ are the polynomials associated with $\mathbf{u}$ and $\mathbf{v}$, respectively.

Let $F = GF(q)$ and let r be an integer relatively prime to q. Denote by h the multiplicative order of q in the ring modulo r and let β be an element of order r in $\Phi = GF(q^h)$. The *r-dimensional Fourier transform* on Φ^r is a linear transformation $\Phi^r \to \Phi^r$ defined by $\mathbf{v} \mapsto \hat{\mathbf{v}} \triangleq \mathbf{v}\ T$, where $T = [\ \beta^{ij}\ ]_{0 \le i, j \le r-1}$ is the *Fourier matrix*. It follows that

$$\hat{\mathbf{v}} = [v(1)\ v(\beta) \cdots v(\beta^{r-1})]\ .$$

The inverse of T is given by $T^{-1} = \frac{1}{r}\ [\ \beta^{-ij}\ ]_{0 \le i, j \le r-1}$ and, for every $\mathbf{u} \in \Phi^r$, $\hat{\mathbf{u}}\ T^{-1}$ is the *inverse* Fourier transform of $\hat{\mathbf{u}}$.

Denote by $\mathbf{a} * \mathbf{b}$ the term-by-term product of two vectors $\mathbf{a}, \mathbf{b} \in \Phi^r$, that is, the i-th component of $\mathbf{a} * \mathbf{b}$ is $a_i \cdot b_i$, $0 \le i \le r-1$. Then, $w(x) = u(x) \cdot v(x) \pmod{x^r - 1}$ if and only if $\hat{\mathbf{w}} = \hat{\mathbf{u}} * \hat{\mathbf{v}}$, which is known as the *convolution property* of the Fourier transform. Similarly, $\mathbf{w} = \mathbf{u} * \mathbf{v}$ if and only if $\hat{w}(x) = \frac{1}{r}\ \hat{u}(x) \cdot \hat{v}(x) \pmod{x^r - 1}$.

The above properties reveal the close relationship between circulant matrices and the Fourier transform. Let A be an $r \times r$ circulant matrix over F with $(r, q) = 1$ and let $a(x)$ be the defining polynomial of A. If $\mathbf{v} = \mathbf{u}\ A$, we have $v(x) = u(x) \cdot a(x) \pmod{x^r - 1}$, or, $\hat{\mathbf{v}} = \hat{\mathbf{u}} * \hat{\mathbf{a}}$. Let $\hat{\xi}_i = [0\ \underset{\leftarrow\ i\ \rightarrow}{0\ \cdots\ 0}\ ,1\ ,\ 0 \cdots 0]$, $0 \le i \le r-1$, denote the i-th unit vector in Φ^r. Since $\hat{\xi}_i * \hat{\mathbf{a}} = \hat{a}_i \hat{\xi}_i$, we have $\xi_i A = \hat{a}_i \xi_i$, meaning that the $\hat{a}_i$ are eigenvalues of A corresponding to the eigenvectors

$$\xi_i = \hat{\xi}_i T^{-1} = \frac{1}{r}\,[\,1\ \beta^{-i}\ \cdots\ \beta^{-i(r-1)}\,]\,, \quad 0 \le i \le r-1\,.$$

Denoting by $D(\hat{\mathbf{a}})$ the diagonal matrix with the elements of $\hat{\mathbf{a}}$ on its main diagonal, we obtain

$$A = T \cdot D(\hat{\mathbf{a}}) \cdot T^{-1}\,.$$

In the sequel, we shall also deal with the special case when $F = \Phi$ and

$$\hat{\mathbf{a}} = [1\ \ \delta\ \ \delta^2\ \ \cdots\ \ \delta^{r-1}]$$

for some $\delta \in F - \{0\}$ such that $\delta^r \neq 1$. In this case the defining polynomial of A is given by

$$a_j = \frac{\frac{1}{r}(1-\delta^r)}{1-\delta\beta^{-j}}\,, \quad 0 \le j \le r-1\,, \tag{1}$$

and, similarly, those of $A^m = [a_{j-i}^{(m)}] = T[D(\hat{\mathbf{a}})]^m T^{-1}$ are given by

$$a_j^{(m)} = \frac{\frac{1}{r}(1-\delta^{rm})}{1-\delta^m\beta^{-j}}\,, \quad 0 \le j \le r-1\ \ , \tag{2}$$

provided $\delta^{rm} \neq 1$.

Let $\alpha \in F$ be of order $n = r \cdot t$, let $\beta = \alpha^t$, and let $\delta = \alpha^b$ with $(b, t) = 1$. In this case $\delta^{rm} \neq 1$ for all $1 \le m \le t-1$. A standard parity-check matrix of an $[n, n-r]$ RS code over F is given by

$$H_0 = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ . & . & . & \cdots & . \\ 1 & \alpha^{r-1} & \alpha^{2(r-1)} & \cdots & \alpha^{(r-1)(n-1)} \end{bmatrix}. \tag{3}$$

For any integer l, $0 \le l \le n-1$, let m and j be the (unique) integers such that $l \equiv (b \cdot m + t \cdot j) \bmod n$, $\quad 0 \le m \le t-1$, $\quad 0 \le j \le r-1$. Define the permutation π on $\{0, 1, \cdots, n-1\}$ by

$$\pi(l) = (t-1-m)r + j \triangleq < m, j >\,, \quad 0 \le l \le n-1\,. \tag{4}$$

Applying π to the code coordinates, we obtain an equivalent code C whose parity-check matrix

is of the form

$$\hat{H} = \left[\begin{array}{cccc} V^{t-1}T & V^{t-2}T & \cdots & VT \quad T \end{array} \right],$$

where $T = [\ \beta^{ij}\ ]$ and $V = D([1 \ \ \delta \ \ \delta^2 \ \cdots \ \delta^{r-1}])$. As any nonsingular linear operation on the rows of $\hat{H}$ results in a parity-check matrix for C, we can obtain another such matrix

$$H = T^{-1}\hat{H} = \left[\begin{array}{cccc} T^{-1}V^{t-1}T & T^{-1}V^{t-2}T & \cdots & T^{-1}VT \quad I \end{array} \right] = \left[\begin{array}{cccc} (A^{t-1})' & (A^{t-2})' & \cdots & A' \quad I \end{array} \right], \qquad (5)$$

where all the components $A^m = T \cdot V^m \cdot T^{-1}$ of H are circulant matrices whose defining polynomials are given in (2). A similar result was obtained by Solomon and van Tilborg in [13]. Decoding of such a code is discussed in Section IV.

III. FOURIER ANALYSIS AND SYNTHESIS OF DOUBLE-CIRCULANT CODES

Let C be an $[n = 2r, k = r]$ double-circulant code over $F = GF(q)$ with $(r, q) = 1$, generated by $G = [I \ A]$, where A is an $r \times r$ circulant matrix over F. Each codeword of C has the form $[\mathbf{u} \ \ \mathbf{u} \ A]$ for some $\mathbf{u} \in F^r$. Let $\rho_r(\hat{\mathbf{u}}) \triangleq \deg \gcd(\hat{u}(x), x^r - 1)$, that is, $\rho_r(\hat{\mathbf{u}})$ is the number of distinct r-th roots of unity in Φ which are zeros of $\hat{\mathbf{u}}$. Since the number of zero-components in $\mathbf{u} \in F^r$ equals to $\rho_r(\hat{\mathbf{u}})$, it follows that the minimum distance d of C is given by

$$d \ = \ 2r \ - \ \max_{\substack{\hat{\mathbf{u}} = \mathbf{u}\,T \\ \mathbf{u} \in F^r - \{\mathbf{0}\}}} \ \{ \ \rho_r(\hat{\mathbf{u}}) + \rho_r(\hat{\mathbf{u}} * \hat{\mathbf{a}}) \ \} \ , \qquad (6)$$

where $\mathbf{a}$ is the defining polynomial of A.

We consider first $[n = 2r, k = r]$ double-circulant codes over $F = GF(q)$ with $(r, q) = 1$, defined by $\mathbf{a}$ such that $\hat{\mathbf{a}} \in F^r$. Such codes will be called *base-field-transform* (or, in short, *F-transform*) *codes*. Since $\mathbf{a}$ is a vector over F, the entries of $\hat{\mathbf{a}}$ must obey the so-called *Mattson-Solomon condition* $\hat{a}_{iq} = (\hat{a}_i)^q$, $0 \le i \le r - 1$, and, therefore, the values $\hat{a}_i$ must be constant along indices i belonging to the same cyclotomic coset modulo r.

Theorem 1. *Let C be an F-transform code over $F = GF(q)$ with $\hat{\mathbf{a}}$ being the Fourier transform of the defining polynomial of C. For any $\varepsilon \in F - \{0\}$, let s be the longest cyclic run of ε in $\hat{\mathbf{a}}$, and let t be the longest cyclic run of elements of $F - \{\varepsilon\}$ in $\hat{\mathbf{a}}$. Then the minimum distance d of C satisfies*

$$d \geq \min \{ s+1, 2t+2 \} . \tag{7}$$

Proof. Let $\hat{\mathbf{a}}$ be of the form

$$\mathbf{a}\, T = \hat{\mathbf{a}} = [\cdots , \varepsilon \underbrace{\varepsilon \cdots \varepsilon}_{\leftarrow s \rightarrow} , \underbrace{\cdots}_{\leftarrow l \rightarrow} , \omega_1 \, \omega_2 \cdots \omega_t , \underbrace{\cdots}_{\leftarrow m \rightarrow}] \in F^r ,$$

where $\omega_i \neq \varepsilon$ for all $1 \leq i \leq t$. Denote by $\rho_r(\hat{\mathbf{u}}, \hat{\mathbf{v}})$ the number of distinct r-th roots of unity in Φ which are zeros of both $\hat{u}(x)$ and $\hat{v}(x)$. Clearly,

$$\rho_r(\hat{\mathbf{u}}) + \rho_r(\hat{\mathbf{v}}) \leq r + \rho_r(\hat{\mathbf{u}}, \hat{\mathbf{v}}) . \tag{8}$$

Let $\mathbf{c} = [\mathbf{u} \;\; \mathbf{u} \;\; A]$. If $\varepsilon\hat{\mathbf{u}} \neq \hat{\mathbf{u}} * \hat{\mathbf{a}} = \hat{\mathbf{v}}$, we have

$$\rho_r(\hat{\mathbf{u}}, \hat{\mathbf{u}} * \hat{\mathbf{a}}) \leq \deg \{ [x^{l+t+m} \cdot (\varepsilon\hat{u}(x) - \hat{v}(x))] \bmod (x^r - 1) \} \leq r - 1 - s ,$$

which, together with (8) yields

$$\rho_r(\hat{\mathbf{u}}) + \rho_r(\hat{\mathbf{u}} * \hat{\mathbf{a}}) \leq 2r - 1 - s . \tag{9}$$

On the other hand, if $\varepsilon\hat{\mathbf{u}} = \hat{\mathbf{u}} * \hat{\mathbf{a}} \neq \mathbf{0}$, $\hat{\mathbf{u}}$ must have zeros in the t positions occupied in $\hat{\mathbf{a}}$ by the ω_i and, consequently,

$$\rho_r(\hat{\mathbf{u}}) + \rho_r(\hat{\mathbf{u}} * \hat{\mathbf{a}}) = 2\rho_r(\hat{\mathbf{u}}) \leq 2 \deg \{ (x^m \cdot \hat{u}(x)) \bmod (x^r - 1) \} \leq 2(r - 1 - t) . \tag{10}$$

By (6),(9) and (10) it follows that $d \geq \min \{s+1, 2t+2\}$. □

By Theorem 1, we can obtain F-transform codes with high lower bounds on their minimum distance by assigning values of F to the cyclotomic cosets modulo r so that the runs of ε and non-ε values will be as large as possible with the appropriate ratio of 2:1 between s and t, as reflected in (7).

Theorem 1 resembles the well-known BCH bound. As a matter of fact, the decoding procedure for F-transform codes up to the *designed distance*, given by the right-hand side of (7), is as easy as that for BCH codes. Assume s is even, so that the designed distance is at least $2\tau+1$, where $\tau \triangleq \min\{s/2, t\}$. We now show how to correct τ errors. Suppose a codeword $\mathbf{c} = [\mathbf{u}\ \ \mathbf{u}\ A]$ is transmitted and the word

$$\mathbf{y} = \mathbf{c} + \mathbf{e} = [\mathbf{u} + \mathbf{e}_1 \quad \mathbf{u}\ A + \mathbf{e}_0] = [\mathbf{y}_1\ \ \mathbf{y}_0]$$

is received, with the error word $\mathbf{e}$ having weight $\le \tau$. Since $\varepsilon\hat{\mathbf{u}} - (\hat{\mathbf{u}} * \hat{\mathbf{a}})$ contains s consecutive zeros, we may regard $\varepsilon\mathbf{u} - \mathbf{u}A$ as a codeword of a BCH code of length r and designed distance $s+1$. Applying the standard BCH decoding technique to $\varepsilon\mathbf{y}_1 - \mathbf{y}_0$ yields the vector $\tilde{\mathbf{e}} \triangleq \varepsilon\mathbf{e}_1 - \mathbf{e}_0$ of weight $\le s/2$ [4, Ch. 9]. Denote by $\Theta(\mathbf{v})$ the support of a vector $\mathbf{v}$ and by $\mathrm{w}(\mathbf{v}) \triangleq |\Theta(\mathbf{v})|$ its Hamming weight. Define $Y \triangleq \Theta(\tilde{\mathbf{e}})$ and $Z \triangleq \Theta(\mathbf{e}_1) - Y = \Theta(\mathbf{e}_0) - Y$. That is, Z is the set of coordinates in which the nonzero entries of $\varepsilon\mathbf{e}_1$ and $\mathbf{e}_0$ are identical. We have,

$$|Y| + 2|Z| \le \mathrm{w}(\mathbf{e}) \le \tau \le t\ .$$

Having found $\tilde{\mathbf{e}}$, we know the set Y and the vector $\varepsilon\hat{\mathbf{u}} - (\hat{\mathbf{u}} * \hat{\mathbf{a}})$, by which we obtain t consecutive values of $\hat{\mathbf{u}}$ and, hence, of $\hat{\mathbf{e}}_1$. Therefore, we may apply this information and the BCH decoding algorithm to $\hat{\mathbf{y}}_1$ to correct $|Y|$ *erasures* and $|Z| \le \frac{1}{2}(t - |Y|)$ errors [4, §9.2], thus retrieving $\mathbf{e}_1$ and, subsequently, $\mathbf{u}$.

Example 1. The following is an example of an F-transform code over $GF(2)$ with $s = 2^{h/2+1} - 2$ and $t = 2^{h/2} - 1$. Let $r = 2^h - 1$, h even, resulting in a $[2^{h+1} - 2,\ 2^h - 1]$ double-circulant code C. For an integer i, $0 \le i \le 2^h - 2$, denote by $\mathbf{i} = [i_{h-1}\ i_{h-2} \cdots i_0]$ the base-2 representation of i. Let Ω_i be the cyclotomic coset modulo $2^h - 1$ containing i. Then Ω_i contains all integers j such that $\mathbf{j}$ is a cyclic shift of $\mathbf{i}$. Let $s = 2^{h/2+1} - 2$ and assign $\hat{a}_j = 1$ for all $j \in \Omega_i$, $1 \le i \le s$. Here, $\mathrm{w}(\mathbf{j}) \le h/2$ and so the largest index $j_{\max}$ for which $\hat{a}_{j_{\max}} = 1$ is given by

$$\mathbf{j}_{\max} = [\underbrace{1\,1\cdots1}_{\leftarrow\ h/2\ \rightarrow}\ \underbrace{0\,0\cdots0}_{\leftarrow\ h/2\ \rightarrow}]\ ,$$

i.e., $j_{\max} = 2^h - 2^{h/2}$. Hence, we may set $\hat{a}_j = 0$ for all $2^h - 2^{h/2} + 1 \le j \le 2^h - 2$ and for $j = 0$. Thus we have $t \ge 2^{h/2} - 1$, which implies

$$d \ge 2^{h/2+1} - 1 = 2\sqrt{r+1} - 1 .$$

Example 2. We show now how a code of Example 1 can be extended into a $[2^{h+1}, 2^h, 2^{h/2+1}]$ code. Consider the affine space

$$\tilde{C} = \{ [\mathbf{u} \quad \mathbf{u}\, A + \mathbf{1}] \mid \mathbf{u} \in F^r \} ,$$

where A corresponds to the F-transform code C of Example 1 and $\mathbf{1}$ is the all-one r-vector. Note that $\mathbf{1} \cdot T = [1\ 0\ 0 \cdots 0]$ and, therefore, the Fourier transform of $\mathbf{v} = \mathbf{u}A$ and $\mathbf{v} + \mathbf{1}$ are identical except for the first entry $\hat{v}_0$. By arguments similar to those in Example 1, we conclude that the weight of each word in $\tilde{C}$ is lower-bounded by $2^{h/2+1} - 2$. Since $\hat{a}_0 = 0$, $\mathbf{a}$ has even weight and, so, the $[2^{h+1}, 2^h]$ *bordered* double-circulant code, generated by

$$G = \begin{bmatrix} & & \mathbf{1} & 0 \\ & I & & \\ & & A & \mathbf{1}' \end{bmatrix},$$

must have even minimum distance $\ge 2^{h/2+1} - 1$, i.e., $d \ge 2^{h/2+1}$.

For instance, $h = 2$ yields a $[6, 3, 3]$ double-circulant code with $\mathbf{a} = [0\ 1\ 1]$ and the corresponding bordered double-circulant code is the $[8, 4, 4]$ self-dual extended Hamming code. For $h = 4$ we obtain a $[32, 16, 8]$ bordered double-circulant code with $\mathbf{a} = [0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1]$.

Remark 1. The bound $d \ge 2^{h/2+1}$ applies also to the $[2^{h+1}, 2^h]$ binary Reed-Muller code $\mathrm{RM}(\frac{h}{2}, h+1)$ of order $\frac{h}{2}$ [2, §15.3], although the two code families are not equivalent; the weights of the codewords in $\mathrm{RM}(\frac{h}{2}, h+1)$ are multiples of 4 [11, p. 447], whereas the $[32, 16, 8]$ bordered F-transform code of Example 2 contains codewords of weights 10, 14, 18 and 22. However, there exists a close relationship between (bordered) F-transform codes and Reed-Muller codes. As a special case of Example 1, we can assign $\hat{a}_j = 1$ for all j where $1 \le \mathrm{w}(\mathbf{j}) \le h/2$, and $\hat{a}_j = 0$ otherwise. In this manner we can use a majority-logic decoder of the

punctured Reed-Muller code RM$(\frac{h}{2}-1, h)^*$ [11, p. 377] as the first decoding step, and then an erasure-and-error decoder of RM$(\frac{h}{2}, h)^*$ (enhanced by a parity bit corresponding to $\hat{a}_0 = 0$) as the second decoding step.

Remark 2. The bound $2\sqrt{r+1}-1$ is attainable also for general q and even h with $r = q^h - 1$. For odd h, one can readily verify the bound $d \geq q^{\frac{1}{2}(h+1)} - O(q)$.

We turn now to the more general case where $\hat{\mathbf{a}}$ is not necessarily in F^r.

Theorem 2. *Let C be an $[n = 2r, k = r]$ double-circulant code over $F = GF(q)$, $(r, q) = 1$, with $\hat{\mathbf{a}}$ being the Fourier transform of the defining polynomial of C. Let s be the longest cyclic run of any element $\varepsilon \notin F$ in $\hat{\mathbf{a}}$. Then the minimum distance d of C satisfies $d \geq s+1$.*

Proof. Consider the vector $\hat{\mathbf{v}} = \varepsilon\hat{\mathbf{u}} - (\hat{\mathbf{u}} * \hat{\mathbf{a}})$, corresponding to some input vector $\mathbf{u} \in F^r$. Clearly, $\hat{\mathbf{v}}$ contains a run of s zeros. Furthermore, if $\mathbf{u} \neq \mathbf{0}$, we must have $\mathbf{v} \neq \mathbf{0}$, or else $\hat{u}_i = 0$ for all i such that $\hat{a}_i \neq \varepsilon$ and, in particular, when $\hat{a}_i = \varepsilon^q \triangleq \omega$. By the Mattson-Solomon condition on $\hat{\mathbf{u}}$, this requires $\hat{u}_i = 0$ also when $\hat{a}_i = \varepsilon$, i.e., $\hat{\mathbf{u}} = \mathbf{0}$. Therefore, the weight of $\mathbf{v}$, and hence that of $[\mathbf{u} \;\; \mathbf{u}\; A]$, is at least $s+1$ for all $\mathbf{u} \neq \mathbf{0}$. □

In the special case of $q = 2$, the lower bound of Theorem 2 can be improved to $d \geq s+2$ if s is even and $\hat{a}_0 = 1$, as the latter implies an even minimum distance for C.

Like the case of F-transform codes, the above proof suggests a decoding procedure up to the designed distance $s+1$. Note that a run of s ε's in $\hat{\mathbf{a}}$ implies the existence of a sequence

$$\hat{a}_m = \hat{a}_{m+q} = \hat{a}_{m+2q} = \cdots = \hat{a}_{m+(s-1)q} = \varepsilon^q \triangleq \omega$$

for some m and, so, given a received word $[\mathbf{y}_1 \;\; \mathbf{y}_0]$, $\mathbf{y}_1 = \mathbf{u} + \mathbf{e}_1$ and $\mathbf{y}_0 = \mathbf{u}\; A + \mathbf{e}_0$, we can apply the BCH decoding algorithm to both $\varepsilon\mathbf{y}_1 - \mathbf{y}_0$ and $\omega\mathbf{y}_1 - \mathbf{y}_0$ to obtain $\varepsilon\mathbf{e}_1 - \mathbf{e}_0$ and $\omega\mathbf{e}_1 - \mathbf{e}_0$, and then solve for $\mathbf{e}_1$.

Exploiting the condition of Theorem 2, we try to obtain an $\hat{\mathbf{a}}$ with long runs of elements of $\Phi - F$ by limiting the number of distinct elements of this kind (say, only two of them) in $\hat{\mathbf{a}}$. Let $F = GF(q)$ and assume that the multiplicative order h of q modulo r is even. With each cyclotomic coset

$$\Omega_i = \{ (q^j \cdot i) \bmod r \}_j$$

of even size we associate two *quadratic cosets*

$$\Omega_i^e = \{ (q^{2j} \cdot i) \bmod r \}_j$$

and

$$\Omega_i^o = \{ (q^{2j+1} \cdot i) \bmod r \}_j ,$$

each of half the size of Ω_i. Ω_i^e and Ω_i^o are called *conjugate* quadratic cosets, corresponding to the cyclotomic coset Ω_i.

Let $K = GF(q^2)$, let $\varepsilon \in K - F$, and let $\omega = \varepsilon^q$. A *quadratic assignment* $f : \{ 0, 1, \cdots, r-1 \} \rightarrow \{ \varnothing, \varepsilon, \omega \}$ of the ring modulo r over $GF(q)$ is an assignment of the two elements ε and ω to the quadratic cosets such that conjugate quadratic cosets have distinct assignments. Elements which do not belong to any quadratic coset (i.e., elements from cyclotomic cosets of odd size) are assigned the "don't care" mark $\varnothing$ (e.g., $f(0) = \varnothing$).

An example of a quadratic assignment of the ring modulo 17 over $GF(2)$ is given by

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varnothing$	ε	ω	ε	ε	ε	ω	ω	ω	ω	ω	ω	ε	ε	ε	ω	ε

where the quadratic cosets are $\Omega_1^e = \{1, 4, 13, 16\}$, $\Omega_1^o = \{2, 8, 9, 15\}$, $\Omega_3^e = \{3, 5, 12, 14\}$, and $\Omega_3^o = \{6, 7, 10, 11\}$.

A *quadratic-field-transform* (*K-transform*) *code* C over $F = GF(q)$, generated by $G = [I \; A]$, is a $[2r, r]$ double-circulant code, $(r, q) = 1$, defined as follows. Let the order h of q modulo r be even, let $\Phi = GF(q^h)$, and let $f : \{ 0, 1, \cdots, r-1 \} \rightarrow \{ \varnothing, \varepsilon, \omega \}$ be a quadratic assignment of the ring modulo r (note that $\varepsilon, \omega \in \Phi$). The Fourier transform $\hat{\mathbf{a}}$ of the defining

polynomial of A is given by $\hat{a}_i = f(i)$ if $f(i) \in \{\varepsilon, \omega\}$ and $\hat{a}_i \in F$ if $f(i) = \varnothing$ (satisfying the Mattson-Solomon condition).

Example 3. While trying to construct K-transform codes over $GF(2)$ it transpires that Theorem 2 is most effective for values of r which are Fermat primes, i.e., primes of the form $r = 2^{2^m} + 1$. When this is the case, the following runs can be obtained (compare with the example of $r = 17$):

n	r	s	$d \geq$
10	5	2	4
34	17	6	8
514	257	28	30
131074	65537	508	510

For $r = 5$ and $r = 17$ the corresponding codes have the maximal possible minimum distance for the given rate (one half) and dimensions.

Remark 3. There exist known K-transform constructions for which the bound of Theorem 2 is far from the true minimum distance. One example of such a construction is the family of $[2p, p]$ double-circulant codes over $GF(2)$, with p being a prime such that 2 is a quadratic non-residue in $GF(p)$, and the defining polynomial of A is given by

$$a(x) = 1 + \sum_{l=1}^{(p-1)/2} x^{(l^2 \bmod p)}$$

[11, p. 507]. It can be verified that the resulting code is, indeed, a K-transform code. The lower bound of Theorem 2 is equal to one plus the maximal number of consecutive quadratic residues (or non-residues) modulo p, which is quite a poor bound as this number is conjectured to be $O(\log^2 p)$ [1]. On the other hand, Calderbank [6] has proved a square-root bound of $\sqrt{2p} + O(1)$ on the minimum distance of these codes (a similar gap exists between the BCH bound and a square-root bound on the minimum distance of quadratic-residue codes [11, Ch. 16]).

A possible generalization of double-circulant codes is the family of codes having a generator matrix of the form $[I \; A_1 \; A_2 \cdots A_{m-1}]$, where the A_i are circulant matrices, or the family of

codes having a parity-check matrix of this form [14]. In the next section we discuss such a family of MDS codes.

IV. SYSTEMATIC DECODING OF REED-SOLOMON CODES

A. ENCODING AND SYNDROME EVALUATION

We describe now the decoding process of $[n, n-r]$ RS codes over $F = GF(q)$ with parity check matrices of the form (5). We assume first that $n \mid q-1$ and that $n = r \cdot t$, and we shall show later on how the proposed algorithm may be applied while allowing relaxation of these requirements.

Let $\mathbf{y} \in F^n$ be a received word. Partitioning $\mathbf{y}$ into

$$\mathbf{y} = \left[\mathbf{y}_{t-1}\ \mathbf{y}_{t-2} \cdots \mathbf{y}_1\ \mathbf{y}_0\right],$$

where each $\mathbf{y}_m$ is a block of length r, we can express the syndrome $\mathbf{s} = [s_0\ s_1 \cdots s_{r-1}] = \mathbf{y}H'$ as a polynomial in A,

$$\mathbf{s} = \sum_{m=0}^{t-1} \mathbf{y}_m A^m ,$$

which can be computed by the following Horner-like procedure *SYNDROME*.

procedure *SYNDROME*$(\mathbf{y})$ **output: s ;**

begin

$\mathbf{s} \leftarrow \mathbf{y}_{t-1}$**;**

for $m \leftarrow t-1$ **downto** 1 **do**

$\mathbf{s} \leftarrow \mathbf{y}_{m-1} + \mathbf{s}\ A$

end

Since A is a circulant matrix, $\mathbf{s}\,A$ can be viewed as the product of the polynomials $s(x) = \sum_{i=0}^{r-1} s_i x^i$ and $\sum_{i=0}^{r-1} a_i x^i$ modulo $x^r - 1$. Performing t such multiplications requires n shift steps of an r-tap shift-register. Note that the time required for *serial* multiplication is of the same order of magnitude (at least $t \cdot r \cdot \log r = n \cdot \log r$ operations) as that for the frequency-domain syndrome evaluation using the Fast Fourier Transform. Thus, the benefit of the proposed decoding procedure lies in the hardware scheme rather than in the sequential mode.

A systematic generator matrix of C is given by

$$G = \begin{bmatrix} & & -A^{t-1} \\ & & -A^{t-2} \\ & I & \cdot \\ & & -A^2 \\ & & -A \end{bmatrix}.$$

Given an input information word

$$\mathbf{u} = \left[\mathbf{u}_{t-1}\ \mathbf{u}_{t-2} \cdots \mathbf{u}_1\right],$$

where each $\mathbf{u}_i$ is a block of length r, the corresponding codeword takes the form

$$\mathbf{c} = \left[\mathbf{u}_{t-1}\ \mathbf{u}_{t-2} \cdots \mathbf{u}_1\ \mathbf{c}_0\right],$$

where the check symbols are given by

$$\mathbf{c}_0 = -\sum_{m=1}^{t-1} \mathbf{u}_m A^m\ .$$

Since the code is represented in a systematic form, the check symbols can be evaluated by the same scheme as the syndrome, where $\mathbf{y}$ is replaced by the input $[-\mathbf{u}\ \mathbf{0}\ ]$ (of length $n = r \cdot t$).

B. ERROR LOCATIONS AND VALUES

We turn now to the error locator polynomial $\Lambda(x)$. Using the notation defined in (4), let $y_{m,j}$ denote the $< m, j >$-th entry in $\mathbf{y}$, $0 \le m \le t-1$, $0 \le j \le r-1$. Given that $\tau \le \frac{r}{2}$ errors have

occurred at locations $\{ < m_i, j_i > \}_{i=1}^{\tau}$, $\Lambda(x)$ is defined by

$$\Lambda(x) = \sum_{i=0}^{\tau} \Lambda_i x^i = 1 + \sum_{i=1}^{\tau} \Lambda_i x^i = \prod_{i=1}^{\tau} (1 - x \cdot \delta^{m_i} \beta^{j_i}) . \qquad (11)$$

Recall that α is an element of order n, $\beta = \alpha^t$ is an element of order r, and $\delta = \alpha^b$ with $(b, t) = 1$. Regarding the coefficients of $\Lambda(x)$ as an r-vector Λ over F (with $r - \tau - 1$ trailing zeros), we denote by λ_0 its r-dimensional inverse Fourier transform, i.e.,

$$\lambda_{0,j} = \frac{1}{r} \Lambda(\beta^{-j}), \quad 0 \le j \le r - 1 .$$

Following [5], we transform the Berlekamp-Massey decoding algorithm using an r-dimensional transform into the time domain, resulting in the procedure *ELP* below. In this procedure we make use of an auxiliary r-vector **b**, which is the inverse Fourier transform of the polynomial $B(x)$, denoting the error locator polynomial prior to the last update of the recursion length L [12].

procedure $ELP(\mathbf{s})$ **output:** λ_0 **;**

begin **{** λ_0 **obtained is up to a multiplying scalar** r **}**

λ_0, $\mathbf{b} \leftarrow \mathbf{1}$ **{ all-one vector } ;** $L \leftarrow 0$ **;**

for $N \leftarrow 0$ **to** $r - 1$ **do begin { main loop }**

$\Delta \leftarrow \sum_{j=0}^{r-1} \beta^{jN} \lambda_{0,j} s_j$ **;**

if $\Delta \neq 0$ **and** $2L \le N$ **then begin**

$L \leftarrow N + 1 - L$ **;**

$\mathbf{U}_0 \leftarrow [1 \;\; \Delta^{-1}]$ **;** $\mathbf{U}_1 \leftarrow [-\Delta \;\; 0]$ **end**

else begin

$\mathbf{U}_0 \leftarrow [1 \;\; 0]$ **;** $\mathbf{U}_1 \leftarrow [-\Delta \;\; 1]$ **end;**

for $j \leftarrow 0$ **to** $r-1$ **do begin**

{ error evaluator polynomial will be inserted here }

$[\lambda_{0,j}\ b_j] \leftarrow \lambda_{0,j}\mathbf{U}_0 + b_j\beta^{-j}\mathbf{U}_1$ **end**

end { main loop }

end

It is easy to see that $\lambda_{0,j} = 0$ if and only if the j-th entry in $\mathbf{y}_0$, $0 \le j \le r-1$, is erroneous. These coordinates correspond to the check symbols of the received word ($m = 0$). In order to obtain the other error locations, we find the n-dimensional inverse Fourier transform of Λ (now appended with $n-r$ zero coordinates) by *interpolation*: we use λ_0 to find the values of $\Lambda(x)$ at points $x = \delta^{-m}\beta^{-j}$. Define

$$\lambda_{m,j} = \frac{1}{r}\Lambda(\delta^{-m}\beta^{-j}), \quad 0 \le j \le r-1, \quad 0 \le m \le t-1.$$

Then, up to a permutation π of coordinates (as given in (4)) and a scaling factor n/r,

$$\lambda = \left[\lambda_{t-1}\ \lambda_{t-2} \cdots \lambda_1\ \lambda_0\right]$$

is the n-dimensional inverse Fourier transform of Λ and we have $\lambda_{m,j} = 0$ if and only if $y_{m,j}$ is erroneous.

Let S be the $r \times r$ circulant (permutation) matrix defined by $S_{0,1} = 1$ and $S_{0,j} = 0$ for all $j \neq 1$. It is easy to verify that for $\mathbf{v} \in F^r$, $\mathbf{v}S$ is a right cyclic shift of $\mathbf{v}$ and that $A^t = S^b$. We also have,

$$\lambda_m = \Lambda V^{-m}T^{-1} = \lambda_0 T V^{-m}T^{-1} = \lambda_0 A^{-m}, \quad 0 \le m \le t-1.$$

Thus, by shifting the contents of λ_0 cyclically, we can obtain the initial vector $\lambda_t \triangleq \lambda_0 S^{-b}$, from which we compute λ_m iteratively using the formula

$$\lambda_m = \lambda_{m+1} A\,, \quad m = t-1,\, t-2, \cdots, 1\,, \tag{12}$$

and reusing the same memory of size r. Note that the λ_m can be evaluated by the syndrome circuit, now used to perform $t-1$ multiplications by A. Furthermore, if $(r,t)=1$, we can choose $b=r$, in which case $\lambda_t = \lambda_0$.

The standard computation of the n-dimensional error vector **e** employs the error evaluator polynomial which, using the notation of (11), is defined by

$$\Gamma(x) \;=\; \sum_{i=0}^{\tau-1} \Gamma_i x^i \;=\; \sum_{i=1}^{\tau} e_{m_i,j_i} \prod_{l \neq i} (1 - x \cdot \delta^{m_l} \beta^{j_l})\,.$$

Let $\Lambda'(x)$ denote the x-derivative of $\Lambda(x)$ and define $M(x) \triangleq x\Lambda'(x)$; it is known that [11, Ch. 8, §6]

$$e_{m_i,j_i} = -\,\frac{\Gamma(\delta^{-m_i}\beta^{-j_i})}{M(\delta^{-m_i}\beta^{-j_i})}\,, \quad 1 \le i \le \tau\,.$$

Now let $\gamma = [\gamma_{t-1}\ \gamma_{t-2} \cdots \gamma_0]$ and $\mu = [\mu_{t-1}\ \mu_{t-2} \cdots \mu_0]$ denote the permuted n-dimensional inverse Fourier transforms of Γ and **M**, i.e., the n-dimensional interpolations of γ_0 and μ_0, respectively. The error values $e_{m,j}$ are then given by

$$e_{m,j} \;=\; \begin{cases} -\,\dfrac{\gamma_{m,j}}{\mu_{m,j}} & \text{if } \lambda_{m,j} = 0 \\ 0 & \text{otherwise} \end{cases}\,, \quad 0 \le j \le r-1\,, \quad 0 \le m \le t-1\,.$$

It remains to evaluate both γ and μ. Following the example of λ, we first calculate γ_0 and μ_0 and then interpolate as in (12). Like in [5], we introduce two auxiliary r-vectors σ and η, the latter standing for the r-dimensional inverse Fourier transform of $x \cdot B'(x)$. We incorporate the evaluation of γ_0 and μ_0 into *ELP* by adding the statements

$$[\mu_{0,j}\ \eta_j] \leftarrow \mu_{0,j}\mathbf{U}_0 + (b_j + \eta_j)\beta^{-j}\mathbf{U}_1\,; \quad [\gamma_{0,j}\ \sigma_j] \leftarrow \gamma_{0,j}\mathbf{U}_0 + \sigma_j\beta^{-j}\mathbf{U}_1\,;$$

in the indicated position, with the initial conditions $\gamma_0 \leftarrow \mathbf{1}$ and μ_0, η, $\sigma \leftarrow \mathbf{0}$. The resulting augmented procedure is called *ELP**.

Since encoding, syndrome calculation, and computation of the error locator polynomial are executed at different times, the same pieces of hardware can be used in all these procedures. We shall refer to this unit as the Encoding-Syndrome-Interpolation Circuit (in short, *ESIC*), consisting of an r-tap cyclic convolution (in particular, *ESIC* realizes *SYNDROME*). Also, μ_m and γ_m can be multiplexed with λ_m after each block of r symbols.

To summarize, the encoding-decoding hardware consists of the following registers of length r: register $\mathbf{c}_0/\mathbf{s}$ (used for the generation of check symbols in encoding, syndrome computation in decoding); registers λ_m (error locator polynomial), γ_m (error evaluator polynomial), and μ_m — all connected to *ESIC* — along with the auxiliary registers **b**, η, and σ. The external input to *ESIC* is multiplexed among the information vector [**–u 0**], the received word **y**, and a zero vector **0**. Once the syndrome has been calculated by *ESIC*, these seven registers pass r phases of update by ELP^* (N being the phase counter), after which *ESIC* is invoked again to generate the values of λ, γ and μ.

The foregoing discussion remains practically unchanged when we relax our requirements for β and δ so that β is any element of order r in F, $n = r \cdot t \leq q-1$, and $\delta \in F - \{0\}$ is such that $\delta^{rm} \neq 1$ for all $1 \leq m \leq t-1$ (say, δ is a primitive element of F). This generalization affects the decoding procedure only in that A^t is no longer necessarily the shift operator and, therefore, λ_t cannot always be calculated as indicated. Instead, we can use the recursion $\lambda_{m+1} = \lambda_m A^{-1}$, where A^{-1} is a circulant matrix as before, thus entailing only a change in the defining polynomial **a** in *ESIC*.

C. APPLICATION TO DOUBLE-CIRCULANT REED-SOLOMON CODES

Considerable simplification of the proposed decoding scheme can be achieved in the special case where C is a double-circulant code, that is, $n = 2r$ and $H = [\, A' \;\; I \,]$. In this case, with only the information symbols needing correction, it is more convenient to assume generator matrices of the form

$$\bar{G} = \left[\; -A^{-1} \;\; I \; \right], \tag{13}$$

(with the information word **u** occupying the *last r* coordinates) since now the interpolation step becomes unnecessary.

This special case can also be approached in a different manner, starting with a "weighted average" estimation of the information word, followed by a succession of estimations of the error pattern, and terminating with the correct transmitted information symbols. In such a scheme we shall need just the registers $\mathbf{c}_0/\mathbf{s}$, λ_0, and **b**. This approach is based on the first scheme presented in [5].

Given a received word $[\mathbf{y}_1 \;\; \mathbf{y}_0] = [-\mathbf{u}\, A^{-1} + \mathbf{e}_1 \quad \mathbf{u} + \mathbf{e}_0]$, let

$$\hat{\mathbf{s}} \triangleq \mathbf{e}_0 T + \mathbf{e}_1 TV \tag{14}$$

be the r-dimensional Fourier transform of the syndrome **s**, let

$$\hat{\mathbf{w}} \triangleq \mathbf{e}_0 T + \mathbf{e}_1 TV\delta^r \; , \tag{15}$$

and let $\mathbf{E} = [E_0 \; E_1 \cdots E_{n-1}] \triangleq [\hat{\mathbf{s}} \;\; \hat{\mathbf{w}}]$. It is easy to verify that when $\delta^n = 1$, **E** is the n-dimensional Fourier transform of **e**. However, here we assume the general case where δ is any nonzero element of F such that $\delta^r \neq 1$.

Defining $\theta \triangleq 1/(1-\delta^r)$ and applying the inverse Fourier transform on (14)-(15), we obtain

$$\mathbf{e}_0 = \theta \cdot \mathbf{w} + (1-\theta) \cdot \mathbf{s} \; .$$

To complete the decoding, it remains to evaluate **w**. It is well known [11, Ch. 12, §9][12] that $\Lambda(x) = \sum_{i=0}^{\tau} \Lambda_i x^i$ is the characteristic polynomial of the linear recurrence satisfied by the E_i, namely,

$$E_i + \sum_{l=1}^{\tau} \Lambda_l E_{i-l} = 0 \; , \quad 0 \le i \le n-1 \; . \tag{16}$$

Transforming (16) into the time domain and using the convolution property, we obtain the following procedure *MAIN_LOOP* for the evaluation of **w** (compare with the **main loop** of *ELP*).

procedure *MAIN_LOOP*(**s**, λ_0) **output: w ;**

begin

w $\leftarrow$ **s ;**

for $N \leftarrow 0$ **to** $r-1$ **do begin { main loop }**

$\Delta \leftarrow \sum_{j=0}^{r-1} \beta^{jN} \lambda_{0,j} w_j$ **;**

for $j \leftarrow 0$ **to** $r-1$ **do**

$w_j \leftarrow w_j - \Delta \cdot \beta^{-jN}$

end

end

The corrected information vector $\tilde{\mathbf{u}}$ is given by

$$\tilde{\mathbf{u}} \;=\; \mathbf{y}_0 - \mathbf{e}_0 \;=\; \mathbf{y}_0 - \theta \cdot \mathbf{w} - (1-\theta)\cdot \mathbf{s} \;=\; \theta \cdot \mathbf{y}_0 - (1-\theta)\cdot \mathbf{y}_1 A - \theta \cdot \mathbf{w} \;\stackrel{\Delta}{=}\; \tilde{\mathbf{y}}_0 - \tilde{\mathbf{e}}\,,$$

where $\tilde{\mathbf{y}}_0 = \theta \cdot \mathbf{y}_0 + (1-\theta)\cdot(-\mathbf{y}_1 A)$ and $\tilde{\mathbf{e}} = \theta \cdot \mathbf{w}$. Note that $\tilde{\mathbf{y}}_0$ may be regarded as an *initial estimate* for **u**, obtained by a "weighted average" of $\mathbf{y}_0$ and $-\mathbf{y}_1 A$, where these two vectors must equal the transmitted information vector **u** if no errors have occurred.

Defining $\tilde{\mathbf{s}} \stackrel{\Delta}{=} \theta \cdot \mathbf{s} = \dfrac{\theta}{1-\theta}(\mathbf{y}_0 - \tilde{\mathbf{y}}_0)$, the *estimation error*, we obtain the following procedure for evaluating $\tilde{\mathbf{u}}$:

procedure $AVERAGE\_DECODER([\mathbf{y}_1 \quad \mathbf{y}_0])$ **output:** $\tilde{\mathbf{u}}$ **;**

begin

Evaluate $\tilde{\mathbf{y}}_0 \leftarrow \theta \cdot \mathbf{y}_0 + (1-\theta) \cdot (-\mathbf{y}_1 A)$ **(by** $ESIC$**) and** $\tilde{\mathbf{s}} \leftarrow \dfrac{\theta}{1-\theta}(\mathbf{y}_0 - \tilde{\mathbf{y}}_0)$ **;**

$\lambda_0 \leftarrow ELP(\tilde{\mathbf{s}})$ **;**

$\tilde{\mathbf{e}} \leftarrow MAIN\_LOOP(\tilde{\mathbf{s}}, \lambda_0)$ **;**

$\tilde{\mathbf{u}} \leftarrow \tilde{\mathbf{y}}_0 - \tilde{\mathbf{e}}$

end

When q is odd and $\delta^n = 1$, we have $\theta = 1/2$, in which case $\tilde{\mathbf{y}}_0$ and $\tilde{\mathbf{s}}$ become $\tilde{\mathbf{y}}_0 = \dfrac{1}{2}(\mathbf{y}_0 - \mathbf{y}_1 A)$ and $\tilde{\mathbf{s}} = \mathbf{s} = \mathbf{y}_0 - \tilde{\mathbf{y}}_0$.

D. CONCLUDING REMARKS

The encoding-decoding procedure presented here can be summarized as follows:

Encoding:

* Evaluate the check symbols for the given information word using *ESIC*.

Decoding:

* Evaluate the time-domain syndrome using *ESIC*.
* Find the error locator polynomial and the error evaluator polynomial using *ELP*.
* Reusing *ESIC*, interpolate the outputs of *ELP* to obtain the error values.

Note:

(i) The decoding methods described here can be generalized to include erasures as well.

(ii) Given a field F and a code length n, the dependency of the logical circuit on r boils down to the choice of β and δ which, by (1), can be used to calculate the coefficients a_j.

(iii) If the redundancy r of the desired code does not divide n, a shortened version of the code C can be used: add a zero prefix to the information symbols (without transmitting it), thus resulting in a (generalized) Reed-Solomon code of lower rate and length $\tilde{n} \geq n$. Thus, any $[n, n-r]$ (generalized) RS code with $r \mid (q-1, \tilde{n})$ where $n \leq \tilde{n} \leq q-1$ can be decoded by the suggested scheme.

REFERENCES

[1] N.C. Ankeny, "The least quadratic non-residue", *Ann. of Math.,* 55, 1952, pp. 65-72.

[2] E.R. Berlekamp, *Algebraic coding Theory,* McGraw-Hill, New York, 1968.

[3] V.K. Bhargava, S.E. Tavares, S.G.S. Shiva, "Difference sets of the Hadamard type and quasi-cyclic codes", *Inform. Control*, 26, 1974, pp. 341-350.

[4] R.E. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley, Reading, Massachusetts, 1983.

[5] R.E. Blahut, "A universal Reed-Solomon decoder", *IBM J. Res. Develop.,* 28, 1984, pp. 150-158.

[6] R. Calderbank, "A square root bound on the minimum weight in quasi-cyclic codes", *IEEE Trans. Inform. Theory*, IT-29, 1983, pp. 332-337.

[7] C.L. Chen, W.W. Peterson, E.J. Weldon, Jr., "Some results on quasi-cyclic codes, *Inform. Control*, 15, 1969, pp. 407-423.

[8] C.W. Hoffner, II, S.M. Reddy, "Circulant bases for cyclic codes", *IEEE Trans. Inform. Theory,* IT-16, 1970, pp. 511-512.

[9] M. Karlin, "New binary coding results by circulants", *IEEE Trans. Inform. Theory,* IT-15, 1969, pp. 81-92.

[10] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", *IEEE Trans. Inform. Theory,* IT-20, 1974, p. 679.

[11] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[12] J.L. Massey, "Shift-register synthesis and BCH decoding", *IEEE Trans. Inform. Theory,* IT-15, 1969, pp. 122-127.

[13] G. Solomon, H.C.A. van Tilborg, "A connection between block and convolutional codes", *SIAM J. Appl. Math.,* 37, 1979, pp. 358-369.

[14] S.E. Tavares, V.K. Bhargava, S.G.S Shiva, "Some rate-$p/(p+1)$ quasi-cyclic codes", *IEEE Trans. Inform. Theory,* IT-20, 1974, pp. 133-135.