AARHUS UNIVERSITET, DATALOGI

Protokolteori - Aflevering 1

Peter Burgaard - 201209175

January 31, 2017

EXERCISE 1: Call a function $f : \mathbf{N} \to \mathbf{R}$ *polynpmial in l* if there exist polynomial p and constant l_0 such that $f(l) \leq p(l)$ for all $l > l_0$. Recall that a function $\epsilon : \mathbf{N} \to \mathbf{R}$ is *negligible in l* if for all polynomials p there exists a constant l_p such that $\epsilon(l) \leq \frac{1}{p(l)}$ for all $l > l_p$.

1) PROVE THAT IF ϵ AND δ ARE NEGLIGIBLE IN l, THE $\epsilon + \delta$ IS NEGLIGIBLE IN l

Let $\mathbb{P}[X]$ be all polynomials.

If ϵ and δ are negligible in l then:

$$\forall p \in \mathbb{P}[X] \forall l > l_p : \epsilon(l) \leq \frac{1}{p(l)}$$
$$\forall p' \in \mathbb{P}[X] \forall l' > l_{p'} : \delta(l') \leq \frac{1}{p'(l')}$$

let

$$l_q = \max\{l_p, l_{p'}\}$$

Since this applies for all polynomials $p \in \mathbb{P}[X]$ defined on l, we'll define one as $l^{(c+1)}$, and we have

$$\forall l > l_q$$
$$\epsilon(l) + \delta(l) \leq 2l^{-(c+1)} \leq l \cdot l^{-(c+1)} = l^{-(c)} = \frac{1}{l^c}$$

Since $l^c \in \mathbb{P}[X]$, and since $\epsilon(l), \delta(l)$ and $\epsilon(l) + \delta(l) \leq \frac{1}{l^c}$ we're done. □

2) PROVE THAT IF ϵ IS NEGLIGIBLE IN l AND f IS POLYNOMIAL IN l, THE $f \cdot \epsilon$ IS NEGLIGIBLE IN l

Assume that there exists a $f \in \mathbb{P}[X]$ such that $\epsilon(l) \cdot f(l) \not\leq \frac{1}{p(l)} \forall p \in \mathbb{P}[X]$, this would imply

$$\epsilon(l) \not\leq \frac{1}{\left(\frac{p(l)}{f(l)}\right)} = \frac{1}{h(l)}$$

which again would mean $h(l) \not\in \mathbb{P}[X]$. Since $\epsilon(l)$ is negligible $\forall p \in \mathbb{P}[X] \forall l > l_p$ ↯

Therefore $\epsilon(l) \cdot f(l) \leq \frac{1}{p(l)}$ and is negligible. □