INFORMATION AND CONTROL **10**, 553–564 (1967)

On the Solution of Algebraic Equations over Finite Fields

E. R. BERLEKAMP,* H. RUMSEY, AND G. SOLOMON†

Jet Propulsion Laboratory, Pasadena, California 91103

This article gives new fast methods for decoding certain error-correcting codes by solving certain algebraic equations. As described by Peterson (1961), the locations of a Bose–Chaudhuri Hocquenghem code over a field of characteristic p are associated with the elements of an extension field, $GF(p^k)$. The code is designed in such a way that the weighted power-sum symmetric functions of the error locations can be obtained directly by computing appropriately chosen parity checks on the received word. Good methods for computing the elementary symmetric functions from the weighted power-sum symmetric functions have been presented by Berlekamp (1967). The elementary symmetric functions, $\sigma_1, \sigma_2, \cdots, \sigma_t$ are the coefficients of an algebraic equation whose roots are the error locations

$$x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \cdots + \sigma_t = 0.$$

Previous methods for finding the roots of this equation have searched all of the elements in $GF(p^k)$ (Chien, 1964) or looked up the answer in a large table (Polkinghorn, 1966). We present here improved procedures for extracting the roots of algebraic equations of small degrees.

QUADRATIC EQUATIONS IN FIELDS OF CHARACTERISTIC TWO

CASE 1: WITH REPEATED ROOTS

In order to solve a quadratic equation of the type $x^2 + c = 0$, where c and $x \in GF(2^k)$, we must extract the square root of c. Since in any field of characteristic two we have the identity $(x + y)^2 = x^2 + y^2$ and similarly, $(x + y)^{1/2} = x^{1/2} + y^{1/2}$ the square root is a linear operation. In terms of a fixed basis of $GF(2^k)$, namely $u_1, u_2, \cdots, u_k$, we may write $c = \sum_{i=1}^{k} c_i u_i$, where $c_i \in GF(2)$. Because of the linearity of the square root, we then have $c^{1/2} = \sum_{i=1}^{k} c_i (u_i)^{1/2}$. Of course, $(u_i)^{1/2}$ can also be

* Present address: Bell Telephone Laboratories, Murray Hill, New Jersey 07971.
† Present address: TRW Systems, Redondo Beach, California 90278.

represented in terms of this same basis, with $(u_i)^{1/2} = \sum_j R_{i,j} u_j$, with $R_{i,j} \in GF(2)$. We then have

$$c^{1/2} = \sum_{i=1}^{k} \sum_{j=1}^{k} c_i R_{i,j} u_j$$

$$= \sum_{j=1}^{k} \left(\sum_{i=1}^{k} c_i R_{i,j} \right) u_j .$$

For example, in $GF(2^5)$, let us take the basis consisting of $u_i = \alpha^{5-i}$ for $i = 1, 2, 3, 4, 5$, where α satisfies the equation $\alpha^5 + \alpha^2 + 1 = 0$. The representation of all of the elements of $GF(2^5)$ in terms of this basis is given in the appendix. We see that

$$(u_1)^{1/2} = (\alpha^4)^{1/2} = \alpha^2$$

$$(u_2)^{1/2} = (\alpha^3)^{1/2} = \alpha^{17} = \alpha^4 + \alpha + 1$$

$$(u_3)^{1/2} = (\alpha^2)^{1/2} = \alpha$$

$$(u_4)^{1/2} = (\alpha^1)^{1/2} = \alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$$

$$(u_5)^{1/2} = (\alpha^0)^{1/2} = 1.$$

Hence, the matrix R is given by

$$R = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

For example, if we wish to take the square root of $c = \alpha^4 + \alpha^2 + \alpha + 1$ we write

$$c^{1/2} = \mathbf{c}R = [1\ 0\ 1\ 1\ 1] \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = [1\ 1\ 1\ 0\ 0].$$

We can verify this by checking that $c = \alpha^{26}$; $c^{1/2} = \alpha^{13}$.

CASE 2: WITHOUT REPEATED ROOTS

In general, the quadratic equation may be written as $x^2 + bx + c = 0$. We have just seen that if $b = 0$, this equation has a unique solution in

$GF(2^k)$, and that this solution may be found by multiplying the vector representing c by the matrix R which extracts square roots.

If $b \neq 0$, we first transform the equation by introducing the new variable $y = x/b$. This new variable satisfies the equation $b^2y^2 + b^2y + c = 0$, or $y^2 + y = d$, where $d = c/b^2$. We now notice that if $y_i^2 + y_i = v_i$ and $y_j^2 + y_j = v_j$, then $(y_i + y_j)^2 + (y_i + y_j) = v_i + v_j$. Hence, a solution of the equation $y^2 + y = d = \Sigma\, d_i v_i$; $d_i \in GF(2)$, is given by $y = \Sigma\, d_i y_i$, where y_i is a solution of the equation $y_i^2 + y_i = v_i$. This shows that the set of v for which the equation $y^2 + y = v$ has a solution in $GF(2^k)$ forms a linear subspace of the vector space $GF(2^k)$, and since each value of v corresponds to two values of y, the dimensionality of the subspace is evidently $k - 1$. Consequently, the solutions of the equation $y^2 + y + d = 0$ may be represented in terms of solutions to the equations $y_i^2 + y_i + v_i = 0$, for $i = 1, 2, \cdots, k - 1$, where the v_i span the space of v's for which $y^2 + y + v = 0$ has solutions in $GF(2^k)$. If d is not expressible as a sum of such v's, the equation $y^2 + y + d$ has no solutions in $GF(2^k)$. If $d = \Sigma\, d_i v_i$, then $y = \Sigma\, d_i y_i$ is a solution of $y^2 + y + d$. The other solution is found by adding to the first solution a solution of $y^2 + y = 0$, namely, $y = 1$.

If $y_i^2 + y_i = v_i$, then we may square both sides to obtain $(y_i^2)^2 + y_i^2 = v_i^2$. By repeatedly squaring, we find that $y_i^{2^{j+1}} + y_i^{2^j} = v_i^{2^j}$. Summing on j gives

$$\sum_{j=0}^{k-1} (y_i^{2^{j+1}} + y_i^{2^j}) = \sum_{j=0}^{k-1} v_i^{2^j}.$$

The left-hand side of this equation is equal to $y_i^{2^k} + y_i$, which is 0 for all $y_i \in GF(2^k)$. Therefore, if the quadratic equation $y^2 + y = v$ has solutions in $GF(2^k)$, then $\mathrm{Tr}\,(v) = 0$, where $\mathrm{Tr}\,(v)$ is defined as $\sum_{j=0}^{k-1} v^{2^j}$. However, all elements in $GF(2^k)$ are roots of the equation $x^{2^k} + x = 0$. From the factorization

$$x^{2^k} + x = (x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}}) \cdot (1 + x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}}) = (\mathrm{Tr}\,(x))(1 + \mathrm{Tr}\,(x)),$$

we see that exactly half of the elements in $GF(2^k)$ have $\mathrm{Tr}\,(x) = 0$ and exactly half have $\mathrm{Tr}\,(x) = 1$. Since the space of v's for which $y^2 + y = v$ has solutions in $GF(2^k)$ has dimension $k - 1$, we have the following theorem.

THEOREM 1. *If $v \in GF(2^k)$, the quadratic equation $y^2 + y = v$ has solutions in $GF(2^k)$* iff $\mathrm{Tr}\,(v) = 0$.

We have recently learned that various versions of this theorem have been independently discovered by various people. The earliest version we have seen is given by Hughes (1959), where it is attributed to Marshall Hall.

EXAMPLE. In $GF(2^5)$, with $\alpha^5 + \alpha^2 + 1 = 0$, the equations $y_i^2 + y_i = v_i$ have the solutions

$$v_1 = \alpha, \qquad y_1 = \alpha^3,$$
$$v_2 = \alpha^2, \qquad y_2 = \alpha^6 = \alpha^3 + \alpha,$$
$$v_3 = \alpha^4, \qquad y_3 = \alpha^{12} = \alpha^3 + \alpha^2 + \alpha,$$
$$v_4 = \alpha^8 = \alpha^3 + \alpha^2 + 1, \qquad y_4 = \alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

or preferably,

$$v_4 = \alpha^3 + 1, \qquad y_4 = \alpha^4 + \alpha^2.$$

There are no solutions to the equations $y^2 + y + 1 = 0$, or $y^2 + y + \alpha^3 = 0$. Thus $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha^4) = 0$ but $\mathrm{Tr}(1) = \mathrm{Tr}(\alpha^3) = 1$. In terms of our previous basis $u_i = \alpha^{5-i}$, $i = 1, 2, \cdots, 5$, with $y = \Sigma\, d_i u_i$, the solution of the equation $y^2 + y + d = 0$ is given by

$$[y_1, y_2, y_3, y_4] = [d_1, d_2, d_3, d_4] \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

if $d_5 = d_2$. If $d_5 \neq d_2$, no solutions exist, because $\mathrm{Tr}(\Sigma\, d_i u_i) = \Sigma\, d_i \mathrm{Tr}(u_i) = d_2 + d_5$. If solutions exist, y_5 may be arbitrarily assigned either the value 0 or the value 1, corresponding to the two different solutions of the quadratic.

FURTHER USES OF THE TRACE OPERATOR

We have seen that the quadratic equation, $x^2 + ax + b = 0$, $a, b \in GF(2^k)$, $a \neq 0$, has solutions in $GF(2^k)$ iff $\mathrm{Tr}(b/a^2) = 0$, where $\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{k-1}}$. This operator has the important properties that $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$ and $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ for all $x, y \in GF(2^k)$. Astute use of these properties enables one to derive conditions for the existence of solutions in $GF(2^k)$ of certain cubic equations, as evidenced by the following theorem.

THEOREM 2. *The cubic equation* $x^3 + x = a$, $a \in GF(2^k)$, $a \neq 0$ *has a unique* solution, $x \in GF(2^k)$, iff $\mathrm{Tr}(a^{-1}) \neq \mathrm{Tr}(1)$.

Remark. The general cubic, $x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0$ may be reduced

to the form $z^3 + z = a$ as follows. First, the substitution $x = y + \sigma_1$, eliminates the quadratic term, giving $y^3 + (\sigma_2 + \sigma_1^2)y + (\sigma_3 + \sigma_1\sigma_2) = 0$. Except in the degenerate case when $\sigma_2 = \sigma_1^2$, we may then set $y = z(\sigma_2 + \sigma_1^2)^{1/2}$ so that $z^3 + z + a = 0$ where $a = (\sigma_3 + \sigma_1\sigma_2)/(\sigma_2 + \sigma_1^2)^{3/2}$.

Proof. Setting $x = 1/y$ transforms the equation to $ay^3 + y^2 + 1 = 0$; setting $y = z + 1$ transforms this equation to $az^3 + (a + 1)z^2 + az + z = 0$, or $z^3 + bz^2 + z + 1 = 0$. These transformations map roots in $GF(2^k)$ into other roots in $GF(2^k)$, so the equation

$$x^3 + x + a = 0 \tag{1}$$

has a unique solution in $GF(2^k)$ iff

$$z^3 + bz^2 + z + 1 = 0 \tag{2}$$

has a unique solution in $GF(2^k)$, where $b = (a + 1)/a$. If u is a solution of (2), then a solution of (1) is given by $v = 1/(u + 1)$ or $u = (v + 1)/v$. Suppose u is a solution to (2), $u \in GF(2^k)$. Then $u^3 + bu^2 + u + 1 = 0$, and $u^4 + bu^3 + u^2 + u = 0$, so $\mathrm{Tr}(u^4 + bu^3 + u^2 + u) = \mathrm{Tr}(0) = 0 = \mathrm{Tr}(u^4) + \mathrm{Tr}(bu^3) + \mathrm{Tr}(u^2) + \mathrm{Tr}(u)$. Since $\mathrm{Tr}(u^4) = \mathrm{Tr}((u^2)^2) = \mathrm{Tr}(u^2)$, we have $\mathrm{Tr}(bu^3) = \mathrm{Tr}(u)$. However, we also have $bu^3 + b^2u^2 + bu + b = 0$, so $0 = \mathrm{Tr}(bu^3 + b^2u^2 + bu + b) = \mathrm{Tr}(bu^3) + \mathrm{Tr}(b)$. Therefore, $\mathrm{Tr}(bu^3) = \mathrm{Tr}(b)$, so $\mathrm{Tr}(u) = \mathrm{Tr}(b)$ because both are equal to $\mathrm{Tr}(bu^3)$.

Since u is a root of (2), we may factor it out, obtaining

$$(z^3 + bz^2 + z + 1) = (z + u)\left(z^2 + \left(\frac{u + 1}{u^2}\right)z + \frac{1}{u}\right).$$

Thus u is the unique root in $GF(2^k)$ iff

$$1 = \mathrm{Tr}\left(\frac{u^4}{u(u + 1)^2}\right) = \mathrm{Tr}\left(\frac{u^3}{(u + 1)^2}\right).$$

But

$$\frac{u^3}{(u + 1)^2} = \frac{u^3}{1 + u^2} = u + \frac{u}{1 + u} + \frac{u^2}{(1 + u)^2},$$

so

$$\mathrm{Tr}\left(\frac{u^3}{(u + 1)^2}\right) = \mathrm{Tr}(u) + \mathrm{Tr}\left(\frac{u}{1 + u}\right) + \mathrm{Tr}\left(\frac{u^2}{(1 + u)^2}\right) = \mathrm{Tr}(u) = \mathrm{Tr}(b).$$

Thus, if (2) has a unique root in $GF(2^k)$, $\mathrm{Tr}(b) = 1$; if (2) has three distinct roots in $GF(2^k)$, $\mathrm{Tr}(b) = 0$. Correspondingly, if (1) has a unique root, $v \in GF(2^k)$, $\mathrm{Tr}((v+1)/v) = 1 = \mathrm{Tr}((a+1)/a) = \mathrm{Tr}(1) + \mathrm{Tr}(a^{-1})$ and $\mathrm{Tr}(a^{-1}) \neq \mathrm{Tr}(1)$; if (1) has three distinct roots in $GF(2^k)$, $\mathrm{Tr}((a+1)/a) = 0$ and $\mathrm{Tr}(a^{-1}) = \mathrm{Tr}(1)$. No cubic over $GF(2^k)$ can have exactly two roots in $GF(2^k)$, (since the sum of the roots is the coefficient of the quadratic term), but some cubics over $GF(2^k)$ have no roots in $GF(2^k)$. To complete the proof, we must show that if (1) has no roots in $GF(2^k)$, then $\mathrm{Tr}(1) = \mathrm{Tr}(a^{-1})$, or equivalently, if $\mathrm{Tr}(1) \neq \mathrm{Tr}(a^{-1})$, then (1) has a unique root in $GF(2^k)$. This is most readily seen by a counting argument.

Let $A_i (i = 0, 1, 3)$ be the set of $a \in GF(2^k) - 0$ such that the equation $x^3 + x = a$ has i solutions in $GF(2^k)$. Let $X_i (i = 1, 3)$ be the corresponding solution sets. Clearly $|X_3| = 3|A_3|$; $|X_1| = |A_1|$. Since 0 and 1 are the only solutions of $x^3 + x = 0$, all $x \in GF(2^k) - GF(2)$ must correspond to some nonzero a, and $X_1 \cup X_3 = GF(2^k) - GF(2)$. Let T_i, $(i = 0, 1)$ be the set of $x \in GF(2^k) - GF(2)$ such that $\mathrm{Tr}((x+1)/x) = i$, or equivalently, $\mathrm{Tr}(x^{-1}) + \mathrm{Tr}(1) = i$. We have shown that $X_1 \subseteq T_1$, $X_3 \subseteq T_0$, $A_1 \subseteq T_1$, $A_3 \subseteq T_0 \cup 1$. Since $X_1 \cup X_3 = T_1 \cup T_0$, we conclude that $X_1 = T_1$, $X_3 = T_0$. Since $|A_1| = |X_1| = |T_1|$, we also have $A_1 = X_1 = T_1$. Q.E.D.

Although this theorem enables us to determine whether or not the equation $x^3 + x = a$ has a unique solution in $GF(2^k)$ by making a simple parity-check calculation on some of the bits in the representation of a^{-1}, it does not enable us to find this unique solution if there is one. Furthermore, if there is not a unique solution, we do not know whether there are no solutions or three solutions. One form of an answer to this question is given by the following theorem.

THEOREM 3. *A necessary and sufficient condition that all three roots of the cubic polynomial $x^3 + x + a$ lie in $GF(2^k)$ is that $P_k(a) = 0$ where the polynomials $P_k(x)$ may be defined recursively by the equations*

$$P_1(x) = x, \qquad P_2(x) = x,$$

$$P_k(x) = P_{k-1}(x) + x^{2^{k-3}} P_{k-2}(x).$$

The proof, which is lengthy, is given by Berlekamp, Solomon, and Rumsey (1966).

Although this theorem provides a theoretical answer to the question of

whether $x^3 + x = a$ has three roots or zero roots [given $\mathrm{Tr}(a^{-1}) = \mathrm{Tr}(1)$], it is not as useful in practice as the methods introduced in the next section, which enable one to find all of the roots in $GF(2^k)$ in addition to determining how many roots there are.

p-POLYNOMIALS AND TRANSLATED p-POLYNOMIALS

DEFINITIONS. *A polynomial, $L(z)$ over $GF(p^m)$, p prime, is said to be a p-polynomial iff it is of the form $L(z) = \sum_{i=0}^{k} L_i z^{p^i}$; a polynomial $A(z)$ over $GF(p^m)$ is said to be a translated p-polynomial iff it is of the form $A(z) = L(z) - u$ where $u \in GF(p^m)$ and $L(z)$ is a p-polynomial.*

The p-Polynomials were first introduced by Ore (1933, 1934) in two important papers which expounded many of their theoretical properties. For our purposes, the main value of translated p-polynomials lies in the practical ease with which one may compute their roots in $GF(p^m)$.

If $Z_k \in GF(p)$, and $\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{m-1}$ are a standard basis for $GF(p^m)$, then.

$$\left(\sum_k Z_k \alpha^k\right)^{p^i} = \sum_k Z_k^{p^i} (\alpha^k)^{p^i} = \sum_k Z_k (\alpha^k)^{p^i}.$$

From this we see that

If $L(z)$ is a p-polynomial, and if $z = \sum Z_k \alpha^k$, $Z_k \in GF(p)$, then $L(z) = \sum_k Z_k L(\alpha^k)$.

If we also use the standard representation to express the value of the field elements $L(\alpha^0), L(\alpha^1), \cdots, L(\alpha^{m-1})$, we may write $L(\alpha^i) = \sum_{j=0}^{m-1} L_{i,j}\alpha^j$, $L_{i,j} \in GF(p)$. The coefficients of the standard representation for the value of the polynomial $L(z)$ may therefore be obtained by postmultiplying the row vector $Z = [Z_0, Z_1, \cdots, Z_{m-1}]$ by the $m \times m$ matrix L over $GF(p)$:

$$[Z_0, Z_1, \cdots, Z_{m-1}] \begin{bmatrix} L_{0,0} & L_{0,1} & L_{0,2} & \cdots & L_{0,m-1} \\ L_{1,0} & L_{1,1} & L_{1,2} & \cdots & L_{1,m-1} \\ \vdots & & & & \\ L_{m-1,0} & & & & L_{m-1,m-1} \end{bmatrix}.$$

For example, let us consider the polynomial

$$L(z) = z^{16} + \alpha^{13} z^8 + \alpha^{30} z^4 + \alpha^{18} z^2 + \alpha^{20} z$$

over $GF(2^5)$, where α is a root of the primitive irreducible binary polynomial, $x^5 + z^2 + 1$. Using the tables of logs and antilogs in the

appendix, we may calculate

$$L(1) = \alpha^0 + \alpha^{13} + \alpha^{30} + \alpha^{18} + \alpha^{20} = 0,$$
$$L(\alpha) = \alpha^{16} + \alpha^{21} + \alpha^3 + \alpha^{20} + \alpha^{21} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4,$$
$$L(\alpha^2) = \alpha^1 + \alpha^{29} + \alpha^7 + \alpha^{22} + \alpha^{22} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4,$$
$$L(\alpha^3) = \alpha^{17} + \alpha^6 + \alpha^{11} + \alpha^{24} + \alpha^{23} = 1 + \alpha + \alpha^2 + \alpha^3,$$
$$L(\alpha^4) = \alpha^2 + \alpha^{14} + \alpha^{15} + \alpha^{26} + \alpha^{24} = 1 + \alpha + \alpha^2 + \alpha^3;$$

so L is represented by the 5×5 binary matrix

$$L = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

If, for example, we wish to compute $L(\alpha^{22})$, we write α^{22} in its standard representation, namely $\alpha^{22} = 1 + \alpha^2 + \alpha^4$ or more simply, [10101]. Then [10101]L = [00001], so $L(\alpha^{22}) = \alpha^4$.

The major value of the matrix representation of a p-polynomial is that it transforms the polynomial $L(z) - u = 0$ into the matrix equation $\mathbf{Z}L = \mathbf{U}$. Thus, we may find the roots in $GF(p^m)$ of the translated p-polynomial $L(z)$ by solving m simultaneous linear equations over $GF(p)$. In general, this may be done by reducing the $m \times m$ L-matrix to any of several "canonical" forms by appropriate column operations on the augmented L-matrix. The form which is most convenient for the present problem is the reduced triangular idempotent form, $\check{L}$, in which every entry below the main diagonal is zero, every entry on the main diagonal is zero or one, and every entry in the same column as a main diagonal zero or the same row as a main diagonal one is zero. Any square L-matrix can be reduced to such an $\check{L}$-matrix by appropriate column operations. These same column operations, applied to the augmented row $\mathbf{U}$, will transform it into another row, $\check{\mathbf{U}}$. The equation $\mathbf{Z}L = \mathbf{U}$ then becomes $\mathbf{Z}\check{L} = \check{\mathbf{U}}$.

From the triangular idempotent form of the $\check{L}$-matrix, it is readily seen that $\check{L}$ is a linear combination of the rows of $\check{L}$ iff $\check{\mathbf{U}}$ has a zero corresponding to each diagonal component of $\check{L}$. Equivalently, the product of each component of $\check{\mathbf{U}}$ and the corresponding diagonal component of $\check{L} - I$ must be zero. If the product of any component of $\check{U}$ and the cor-

responding diagonal component of $\check{L} - I$ is nonzero then $\check{U}$ is not a linear combination of rows of $\check{L}$ and the equations $\mathbf{Z}\check{L} = \check{\mathbf{U}}$ and $\mathbf{Z}L = \mathbf{U}$ have no solutions. If the product of every component of $\check{\mathbf{U}}$ and the corresponding diagonal component of $\check{L} - I$ is zero, then $\check{\mathbf{U}}$ is a linear combination of the rows of $\check{L}$, and one particular solution of the equations $\mathbf{Z}\check{L} = \check{\mathbf{U}}$ and $\mathbf{Z}L = \mathbf{U}$ is given by $\mathbf{Z} = \check{\mathbf{U}}$. In order to find the general solution we may add to $\check{\mathbf{U}}$ any solution of the equations $\mathbf{Z}\check{L} = 0$ and $\mathbf{Z}L = \mathbf{0}$. From the form of $\check{L}$, it is easily seen that $\check{L}^2 = \check{L}$, so that $(\check{L} - I)\check{L} = 0$. Furthermore, Rank $(\check{L} - I)$ + Rank $(\check{L}) = m$, so that the null space of $\check{\mathbf{U}}$ is spanned by the rows of $\check{L} - I$. Thus, the general solution of $\mathbf{Z}L = \mathbf{U}$ is given by $\check{\mathbf{U}}$ + any linear combination of rows of $(\check{L} - I)$.

As an example, we consider the translated 2-polynomial over $GF(2^5)$, $A(z) = z^{16} + \alpha^{13}z^8 + \alpha^{30}z^4 + \alpha^{18}z^2 + \alpha^{20}z + \alpha^4$. As shown in an earlier example, the polynomial $A(z) - \alpha^4$ is represented by the matrix

$$L = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

We form the augmented matrix by annexing the additional row corresponding to $u = \alpha^4$, $\mathbf{U} = 00001$. The L-matrix may be reduced to a triangular idempotent form by adding the third column into all of the other columns and then adding the fifth column into the third column, giving

$$\check{L} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \check{L} - I = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

$$\check{U} = \begin{matrix} 0 & 0 & 1 & 0 & 1 \end{matrix}$$

One solution is seen to be $00101 = \alpha^7$. The other seven roots of $A(z)$ in $GF(2^5)$ are 10101, 01001, 11001, 00110, 10110, 01010, and 11010.

Thus, one may find all of the roots in $GF(p^m)$ of a translated p-polynomial by a straightforward procedure, which in practice is much simpler than the Chien search. Unfortunately, however, most poly-

nomials are not translated p-polynomials. Over fields of characteristic two, quadratics are translated 2-polynomials but cubics are not. However, if we multiply the general cubic, $x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$ by the factor $(x + \sigma_1)$, we obtain a translated 2-polynomial whose roots include the 3 roots of the cubic and the extraneous root σ_1. In general, *any* polynomial has a multiple which is a translated p-polynomial, and this multiple may be computed by a straightforward procedure: If $\sigma(x)$ has degree d, then compute the polynomials $r^{(0)}(x), r^{(1)}(x), \cdots, r^{(d-1)}(x)$ where $x^{p^k} \equiv r^{(k)}(x) \bmod \sigma(x)$ and $\deg r^{(k)}(x) < d = \deg \sigma(x)$. The $d + 1$ polynomials $1, r^{(0)}(x), r^{(1)}(x), \cdots, r^{(d-1)}(x)$ all have degree less than d, so they satisfy a linear dependence $c + \sum_{k=0}^{d-1} c_k r^{(k)}(x) = 0$, from which we deduce that $c + \sum_{k=0}^{d-1} c_k x^{p^k}$ is a multiple of $\sigma(x)$. It is obviously a translated p-polynomial of degree at most p^{d-1}. Similarly, Ore (1933) has shown that $\sigma(x)$ has a multiple which is a p-polynomial of degree at most p^d.

In general, if $\sigma(x)$ is any polynomial over $GF(p^m)$, one may compute the roots of $\sigma(x)$ in $GF(p^m)$ as follows: First, one finds the least multiple of $\sigma(x)$ which is a translated p-polynomial. Then, by solving the corresponding set of linear equations over $GF(p)$, one finds the roots of this translated p-polynomial in $GF(p^m)$. Finally, one examines each of the roots of this translated p-polynomial to decide which are roots of $\sigma(x)$.

If a BCH code of block length $p^m - 1$ is designed to correct t errors, then the degree of $\sigma(x)$ will be at most t, and the degree of its least multiple which is a translated p-polynomial will be at most p^{t-1}. If t is small compared to m, then our procedure results in considerable savings over the conventional Chien search. However, if $t > m$, then our procedure gains nothing, since in that case the least multiple of $\sigma(x)$ which is a translated p-polynomial is likely to be $x^{p^m} - x$. In that case, all elements in the field must still be tested.

In some cases, other transformations prove helpful. For example, consider the quartic equation over a field of characteristic 2: $x^4 + \sigma_1 x^3 + \sigma_2 x^2 + \sigma_3 x + \sigma_4$. Setting $y = x + (\sigma_3/\sigma_1)^{1/2}$ eliminates the linear term; setting $z = 1/y$ then gives a quartic which is a translated 2-polynomial. This quartic has $\sigma_1 = 0$. More generally, it can be shown that if p divides $\deg \sigma(x)$ and $\sigma_1 = 0$, then $\sigma(x)$ has a multiple of degree at most p^{d-2} which is a translated p-polynomial. If p does not divide $\deg \sigma(x)$, then $\sigma_1 = 0$ implies only that $\sigma(x)$ has a multiple of degree at most p^{d-1} which is a p-polynomial.

APPENDIX: Logs and Antilogs in GF(2^5), Base α, a Root of $z^5 + z^2 + 1$

We say $\log_\alpha \xi = k$ iff $\xi = \alpha^k$. We than have $\log_\alpha(\xi\eta) = \log_\alpha \xi + \log_\alpha \eta \bmod N$, where N is the least positive integer such that $\alpha^N = 1$.

		$1\alpha\alpha^2\alpha^2\alpha^4$	$1\alpha\alpha^2\alpha^3\alpha^4$	
-31	0	10000	00000	∞
-30	1	01000	00001	4
-29	2	00100	00010	3
-28	3	00010	00011	21
-27	4	00001	00100	2
-26	5	10100	00101	7
-25	6	01010	00110	20
-24	7	00101	00111	13
-23	8	10110	01000	1
-22	9	01011	01001	30
-21	10	10001	01010	6
-20	11	11100	01011	9
-19	12	01110	01100	19
-18	13	00111	01101	28
-17	14	10111	01110	12
-16	15	11111	01111	24
-15	16	11011	10000	0
-14	17	11001	10001	10
-13	18	11000	10010	29
-12	19	01100	10011	25
-11	20	00110	10100	5
-10	21	00011	10101	22
-9	22	10101	10110	8
-8	23	11110	10111	14
-7	24	01111	11000	18
-6	25	10011	11001	17
-5	26	11101	11010	27
-4	27	11010	11011	16
-3	28	01101	11100	11
-2	29	10010	11101	26
-1	30	01001	11110	23
	31	10000	11111	15

Received: June 10, 1966; revised May 4, 1967.

REFERENCES

BERLEKAMP, E. R., RUMSEY, H. AND SOLOMON, G. (1966), Solutions of algebraic equations in fields of characteristic 2. *Jet Propulsion Lab. Space Programs Summary* **4**, 37–39.

BERLEKAMP, E. R. (1967), Nonbinary BCH decoders. To be presented at IEEE International Symposium on Information Theory at Athens, Greece, and subsequently published in Transactions of the Professional Group on Information Theory (vol. **13** or **14**).

CHIEN, R. T. (1964), Cyclic decoding procedures for BCH codes. *PGIT* **IT 10**, 357–363.

HUGHES, D. R. (1959), Collineation groups of non-Desarguesian planes. *Am. J. Math.* **81**, 921–938 (see Lemma 5.1 on p. 934 and last paragraph of introduction, pp. 921, 922); *ibid.* **82**, 113–119.

ORE, O. (1933), On a special class of polynomials. *Trans. Am. Math. Soc.* **35**, 559–584; *ibid.* **36**, 275.

ORE, O. (1934), Contribution to the theory of finite fields. *Trans. Am. Math. Soc.* **36**, 243–274.

PETERSON, W. W. (1961), "Error Correcting Codes." Wiley, New York.

POLKINGHORN, F. A. (1966), Decoding of double and triple error correcting BCH codes. *PGIT* **IT 12**, 480–481.