November 2011

MADALGO seminars by Raphael Clifford, University of Bristol

Lower bounds for online integer multiplication and convolution in the cell-probe model

Abstract:
We will discuss time lower bounds for both online integer multiplication and convolution in the cell-probe model. For the multiplication problem, one pair of digits, each from one of two *n* digit numbers that are to be multiplied, is given as input at step *i*. The online algorithm outputs a single new digit from the product of the numbers before step *i*+1. We give a lower bound of Omega((*d*/*w*)*log *n*) time on average per output digit for this problem where 2^d is the maximum value of a digit and *w* is the word size. In the convolution problem, we are given a fixed vector *V* of length *n* and we consider a stream in which numbers arrive one at a time. We output the inner product of *V* and the vector that consists of the last *n* numbers of the stream. We show an Omega((*d*/*w*)*log *n*) lower bound for the time required per new number in the stream. All the bounds presented hold under randomization and amortization. These are the first unconditional lower bounds for online multiplication or convolution in this popular model of computation.

Joint work with Elad Verbin