ON THE ROOTS OF THE SUBSTITUTION DICKSON POLYNOMIALS

JAVIER GOMEZ-CALDERON

Received 10 April 2001

We show that under the composition of multivalued functions, the set of the y -radical roots of the Dickson substitution polynomial $g_d(x, a) - g_d(y, a)$ is *generated* by one of the roots. Hence, we show an expected generalization of the fact that, under the composition of the functions, the y -radical roots of $x^d - y^d$ are generated by $\zeta_d y$.

2000 Mathematics Subject Classification: 11Txx, 11T06.

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 set of values $f(x)$, see for example Wan [8], Dickson [4], Hayes [6], and Gomez-Calderon and Madden [5]. The linear and quadratic factors of $f^*(x, y)$ have been studied by Cohen [2, 3] and also by Acosta and Gomez-Calderon [1]. A factor of $f^*(x, y)$ is said to be a *radical factor* if it has the form

$$c(x - R_1(y))(x - R_2(y)) \cdots (x - R_m(y)), \quad c \in F_q, \quad (1)$$

where $r_j(y)$, $1 \leq j \leq m$, denotes a radical expression in y over the algebraic closure of the field of functions $F_q(y)$. If $R_i(y)$ and $R_j(y)$ are *radical roots* of $f^*(x, y)$, then the *composite multivalued function* $R_i(R_j(y))$ provides a set of radical roots of $f^*(x, y)$; that is, $f(R_i(R_j(y))) = f(y)$ for all values of $R_i(R_j(y))$. For example, for q odd,

$$x^3 + x - y^3 - y = (x - R_0(y))(x - R_1(y))(x - R_2(y)), \quad (2)$$

where $R_0(y) = y$, $2R_1(y) = -y + \sqrt{-3y^2 - 4}$, and $2R_2(y) = -y - \sqrt{-3y^2 - 4}$. Thus,

$$R_1(R_1(y)) = \frac{\left[y - \sqrt{-3y^2 - 4} + \left((3y + \sqrt{-3y^2 - 4})^2 \right)^{1/2} \right]}{4} = \{R_0(y), R_2(y)\}. \quad (3)$$

DEFINITION 1. Let F_q denote the finite field of order q and characteristic p . For $a \in F_q$ and an integer $d \geq 1$, let

$$g_d(x, a) = \sum_{t=0}^{\lfloor d/2 \rfloor} \frac{d}{d-t} \binom{d-t}{t} (-a)^t x^{d-2t} \quad (4)$$

denote the Dickson polynomial of degree d over F_q .

LEMMA 2. *Let d be a positive integer and assume that F_q contains a primitive d th root of unity ζ . Put*

$$A_k = \zeta^k + \zeta^{-k}, \quad B_k = \zeta^k - \zeta^{-k}. \quad (5)$$

Then, for each a in F_q ,

(i) *if d is odd,*

$$g_d(x, a) - g_d(y, a) = \prod_{i=1}^{(d-1)/2} (x - y)(x^2 - A_i xy + y^2 + B_i^2 a); \quad (6)$$

(ii) *if d is even,*

$$g_d(x, a) - g_d(y, a) = \prod_{i=1}^{d/2} (x^2 - y^2)(x^2 - A_i xy + y^2 + B_i^2 a). \quad (7)$$

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

PROOF. See [7, Theorem 3.12]. □

THEOREM 3. *If q is odd, $0 \neq a \in F_q$, and $(d, q) = 1$, then*

- (i) $g_d(x, a) - g_d(y, a) = \prod_{i=1}^d (x - R_i(y))$, where $R_1(y), R_2(y), \dots, R_d(y)$ denote d -radical expressions in y over the algebraic closure of the field of functions $F_q(y)$;
- (ii) *under the composition of multivalued functions, the set of roots $R_1(y), R_2(y), \dots, R_d(y)$ is generated by one of the roots $R_i(y)$.*

PROOF. Let ζ be a d th primitive root over the field F_q . With notation as in Lemma 2, write,

(a) if d is odd,

$$\begin{aligned} g_d(x, a) - g_d(y, a) &= (x, y) \prod_{i=1}^{(d-1)/2} (x^2 - A_i xy + y^2 + B_i^2 a) \\ &= (x - \sigma_0(y)) \prod_{i=1}^{(d-1)/2} (x - \sigma_k y^+)(x - \sigma_k y^-), \end{aligned} \quad (8)$$

where $\sigma_0(y^\pm) = y$, $2\sigma_k(y^+) = A_k y + B_k \sqrt{y^2 - 4a}$, and $2\sigma_k(y^-) = A_k y - B_k \sqrt{y^2 - 4a}$ for $1 \leq k \leq (d-1)/2$;

(b) if d is even,

$$\begin{aligned} g_d(x, a) - g_d(y, a) &= (x^2 - y^2) \prod_{i=1}^{d/2} (x^2 - A_i xy + y^2 + B_i^2 a) \\ &= (x - \sigma_0(y))(x - \sigma_{d/2}(y)) \prod_{i=1}^{d/2} (x - \sigma_k(y^+))(x - \sigma_k(y^-)), \end{aligned} \quad (9)$$

where $\sigma_0(y) = y$, $\sigma_{d/2}(y) = -y$, $2\sigma_k(y^+) = A_k y + B_k \sqrt{y^2 - 4a}$, and $2\sigma_k(y^-) = A_k y - B_k \sqrt{y^2 - 4a}$ for $1 \leq k \leq d/2$.

Now we consider the composite multivalued function $\sigma_1(\mathcal{Y}^+) \circ \sigma_k(\mathcal{Y}^+)$

$$\begin{aligned}
 \sigma_1(\mathcal{Y}^+) \circ \sigma_k(\mathcal{Y}^+) &= \sigma_1\left(\frac{[A_k\mathcal{Y} + B_k\sqrt{\mathcal{Y}^2 - 4a}]}{2}\right) \\
 &= \frac{[A_1A_k\mathcal{Y} + A_1B_k\sqrt{\mathcal{Y}^2 - 4a} + B_1((A_k\mathcal{Y} + B_k\sqrt{\mathcal{Y}^2 - 4a})^2 - 16a)^{1/2}]}{4} \\
 &= \frac{[A_1A_k\mathcal{Y} + A_1B_k\sqrt{\mathcal{Y}^2 - 4a} + B_1(A_k^2\mathcal{Y}^2 + 2\mathcal{Y}A_kB_k\sqrt{\mathcal{Y}^2 - 4a} + B_k^2\mathcal{Y}^2 - 4aB_k^2 - 16a)^{1/2}]}{4} \\
 &= \frac{[A_1A_k\mathcal{Y} + A_1B_k\sqrt{\mathcal{Y}^2 - 4a} + B_1(A_k^2\mathcal{Y}^2 + 2\mathcal{Y}A_kB_k\sqrt{\mathcal{Y}^2 - 4a} + B_k^2\mathcal{Y}^2 - 4aA_k^2)^{1/2}]}{4} \\
 &= \frac{[A_1A_k\mathcal{Y} + A_1B_k\sqrt{\mathcal{Y}^2 - 4a} + B_1(B_k\mathcal{Y} + A_k\sqrt{\mathcal{Y}^2 - 4a})]}{4} \\
 &= \frac{[A_1A_k\mathcal{Y} + A_1B_k\sqrt{\mathcal{Y}^2 - 4a} \pm B_1(B_k\mathcal{Y} + A_k\sqrt{\mathcal{Y}^2 - 4a})]}{4} \\
 &= \left\{ (A_1A_k + B_1B_k)\mathcal{Y} + \frac{(A_1B_k + A_kB_1)\sqrt{\mathcal{Y}^2 - 4a}}{4}, \right. \\
 &\quad \left. (A_1A_k - B_1B_k)\mathcal{Y} + \frac{(A_1B_k - A_kB_1)\sqrt{\mathcal{Y}^2 - 4a}}{4} \right\}.
 \end{aligned} \tag{10}$$

Thus,

$$\sigma_1(\mathcal{Y}^+) \circ \sigma_k(\mathcal{Y}^+) = \begin{cases} \sigma_{k+1}(\mathcal{Y}^+), \sigma_{k-1}(\mathcal{Y}^+), & \text{if } 1 \leq k \leq \frac{d-3}{2}, d \text{ is odd,} \\ \sigma_{(d-1)/2}(\mathcal{Y}^-), \sigma_{(d-3)/2}(\mathcal{Y}^+), & \text{if } k = \frac{d-1}{2}, d \text{ is odd,} \\ \sigma_{k+1}(\mathcal{Y}^+), \sigma_{k-1}(\mathcal{Y}^+), & \text{if } 1 \leq k \leq \frac{d}{2} - 1, d \text{ is even,} \\ \sigma_{d/2-1}(\mathcal{Y}^+), \sigma_{d/2-1}(\mathcal{Y}^-), & \text{if } k = \frac{d}{2}, d \text{ is even.} \end{cases} \tag{11}$$

Similarly, we get

$$\sigma_1(\mathcal{Y}^+) \circ \sigma_k(\mathcal{Y}^+) = \begin{cases} \sigma_{k+1}(\mathcal{Y}^-), \sigma_{k-1}(\mathcal{Y}^-), & \text{if } 1 \leq k \leq \frac{(d-3)}{2}, d \text{ is odd,} \\ \sigma_{(d-1)/2}(\mathcal{Y}^+), \sigma_{(d-3)/2}(\mathcal{Y}^-), & \text{if } k = \frac{d-1}{2}, d \text{ is odd,} \\ \sigma_{k+1}(\mathcal{Y}^-), \sigma_{k-1}(\mathcal{Y}^-), & \text{if } 1 \leq k \leq \frac{d}{2} - 1, d \text{ is even,} \\ \sigma_{d/2-1}(\mathcal{Y}^+), \sigma_{d/2-1}(\mathcal{Y}^-), & \text{if } k = \frac{d}{2}, d \text{ is even.} \end{cases} \tag{12}$$

Therefore, $\sigma_1(\mathcal{Y}^+)$ generates the set of radical roots $\sigma_i(\mathcal{Y}^+)$, $\sigma_i(\mathcal{Y}^-)$, for all values i .

□

The set of the γ -radical roots of a substitution polynomial may require more than one generator as we illustrate in the following theorem.

THEOREM 4. For $0 \neq b \in F_q$ and $(mn, q) = 1$, let $f_{m,n}(x, b)$ denote the polynomial $(x^m + b)^n$. Then,

(i) $f_{m,n}(x, b) - f_{m,n}(\gamma, b) = \prod_{i=1}^{mn} (x - R_i(\gamma))$, where $R_1(\gamma), R_2(\gamma), \dots, R_{mn}(\gamma)$ denote radical expressions in γ over algebraic closure of the field of functions $F_q(\gamma)$.

(ii) Under the composition of multivalued functions, the set of roots $R_1(\gamma), R_2(\gamma), \dots, R_{mn}(\gamma)$ is generated by at least m of the roots $R_i(\gamma)$.

PROOF. Let ζ and ξ be primitive roots of unity of order n and m , respectively, over the field F_q . Then

$$\begin{aligned} f_{m,n}(x, b) - f_{m,n}(\gamma, b) &= \prod_{k=1}^n [(x^m + b) - \zeta^k(\gamma^m + b)] \\ &= \prod_{k=1}^n \prod_{i=1}^m [x - \xi^i(\zeta^k \gamma^m + b(1 - \zeta))]^{1/m} \\ &= \prod_{k=1}^n \prod_{i=1}^m (x - \sigma_{ik}(\gamma)). \end{aligned} \quad (13)$$

Now we consider the composite multivalued function $\sigma_{j1}(\gamma) \circ \sigma_{ik}(\gamma)$.

$$\begin{aligned} \sigma_{ji}(\gamma) \circ \sigma_{ik}(\gamma) &= \xi^j ((\zeta(\xi^i(\zeta^k \gamma^m + b(1 - \zeta^k)))^{1/m})^m + b(1 - \zeta))^{1/m} \\ &= \xi^j ((\zeta(\zeta^k \gamma^m + b(1 - \zeta^k)) + b(1 - \zeta))^{1/m})^m \\ &= \xi^j (\zeta^{k+1} \gamma^m + b(1 - \zeta^{k+1}))^{1/m} \\ &= \begin{cases} \sigma_{jk+1}(\gamma), & \text{if } 1 \leq k \leq n-2, 1 \leq j \leq m, \\ \{\sigma_{10}(\gamma), \sigma_{20}(\gamma), \dots, \sigma_{m0}(\gamma)\}, & \text{if } k = n-1, 1 \leq j \leq m. \end{cases} \end{aligned} \quad (14)$$

Therefore, $\sigma_{11}(\gamma), \sigma_{21}(\gamma), \dots, \sigma_{m1}(\gamma)$ generate the set of roots $\{\sigma_{jk}(\gamma) : 1 \leq j \leq m, 1 \leq k \leq n\}$. $\square$

REFERENCES

- [1] M. T. Acosta and J. Gomez-Calderon, *The second-order factorable core of polynomials over finite fields*, Rocky Mountain J. Math. **29** (1999), no. 1, 1-12.
- [2] S. D. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials*, Enseign. Math. (2) **36** (1990), no. 1-2, 53-65.
- [3] ———, *The factorable core of polynomials over finite fields*, J. Austral. Math. Soc. Ser. A **49** (1990), no. 2, 309-318.
- [4] L. E. Dickson, *The analytic representation of substitutions on a prime power of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65-120, 161-183.
- [5] J. Gomez-Calderon and D. J. Madden, *Polynomials with small value set over finite fields*, J. Number Theory **28** (1988), no. 2, 167-188.
- [6] D. R. Hayes, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J. **34** (1967), 293-305.

- [7] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific and Technical, Harlow, 1993.
- [8] D. Q. Wan, *On a conjecture of Carlitz*, J. Austral. Math. Soc. Ser. A **43** (1987), no. 3, 375–384.

JAVIER GOMEZ-CALDERON: DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, NEW KENSINGTON CAMPUS, NEW KENSINGTON, PA 15068, USA

E-mail address: jxg11@psu.edu