

# Chipping Away at P vs NP: How Far Are We from Proving Circuit Size Lower Bounds?

Eric Allender

Rutgers, the State University of New Jersey  
Piscataway, New Jersey, USA

Many people are pessimistic about seeing a resolution to the P vs NP question any time soon. This pessimism extends also to questions about other important complexity classes, including two classes that will be the focus of this talk:  $TC^0$  and  $NC^1$ .

$TC^0$  captures the complexity of several important computational problems, such as multiplication, division, and sorting; it consists of all problems computable by constant-depth, polynomial-size families of circuits of MAJORITY gates.  $TC_d^0$  is the subclass of  $TC^0$  solvable with circuits of depth  $d$ . Although  $TC^0$  seems to be a small subclass of P, it is still open if  $NP = TC_3^0$ .

$NC^1$  is the class of problems expressible by Boolean formulae of polynomial size.  $NC^1$  contains  $TC^0$ , and captures the complexity of evaluating a Boolean formula.

Any proof that NP is not equal to  $TC^0$  will have to overcome the obstacles identified by Razborov and Rudich in their paper on “Natural Proofs”. That is, a “natural” proof that NP is not equal to  $TC^0$  yields a proof that no pseudorandom function generator is computable in  $TC^0$ . This is problematic, since some popular cryptographic conjectures imply that such generators do exist. This leads to pessimism about the even more difficult task of separating  $NC^1$  from  $TC^0$ .

Some limited lower bounds are within the grasp of current techniques, however. For example, several problems in P are known to require formulae of quadratic size — but this seems to be of little use in trying to prove superpolynomial formula size. Along similar lines, it is known that, for every  $d$ , there is a constant  $c > 1$  such that the formula evaluation problem (one of the standard complete problems for  $NC^1$ ) requires  $TC_d^0$  circuits of size at least  $n^c$ .

It might not seem too outrageous to hope to obtain a slightly stronger lower bound, showing that there is a  $c > 1$  such that this same set requires uniform  $TC^0$  circuits of size  $n^c$  (regardless of the depth  $d$ ). We show that this would be sufficient to prove that  $TC^0$  is properly contained in  $NC^1$ .

This is joint work with Michal Koucký, Czech Academy of Sciences, Prague.