SEM3 für MTD und CMS
FHS Hagenberg
1. Übungsblatt für den 9. Oktober 2002

1. Wir codieren jedes Wort $(x_1, x_2, x_3, x_4) \in {\mathbb{Z}_2}^4$ als

$$K((x_1, x_2, x_3, x_4)) := (x_1, x_2, x_3, x_4) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   (a) Begründen Sie, dass sich zwei Elemente im Bildbereich von K stets an mindestens 3 Stellen unterscheiden.

   (b) Zeigen Sie, dass sich jedes Wort in ${\mathbb{Z}_2}^7$ von mindestens einem Wort im Bildbereich von K an höchstens einer Stelle unterscheidet. *Hinweis:* Zählen Sie die Wörter, die sich von den 16 Wörtern im Bildbereich von K an höchstens einer Stelle unterscheiden.

2. Im folgenden Beispiel untersuchen wir, ob das Mitschicken von Kontrollstellen im vorigen Beispiel wirklich einen Sicherheitsgewinn gebracht hat. Wir schicken Binärzeichen durch einen Kanal, der jedes Zeichen mit Wahrscheinlichkeit 0.1 falsch überträgt.

   (a) Berechnen Sie die Wahrscheinlichkeit, dass in einem Wort aus 4 Zeichen kein Fehler auftritt.

   (b) Berechnen Sie die Wahrscheinlichkeit, dass in einem Wort aus 7 Zeichen maximal ein Fehler auftritt.

   In den folgenden Übungsbeispielen geht es darum, Algorithmen für einige häufig auftretende Probleme der Arithmetik zu finden. Implementieren Sie Ihre Algorithmen (etwa in Mathematica); versuchen Sie, möglichst effiziente Algorithmen zu finden!

3. Finden Sie einen Algorithmus für folgendes Problem:

   - Eingabe: Eine natürliche Zahl n.
   - Ausgabe: Die Binärdarstellung $(\alpha_m, \alpha_{m-1}, \ldots, \alpha_0)$ von n.

4. Finden Sie einen Algorithmus für folgendes Problem:

   - Eingabe: Eine natürliche Zahl n.
   - Ausgabe: Die Einerziffer der Binärdarstellung von n.

5. Finden Sie einen Algorithmus für folgendes Problem:

   - Eingabe: Die Binärdarstellung $(\alpha_m, \alpha_{m-1}, \ldots \alpha_0)$ einer natürlichen Zahl n.
   - Ausgabe: n.

6. Finden Sie einen Algorithmus für folgendes Problem:

   - Eingabe: Drei natürliche Zahlen n, m, p;
   - Ausgabe: Der Rest von n^m bei Division durch p.

   Funktioniert Ihr Programm mit $n = 2$, $m = 10^{20}$, $p = 19$?