ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 1, Spring 1999

THE SECOND-ORDER FACTORABLE CORE OF POLYNOMIALS OVER FINITE FIELDS

MARIA T. ACOSTA AND JAVIER GOMEZ-CALDERON

ABSTRACT. Let F_q denote the finite field of order q and odd characteristic p. For $f(x)$ in $F_q[x]$, let $f^*(x,y)$ denote the polynomial $f(x)-f(y)$. Assume that the degree of $f(x)$ is relatively prime to q. Let $r+s$ denote the total number of quadratic irreducible factors of $f^*(x,y)$ over the algebraic closure of F_q, r with nonzero xy-term and $s(\geq 1)$ with no xy-term. We show that $f(x-c)=h((x^2+b)^{s+1})$ for some $h(x)$ in $F_q[x]$ and that either $f(x-c)=g(D_{2r+1,a}(x))$ or $f(x-c)=g(D_{2r+2,a}(x))$ for some $g(x)$ in $F_q[x]$ where $D_{m,a}(x)\in F_q[x]$ denotes a Dickson polynomial of degree m and parameter a.

1. Introduction. Let F_q denote the finite field of order q and characteristic p. For $f(x)$ in $F_q[x]$, let $f^*(x,y)$ denote the substitution polynomial $f(x)-f(y)$. The polynomial $f^*(x,y)$ has frequently been used in questions on the value set of $f(x)$, see, for example, Wan [**7**], Dickson [**3**], Hayes [**5**] and Gomez-Calderon and Madden [**4**]. Recently in [**1**], Cohen showed that if $f(x)$ is separable (not in $F_q[x^p]$) then $f^*(x,y)$ is factorable, a product of linear factors in $F_q[x,y]$, if and only if $f(x)=L^r(x)+b$ where $b\in F_q$ and L is an affine p^s-polynomial over F_q, with $r|(p^s-1)$ if L is actually an affine p-polynomial of degree exceeding 1. Also in [**1**], Cohen proved that if $f(x)$ is separable and monic, then $f(x)=g(h(x))$ for some factorable polynomial $h(x)$, in $F_q[x]$, of degree L, where L denotes the total number of linear factors of $f^*(x,y)$. Now in [**2**], Cohen showed that if $f(x)$ is indecomposable in $F_q[x]$ and $f^*(x,y)$ has an irreducible quadratic, then $f(x)=aD(x+b)+c$, where $a(\neq 0), b, c$ belong to F_q and either $D(x)$ is a Dickson polynomial of odd prime degree $(\neq 0)$ or p is odd and $D(x)$ is a $(p,2)$-polynomial in C_4, a special class of polynomials introduced in [**1**].

In this paper we will use an elementary approach to show that if $f(x)$ has degree d relatively prime to q (odd) and $f^*(x,y)$ has a total of $r+s$ quadratic irreducible factors over $\overline{F}_q$, the algebraic closure of F_q, r with nonzero xy-terms and $s(\geq 1)$ with no xy-terms, then

Received by the editors on March 30, 1995, and in revised form on May 5, 1997.

(i) $f(x-c) = h((x^2+b)^{s+1})$ for some $h(x) \in F_q[x]$.

(ii) The product of all the quadratic irreducible factors with nonzero xy-term of $f^*(x,y)$ can be written as

$$\prod_{i=1}^{r}(x^2 - (\mu_i + \mu_i^{-1})xy + y^2 + e(\mu_i - \mu_i^{-1})^2)$$

for some dth roots of unity $\mu_1, \mu_2, \ldots, \mu_r$.

(iii)

$$f(x-b) = \begin{cases} g(D_{2r+1,a}(x)) & \text{for some } g(x) \text{ in } F_q[x] \\ & \text{if } \mu_i\mu_k^{-1} \neq -1 \text{ for all } 1 \leq i,\, k \leq r \\ g(D_{2r+2,a}(x)) & \text{for some } g(x) \text{ in } F_q[x], \text{ otherwise} \end{cases}$$

where $D_{t,a}(x)$ denotes a Dickson polynomial of degree t defined by

$$D_{t,a}(x) = \sum_{i=0}^{[t/2]} \frac{t}{t-i}\binom{t-i}{i}(-a)^i x^{t-2i}, \quad a \in F_q.$$

Hence, $D_{t,a}(x)$ and $Q_{s,b}(x) = (x^2+b)^{s+1}$ can be seen as the second-order factorable part of $f(x)$ in $F_q[x]$.

2. Theorem and proof. The following lemmas will be needed to prove our main result.

Lemma 1. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q. Assume $a_{d-1} = 0$. Let the prime factorization of $f^*(x,y) = f(x) - f(y)$ be given by*

$$f^*(x,y) = (x-y)\prod_{i=1}^{r} f_i(x,y).$$

Let

$$f_i(x,y) = \sum_{j=1}^{n_i} h_{ij}(x,y)$$

be the homogeneous decomposition of $f_i(x,y)$ so that $h_{ij}(x,y)$ is homogeneous of degree j and $\deg(h_{in_i}(x,y)) = n_i = \deg(f_i)$. Then $h_{in_i-1}(x,y) = 0$ for $i = 1, 2, \ldots, r$.

Proof. First we consider the homogeneous decomposition

$$(x-y)\prod_{i=1}^{r} f_i(x,y) = f^*(x,y) = x^d - y^d + a_{d-1}(x^{d-1} - y^{d-1}) + \cdots + a_1(x-y).$$

Simply by multiplying, we can interpret the first two terms as

$$x^d - y^d = (x-y)\prod_{i=1}^{r} h_{in_i}(x,y) \tag{1}$$

$$a_{d-1}(x^{d-1} - y^{d-1}) = (x-y)\sum_{i=1}^{r}\left(\prod_{j\neq i} h_{jn_j}(x,y)\right) h_{in_i-1}(x,y). \tag{2}$$

Dividing (2) by (1), we find

$$\frac{a_{d-1}(x^{d-1} - y^{d-1})}{x^d - y^d} = \sum_{i=1}^{r} \frac{h_{in_i-1}(x,y)}{h_{in_i}(x,y)}$$

which is a partial decomposition, since $(d,q) = 1$, and therefore unique. Thus $a_{d-1} = 0$ implies $h_{in_i-1}(x,y) = 0$ for all i. □

Lemma 2. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q. Assume $a_{d-1} = 0$. Let $L(x,y)$ denote the product of all the linear factors of $f^*(x,y)$ in $\overline{F}_q[x,y]$ where $\overline{F}_q$ denotes the algebraic closure of F_q. Then*

i) *$L(x,y) = \prod_{i=1}^{r}(x - \mu^i y) = x^r - y^r$ for some rth primitive root of unity μ,*

ii) *$f(x) = h(x^r)$ for some $h(x)$ in $F_q[x]$.*

Proof. By Lemma 1 every linear factor of $f^*(x,y)$ is homogeneous. Thus,

$$L(x,y) = \prod_{i=1}^{r}(x - b_i y)$$

for some $b_1, b_2, \ldots, b_r$ in F_q. Hence, $f(b_i x) = f(x)$ for $1 \leq i \leq r$ and so $f(b_i b_k x) = f(b_k x) = f(x)$ for all i and k. Therefore, $b_1, b_2, \ldots, b_r$ form a multiplicative cyclic group of order r, $r|d$ and

$$f^*(x,y) = (x^r - y^r) \prod_{i=1}^{s} f_i(x,y) \tag{3}$$

where $f_1(x,y), f_2(x,y), \ldots, f_s(x,y)$ are irreducible polynomials. Now write

$$f(x) = f_0(x) + f_1(x)x^r + f_2(x)x^{2r} + \cdots + f_m(x)x^{rm}$$

with $\deg(f_i(x)) < r$. This decomposition is clearly unique. So, $f(x) = f(b_i x)$ for $1 \leq i \leq r$ implies

$$\begin{aligned} f(x) &= f_0(x) + f_1(x)x^r + \cdots + f_m(x)x^{mr} \\ &= f_0(b_i x) + f_1(b_i x)x^r + \cdots + f_m(b_i x)x^{mr} \end{aligned}$$

for $i = 1, 2, \ldots, r$. Therefore, $f_i(x) = c_i \in F_q$ and $f(x) = c_0 + c_1 x^r + \cdots + c_m x^{mr} = h(x^r)$ where $h(x) = c_0 + c_1 x + \cdots + c_m x^m \in F_q[x]$. □

Lemma 3. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q. Assume $a_{d-1} = 0$. Assume $x^2 + bxy + cy^2 + e$ is an irreducible factor of $f^*(x,y)$ over $\overline{F}_q$. Then*

(i) $a_{d-2} \neq 0$

(ii) $b(c-1) = 0$

(iii) *If $c = 1$, then $ed = -a_{d-2}(\mu_1 - \mu_1^{-1})^2$.*

(iv) *If $b = 0$, then $ed = 2a_{d-2}(1 - \mu_1^2)$ where $(x - \mu_1 y)(x - \mu_2 y) = x^2 + bxy + cy^2$ and $\mu_1^d = \mu_2^d = 1$.*

Proof. Let the prime factorization of $f^*(x,y)$ be given by

$$f^*(x,y) = \prod_{i=1}^{s} f_i(x,y),$$

where $f_1(x,y) = x^2 + bxy + cy^2 + e$. Then, comparing the highest degree terms $x^2 + bxy + cy^2 = (x - \mu_1 y)(x - \mu_2 y)$ for two distinct dth roots of

unity μ_1 and μ_2. Now, with notation as in Lemma 1, we consider the ratio of the highest two homogeneous components to find

$$\begin{aligned}\frac{(x^{d-2}-y^{d-2})a_{d-2}}{x^d-y^d} &= \sum_{i=1}^{s}\frac{h_{in_i-2}(x,y)}{h_{in_i}(x,y)}\\ &= \frac{e}{(x-\mu_1 y)(x-\mu_2 y)}+\sum_{i=2}^{s}\frac{h_{in_i-2}(x,y)}{h_{in_i}(x,y)}\\ &= \frac{e}{y(\mu_1-\mu_2)}\left(\frac{1}{(x-\mu_1 y)}+\frac{-1}{(x-\mu_2 y)}\right)\\ &\quad+\sum_{i=2}^{s}\frac{h_{in_i-2}(x,y)}{h_{in_i}(x,y)}.\end{aligned} \tag{4}$$

On the other hand,

$$\frac{x^{d-2}-y^{d-2}}{x^d-y^d}=\sum_{i=0}^{d-1}\frac{A_i}{x-\mu^i y}$$

for a dth primitive root of unity μ and some constants $A_0, A_1, \ldots, A_{d-1}$ in the algebraic closure of the rational function field $F_q(y)$. So, solving for the A_i in the usual way,

$$\frac{x^{d-2}-y^{d-2}}{x^d-y^d}=\sum_{i=0}^{d-1}\frac{\mu^{-i}-\mu^i}{dy(x-\mu^i y)}. \tag{5}$$

Hence, combining (4) and (5),

$$\begin{aligned}\frac{e}{y(\mu_1-\mu_2)} &= \frac{(\mu_1^{-1}-\mu_1)a_{d-2}}{dy}\\ \frac{e}{y(\mu_2-\mu_1)} &= \frac{(\mu_2^{-1}-\mu_2)a_{d-2}}{dy}.\end{aligned}$$

Therefore,

$$a_{d-2}(\mu_1^{-1}-\mu_1)=-(\mu_2^{-1}-\mu_2)a_{d-2}$$

and

$$a_{d-2}(\mu_1+\mu_2)(1-\mu_1\mu_2)=-a_{d-2}b(1-c)=0.$$

Thus, if $c = \mu_1\mu_2 = 1$, then

$$de = a_{d-2}(\mu_1 - \mu_2)(\mu_1^{-1} - \mu_1) = -a_{d-2}(\mu_1 - \mu_1^{-1})^2$$

while if $b = \mu_1 + \mu_2 = 0$, we have

$$de = a_{d-2}(\mu_1 - \mu_2)(\mu_1^{-1} - \mu_1) = 2a_{d-2}(1 - \mu_1^2). \qquad \square$$

Lemma 4. *Let d be a positive integer and assume that F_q contains a primitive dth root of unity μ. Put*

$$A_i = \mu^i + \mu^{-i} \quad \textit{and} \quad B_i = \mu^i - \mu^{-i}.$$

Then, for each a in F_q, we have

(i) *If d is odd,*

$$D_{d,a}(x) - D_{d,a}(y) = (x - y) \prod_{i=1}^{(d-1)/2} (x^2 - A_i xy + y^2 + B_i^2 a).$$

(ii) *If d is even,*

$$D_{d,a}(x) - D_{d,a}(y) = (x^2 - y^2) \prod_{i=1}^{(d-2)/2} (x^2 - A_i xy + y^2 + B_i^2 a).$$

Moreover, for $a \neq 0$, the quadratic factors are different from each other and are irreducible in $F_q[x, y]$.

Proof. See [**6**, Theorem 3.12]. $\square$

Lemma 5. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q (odd). Assume $a_{d-1} = 0$. Let*

$$Q_{xy}(x, y) = \prod_{i=1}^{r} (x^2 - (\mu_i + \mu_i^{-1})xy + y^2 + e(\mu_i - \mu_i^{-1})^2)$$

denote the product of all quadratic irreducible factors with nonzero xy-term of $f^*(x,y)$ *over* $\overline{F}_q$*, the algebraic closure of* F_q*. Assume* $\deg_x(Q_{xy}) = 2r > 1$*. Then*

(i) *If* $\mu_i\mu_k \neq -1$ *for all* $1 \leq i,k \leq r$*, then* $(2r+1)|d$*,* $(x-y)Q_{xy}(x,y) = D_{2r+1,a}(x) - D_{2r+1,a}(y)$*, and* $f(x) = g(D_{2r+1,a}(x))$ *for some* $a \in F_q$ *and* $g(x) \in F_q[x]$*.*

(ii) *If* $\mu_i\mu_k = -1$ *for some* $1 \leq i,k \leq r$*, then* $(2r+2)|d$*,* $f(x)$ *is an even function,* $(x^2-y^2)Q_{xy}(x,y) = D_{2r+2,a}(x) - D_{2r+2,a}(y)$ *and* $f(x) = g(D_{2r+2,a}(x))$ *for some* $a \in F_q$ *and* $g(x) \in F_q[x]$*.*

Proof. Working formally, i.e., working in the algebraic closure of the rational function field $F_q(y)$, we obtain

$$f(y) = f\left(\frac{A_i y \pm B_i\sqrt{y^2-4e}}{2}\right)$$

where $A_i = \mu_i + \mu_i^{-1}$ and $B_i = \mu_i - \mu_i^{-1}$ for $1 \leq i \leq r$. Thus,

$$f(y) = f\left(\frac{A_iA_ky \pm A_iB_k\sqrt{y^2-4e} \pm B_i\sqrt{(A_ky \pm B_k\sqrt{y^2-4e})^2-16e}}{4}\right)$$

for $i = 1,2,\ldots,r$. Therefore,

$$\begin{aligned}
\phi_{ik}^{(1)} &= \Big(A_iA_ky + A_iB_k\sqrt{y^2-4e} \\
&\qquad + B_i\sqrt{(A_ky + B_k\sqrt{y^2-4e})^2-16e}\Big)\Big/4, \\
\phi_{ik}^{(2)} &= \Big(A_iA_ky + A_iB_k\sqrt{y^2-4e} \\
&\qquad - B_i\sqrt{(A_ky + B_k\sqrt{y^2-4e})^2-16e}\Big)\Big/4, \\
\phi^{(3)} &= \Big(A_iA_ky - A_iB_k\sqrt{y^2-4e} \\
&\qquad + B_i\sqrt{(A_ky - B_k\sqrt{y^2-4e})^2-16e}\Big)\Big/4,
\end{aligned}$$

and

$$\begin{aligned}
\phi_{ik}^{(4)} &= \Big(A_iA_ky - A_iB_k\sqrt{y^2-4e} \\
&\qquad - B_i\sqrt{(A_ky - B_k\sqrt{y^2-4e})^2-16e}\Big)\Big/4
\end{aligned}$$

are roots of $f^*(x,y)$. It is clear that $\phi_{ik}^{(1)} \neq \phi_{ik}^{(2)}$ and $\phi_{ik}^{(3)} \neq \phi_{ik}^{(4)}$. One also sees, by straightforward simplification, that the four roots are distinct if $B_i^2 \neq B_k^2$.

Now we set

$$4x = A_iA_ky \pm A_iB_k\sqrt{y^2-4e} \pm B_i\sqrt{(A_ky \pm B_k\sqrt{y^2-4e})^2 - 16e}$$

and then remove radicals to obtain

$$\begin{aligned} F_{ik}(x,y) = {} & x^4 - A_iA_kx^3y + (A_i^2 - 2 + A_k^2)x^2y^2 - A_iA_kxy^3 \\ & + y^4 + (A_i^2A_k^2 - 2A_i^2 - 2A_k^2)ex^2 \\ & - A_iA_ke(A_i^2 - 8 + A_k^2)xy - (2A_i^2 - A_i^2A_k^2 + 2A_k^2)ey^2 \\ & + (A_i^2 - A_k^2)^2e^2. \end{aligned}$$

Factoring $F_{ik}(x,y)$, we get

$$\begin{aligned} F_{ik}(x,y) = {} & (x^2 - (\mu_i\mu_k + \mu_i^{-1}\mu_k^{-1})xy + y^2 + (\mu_i\mu_k - \mu_i^{-1}\mu_k^{-1})^2e) \\ & (x^2 - (\mu_i\mu_k^{-1} + \mu_i^{-1}\mu_k)xy + y^2 + (\mu_i\mu_k^{-1} - \mu_i^{-1}\mu_k)^2e) \end{aligned}$$

where the quadratic factors are reducible and perfect squares if and only if $(\mu_i\mu_k)^2 = 1$ and $(\mu_i\mu_k^{-1})^2 = 1$, respectively. Therefore, $f^*(x,y)$ is divisible by

$$\begin{cases} F_{ik}(x,y) & \text{if } B_i^2 \neq B_k^2, \\ x^2 - (\mu_i\mu_k^{-1} + \mu_i^{-1}\mu_k)xy + y^2 + (\mu_i\mu_k^{-1} - \mu_i^{-1}\mu_k)^2e & \text{if } (\mu_i\mu_k)^2 = 1, \\ x^2 - (\mu_i\mu_k + \mu_i^{-1}\mu_k^{-1})xy + y^2 + (\mu_i\mu_k - \mu_i^{-1}\mu_k^{-1})^2e & \text{if } (\mu_i\mu_k^{-1})^2 = 1. \end{cases}$$

Hence, the set $\{1, \mu_1, \mu_1^{-1}, \mu_2, \mu_2^{-1}, \ldots, \mu_r, \mu_r^{-1}\}$ is a cyclic multiplicative group if $\mu_i\mu_k \neq -1$ for all $1 \leq i,k \leq r$.

Now we set $R_0(y) = y$ and write

$$\overline{Q}_{xy}(x,y) = (x-y)Q_{xy}(x,y) = \prod_{i=0}^{2r}(x - R_i(y))$$

where $R_1(y), R_2(y), \ldots, R_{2r}(y)$ denote radical expressions in y over $\overline{F}_q$. Thus, $R_i(R_k(y)) \in \{-R(y_0), R(y_0), R_1(y), \ldots, R_{2r}(y)\}$ for all

$0 \le i,k \le 2r$. Assume that $R_i(R_k(y) \ne -R_0(y)$ for all $0 \le i,k \le 2r$ and then write

$$\overline{Q}_{xy}(x,y) = \sum_{i=0}^{2r+1} a_i(y)x^i$$

where $a_i(y) \in F_q[y]$ for $0 \le i \le 2r+1$ and $\deg(a_i(y)) \le 2r$ for $1 \le i \le 2r+1$. So,

$$\sum_{i=0}^{2r+1} a_i(R_j(y))x^i = \overline{Q}_{xy}(x,R_j(y)) = \overline{Q}_{xy}(x,y) = \sum_{i=0}^{2r+1} a_i(y)x^i$$

for all $0 \le j \le 2r$. Thus, $a_i(y) = c_i \in F_q$ for $i = 1,2,\dots,2r+1$ and $Q_{xy}(x,y) = H_1(y) + H_2(x)$ for some polynomials $H_1(x)$ and $H_2(y)$ with coefficients in F_q. Further, since $Q_{xy}(x,x) = 0$, $H_1(x)+H_2(x) = 0$ and so $Q_{xy}(x,y) = H_1(x) - H_1(y)$. Hence, comparing only the highest degree terms, $\mu_i^{2r+1} = 1$ for all i. Therefore, if $\mu_i\mu_k = -1$ for some i and k, then $x + R_0(y) = x + y$ is a factor of $f^*(x,y)$. Thus, $f(x)$ is an even function and the set $\{1,-1,\mu_1,\mu_1^{-1},\mu_2,\mu_2^{-1},\dots,\mu_r,\mu_r^{-1}\}$ is a cyclic multiplicative group.

Therefore, combining with Lemma 4,

(6) $(x-y)Q_{xy}(x,y) =$

$$\begin{cases} D_{2r+1,a}(x) - D_{2r+1,a}(y) & \text{if } \mu_i\mu_k \ne -1 \text{ for all } 1 \le i,k \le r, \\ (D_{2r+2,a}(x) - D_{2r+2,a}(y))/(x+y) & \text{if } \mu_i\mu_k = -1 \text{ for some } 1 \le i,k \le r. \end{cases}$$

Now write

$$f(x) = f_0(x) + f_1(x)D_{t,a}(x) + f_2(x)D_{t,a}^2(x) + \cdots + f_m(x)D_{t,a}^m(x),$$

where $D_{t,a}(x)$ denotes the Dickson polynomial in (6) and $\deg(f_i(x)) = t_i < t$ for $0 \le i \le m$.

This decomposition is clearly unique. One also sees that

$$f(x) = \sum_{i=0}^{m} f_i(x)D_{t,a}^i(x) = \sum_{i=0}^{m} f_i(h(x))D_{t,a}^i(x)$$

for all $h(x) \in \{R_0(x), R_1(x), \dots, R_{2r}(x)\} = W$ if $t = 2r+1$ and, for all $h(x) \in W \cup \{-R_0(x)\}$ if $t = 2r+2$. Therefore, $f_i(x) = c_i \in F_q$ and

$$f(x) = \sum_{i=0}^{m} c_i D_{t,a}^i(x) = g(D_{t,a}(x))$$

where $g(x) = c_0 + c_1 x + \cdots + c_m x^m \in F_q[x]$. □

Corollary 6. *With assumptions and notation as in Lemma 5, if d is odd, then*

$$f(x) = g(D_{2r+1,a}(x))$$

for some $g(x)$ in $F_q[x]$.

Lemma 7. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q (odd). Assume $a_{d-1} = 0$. Let $Q(x,y)$ denote the product of all quadratic irreducible factors with no xy-term of $f^*(x,y)$ over $\overline{F}_q$, the algebraic closure of F_q. Assume $\deg_x(Q(x,y)) = 2s > 1$. Then,*

(i) *$Q(x,y) = (x^2+b)^{s+1} - (y^2+b)^{s+1}$ for some b in F_q.*

(ii) *$(s+1)|d$ and $f(x) = g((x^2+b)^{s+1})$ for some $b \in F_q$ and $g(x)$ in $F_q[x]$.*

Proof. By Lemma 3, $Q(x,y) = \prod_{i=1}^{s}(x^2 - \mu_i^2 y^2 + \partial(\mu_i^2 - 1))$ where $\mu_1, \mu_2, \ldots, \mu_s$ denote s distinct dth roots of unity and $\partial = -2a_{d-2}/d \neq 0$. Hence, working formally, we obtain

$$f(y) = f(\pm\sqrt{\mu_i^2 y^2 - \partial(\mu_i^2 - 1)})$$

for all $1 \leq i \leq s$. Therefore,

$$f(y) = f(\pm\sqrt{\mu_i^2(\mu_k^2 y^2 - \partial(\mu_k^2 - 1)) - \partial(\mu_i^2 - 1)})$$

for $1 \leq i, k \leq s$ and consequently $x^2 - \mu_i^2\mu_k^2 y^2 + \partial(\mu_i^2\mu_k^2 - 1)$ is also a factor of $f^*(x,y)$. Thus, the set $\{1, \mu_1^2, \mu_2^2, \ldots, \mu_s^2\}$ is a multiplicative cyclic group and

$$\begin{aligned}(x^2 - y^2)Q(x,y) &= \prod_{i=0}^{s}(x^2 - \mu^i y^2 + (\mu^i - 1)\partial) \\ &= (x^2 - \partial)^{s+1} - (y^2 - \partial)^{s+1}\end{aligned}$$

for some $(s+1)$th primitive root of unity μ. Therefore,

$$f^*(x,y) = (H(x) - H(y))\prod_{i=1}^{t} f_i(x,y)$$

where $H(x) = (x^2 - \partial)^{s+1}$ and $f_1(x,y), f_2(x,y), \ldots, f_t(x,y)$ are irreducible over F_q.

Now we write the unique representation

$$f(x) = f_0(x) + f_1(x)H(x) + \cdots + f_m(x)H^m(x)$$

where $\deg(f_i) - t_i < 2s+2$. We also write

$$H(x) - H(y) = \prod_{i=1}^{2s+2} (x - R_i(y))$$

where $R_1(y), R_2(y), \ldots, R_{2s+2}(y)$ denotes radical expressions on y over F_q. Hence,

$$f(x) = \sum_{i=0}^{m} f_i(R_j(x))H^i(x)$$

for all $1 \le j \le 2s+2$. Therefore, $f_i(x) = c_i \in F_q$ and $f(x) = g(H(x))$ where $g(x) = \sum_{i=0}^{m} c_i x^i \in F_q[x]$. □

We are ready for our main result.

Theorem 8. *Let $f(x)$ denote a monic polynomial with coefficients in F_q and degree d relatively prime to q* (odd). *Assume $f^*(x,y) = f(x) - f(y)$ has a total of $r+s$ quadratic irreducible factors over $\overline{F}_q$, the algebraic closure of F_q, r with nonzero xy-term and s with no xy-term. Then*

(i) *If $s \ge 1$, then $(s+1)|d$ and $f(x - a_{d-1}/d) = h((x^2+b)^{s+1})$ for some $b \in F_q$ and $h(x) \in F_q[x]$.*

(ii) *If $r \ge 1$, then the product of all quadratic irreducible factors with nonzero xy-term of $f^*(x - a_{d-1}/d, y - a_{d-1}/d)$ can be written as*

$$Q_{xy}(x,y) = \prod_{i=1}^{r} (x^2 - (\mu_i + \mu_i^{-1})xy + y^2 - a_{d-2}(\mu_i - \mu_i^{-1})^2/d)$$

where μ_i denotes a dth root of unity.

(iii) *If $\mu_i \mu_k \ne -1$ for all $1 \le i,k \le r$, then $(2r+1)|d$, $(x-y)Q_{xy}(x,y) = D_{2r+1,a}(x) - D_{2r+1,a}(y)$, and $f(x) = g(D_{2r+1,a}(x))$ for some $a \in F_q$ and $g(x) \in F_q[x]$.*

(iv) *If* $\mu_i\mu_k = -1$ *for some* $1 \leq i,k \leq r$, *then* $(2r+2)|d$, $f(x)$ *is an even function,* $(x^2-y^2)Q_{xy}(x,y) = D_{2r+2,a}(x) - D_{2r+2,a}(y)$, *and* $f(x) = g(D_{2r+2,a}(x))$ *for some* $a \in F_q$ *and* $g(x) \in F_q[x]$.

Proof. Since $(d,q)=1$, $f(x-a_{d-1}/d)) = x^d + a_{d-2}x^{d-2} + \cdots + a_1x + a_0$. Therefore, the theorem follows from Lemmas 5 and 7. □

Acknowledgment. The authors thank the referee for his suggestions which improved the final version of the paper.

REFERENCES

1. S.D. Cohen, *The factorable core of polynomials over finite fields*, J. Austral. Math. Soc. **49** (1990), 309–318.

2. ———, *Exceptional polynomials and the reducibility of substitution polynomials*, Enseign. Math. (2) **36** (1990), 53–65.

3. L.E. Dickson, *The analytic representation of substitutions on a power prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.

4. J. Gomez-Calderon and D.J. Madden, *Polynomials with small value set over finite fields*, J. Number Theory **28** (1988), 167–188.

5. D.R. Hayes, *A geometric approach to permutations polynomials over a finite field*, Duke Math. J. **34** (1967), 293–305.

6. R. Lidl, G.L. Mullen and G. Turnwald, *Dickson polynomials*, Longman Scientific and Technical, Essex, England, 1993.

7. D. Wan, *On a conjecture of Carlitz*, J. Austral. Math. Soc. **43** (1987), 375–384.

Department of Mathematics, Southwest Texas State University, San Marcos, Texas 78666-4603

Department of Mathematics, The Pennsylvania State University, New Kensington Campus, New Kensington, Pennsylvania 15068
E-mail address: JxG11@psuvm.psu.edu