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. 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, $x \in \mathcal{R}$ such that $x \neq 0$, $p \in \mathcal{R}$ such that $p \neq 0$ and $n \in \mathbb{R}^+$, by the division algorithm on topologically completed semirings there exist unique $N \in \mathbb{Z}$ and $a_1, a_2, ... \in \{0\} \cup (\mathbb{N} \cap (p^{-1}, p))$ such that $x = \sum_{i=0}^{\infty} a_{N-i} p^{N-i}$ and $a_N \neq 0$. Also by the division algorithm on topologically completed rings for $N \in \mathbb{Z} \subset \mathbb{R}$ there exist unique integer q and positive r such that $N = nq + r$ and $0 \leq \deg_{\mathbb{R}} r < \deg_{\mathbb{R}} n$, 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 $g_0, g_1 ... \in \mathcal{R}$ 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 each i such that $i > 0$.
At the first step find

$$y_0 = \max\{y \in \{0\} \cup (\mathbb{N} \cap (p^{-1}, p)) : y^n \leq g_0\}$$

and write

$$r_0 = g_0 - y_0^n$$

and

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

Afterwards find

$$y_1 = \max\{y \in \{0\} \cup (\mathbb{N} \cap (p^{-1}, p)) : \sum_{j=1}^{\infty} \binom{n}{j} (py_0)^j y^{n-j} \leq d_0\}$$

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

$$y_i = \max\{y \in \{0\} \cup (\mathbb{N} \cap (p^{-1}, p)) : \sum_{j=1}^{\infty} \binom{n}{j} (\sum_{k=0}^{i-1} p^{i-k} y_k)^j y^{n-j} \leq d_{i-1}\}$$

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 because for an input nonzero semiring element of length ν in terms of its p-adic expansion for any nonzero semiring element p, since the n-th root is an isomorphism between the multiplicative positive group and the additive real group for every $n \in \mathbb{R}^+$ and by the division algorithm on topologically completed semirings 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 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 $k = 1$ for $n = 1$, $k = 2$ for $n = 2$, $k = 3$ for $n \in \mathbb{N} \backslash \{0, 1, 2\}$ 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 is $T(n) = O(n)$ for $n = 1$, $T(n) = O(n^2)$ for $n = 2$, $T(n) = O(n^3)$ for integer values of n greater than 2, and $T(n) = O(n^4)$ for noninteger values of n.

The algorithm as a theorem of the theory of semirings

The algorithm is a consequence of the binomial theorem on the theory of topologically completed semirings that for every topologically completed semiring $\mathcal{R}$, and every $x_1, x_2, ..., x_m \in \mathcal{R}$, $a_1, a_2, ..., a_m \in \mathbb{R}^+ \cup \{0\}$, $n \in \mathbb{R}^+$ and $m \in \mathbb{N}$ such that $m \neq 0$,

$$(a_1 x_1 + a_2 x_2 + \cdots + a_m x_m)^n = a_1^n x_1^n + \sum_{j=2}^{m} \sum_{i=1}^{\infty} \binom{n}{i} (\sum_{k=1}^{j-1} a_k x_k)^{n-i} (a_j x_j)^i$$

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