The n-th root algorithm

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

In this paper we give the n-th root algorithm on topologically completed semirings with division. The algorithm starts with a nonzero semiring element in terms of its p-adic expansion for any semiring nonzero element p, thereafter for a nonzero natural number m, calculates and writes $O(m)$ semiring elements of length $O(1)$ to go through $O(m)$ steps in each of which compares, calculates and writes $O(1)$ semiring elements of length $O(m^k)$ for some natural number k.

Let $\mathcal{R}$ be a topologically completed semiring with division with the Zariski topology $\mathcal{F}$, $\mathbb{N}_{\mathcal{R}} \subset \mathcal{R}$ be the topologically completed subsemiring with division of $\mathcal{R}$ isomorphic to the natural topologically completed semiring with division $\mathbb{N}$, $x \in \mathcal{R}$ such that $x \neq 0_{\mathcal{R}}$, $p \in \mathcal{R}$ such that $p \neq 0_{\mathcal{R}}$, $\mathbb{R}^+$ be the positive locally compact multiplicative group, $n \in \mathbb{R}^+$, $\mathbb{R}^+ \cup \{0\}[x]$ be the topologically completed semiring with division of polynomials of one variable in $\mathcal{R}$ over the positive topologically completed semiring with division $\mathbb{R}^+ \cup \{0\}$, and $\mathcal{B}$ be the basis of the Zariski topology $\mathcal{F}$, 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 $f \in \mathbb{R}^+ \cup \{0\}[x]$ such that $f(s) = 0_{\mathcal{R}}$, $F_s = \mathrm{Var}(f)$ and $F = F_s$.

By the division algorithm on topologically completed semirings with division for x and p there exist unique $N \in \mathbb{Z}$ and $a_1, a_2, \ldots \in \mathbb{N}_{\mathcal{R}}$ such that

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

and $a_N \neq 0_{\mathcal{R}}$. Also by the division algorithm on topologically completed rings with division for $N \in \mathbb{Z} \subset \mathbb{R}$ and n there exist unique integer q and positive r such that $N = nq + r$ and either $0 \leq \deg_{\mathbb{R}} r < \deg_{\mathbb{R}} n^{-1}$ if $\deg_{\mathbb{R}} n < 1$ or $0 \leq \deg_{\mathbb{R}} r < \deg_{\mathbb{R}} n$ if $\deg_{\mathbb{R}} n > 1$, that is either $0 \leq r < n^{-1}$ if $n < 1$ or $0 \leq r < n$ if $n > 1$, then

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

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

$$g_0 = a_{nq+r} p^{nq+r} + \sum_{\substack{k \in \mathbb{N} \\ 0 \leq k < r}} a_{nq+k} p^k$$

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

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

and write

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

and

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

At the i-th step find

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

and write

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

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 for every $n \in \mathbb{R}^+$ because for a topologically completed semiring with division input nonzero element of length ν in terms of its p-adic expansion for any nonzero semiring element p, since both the n-th root is an isomorphism between the multiplicative positive group and the additive real group and by the division algorithm on topologically completed semirings with division for $\nu - 1 \in \mathbb{N} \subset \mathbb{R}^+ \cup \{0\}$ and $n \in \mathbb{R}^+ \subset \mathbb{R}^+ \cup \{0\}$ there exist unique $m \in \mathbb{N}$ and $\rho \in \mathbb{R}^+ \cup \{0\}$ such that $\nu = nm + \rho$ and either $1 \leq \rho < n^{-1} + 1$ if $n < 1$ or $1 \leq \rho < n + 1$ if $n > 1$, 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 $O(m)$ semiring elements of length $O(1)$ so in time $O(m)$ the algorithm compares and writes $O(1)$ semiring elements calculated in time $O(m^k)$ thereby of length $O(m^k)$ so also in time $O(m^k)$ where $k = 1$ if $n = 1$, $k = 2$ if $n = 2$, $k = 3$ if $n \in \mathbb{N}\backslash\{0, 1, 2\}$ and $k = 4$ for every noninteger value of n, therefore since $O(m^k) = O(\nu^k)$, the time complexity of the n-th root algorithm for $n = 1$, $n = 2$, integer values of n greater than 2, and noninteger values of n is $T(n) = O(n)$, $T(n) = O(n^2)$, $T(n) = O(n^3)$ and $T(n^4) = O(n^4)$, respectively.

A theorem of the theory of topologically completed semirings with division

The n-th root algorithm is a consequence of both the division algorithm on the theory of topologically completed semirings with division and of a corollary of the binomial theorem on the theory of topologically completed semirings that states for every topologically completed semiring $\mathcal{R}$ with division, $n \in \mathbb{R}^+ \subset \mathbb{R}$, $m \in \mathbb{N}$, $x_0, x_1, \ldots, x_m \in \mathcal{R}$,

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

Thus the existence of the n-th root algorithm on topologically completed semirings with division for every positive n is in accordance neither with the incompleteness of the theory of topologically completed groups, nor with the incompleteness of the theory of topologically completed semirings, but with the incompleteness of the theory of topologically completed semirings with division.