THE N-TH ROOT ALGORITHM

DANIEL CORDERO GRAU

E-mail: dcgrau01@yahoo.co.uk

In this paper we give the $\mathbf{n}$-th root algorithm in complete normed euclidean semialgebras for every nonzero real $\mathbf{n}$ not Newton's approximation by differentials. The algorithm starts with an input semialgebra nonzero element x with arbitrary length n, thereafter writes $O(n)$ semialgebra elements in time $O(n)$ to go through $O(n)$ steps in each of which compares, computes and writes $O(1)$ semialgebra elements in space $O(n^2)$, and so, in time $O(n^3)$.

Let $\mathcal{R}$ be a complete normed euclidean semialgebra with Zariski topology $\mathcal{F}$ and let $\mathbb{N}_{\mathcal{R}}$ be its prime semialgebra. Let $x \in \mathcal{R}$ such that $x \neq 0_{\mathcal{R}}$. Let $p \in \mathbb{N}_{\mathcal{R}}$ such that $\deg p > 0$ and $p \neq 1_{\mathcal{R}}$, that is, since $\mathcal{R}$ is normed, the multiplicative cyclic subgroup $\langle p \rangle$ is a basis for $\mathcal{R}$. Let $\mathbf{n} \in \mathbb{N}$ such that $\mathbf{n} > 1$. Let $\mathbb{Z}_{\mathcal{R}}[x]$ be the algebra of polynomials of one variable in $\mathcal{R}$ over the algebra $\mathbb{Z}_{\mathcal{R}}$ generated by the semialgebra $\mathbb{N}_{\mathcal{R}}$ and let $\mathcal{B}$ be the basis for the Zariski topology $\mathcal{F}$ for $\mathcal{R}$, that is, $\mathcal{B} \subset \mathcal{F}$ such that for every $F \in \mathcal{B}$ there exists $s \in \mathcal{R}$ and $F_s \in \mathcal{F}$ such that there exists a linear polynomial $f \in \mathbb{Z}_{\mathcal{R}}[x]$ such that $f(s) = 0_{\mathcal{R}}$, $F_s = \mathrm{Var}(f)$ and $F = F_s$.

By the division algorithm in complete semialgebras, for x and $\langle p \rangle$ there exist unique $N \in \mathbb{Z}$ and $a_N, a_{N-1}, \ldots \in \mathbb{N}_{\mathcal{R}}$ such that $a_N \neq 0$,

$$x = \sum_{i=0}^{\infty} a_{N-i} p^{N-i}$$

and $0 \leq \deg a_{N-i} < \deg p$ for every $i \in \mathbb{N}$. Also, by the division algorithm in algebras, for $N \in \mathbb{Z}$ and $\mathbf{n} \in \mathbb{N}$ there exist unique $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ such that $N = \mathbf{n}q + r$ and $0 \leq \deg_{\mathbb{Z}} r < \deg_{\mathbb{Z}} \mathbf{n}$, that is, $0 \leq r < \mathbf{n}$, then

$$x = \sum_{k=0}^{r} a_{\mathbf{n}q+k} p^{\mathbf{n}q+k} + \sum_{i=1}^{\infty} \sum_{k=0}^{\mathbf{n}-1} a_{\mathbf{n}(q-i)+k} p^{\mathbf{n}(q-i)+k}.$$

Let $g_0, g_1, \ldots \in \mathcal{R}$ such that

$$g_0 = \sum_{k=0}^{r} a_{\mathbf{n}q+k} p^k$$

and

$$g_i = \sum_{k=0}^{\mathbf{n}-1} a_{\mathbf{n}(q-i)+k} p^k$$

for every $i > 0$. At the first step find

$$y_0 = \max\{y \in \bigcup_{\substack{s \in \mathbb{N}_{\mathcal{R}} \\ \deg s < \deg p}} F_s \colon\ y^{\mathbf{n}} \leq g_0\}$$

and write

$$r_0 = g_0 - y_0^{\mathbf{n}}$$

and

$$d_0 = p^{\mathbf{n}} r_0 + g_1.$$

Afterwards find

$$y_1 = \max\{y \in \bigcup_{\substack{s\in\mathbb{N}_{\mathcal{R}}\\ \deg s<\deg p}} F_s\colon \sum_{j=1}^{\infty} \tbinom{\mathbf{n}}{j} (py_0)^{\mathbf{n}-j} y^j \leq d_0\}$$

and write

$$r_1 = d_0 - \sum_{j=1}^{\infty} \tbinom{\mathbf{n}}{j} (py_0)^{\mathbf{n}-j} y_1^j$$

and

$$d_1 = p^{\mathbf{n}} r_1 + g_2.$$

At the i-th step find

$$y_i = \max\{y \in \bigcup_{\substack{s\in\mathbb{N}_{\mathcal{R}}\\ \deg s<\deg p}} F_s\colon \sum_{j=1}^{\infty} \tbinom{\mathbf{n}}{j} (\sum_{k=0}^{i-1} p^{i-k} y_k)^{\mathbf{n}-j} y^j \leq d_{i-1}\}$$

and write

$$r_i = d_{i-1} - \sum_{j=1}^{\infty} \tbinom{\mathbf{n}}{j} (\sum_{k=0}^{i-1} p^{i-k} y_k)^{\mathbf{n}-j} y_i^j$$

and

$$d_i = p^{\mathbf{n}} r_i + g_{i+1}.$$

Finally, the **n**-th root z of x is

$$z = \sum_{i=0}^{\infty} y_i p^{q-i}.$$

In general, for any nonzero real $\mathbf{n} \in \mathbb{R}$ the **n**-th root algorithm multiplies the integer powers of $\mathbf{p}^i$-th roots of x in the expansion for $\frac{1}{\mathbf{n}}$ in terms of any basis $\left\{\mathbf{p}^i\right\}_{i\in\mathbb{Z}}$ for $\mathbb{R}$, dividing after if necessary.

Time complexity of the n-th root algorithm

The **n**-th root algorithm is of polynomial time complexity because for every complete semialgebra $\mathcal{R}$, for every positive integer $\mathbf{n} > 1$, for an input semialgebra nonzero element $x \in \mathcal{R}$ with length n, since the **n**-th root is an isomorphism between the positive multiplicative algebra and the real algebra and by the division algorithm in semialgebras for $n-1 \in \mathbb{N}$ and $\mathbf{n} \in \mathbb{N}$ there exist unique $m \in \mathbb{N}$ and $\rho \in \mathbb{N}$ such that $n = \mathbf{n}m + \rho$ and $1 \leq \rho < \mathbf{n} + 1$, the output has length $m + 1 = O(m)$ if it is finite, as is the number of steps in which it is computed at the i-th of which, after writing $O(m)$ elements with length $O(1)$, so, in time $O(m)$, the **n**-th root algorithm compares and writes $O(1)$ elements computed in space $O(m^{\mathbf{2}})$, so, in time $O(m^{\mathbf{2}})$, therefore, since $O(m^{\mathbf{3}}) = O(n^{\mathbf{3}})$, the time complexity of the **n**-th root algorithm is $T(n) = O(n^{\mathbf{3}})$ for integer **n**. And because for every noninteger real **n** and for every length $O(\boldsymbol{n})$ of $\mathbf{n}^{-1}$ in terms of any basis $\left\{\mathbf{p}^i\right\}_{i\in\mathbb{Z}}$ for $\mathbb{R}$, if the length of the **n**-th root of x is finite, the **n**-th root algorithm multiplies $O(\boldsymbol{n})$ integer powers of $\mathbf{p}^i$-th roots of x with length $O(n)$, therefore the time complexity of the **n**-th root algorithm is $T(n) = O(n^{\mathbf{3}})$.

Theorem of the theory of complete semialgebras

The **n**-th root algorithm is a logical consequence of the division algorithm in complete semialgebras and the binomial theorem in semialgebras which states for every semialgebra $\mathcal{R}$ with semialgebra of polynomials of m variables $\mathcal{R}[x_1, \ldots, x_m]$, for every $\mathbf{n} \in \mathbb{N}$ with $\mathbf{n} > 0$ and for every $y_0, y_1, \ldots, y_n \in \mathcal{R}[x_1, \ldots, x_m]$ with $n > 0$,

$$(y_0 + y_1 + \cdots + y_n)^{\mathbf{n}} = \sum_{i=0}^{\infty} \binom{\mathbf{n}}{i} (\sum_{k=0}^{n-1} y_k)^{\mathbf{n}-i} y_n^i.$$

Thus is the **n**-th root algorithm not a theorem of the theory of semialgebras, but a theorem of the theory of complete semialgebras.

This paper is dedicated to my mother Susana Grau Avila