THE N-TH ROOT ALGORITHM

DANIEL CORDERO GRAU
E-mail: dcgrau01@yahoo.co.uk

In this paper we give the **n**-th root algorithm in topologically complete injective simple semialgebras not Newton's approximation by differentials. The algorithm starts with an input semialgebra nonzero element of 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 $\mathcal{A}$ be topologically complete injective simple semialgebra which is not equal to itself as an algebra. $\mathcal{A}$ is a nonzero semialgebra for it is not equal to itself as an algebra, so it is a semifield not $\mathbb{C}$ for it is a nonzero injective simple semialgebra which is also a projective semialgebra over the positive semialgebra as any topologically complete injective simple semialgebra, but not a semialgebra over $\mathbb{C}$ because if so it is equal to $\mathbb{C}$ since it is simple, but $\mathbb{C}$ is equal to itself as an algebra, and so $\mathcal{A}$ is the positive semialgebra.

Let $\mathcal{F}$ be the Zariski topology on the prime semialgebra $\mathbb{N}$. Let $\mathbb{Z}\,[x]$ be the algebra of polynomials of one variable in $\mathbb{N}$ over the prime algebra $\mathbb{Z}$, and let $\mathcal{B}$ be the basis for the Zariski topology $\mathcal{F}$ for $\mathbb{N}$, that is, $\mathcal{B} \subset \mathcal{F}$ such that for every $F \in \mathcal{F}$ and for every $s \in F$ there exists $F_s \in \mathcal{B}$ such that there exists a linear polynomial $f \in \mathbb{Z}[x]$ with $f(s) = 0$, $F_s = \mathrm{Var}(f)$ and $F_s \subset F$. Let $x \in \mathcal{A}$ with $x \neq 0$ and let $p \in \mathbb{N}$ with $p > 1$.

The semialgebra $\mathcal{A}$ is equal to the subsemialgebra $\sum\limits_{i\in\mathbb{Z}} p^i\mathbb{N}$ for it is a simple semialgebra. By the division algorithm in topologically complete injective simple semialgebras for x and p there exist unique $N \in \mathbb{Z}$ and $a_N, a_{N-1}, \ldots \in \mathbb{N}$ such that $a_N \neq 0$,

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

and $0 \leq a_{N-i} < p$ for every i. 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 $0 \leq r < \mathbf{n}$, 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 $g_0, g_1, \ldots \in \mathcal{A}$ 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

$$y_0 = \max\{y \in \bigcup_{s<p} F_s : \ y^{\mathbf{n}} \le g_0\}$$

and write

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

and

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

Afterwards find

$$y_1 = \max\{y \in \bigcup_{s<p} F_s : \ \sum_{j=1}^{\infty} \binom{\mathbf{n}}{j} (py_0)^{\mathbf{n}-j} y^j \le d_0\}$$

and write

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

and

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

At the i-th step find

$$y_i = \max\{y \in \bigcup_{s<p} F_s : \ \sum_{j=1}^{\infty} \binom{\mathbf{n}}{j} (\sum_{k=0}^{i-1} p^{i-k} y_k)^{\mathbf{n}-j} y^j \le d_{i-1}\}$$

and write

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

and

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

Finally the $\mathbf{n}$-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 $\mathbf{n}$-th root algorithm expands $\mathbf{n}^{-1}$ in terms of any positive integer basis $\{\mathbf{p}^i\}_{i \in \mathbb{Z}}$ for $\mathbb{R}$ over $\mathbb{Z}$ and multiplies the product of the $\mathbf{p}^i$-powers and the $\mathbf{p}^i$-th roots of x in the expansion for $x^{\mathbf{n}^{-1}}$ as a product of integer powers of $\left\{x^{\mathbf{p}^i}\right\}_{i \in \mathbb{Z}}$ dividing after if $\mathbf{n}$ <0.

Time complexity of the n-th root algorithm

The **n**-th root algorithm is of polynomial time complexity because for every topologically complete injective simple semialgebra $\mathcal{A}$ not $\mathbb{C}$, for every input nonzero $x \in \mathcal{A}$ of length n, for every positive integer $\mathbf{n} > 1$, 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 $k \in \mathbb{N}$ such that $n = \mathbf{n}m + k$ and $1 \leq k < \mathbf{n} + 1$, the output is of length $m + 1 = O(m) = O(n)$ 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 $O(m^{\mathbf{2}})$, and so in time $O(n^{\mathbf{3}})$. And because for every noninteger real $\mathbf{n}$ and for every length $O(\boldsymbol{n})$ of $\mathbf{n}^{-1}$ in terms of any positive integer basis $\left\{\mathbf{p}^i\right\}_{i\in\mathbb{Z}}$ for $\mathbb{R}$ over $\mathbb{Z}$ the **n**-th root algorithm multiplies $O(\boldsymbol{n})$ integer powers of $\mathbf{p}^i$-powers and $\mathbf{p}^i$-th roots of x of length $O(n)$ if the length of the **n**-th root of x is finite, and so in time $O(n^2)$, therefore the time complexity of the **n**-th root algorithm is $T(n) = O(n^{\mathbf{3}})$.

Theorem of the theory of topologically complete semialgebras

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

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

On the other hand the **n**-th root algorithm characterizes the positive semialgebra as the unique topologically complete injective simple semialgebra not an algebra up to isomorphism, that from which any topological homomorphism to any nonzero topologically complete injective semialgebra is an embedding.

Therefore the **n**-th root algorithm is a theorem of the theory of topologically complete semialgebras.

This paper is dedicated to my mother Susana Grau Avila