Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

Wintersemester 2005
Übungsblatt 7
12. Dezember 2005

Diskrete Strukturen

Abgabetermin: 16. Dezember 2005 **vor** *der Vorlesung*

Aufgabe 1

Beim Cyclic Redundancy Check (CRC) wird eine Nachricht $(a_{n-1}, \ldots, a_0)$ von n Bits zusammen mit einer r-Bit-Checksumme $(p_{r-1}, \ldots, p_0)$ übertragen. Sowohl die Nachricht als auch die Checksumme werden als Polynome $a(x) = \sum_{i=0}^{n-1} a_i x^i$ bzw. $p(x) = \sum_{i=0}^{r-1} p_i x^i$ im Ring $\mathbb{Z}_2[x]$ aufgefasst. Die Checksumme wird aus der Nachricht mit Hilfe eines fest vorgegebenen Generatorpolynoms $g(x) \in \mathbb{Z}_2[x]$ mit $grad(g) = r$ wie folgt berechnet:
$p(x)$ ist der Divisionsrest bei Division von $a(x)x^r$ durch $g(x)$, es gilt also

$$a(x)x^r = g(x) \cdot q(x) + p(x) \quad \text{bzw.} \quad a(x)x^r + p(x) = g(x) \cdot q(x)\,,$$

denn wir rechnen in $\mathbb{Z}_2$. Bei Empfang der Nachricht wird überprüft, ob $a(x)x^r + p(x)$ durch $g(x)$ teilbar ist. Falls dies nicht gilt, so ist ein Fehler aufgetreten.

1. Zeigen Sie, dass 1-Bit-Fehler (d. h. ein Bit a_i ist durch $1 - a_i$ ersetzt worden) immer erkannt werden, wenn das Generatorpolynom $g(x) \neq x^r$ ist.

2. Welche Bedingungen muss man an das Generatorpolynom $g(x)$ stellen, damit alle 2-Bit-Fehler erkannt werden?

3. Wir nehmen an, dass $n = 6,\ r = 3$ und $g(x) = x^3 + x^2 + x + 1$. Sie erhalten als Nachricht $a(x) = x^5 + x^2 + x$.

   Überprüfen Sie, ob die Checksumme $p(x) = x$ zur Nachricht passt!
   Welche Fehler könnten aufgetreten sein?

Aufgabe 2

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen. Es sei $i \in \mathbb{C}$ mit $i^2 = -1$ (*imaginäre Einheit*).

1. Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die komplexe Zahl $e^{\frac{2\pi i}{n}}$ eine multiplikative Untergruppe W_n von $\mathbb{C}$ erzeugt, die isomorph ist zu $\mathbb{Z}_n$.

   Stellen Sie W_n in der Gaußschen Zahlenebene dar und machen Sie sich klar, was in Ihrer Darstellung die Multiplikation in W_n bedeutet.

2. Sei $p(x) \in \mathbb{C}[x]$ ein Polynom vom Grad $n-1$ mit den Koeffizienten $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$, d. h.

$$p(x) = P_{\vec{a}}(x)\,.$$

Wir betrachten speziell $n = 8$, $\vec{a} = (1, 1, 1, 1, 1, 1, 1, 1)$ und $\omega = e^{\frac{2\pi i}{8}}$.

Berechnen Sie die Fouriertransformierte

$$\mathcal{F}_{n,\omega}(\vec{a}) = (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1}))$$

auf zwei verschiedene Arten:

i) Durch Ausführung des Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$.

ii) Durch direkte Berechnung unter Ausnutzung der Formel

$$x^n - 1 = (x^{n-1} + \ldots + x^2 + x + 1)(x - 1)\,.$$

3. Durch welche Matrix kann die Fouriertransformation $\mathcal{F}_{8,e^{\frac{2\pi i}{8}}}$ dargestellt werden?

Aufgabe 3

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$. Beachten und nutzen Sie im Folgenden die Isomorphie zwischen $\langle \mathbb{Z}_3[x]/(g), +, \cdot \rangle$ und $\langle \mathbb{Z}_3[x]_{\text{grad}(g)}, +_g, \cdot_g \rangle$, die für alle $g \in R$ durch die Abbildung $[f]_g \to Rem_g(f)$ gegeben ist. Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\text{grad}(g)}$.

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(x^2 + 2x + 1)$.
2. Bestimmen Sie die Spalten der Additions- und Multiplikations-Verknüpfungstafeln zum Element $x + 2 \in \mathbb{Z}_3[x]/(x^2 + 2x + 1)$.
3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft

$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$

4. Ist der Restklassenring $\mathbb{Z}_3[x]/(x^2 + 2x + 1)$ ein Körper? Begründung!

Aufgabe 4

Lösen Sie mit Maple die folgenden Aufgaben.

1. Stellen Sie die rationale Funktion

$$f(x) = \prod_{i \geq 1}^{5} \frac{1}{(x - i)^2}$$

dar als Summe von Brüchen $\frac{A_i}{x-i}$ und $\frac{B_i}{(x-i)^2}$ mit $A_i, B_i \in \mathbb{Z}$.

2. Stellen Sie die rationale Funktion

$$f(x) = \prod_{i \geq 1}^{5} \frac{1}{(x + ix + 1)^2}$$

dar als Summe von Brüchen $\frac{p(x)}{q(x)}$,

(a) wobei p höchstens vom Grad 1, q höchstens vom Grad 2 und die Koeffizienten der Polynome aus $\mathbb{Z}$ seien.

(b) wobei q vom Grad 1 sei. In diesem Fall dürfen die Koeffizienten der Polynome aus $\mathbb{C}$ sein.

Hinweis: Benutzen Sie die Maplefunktion `convert`.