PROF. C. P. SCHNORR Sommersemester 2004

Kryptographische Algorithmen

Blatt 1, 21.04.2004, Abgabe 28.04.2004

Aufgabe 1. Die Algorithmen von Floyd bzw. Brent bestimmen das kleinste n mit $x_n = x_{2n}$, $n \geq \mu$ bzw. $x_n = x_{\ell(n)-1}$, $\ell(n) - 1 \geq \mu$,
$\ell(n) =_{\text{def}} \max\{2^i \mid 2^i \leq n\}$.

Formuliere Brent's Alg. und zeige folgende Laufzeit-Schranken

$$\text{Floyd}: \ 3(\mu+\lambda), \qquad \text{Brent}: \ 2^{\lceil \lg \max(\mu+1,\lambda)\rceil} - 1 + \lambda \leq 2\max(\mu+1,\lambda) + \lambda.$$

Hinweis. Knuth, Exercises 3.1.6, 3.1.7.

Aufgabe 2. Woodruff's Alg. zum Perioden-Finden benützt eine Zerlegung von D in $k \geq 2$ zufällige Klassen $[\nu] \subset D$, $\nu = 0, ..., k-1$ der Grösse $|D|/k$ und speichert für jedes ν ein (x_i, i) mit $x_i \in [\nu]$ in der Liste S.

Schritt j: Bestimme die Klasse $[\nu]$ von x_j, $0 \leq \nu < k$, $(x_l, l) := S[\nu]$.

IF $x_l = x_j$ THEN return "$\lambda \mid (j-l)$"

ELSE $S[\nu] := (x_j, j)$ mit Ws. k/i

Zeige 1. Zur Zeit $n \gg k$ ist $S[\nu]$ nahezu gleichverteilt über den $x_i, i \leq n$, der Klasse $[\nu]$.

2. Die Gleichverteilung in 1. liefert mittlere Laufzeit $(\mu+\lambda)(1+\frac{1}{k-1})$.

Aufgabe 3. Chernoff-Schranke

Seien $X_1, \ldots, X_n$ unabh. 0,1-wertige Z.V. mit $\Pr[X_i] = \frac{1}{2}$.
Zeige: $\Pr[\sum_{i=1}^{n} X_i \geq \frac{n}{2} + \varepsilon n] = \Pr[\sum_{i=1}^{n} X_i \leq \frac{n}{2} + \varepsilon n] \leq \exp(-2n\varepsilon^2)$.
Hinweis: Definiere $f(X_1, \ldots, X_n) = (1+2\varepsilon)^{\sum_i X_i}(1-2\varepsilon)^{n-\sum_i X_i}$.
Zeige: $\sum_{i=1}^{n} X_i \geq \frac{n}{2} + \varepsilon n \ \Rightarrow \ f(X_1, \ldots, X_n) \geq \exp(n(2\varepsilon^2 + \frac{4}{3}\varepsilon^4))$ und wende die Markow'sche Ungleichung an auf $X := f(X_1, \ldots, X_n)$. Zeige $E[X] = 1$.

Literatur: Motwani, Raghavan: Randomized Algorithms. Cambridge University Press, 1995, Theorems 4.1, 4.2.