Technische Universität München
Institut für Informatik
Lehrstuhl für Theoretische Informatik und
Grundlagen der Künstlichen Intelligenz
Prof. Dr. Dr. h.c. Wilfried Brauer

Wintersemester 2004/05
Diskrete Strukturen I
Übungsblatt 4
17. November 2004
Sebastian Wernicke

Diskrete Strukturen I

12. Polynomevaluation

a) Berechnen Sie $(3x^3+x^2-4x-5)/(x-2)$. Was ist demnach $(3x^3+x^2-4x-5) \mod (x-2)$?

b) Sei $P(x) = 3x^3 + 4x^2 - 5x + 10$. Evaluieren Sie $P(-1)$ nach dem Hornerschema.

c) Berechnen Sie die Partialbruchzerlegung des auf den komplexen Zahlen definierten Ausdrucks

$$\frac{2x^3 - 13x^2 + 18x - 4}{(x-3)^2(x+2i)(x-2i)}.$$

(Hinweis: Es sei i die Lösung der Gleichung $i^2 = -1$.)

13. Prüfpolynome

Bei der Übertragung von Daten verwendet man zur Fehlererkennung häufig CRC-Prüfsummen (Cyclic Redundancy Check). Dabei interpretiert man die bitweise Darstellung der Nachricht als Folge der Koeffizienten eines Polynoms $a(x)$. An diese Folge möchte man k weitere (Prüf-)Bits anhängen (die einem Polynom $p(x)$ entsprechen), so dass das entstehende Polynom $b(x)$ durch ein festgelegtes Generatorpolynom $g(x)$ ohne Rest teilbar ist.

Es soll also gelten: $b(x) = a(x)x^k + p(x)$, sowie $b(x) = t(x)g(x)$.

Man kann daher die Prüfziffern berechnen, indem man den Rest einer Polynomdivision über $\mathbb{Z}_2$ von $a(x)x^k$ durch $g(x)$ bestimmt.

Auf der Empfängerseite kann man Übertragungsfehler feststellen, indem man die empfangene Bitfolge ebenfalls als Polynom $b'(x)$ interpretiert und überprüft, ob sich $b'(x)$ durch $g(x)$ ohne Rest teilen läßt.

a) Berechnen Sie die Prüfsumme für die Bitfolge 101001 (also $a(x) = x^5 + x^3 + 1$) und das Generatorpolynom $g(x) = x^3 + x + 1$ mit $k = 3$.

b) Bei einer weiteren Übertragung wurde das gleiche Generatorpolynom benutzt. Der Empfänger erhielt die Bitfolge 100101111. Stellen Sie fest, ob bei der Übertragung ein Fehler aufgetreten ist.

c) Kann man auf der Empfängerseite aus einer Teilbarkeit von $b'(x)$ durch $g(x)$ mit Sicherheit schlußfolgern, dass kein Übertragungsfehler aufgetreten ist?

14. Permutationszyklen

Eine Permutation $\sigma \in \mathcal{S}_n$ $(n \geq 2)$ heißt *Zyklus der Länge* r $(2 \leq r \leq n)$, wenn es r paarweise verschiedene Elemente $i_1, \ldots, i_r \in \{1, \ldots, n\}$ derart gibt, dass gilt:

$$\begin{array}{lcll} \sigma(i_k) & = & i_{k+1} & \text{für } k = 1, \ldots, r-1 \\ \sigma(i_r) & = & i_1 & \\ \sigma(i) & = & i & \text{für } i \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}; \end{array}$$

man schreibt dann $\sigma = (i_1, \ldots, i_r)$. Zwei Zyklen $(i_1, \ldots, i_r)$ und $(i'_1, \ldots, i'_s)$ heißen *disjunkt*, wenn

$$\{i_1, \ldots, i_r\} \cap \{i'_1, \ldots, i'_s\} = \emptyset$$

gilt. Zeigen Sie:

a) Sind σ und τ disjunkte Zyklen in $\mathcal{S}_n$, so gilt $\sigma \circ \tau = \tau \circ \sigma$.

b) Jede Permutation $\sigma \in \mathcal{S}_n \setminus \{\mathrm{id}\}$ (id = identische Abbildung, $x \mapsto x$) ist ein Produkt von paarweise disjunkten Zyklen, d.h. es gibt paarweise disjunkte Zyklen $\tau_1, \ldots, \tau_p$ in $\mathcal{S}_n$ ($p \in \mathbb{N}$) mit $\sigma = \tau_1 \circ \cdots \circ \tau_p$.

c) Die Darstellung in b) ist bis auf die Reihenfolge der Faktoren eindeutig, d.h. sind $\sigma = \tau_1 \circ \cdots \circ \tau_p$ und $\sigma = \tau'_1 \circ \cdots \circ \tau'_q$ zwei Darstellungen von σ als Produkt von paarweise disjunkten Zyklen, so gilt $p = q$ und $\{\tau_1, \cdots, \tau_p\} = \{\tau'_1, \cdots, \tau'_q\}$.