Kryptographische Algorithmen

Blatt 4 19.05.2004, Abgabe 26.05.2004

Sei $F_n \in_R [n]^{[n]}, x_0, x_0' \in [n], x_{i+1} = F_n(x_i)$, $x'_{i+1} = F_n(x'_i)$ mit $\mu + \lambda, \mu' + \lambda'$ und Funktionsgraph G_n. $x_0 \equiv x_0'$ bedeute $\exists i, i' : x_i = x'_{i'}$. $[x_0]$ bezeichnet die Z.h.–Komponente von x_0.

Aufgabe 1. Zeige:

1. $\mathbf{Ws}[\mu + \lambda \leq \sqrt{\frac{n}{2\pi}}] = O(\frac{1}{\sqrt{n}})$
2. $\mathbf{Ws}[x_0 \not\equiv x_0' \mid \mu + \lambda = k, \mu' + \lambda' = k'] \leq e^{\frac{-kk'}{n}}$.

Hinweis: Benutze Aufgabe 1, Blatt 3.

Aufgabe 2. Zeige mittels Aufgabe 1:

1. $\mathrm{Ws}[x_0 \not\equiv x_0'] \leq e^{-\frac{1}{2\pi}} + O(\frac{1}{\sqrt{n}})$
2. $\mathrm{Ws}[x_0 \equiv x_0'] \geq \gamma$ für eine absolute Konstante $\gamma > 0$ (für $n \geq n_0$).

Aufgabe 3. Zeige: $\mathbf{E}[|[x_0]|] \geq \gamma\, n$.

Aufgabe 4. Zeige für beliebige $k \in \mathbf{N}$:

$$\mathbf{Ws}[|[x_0']| \geq k/\gamma \mid x_0 \not\equiv x_0',\ |[x_0]| \geq \gamma n] \leq e^{-k}.$$

(Damit gibt es in G_n neben der Giant–Komponente im Mittel nur Komponenten mit $O(1)$ Knoten.)