PACIFIC JOURNAL OF MATHEMATICS
Vol. 96, No. 1, 1981

ROUND TRINOMIALS

RICHARD W. MARSH, W. H. MILLS, ROBERT L. WARD
HOWARD RUMSEY, JR. AND LLOYD R. WELCH

Let $F(x)$ be a polynomial of degree D. We say that $F(x)$ is *round* if all its irreducible factors have relatively small degree (e.g., bounded by a small multiple of $\log D$). In the present paper we introduce new methods for the study of round polynomials. Using these methods we prove the existence of many classes of round trinomials over $GF(2)$, including all the previously known ones as well as many new ones.

Let $F(x)$ be a polynomial over $GF(2)$, and let α be a root of $F(x)$. Let Q be a power of 2, say $Q = 2^q$, and let σ be the automorphism of the splitting field of $F(x)$ defined by $\sigma\xi = \xi^Q$. We seek a linear relation over $GF(2)$ among $\alpha, \sigma\alpha, \sigma^2\alpha, \cdots, \sigma^m\alpha$ with m reasonably small. In § 2 we will show how to use such a linear relation to show that $F(x)$ is round.

The archetypical example of a round polynomial over $GF(2)$ is $F(x) = x^Q + x$. The irreducible factors of $F(x)$ are precisely all the irreducible polynomials whose degrees are divisors of q. Here we have $\sigma\alpha + \alpha = 0$, which is a linear relation of the desired type. The methods of § 2 show that this linear relation implies that the degree of the irreducible factor of $F(x)$ satisfied by α must divide q.

Our example is extended below to other cases in which the exponents of $F(x)$ are expressed in terms of Q. Even more generally we will consider polynomials $F(x)$ over $GF(2)$ whose exponents depend on two powers of 2, Q and R, and where the linear relation among the $\sigma^i\alpha$ has coefficients in $GF(R)$.

Our methods can clearly be generalized to work on polynomials over arbitrary finite fields—generalizations to polynomials over other finite fields of characteristic 2 are particularly easy, but we are primarily interested in trinomials over $GF(2)$, so we will stick to this case. Some of the old results we present have already been generalized to arbitrary finite fields and we will content ourselves with giving appropriate references.

Most of the results of this paper were first suggested by actual factorizations of trinomials, and then later proofs were found. Indeed a table of all trinomial factorizations over $GF(2)$ through degree 599 was compiled by the authors using a CDC-6600 computer program written by Neal Zierler. All of the really striking examples of round trinomials that were found this way can be accounted for by the theorems of this paper.

Solomon W. Golomb [3] has made two conjectures concerning possible families of round trinomials. The first was proved by Mills and Zierler [5] and is a special case of Theorem 7 of the present paper. The second concerns the family

$$x^{2^q+1} + x^{2^q-2} + 1 .$$

Here we note that the cases $q = 2, 4, 5, 6$ of this conjecture are special cases of theorems of the present paper, and thus these trinomials are round for other reasons. We have factored these polynomials for all $q \leqq 12$, and the results do not suggest any general result.

For many of the trinomials we study, a more careful analysis yields a good deal of additional information about the periods of the roots and about the number of roots in various extension fields of $GF(Q)$. Some of the trinomials we study are closely related to each other. Moreover there are a number of trinomials whose irreducible factors all have the same degree. In the interest of brevity we omit all this.

We will work throughout this paper in a finite field of characteristic 2 that is sufficiently large to contain all the roots of $F(x)$ as well as finite fields of Q elements and R elements. Thus we can regard $GF(Q)$ and $GF(R)$ as subfields of this large field.

Throughout this paper we will adopt the convention that

$$\beta_i = \sigma^i\beta = \beta^{Q^i}$$

for any element β in one of our finite fields. This convention will not apply to matrices.

2. **Consequences of the linear relation.** Let $Q = 2^q$ and $R = 2^r$ be two fixed powers of 2. Let $F(x)$ be a polynomial over $GF(2)$, and let α be any root of $F(x)$. We have to rely on *ad hoc* methods to find a linear relation between the α_i. Once we have such a relation we can proceed systematically. In this section we show how to do this.

Suppose we have a linear relation

$$\alpha_m = a\alpha_{m-1} + b\alpha_{m-2} + \cdots + d\alpha_1 + e\alpha_0 , \tag{1}$$

where $a, b, \cdots, d, e$ are elements of $GF(R)$ and $e \neq 0$. Raising both sides of (1) to the Q^jth power we get

$$\alpha_{m+j} = a_j\alpha_{m+j-1} + b_j\alpha_{m+j-2} + \cdots + d_j\alpha_{j+1} + e_j\alpha_j$$

for any nonnegative integer j. We let W_j be the m by m nonsingular matrix

$$W_j = \begin{bmatrix} a_j & b_j \cdots d_j & e_j \\ 1 & 0 \cdots 0 & 0 \\ 0 & 1 \cdots 0 & 0 \\ & \vdots & \\ 0 & 0 \cdots 1 & 0 \end{bmatrix}$$

and we set $P_j = W_{j-1} \cdots W_1 W_0$. Then we have

$$\begin{bmatrix} \alpha_{m+j-1} \\ \vdots \\ \alpha_{j+1} \\ \alpha_j \end{bmatrix} = P_j \begin{bmatrix} \alpha_{m-1} \\ \vdots \\ \alpha_1 \\ \alpha_0 \end{bmatrix}.$$

In particular if $P_v = I$ for some integer v, then $\alpha_v = \alpha_0$, and α lies in the field $GF(Q^v)$. We let s denote the greatest common divisor (q, r) of q and r, $S = 2^s$, and $t = r/s$. Then $GF(R) \subseteq GF(Q^t)$, and therefore $W_{j+t} = W_j$ for all j. We now set $P = P_t$. We have $P_{kt} = P^k$ for all nonnegative integers k. Let σ be the automorphism of $GF(R)$ such that $\sigma\xi = \xi^Q = \xi_1$ for all ξ in $GF(R)$. Then we have $\sigma W_j = W_{j+1}$ for all j so that

$$\sigma P = W_t W_{t-1} \cdots W_2 W_1 = W_0 W_{t-1} \cdots W_2 W_1 = W_0 P W_0^{-1}.$$

Let $H(x)$ be the characteristic polynomial of P. Since $\sigma P = W_0 P W_0^{-1}$, it follows that the coefficients of $H(x)$ are left fixed by σ so that they lie in $GF(Q)$ as well as in $GF(R)$. Since $GF(S) = GF(Q) \cap GF(R)$ these coefficients lie in $GF(S)$.

It is sufficient to find an integer k such that $H(x) | (x^k + 1)$, for then we have $P_{kt} = P^k = I$, $\alpha_{kt} = \alpha_0$, $\alpha \in GF(Q^{kt})$, and the degree of the irreducible polynomial which has α as a root must be a factor of qkt.

It frequently happens that $GF(R) \subseteq GF(Q)$. In this case $t = 1$, $P = W_0$, and

$$H(x) = x^m + ax^{m-1} + bx^{m-2} + \cdots + e.$$

3. Known results. In this section we discuss some previously known results about round trinomials over $GF(2)$.

It is clear that if two polynomials $F(x)$ and $G(x)$ satisfy a relation of the type $F(x^n) = G(x^m)$ where n and m are positive integers, then the degrees of their irreducible factors are related. We say that two polynomials belong to the same equivalence class if they are related in this way, and we will study only one polynomial in any given equivalence class.

Naturally we will consider only trinomials of the form

$$F(x) = x^n + x^a + 1.$$

The reverse polynomial $x^n + x^{n-a} + 1$ factors in the same way and we need only consider one of these two polynomials.

Perhaps the best known round trinomials are the ones of the form

$$F(x) = x^Q + x + 1 , \quad Q = 2^q .$$

Here we have

$$\alpha_1 + \alpha_0 + 1 = F(\alpha) = 0$$

for any root α of $F(x)$. Raising both sides of this equation to the Qth power we get $\alpha_2 + \alpha_1 + 1 = 0$, so that we must have $\alpha_2 = \alpha_0$. Thus $\alpha \in GF(Q^2)$. If $\alpha \in GF(Q)$, then $\alpha_1 = \alpha_0$ so that $F(\alpha) = 1$, a contradiction. Therefore $\alpha \notin GF(Q)$. Thus we see that all roots of $x^Q + x + 1$ lie in $GF(Q^2)$, but not in $GF(Q)$, and we have the following result.

THEOREM 1. *(Riordan) Suppose $F(x) = x^Q + x + 1$, where $Q = 2^q$, and let $f(x)$ be an irreducible factor of $F(x)$ over $GF(2)$. Then the degree of $f(x)$ divides $2q$, but not q.*

Another formulation of Theorem 1 states that all the irreducible factors of $F(x)$ over $GF(Q)$ have degree 2.

Next we come to trinomials of the type

$$F(x) = x^{Q^n - 1} + x^{Q^a - 1} + 1 , \quad Q = 2^q ,$$

where n and a are positive integers, $n > a$. For any root α of $F(x)$ we have

$$0 = \alpha F(\alpha) = \alpha_n + \alpha_a + \alpha_0 .$$

Thus we already have a linear relation of the type we need. We apply the results of § 2 with $R = 2$, $r = s = t = 1$, and $H(x) = x^n + x^a + 1$. We see that if k is a positive integer such that $H(x) | (x^k + 1)$, then $\alpha \in GF(Q^k)$, and the degree of the irreducible polynomial with root α must divide qk. Thus we have the following result.

THEOREM 2. *Suppose that $F(x) = x^{Q^n - 1} + x^{Q^a - 1} + 1$, where $Q = 2^q$, and n and a are positive integers, $n > a$. Suppose that k is a positive integer such that*

$$(x^n + x^a + 1) | (x^k + 1) .$$

Let $f(x)$ be an irreducible factor of $F(x)$ over $GF(2)$. Then the degree of $f(x)$ divides kq.

Theorem 2 is usually stated in terms of the polynomial

$$x^{(Q^n - 1)/(Q-1)} + x^{(Q^a - 1)/(Q-1)} + 1 ,$$

whose roots are the $(Q-1)$st powers of the roots of $F(x)$. If we set $n=2$ and $a=1$ we get the celebrated round trinomial

$$x^{Q+1}+x+1\,,$$

which was first studied by Riordan.

Theorem 2 can be easily generalized [4] to the case of polynomials with an arbitrary number of terms over an arbitrary finite field.

4. **Some new results.** Next we come to some examples in which there are relations between the α_i that contain quadratic, cubic, and quartic terms, and it is necessary to do some algebraic manipulation to obtain the kind of linear identity we need. The first of these is the polynomial

$$F(x)=x^{Q^2+1}+x^Q+1\,,\quad Q=2^q\,.$$

Letting α be a root of $F(x)$ as usual, we obtain

$$\alpha_0\alpha_2+\alpha_1+1=F(\alpha)=0\,.$$

Raising both sides of this to the Qth power we get

$$\alpha_1\alpha_3+\alpha_2+1=0\,.$$

Adding the last two equations we get

$$\alpha_2(\alpha_0+1)+\alpha_1(\alpha_3+1)=0\,.$$

Raising this to the Qth power we get

$$\alpha_3(\alpha_1+1)+\alpha_2(\alpha_4+1)=0\,.$$

Since $\alpha_1+1=\alpha_0\alpha_2$, it follows that $\alpha_4+1=\alpha_3\alpha_5$. Substituting these two in the previous equation we get

$$0=\alpha_0\alpha_2\alpha_3+\alpha_2\alpha_3\alpha_5=\alpha_2\alpha_3(\alpha_0+\alpha_5)\,.$$

Clearly $\alpha\neq 0$, so that $\alpha_2\neq 0$ and $\alpha_3\neq 0$. Therefore we must have $\alpha_5=\alpha_0$, so that $\alpha\in GF(Q^5)$.

If α is a root of $F(x)$ that lies in $GF(Q)$, then we must have $\alpha^2+\alpha+1=0$ and q must be even. Therefore an irreducible factor $f(x)$ of $F(x)$ has degree dividing q if and only if q is even and $f(x)=x^2+x+1$. Thus we have the following result.

THEOREM 3. *Suppose* $F(x)=x^{Q^2+1}+x^Q+1$, $Q=2^q$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $5q$. *If the degree of* $f(x)$ *divides* q, *then* q *is even and* $f(x)=x^2+x+1$.

Another formulation of Theorem 3 states that the irreducible factors of $F(x)$ over $GF(Q)$ all have degree 5 except for two linear factors that occur when q is even.

A typical example of Theorem 3 is $x^{257} + x^{16} + 1$, which has 1 irreducible factor of degree 2, 1 of degree 5, 1 of degree 10, and 12 of degree 20. Moreover the polynomial $x^{1025} + x^{32} + 1$ has 41 irreducible factors, all of degree 25.

Our next example is the polynomial

$$F(x) = x^{Q+1} + x^A + 1 , \quad A^2 = 2Q = 2^{q+1} .$$

Here, of course, q is odd. We have

$$\alpha_0\alpha_1 + \alpha_0^A + 1 = F(\alpha) = 0 ,$$

so that we get

$$\alpha_0^A = \alpha_0\alpha_1 + 1 .$$

Raising both sides of this to the Ath power we obtain

$$\begin{aligned} \alpha_1^2 = \alpha_0^{A^2} &= \alpha_0^A\alpha_1^A + 1 = (\alpha_0\alpha_1 + 1)(\alpha_1\alpha_2 + 1) + 1 \\ &= \alpha_0\alpha_1^2\alpha_2 + \alpha_0\alpha_1 + \alpha_1\alpha_2 . \end{aligned}$$

Since $\alpha \neq 0$, we have $\alpha_1 \neq 0$, and we get

$$\alpha_0\alpha_1\alpha_2 = \alpha_0 + \alpha_1 + \alpha_2 . \tag{2}$$

We note that if $\alpha \in GF(Q)$, then $\alpha_0 = \alpha_1 = \alpha_2 = \alpha$ and (2) yields $\alpha^3 = \alpha$, which implies that $\alpha = 0$ or 1, which is impossible. Therefore $F(x)$ has no roots in $GF(Q)$.

Raising both side of (2) to the Qth power we get

$$\alpha_1\alpha_2\alpha_3 = \alpha_1 + \alpha_2 + \alpha_3 .$$

Adding this to (2) we obtain $(\alpha_0 + \alpha_3)\alpha_1\alpha_2 = \alpha_0 + \alpha_3$, or

$$0 = (\alpha_0 + \alpha_3)(\alpha_1\alpha_2 + 1) = \alpha_1^A(\alpha_0 + \alpha_3) .$$

It follows that $\alpha_3 = \alpha_0$. Thus we have the following result.

THEOREM 4. *Suppose* $F(x) = x^{Q+1} + x^A + 1$, *where* $Q = 2^q$ *and* $A^2 = 2Q$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $3q$ *but not* q.

Another formulation of Theorem 4 states that the irreducible factors of $F(x)$ over $GF(Q)$ all have degree 3.

Next we come to the polynomial

$$F(x) = x^{Q+A} + x^{Q-1} + 1 , \quad A^2 = 2Q = 2^{q+1} .$$

Here again q must be odd. We have

$$\alpha_0^{A+1}\alpha_1 + \alpha_1 + \alpha_0 = \alpha F(\alpha) = 0 .$$

Now $\alpha \neq 0$, so that $\alpha_0^{A+1}\alpha_1 \neq 0$ and we have $\alpha_1 + \alpha_0 \neq 0$. This implies that $\alpha \notin GF(Q)$.

We must now get rid of the A in our equality. To do this we raise both sides to the Ath power to obtain

$$0 = \alpha_0^{A^2+A}\alpha_1^A + \alpha_1^A + \alpha_0^A = \alpha_1^2\alpha_0^A\alpha_1^A + \alpha_1^A + \alpha_0^A .$$

Multiplying both sides by $\alpha_0\alpha_1\alpha_2$ and using $\alpha_0^{A+1}\alpha_1 = \alpha_1 + \alpha_0$ and $\alpha_1^{A+1}\alpha_2 = \alpha_2 + \alpha_1$ we get

$$\begin{aligned} 0 &= \alpha_0^{A+1}\alpha_1^{A+3}\alpha_2 + \alpha_0\alpha_1^{A+1}\alpha_2 + \alpha_0^{A+1}\alpha_1\alpha_2 \\ &= \alpha_1(\alpha_1 + \alpha_0)(\alpha_2 + \alpha_1) + \alpha_0(\alpha_2 + \alpha_1) + \alpha_2(\alpha_1 + \alpha_0) \\ &= \alpha_1(\alpha_1 + \alpha_0)(\alpha_2 + \alpha_1) + \alpha_0\alpha_1 + \alpha_1\alpha_2 . \end{aligned}$$

Since $\alpha_1 \neq 0$ this yields

$$(\alpha_1 + \alpha_0)(\alpha_2 + \alpha_1) = \alpha_2 + \alpha_0 .$$

We have already seen that $\alpha_1 + \alpha_0 \neq 0$, so that $\alpha_2 + \alpha_1 \neq 0$, and our last equality gives us $\alpha_2 \neq \alpha_0$. Thus none of the roots of $F(x)$ lies in $GF(Q^2)$.

From our last equality we get

$$(\alpha_2 + \alpha_1)(\alpha_3 + \alpha_2) = \alpha_3 + \alpha_1 ,$$

and hence

$$(\alpha_2 + \alpha_0)(\alpha_2 + \alpha_1)(\alpha_3 + \alpha_2) = (\alpha_1 + \alpha_0)(\alpha_2 + \alpha_1)(\alpha_3 + \alpha_1) .$$

This can be written in the form

$$(\alpha_2 + \alpha_1)^2(\alpha_3 + \alpha_2 + \alpha_1 + \alpha_0) = 0 .$$

We have already observed that $\alpha_2 + \alpha_1 \neq 0$, so that we obtain

$$\alpha_3 + \alpha_2 + \alpha_1 + \alpha_0 = 0 ,$$

which implies that $\alpha_4 = \alpha_0$ and $\alpha \in GF(Q^4)$.

We have proved the following result.

THEOREM 5. *Suppose* $F(x) = x^{Q+A} + x^{Q-1} + 1$, *where* $Q = 2^q$ *and* $A^2 = 2Q$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $4q$ *but not* $2q$.

Another formulation of Theorem 5 states that the irreducible factors of $F(x)$ over $GF(Q)$ all have degree 4.

Next we study the trinomial

$$F(x) = x^{3Q+2} + x^{2Q+3} + 1 , \quad Q = 2^q .$$

We begin by noting that if the root α of $F(x)$ is an element of $GF(Q)$, then $F(\alpha) = 1$, a contradiction. Thus none of the roots of $F(x)$ lies in $GF(Q)$.

Since α is a root of $F(x)$ we have

$$0 = F(\alpha) = \alpha_0^2\alpha_1^3 + \alpha_0^3\alpha_1^2 + 1 .$$

Raising both sides to the Qth power we get

$$0 = \alpha_1^2\alpha_2^3 + \alpha_1^3\alpha_2^2 + 1 .$$

Adding these two equations we get

$$\begin{aligned} 0 &= \alpha_1^2(\alpha_2^3 + \alpha_0^3) + \alpha_1^3(\alpha_2^2 + \alpha_0^2) \\ &= \alpha_1^2(\alpha_2 + \alpha_0)(\alpha_2^2 + \alpha_0\alpha_2 + \alpha_0^2 + \alpha_0\alpha_1 + \alpha_1\alpha_2) . \end{aligned}$$

Since $\alpha \notin GF(Q)$, we have $\alpha \neq 0$, so that $\alpha_1 \neq 0$. Hence we have either $\alpha_2 = \alpha_0$ or

$$\alpha_2^2 + \alpha_0\alpha_2 + \alpha_0^2 + \alpha_0\alpha_1 + \alpha_1\alpha_2 = 0 . \tag{3}$$

If $\alpha_2 = \alpha_0$, then $\alpha \in GF(Q^2)$, and the degree of the irreducible polynomial with root α divides $2q$.

Now suppose that (3) holds. Raising both sides of (3) to the Qth power and adding the result to (3) we get

$$\begin{aligned} 0 &= \alpha_3^2 + \alpha_1\alpha_3 + \alpha_1^2 + \alpha_2\alpha_3 + \alpha_2^2 + \alpha_0\alpha_2 + \alpha_0^2 + \alpha_0\alpha_1 \\ &= (\alpha_3 + \omega\alpha_2 + \omega\alpha_1 + \alpha_0)(\alpha_3 + \omega^2\alpha_2 + \omega^2\alpha_1 + \alpha_0) , \end{aligned}$$

where ω is a root of $x^2 + x + 1$, i.e., a primitive cube root of unity. Since ω and ω^2 are the roots of $x^2 + x + 1$, we have

$$\alpha_3 + \omega\alpha_2 + \omega\alpha_1 + \alpha_0 = 0 , \tag{4}$$

for some ω satisfying $\omega^2 + \omega + 1 = 0$. Thus we have a linear relation of the type given by (1), so we can apply the results of § 2 with $R = 4$, $r = 2$. There are two cases.

Case 1. q even. In this case $GF(R) \subseteq GF(Q)$. By the results of § 2 the characteristic polynomial $H(x)$ of P is

$$H(x) = x^3 + \omega x^2 + \omega x + 1 = (x + 1)(x^2 + \omega^2 x + 1) .$$

We see at once that $H(x)$ is a factor of $x^5 + 1$, and we have $\alpha_5 = \alpha_0$, $\alpha \in GF(Q^5)$, and the degree of the irreducible polynomial satisfied by α divides $5q$.

Case 2. q odd. In this case $\omega^Q = \omega^2$. Here, in the notation of § 2, we have $s = 1$, $t = 2$,

$$P = \begin{bmatrix} \omega^2 & \omega^2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \omega & \omega & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \omega & 0 & \omega^2 \\ \omega & \omega & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and $H(x) = x^3 + 1$. Thus we have $\alpha_6 = \alpha_0$, $\alpha \in GF(Q^6)$, and the degree of the irreducible polynomial with α as a root must divide $6q$.

In this case if $\alpha \in GF(Q^3)$, then $\alpha_3 = \alpha_0$ and (4) yields $\alpha_2 = \alpha_1$, which in turn implies that $\alpha_1 = \alpha_0$ and $\alpha \in GF(Q)$, a contradiction.

We sum up these results in the following theorem.

THEOREM 6. *Let* $F(x) = x^{3Q+2} + x^{2Q+3} + 1$ *where* $Q = 2^q$. *If* q *is even then the degrees of the irreducible factors of* $F(x)$ *over* $GF(2)$ *all divide either* $2q$ *or* $5q$, *but not* q. *If* q *is odd, then the degrees of the irreducible factors of* $F(x)$ *divide* $6q$, *but not* $3q$.

5. **The M function.** As before we let R be a fixed power of 2.

Given n variables $U, V, \cdots, Y, Z$, let $M(U, V, \cdots, Y, Z)$ denote the determinant

$$M(U, V, \cdots, Y, Z) = \begin{bmatrix} U & V & \cdots & Y & Z \\ U^R & V^R & \cdots & Y^R & Z^R \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ U^{R^{n-1}} & V^{R^{n-1}} & \cdots & Y^{R^{n-1}} & Z^{R^{n-1}} \end{bmatrix}.$$

When we wish to emphasize the number n of variables we will write $M_n(U, V, \cdots, Y, Z)$ for $M(U, V, \cdots, Y, Z)$. This function has a number of properties that we will need later.

Property I. $M(U, V, \cdots, Y, Z)$ is a symmetric function of $U, V, \cdots, Y, Z$.

Since we are working over $GF(2)$ any interchange of columns leaves our determinant unchanged so that Property I holds.

Property II. If any two of $U, V, \cdots, Y, Z$ are equal then $M(U, V, \cdots, Y, Z) = 0$.

This is an immediate consequence of the fact that a determinant with two identical columns must vanish.

Property III. The M function is a linear function in each variable over $GF(R)$ in the sense that

$$M(U, \cdots, V, A + B, X, \cdots, Z) = M(U, \cdots, V, A, X, \cdots, Z) + M(U, \cdots, V, B, X, \cdots, Z),$$

and

$$M(U, \cdots, V, aW, X, \cdots, Z) = aM(U, \cdots, V, W, X, \cdots, Z)$$

for any a in $GF(R)$.

Since R is a power of 2, we have $(A + B)^{R^i} = A^{R^i} + B^{R^i}$. Since a is in $GF(R)$ we have $(aW)^{R^i} = aW^{R^i}$. Property III follows immediately.

Property IV. $M_n(U, V, \cdots, Y, Z)$ has the factorization

$$M_n(U, V, \cdots, Y, Z) = M_{n-1}(V, \cdots, Y, Z) \cdot \prod (U + \eta V + \cdots + \mu Y + \nu Z)$$

where the product is over all $\eta, \cdots, \mu, \nu$ in $GF(R)$. Thus there are R^{n-1} factors in this product.

If we regard $M_n(U, V, \cdots, Y, Z)$ as a polynomial in U we see that it has degree R^{n-1} and its leading coefficient is $M_{n-1}(V, \cdots, Y, Z)$. Moreover by Properties II and III we see that every linear combination of $V, \cdots, Y, Z$ over $GF(R)$ is a root. Since the number of such linear combinations equals the degree of our polynomial, Property IV follows immediately.

It follows from Property IV that $M(U, V, \cdots, Y, Z) = 0$ if and only if some linear combination of its arguments is zero.

Property V. The following identity holds:

$$M_2(M_{n-1}(U, V, \cdots, Y), M_{n-1}(V, \cdots, Y, Z)) = (M_{n-2}(V, \cdots, Y))^R \cdot M_n(U, V, \cdots, Y, Z) .$$

This can be verified by factoring both sides using Properties IV, I, and III. It is more elegant to note that

$$(M_{n-2}(V, \cdots, Y))^R = M_{n-2}(V^R, \cdots, Y^R)$$

is the value of the $n - 2$ by $n - 2$ determinant obtained from the determinant for $M_n(U, V, \cdots, Y, Z)$ by removing its first and last rows and its first and last columns. Hence by Jacobi's theorem on the minors of the adjoint (for example see [1, pages 97-99]), the right hand side of our identity must equal the determinant

$$\begin{vmatrix} A_{11} & A_{1n} \\ A_{n1} & A_{nn} \end{vmatrix}$$

where A_{ij} denotes the cofactor of the element in the ith row and the jth column of our n by n matrix. We have

$$A_{11} = (M_{n-1}(V, \cdots, Y, Z))^R ,$$

$$A_{1n} = (M_{n-1}(U, V, \cdots, Y))^R ,$$
$$A_{n1} = M_{n-1}(V, \cdots, Y, Z) ,$$
$$A_{nn} = M_{n-1}(U, V, \cdots, Y) .$$

Since $M_2(X, Y) = XY^R + X^RY$, Property V follows immediately.

6. The trinomial $x^{QR+1} + x^{Q+R} + 1$. In this section we study the trinomial

$$F(x) = x^{QR+1} + x^{Q+R} + 1 , \quad Q = 2^q , \quad R = 2^r .$$

We let α be a root of $F(x)$. We use the notation and results of § 2 as well as the M function of the last section.

We begin by noting that if α is an element of $GF(Q)$, then $F(\alpha) = 1$, a contradiction. Thus none of the roots of $F(x)$ lies in $GF(Q)$. By symmetry none of the roots of $F(x)$ lies in $GF(R)$.

Since α is a root of $F(x)$ we have

$$1 = F(\alpha) + 1 = \alpha_0\alpha_1^R + \alpha_0^R\alpha_1 = M(\alpha_0, \alpha_1) .$$

Raising this to the Qth power we get

$$1 = M(\alpha_1, \alpha_2) = M(\alpha_2, \alpha_1) .$$

Adding these two and using the properties of the M function we get

$$\begin{aligned} 0 &= M(\alpha_2, \alpha_1) + M(\alpha_0, \alpha_1) \\ &= M(\alpha_2 + \alpha_0, \alpha_1) = M(\alpha_1) \prod_{\tau} (\alpha_2 + \alpha_0 + \tau\alpha_1) , \end{aligned}$$

where the product is over all τ in $GF(R)$. Since $M(\alpha_1) = \alpha_1 \neq 0$ we we have $\alpha_2 + \tau\alpha_1 + \alpha_0 = 0$ for some τ in $GF(R)$.

Following the notation of § 2, we let s denote the greatest common divisor (q, r) of q and r, $S = 2^s$, and $t = r/s$. We also set $w = qt$, the least common multiple of q and r.

We now use the results of § 2 with (1) specialized to

$$\alpha_2 = \tau\alpha_1 + \alpha_0 .$$

In particular we have $m = 2$, and

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

Then as in § 2 we set $P = W_{t-1} \cdots W_1 W_0$, and we let $H(x)$ be the characteristic polynomial of P. Since the determinant of W_j is 1, the constant term of $H(x)$ is also 1, so that $H(x)$ is of the form $H(x) = x^2 + \xi x + 1$, where $\xi \in GF(S)$.

We now distinguish three cases.

Case 1. $H(x)$ is irreducible over $GF(S)$. Here the roots of $H(x)$ are distinct and any root γ of $H(x)$ satisfies $\gamma^{S+1} = 1$. Therefore $H(x) | (x^{S+1} + 1)$. In this case $\alpha \in GF(Q^{(S+1)t})$, and the degree of the irreducible polynomial with α as a root divides $w(S + 1)$.

Case 2. The roots of $H(x)$ are distinct and lie in $GF(S)$. Here $H(x) | (x^{S-1} + 1)$, and we have $\alpha \in GF(Q^{(S-1)t})$. Therefore the degree of the irreducible polynomial with α as a root divides $w(S - 1)$.

Case 3. The roots of $H(x)$ are equal. Here we must have $H(x) = x^2 + 1$, and so $\alpha \in GF(Q^{2t})$. This implies that the degree of the irreducible polynomial with α as a root divides $2w$.

Thus we have the following result.

THEOREM 7. *Let* $F(x) = x^{QR+1} + x^{Q+R} + 1$, *where* $Q = 2^q$ *and* $R = 2^r$. *Let* s *be the greatest common divisor of* q *and* r, *and let* w *be the least common multiple of* q *and* r. *Let* $S = 2^s$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $w(S + 1)$, $w(S - 1)$, *or* $2w$. *The degree of* $f(x)$ *does not divide either* q *or* r.

The special case $r = 1$ of this theorem was a conjecture of Golomb, which was first proved by Mills and Zierler [5]. It has been generalized to arbitrary finite fields by Carlitz [2]. In these two papers additional information about the roots is obtained.

7. **The trinomial** $x^{QR-A+1} + x^{Q-A+R} + 1$. In this section we study the trinomial

$$F(x) = x^{QR-A+1} + x^{Q-A+R} + 1 ,$$

where $Q = 2^q$, $R = 2^r$, and $A^2 = QR$, so that A is as a power of 2, and q and r have the same parity. We found this class of polynomials by generalizing the interesting factorization of $x^{241} + x^{114} + 1$, which has 1 irreducible factor of degree 3, 6 irreducible factors of degree 21, and 4 irreducible factors of degree 28. Even more spectacular is the trinomial $x^{993} + x^{482} + 1$, which has 1 irreducible factor of degree 12, 19 irreducible factors of degree 27, and 13 irreducible factors of degree 36.

As usual let α be a root of $F(x)$. Then we have

$$\alpha^A = \alpha_0^R \alpha_1 + \alpha_0 \alpha_1^R = M(\alpha_0, \alpha_1) .$$

Raising this to the Qth power we get

$$\alpha_1^A = M(\alpha_1, \alpha_2) .$$

Therefore, using the properties of the M function, we obtain

$$\alpha_1^R = \alpha^{QR} = \alpha^{A^2} = M(\alpha_0^A, \alpha_1^A) = M(M(\alpha_0, \alpha_1), M(\alpha_1, \alpha_2))$$
$$= M(\alpha_1^R)M(\alpha_0, \alpha_1, \alpha_2) = \alpha_1^R M(\alpha_0, \alpha_1, \alpha_2) .$$

Since $\alpha \neq 0$, we have $\alpha_1 \neq 0$, and therefore

$$1 = M(\alpha_0, \alpha_1, \alpha_2) .$$

Raising this to the Qth power we get

$$1 = M(\alpha_1, \alpha_2, \alpha_3) = M(\alpha_3, \alpha_1, \alpha_2) .$$

Using Properties III and IV of the M function we obtain

$$0 = M(\alpha_0, \alpha_1, \alpha_2) + M(\alpha_3, \alpha_1, \alpha_2) = M(\alpha_0 + \alpha_3, \alpha_1, \alpha_2)$$
$$= M(\alpha_1, \alpha_2) \cdot \prod_{\tau, \lambda \in K} (\alpha_0 + \alpha_3 + \tau\alpha_1 + \lambda\alpha_2) ,$$

where K is the finite field $GF(R)$. Since

$$M(\alpha_1, \alpha_2) = \alpha_1^A \neq 0$$

we must have

$$\alpha_0 + \tau\alpha_1 + \lambda\alpha_2 + \alpha_3 = 0$$

for some τ, λ in K.

Following the notation of §2, we let $s = (q, r)$, $S = 2^s$, and $t = r/s$. We also set $w = qt$, the least common multiple of q and r.

We now use the results of §2 with (1) specialized to

$$\alpha_3 = \lambda\alpha_2 + \tau\alpha_1 + \alpha_0 .$$

In particular we have $m = 3$, and

$$W_j = \begin{bmatrix} \lambda_j & \tau_j & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} .$$

Then as in §2 we set $P = W_{t-1} \cdots W_1 W_0$, and we let $H(x)$ be the characteristic polynomial of P. Since the determinant of W_j is 1, the constant term of $H(x)$ is also 1, so that $H(x)$ is of the form $H(x) = x^3 + \xi x^2 + \phi x + 1$, where $\xi, \phi \in GF(S)$.

We now distinguish four cases.

Case 1. $H(x)$ is irreducible over $GF(S)$. Here the roots of $H(x)$ are distinct. Any root γ of $H(x)$ satisfies

$$\gamma^{S^2+S+1} = 1 .$$

Therefore

$$H(x) \mid (x^{S^2+S+1} + 1) .$$

In this case $\alpha \in GF(Q^{(S^2+S+1)t})$, and the degree of the irreducible polynomial with α as a root divides $w(S^2 + S + 1)$.

Case 2. $H(x)$ is reducible over $GF(S)$ and its three roots are distinct. Here these three roots must lie in $GF(S^2)$. This gives us

$$H(x) \mid (x^{S^2-1} + 1) ,$$
$$\alpha \in GF(Q^{(S^2-1)t}) ,$$

and the degree of the irreducible polynomial with α as a root divides $w(S^2 - 1)$.

Case 3. $H(x)$ has exactly two equal roots. Here the roots of $H(x)$ all lie in $GF(S)$, and therefore

$$H(x) \mid (x^{S-1} + 1)^2 = x^{2S-2} + 1 ,$$
$$\alpha \in GF(Q^{2(S-1)t}) ,$$

and the degree of the irreducible polynomial with α as a root divides $2w(S - 1)$.

Case 4. The three roots of $H(x)$ are equal. Since the product of these three roots is 1, we must have $H(x) = (x + \omega)^3$, where ω is a cube root of unity, $\omega \in GF(S)$.

If $\omega \neq 1$, then ω is a generator of $GF(4)$ so that $GF(4) \subseteq GF(S)$, which implies that s is even,

$$H(x) \mid (x^3 + 1)^4 = x^{12} + 1 ,$$

$\alpha \in GF(Q^{12t})$, and the degree of the irreducible polynomial with α as a root divides $12w$.

On the other hand if $\omega = 1$, then $H(x) \mid (x + 1)^4$, $\alpha \in GF(Q^{4t})$, and the degree of the irreducible polynomial with α as a root divides $4w$.

Finally we observe that $\alpha_2 + \alpha_0$ is one of the factors of $M(\alpha_0, \alpha_1, \alpha_2)$, which is not zero. Thus none of the roots of $F(x)$ lies in $GF(Q^2)$. By symmetry none of the roots of $F(x)$ lies in $GF(R^2)$.

Thus we have the following result.

THEOREM 8. *Let* $F(x) = x^{QR-A+1} + x^{Q-A+R} + 1$, *where* $Q = 2^q$, $R = 2^r$, *and* $A^2 = QR$. *Let* s *be the greatest common divisor of* q *and* r, *and let* w *be the least common multiple of* q *and* r. *Let* $S = 2^s$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $w(S^2 + S + 1)$, $w(S^2 - 1)$, $2w(S - 1)$, *or* $12w$. *If* s *is odd, then* $12w$ *can be replaced by* $4w$. *The degree of* $f(x)$ *does not divide either* $2q$ *or* $2r$.

The factorizations of the first 15 members of this family, i.e., those with $q + r \leqq 10$, suggest that Theorem 8 is too weak. In all these examples the degrees of the irreducible factors of $F(x)$ divide $w(S^2 - 1)$, $2w(S - 1)$, or $12w$. Perhaps this always holds.

8. **The trinomial $x^{QR-B+1} + x^{Q-B+R} + 1$.** In this section we study the trinomial

$$F(x) = x^{QR-B+1} + x^{Q-B+R} + 1 ,$$

where $Q = 2^q$, $R = 2^r$, and $B^2 = 2QR$, so that B is a power of 2 and q and r have the opposite parity. We let α be a root of $F(x)$.

We begin by noting that if α is an element of $GF(Q)$, then $F(\alpha) = 1$, a contradiction. Thus none of the roots of $F(x)$ lies in $GF(Q)$. By symmetry none of the roots of $F(x)$ lies in $GF(R)$.

Since α is a root of $F(x)$ we have

$$\alpha^B = \alpha_0^R \alpha_1 + \alpha_0 \alpha_1^R = M(\alpha_0, \alpha_1) .$$

Raising this to the Qth power we get

$$\alpha_1^B = M(\alpha_1, \alpha_2) .$$

Therefore, using the properties of the M function, we obtain

$$\begin{aligned} \alpha_1^{2R} = \alpha^{2QR} = \alpha^{B^2} = M(\alpha_0^B, \alpha_1^B) = M(M(\alpha_0, \alpha_1), M(\alpha_1, \alpha_2)) \\ = M(\alpha_1^R) M(\alpha_0, \alpha_1, \alpha_2) = \alpha_1^R M(\alpha_0, \alpha_1, \alpha_2) . \end{aligned}$$

Since $\alpha \neq 0$, we have $\alpha_1 \neq 0$, and therefore

$$\alpha_1^R = M(\alpha_0, \alpha_1, \alpha_2) .$$

Raising this to the Qth power we obtain

$$\alpha_2^R = M(\alpha_1, \alpha_2, \alpha_3) .$$

Iterating the M function again we get

$$\begin{aligned} (M(\alpha_1, \alpha_2))^R = M(\alpha_1^R, \alpha_2^R) = M(M(\alpha_0, \alpha_1, \alpha_2), M(\alpha_1, \alpha_2, \alpha_3)) \\ = (M(\alpha_1, \alpha_2))^R \cdot M(\alpha_0, \alpha_1, \alpha_2, \alpha_3) . \end{aligned}$$

Now $M(\alpha_1, \alpha_2) = \alpha_1^B \neq 0$ so that we have

$$1 = M(\alpha_0, \alpha_1, \alpha_2, \alpha_3) .$$

Raising this to the Qth power we get

$$1 = M(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = M(\alpha_4, \alpha_1, \alpha_2, \alpha_3) .$$

Using Properties III and IV of the M function we obtain

$$0 = M(\alpha_0, \alpha_1, \alpha_2, \alpha_3) + M(\alpha_4, \alpha_1, \alpha_2, \alpha_3) = M(\alpha_0 + \alpha_4, \alpha_1, \alpha_2, \alpha_3)$$
$$= M(\alpha_1, \alpha_2, \alpha_3) \cdot \prod (\alpha_0 + \alpha_4 + \tau\alpha_1 + \lambda\alpha_2 + \mu\alpha_3) ,$$

where the product is over all τ, λ, μ in $GF(R)$. Since

$$M(\alpha_1, \alpha_2, \alpha_3) = \alpha_2^R \neq 0 ,$$

we must have

$$\alpha_0 + \tau\alpha_1 + \lambda\alpha_2 + \mu\alpha_3 + \alpha_4 = 0$$

for some τ, λ, μ in $GF(R)$.

Following the notation of § 2, we let $s = (q, r)$, $S = 2^s$, and $t = r/s$. We also set $w = qt$, the least common multiple of q and r.

We now use the results of § 2 with (1) specialized to

$$\alpha_4 = \mu\alpha_3 + \lambda\alpha_2 + \tau\alpha_1 + \alpha_0 .$$

In particular we have $m = 4$, and

$$W_j = \begin{bmatrix} \mu_j & \lambda_j & \tau_j & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} .$$

Then as in § 2 we set $P = W_{t-1} \cdots W_1 W_0$, and we let $H(x)$ be the characteristic polynomial of P. Since the determinant of W_j is 1, the constant term of $H(x)$ is also 1, so that $H(x)$ is of the form $H(x) = x^4 + \zeta x^3 + \xi x^2 + \phi x + 1$, with $\zeta, \xi, \phi \in GF(S)$.

We now distinguish four cases.

Case 1. $H(x)$ is irreducible over $GF(S)$. Here the roots of $H(x)$ are distinct. Any root γ of $H(x)$ satisfies

$$\gamma^{S^3+S^2+S+1} = 1 .$$

Therefore

$$H(x) \mid (x^{S^3+S^2+S+1} + 1) .$$

In this case $\alpha \in GF(Q^{(S^3+S^2+S+1)t})$, and the degree of the irreducible polynomial with α as a root divides $w(S^3 + S^2 + S + 1)$.

Case 2. $H(x)$ has an irreducible factor of degree three over $GF(S)$. Here the roots of $H(x)$ are distinct and all four of them lie in $GF(S^3)$. This gives us

$$H(x) \mid (x^{S^3-1} \quad 1) ,$$
$$\alpha \in GF(Q^{(S^3-1)t}) ,$$

and the degree of the irreducible polynomial with α as a root divides $w(S^3 - 1)$.

Case 3. All the roots of $H(x)$ lie in $GF(S^2)$ and $H(x)$ has no roots of multiplicity three. Here we have

$$H(x) \mid (x^{S^2-1} + 1)^2 = x^{2S^2-2} + 1 ,$$
$$\alpha \in GF(Q^{2(S^2-1)t}) ,$$

and the degree of the irreducible polynomial with α as a root divides $2w(S^2 - 1)$.

Case 4. At least three of the roots of $H(x)$ are equal. Here the roots of $H(x)$ all lie in $GF(S)$ and

$$H(x) \mid (x^{S-1} + 1)^4 = (x^{4S-4} + 1) ,$$
$$\alpha \in GF(Q^{4(S-1)t}) ,$$

and the degree of the irreducible polynomial with α as a root divides $4w(S - 1)$.

Thus we have the following result.

THEOREM 9. *Let* $F(x) = x^{QR-B+1} + x^{Q-B+R} + 1$, *where* $Q = 2^q$, $R = 2^r$, *and* $B^2 = 2QR$. *Let* s *be the greatest common divisor of* q *and* r, *and let* w *be the least common muliple of* q *and* r. *Let* $S = 2^s$, *and let* $f(x)$ *be an irreducible factor of* $F(x)$ *over* $GF(2)$. *Then the degree of* $f(x)$ *divides* $w(S^3 + S^2 + S + 1)$, $w(S^3 - 1)$, $2w(S^2 - 1)$, *or* $4w(S - 1)$. *The degree of* $f(x)$ *does not divide either* q *or* r.

We suspect that Theorem 9 is too weak, and that it could be sharpened by the use of stronger techniques.

9. A final example. It can be shown that any root α of the trinomial

$$F(x) = x^{3Q+1} + x^{Q+3} + 1$$

satisfies

$$(\alpha_2 + \alpha_0)(\alpha_2^2 + \alpha_2\alpha_0 + \alpha_1^2 + \alpha_0^2) = 0 .$$

Here we have an example where the α_i satisfy a linear relation for some α and a quadratic relation for the remaining α. This polynomial is a kind of a cross between a round trinomial and a typical polynomial. It has an unusual number of factors whose degrees divide $2q$, but the remaining factors do not seem to fit a pattern. For example for $q = 9$, $F(x)$ has 28 irreducible factors of degree 18,

1 of degree 6, and 1 of degree 2, however the remaining factors have degrees 5, 34, 39, 41, 49, 61, 65, 68, 71, 78, 85, 88, 94, 118, and 129.

REFERENCES

1. A. C. Aitken, *Determinants and Matrices*, Oliver and Boyd, Edinburgh and London, 1958.
2. L. Carlitz, *Factorization of a special polynomial over a finite field*, Pacific J. Math., **32** (1970), 603-614.
3. Solomon W. Golomb, *Shift Register Sequences*, Holden-Day, Inc., San Francisco, Cambridge, London, Amsterdam, 1967.
4. W. H. Mills, *The degrees of the factors of certain polynomials over finite fields*, Proc. Amer. Math. Soc., **25** (1970), 860-863.
5. W. H. Mills and Neal Zierler, *On a conjecture of Golomb*, Pacific J. Math., **28** (1969), 635-640.

Received January 30, 1980.

RICHARD W. MARSH
DEPARTMENT OF DEFENSE,
FORT GEORGE G. MEADE, MARYLAND 20755

W. H. MILLS
INSTITUTE FOR DEFENSE ANALYSES,
PRINCETON, NEW JERSEY 08540

ROBERT L. WARD
DEPARTMENT OF DEFENSE,
FORT GEORGE G. MEADE, MARYLAND 20755

HOWARD RUMSEY, JR.
INSTITUTE FOR DEFENSE ANALYSES,
PRINCETON, NEW JERSEY 08540

LLOYD R. WELCH
UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CALIFORNIA 90007