Übungsblatt 5

Aufgabe 18

Sei $\mathcal{C} = (C_n)_{n\in\mathbb{N}}$ eine Schaltkreisfamilie der Tiefe d und Größe s über der Basis $\mathcal{B}_0$ ($\mathcal{B}_1$, bzw. $\mathcal{B}_1(p) := \mathcal{B}_1 \cup \{\mathrm{MOD}_p\}$ für eine Primzahl p). Zeigen Sie, dass es eine äquivalente geschichtete Schaltkreisfamilie $\mathcal{C}'$ der Größe $s^{\mathcal{O}(1)}$ und Tiefe $\mathcal{O}(d)$ über derselben Basis gibt.

Aufgabe 19

Sei $f : \{0,1\}^2 \to \mathbb{Z}_3$ definiert durch $f(x_1, x_2) = (x_1 + 1)^{(x_2+1)}$ mit Arithmetik über $\mathbb{Z}_3$. Bestimmen Sie die Darstellung von f als multilineares Polynom $f(x_1, x_2) = a_0 + a_1x_1 + a_2x_2 + a_3x_1x_2$ mit Koeffizienten $a_i \in \mathbb{Z}_3$.

Aufgabe 20

Sei p prim, $k \geq 1$ und $x_i \in \{0,1\}$ für $i = 1, \dots, n$. Zeigen Sie für die Arithmetik in $\mathbb{Z}_p$:

a) $\mathrm{MOD}_p(x_1, \dots, x_n) = 1 - (\sum_{i=1}^n x_i)^{p-1}$.

b) Es gibt ein Polynom q vom Grad höchstens $(p-1)k$ und eine Menge $D \subseteq \{0,1\}^n$ mit $\|D\| \geq 2^n(1-p^{-k})$, so dass $q(x_1, \dots, x_n) = \bigvee(x_1, \dots, x_n)$ für alle $(x_1, \dots, x_n) \in D$ ist.

c) Es gibt ein Polynom q vom Grad höchstens $(p-1)k$ und eine Menge $D \subseteq \{0,1\}^n$ mit $\|D\| \geq 2^n(1-p^{-k})$, so dass $q(x_1, \dots, x_n) = \bigwedge(x_1, \dots, x_n)$ für alle $(x_1, \dots, x_n) \in D$ ist.

Hinweis: Kleiner Satz von Fermat.

Aufgabe 21

Zeigen Sie, dass für $m \geq 2$ gilt: $\|\{u_1 \cdots u_n \in \{0,1,\dots,m-1\}^n \mid \sum_{i=1}^n u_i \equiv_m 0\}\|/m^n = 1/m$ und $\|\{u_1 \cdots u_n \in \{0,1\}^n \mid \sum_{i=1}^n u_i \equiv_m 0\}\|/2^n \leq 1/2$.

Aufgabe 22

Für $m \geq 1$ und $i = 0, \dots, m-1$ sei

$$\mathrm{MOD}^n_{m,i}(x_1, \dots, x_n) = \begin{cases} 1, & \sum_{j=1}^n x_j \equiv_m i \\ 0, & \text{sonst.} \end{cases}$$

a) Zeigen Sie, dass $\mathrm{MOD}_m \equiv_{cd} \mathrm{MOD}_{m,i}$ für $i = 0, \dots, m-1$ gilt.

b) Zeigen Sie, dass $\mathrm{MOD}_m \leq_{cd} \mathrm{MOD}_s$ gilt, falls m ein Teiler von s ist.

c) Zeigen Sie, dass $\mathrm{MOD}_{p^k} \equiv_{cd} \mathrm{MOD}_p$ gilt, falls p prim ist.