Prof. C. P. Schnorr Sommersemester 2004

Kryptographische Algorithmen

Blatt 2, 28.04.2004, Abgabe 05.05.2004

Aufgabe 1. Sei $F_n : [n] \to [n]$ Zufallsfunktion, $F_n \in_R [n]^{[n]}$. Zeige:

1. $\lim_{n\to\infty} \mathbf{E}[\,|F_n([n])|\,] = n - n/e$,
2. $|F_n^{(k)}([n])| \geq \sum$ der Perioden λ des Funktionsgraphen von F_n.

Hinweis: Nach [MOV, 96] Fact 2.3.4 (iv) gilt

$$\lim_{n\to\infty} \mathbf{E}[\,|F_n^{(k)}([n])|\,] = (1-\tau_k)n \text{ mit } \tau_0 = 0,\ \tau_k = e^{-1+\tau_{k-1}},$$

also $(1-\tau_2) = (1-e^{-1+e^{-1}}) \approx 0.4854 > (1-e^{-1})^2 \approx 0.39957$.

Aufgabe 2. Sei $n' := |F_n([n])|$, $\sigma : [n'] \to F_n([n])$ bijektiv. Zeige:

1. $\{\sigma^{-1}F_n\sigma \in [n']^{[n']}\sigma \,|\, F_n \in [n]^{[n]}\} = \{F_{n'} \in [n']^{[n']} \,|\, n - n' \geq n' - |F_{n'}([n'])|\}$.
2. Für $E_k := \lim_{n\to\infty} \mathbf{E}[\,|F_n^{(k)}([n])|\,]$ gilt
   $E_{k-1} - E_k \leq E_{k-2} - E_{k-1} \leq E_0 - E_1 = e^{-1}$ für $k \geq 2$.

Aufgabe 3. Zeige für $\varepsilon_k := 1 - \tau_k = e^{-1+e^{-1+e^{-1+\cdots}}}$ $\Big\}$ k-mal:

1. $\varepsilon_{k+1} = 1 - e^{-\varepsilon_k} = \varepsilon_k - \varepsilon_k^2/2 + \varepsilon_k^3/6 - \varepsilon_k^4/24 + \cdots$
2. $\lim_{k\to\infty} \varepsilon_k = 0$, $\lim_{k\to\infty} \tau_k = 1$.

Aufgabe 4. Konstruiere die Funktionsgraphen der Abbildungen $F_{13}(x) = x^2 + 1 \bmod 13$ und $F_{17}(x) = x^2 + 1 \bmod 17$. Zerlege $n = 221$ mit dem ρ-Algorithmus und Anfangswerten $x_0 = 0, 3, 5$. Erläutere das Zerlegen von 221 an den Funktionsgraphen.