ESKİŞEHİR TEKNİK ÜNİVERSİTESİ BİLİM VE TEKNOLOJİ DERGİSİ
B- TEORİK BİLİMLER

Eskişehir Technical University Journal of Science and Technology B- Theoretical Sciences

2021, 9(2), pp. 25-29, DOI:10.20290/estubtdb.841749

RESEARCH ARTICLE

AN ALGORITHM TO COMPUTE THE DEGREE OF A DICKSON POLYNOMIAL

Erdal İMAMOĞLU *

Department of Mathematics, Faculty of Arts and Sciences, Kirklareli University, Kırklareli, Turkey

ABSTRACT

In this study, we describe an algorithm that computes the degree of a Dickson Polynomial of the First Kind from its known value at a point. Our algorithm is based on a mathematical relation between Dickson Polynomials of the First Kind and Chebyshev Polynomials of the First Kind.

Keywords: Symbolic Computation, Algorithms, Dickson Polynomials, Pohlig-Hellman Algorithm

1. INTRODUCTION

Dickson Polynomials are introduced in [1] by L.E. Dickson. Let K be a finite field with characteristic $char(K) = p$ and $a \in K$. Dickson Polynomials of the First Kind are polynomials in x over K and they are denoted by $D_n(x, a)$ where n is the degree of the polynomial. They can be defined by the recurrence relation

$$\begin{aligned} &D_0(x,a) = 2 \\ &D_1(x,a) = x \\ &D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a), \forall n \geq 2. \end{aligned} \tag{1}$$

Similarly, Dickson Polynomials of the Second Kind are denoted by $E_n(x, a)$ and they can be defined by the same recurrence relation with a different initialization at the degree $n = 0$:

$$\begin{aligned} &E_0(x,a) = 1 \\ &E_1(x,a) = x \\ &E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a), \forall n \geq 2. \end{aligned} \tag{2}$$

Wang and Yucas [2] extend the Dickson Polynomials to a family depending on a new integer parameter $k \in \mathbb{Z}_{\geq 0}$ which they call Dickson Polynomials of the $(k+1)$-th Kind. Those polynomials are denoted by $D_{n,k}(x, a)$ and can be defined similarly:

$$\begin{aligned} &D_{0,k}(x,a) = 2 - k \\ &D_{1,k}(x,a) = x \\ &D_{n,k}(x,a) = xD_{n-1,k}(x,a) - aD_{n-2,k}(x,a), \forall n \geq 2. \end{aligned} \tag{3}$$

Here the integers $k = 0$ and $k = 1$ yield Dickson Polynomials of the First Kind and the Second Kind respectively. Alternatively, Dickson Polynomials of all kinds, can be computed via the matrix formula below:

*Corresponding Author: eimamoglu@klu.edu.tr
Received: 16.12.2020 Published: 30.08.2021

$$\begin{bmatrix} D_{n,k}(x,a) \\ D_{n+1,k}(x,a) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -a & x \end{bmatrix}^n \begin{bmatrix} 2-k \\ x \end{bmatrix}. \tag{4}$$

The matrix method gives rise to an algorithm that computes all Dickson Polynomials of the $(k+1)$-th Kind, $D_{n,k}(x,a)$, in $O(log(n))$ scalar operations.

Dickson Polynomials are examples of orthogonal polynomials and they satisfy several useful properties. The polynomials $D_n(x,a)$ and $E_n(x,a)$ satisfy the differential equations

$$\begin{aligned} &(x^2-4a)D_n''(x,a) + xD_n'(x,a) - n^2 D_n(x,a) = 0 \\ &(x^2-4a)E_n''(x,a) + 3xE_n'(x,a) - n(n+2)E_n(x,a) = 0 \end{aligned} \tag{5}$$

and, in general, the polynomials $D_{n,k}(x,a)$ satisfy the differential equation

$$\begin{aligned} (x^2-4a)D_{n,k}''(x,a) - 4nD_{n+1,k}(x,a)D_{n,k}'(x,a) + (2n+3)xD_{n,k}'(x,a) + n(n+2)D_{n,k}(x,a) \\ = 0. \end{aligned} \tag{6}$$

Dickson Polynomials arise in various areas in mathematics, such as integro-differential-difference equations [4-6], cryptography and number theory [7,8]. Further details about Dickson Polynomials can be found at [3-8] and references within. Equation (6) can be found at [3, Proposition 5].

We address the following problem in this article:

Problem 1.1 From given $p = char(K),\ \beta \in K\backslash\{0\}, a, b \in K$ such that $b^2 = a$ and $\xi = D_\delta(\beta, a) \in K$ compute the degree δ of the Dickson Polynomial of the First Kind $D_\delta(x,a)$.

Dickson Polynomials of the First Kind are related to Chebyshev Polynomials of the First Kind.

Theorem 1.1 If $a \in K, b^2 = a$, then

$$D_n(x,a) = 2b^n T_n\left(\frac{x}{2b}\right). \tag{7}$$

Chebyshev Polynomials of the First Kind have the following two useful properties.

Theorem 1.2. Let $m, n \in \mathbb{Z}_{\geq 0}$. Then:

1. $T_n(T_m(x)) = T_{nm}(x) = T_m(T_n(x))$.
2. $T_n\left(\frac{x+\frac{1}{x}}{2}\right) = \frac{x^n+\frac{1}{x^n}}{2}$ for all $n \geq 0$.

An algorithm that computes the degree of a Chebyshev Polynomial of the First Kind by using its known value at a point is given in [9]. That algorithm makes use of Theorem 1.1 and the idea lying behind of the Pohlig-Hellman Algorithm (which is also known as Silver-Pohlig-Hellman Algorithm) [10]. More details about the Pohlig-Hellman Algorithm and a survey of several discrete logarithm algorithms can be found at [11]. The algorithm in [9], at the end, computes and returns the mixed-radix form of the unknown degree of the Chebyshev Polynomial.

In this paper, we make use of Theorem 1.1, Theorem 1.2(2) and the algorithm in [9] to introduce a method which solves Problem 1.1.

2. DISCUSSION, RESULTS AND ALGORITHM

We want to solve Problem 1.1, i.e., we want to compute the degree δ from given the value $\xi = D_\delta(\beta, a) \in K$ at $x = \beta$. We assume that $\beta \in K\backslash\{0\}$, $a, b \in K$ such that $b^2 = a$ and $p = char(K)$ are known. We may assume, without loss of generality, $\beta = b\left(\omega + \frac{1}{\omega}\right)$ for some unknown $\omega \in \overline{K}$. We do not need to know $\omega \in \overline{K}$. We make use of Theorem 1.1 and Theorem 1.2(2) and proceed as follows:

$$\xi = D_\delta(\beta, a) = D_\delta b\left(b\left(\omega + \frac{1}{\omega}\right), a\right) = 2b^\delta T_\delta\left(\frac{\omega + \frac{1}{\omega}}{2}\right). \tag{8}$$

From the last equation we get

$$\zeta = \xi\left(2b^\delta\right)^{-1} = T_\delta\left(\frac{\omega + \frac{1}{\omega}}{2}\right). \tag{9}$$

If $\zeta = \xi\left(2b^\delta\right)^{-1}$ is known, then algorithm in [9] can compute the degree δ from given $\zeta = T_\delta(\gamma)$, where $\gamma = \left(\omega + \frac{1}{\omega}\right)/2$. Since the degree δ is unknown, here also $\zeta = \xi\left(2b^\delta\right)^{-1}$ remains unknown. Note that, since $b \in K$ is a known value, here two cases occur:

1. If it is given that the order of $b \in K$ divides δ, then $\zeta = \xi\left(2b^\delta\right)^{-1} = \xi/2$. In this case, one can directly use the algorithm in [9] to compute δ.
2. Otherwise, one can compute the order m of $b \in K$ first. Then:

$$\zeta^m = \left(\xi\left(2b^\delta\right)^{-1}\right)^m = \xi^m 2^{-m} = \left(\frac{\xi}{2}\right)^m \tag{10}$$

   From $\zeta^m = (\xi/2)^m$, one can compute ζ. Once ζ is computed, one can use the algorithm in [9] and can compute δ.

We summarize our algorithm as follow:

Algorithm 2.1

Input:

- $a, b \in K$ such that $b^2 = a$
- $p = char(K) \geq 3$
- $\beta = b\left(\omega + \frac{1}{\omega}\right) \in K\backslash\{0\}$
- $\xi = D_\delta(\beta, a) \in K$

Output:

- The order n of ω
- $\delta \bmod n$ or $-\delta \bmod n$

1. Use Theorem 1.1 and Theorem 1.2(2) to get $\zeta = T_\delta(\gamma)$, where $\gamma = \left(\omega + \frac{1}{\omega}\right)/2$, from $\xi = D_\delta(\beta, a)$.
    a. If it is given that the order of b divides δ, let $\zeta = \xi/2$, and proceed to Step 2.
    b. Otherwise:
        i. Compute the order m of b.
        ii. Compute ζ from $\zeta^m = (\xi/2)^m$.

2. Use algorithm in [9] to compute ζ from $\zeta = T_\delta(\gamma)$ where $\gamma = \left(\omega + \frac{1}{\omega}\right)/2$ and return order n of ω, and, $\delta \; mod \; n$ or $-\delta \; mod \; n$.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referees for their helpful comments and suggestions. The authors are supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Project 119F426.

CONFLICT OF INTEREST

The author stated that there are no conflicts of interest regarding the publication of this article.

REFERENCES

[1] Dickson LE. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. Ann Math 1896; 1; 6, 65-120.

[2] Wang Q, Yucas JL. Dickson polynomials over finite fields. Finite Fields Th App 2012; 18, 4, 814-831.

[3] Dominici D. Orhogonality of the Dickson polynomials of the (k+1)-th kind. https://arxiv.org/abs/2011.10673, 2020.

[4] Kürkçü ÖK, Aslan E, Sezer M. A numerical approach with error estimation to solve general integro-differential–difference equations using Dickson polynomials, Appl Math Comput 2016; 276, 324-339.

[5] Kürkçü ÖK, Aslan E, Sezer M. A numerical method for solving some model problems arising in science and convergence analysis based on residual function. Appl Numer Math 2017; 121, 134-148.

[6] Kürkçü ÖK, Aslan E, Sezer M. An inventive numerical method for solving the most general form of integro-differential equations with functional delays and characteristic behavior of orthoexponential residual function. Comput Applied Math 2019; 34

[7] Lindl R. Theory and applications of Dickson polynomials. World Scientific, 1991.

[8] Lindl R, Niederreiter H. Finite fields. Cambridge University Press, 1997.

[9] Imamoglu E, Kaltofen EL. On computing the degree of a Chebyshev polynomial from its value. J Symb Comput 2021; 104, 159-167.

[10] Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE T Inform Theory 1978; 24, 1, 106-110.

[11] Menezes AJ, Vanstone SA, Van Oorschost PC. Handbook of applied cryptography. Boca Raton, FL, CRC Press, 1996.