A Novel Algorithm for #SAT

Gorokhovsky, Elliot

An exact algorithm for counting the models of Boolean formulas in CNF (the #SAT problem) was developed. Unlike conventional backtracking-based approaches which measure the effect of incrementally setting the literals of the formula true or false, the algorithm instead counts the number of unique models that falsify each clause of the formula and removes duplicates by recursively solving smaller and smaller instances. Additionally, the algorithm can be memoized so that, for many instances, its runtime depends mainly on how the formula is ordered instead of the number of variables or clauses. This makes possible an interesting backdoor approach to #SAT focusing on preprocessing and clustering instead of counting. Since #SAT is a #P-complete problem, all the problems in NP reduce to it, as well as all the problems in #P and search problems that can be reduced to NP decision problems. This means that an efficient algorithm, even one that takes exponential time in the worst case, would have profound theoretical repercussions as well as immense practical applications, most realistically in cryptography and formal verification. The algorithm developed shows promise for future development and extension, both as an independent approach and a complement to traditional techniques.

Awards Won:

First Award of $5,000

National Security Agency Research Directorate : Second Life Science Award of $1,000