Martin Ziegler

Ausgabe am 12.1.2011
Abzugeben am 19.1.2011 11h40

Komplexitätstheorie

WS 2010/2011, Aufgabenzettel #10

AUFGABE 26:
Seien $\Gamma \subseteq \{0,1\}^k$ und $Q \subseteq \{0,1\}^\ell$ sowie $\delta : \Gamma \times Q \mapsto \Gamma \times Q \times \{00,01,10\}$.

a) Beschreiben Sie einen Schaltkreis C_δ, der δ berechnet.

b) Sei $\mathcal{M} = (Q, \Sigma, \Gamma, \delta)$ eine DTM und $s \in \mathbb{N}$. Beschreiben Sie einen Schaltkreis $C'_{\delta,s}$, der folgende Funktionalität realisiert:
Seine Eingabe besteht aus der Kodierung einer Konfiguration von $\mathcal{M}$, bestehend aus Zustand und dem Bandinhalt (Länge $\leq s$), wobei jede Zelle zustätzlich zu ihrem Inhalt ein Bit als Indikator besitzt, ob der Kopf gerade auf ihr steht. Die Ausgabe von $C'_{\delta,s}$ gibt dann die Konfiguration von $\mathcal{M}$ einen Schritt später an, also den neuen Zustand und den neuen Bandinhalt mit aktualisiertem Indikator für die Kopfposition.
Wie groß und wie tief ist $C'_{\delta,s}$ in Abhängigkeit von s?

c) Sei $n \in \mathbb{N}$, $s \geq S_\mathcal{M}(n)$ und $t \geq T_\mathcal{M}(n)$. Beschreiben Sie einen Schaltkreis $C'_{\mathcal{M},s,t}$, der $\mathcal{M}$ auf allen Eingaben der Länge n simuliert.
Wie groß und wie tief ist $C'_{\delta,s,t}$ in Abhängigkeit von s und t?

d) Zeigen Sie: Eine polynomialzeitbeschränkte DTM $\mathcal{M}$ kann durch eine uniforme Familie von Schaltkreisen simuliert werden. Genauer: CIRCUITVAL is $\mathcal{P}$-hart.

AUFGABE 27:

a) Installieren Sie das *public-key* System `pgp` auf Ihrem Computer; freie Versionen sind beispielsweise von `GNU` für LINUX, WINDOWS und MACOS X erhältlich.
(Sofern Sie Rechner des Mathematik-Pools verwenden, können Sie diesen Aufgabenteil überspringen und das dort installierte `gpg` verwenden.)

b) Machen Sie sich mit der Verwendung der unter a) installierten Software vertraut; beispielsweise durch Lesen der Anleitung (RTFM).

c) Erstellen Sie ein Schlüsselpaar.
Denken Sie darüber nach, wo und wie Sie den privaten Teil speichern!
Machen Sie den öffentlichen Teil zugänglich: auf Ihrer Homepage und/oder einem sog. *key-server* wie beispielsweise `http://wwwkeys.de.pgp.net/`
Bringen Sie am 19.1.2011 jeweils 10 Ausdrucke des sog. *fingerprints* (einer Art Kurzfassung des öffentlichen Schlüssels) mit.

d) Schicken Sie mir eine Email beliebigen (warum nicht vorgegebenen?) Inhalts, die Sie mit meinem[†] öffentlichen Schlüssel kodieren und mit Ihrem privatem 'signieren'.

[†] erhältlich bspw. unter `http://www.mathematik.tu-darmstadt.de/~ziegler/public.key`, fingerprint: `AF37 ECD4 AEBE 3D4E 76EB 4445 227F 4D27 4A4B E6FE`