IBM Journal of research and development

Vol. 24, No. 1, January 1980

Shu Lin
George Markowsky

On a Class of One-Step Majority-Logic Decodable Cyclic Codes

ISSN 18-8646. Printed in U.S.A.

Shu Lin
George Markowsky

On a Class of One-Step Majority-Logic Decodable Cyclic Codes

Majority-logic decoding is attractive for three reasons: (1) It can be simply implemented; (2) the decoding delay is short; and (3) its performance, while suboptimal, is always superior to bounded distance decoding. For these reasons, majority-logic decodable cyclic codes are very suitable for error control in high speed digital data transmission systems. Among the majority-logic decodable codes, the one-step decodable codes can be most easily implemented; they employ a single majority-logic gate. In this paper we study a class of one-step majority-logic decodable cyclic codes. First, we describe these codes in a simple manner. Second, a way of finding the orthogonal polynomials for decoding these codes is presented. Third, we show that for a given error correction capability, the ratio of the number of parity digits to the code length goes to zero as the code length increases. For error correction capabilities of the form $2^k - 1$ or 2^k, we determine the dimensions of the codes exactly.

1. Introduction

Majority-logic decoding is attractive for three reasons: (1) It can be simply implemented; (2) the decoding delay is short; and (3) its performance, while suboptimal, is superior to bounded distance decoding [1]. For these reasons, majority-logic decodable cyclic codes are very suitable for error control in high speed digital data transmission systems. Among the majority-logic decodable codes, the one-step decodable codes can be most easily implemented, since they employ a single majority-logic gate [1-3]. In this paper, we study a class of one-step majority-logic decodable codes. This class of codes is a subclass of the generalized Euclidean geometry codes (which are not in general one-step majority-logic decodable) studied by Delsarte [4], Kasami and Lin [5], and Lin and Yiu [6]. First, we briefly describe the codes in a simple manner. Second, a method of finding the orthogonal polynomials (or orthogonal parity-sums) for decoding these codes is presented. Third, we show that for a given error correction capability, the ratio of the number of parity-check digits to the code length goes to zero as the code length increases. For error correction capabilities of the form $2^k - 1$ or 2^k, we determine the dimensions of the codes exactly. At the end, we present an example to illustrate the process of finding the orthogonal polynomials.

Since the decoding of these codes is based on the property that these codes, when extended by the addition of an overall parity-check digit, are invariant under the affine group of permutations, we give a brief discussion of this invariant property here.

Let C be a binary cyclic code of length $n = 2^m - 1$, generated by the polynomial $\mathbf{g}(X)$. Let C_e be a code obtained from C by appending an overall parity-check digit to every code vector in C, *i.e.*, if

$$(u_0, u_1, u_2, \cdots, u_{n-1})$$

is a vector in C, then

$$(u_\infty, u_0, u_1, u_2, \cdots, u_{n-1})$$

is a vector in C_e, where u_∞ is the overall parity-check digit and

$$u_\infty = u_0 \oplus u_1 \oplus u_2 \oplus \cdots \oplus u_{n-1},$$

where $\oplus$ denotes the modulo-2 addition. Clearly, the length of C_e is 2^m.

Let $GF(2^m)$ be the Galois field of 2^m elements. Let α be a primitive element in $GF(2^m)$. Then the nonzero elements in $GF(2^m)$ can be expressed as powers of α, $\alpha^0 = 1, \alpha^1, \alpha^2, \cdots, \alpha^{2^m-2} (\alpha^{2^m-1} = 1)$. The zero element 0 in $GF(2^m)$ is sometimes represented by α^∞. Now, we number the components of a vector $(u_\infty, u_0, u_1, \cdots, u_{2^m-2})$ in C_e by the elements of $GF(2^m)$ as follows: The component u_∞ is numbered α^∞, the component u_0 is numbered α^0, and, for $1 \le i < 2^m - 1$, the component u_i is numbered α^i. These numbers are called *location numbers*. Let Y denote the location of a component in $(u_\infty, u_0, u_1, \cdots, u_{2^m-2})$. An *affine permutation* with parameters a and b in $GF(2^m)$ and $a \ne 0$ is a permutation that carries the component at location Y to the location $aY + b$. The code C_e is said to be *invariant* under the affine group of permutations if every affine permutation carries every code vector in C_e into another code vector in C_e.

Let h be a nonnegative integer less than 2^m. The radix-2 expansion of h is

$$h = \delta_0 + \delta_1 2 + \delta_2 \cdot 2^2 + \cdots + \delta_{m-1} 2^{m-1},$$

where δ_i is either 0 or 1 for $0 \le i < m$. Let h' be another nonnegative integer $< 2^m$ whose radix-2-expansion is

$$h' = \delta'_0 + \delta'_1 \cdot 2 + \delta'_2 \cdot 2^2 + \cdots + \delta'_{m-1} 2^{m-1}.$$

The integer h' is said to be a *descendant* of h if $\delta'_i \le \delta_i$ for $0 \le i < m$. We also write $h' \le^* h$ meaning that h' is a descendant of h. Clearly, for all h, $0 \le^* h$. Let $\Delta(h)$ denote the set of all nonzero descendants of h. The following theorem characterizes the necessary and sufficient condition for the extension C_e of a cyclic code C to be invariant under the affine group of permutations.

• *Theorem 1* (Kasami, Lin, and Peterson [7])
Let C be a cyclic code of length $2^m - 1$ generated by $\mathbf{g}(X)$. Let C_e be the extended code obtained from C by appending an overall parity-check digit. Let $GF(2^m)$ be the Galois field of 2^m elements. Let α be a primitive element of $GF(2^m)$. Then the extended code C_e is invariant under the affine group of permutations if and only if, for every α^h that is a root of the generator polynomial $\mathbf{g}(X)$ of C, for every $h' \in \Delta(h)$, $\alpha^{h'}$ is also a root of $\mathbf{g}(X)$, and α^0 is not a root of $\mathbf{g}(X)$. □

A cyclic code of length $2^m - 1$ whose generator polynomial satisfies the conditions given in the above theorem is said to have the *doubly transitive invariant property*. In the next section, we describe a class of one-step majority-logic decodable cyclic codes whose dual codes have the doubly transitive invariant property.

2. The codes

Let J and L be two factors of $2^m - 1$ such that $J \cdot L = 2^m - 1$. The polynomial $X^{2^m-1} + 1$ can be factored as follows:

$$X^{2^m-1} + 1 = (1 + X^J)(1 + X^J + X^{2J} + \cdots + X^{(L-1)J}).$$

Let

$$\sigma(X) = 1 + X^J + X^{2J} + \cdots + X^{(L-1)J}. \tag{1}$$

It is well known that the $2^m - 1$ nonzero elements of $GF(2^m)$ form the $2^m - 1$ roots of $X^{2^m-1} + 1$. Let α be a primitive element of $GF(2^m)$. Since $\alpha^{2^m-1} = 1$, it is easy to see that $1, \alpha^L, \alpha^{2L}, \cdots, \alpha^{(J-1)L}$ are the J roots of $1 + X^J$. Therefore, the polynomial $\sigma(X) = 1 + X^J + X^{2J} + \cdots + X^{(L-1)J}$ has α^h, $0 < h < 2^m - 1$, as a root if and only if h is not a multiple of L.

Now, we form a polynomial $H(X)$ over $GF(2)$ as follows: $H(X)$ has α^h as a root if and only if both of the following are satisfied:

1. α^h is a root of $\sigma(X)$, and
2. For every $h' \in \Delta(h)$, $\alpha^{h'}$ is also a root of $\sigma(X)$ $(0 \notin \Delta(h))$.

Let α^i be a root of $H(X)$. Let $\mathbf{m}_i(X)$ be the minimal polynomial of α^i. Then

$$H(X) = \text{LCM } \{\text{minimal polynomials } \mathbf{m}_i(X) \text{ of the roots of } H(X)\}.$$

It is clear that $H(X)$ is a factor of $\sigma(X)$.

Let $\tilde{C}$ be the cyclic code of length $2^m - 1$ generated by $H(X)$. It follows from Theorem 1 that $\tilde{C}$ has the doubly transitive invariant property, *i.e.*, the extended code $\tilde{C}_e$ of $\tilde{C}$ is invariant under the affine group of permutations. Now, let C be the dual code of $\tilde{C}$. Then C is also cyclic. Since $H(X)$ divides $X^{2^m-1} + 1$, we have

$$X^{2^m-1} + 1 = G(X)H(X).$$

Let k be the degree of $H(X)$. Then the degree of $G(X)$ is $2^m - k - 1$. It follows from the theory of cyclic codes that the generator polynomial of C is

$$\mathbf{g}(X) = X^{2^m-k-1} G(X^{-1}). \tag{2}$$

In the next section, we show that C generated by $\mathbf{g}(X) = X^{2^m-k-1} G(X^{-1})$ is one-step majority-logic decodable and is capable of correcting at least $t_{ML} = (J - 1)/2$ or fewer errors (note that J is odd).

3. Orthogonal parity-check sums and decoding

Since $\sigma(X)$ is a multiple of $H(X)$, it is a code polynomial in code $\tilde{C}$ generated by $H(X)$. Since $\tilde{C}$ is cyclic, $X\sigma(X)$, $X^2\sigma(X), \cdots, X^{J-1}\sigma(X)$ are also code polynomials in $\tilde{C}$. It can be seen easily that, for $i \ne j$, $X^i\sigma(X)$ and $X^j\sigma(X)$ do not have any common component. Let $\mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_{J-1}$ be the corresponding vectors (with length $2^m - 1$) of $\sigma(X)$, $X\sigma(X), \cdots, X^{J-1}\sigma(X)$. The Hamming weight of each of these vectors is L. Adding an overall parity-check digit to each of these vectors, we obtain J vectors $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{J-1}$ of length 2^m. The vectors $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{J-1}$ are code vectors in $\tilde{C}_e$ (the extension of $\tilde{C}_e$). Since L is odd, the overall parity-check digit of each $\mathbf{u}_i$ is a 1. Thus, $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{J-1}$ have the following properties:

1. They all have 1 at location α^∞ (overall parity-check digit location);
2. One and only one vector has a 1 at location α^j for $j = 0, 1, 2, \cdots, 2^m - 2$.

These vectors are said to be *orthogonal* on the digit at location α^∞ [1].

Now, we apply the affine permutation

$$Z = \alpha Y + \alpha^{2^m-2}$$

to $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{J-1}$. This permutation carries the set of J vectors $\mathbf{u}_0, \mathbf{u}_1, \cdots, \mathbf{u}_{J-1}$ into another J vectors $\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \cdots, \boldsymbol{\omega}_{J-1}$ in $\tilde{C}_e$. Note that the permutation carries the component of $\mathbf{u}_i$ at location α^∞ to location α^{2^m-2}. Thus, the vectors $\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \cdots, \boldsymbol{\omega}_J$ have the following properties:

1. All the vectors have a 1 at location α^{2^m-2};
2. One and only one vector has a 1 at location α^j for $j = \infty, 0, 1, \cdots, 2^m - 3$.

Hence, $\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \cdots, \boldsymbol{\omega}_{J-1}$ are orthogonal on the digit at location α^{2^m-2}. Deleting the digit at location α^∞ from $\boldsymbol{\omega}_0, \boldsymbol{\omega}_1, \cdots, \boldsymbol{\omega}_{J-1}$, we obtain J vectors $\mathbf{z}_0, \mathbf{z}_1, \cdots, \mathbf{z}_{J-1}$ of length $2^m - 1$ which are code vectors in code $\tilde{C}$. These vectors are still orthogonal to the digit at location α^{2^m-2} and will be used for decoding the code C generated by $\mathbf{g}(X) = X^{2^m-k-1}\, G(X^{-1})$.

Suppose a vector in C is transmitted and a vector $\mathbf{r} = (r_0, r_1, \cdots, r_{2^m-2})$ is received. For decoding $\mathbf{r}$, we form the following inner products:

$$A_0 = \mathbf{r} \cdot \mathbf{z}_0 = r_0 \cdot z_{00} \oplus r_1 z_{01} \oplus \cdots \oplus r_{2^m-1} \cdot z_{0,2^m-2},$$

$$A_1 = \mathbf{r} \cdot \mathbf{z}_1 = r_0 \cdot z_{10} \oplus r_1 \cdot z_{11} \oplus \cdots \oplus r_{2^m-2} \cdot z_{1,2^m-2},$$

$$\vdots$$

$$A_{J-1} = \mathbf{r} \cdot \mathbf{z}_{J-1}$$
$$= r_0 \cdot z_{J-1,0} \oplus r_1 \cdot z_{J-1,1} \oplus \cdots \oplus r_{2^m-2} \cdot z_{J-1,2^m-2}, \tag{3}$$

where $\mathbf{r} \cdot \mathbf{z}_i$ denotes the inner product of $\mathbf{r}$ and $\mathbf{z}_i$ and z_{ij} denotes the jth component of $\mathbf{z}_i$. These J inner products are called *parity-check sums* [1]. Since C and $\tilde{C}$ are dual codes and since $\mathbf{z}_0, \mathbf{z}_1, \cdots, \mathbf{z}_{J-1}$ are vectors in $\tilde{C}$, if $\mathbf{r}$ is a code word in C, then $\mathbf{r} \cdot \mathbf{z}_i = 0$ for $i = 0, 1, \cdots, J-1$, *i.e.*, $A_0 = A_1 = \cdots = A_{J-1} = 0$. If the received vector $\mathbf{r}$ is not a code word in C, it must be a sum of the transmitted code word $\mathbf{x}$ and an unknown error vector $\mathbf{e} = (e_0, e_1, \cdots, e_{2^m-2})$, *i.e.*,

$$\mathbf{r} = \mathbf{x} \oplus \mathbf{e}.$$

Since $\mathbf{x} \cdot \mathbf{z}_i = 0$ for $i = 0, 1, \cdots, J - 1$, we obtain, from (3), the following relations between the parity-check sums $A_0, A_1, \cdots, A_{J-1}$ and the error digits:

$$A_0 = \mathbf{r} \cdot \mathbf{z}_0 = \mathbf{e} \cdot \mathbf{z}_0 = e_0 \cdot z_{00} \oplus e_i z_{01} \oplus \cdots \oplus e_{2^m-2},$$

$$A_1 = \mathbf{r} \cdot \mathbf{z}_1 = \mathbf{e} \cdot \mathbf{z}_1 = e_0 \cdot z_{10} \oplus e_i z_{11} \oplus \cdots \oplus e_{2^m-2},$$

$$\vdots$$

$$A_{J-1} = \mathbf{r} \cdot \mathbf{z}_{J-1}$$
$$= \mathbf{e} \cdot \mathbf{z}_{J-1} = e_0 \cdot z_{J-1,0} \oplus e_i z_{J-1,1} \oplus \cdots \oplus e_{2^m-2}. \tag{4}$$

(Note that $z_{0,2^m-2} = z_{1,2^m-2} = \cdots = z_{J-1,2^m-2} = 1$.) From (4), we see that the error digit e_{2^m-2} appears in every parity-check sum.

Suppose there are $t_{\mathrm{ML}} = (J - 1)/2$ or fewer transmission errors in $\mathbf{e}$. We will show that the error digit e_{2^m-2} can be correctly determined from the parity-check sums. If $e_{2^m-2} = 1$, then the other nonzero error digits can distribute among at most $[(J - 1)/2] - 1$ parity-check sums. Hence, at least $J - [(J - 1)/2] + 1 = (J + 3)/2$, or more than half of the parity-check sums, are equal to $e_{2^m-2} = 1$. However, if $e_{2^m-2} = 0$, the nonzero error digit can distribute among at most $(J - 1)/2$ parity-check sums. Hence, at least $J - (J - 1)/2 = (J + 1)/2$ (more than half) parity-check sums are equal to $e_{2^m-2} = 0$. Thus, if the number of errors in $\mathbf{e}$ is $(J - 1)/2$ or less, the value of e_{2^m-2} is simply equal to the value assumed by a *majority* of the parity-check sums $A_0, A_1, \cdots, A_{J-1}$. Based on the above facts, an algorithm for decoding e_{2^m-2} can be formulated as follows: The error digit e_{2^m-2} is decoded as 1 if a clear majority of the parity-check sums is 1; otherwise, e_{2^m-2} is decoded as 0. Since C is cyclic, decoding of other error digits is the same as decoding e_{2^m-2} [2, 3]. The above decoding algorithm is referred to as one-step majority decoding.

The decoding can be implemented with a single J-input majority-logic gate. When $\mathbf{r}$ is received, the parity-check sums are formed. These parity-check sums are the inputs to a majority-logic gate. The output of this gate is the estimate of e_{2^m-2}. Once e_{2^m-2} is decoded, we correct the received digits r_{2^m-2} by taking the sum $r_{2^m-2} \oplus e_{2^m-2}$. Then the received vector is shifted cyclically one place to the right, and the error digit e_{2^m-3} is ready to be decoded. The error digits are decoded sequentially from e_{2^m-2} to e_0.

4. Numerical parameters

For the codes described above, we have that the number of the parity check digits is $2^m - 1 - \deg H(X)$, while the total length of the code is $2^m - 1$. We will show that

$$\lim_{L\to\infty} \frac{\deg H(X)}{2^m - 1} = 1,$$

and, for J of the form $2^k \pm 1$, give the exact formulas for $\deg H(X)$.

• *Lemma 2*

Let $J \geq 3$ be any odd integer. There exists a positive integer δ such that we can find an L solving $JL = 2^m - 1$ iff $m \equiv 0 \pmod{\delta}$. Furthermore, if we let L_1 be such that $JL_1 = 2^\delta - 1$, then, if $JL_\lambda = 2^{\lambda\delta} - 1$,

$$L_\lambda = \sum_{i=0}^{\lambda-1} 2^{i\delta} L_1.$$

Proof Since J is odd, 2 is a member of the *group* of units of Z_J and has an order δ. We claim that δ has all the properties stated above. This is fairly straightforward since solving $JL = 2^m - 1$ is equivalent to solving $2^m \equiv 1 \pmod{J}$ and since δ is the order of 2. To conclude the proof of the lemma we observe that

$$JL_\lambda = JL_1 \left(\sum_{i=0}^{\lambda-1} 2^{i\delta} \right) = (2^\delta - 1) \left(\frac{2^{\lambda\delta-1}}{2^\delta - 1} \right) = 2^{\lambda\delta} - 1. \ \square$$

Let J, δ, λ, and L_λ be as above and $m = \lambda\delta$. Then it follows that $\deg H(X) = (2^m - 1) - U$, where $U = |\{h | 1 \leq h \leq 2^m - 1 \text{ and } \exists\, \Theta \text{ with } \Theta L_\lambda \leq^* h\}|$. Note that U gives the number of parity bits, since it enumerates those integers which have multiples of L_λ as descendants.

• *Theorem 3*

$$\lim_{\lambda\to\infty} \frac{U}{2^m - 1} = 0.$$

Thus,

$$\lim_{\lambda\to\infty} \frac{\deg H(X)}{2^m - 1} = 1.$$

Proof By the principle of inclusion and exclusion [8],

$$U = \sum_{i=1}^{J} M_{m,iL_\lambda} - \sum_{\substack{i_1,i_2=1 \\ i_1<i_2}}^{J} M_{m,i_1L_\lambda,i_2L_\lambda} + \sum_{\substack{i_1,i_2,i_3=1 \\ i_1<i_2<i_3}}^{J} M_{m,i_1L_\lambda,i_2L_\lambda,i_3L_\lambda} + \cdots,$$

where for k m-digit binary numbers $a_1, \cdots, a_k$,

$$M_{m,a_1,\cdots,a_k} = |\{h | 1 \leq h \leq 2^m - 1 \text{ and } a_i \leq^* h\ \forall\, i\}|.$$

From Lemma 2, we see that each L_λ looks like λ copies of L_1 with sufficient leading 0's to make λ consecutive blocks of size δ. Since we only allow our indices to range between 1 and J (recall $JL_1 = 2^\delta - 1$), each iL_λ looks like λ copies of iL_1. Thus, looking at the λ blocks of size δ we see that $M_{m,i_1L_\lambda,\cdots,i_kL_\lambda} = M^\lambda_{\delta,i_1L_1,\cdots,i_kL_1}$.

Now, we see that

$$U = \sum_{i=1}^{J} M^\lambda_{\delta,iL_1} - \sum_{\substack{i_1,i_2=1 \\ i_1<i_2}}^{J} M^\lambda_{\delta,i_1L_1,i_2L_1} + \cdots.$$

Thus,

$$\frac{U}{2^m} \leq (2^J - 1) \left(\frac{\Gamma}{2^\delta} \right)^\lambda,$$

where $\Gamma = \max\{M_{\delta,iL_1} | i = 1, \cdots, J\}$. Note that since iL_1 is not 0, $M_{\delta,iL_1} \leq 2^{\delta-1}$. Actually, since L_1 is odd, iL_1 contains at least two 1's in its binary representation and $M_{\delta,iL_1} \leq 2^{\delta-2}$. Thus

$$\frac{U}{2^m} \leq \frac{(2^J - 1)}{4^\lambda},$$

which goes to 0 as $\lambda \to \infty$. $\square$

We now give some additional information about U.

• *Corollary 4*

In the above notation,

$$\lim_{\lambda\to\infty} \frac{U}{\rho\Gamma^\lambda} = 1,$$

where $\rho = |\{i | M_{\delta,iL_1} = \Gamma\}|$.

Proof We claim that $M_{\delta,i_1L_1,i_2L_1,\cdots,i_kL_1} < \Gamma$ for all $i_1 < i_2 < \cdots < i_k$ and $k \geq 2$. To see this note that $M_{\delta i_1L_1,\cdots,i_kL_1} \leq \min\{M_{\delta i_1L_1}, M_{\delta i_2L_1}, \cdots, M_{\delta i_kL_1}\}$. If all the $M_{\delta,i_jL_1} = \Gamma$, then note that $M_{\delta i_1L_1,\cdots,i_kL_1} \leq M_{\delta i_1L_1,i_2L_1} \leq A$, where $A = |\{h | 1 \leq h \leq 2^m - 1 \text{ and } i_1L_1 \cup i_2L_1 \leq^* h\}|$. By $i_1L_1 \cup i_2L_1$ we mean the binary number having a 1 whenever i_1L_1 or i_2L_1 have a 1. Since i_1L_1 and i_2L_1 are distinct numbers having the same number of digits, the number $i_1L_1 \cup i_2L_1$ has strictly more digits than either of them, whence $A < \Gamma$. The formula for U derived in the proof of Theorem 2 shows that as $\lambda \to \infty$ we need only worry about those M_δ equal to Γ. The above argument shows this can only happen for terms in the first sum. $\square$

Note that $\Gamma = 2^{\delta-p}$, where p is the smallest number of binary digits in any of the numbers $L_1, 2L_1, \cdots, JL_1$. Determining this quantity in general is probably best carried out by direct calculation. We now turn our attention to J's of the form $2^k - 1$ or $2^k + 1$.

• *Theorem 5*
Let $J = 2^k - 1$ for some $k \geq 2$. Then $m = \lambda k$ and deg $H(X) = (2^\lambda - 1)^k - 1$.

Proof Clearly the δ of Lemma 2 is k and $L_1 = 1$. Thus $m = \lambda k$ for some integer λ and

$$L_\lambda = \sum_{i=0}^{\lambda-1} 2^{ik}.$$

We note that because of the structure of $L_\lambda (L_1 = 1)$, for each integer ρ,

$$\rho L_\lambda = \bigcup_{i=0}^{k-1} a_i 2^i L_\lambda,$$

where

$$\rho = \sum_{i=0}^{k-1} a_i 2^i.$$

Thus, to calculate U it is enough to work with the quantities L_λ, $2L_\lambda$, $4L_\lambda$, $\cdots$, $2^{k-1}L_\lambda$, since they are the minimal elements with respect to $\leq^*$. A bit of reflection shows that we can adapt the inclusion-exclusion formula of Theorem 3 to read as follows:

$$U = \sum_{i=0}^{k-1} M_{m,2^i L_\lambda} - \sum_{\substack{i_1,i_2=0 \\ i_1<i_2}}^{k-1} M_{m,2^{i_1}L_\lambda,\, 2^{i_2}L_\lambda} + \cdots.$$

Furthermore, note that $\mathrm{M}_{m,2^{i_1}L_\lambda,\cdots,2^{i_c}L_\lambda} = 2^{m-c\lambda}$. Thus we get that

$$\deg H(X) = 2^m - 1 + \sum_{c=1}^{k} \binom{k}{c} 2^{m-c\lambda}(-1)^c$$
$$= (2^\lambda - 1)^k - 1. \square$$

• *Theorem 6*
Let $J = 2^k + 1$ for some $k \geq 1$. Then $m = 2\rho k$ for some $\rho \geq 1$ and deg $H(X) = (2^m - 1) - (2^{(\rho+1)} - 1)^k$.

Proof Since $2^k \equiv -1 \pmod{J}$, $2^{2k} \equiv 1 \pmod{J}$, and $2^i \not\equiv 1 \pmod{J}$ for all $i = 1, \cdots, k$, it follows that the δ of Lemma 1 is $2k$. Thus, $m = 2\rho k$ for some $\rho \geq 1$. Furthermore, $L_1 = 2^k - 1$. Thus, L_λ looks like

$$\overbrace{\underbrace{00\cdots0}_{k} \quad \underbrace{11\cdots1}_{k} \quad \underbrace{00\cdots0}_{k} \quad \underbrace{11\cdots1}_{k} \quad \cdots\cdots \quad \underbrace{00\cdots0}_{k} \quad \underbrace{11\cdots1}_{k}}^{\rho\text{-pairs}}.$$

We now show that all nonzero multiples of L_λ smaller than $JL_\lambda = 2^m - 1$ have a binary expansion that looks like

$$\underbrace{\bar{W}W\bar{W}W \cdots \bar{W}W}_{\rho\text{-pairs}},$$

where W is a k-bit string and $\bar{W}$ is the complementary k-bit string. Furthermore, we show that every such string is a multiple of L_λ. Let M be an integer between 1 and $2^k - 1$, and consider that

$$ML_1 = \left(\sum_{i=0}^{q} 2^{\alpha_i}\right)(2^k - 1) = \sum_{i=1}^{q} 2^{\alpha_i+k} + 2^{\alpha_0+k} - \sum_{i=0}^{q} 2^{\alpha_i},$$

where $q \leq k - 1$. Note that in order to perform the subtraction we write 2^{α_0+k} as

$$\sum_{i=0}^{\alpha_0+k-1} 2^i + 1$$

and then cancel out the 1's corresponding to the 2^{α_i}'s and add in the 1. Considering the two cases $\alpha_0 = 0$ and $\alpha_0 \geq 1$ shows that we get a string of the form $\bar{W}W$. Since ML_λ looks like ρ copies of ML_1, the result follows.

Note that $2^k L_\lambda$ has the same form with W being a string of k zeros. Since there are 2^k strings of the type $\bar{W}W$ and 2^k multiples of L_λ less than JL_λ, we see that there is a one-to-one correspondence between such strings and multiples of $L_\lambda < 2^m - 1$. Since $L_\lambda \leq^* 2^m - 1$, we can ignore $2^m - 1 = JL_\lambda$ in calculating $U_{J,\lambda}$, since we need only consider those multiples which are minimal with respect to $\leq^*$. Note that the above argument shows that L_λ, $2L_\lambda$, $3L_\lambda$, $\cdots$, $2^k L_\lambda$ are all minimal with respect to $\leq^*$.

Rather than using the inclusion-exclusion formula of Theorem 2 to calculate $U_{J,\lambda}$, we calculate it directly. Suppose $\Theta L_\lambda \leq^* M$ for some integers $\Theta \leq 2^k$ and M. Write ΘL_λ as $a_1 b_1 a_2 b_2 \cdots a_\rho b_\rho$, where each a_i, b_i is a string of k digits and where $\bar{W} \leq^* a_i$ and $W \leq^* b_i$ for all i.

Let $A = \{h | 1 \leq h \leq 2^m - 1 \text{ and } \exists\, \Theta \text{ with } \Theta L_\lambda \leq^* H\}$. We consider each h to be in the form $a_1 b_1 a_2 b_2 \cdots a_\rho b_\rho$. For each g between 1 and $2^k - 1$, let

$$A_g = \{h \in A | \bigcap_{i=1}^{\rho} b_i = g\}$$

where

$$\bigcap_{i=1}^{\rho} b_i$$

is the number whose binary expansion has a 1 in the jth place iff each b_i has a 1 in the jth place of its binary expansion. Assume g has s 1's in its representation. Then each b_i must have at least those s 1's. In order for $\cap b_i = g$, we must pick the remaining digits of the b_i so that some b_i has a 0 in each of the $k - s$ positions where g has a 0. If we focus our attention on a particular position and try to fill it in all b_i's simultaneously, we see that this can be done in $2^\rho - 1$ ways. Thus the b_i's can be picked in $(2^\rho - 1)^{k-s}$ ways. Each a_i must contain $\bar{W}$, but there are no restrictions on the remaining bits. Thus we see that $|A_g| = (2^\rho - 1)^{k-s}(2^\rho)^s$ and, since there are (k/s) strings g having s 1's, we see that

$$U = |A| = \sum_{s=0}^{k} \binom{k}{s} (2^\rho - 1)^{k-s}(2^\rho)^s = (2^{\rho+1} - 1)^k. \square$$

5. An example

The following example illustrates the code construction and decoding described above, as well as Theorem 5.

Let $m = 4$. The polynomial $X^{2^4-1} + 1 = X^{15} + 1$ can be factored as follows:

$$X^{15} + 1 = (1 + X^3)(1 + X^3 + X^6 + X^9 + X^{12}).$$

Thus, $J = 3$, $L = 5$, and

$$\sigma(X) = 1 + X^3 + X^6 + X^9 + X^{12}.$$

The Galois field $GF(2^4)$ is given by Table 1, where α is a primitive element and is a root of $p(X) = 1 + X + X^4$, *i.e.*, $p(\alpha) = 1 + \alpha + \alpha^4 = 0$. Note that $\alpha^{15} = 1$. The polynomial $\sigma(X)$ has

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$$

as roots.

Next, we form the polynomial $H(X)$. The polynomial $H(X)$ has α^h as a root if and only if α^h is a root of $\sigma(X)$ and, for every nonzero descendant h' of h, $\alpha^{h'}$ is also a root of $\sigma(X)$. For example α^{12} is a root of $\sigma(X)$. The nonzero descendants of 12 are 4 and 8, and both α^4 and α^8 are roots of $\sigma(x)$. Thus, α^{12} is a root of $H(X)$. The roots of $H(X)$ are

$$\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12},$$

and we see that deg $H(X) = 8$ as predicted by Theorem 5. The roots α^1, α^2, α^4, and α^8 are conjugates, and they have the same minimal polynomial

$$m_1(X) = (X + \alpha^1)(X + \alpha^2)(X + \alpha^4)(X + \alpha^8).$$

Using Table 1, we obtain

$$m_1(X) = 1 + X + X^4.$$

The roots α^3, α^6, α^{12}, $\alpha^{24} = \alpha^9$ are conjugates and their minimal polynomial is

$$m_3(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9)$$
$$= 1 + X + X^2 + X^3 + X^4.$$

Therefore,

$$H(X) = m_1(X)m_3(X)$$
$$= 1 + X^4 + X^6 + X^7 + X^8,$$

Table 1 The Galois field of 2^4 elements ($GF(2^4)$) with $p(\alpha) = \alpha^4 + \alpha + 1 = 0$ (or $\alpha^4 = \alpha + 1$).

0	
1	
α	
α^2	
α^3	
α^4	$= \alpha + 1$
α^5	$= \alpha(\alpha + 1) = \alpha^2 + \alpha$
α^6	$= \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2$
α^7	$= \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$
α^8	$= \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha$
	$= \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1$
α^9	$= \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$
α^{10}	$= \alpha(\alpha^3 + \alpha) = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$
α^{11}	$= \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha$
α^{12}	$= \alpha(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$= \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + \alpha + 1$
	$= \alpha^3 + \alpha^2 + 1$
α^{14}	$= \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha + \alpha + 1 = \alpha^3 + 1$
α^{15}	$= \alpha^4 + \alpha = \alpha + \alpha + 1 = 1$

Table 2 Location numbers.

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$\mathbf{v}_0 =$	(1	0	0	1	0	0	1	0	0	1	0	0	1	0	0)
$\mathbf{v}_1 =$	(0	1	0	0	1	0	0	1	0	0	1	0	0	1	0)
$\mathbf{v}_2 =$	(0	0	1	0	0	1	0	0	1	0	0	1	0	0	1)

which is the generator polynomial of the code $\tilde{C}$ with length 15, and

$$\sigma(X) = (1 + X^3 + X^4)H(X).$$

Therefore, $\sigma(X)$, $X\sigma(X)$, $X^2\sigma(X)$ are code polynomials in $\tilde{C}$.

Also, $H(X)$ divides $X^{15} + 1$ and

$$X^{15} + 1 = (1 + X^4 + X^6 + X^7)H(X).$$

Thus,

$$G(X) = 1 + X^4 + X^6 + X^7.$$

The generator polynomial of the code C (the dual of $\tilde{C}$) is

$$g(X) = X^7 G(X^{-1})$$
$$= 1 + X + X^3 + X^7.$$

Thus, C is a (15, 8) cyclic code.

To decode C, we need to find parity-check sums that are orthogonal on error digit e_{14}. The vectors corresponding to $\sigma(X)$, $X\sigma(X)$, and $X^2\sigma(X)$, which are code vectors

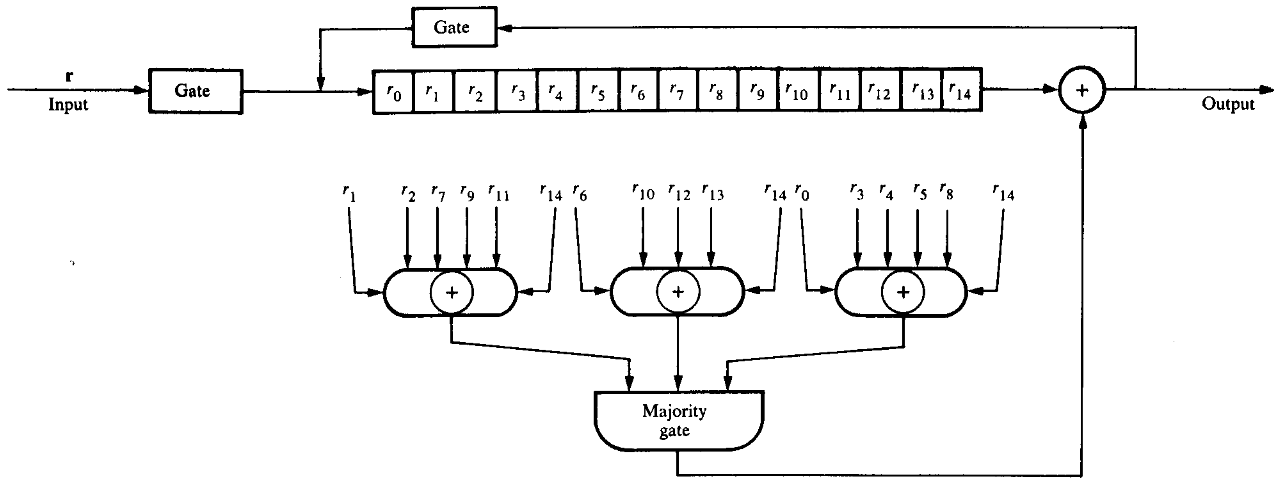

Figure 1 One-step-majority-logic decoder.

Table 3 Resulting vectors after adding parity-check digit.

	α^∞	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$\mathbf{u}_0$ =	(1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0)
$\mathbf{u}_1$ =	(1	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0)
$\mathbf{u}_2$ =	(1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1)

Table 4 Resulting vectors after permutation.

	α^∞	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$\boldsymbol{\omega}_0$ =	(0	0	1	1	0	0	0	0	1	0	1	0	1	0	0	1)
$\boldsymbol{\omega}_1$ =	(1	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1)
$\boldsymbol{\omega}_2$ =	(0	1	0	0	1	1	1	0	0	1	0	0	0	0	0	1)

Table 5 Vectors after deletion of parity-check digit.

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$\mathbf{z}_0$ =	(0	1	1	0	0	0	0	1	0	1	0	1	0	0	1)
$\mathbf{z}_1$ =	(0	0	0	0	0	0	1	0	0	0	1	0	1	1	1)
$\mathbf{z}_2$ =	(1	0	0	1	1	1	0	0	1	0	0	0	0	0	1)

in C, are shown in Table 2. Adding an overall parity-check digit to each of these vectors, we obtain the vectors in Table 3. These are code vectors in $\tilde{C}_e$ (the extension of $\tilde{C}$). Now, we apply the affine permutation

$$Z = \alpha Y + \alpha^{14}$$

to permute the components of $\mathbf{u}_0$, $\mathbf{u}_1$, $\mathbf{u}_2$. The resultant vectors are given in Table 4. Deleting the overall parity-check digit from the above vectors, we obtain the vectors in Table 5, which are vectors in $\tilde{C}$. We see that these vectors are orthogonal on the digit at location α^{14}. Let

$$\mathbf{r} = (r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14})$$

be the received vector. Then the parity-check sums orthogonal on error digit e_{14} are

$$A_0 = \mathbf{r} \cdot \mathbf{z}_0 = r_1 \oplus r_2 \oplus r_7 \oplus r_9 \oplus r_{11} \oplus r_{14},$$

$$A_1 = \mathbf{r} \cdot \mathbf{z}_1 = r_6 \oplus r_{10} \oplus r_{12} \oplus r_{13} \oplus r_{14},$$

$$A_2 = \mathbf{r} \cdot \mathbf{z}_2 = r_0 \oplus r_3 \oplus r_4 \oplus r_5 \oplus r_8 \oplus r_{14}.$$

The decoding circuit is shown in Fig. 1. The code is capable of correcting any single error over the span of 15 digits. The code C has minimum distance 4 (the generator polynomial has weight 4). Thus, the code is capable of correcting single errors and detecting any double errors.

6. Summary

In this paper we have investigated a class of one-step majority-logic decodable codes. A method of decoding these codes has been presented. Combinatorial expressions for determining the dimensions of these codes have been derived. These codes are effective compared with other majority-logic decodable codes [3, pp. 176–177]. Most important, they can be decoded in one step with a single majority-logic gate. A list of these codes is given in Table 6.

For short length, these codes are comparable with BCH codes in efficiency. For example, there exists a (63, 36) one-step majority-logic decodable code which is capable of correcting 4 or fewer errors. The corresponding 4-error-correcting BCH code of the same length is a (63, 39) code which has 3 information digits more than the one-step majority-logic decodable code. For large block length, the codes presented in this paper are much less efficient than the BCH codes of the same length and the same error-correcting capability.

Due to their decoding simplicity, the codes presented in this paper may find applications in data communication systems where cost and decoding speed are critical.

Table 6 Some one-step majority-logic decodable codes.

n	k	t_{ML}	n	k	t_{ML}
15	8	1	2047	1210	11
	6	2		572	44
63	48	1	4095	3968	1
	36	4		3870	2
	12	10		3752	4
255	224	1		3366	32
	206	2		2706	17
	174	8		2261	19
	36	25		2073	22
	20	42		1648	45
511	342	3		1392	52
	138	36		1376	136
1023	960	1		405	292
	832	5		100	409
	780	16		42	682
	150	46			
	30	170			

References

1. J. L. Massey, *Threshold Decoding*, The MIT Press, Cambridge, MA, 1963.
2. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd edition, MIT Press, Cambridge, MA, 1971.
3. S. Lin, *An Introduction to Error-Correcting Codes*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1970.
4. P. Delsarte, "A Geometric Approach to a Class of Cyclic Codes," *J. Combinat. Theor.* **6**, 340–358 (1969).
5. T. Kasami and S. Lin, "On Majority-Logic Decoding for the Duals of Primitive Polynomial Codes," *IEEE Trans. Info. Theor.* **IT-17**, 322–331 (1971).
6. S. Lin and K. P. Yiu, "An Improvement to Multifold Euclidean Geometry Codes," *Info. Control* **28**, 221–265 (1975).
7. T. Kasami, S. Lin, and W. W. Peterson, "Some Results on Cyclic Codes Which are Invariant Under the Affine Group of Permutations and Their Applications," *Info. Control* **11**, 475–496 (1967).
8. C. L. Liu, *Introduction to Combinatorial Mathematics*, McGraw-Hall Book Co., Inc., New York, 1968.

Received November 1, 1978; revised June 29, 1979

Professor Lin is located at the University of Hawaii at Manoa but was a Visiting Professor at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, when this work was done. Dr. Markowsky is at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598.