ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Ultrametric versus Archimedean automata

Rūsiņš Freivalds

(University of Latvia)

European Social Fund project Nr. 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Pascal and Fermat believed that every event of indeterminism can be described by a real number between 0 and 1 called *probability*. Quantum physics introduced a description in terms of complex numbers called *amplitude of probabilities* and later in terms of probabilistic combinations of amplitudes most conveniently described by *density matrices*.

String theory , chemistry and molecular biology have used p-adic numbers to describe measures of indeterminism.

We consider a new type of indeterministic algorithms called *ultrametric* algorithms. They are very similar to probabilistic algorithms but while probabilistic algorithms use real numbers r with $0 \leq r \leq 1$ as parameters, ultrametric algorithms use *p-adic* numbers as the parameters. Slightly simplifying the description of the definitions one can say that ultrametric algorithms are the same probabilistic algorithms, only the interpretation of the probabilities is different.

However, p-adic numbers is not merely one of generalizations of rational numbers. They are related to the notion of *absolute value* of numbers.

If X is a nonempty set, a distance, or metric, on X is a function d from pairs of elements (x, y) of X to the nonnegative real numbers such that

1. $d(x, y) = 0$ if and only if $x = y$,
2. $d(x, y) = d(y, x)$,
3. $d(x, y) \leq d(x, z) + d(z, y)$ for all $z \in X$.

Absolute value of rational number x is called *trivial* if it equals 0 for the number 0, and eqals 1 for all the other numbers.

For a prime number p, the p-adic absolute value on Q is defined as follows: any non-zero rational x, can be written uniquely as $x = p^n \frac{a}{b}$ with a, b and p pairwise coprime and $n \in \mathbb{Z}$ some integer; so we define

$$|x|_p := \begin{cases} 0, & \text{if } x = 0 \\ p^{-n}, & \text{if } x \neq 0. \end{cases}$$

In 1916 Alexander Ostrowski proved that any non-trivial absolute value on the rational numbers Q is equivalent to either the usual real absolute value or a p-adic absolute value for some prime number p.

A. Ostrowski's theorem shows that using p-adic numbers is not merely one of many possibilities to generalize the definition of deterministic algorithms but rather the only remaining possibility not yet explored.

The *norm* of an element $x \in X$ is the distance from 0:

1. $\| x \| = 0$ if and only if $x = y$,
2. $\| x.y \| = \| x \| . \| xy \|$,
3. $\| x + y \| \leq \| x \| + \| y \|$.

We know one metric on Q induced by the ordinary absolute value. However, there are other norms as well.

A norm is called *ultrametric* if the third requirement can be replaced by the stronger statement: $\| x + y \| \leq \max\{\| x \|, \| y \|\}$. Otherwise, the norm is called *Archimedean*.

Distances using the usual absolute value are called *Archimedean*, and the distances using p-adic absolute values are called *ultrametric*. P.Turakainen proved that probabilistic automata can be generalized using arbitrary real numbers instead of probabilities and the languages recognized by these Archimedean automata are the same stochastic languages.

We generalize probabilistic automata in the same way, only we use arbitrary p-adic numbers numbers instead of probabilities.

There is an important feature that distinguishes p-adic numbers from real numbers. Real numbers (both rational and irrational) are linearly ordered. p-adic numbers cannot be linearly ordered. This is why *valuations* and *norms* of p-adic numbers are considered.

The situation is similar in Quantum Computation. Quantum amplitudes are complex numbers which also cannot be linearly ordered. The counterpart of valuation for quantum algorithms is *measurement* translating a complex number $a+bi$ into a real number a^2+b^2. Norms of p-adic numbers are rational numbers.

Theorem. There is a continuum of languages recognizable by finite ultrametric automata.

Definition. We say that a finite ultrametric automaton is *rational* if all its parameters are rational numbers.

Theorem. The language

$$L = \{x \mid x = x^{\mathrm{rev}} \& (\exists n)(\mid x \mid = 2n + 1 \& x_n = 1\}$$

is not stochastic but for arbitrary prime $p \geq 3$
L is recognizable by a p-ultrametric finite automaton.

Hence we restrict ourselves to consider only ultrametric automata all parameters of which are p-adic integers. However, even such a restriction allows some non-regular languages to be recognizable.

Definition. A finite ultrametric automaton is called **regulated** if there exist constants $c > 0$ and λ such that for arbitrary input word x the norm $\lambda - c < \| \gamma \|_p < \lambda + c$. We say that the word x is accepted if $\| \gamma \|_p > \lambda$ and it is rejected if $\| \gamma \|_p \leq \lambda$.

Theorem. (1) If a language M is recognized by a regulated finite ultrametric automaton then M is regular. (2) For arbitrary prime number p there is a constant c_p such that if a language M is recognized by a regulated finite p-ultrametric automaton with k states then there is a deterministic finite automaton with $(c_p)^{k.\log k}$ states recognizing the language M.

M.O.Rabin proved in 1963 that error-bounded probabilistic automata with k can be simulated by deterministic automata with c^k states.

Helmut Hasse's local-global principle states that certain types of equations have a rational solution if and only if they have a solution in the real numbers and in the p-adic numbers for each prime p.

Suppose, a counterpart of this principle is found for computing functions:

"If a function F can be computed in polynomial time by Quantum Turing machines and by p-ultrametric Turing machines for all primes p, then F can be computed in polynomial time by probabilistic Turing machines as well."

This would solve long standing problems in Quantum Computation without physical implementation of ultrametric Turing machines.

Thank you