The n-th root algorithm

Daniel Cordero Grau
email: dcgrau01@yahoo.co.uk

In this paper we give the n-th root algorithm in completions of fraction semifields of normed euclidean $\mathbb{N}$-semialgebras for every natural $n > 1$. The algorithm starts with a nonzero element in terms of its p-adic expansion for a nonunit of nonzero degree element p of the normed euclidean $\mathbb{N}$-semialgebra, thereafter, for a nonzero natural m, calculates and writes $O(m)$ elements of length $O(1)$ to go through $O(m)$ steps in each of which compares, calculates and writes $O(1)$ elements of length $O(m^k)$ for some natural number k.

Let $\mathcal{R}$ be the completion of the fraction semifield $\mathbb{Q}^+_{\mathcal{R}}$ of a normed euclidean semialgebra $\mathbb{N}_{\mathcal{R}}$ with the Zariski topology $\mathcal{F}$, 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, for $\mathbb{N}_{\mathcal{R}}$ is a normed euclidean semiring and $\mathcal{R}$, a complete free $\mathbb{N}_{\mathcal{R}}$-semialgebra, its multiplicative cyclic subgroup $\langle p\rangle$ is a basis of $\mathcal{R}$. Let $n \in \mathbb{N}$ such that $n > 1$. Let $\mathbb{Z}[x]$ be the $\mathbb{N}$-algebra of polynomials of one variable in $\mathcal{R}$ over $\mathbb{Z}$ with the Zariski topology, and let $\mathcal{B}$ be the basis of the Zariski topology $\mathcal{F}$ for $\mathbb{Z}[x]$, 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 $f \in \mathbb{Z}[x]$ such that $f(s) = 0_{\mathcal{R}}$, $F_s = \mathrm{Var}(f)$ and $F = F_s$.

By the division algorithm in normed euclidean 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, for $\mathcal{R}$ is a complete free $\mathbb{N}_{\mathcal{R}}$-semialgebra and $\langle p\rangle$, a cyclic basis of it, the right member of this equation known as the p-adic expansion of x. Also by the division algorithm in integer normed euclidean $\mathbb{N}$-algebras, for $N \in \mathbb{Z}$ and n there exist unique $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ such that $N = nq + r$ and $0 \leq \deg_{\mathbb{Z}} r < \deg_{\mathbb{Z}} n$, that is, $0 \leq r < n$, then

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

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

$$g_0 = \sum_{k=0}^{r} a_{nq+k} p^k$$

and

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

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

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

and write

$$r_0 = g_0 - y_0^n$$

and

$$d_0 = p^n r_0 + g_1.$$

Afterwards find

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

and write

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

and

$$d_1 = p^n r_1 + g_2.$$

At the i-th step find

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

and write

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

and

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

Finally the n-th root z of x is

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

Time complexity of the algorithm

The n-th root algorithm is of polynomial time complexity because in every completion $\mathcal{R}$ of the fraction semifield of a normed euclidean $\mathbb{N}$-semialgebra, for every natural $n > 1$, for an input nonzero element of length ν in terms of its p-adic expansion for a nonunit of nonzero degree element p of the normed euclidean $\mathbb{N}$-semialgebra, since both the n-th root is an isomorphism between the positive multiplicative group and the real additive group and by the division algorithm in normed euclidean $\mathbb{N}$-semialgebras, for $\nu - 1 \in \mathbb{N}$ and n, there exist unique $m \in \mathbb{N}$ and $\rho \in \mathbb{N}$ such that $\nu = nm + \rho$ and $1 \leq \rho < n + 1$, the output its n-th root is of length $m + 1 = O(m)$ in terms of its p-adic expansion if it is finite as is the number of steps in which it is calculated, at the i-th of which after writing $O(m)$ elements of length $O(1)$, so in time $O(m)$, for $n \geq 3$ the n-th root algorithm compares and writes $O(1)$ elements calculated in time $O(m^3)$, thereby of length $O(m^3)$, so also in time $O(m^3)$, as does the squared root algorithm in time $O(m^2)$, therefore, since $O(m^k) = O(\nu^k)$, the time complexity of the n-th root algorithm, for $n = 2$, is $T(n) = O(n^2)$, and, for $n \geq 3$, $T(n) = O(n^3)$.

A theorem of the theory of complete $\mathbb{N}$-semialgebras

The n-th root algorithm is a consequence of both the division algorithm in the theory of completions of fraction semifields of normed euclidean $\mathbb{N}$-semialgebras and of a corollary of the binomial theorem in the theory of semirings that states in every semiring $\mathcal{R}$, for every $n \in \mathbb{N}$, $m \in \mathbb{N}$ and $x_0, x_1, \ldots, x_m \in \mathcal{R}$,

$$(x_0 + x_1 + \cdots + x_m)^n = \sum_{i=0}^{\infty} \binom{n}{i} (\sum_{k=0}^{m-1} x_k)^{n-i} {x_m}^i$$

Thus the existence of the n-th root algorithm in completions of fraction semifields of normed euclidean $\mathbb{N}$-semialgebras is in accordance not only with the completeness of the theory of semirings and with the completeness of the theory of semifields but also with the incompleteness of the theory of complete $\mathbb{N}$-semialgebras.

This paper is dedicated to my mother Susana Grau Avila