Algorithmen in Zellularautomaten
Aufgabenblatt 4

Aufgabe 4.1
Beweisen Sie, dass für alle $n \in \mathbb{N}_+$ und alle $t \in \mathbb{N}_+$ gilt:

$$(x_1 + \cdots + x_n)^t = \sum_{i_1+\cdots+i_n=t} \binom{i_1 + \cdots + i_n}{i_1; \cdots ; i_n} x_1^{i_1} \cdots x_n^{i_n}$$

Lösung 4.1
Induktion über n; der Fall $n = 2$ ist klar.
Induktionsschritt:

$$\begin{aligned}
&(x_1 + \cdots + x_n + x_{n+1})^t \\
&\qquad = ((x_1 + \cdots + x_n) + x_{n+1})^t \\
&\qquad = \sum_{j=0}^{t} \binom{t}{j; t-j} (x_1 + \cdots + x_n)^{t-j} \cdot x_{n+1}^j \\
&\qquad = \sum_{j=0}^{t} \binom{t}{j; t-j} \sum_{i_1+\cdots+i_n=t-j} \binom{i_1 + \cdots + i_n}{i_1; \cdots ; i_n} x_1^{i_1} \cdots x_n^{i_n} x_{n+1}^j \\
&\qquad = \sum_{i_{n+1}=0}^{t} \binom{t}{i_{n+1}; t-i_{n+1}} \sum_{i_1+\cdots+i_n=t-i_{n+1}} \binom{i_1 + \cdots + i_n}{i_1; \cdots ; i_n} x_1^{i_1} \cdots x_n^{i_n} x_{n+1}^{i_{n+1}} \\
&\qquad = \sum_{i_1+\cdots+i_n+i_{n+1}=t} \binom{t}{i_{n+1}; t-i_{n+1}} \binom{i_1 + \cdots + i_n}{i_1; \cdots ; i_n} x_1^{i_1} \cdots x_n^{i_n} x_{n+1}^{i_{n+1}} \\
&\qquad = \sum_{i_1+\cdots+i_n+i_{n+1}=t} \binom{i_1 + \cdots + i_n + i_{n+1}}{i_1; \cdots ; i_n; i_{n+1}} x_1^{i_1} \cdots x_n^{i_n} x_{n+1}^{i_{n+1}}
\end{aligned}$$

Aufgabe 4.2
Das Pascalsche Dreieck enthält die Binomialkoeffizienten. Können Sie etwas Analoges für „Trinomialkoeffizienten“ finden?

Lösung 4.2
`https://en.wikipedia.org/wiki/Pascal's_pyramid`

Aufgabe 4.3
Es sei p eine Primzahl und $i_1 + \cdots + i_n = p$.

a) Beweisen Sie

$$\binom{p}{i_1; \cdots ; i_n} \bmod p = \begin{cases} 1 & \text{falls für ein } j \text{ gilt: } i_j = p \\ 0 & \text{sonst} \end{cases}$$

b) Beweisen Sie, dass in $\mathbb{Z}_p[x_1, \ldots, x_n]$ für alle $k \in \mathbb{N}_+$ gilt:

$$(x_1 + \cdots + x_n)^{p^k} = x_1^{p^k} + \cdots + x_n^{p^k}$$

Lösung 4.3

a) Es gibt zwei Fälle:

(i) Falls ein $i_j = p$ ist, ist

$$\binom{p}{i_1; \cdots ; i_n} = \frac{p!}{p!} = 1$$

(ii) Falls *alle* $i_j < p$ sind, dann steht im Zähler von

$$\binom{p}{i_1; \cdots ; i_n} = \frac{p!}{i_1! \cdots i_n!}$$

der Primfaktor p, aber im Nenner nur Zahlen echt kleiner als p. Also ist der Polynomialkoeffizient ein Vielfaches von p und daher modulo p gleich 0.

b) Beweis durch Induktion über k.

- Ind.anfang: Im Fall $k = 1$ liefert Teilaufgabe a) die wesentliche Zutat.
- Für den Ind.schritt schreibt man

$$\begin{aligned}
(x_1 + \cdots + x_n)^{p^{k+1}} &= \left((x_1 + \cdots + x_n)^{p^k}\right)^p \\
&= \left(x_1^{p^k} + \cdots + x_n^{p^k}\right)^p && \text{nach Ind.vor., Fall } k \\
&= \left(x_1^{p^k}\right)^p + \cdots + \left(x_n^{p^k}\right)^p && \text{nach Ind.vor., Fall } 1 \\
&= x_1^{p^{k+1}} + \cdots + x_n^{p^{k+1}}
\end{aligned}$$