

Equivalence between turing machines and the circuit model of computation

Two theorems to talk about.

1. Razborov complexity of circuits
2. Peter Shor's algorithm for factorizing using a quantum computer

What a Turing machine is, informally.

Tape, string of 0s and 1s.

State: S_i pointing at a place in the tape.

Possible states S_0, \dots, S_k .

What happens at a particular state of the computation.

S_i is a sequence of instructions concerning what the bit on the tape place is and what state and place the machine should be at the next step.

For example, "if place is zero, change it into a one, move to the right by one and change the state of the machine to S_j ; if it is one, stay put and change to state S_h ". Typical instruction of S_i .

A state doesn't know which position the tape is in, it is very local.

To know where it is, the information must be encoded in the state somehow, maybe by writing information on the tape.

Example Turing machine which takes a string of ones and tells whether the number of ones is even or odd.