

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,*

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

(ii) *if d is even,*

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

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,*

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

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,*

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

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 $\sigma_1(y^+) \circ \sigma_k(y^+)$

$$\begin{aligned}
& \sigma_1(y^+) \circ \sigma_k(y^+) \\
&= \sigma_1\left(\frac{[A_k y + B_k \sqrt{y^2 - 4a}]}{2}\right) \\
&= \frac{[A_1 A_k y + A_1 B_k \sqrt{y^2 - 4a} + B_1 \left(\left(A_k y + B_k \sqrt{y^2 - 4a}\right)^2 - 16a\right)^{1/2}]}{4} \\
&= \frac{[A_1 A_k y + A_1 B_k \sqrt{y^2 - 4a} + B_1 \left(A_k^2 y^2 + 2y A_k B_k \sqrt{y^2 - 4a} + B_k^2 y^2 - 4a B_k^2 - 16a\right)^{1/2}]}{4} \\
&= \frac{[A_1 A_k y + A_1 B_k \sqrt{y^2 - 4a} + B_1 \left(A_k^2 y^2 + 2y A_k B_k \sqrt{y^2 - 4a} + B_k^2 y^2 - 4a A_k^2\right)^{1/2}]}{4} \\
&= \frac{[A_1 A_k y + A_1 B_k \sqrt{y^2 - 4a} + B_1 \left(B_k y + A_k \sqrt{y^2 - a}\right)]}{4} \\
&= \frac{[A_1 A_k y + A_1 B_k \sqrt{y^2 - 4a} \pm B_1 \left(B_k y + A_k \sqrt{y^2 - a}\right)]}{4} \\
&= \left\{ (A_1 A_k + B_1 B_k) y + \frac{(A_1 B_k + A_k B_1) \sqrt{y^2 - 4a}}{4}, \right. \\
&\quad \left. (A_1 A_k - B_1 B_k) y + \frac{(A_1 B_k - A_k B_1) \sqrt{y^2 - 4a}}{4} \right\}. \tag{10}
\end{aligned}$$

Thus,

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

Similarly, we get

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

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

□

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

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

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

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

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

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

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

Special Issue on Modeling Experimental Nonlinear Dynamics and Chaotic Scenarios

Call for Papers

Thinking about nonlinearity in engineering areas, up to the 70s, was focused on intentionally built nonlinear parts in order to improve the operational characteristics of a device or system. Keying, saturation, hysteretic phenomena, and dead zones were added to existing devices increasing their behavior diversity and precision. In this context, an intrinsic nonlinearity was treated just as a linear approximation, around equilibrium points.

Inspired on the rediscovering of the richness of nonlinear and chaotic phenomena, engineers started using analytical tools from "Qualitative Theory of Differential Equations," allowing more precise analysis and synthesis, in order to produce new vital products and services. Bifurcation theory, dynamical systems and chaos started to be part of the mandatory set of tools for design engineers.

This proposed special edition of the *Mathematical Problems in Engineering* aims to provide a picture of the importance of the bifurcation theory, relating it with nonlinear and chaotic dynamics for natural and engineered systems. Ideas of how this dynamics can be captured through precisely tailored real and numerical experiments and understanding by the combination of specific tools that associate dynamical system theory and geometric tools in a very clever, sophisticated, and at the same time simple and unique analytical environment are the subject of this issue, allowing new methods to design high-precision devices and equipment.

Authors should follow the Mathematical Problems in Engineering manuscript format described at <http://www.hindawi.com/journals/mpe/>. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at <http://mts.hindawi.com/> according to the following timetable:

Manuscript Due	December 1, 2008
First Round of Reviews	March 1, 2009
Publication Date	June 1, 2009

Guest Editors

José Roberto Castilho Piqueira, Telecommunication and Control Engineering Department, Polytechnic School, The University of São Paulo, 05508-970 São Paulo, Brazil; piqueira@lac.usp.br

Elbert E. Neher Macau, Laboratório Associado de Matemática Aplicada e Computação (LAC), Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 12227-010 São Paulo, Brazil ; elbert@lac.inpe.br

Celso Grebogi, Center for Applied Dynamics Research, King's College, University of Aberdeen, Aberdeen AB24 3UE, UK; grebogi@abdn.ac.uk