11. Übung **Mathematik für Informatiker III** **WS 11/12**

Klaus Kriegel **Abgabe: 25.01.2012, 12:00 Uhr**

Aufgabe 1: **Kongruenzsysteme** (5 Punkte)

Welche der folgenden Kongruenzsysteme haben eine Lösung und welche nicht. Es reicht aus, die Frage richtig zu beantworten **und** kurz zu begründen - man muss für eine positive Antwort nicht unbedingt eine konkrete Lösung ausrechnen!

$$\begin{array}{llllll} a) & x \equiv 17 \ (\boldsymbol{mod}\ 30) & \text{und} & x \equiv 24 \ (\boldsymbol{mod}\ 49) \\ b) & x \equiv 15 \ (\boldsymbol{mod}\ 30) & \text{und} & x \equiv 15 \ (\boldsymbol{mod}\ 51) \\ c) & x \equiv 17 \ (\boldsymbol{mod}\ 30) & \text{und} & x \equiv 22 \ (\boldsymbol{mod}\ 51) \\ d) & x \equiv 17 \ (\boldsymbol{mod}\ 30) & \text{und} & x \equiv 29 \ (\boldsymbol{mod}\ 51) \end{array}$$

Aufgabe 2: **Minimalabstände** ($2+3+4$ Punkte)

Sei $m = 2^K \geq 8$ eine Zweierpotenz und $A = \{0,1\}^m$ die Menge aller binären m–Tupel. Im Folgenden werden verschiedene Codierungen von A beschrieben, welche die Tupel $\vec{v} = (v_1, v_2, \ldots, v_m) \in A$ durch zusätzliche Paritätsbits ergänzen. Analysieren Sie die Minimalabstände und Informationsraten der so entstandenen Codes.

a) Es werden die Paritätsbits $p_1 = (v_1 + v_2) \bmod 2, \ldots \quad , p_{m-1} = (v_{m-1} + v_m) \bmod 2$ und $p_m = (v_m + v_1) \bmod 2$ hinzugefügt.

b) Es werden die Paritätsbits $p_{i,j}$ für alle $1 \leq i < j \leq m$ hinzugefügt, die jeweils durch $p_{i,j} = (v_i + v_j) \ \bmod 2$ definiert sind.

c) Es werden die Paritätsbits $p_{i,k}$ für alle $1 \leq i \leq m$ und alle $1 \leq k \leq 2$ hinzugefügt, die jeweils durch $p_{i,k} = (v_i + v_{(i+k) \bmod m}) \bmod 2$ definiert sind.

Aufgabe 3: **Hamming–Abstand** ($4+2$ Punkte)

a) Zeigen Sie dass für Q={0,1}, ein beliebiges $n > 1$ und beliebige $\vec{v}, \vec{w} \in Q^n$ mit ungeradem Hamming–Abstand voneinander kein $\vec{u} \in Q^n$ existieren kann, so dass $d_H(\vec{v}, \vec{u}) = d_H(\vec{w}, \vec{u})$.

Hinweis: Versuchen Sie einen indirekten Beweis (mit Kontraposition) und verwenden Sie den folgenden Fakt: Sind A und B zwei endliche Mengen und $C = (A \setminus B) \cup (B \setminus A)$ die symmetrische Differenz der beiden, dann gilt $|C| \equiv (|A| + |B|) \ (\boldsymbol{mod}\ 2)$, d.h. $|C|$ ist genau dann ungerade, wenn $|A|$ und $|B|$ verschiedene Parität haben. Zu einer vollständigen Lösung gehört natürlich auch ein Beweis dieses Fakts.

b) Zeigen Sie dass für Q={0,1,2}, ein beliebiges $n > 1$ und beliebige $\vec{v}, \vec{w} \in Q^n$ immer ein $\vec{u} \in Q^n$ existiert, so dass $d_H(\vec{v}, \vec{u}) = d_H(\vec{w}, \vec{u}) = \left\lceil \frac{d_H(\vec{v}, \vec{w})}{2} \right\rceil$.