Complexity of Circuit Satisfiability

R. Paturi and P. Pudlák

November 16, 2009

definitions

- *Description length* of a circuit of size s is $m = s \log s$.
- **CircuitSat**(n, m) is the (parameterized) problem:
  for a given circuit with description length m and n input variables to decide if it is satisfiable.
- *One-sided error probabilistic circuit C (Turing machine M)* for **CircuitSat**:
  for a given string encoding a circuit D, if C (respectively, M) accepts, then D is satisfiable.
- The *success probability* of a probabilistic circuit C (Turing machine T) is the probability that it accepts every satisfiable D.
- It is possible to generalize our results to $\mathbf{NP}(n, m)$, where m is the input size and n is the number of nondeterministic bits needed to specify the instance.

motivation, examples

- polynomial time probabilistic algorithms for **k-CNF-SAT** with success probability $2^{-(1-\frac{c}{k})n}$, [PPZ], [Schoening];
- slightly superpolynomial [PPSZ];
- polynomial time probabilistic algorithms for **CNF-SAT** with success probability $2^{-(1-\frac{1}{\log m})n}$, [Schuler].

Conjecture
No probabilistic polynomial time algorithm for **CircuitSat** achieves the success probability $2^{-\delta n}$ for any $\delta < 1$.

results: probabilistic polynomial time

Theorem

If **CircuitSat**(n, m) *can be decided with probabilistic circuits of size* $m^{O(1)}$ *with success probability* $2^{-\delta n}$ *for* $\delta < 1$*, then there exists a* $\mu < 1$ *such that* **CircuitSat**(n, m) *can be decided by deterministic circuits of size* $2^{O(n^{\mu} \log^{1-\mu} m)}$.

The consequence amounts to $2^{n^{\mu}}$, $\mu < 1$, size deterministic circuits for **CircuitSat**$(n, n^{O(1)})$.

uniform version

Theorem

If **CircuitSat**(n, m) *can be decided by a probabilistic Turing machine running in time* $m^{O(1)}$ *with success probability* $2^{-\delta n}$ *for* $\delta < 1$, *then* $W[P] = FPT$.

result: quasilinear time

Theorem

If **CircuitSat**(n, m) *can be decided with probabilistic circuits of size* $m(\log m)^{O(1)}$ *with success probability* $2^{-\delta n}$ *for* $\delta < 1$, *then* **CircuitSat**(n, m) *can be decided by deterministic circuits of size* $m^{O(1)} n^{O(\log \log m)}$.

We can weaken the assumption to $\delta = 1 - \varepsilon / \log n$, for $\varepsilon > 0$.

result: subexponential in n and quasilinear in m

Theorem

If **CircuitSat**(n, m) *can be decided with probabilistic circuits of size* $2^{o(n)} m(\log m)^{O(1)}$ *with success probability* $2^{-\delta n}$ *for* $\delta < 1$, *then* **CircuitSat**(n, m) *can be decided by deterministic circuits of size* $2^{o(n)} m^{O(1)}$.

Thank You