PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 36, No. 2, December 1972

QUARTICS OVER GF(2^n)

PHILIP A. LEONARD AND KENNETH S. WILLIAMS[1]

ABSTRACT. A description of the factorization of a quartic polynomial over the field GF(2^n) is given in terms of the roots of a related cubic.

1. **Introduction.** A description of the factorization of a quartic polynomial over the field GF(p^n) in terms of the roots of a related cubic is known when the characteristic p of the field is odd. For $n=1$ the result is due to Skolem [**4**], and a more recent proof [**3**] of Skolem's result can be carried over to GF(p^n), p odd and n arbitrary ($n\geqq 1$). Our object in this paper is to obtain a precisely analogous result for quartics over GF(2^n). For results concerning quadratics and cubics over GF(2^n), we refer the reader to [**1**] and [**2**]. We mention only the well-known fact [**2**], which is useful below, that the polynomial x^2+bx+c, $b\neq 0$, is reducible over GF(2^n) if and only if $\mathrm{tr}(c/b^2)=0$, where for $\lambda \in \mathrm{GF}(2^n)$, $\mathrm{tr}(\lambda)=\lambda+\lambda^2+\lambda^{2^2}+\cdots+\lambda^{2^{n-1}}$ denotes the trace of λ over GF(2).

Given a quartic polynomial $f(x)=A_4x^4+A_3x^3+A_2x^2+A_1x+A_0$ with $A_i \in \mathrm{GF}(2^n)$, $0\leqq i\leqq 4$, and $A_4\neq 0$, we make a few simplifications. If $A_3=0$, we work with

$$\frac{1}{A_4}f(x) = x^4 + \frac{A_2}{A_4}x^2 + \frac{A_1}{A_4}x + \frac{A_0}{A_4}. \tag{1.1}$$

If $A_3\neq 0$, we let $\alpha \in \mathrm{GF}(2^n)$ be defined by $\alpha^2=A_1/A_3$, and consider

$$x^4 f\left(\frac{1}{x}+\alpha\right) = A_0'x^4 + A_2'x^2 + A_3x + A_4, \tag{1.2}$$

where

$$A_0' = A_4\alpha^4 + A_3\alpha^3 + A_2\alpha^2 + A_1\alpha + A_0, \quad A_2' = A_3\alpha + A_2.$$

If $A_0'=0$, then α is a root of $f(x)=0$ in GF(2^n), and $f(x)$ can be reduced

Received by the editors February 28, 1972.
AMS 1970 *subject classifications*. Primary 12C05.
Key words and phrases. Quartic polynomial, cubic polynomial, factorization, GF(2^n).
[1] The research of both authors was supported by the National Research Council of Canada under grant A-7233.

to a cubic. Otherwise, we work with

$$\frac{1}{A_0'}x^4 f\left(\frac{1}{x}+\alpha\right) = x^4 + \frac{A_2'}{A_0'}x^2 + \frac{A_3}{A_0'}x + \frac{A_4}{A_0'}. \tag{1.3}$$

In all cases we can retrieve the factorization of $f(x)$, and so it suffices to consider quartics of the form

$$f(x) = x^4 + a_2x^2 + a_1x + a_0. \tag{1.4}$$

Clearly we may assume $a_0 \neq 0$. Further we can assume $a_1 \neq 0$, for otherwise we have $f(x)=x^4+a_2x^2+a_0=(x^2+b_2x+b_0)^2$, where b_0, b_2 are defined by $b_0^2=a_0$, $b_2^2=a_2$.

2. **Preliminary remarks.** Beginning with $f(x)=x^4+a_2x^2+a_1x+a_0$, with $a_i \in \mathrm{GF}(2^n)$, $0 \leqq i \leqq 2$, and $a_0a_1 \neq 0$, we suppose that $f(x)$ has a factorization over $\mathrm{GF}(2^n)$ as the product of two quadratics, say

$$f(x) = (x^2 + rx + s)(x^2 + rx + t). \tag{2.1}$$

Equating coefficients in (2.1) we obtain

$$a_2 = r^2 + s + t, \qquad a_1 = r(s + t), \qquad a_0 = st. \tag{2.2}$$

As $a_1 \neq 0$, we have $r \neq 0$; eliminating $s+t$, we find that $y=r$ must be a root of the equation

$$g(y) = y^3 + a_2y + a_1 = 0. \tag{2.3}$$

On the other hand, if $y=r$ is a root of (2.3), then from $s+t=a_1/r$, $st=a_0$ in (2.2), we see that s and t can be found in $\mathrm{GF}(2^n)$ precisely when the quadratic $z^2+(a_1/r)z+a_0=0$ is reducible, i.e., precisely when

$$\mathrm{tr}\left(\frac{a_0r^2}{a_1^2}\right) = 0. \tag{2.4}$$

The following additional remarks about (2.3) will be useful:

(i) Since $a_1 \neq 0$, the equation (2.3) has no repeated roots.

(ii) If $y=r$ is a root of (2.3) then, eliminating the linear factor $y+r$, we see that $y=r$ is the only root of (2.3) in $\mathrm{GF}(2^n)$ if and only if $\mathrm{tr}(1+a_2/r^2)=1$. In this case

$$\mathrm{tr}\left(\frac{s+t}{r^2}\right) = \mathrm{tr}\left(\frac{a_2+r^2}{r^2}\right) = \mathrm{tr}\left(1+\frac{a_2}{r^2}\right) = 1, \quad \text{i.e.,} \quad \mathrm{tr}\left(\frac{s}{r^2}\right) \neq \mathrm{tr}\left(\frac{t}{r^2}\right).$$

Therefore, if $y=r$ is the unique root of (2.3), and if it gives rise to a factorization of the form (2.1), then one of the quadratic factors is reducible and the other is irreducible.

(iii) If $y=r_1, r_2, r_3$ are three roots of (2.3) in GF(2^n) then $r_1+r_2+r_3=0$, so that

$$\mathrm{tr}((a_0/a_1^2)(r_1^2 + r_2^2 + r_3^2)) = 0,$$

and thus exactly one or three of the r_i ($i=1, 2, 3$) will satisfy

$$\mathrm{tr}(a_0 r_i^2/a_1^2)=0.$$

3. **Proof of the Theorem.** A few examples will illustrate the shorthand used in the statement of the Theorem. If $h(x)$ is a quartic over GF(2^n) which factors as a product of two linear factors times an irreducible quadratic, we write $h=(1, 1, 2)$; if $h(x)$ is a cubic irreducible over GF(2^n), we write $h=(3)$. Also, we use r_1, r_2, r_3 below to indicate roots of (2.3) when they exist in GF(2^n), and set $w_i=a_0 r_i^2/a_1^2$ in this case.

THEOREM. *The factorizations of $f(x)$ over* GF(2^n) *are characterized as follows*:

(a) $f=(1, 1, 1, 1) \Leftrightarrow g=(1, 1, 1)$ *and* $\mathrm{tr}(w_1)=\mathrm{tr}(w_2)=\mathrm{tr}(w_3)=0$,
(b) $f=(2, 2) \Leftrightarrow g=(1, 1, 1)$ *and* $\mathrm{tr}(w_1)=0$, $\mathrm{tr}(w_2)=\mathrm{tr}(w_3)=1$,
(c) $f=(1, 3) \Leftrightarrow g=(3)$,
(d) $f=(1, 1, 2) \Leftrightarrow g=(1, 2)$ *and* $\mathrm{tr}(w_1)=0$,
(e) $f=(4) \Leftrightarrow g=(1, 2)$ *and* $\mathrm{tr}(w_1)=1$.

PROOF. (a) If $f=(1, 1, 1, 1)$ there are 6 factorizations (2.1), giving rise to 3 distinct values of r. As each r_i does come from a factorization, $\mathrm{tr}(w_i)=0$ for $i=1, 2, 3$. The converse is clear.

(b) If $f=(2, 2)$ then there is precisely one r_1 with $\mathrm{tr}(w_1)=0$, because there are precisely two factorizations (2.1). On the other hand, $y=r_1$ cannot be the unique root of (2.3) by remark (ii) of §2. Thus the conclusion follows, and again the converse is clear.

(c) If $f=(1, 3)$, then no factorization of the form (2.1) can exist, even in the field GF(2^{2n}), a quadratic extension of GF(2^n). If (2.3) has any roots $y=r$ in GF(2^n), then corresponding values s, t may be found, at least in GF(2^{2n}). Therefore there can be no roots, that is $g=(3)$. Conversely, if $g=(3)$ then (2.3) has no roots even in GF(2^{2n}), and we must have $f=(1, 3)$.

(d) If $f=(1, 1, 2)$ then there are exactly 2 factorizations (2.1), corresponding to r_1 with $\mathrm{tr}(w_1)=0$. By (a) and (b), and remark (iii) of §2, $y=r_1$ is the only root of (2.3) and the conclusion follows. The converse comes easily from (ii) of §2.

(e) As all other possibilities have been exhausted, no proof is necessary.

REFERENCES

1. E. R. Berlekamp, H. Rumsey and G. Solomon, *Solutions of algebraic equations in fields of characteristic* 2, Jet Propulsion Lab. Space Programs Summary **4** (1966), 37–39.

2. ———, *On the solution of algebraic equations over finite fields*, Information and Control **10** (1967), 553–564. MR **37** #6266.

3. P. A. Leonard, *On factoring quartics* (mod *p*), J. Number Theory **1** (1969), 113–115. MR **38** #5751.

4. Th. Skolem, *The general congruence of 4th degree modulo p, p prime*, Nordisk Mat. Tidskr. **34** (1952), 73–80. MR 14, 353.

DEPARTMENT OF MATHEMATICS, ARIZONA STATE UNIVERSITY, TEMPE, ARIZONA 85281

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA*

* Current address of both authors.