Polynomial solution to Discrete Logarithm Problem in interval-valued computing

Benedek Nagy (University of Debrecen)
Sándor Vályi (College of Nyíregyháza)

April 29, 2011

Abstract

We show that discrete logarithm can be computed in the framework of interval-valued computations by a polynomial computation. This new computing device is of highly parallel nature: it operates on so-called interval-values which are finite unions of subintervals of [0,1) and constitute an infinite Boolean algebra. The computation process is modelled in the style of Boolean networks but some non-Boolean operators are also allowed: shifts in both directions and a kind of zooming called product. This paradigm in an restricted form has the computation power of PSPACE as shown in [1] when it is used to decision problems. In [2] it is defined how interval-valued computations can be used to calculate discrete functions. In that paper the prime factorization was shown to be computable by a quadratic size interval-valued computation. The calculation of discrete logarithm also an important topic of cryptography. In this talk, we demonstrate an analogous result for the calculation of discrete logarithm.

Keywords: new computing paradigm, interval-valued computing, parallel computing

References

[1] Nagy, B., Vályi, S., *Interval-valued computations and their connection with PSPACE*, Theoretical Computer Science 394/3 (2008), 208-222.

[2] Nagy, B., Vályi, S., *Prime factorization by interval-valued computing*, NTA 2010 – Conference on Number Theory and its Applications – October 2010, Debrecen, Hungary (submitted to a journal special volume for the proceedings).