What One Has to Know when Attacking P vs. NP

Juraj Hromkovič and Peter Rossmanith

September 12, 2017 – FCT 2017

Main Results

Theorem [Chaitin, JACM 1974]

There exists $d \in \mathbb{N}$ such that, for all $n \geq d$ and all $x \in \{0,1\}^*$, there does not exist any proof in AV-mathematics of the fact "$K(x) \geq n$".

Main Results

Theorem

There exists a program P that does not halt on λ, and there is no proof in AV-mathematics of this fact.

Main Results

Theorem

There exist infinitely many TMs (programs) A that do not halt on λ, and such that there is no proof in AV-mathematics for any of them that A does not halt on λ.

Main Results

Rice's Theorem on Unprovability

For each semantically nontrivial decision problem $\mathcal{A}$, there exist infinitely many TMs M' such that there is no proof of "$c(M') \in \mathcal{A}$" and no proof of "$c(M') \notin \mathcal{A}$", that is, one cannot investigate in AV-mathematics whether $c(M')$ is in $\mathcal{A}$ or not.

Main Results

Theorem

There exist infinitely many algorithms which do not work in polynomial time, but for which this fact is not provable in AV-mathematics. Similarly, there exist infinitely many algorithms which work in polynomial time, but for which this fact is not provable in AV-mathematics.

Main Results

Theorem

There are infinitely many algorithms for which it is not provable in AV-mathematics that they do not solve SATISFIABILITY.

Main Results

Theorem

If P = NP, then there exist infinitely many algorithms X for which one cannot prove or disprove in AV-mathematics the statement "X solves SATISFIABILITY in polynomial time".

Main Results

Theorem

If multiplication of two decimal numbers is feasible in linear time, then there exist infinitely many algorithms X, for which one cannot decide in AV-mathematics whether "X solves multiplication in linear time", or "X does not solve multiplication or does not work in linear time".

Main Results

Theorem

There exists an algorithm X_1, for which it is neither provable whether X_1 recognizes SATISFIABILITY nor provable whether X_1 works in polynomial time.

Main Results

Theorem

If the claim "P = NP" ("NLOG = DLOG") is not provable in AV-mathematics, then

$$P_{ver} \neq NP_{ver}$$

$$(DLOG_{ver} \neq NLOG_{ver})$$

Main Results

Theorem

If P = NP, then Algorithm S solves SATISFIABILITY, runs in polynomial time, returns “no” on all no-instances, and returns a satisfying assignment on all but finitely many yes-instances.

Main Results

Theorem

There is a concrete deterministic logspace-bounded algorithm that solves graph reachability iff LOGSPACE = NLOGSPACE.

Main Results

Theorem

If graph isomorphism is in P, then for every $\epsilon > 0$, there exists an algorithm that solves graph isomorphism and has the following properties:

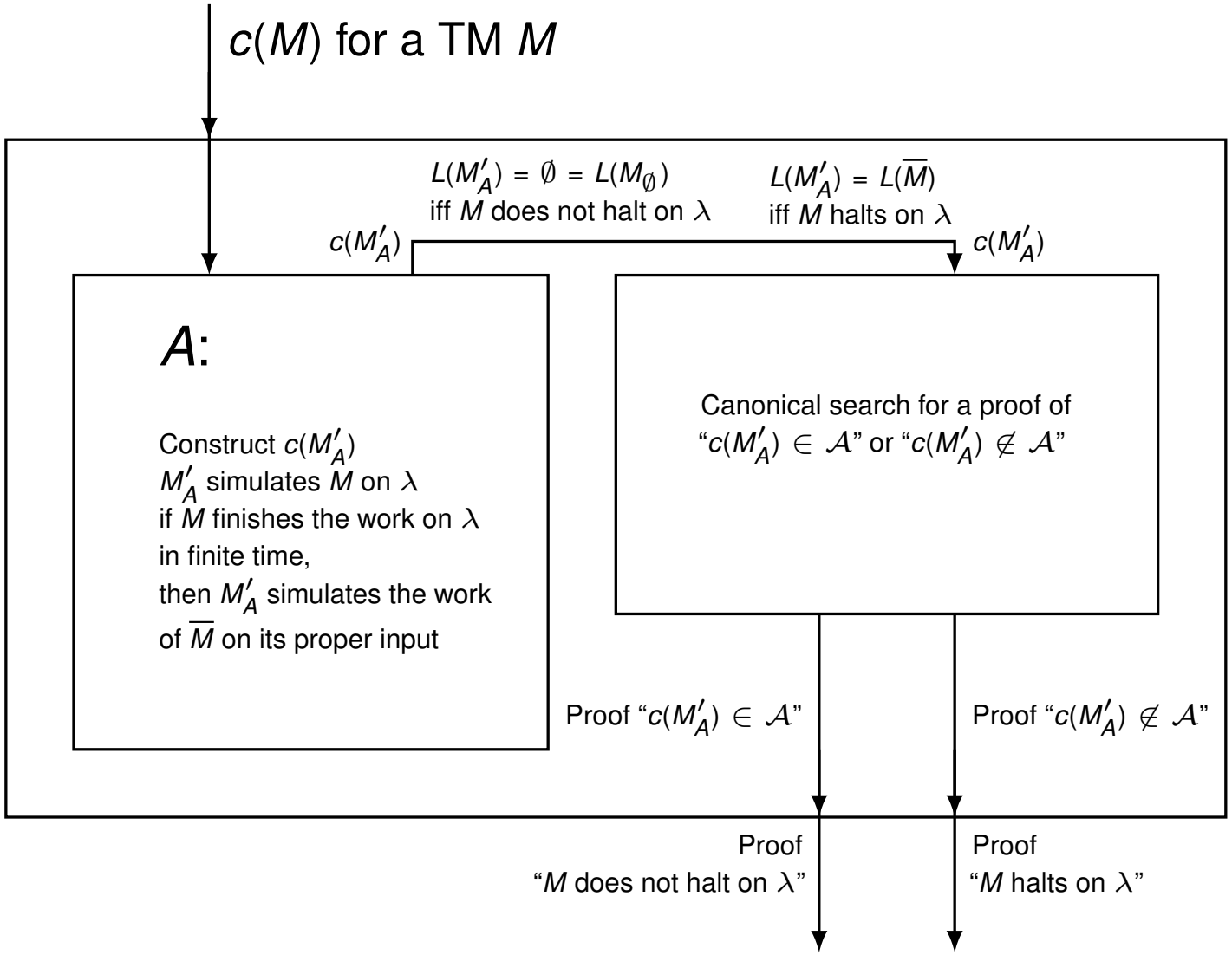
1. It is a randomized algorithm.
2. It runs in expected polynomial time.
3. For all but finitely many yes-instances, it always answers correctly.
4. For the remaining yes-instances, the answer is correct with probability at least $1 - 2^{n^2}$.
5. For all no-instances, it always answers correctly.

Main Results

Theorem

There exists a concrete randomized algorithm that solves QBF in expected polynomial time with error probability at most $1/3$ iff BPP = PSPACE.

Appendix – "Rice's Theorem on Unprovability"



Thanks for your attention