The third-order factorable core of polynomials over finite fields

By Javier GOMEZ-CALDERON

Department of Mathematics, The Pennsylvania State University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1998)

Abstract: Let $\boldsymbol{F}_q$ denote the finite field of order q and characteristic p. For $f(x)$ in $\boldsymbol{F}_q[x]$, let $f^*(x, y)$ denote the substitution polynomial $f(x)$-$f(y)$. In this paper we show that if $f(x) = x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \in F_q[x]$ $(a_{d-2}a_{d-3} \neq 0)$ has degree d prime to q and $f^*(x, y)$ has at least one cubic irreducible factor, then

$f(x) = G(x^4 + (4a_{d-2}/d)x^2 + (4a_{d-3}/d)x)$ for some $G(x) \in \boldsymbol{F}_q[x]$

or

$f(x) = H((x^3 + (3a_{d-2}/d)x + 3a_{d-3}/d)^{r+1})$ for some $H(x) \in \boldsymbol{F}_q[x]$

where r denotes the number of irreducible cubic factors of $f^*(x, y)$ of the form $x^3 - Ty^3 + Ax + By + C$.

Let $\boldsymbol{F}_q$ denote the finite field of order q and characteristic p. For $f(x)$ in $\boldsymbol{F}_q[x]$, 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 values set of $f(x)$, see for example Wan [8], Dickson [4], Hayes [7], and Gomez-Calderon and Madden [6]. Recently in [2] and [3], Cohen and in [1], Acosta and Gomez-Calderon studied the linear and quadratic factors of $f^*(x, y)$. In this paper we consider the irreducible cubic factors of $f^*(x, y)$. We show that if $f(x) = x^d + a_{d-2}x^{d-2} + a_{d-3}x^{d-3} + \cdots + a_1x + a_0 \in \boldsymbol{F}_q[x]$ $(a_{d-2}a_{d-3} \neq 0)$ has degree d prime to q and $f^*(x, y)$ has at least one cubic irreducible factor, then

$$f(x) = G(x^4 + (4a_{d-2}/d)x^2 + (4a_{d-3}/d)x)$$

for some $G(x) \in \boldsymbol{F}_q[x]$

or

$$f(x) = H((x^3 + (3a_{d-2}/d)x + 3a_{d-3}/d)^{r+1})$$

for some $H(x) \in \boldsymbol{F}_q[x]$ where r denotes the number of irreducible cubic factors of $f^*(x, y)$ of the form $x^3 - Ty^3 + Ax + By + C$.

Now we will give a series of lemmas from which our main result, Theorem 7, will follow. Proofs for Lemmas 1 and 2 can be found in [5].

Lemma 1. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ denote a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Let the irreducible factorization of $f^*(x, y) = f(x) - f(y)$ be given by

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

Let
$$f_i(x, y) = \sum_{j=0}^{n_i} g_{ij}(x, y)$$

be the homogeneous decomposition of $f_i(x, y)$ so that $n_i = \deg(f_i(x, y))$ and $g_{ij}(x, y)$ is homogeneous of degree j. Assume $a_{d-1} = a_{d-2} = \cdots = a_{d-r} = 0$ for some $r \geq 1$. Then

$$g_{in_i-1}(x, y) = g_{in_i-2}(x, y) = \cdots = g_{iR_i}(x, y) = 0$$

where

$$R_i = \begin{cases} n_i - r \text{ if } n_i \geq r \\ 0 \quad \text{ if } n_i < r. \end{cases}$$

Lemma 2. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ be a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Let N be the number of homogeneous linear factors of $f^*(x, y) = f(x) - f(y)$ over $\boldsymbol{F}_{q^r}$ for some $r \geq 1$. Then, $f(x) = g(x^N)$ for some $g(x) \in \boldsymbol{F}_q[x]$.

Lemma 3. Let d denote a positive divisor of $q - 1$. Then

$$\frac{x^{d-r} - y^{d-r}}{x^d - y^d} = \sum_{i=0}^{d-1} \frac{\mu^{-i(r-1)} - \mu^i}{dy^{r-1}(x - \mu^i y)}$$

where μ denotes a d-th primitive root of unity in $\boldsymbol{F}_q$.

Proof. Considering the expressions as rational functions in x over the rational function field $\boldsymbol{F}_q(y)$ we obtain

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

for some $A_0, A_1, \ldots, A_{d-1}$ in $\boldsymbol{F}_q(y)$. Hence,

$$x^{d-r} - y^{d-r} = \sum_{i=0}^{d-1} \prod_{j \neq i} (x - \mu^j y)A_i,$$

$$(\mu^i y)^{d-r} - y^{d-r} = \prod_{j \neq i} (\mu^i y - \mu^j y)A_i,$$

and consequently

$$(\mu^{-ir}-1)y^{d-r}=d\mu^{i(d-1)}y^{d-1}A_i,$$

$$\mu^{-i(r-1)}-\mu^{i}=dy^{r-1}A_i,$$

for all $0\leq i\leq d-1$. This completes the proof of the Lemma.

Our next Lemma provides a list of basic identities that will be needed later.

Lemma 4. Working formally, if $x^3-Px^2+Qx-W=(x-a)(x-b)(x-c)$, then

(1) $a+b+c=P$,

(2) $ab+bc+ac=Q$,

(3) $abc=W$,

(4) $a^2+b^2+c^2=P^2-2Q$,

(5) $a^2b^2+a^2c^2+b^2c^2=Q^2-2PW$,

(6) $a^3b^3+a^3c^3+b^3c^3=Q^3-3PQW+3W^2$.

Lemma 5. Let $f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$ be a monic polynomial with coefficients in $\boldsymbol{F}_q$. Assume that $f^*(x,y)$ has a factor of the form $g(x)-cg(y)$ for some $g(x)\in\boldsymbol{F}_q[x]$ and $0\neq c\in\boldsymbol{F}_q$. Then, $f(x)=G(g(x))$ for some $G(x)\in\boldsymbol{F}_q[x]$.

Proof. Let $e=\deg(g(x))>0$, $D=[d/e]$ and

$$f(x)=\sum_{i=0}^{D}b_i(x)g^i(x)$$

for some $b_i(x)\in\boldsymbol{F}_q[x]$ with $\deg(b_i(x))<e$ for all i. Thus,

$$\begin{aligned}0&\equiv f^*(x,y) && (\mathrm{mod}\ (g(x)-cg(y)))\\ &\equiv\sum_{i=0}^{D}(b_i(x)g^i(x)-b_i(y)g^i(y)) && (\mathrm{mod}\ (g(x)-cg(y)))\\ &\equiv\sum_{i=0}^{D}(b_i(x)c^i-b_i(y))g^i(y) && (\mathrm{mod}\ (g(x)-cg(y)))\end{aligned}$$

and consequently

$$\sum_{i=0}^{D}b_i(x)(cg(y))^i-\sum_{i=0}^{D}b_i(y)g^i(y)=(g(x)-cg(y))h(x,y)$$

for some $h(x,y)\in\boldsymbol{F}_q[x,y]$. Further, since the x-degree of $\sum_{i=0}^{D}b_i(x)(cg(y))^i$ is less than e and $\deg(g(x))=e$, then $h(x,y)=0$. So,

$$\sum_{i=0}^{D}b_i(x)(cg(y))^i=\sum_{i=0}^{D}b_i(y)g(y)^i\in\boldsymbol{F}_q(x)[y]$$

and $b_i(x)c^i=b_i(y)=b_i\in\boldsymbol{F}_q$ for all i, $0\leq i\leq D$. Therefore, $e\mid d$ and $f(x)=G(g(x))$ where $G(x)=\sum_{i=0}^{D}b_ix^i\in\boldsymbol{F}_q[x]$.

Lemma 6. Let $f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$ denote a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Assume $a_{d-1}=0$. Assume $x^3-Rx^2y+Sxy^2-Ty^3+Ax+By+C$ is a cubic irreducible factor of $f^*(x,y)$. Then

(i) If $a_{d-2}\neq 0$, then $TR=S$, $dAT=(3T-RS+2ST)a_{d-2}$ and $dBT=(S^2-2RT-3T^2)a_{d-2}$.

(ii) If $a_{d-3}\neq 0$, then $T^2R=S^2-2RT$, $RS^2-2TR^2=TS+2ST^2$ and $dCT^2=(S^3-3TRS+3T^2-3T^3)a_{d-3}$.

(iii) If $RSa_{d-2}a_{d-3}\neq 0$, then $T=-1$.

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

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

where $f_1(x,y)=x^3-Rx^2y+Sxy^2-Ty^3+Ax+By+C$. Write

$$x^3-Rx^2y+Sxy^2-Ty^3=(x-w_1y)(x-w_2y)(x-w_3y)$$

for some d-th roots of unity w_1, w_2, and w_3. So, with notation as in Lemma 1,

$$a_{d-2}(x^{d-2}-y^{d-2})=(Ax+By)\prod_{i=2}^{s}g_{in_i}(x,y)+\sum_{j=2}^{s}(g_{in_j-2}(x,y)\prod_{\substack{i=1\\ i\neq j}}^{s}g_{in_i}(x,y))$$

and

$$a_{d-2}(x^{d-3}-y^{d-3})=C\prod_{i=2}^{s}g_{in_i}(x,y)+\sum_{j=2}^{s}(g_{jn_j-3}(x,y)\prod_{\substack{i=1\\ i\neq j}}^{s}g_{in_i}(x,y)).$$

Thus,

$$a_{d-2}\frac{x^{d-2}-y^{d-2}}{x^d-y^d}=\frac{Ax+By}{g_{13}(x,y)}+\sum_{j=2}^{s}\frac{g_{jn_j-2}(x,y)}{g_{jn_j}(x,y)}$$

and

$$a_{d-3}\frac{x^{d-3}-y^{d-3}}{x^d-y^d}=\frac{C}{g_{13}(x,y)}+\sum_{j=2}^{s}\frac{g_{jn_j-2}(x,y)}{g_{jn_j}(x,y)}.$$

Hence, combining with Lemma 3,

$$\frac{a_{d-2}}{dy}\sum_{j=1}^{3}\frac{w_j^{-1}-w_j}{x-w_jy}=\frac{Ax+By}{g_{13}(x,y)}$$

and

$$\frac{a_{d-3}}{dy^2}\sum_{j=1}^{3}\frac{w_j^{-2}-w_j}{x-w_jy}=\frac{C}{g_{13}(x,y)}.$$

Therefore,

(1) $a_{d-2}(w_1^{-1}-w_1+w_2^{-1}-w_2+w_3^{-1}-w_3)=0$,

(2) $dA=-((w_1^{-1}-w_1)(w_2+w_3)+(w_2^{-1}-w_2)(w_1+w_3)+(w_3^{-1}-w_3)(w_1+w_2))a_{d-2}$,

(3) $dB=((w_1^{-1}-w_1)w_2w_3+(w_2^{-1}-w_2)w_1w_3+(w_3^{-1}-w_3)w_1w_2)a_{d-2}$,

(4) $a_{d-3}(w_1^{-2}-w_1+w_2^{-2}-w_2+w_3^{-2}-w_3)=0$,

(5) $a_{d-3}((w_1^{-2}-w_1)(w_2+w_3)+(w_2^{-2}-w_2)(w_1+w_3)+(w_3^{-2}-w_3)(w_1+w_2))=0,$

and

(6) $dC=((w_1^{-2}-w_1)w_2w_3+(w_2^{-2}-w_2)w_1w_3+(w_3^{-2}-w_3)w_1w_2)a_{d-3}.$

Hence, combining with Lemma 4,

(1') $(S-RT)a_{d-2}=0,$

(2') $dAT=(2ST-SR+3T)a_{d-2},$

(3') $dBT=(S^2-2RT-3T^2)a_{d-2},$

(4') $(S^2-2RT-T^2R)a_{d-3}=0,$

(5') $(RS^2-2R^2T-ST-2ST^2)a_{d-3}=0,$

and

(6') $dCT^2=(S^3-3RST+3T^2-3T^3)a_{d-3}.$

Now, to prove (iii), assume that $RSa_{d-2}a_{d-3}\neq 0$. So, $TR=S$, $T^2R=S^2-2RT$ and consequently $S=T+2$. Therefore,

$$RS^2-2TR^2-TS-2ST^2=0,$$
$$R(T+2)S-2SR-TS-2ST^2=0,$$
$$S(RT+2R-2R-T-2T^2)=0,$$
$$S(S-T-2T^2)=0,$$
$$T=\pm 1.$$

One also notices that $T=1$ gives the contradicting statement that $x^3-Rx^2y+Sxy^2-Ty^3=(x-y)^3$ is a factor of x^d-y^d. Therefore, $T=-1$ and the proof of the lemma is complete.

We are ready for our main result.

Theorem 7. Let $f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$ be a monic polynomial over $\boldsymbol{F}_q$ of degree d prime to q. Assume $a_{d-1}=0$ and $a_{d-2}a_{d-3}\neq 0$. Let

$$\prod_{i=1}^{m}(x^3-R_ix^2y+S_ixy^2-T_iy^3+A_ix+B_iy+C_i)\prod_{i=m+1}^{m+r}(x^3-T_iy^3+A_ix+B_iy+C_i)\quad (R_iS_i\neq 0)$$

denote the product of all the irreducible cubic factors of $f^*(x,y)=f(x)-f(y)$. Then

(i) $m\leq 1$ and $f(x)=G(x^4+(4a_{d-2}/d)x^2+(4a_{d-3}/d)x)$ for some $G(x)\in\boldsymbol{F}_q[x]$ if $m=1$.

(ii) $f(x)=H((x^3+(3a_{d-2}/d)x+3a_{d-3}/d)^{r+1})$ for some $H(x)\in\boldsymbol{F}_q[x]$.

Proof. By Lemma 6, $T_i=R_i=-S_i=-1$, $dA_i=dB_i=4a_{d-2}$ and $dC_i=4a_{d-3}$ for all i, $1\leq i\leq m$. Thus, $m\leq 1$ and if $m=1$, then $f(x)-f(y)$ has a factor of the form

$$\begin{aligned}&(x-y)(x^3+x^2y+xy^2+y^3+(4a_{d-2}/d)x+(4a_{d-2}/d)y+4a_{d-3}/d)\\&=(x^4+(4a_{d-2}/d)x^2+(4a_{d-3}/d)x)-(y^4+(4a_{d-2}/d)y^2+(4a_{d-3}/d)y)\\&=h(x)-h(y).\end{aligned}$$

Therefore, applying Lemma 5, we have $f(x)=G(h(x))$ for some $G(x)\in\boldsymbol{F}_q[x]$.

Similarly, $r\geq 1$ and Lemma 6 give factors of the form

$$\begin{aligned}x^3-T_iy^3+A_ix+B_iy+C_i&=(x^3+(3a_{d-2}/d)x+3a_{d-3}/d)-T_i(y^3+(3a_{d-2}/d)y+3a_{d-3}/d)\\&=g(x)-T_ig(y)\end{aligned}$$

with $T_i\neq 1$ for all $m+1\leq i\leq m+r$. So, again by Lemma 5, $f(x)=G(g(x))$ for some $G(x)\in\boldsymbol{F}_q[x]$ and

$$\begin{aligned}f(x)-f(y)&=(g(x)-g(y))\prod_{i=1}^{r}(g(x)-T_ig(y))\prod_{i=1}^{s}Q_i(g(x),g(y))\\&=(x-y)(x^2+xy+y^2+3a_{d-2}/d)\prod_{i=1}^{r}(g(x)-T_ig(y))\prod_{i=1}^{s}Q_i(g(x),g(y))\end{aligned}$$

for some polynomials $Q_i(x,y)\in\boldsymbol{F}_q[x,y]$, $1\leq i\leq s$. One also sees that if one of the factors $Q_i(g(x),g(y))$ is linear in $g(x)$ and $g(y)$, then it is reducible and of the form

$$\begin{aligned}Q_i(g(x),g(y))&=g(x)+g(y)-6a_{d-3}/d\\&=(x+y)(x^2-xy+y^2+3a_{d-2}/d).\end{aligned}$$

Hence, applying Lemma 2, $f(x)=w(x^2)$ for some $w(x)\in\boldsymbol{F}_q[x]$ and $a_{d-3}=0$. Therefore, $G(g(x))-G(g(y))$ has a total of $r+1$ homogeneous linear factors in $g(x)$ and $g(y)$ and

$$f(x)=H((x^3+3a_{d-2}x+3a_{d-3}/d)^{r+1})$$

for some $H(x)\in\boldsymbol{F}_q[x]$.

References

[1] M. Acosta and J. Gomez-Calderon: The second-order factorable core of polynomials over finite fields. Rocky Moutain J. of Math. (to appear).

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

[3] S. D. Cohen: Exceptional polynomials and reducibility of substitution polynomials. L'Ens. Math., **36**, 53–65 (1990).

[4] L. E. Dickson: The analytic representation of substitution polynomials on a power of a prime number of letters with a discussion of the linear group. Ann. of Math., **11**, 65–120; 161–183 (1897).

[5] J. Gomez-Calderon: A note on polynomials of the form $x^d+a_ex^e+\cdots+a_1x+a_0$ over finite fields. Proc. Japan Acad., **70A**, 187-189 (1994).

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

[7] D. R. Hayes: A geometric approach to permutation polynomials over a finite field. Duke Math. J., **34**,

293–305 (1967).
[8] D. Wan: On a conjecture of Carlitz. J. Austral. Math. Soc, ser. A, **43**, 375–384 (1987).