Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Exercise 5

Task 1
Let $f : \{0,1\}^* \to \mathbb{Z}^{2\times 2}$ be the homomorphism defined by

$$f(0) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad f(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Show that the entries of the matrix $f(w)$ are upper bounded by the $(|w|+1)$-th Fibonacci number $F_{|w|+1}$. Furthermore, give an example for a string w, where at least one entry of $f(w)$ takes indeed the value $F_{|w|+1}$.

Task 2
Let $T = 001100$ and $P = 01$. Use the probabilistic algorithm of the lecture to compute the array $\mathrm{MATCH}[1,\ldots,6]$, which encodes the occurrences of the pattern P in the string T.

Task 3
In this task we will consider an alternative class of fingerprint functions. For a word $w = a_1 \ldots a_n \in \{0,1\}^*$ we define

$$h(a_1 \ldots a_n) = \sum_{i=1}^{n} a_i 2^{n-i}.$$

Let $h_p(w) = h(w) \bmod p$ be the *fingerprint* of w with respect to a prime p.

(a) Construct a randomised pattern matching algorithm by using these fingerprint functions.

(b) What is the probability of an invalid match of your algorithm?

Task 4
For a given number $r \geq 1$ and a prime p let $x = (x_0, x_1, \ldots, x_r)$ with $x_i \in \mathbb{F}_p$. Let $h_x : \mathbb{F}_p^{r+1} \to \mathbb{F}_p$ be the function defined by

$$h_x(a) = \sum_{i=0}^{r} a_i x_i \bmod p, \quad a = (a_0, \ldots, a_r).$$

Show that $\mathcal{H} = \{h_x | x_i \in \mathbb{F}_p, 0 \leq i \leq r\}$ is a universal familiy of hash functions.
Is $\mathcal{H}$ also a familiy of pairwise independent hash functions?