Factoring Polynomials Over Finite Fields

By E. R. BERLEKAMP

(Manuscript received May 9, 1967)

We present here an algorithm for factoring a given polynomial over $GF(q)$ into powers of irreducible polynomials. The method reduces the factorization of a polynomial of degree m over $GF(q)$ to the solution of about $m(q - 1)/q$ linear equations in as many unknowns over $GF(q)$.

There are many applications in which one wishes to factor polynomials. Some programming systems, such as Brown's ALPAK,[1] deal with polynomials and rational functions with integer coefficients. In such a context one is interested not in approximate numerical values for the real and complex roots, but rather in irreducible factors which are themselves polynomials with integer coefficients. One of the standard tricks mentioned by Johnson[2] for finding such irreducible factors is to reduce all of the coefficients of the original polynomial modulo some prime, p, and then factor the reduced polynomial over the Galois Field, $GF(p)$. If the reduced polynomial factors, one gets certain constraints on the factors of the original polynomial; if the reduced polynomial does not factor over $GF(p)$, then one may conclude that the original polynomial is irreducible over the integers. The success of this method for factoring polynomials over the integers clearly depends upon having an efficient procedure for factoring polynomials over $GF(p)$.

The problem of factoring polynomials over finite fields arises directly in Golomb's study[3] of feedback shift register sequences. In Golomb's words, this study "... has found major applications in a wide variety of technological situations, including secure, reliable and efficient communications, digital ranging and tracking systems, deterministic simulation of random processes, and computer sequencing and timing schemes." The properties of all cyclic error correcting codes, including the important Bose-Chaudhuri[4]-Hocquenghem[5] codes, depend on the factors of their generator polynomials in some finite field. Such codes have been studied extensively by Peterson[6] and MacWilliams.[7] Recent advances in decoding techniques by Berlekamp[8] make these codes even more attractive from the practical standpoint.

We present here an algorithm for factoring a given polynomial,

$$f(z) = \sum_{k=0}^{m} f_k z^k, \qquad f_i \in GF(q),$$

into powers of irreducible polynomials.

First, we construct the $m \times m$ matrix Q over $GF(q)$, whose ith row represents $z^{q(i-1)}$ reduced modulo $f(z)$. Specifically,

$$z^{qi} \equiv \sum_{k=0}^{m-1} Q_{i+1,k+1} z^k \bmod f(z).$$

The Q matrix may be computed with a shift register wired to multiply by z mod $f(z)$. The register is started at 1, which is the first row of Q. After q shifts, the register contains the second row of Q; after q more shifts, it contains the third row of Q, $\cdots$, etc. After $q(m - 1)$ shifts, it contains the last row of Q.

Given any polynomial $g(z)$ of degree $<m$ over $GF(q)$, $g(z) = \sum_{i=0}^{m-1} g_i z^i$, we may compute the residue of $(g(z))^q$ mod $f(z)$ by multiplying the row vector $[g_0 , g_1 , \cdots , g_{m-1}]$ by the Q matrix. This follows from the observation that

$$\begin{aligned}(g(z))^q = g(z^q) = \sum_{i=0}^{m-1} g_i z^{qi} &= \sum_{i=0}^{m-1} \left(\sum_{k=0}^{m-1} g_i Q_{i+1,k+1} z^k \right) \\ &= \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} g_i Q_{i+1,k+1} \right) z^k .\end{aligned}$$

Similarly, we could compute $(g(z))^q - g(z)$ mod $f(z)$ by multiplying the row vector $[g_0 , g_1 , \cdots , g_{m-1}]$ by the matrix $(Q - I)$, where I is the $m \times m$ identity matrix over $GF(q)$.

Second, we find a set of row vectors which span the null space of $(Q - I)$. This may be done by appropriate column operations on the matrix $(Q - I)$.[8] Each such row vector in the null space of $(Q - I)$ represents a polynomial $g(z)$ which satisfies the equation $(g(z))^q - g(z) \equiv 0 \bmod f(z)$, and conversely, each $g(z)$ which satisfies this equation is represented by a row vector in the null space of $(Q - I)$.

Third, we select any of the polynomials $g(z)$ found in the second step, and apply Euclid's algorithm to determine the greatest common divisor of $f(z)$ and $g(z) - s$ for each $s \varepsilon GF(q)$.* We then have the factorization

$$f(z) = \prod_{s \varepsilon GF(q)} (\text{g.c.d.}\ (f(z),\ g(z) - s)).$$

Remark: If $g(z)$ is a scalar, then this factorization degenerates into

$$f(z) = \text{g.c.d.}\ (f(z), 0) \prod_{s \neq 0} \text{g.c.d.}\ (b(z), s)$$

$$= f(z) \prod_{s \neq 0} 1.$$

However, if $g(z)$ has positive degree, then the factorization is nontrivial.

Proof: Since $(g(z))^q - g(z) \equiv 0 \bmod f(z)$, $f(z)$ divides $(g(z))^q - g(z) = \prod_{s \varepsilon GF(q)} (g(z)) - s$. Therefore, $f(z)$ also divides

$$\prod_{s \varepsilon GF(q)} (\text{g.c.d.}\ (f(z),\ g(z) - s)).$$

On the other hand, g.c.d. $(f(z),\ g(z) - s)$ divides $f(z)$. If $s \neq t$, and $s,\ t\ \varepsilon\ GF(q)$, then $g(z) - s$ and $g(z) - t$ are relatively prime, as are g.c.d. $(f(z),\ g(z) - s)$, and g.c.d. $(f(z),\ g(z) - t)$. Therefore,

$$\prod_{s \varepsilon GF(q)} (\text{g.c.d.}\ (f(z),\ g(z) - s))$$

divides $f(z)$. Assuming both polynomials to be monic, they must be equal since each divides the other. Q.E.D.

Example I: Let $f(z)$ be the binary polynomial 1110001110001, or $f(z) = 1 + z + z^2 + z^6 + z^7 + z^8 + x^{12}$. The successive powers of z are

100000000000
010000000000
001000000000
000100000000
000010000000
000001000000
000000100000
000000010000
000000001000
000000000100
000000000010
000000000001
111000111000
011100011100
001110001110
000111000111
111011011011
100101010101
101010010010
010101001001
110010011100
011001001110
001100100111

[*] In practice, there is no need to perform all of Euclid's Algorithm q separate times to determine all of the g.c.d.'s. A short cut will be seen in the example.

$$\text{so} \qquad Q = \begin{array}{c} 100000000000 \\ 001000000000 \\ 000010000000 \\ 000000100000 \\ 000000001000 \\ 000000000010 \\ 111000111000 \\ 001110001110 \\ 111011011011 \\ 101010010010 \\ 110010011100 \\ 001100100111 \end{array} \qquad \text{and} \qquad Q - I = \begin{array}{c} 000000000000 \\ 011000000000 \\ 001010000000 \\ 000100100000 \\ 000010001000 \\ 000001000010 \\ 111000011000 \\ 001110011110 \\ 111011010011 \\ 101010010110 \\ 110010011110 \\ 001100100110 \end{array}.$$

If we number the columns of $Q - I$ from 0 to 11, then the upper right quarter of the $Q - I$ matrix may be zeroed if we add the 3rd column to the 6th column, the 1st, 2nd, and 4th columns to the 8th column, and the 5th column to the 10th column. The lower right quarter of the $Q - I$ matrix then becomes

$$R = \begin{array}{c} 011000 \\ 111110 \\ 011001 \\ 010110 \\ 011110 \\ 001110 \end{array}.$$

The equation $[g_6, g_7, \cdots, g_{11}]R = 0$ is found to have solutions $[g_6, g_7, \cdots, g_{11}] = [A, 0, 0, A, 0, A]$ where $A = 0$ or 1. The first six coordinants of g are then readily found from the equation $g(Q - I) = 0$, with solutions $g = [B, A, 0, A, A, 0, A, 0, 0, A, 0, A]$; $A, B \varepsilon GF(2)$. Finally, we apply Euclid's algorithm to $f(z) = 1110001110001$ and $g(z) = s10110100101$. By letting $t = s + 1$, and leaving s as an indeterminate, we may effectively find the g.c.d. of 111000111001 and 010110100101 with the same computation that computes the g.c.d. of 111000111001 and 110110100101:

$$\begin{array}{r} 1110001110001 \\ \underline{s10110100101} \\ 1\,t001110101 \\ \underline{s10110100101} \\ s0\,t11101 \\ \underline{1\,t001110101} \\ 1\,t0\,s1\,s01 \\ \underline{s0\,t11101}. \\ t\,t\,t\,t0\,t \end{array}$$

If $t = 0$, the g.c.d. is 10011101; if $s = 0$, the g.c.d. of 1110001110001 and 010110100101 is equal to the g.c.d. of 111101 and 11001001, which is 111101. Both 111101 and 10011101 are irreducible and the factorization is complete:

$$(1 + z + z^2 + z^6 + z^7 + z^8 + z^{12})$$
$$= (1 + z + z^2 + z^3 + z^5)(1 + z^3 + z^4 + z^5 + z^7) \quad \text{over } GF(2).$$

In general, suppose $f(z) = \prod_i (p^{(i)}(z))^{e_i}$, where each $p^{(i)}(z)$ is an irreducible polynomial over $GF(q)$. Then $f(z)$ divides

$$\prod_{s \varepsilon GF(q)} (g(z) - s)$$

if each $(p^{(i)}(z))^{e_i}$ divides $g(z) - s_i$ for some $s_i \varepsilon GF(q)$. On the other hand, given any set of scalars $s_1, s_2, \cdots, s_n \varepsilon GF(q)$, then the Chinese remainder theorem guarantees the existence of a unique $g(z) \bmod f(z)$ such that $g(z) \equiv s_i \bmod (p^{(i)}(z))^{e_i}$ for all i. Since there are q^n choices of $s_1, s_2, \cdots, s_n$, there are exactly q^n solutions of the equation $(g(z))^q - g(z) \equiv 0 \bmod f(z)$. Therefore,

The number of distinct irreducible factors of $f(z)$ is equal to the dimension of the null space of $(Q - I)$.

In particular, the polynomial $f(z)$ is the power of an irreducible polynomial iff the null space of $(Q - I)$ has dimension 1. In this case, the only solutions of $(g(z))^q - g(z) \equiv 0 \bmod f(z)$ are scalars in $GF(q)$, and the null space of $Q - I$ contains only vectors of the form $[s, 0, 0, \cdots, 0]$. If the null space of $Q - I$ has dimension n, it has a basis consisting of n monic polynomials: $g^{(1)}(z), g^{(2)}(z), \cdots, g^{(n)}(z)$. Without loss of generality, we may assume that $g^{(n)}(z) = 1$ and that the other $n - 1$ basis polynomials have positive degree.

When we apply Euclid's algorithm to $f(z)$ and $g^{(1)}(z) - s$, we obtain a factorization of $f(z)$. If this gives fewer than n factors of $f(z)$, then we may compute the g.c.d. of $g^{(2)}(z) - s$ and each known factor of $f(z)$. By this process, we may continue to refine the factorization of $f(z)$. The following argument shows that this process must eventually yield all n irreducible-powers which are factors of $f(z)$.

Let C be the $n \times n$ matrix over $GF(q)$ defined by the equations $g^{(j)}(z) \equiv C_{i,j} \bmod (p^{(i)}(z))^{e_i}$. Then C must be nonsingular. For if $\sum_j A_j C_{i,j} = 0$ for all i, then $\sum_j A_j g^{(j)}(z) \equiv 0 \bmod (p^{(i)}(z))^{e_i}$ for all i, whence $\sum_j A_j g^{(j)}(z) = 0$, contradicting the linear independence of $g^{(1)}(z), g^{(2)}(z), \cdots, g^{(n)}(z)$. When we apply Euclid's algorithm to $f(z)$ and $g^{(j)}(z) - s$, we obtain a factorization of $f(z)$ into as many different factors as there are distinct elements in the jth row of C. The irreducible-powers $(p^{(i)}(z))^{e_i}$ and $(p^{(k)}(z))^{e_k}$ are separated iff $C_{i,j} \neq C_{k,j}$. Since C is nonsingular, for every i and k there exists some j such that $C_{i,j} \neq C_{k,j}$. Thus, any two irreducible-power factors of $f(z)$ will be separated by some $g^{(i)}(z)$.

The factorization of any power of an irreducible polynomial is readily accomplished by applying Euclid's algorithm to the polynomial and its derivative.

We conclude with another example.

Example II: Following a suggestion of R. L. Graham, we let $f(z) = z^n - 1$ over $GF(q)$, where n and q are relatively prime. Then $Q_{i+1\ ,j+1} = 1$ if $qi \equiv j \bmod n$. Specifically, suppose $n = 15$ and $q = 2$. Then

$$Q = \begin{array}{c}
100000000000000\\
001000000000000\\
000010000000000\\
000000100000000\\
000000001000000\\
000000000010000\\
000000000000100\\
000000000000001\\
010000000000000\\
000100000000000\\
000001000000000\\
000000010000000\\
000000000100000\\
000000000001000\\
000000000000010
\end{array}
\qquad
Q - I = \begin{array}{cr}
000000000000000 & 0\\
011000000000000 & 1\\
001010000000000 & 2\\
000100100000000 & 3\\
000010001000000 & 4\\
000001000010000 & 5\\
000000100000100 & 6\\
000000010000001 & 7\\
010000001000000 & 8\\
000100000100000 & 9\\
000001000010000 & 10\\
000000010001000 & 11\\
000000000100100 & 12\\
000000000001010 & 13\\
000000000000011 & 14
\end{array}$$

By suitably permuting the rows and columns, we can bring $Q - I$ into the form

$$\begin{array}{c|c|c|c|cr}
0 & 0000 & 0000 & 0000 & 00 & 0\\
\hline
0 & 1100 & 0000 & 0000 & 00 & 1\\
0 & 0110 & 0000 & 0000 & 00 & 2\\
0 & 0011 & 0000 & 0000 & 00 & 4\\
0 & 1001 & 0000 & 0000 & 00 & 8\\
\hline
0 & 0000 & 1100 & 0000 & 00 & 7\\
0 & 0000 & 0110 & 0000 & 00 & 14\\
0 & 0000 & 0011 & 0000 & 00 & 13\\
0 & 0000 & 1001 & 0000 & 00 & 11\\
\hline
0 & 0000 & 0000 & 1100 & 00 & 3\\
0 & 0000 & 0000 & 0110 & 00 & 6\\
0 & 0000 & 0000 & 0011 & 00 & 12\\
0 & 0000 & 0000 & 1001 & 00 & 9\\
\hline
0 & 0000 & 0000 & 0000 & 11 & 5\\
0 & 0000 & 0000 & 0000 & 11 & 10
\end{array}$$

A basis for the null space of $Q - I$ is seen to be

$$\begin{aligned} g^{(1)}(z) &= z + z^2 + z^4 + z^8 \\ g^{(2)}(z) &= z^7 + z^{14} + z^{13} + z^{11} \\ g^{(3)}(z) &= z^3 + z^6 + z^{12} + z^9 \\ g^{(4)}(z) &= z^5 + z^{10}. \end{aligned}$$

In general, if $f(z) = z^n - 1$ over $GF(q)$, then we may choose

$$g(z) = \sum_{k \varepsilon C} z^k,$$

where C is any set of numbers which is closed under multiplication by q mod n. Each such polynomial $g(z)$ has some nontrivial factor in common with $z^n - 1$.

REFERENCES

1. Brown, W. S., ALPAK System for Numerical Algebra on a Digital Computer-I:—Polynomials in Several Variables and Truncated Power Series with Polynomial Coefficients, B.S.T.J., *42,* September, 1963, pp. 2081–2119.
2. Johnson, S. C., Tricks for Improving Kronecker's Polynomial Factoring Algorithm, unpublished work.
3. Golomb, S. W., *Shift Register Sequences,* Holden-Day, Inc., 1967.
4. Bose, R. C. and Ray-Chaudhuri, D. K., On a Class of Error-Correcting Binary Group Codes, Inform. Control, *3,* 1960, pp. 68–79.
5. Hocquenghem, A., Codes Correcteurs D'Erreurs, Chiffres, *2,* 1959, pp. 147–156.
6. Peterson, W. W., *Error-Correcting Codes,* MIT Press-Wiley, New York, 1961.
7. MacWilliams, J., The Structure and Properties of Binary Cyclic Alphabets, B.S.T.J., *44,* February 1965, pp. 303–332.
8. Berlekamp, E. R., *Algebraic Coding Theory,* McGraw-Hill Book Company, Inc., New York, 1968.