J. Appl. Math. & Informatics Vol. **29***(2011), No. 1 - 2, pp. 505 - 510*
Website: http://www.kcam.biz

DEGREE BOUND FOR EVALUATION OF ALGEBRAIC FUNCTIONS[†]

SUNG WOO CHOI

ABSTRACT. We give a constructive proof that a (partial) evaluation of a multivariate algebraic function with algebraic numbers is again an algebraic function. Especially, we obtain a bound on the degree of an evaluation with the degrees of the original algebraic function and the algebraic numbers evaluated. Furthermore, we show that our bound is sharp with an example.

AMS Mathematics Subject Classification : 14H05, 68R99
Key words and phrases : algebraic function, degree bound, evaluation

1. Introduction

Algebraic functions form an important class of functions in many areas of mathematics([1, 2, 3]). While they are general enough to encompass many useful functions, they also share a lot of nice properties with polynomials, such as closedness under various operations. Recently, concrete bounds for algebraic functions in general have become important in relation to computational purposes([4]). Especially, the field of exact computation([5]) uses various bounds for algebraic functions on their degrees and heights.

In this paper, we deal with the case when a multivariate algebraic function yields another algebraic function, called an evaluation, by way of evaluating some of its arguments with given algebraic numbers. The fact that an evaluation of an algebraic function is itself an algebraic function needs to be proved. We prove this fact by explicitly constructing the minimal polynomial of the resulting evaluation. The constructed minimal polynomial also gives us a concrete degree bound of the evaluation, in terms of the degree of the original algebraic function and those of the algebraic numbers evaluated. Moreover, we show that our bound is sharp with an example.

Received August 20, 2010. Revised September 7, 2010. Accepted September 8, 2010.
[†] This research was supported by the Duksung Women's University Research Grant 3000001334.

2. Algebraic Functions

Let D be an integral domain, and let α be an element of an extension E of D. Let $D[x]$ be the ring of polynomials in one indeterminate x with coefficients in D. α is called *algebraic* (over D), if there exists a nonzero $P \in D[x]$ such that $P(\alpha) = 0$. Here P is called a *generating polynomial* of α. A generating polynomial irreducible over $D[x]$, and hence with the minimal degree, is called the *minimal polynomial* of α, which is unique up to units in D. The *degree* of α, denoted $\deg(\alpha)$, is the degree of its minimal polynomial. The extension of D by α, denoted $D[\alpha]$, is defined to be the smallest integral domain containing D and α. It is easy to see that

$$D[\alpha] = \{P(\alpha) \mid P \in D[x]\} = \{P(\alpha) \mid P \in D[x], \deg(P) < \deg(\alpha)\},$$

so that $[D[\alpha] : D] = \deg(\alpha)$, where $[D[\alpha] : D]$ is the *extension degree* of $D[\alpha]$ over D which is the dimension of $D[\alpha]$ as a D-module.

Let $\mathbb{Z}$ be the set of integers, and let $\mathbb{C}$ be the set of complex numbers. Consider the case when $D = \mathbb{Z}$. A number α is called an *algebraic number*, if it is algebraic over $\mathbb{Z}$. The set of all algebraic numbers, denoted by $\mathbb{A}$, is a proper subset of $\mathbb{C}$.

A (complex-valued) function $f(x)$ in one complex variable is an *algebraic function*, if there exists a nonzero $F(x, y) \in \mathbb{Z}[x][y]$ such that $F(x, f(x)) = 0$ for every definable x. The degree, $\deg(f)$, of f is the minimal y-degree of such F. Thus f is an algebraic function, if and only if f is algebraic over $\mathbb{Z}[x]$. Note also that $\deg(f) = [\mathbb{Z}[x][f] : \mathbb{Z}[x]]$.

Finally, a (complex-valued) function $f(x_1, \ldots, x_n)$ in several complex variables $x_1, \ldots, x_n$ is called a *multivariate algebraic function*, or just an *algebraic function*, if there exists a nonzero $F \in \mathbb{Z}[x_1, \ldots, x_n][y]$ such that

$$F(x_1, \ldots, x_n, f(x_1, \ldots, x_n)) = 0$$

for every definable $(x_1, \ldots, x_n)$. Again, f is a multivariate algebraic function if and only if f is algebraic over $\mathbb{Z}[x_1, \ldots, x_n]$, and

$$\deg(f) = [\mathbb{Z}[x_1, \ldots, x_n][f] : \mathbb{Z}[x_1, \ldots, x_n]].$$

3. Evaluation of Algebraic Functions

Let $f(x_1, \ldots, x_n)$ be an algebraic function, and let $c_{r+1}, \ldots, c_n$ be algebraic numbers. The function

$$f_{c_{r+1},\ldots,c_n}(x_1, \ldots, x_r) := f(x_1, \ldots, x_r, c_{r+1}, \ldots, c_n)$$

in r variables $x_1, \ldots, x_r$ is called the *evaluation* of f at $c_{r+1}, \ldots, c_n$.

Lemma 1. *Let $f(x_1, \ldots, x_n)$ be an algebraic function, and let c be an algebraic number. Let $f_c(x_1, \ldots, x_{n-1}) := f(x_1, \ldots, x_{n-1}, c)$ be the evaluation of f at c. Then f_c is an algebraic function, and* $\deg(f_c) \le \deg(f) \cdot \deg(c)$.

Proof. Let $d = \deg(f)$, and let $P(x_1, \ldots, x_n, y) = \sum_{j=0}^{d} a_j(x_1, \ldots, x_n) y^j$ in $\mathbb{Z}[x_1, \ldots, x_n][y]$ be the minimal polynomial of f. We first deal with the case when f is constant. If f has a constant value k, then it is easy to see that P is just the minimal polynomial in $\mathbb{Z}[y]$ of the algebraic number k. P is also the minimal polynomial of the evaluation f_c, which has the constant value k. So we have $\deg(f_c) = \deg(f)$, and the desired result holds in this case.

For the rest of proof, we assume that f is nonconstant. From the definition of f_c, we have

$$\begin{aligned} 0 &= P\left(x_1, \ldots, x_{n-1}, c, f\left(x_1, \ldots, x_{n-1}, c\right)\right) \\ &= \sum_{j=0}^{d} a_j\left(x_1, \ldots, x_{n-1}, c\right) f\left(x_1, \ldots, x_{n-1}, c\right)^j \\ &= \sum_{j=0}^{d} a_{j_c}\left(x_1, \ldots, x_{n-1}\right) f_c\left(x_1, \ldots, x_{n-1}\right)^j, \end{aligned}$$

for every definable $(x_1, \ldots, x_{n-1})$. Here,

$$a_{j_c}\left(x_1, \ldots, x_{n-1}\right) := a_j\left(x_1, \ldots, x_{n-1}, c\right)$$

is the evaluation of a_j at c for $0 \le j \le d$.

We first claim that at least one of a_{j_c}, $0 \le j \le d$, is nonzero, where we regard these a_{j_c}'s as elements in the extension field $\mathbb{Z}\left(x_1, \ldots, x_{n-1}\right)[c]$. Let $Q(y) \in \mathbb{Z}[y]$ be the minimal polynomial of the algebraic number c. Note that Q can be regarded as the minimal polynomial $Q\left(x_1, \ldots, x_{n-1}, y\right)$ in $\mathbb{Z}\left[x_1, \ldots, x_{n-1}\right][y]$ of the constant function $c = c\left(x_1, \ldots, x_{n-1}\right) \in \mathbb{Z}\left[x_1, \ldots, x_{n-1}\right][c]$. Now suppose that a_{j_c} is zero for every $0 \le j \le d$. Then

$$a_{j_c}\left(x_1, \ldots, x_{n-1}\right) = a_j\left(x_1, \ldots, x_{n-1}, c\right) = 0,$$

for every definable $(x_1, \ldots, x_{n-1})$. This implies that every a_j has the nontrivial factor Q, and hence P should have the nontrivial factor Q. Since P is minimal, we must have $P = Q$, which involves only the y variable. But this implies that f is constant, which contradicts the assumption that f is nonconstant. Thus there exists at least one $0 \le j \le d$ such that a_{j_c} is nonzero.

Let $\tilde{d}$ be the largest among such j's. Then we have

$$\sum_{j=0}^{\tilde{d}} a_{j_c}\left(x_1, \ldots, x_{n-1}\right) f_c\left(x_1, \ldots, x_{n-1}\right)^j = 0,$$

for every definable $(x_1, \ldots, x_{n-1})$. Since $a_{\tilde{d}c}$is a nonzero element of the extension field $\mathbb{Z}\left(x_1, \ldots, x_{n-1}\right)[c]$, there exists the inverse $a_{\tilde{d}c}^{-1}$ of $a_{\tilde{d}c}$ in $\mathbb{Z}\left(x_1, \ldots, x_{n-1}\right)[c]$, so that

$$a_{\tilde{d}c}^{-1}\left(x_1, \ldots, x_{n-1}\right) = \sum_{i=0}^{\deg(c)-1} b_i\left(x_1, \ldots, x_{n-1}\right) c^i,$$

for some $b_i \in \mathbb{Z}\left(x_1, \ldots, x_{n-1}\right)$, $0 \le i < \deg(c)$.

Let $\overrightarrow{v} = \overrightarrow{v}(x_1, \ldots, x_{n-1})$ be the $\left(\deg(c)\tilde{d}\right)$-dimensional column vector whose elements are

$$v_{i;j} = c^i \cdot f_c(x_1, \ldots, x_{n-1})^j, \quad 0 \le i < \deg(c), \quad 0 \le j < \tilde{d}.$$

Consider $f_c(x_1, \ldots, x_{n-1}) \cdot v_{i;j}$. When $0 \ \le j < \tilde{d} - 1$, we have

$$f_c(x_1, \ldots, x_{n-1}) \cdot v_{i;j} = c^i \cdot f_c(x_1, \ldots, x_{n-1})^{j+1} = v_{i;j+1}.$$

When $j = \tilde{d} - 1$, we have

$$\begin{aligned} & f_c(x_1, \ldots, x_{n-1}) \cdot v_{i;j} \\ = \;& c^i \cdot f_c(x_1, \ldots, x_{n-1})^{\tilde{d}} \\ = \;& -c^i \cdot a_{\tilde{d}c}^{-1}(x_1, \ldots, x_{n-1}) \sum_{j=0}^{\tilde{d}-1} a_{j\,c}(x_1, \ldots, x_{n-1}) f_c(x_1, \ldots, x_{n-1})^j \\ = \;& -c^i \cdot \sum_{k=0}^{\deg(c)-1} b_k(x_1, \ldots, x_{n-1}) c^k \cdot \sum_{j=0}^{\tilde{d}-1} a_{j\,c}(x_1, \ldots, x_{n-1}) f_c(x_1, \ldots, x_{n-1})^j \\ = \;& \sum_{l=0}^{\deg(c)-1} \sum_{j=0}^{\tilde{d}-1} \tilde{b}_{l;j}(x_1, \ldots, x_{n-1}) \cdot v_{l;j}, \end{aligned}$$

for some $\tilde{b}_{l;j} \in \mathbb{Z}(x_1, \ldots, x_r)$, $0 \le l < \deg(c)$, $0 \le j < \tilde{d}$. It follows that there exists a $\left(\deg(c)\tilde{d}\right)$-dimensional square matrix $M = M(x_1, \ldots, x_{n-1}) \in \mathrm{gl}\left(\deg(c)\tilde{d}, \mathbb{Z}(x_1, \ldots, x_{n-1})\right)$ such that

$$M(x_1, \ldots, x_{n-1}) \overrightarrow{v}(x_1, \ldots, x_{n-1}) = f_c(x_1, \ldots, x_{n-1}) \overrightarrow{v}(x_1, \ldots, x_{n-1}).$$

So $\tilde{H}(x_1, \ldots, x_{n-1}, f_c(x_1, \ldots, x_{n-1})) = 0$ for every definable $(x_1, \ldots, x_{n-1})$, where $\tilde{H}(x_1, \ldots, x_{n-1}, y) := \det(M(x_1, \ldots, x_{n-1}) - yI) \in \mathbb{Z}(x_1, \ldots, x_{n-1})[y]$. Multiplying $\tilde{H}$ with appropriate $b \in Z[x_1, \ldots, x_{n-1}]$, we get $H(x_1, \ldots, x_{n-1}, y) := b(x_1, \ldots, x_{n-1}) \tilde{H}(x_1, \ldots, x_{n-1}, y)$ in $\mathbb{Z}[x_1, \ldots, x_{n-1}, y]$, so that

$$H(x_1, \ldots, x_{n-1}, f_c(x_1, \ldots, x_{n-1})) = 0,$$

for every definable $(x_1, \ldots, x_{n-1})$. Thus H is a generating polynomial of f_c, and hence f_c is algebraic. Moreover, we also obtain

$$\deg(f_c) \le \deg_y(H) \le \deg(c)\tilde{d} \le \deg(c)d = \deg(f) \cdot \deg(c),$$

which competes the proof. □

With iterative use of Lemma 1, we immediately obtain the following main result.

Theorem 1 (Degree Bound for Evaluation)**.** *Let $f(x_1, \ldots, x_n)$ be an algebraic function, and let $c_{r+1}, \ldots, c_n$ be algebraic numbers. Let*

$$f_{c_{r+1},\ldots,c_n}(x_1, \ldots, x_r) := f(x_1, \ldots, x_r, c_{r+1}, \ldots, c_n)$$

be the evaluation of f at $c_{r+1},\ldots,c_n$. Then $f_{c_{r+1},\ldots,c_n}$ is an algebraic function, and we have

$$\deg\left(f_{c_{r+1},\ldots,c_n}\right) \le \deg(f)\cdot \prod_{i=r+1}^{n} \deg(c_i).$$

We will show that, in fact, the bound in Theorem 1 is sharp, which means that there exists an example realizing the equality of the bound. To see this fact, we consider the following example: Define $f(x_1,x_2) = \sqrt{x_1^2+x_2}$, which clearly is an algebraic function. It is easy to see that its minimal polynomial is $F(x_1,x_2,y) = y^2 - x_1^2 - x_2$, and hence $\deg(f) = 2$. Let $c = \sqrt{2}$, which is an algebraic number with $\deg(c) = 2$. The evaluation $f_c(x_1) := f(x_1,c)$ of f at c is $f_c(x_1) = \sqrt{x_1^2+\sqrt{2}}$. Consider the generating polynomial $G(x_1,y) = \left(y^2-x_1^2\right)^2 - 2 = y^4 - 2x_1^2y^2 + x_1^4 - 2$ of f_c. We show in the following lemma that G is irreducible in $\mathbb{Z}[x_1,y]$, and hence G is the minimal polynomial of f_c.

Lemma 2. *$G(x_1,y) = y^4 - 2x_1^2y^2 + x_1^4 - 2$ is irreducible in $\mathbb{Z}[x_1,y]$.*

Proof. Suppose G is reducible in $\mathbb{Z}[x_1,y]$. Then G has a factor in $\mathbb{Z}[x_1,y]$ whose y-degree is either 1, or 2.

(Case 1) When G has a factor with y-degree 1: There exist $a(x_1)$, $b(x_1)$, $c(x_1)$, $d(x_1)$ in $\mathbb{Z}[x_1]$, such that

$$\begin{aligned} y^4 - 2x_1^2y^2 + x_1^4 - 2 &= (y+a)\left(y^3+by^2+cy+d\right) \\ &= y^4 + (a+b)y^3 + (ab+c)y^2 + (ac+d)y + ad. \end{aligned}$$

First, we have $a+b=0$, and so $b=-a$. Hence $ab+c = -a^2+c = -2x_1^2$, and so $c = a^2-2x_1^2$. Now $ac+d = a(a^2-2x_1^2)+d = 0$, and so $d = -a(a^2-2x_1^2)$. Finally, we get $ad = -a^2(a^2-2x_1^2) = x_1^4-2$. Since x_1^4-2 is irreducible in $\mathbb{Z}[x_1]$, we must have $a=\pm1$. The we have $-(\pm1)^2\cdot\left((\pm1)^2-2x_1^2\right) = x_1^4-2$, which is a contradiction.

(Case 2) When G has a factor with y-degree 2: There exist $a(x_1)$, $b(x_1)$, $c(x_1)$, $d(x_1)$ in $\mathbb{Z}[x_1]$, such that

$$\begin{aligned} y^4 - 2x_1^2y^2 + x_1^4 - 2 &= (y^2+ay+b)(y^2+cy+d) \\ &= y^4 + (a+c)y^3 + (b+d+ac)y^2 + (ad+bc)y + bd. \end{aligned}$$

First, $a+c=0$, and so $c=-a$. Hence $ad+bc = a(d-b) = 0$, and so we have either $a=0$ or $b=d$.

Suppose $a=0$. Then $c=-a=0$, and $b+d+ac = b+d = -2x_1^2$, $bd = x_1^4-2$. It follows that $bd = -b(b+2x_1^2) = x_1^4-2$. Since x_1^4-2 is irreducible in $\mathbb{Z}[x_1]$, we have either $b=\pm1$, in which case $-(\pm1)\cdot(\pm1+2x_1^2) = x_1^4-2$, or $b+2x_1^2=\pm1$, in which case $-(-2x_1^2\pm1)\cdot(\pm1) = x_1^4-2$. But both cases are impossible.

Now suppose $b=d$. Then $bd = b^2 = x_1^4-2$, which is impossible since x_1^4-2 is irreducible in $\mathbb{Z}[x_1]$.

Thus all the exhausting cases are impossible, which proves that G is irreducible in $\mathbb{Z}[x_1,y]$. □

From Lemma 2, we have $\deg(f_c) = \deg_y(G) = 4 = 2 \cdot 2 = \deg(c)\deg(f)$, which shows the following sharpness result of our bound.

Theorem 2 (Sharpness of The Degree Bound). *The bound in Theorem 1 is sharp.*

References

1. E. Artin, *Algebraic Numbers and Algebraic Functions*, AMS Chelsea Publishing, 2006.
2. G. A. Jones and D. Sinqerman, *Complex Functions: An Algebraic and Geometric Viewpoint*, Cambridge University Press, 1987.
3. F. Klein, *On Riemann's Theory Of Algebraic Functions And Their Integrals*, Merchant Books, 2007.
4. C. K. Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford University Press, 2000.
5. C. K. Yap, *Theory of Real Computation According to EGC*, In P. Hertling, C. M. Hoffmann, W. Luther, N. Revol, Eds., *Reliable Implementation of Real Number Algorithms: Theory and Practice, International Seminar Dagstuhl Castle, Germany, January 8-13, 2006, Revised Papers*, Lecture Notes in Computer Science **5045**(2008), 193-237.

Sung Woo Choi received M.Sc. and Ph.D from Seoul National University. Since 2005, he has been at Duksung Women's University. His current research interests include exact computation.

Department of Mathematics, Duksung Women's University, Seoul 132-714, Korea
e-mail: swchoi@duksung.ac.kr