Lehrstuhl für Automatentheorie
Institut für Theoretische Informatik, TU Dresden
Prof. Dr. F. Baader

Nöthnitzer Str. 46
01187 Dresden
Tel.: 0351/463–38237
Tel.: 0351/463–39171

11. Exercises for the Course „Complexity and Logic“

Exercise 46:

Integer factorization is the following problem: given two numbers n, m in binary, decide whether there is a factor k of m with $k \leq n$. Prove that integer factorization is in NP $\cap$ co-NP.

Hint: you may use the recent (and celebrated) result that testing whether a number is prime is in P.

Show that if integer factorization is in P, then a factorization of a given integer can be computed in polynomial time.

Exercise 47:

Let Φ, Ψ be sets of propositional formulas with $\Phi \subseteq \Psi$. We write $\mathsf{sig}(\Phi)$ to denote the set of propositional letters used in Φ, and similarly for Ψ and propositional formulas φ.

We call Ψ a *conservative extension* of Φ if for all propositional formulas φ with $\mathsf{sig}(\varphi) \subseteq \mathsf{sig}(\Phi)$, we have that $\Psi \models \varphi$ implies $\Phi \models \varphi$. Show the following:

(a) Φ is a conservative extension of Ψ iff

$$\{M|_{\mathsf{sig}(\Phi)} \mid M \text{ is a model of } \Phi\} \subseteq \{M|_{\mathsf{sig}(\Phi)} \mid M \text{ is a model of } \Psi\}$$

where $M|_{\mathsf{sig}(\Phi)}$ denotes the restriction of M to the variables in $\mathsf{sig}(\Phi)$.

(b) given sets of propositional formulas Φ, Ψ with $\Phi \subseteq \Psi$, its is Π_2^p-complete to decide whether Ψ is a conservative extension of Φ.