TU Dresden, Fakultät Informatik
Daniel Borchmann

Summer Term 2016

Advanced Topics in Complexity Theory

Exercise 9: Details on the Proof of $\mathsf{GNI} \in \mathsf{AM}$

2016-06-21

Exercise 9.1 Let G_1, G_2 be two labeled graphs on n vertices. Define

$$S = \{\, (H, \pi) \mid H \simeq G_1 \text{ or } H \simeq G_2 \text{ and } \pi \in \mathrm{Aut}(H) \,\}.$$

Show

$$\begin{aligned} G_1 \simeq G_2 &\implies |S| = n! \\ G_1 \not\simeq G_2 &\implies |S| = 2n! \end{aligned}$$

Exercise 9.2 Show that a set of functions $\mathcal{H}_{n,k}$ from $\{\, 0, 1 \,\}^n$ to $\{\, 0, 1 \,\}^k$ is pairwise independent if and only if for each $x, x' \in \{\, 0, 1 \,\}^n, x \neq x'$, the random variable

$$h \mapsto (h(x), h(x'))$$

is uniformly distributed when choosing $h \in \mathcal{H}_{n,k}$ uniformly at random.

Exercise 9.3 Show that if $\mathcal{H}_{n,k}$ is a set of pairwise independent hash functions, then for $x \in \{\, 0, 1 \,\}^n$ and $y \in \{\, 0, 1 \,\}^k$ we have

$$\Pr(h(x) = y) = 2^{-k},$$

assuming a uniform distribution on $\mathcal{H}$.

Exercise 9.4 Let $n \in \mathbb{N}$. Define for $a, b \in \mathrm{GF}(2^n)$ the mapping $h_{a,b} \colon \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$ by

$$h_{a,b}(x) = ax + b.$$

Show that

$$\mathcal{H}_{n,n} = \{\, h_{a,b} \mid a, b \in \mathrm{GF}(2^n) \,\}$$

is a set of *efficiently computable* pairwise independent hash functions. Conclude that for every choice of $n, k \in \mathbb{N}$ a set $\mathcal{H}_{n,k}$ of efficiently computable pairwise independent hash functions exists.