4. Aufgabenblatt vom Mittwoch, den 02.Mai 2012 zur Vorlesung

# Mathematik für Informatiker II

(Frank Hoffmann)

Abgabe: bis Freitag, den 11. Mai 2012, 10.15 Uhr

1. **Reelles** (4 Punkte)
   Betrachten Sie die folgenden beiden Mengen reeller Zahlen:

$$S = \{\frac{m-n}{m+n} | m, n \in \mathbb{N}, m+n > 0\} \qquad S^* = \{\frac{m-n}{m+n} | m, n \in \mathbb{N} \setminus \{0\}\}$$

   Zeigen Sie, dass beide Mengen beschränkt sind. Bestimmen Sie jeweils Infimum und Supremum. In welchen der beiden Fälle ist das Infimum auch Minimum und das Supremum ein Maximum?

2. **Polynome über $\mathbb{Q}$ und über $\mathbb{Z}_5$** (4 Punkte)
   Bestimmen Sie ein Polynom $p(x) \in \mathbb{Q}[x]$ vom Grad $\leq 3$ mit den folgenden Eigenschaften:

$$p(-1) = -2, \qquad p(0) = 2, \qquad p(1) = 0, \qquad p(2) = 4$$

   Finden Sie dann ein Polynom über $\mathbb{Z}_5$ mit diesen Eigenschaften.

3. **Irreduzible Polynome** (4 Punkte)
   Ein Polynom $f(x) \in \mathbb{K}[x]$ über dem Körper $\mathbb{K}$ mit Grad $> 0$ heißt irreduzible, falls aus $f(x) = a(x) \cdot b(x)$ folgt, dass $a(x)$ oder $b(x)$ ein konstantes Polynom ist.

   (a) Faktorisieren Sie das Polynom $f(x) = x^4 - 4$ in irreduzible Bestandteile über dem Körper $\mathbb{Q}$, dann über dem Körper $\mathbb{R}$ und schließlich das Polynom $f(x) = x^4 + 2$ über dem Körper $\mathbb{Z}_3$.

   (b) Zeigen Sie, dass es über $\mathbb{Q}$ irreduzible Polynome für jeden Grad $n \geq 1$ gibt.

4. **Etwas Praktisches: Horner-Schema und Pattern-Matching** (8 Punkte)
   Die sogenannte Fingerprint-Methode von Karp und Rabin ist ein randomisiertes Verfahren zum Auffinden aller Vorkommen eines Suchwortes $P$ in einem Text $T$. Es beruht auf einer cleveren Anwendung des Horner-Schemas.
   Seien $T = T(1)T(2)\ldots T(m)$ und $P = P(1)P(2)\ldots P(n)$ Wörter der Länge $m$ und $n$ mit $m > n$, die Text und Suchwort darstellen, über dem Körper $\mathbb{Z}_2$. Wir sagen, $P$ matcht $T$ an der Stelle $r$ falls $T_r = T(r)T(r+1)\ldots T(r+n-1) = P$.
   Wir definieren $H(P) = \sum_{i=1}^{n} 2^{n-i} P(i)$ und $H(T_r) = \sum_{i=1}^{n} 2^{n-i} T(r+i-1)$. Suchwort und Textstück werden also einfach als Zahl interpretiert. Offensichtlich matcht das Suchwort $P$ den Text an der Stelle $r$ genau dann, wenn $H(P) = H(T_r)$ ist.
   Der Fingerprint-Trick besteht nun darin, diesen Sachverhalt modulo einer zufälligen Primzahl $p$ zu betrachten, dann das Horner-Schema auszunutzen und die Zwischenergebnisse alle klein zu halten.

(a) Sei $p$ eine Primzahl. Wir setzen $H_p(P) = H(P) \mod p$ und $H_p(T_r) = H(T_r) \mod p$. Zeigen Sie, dass $H_p(P) = H_P(T_r)$ falls $P$ den Text an der Stelle $r$ matcht. Finden Sie ein Beispiel, so dass die Umkehrung nicht gilt.
Hinweis: Der Punkt ist, dass dies bei zufälliger Wahl der Primzahl sehr selten auftritt.

(b) Sei $P = 101111, p = 7$. Berechnen Sie $H_p(P)$, indem Sie zuerst mit Horner-Schema $H(P)$ ausrechnen und dann modulo $p$ rechnen. Wiederholen Sie die Rechnung, indem Sie die $\mod p$–Rechnungen in die Einzelschritte beim Horner-Schema "reinziehen". Weshalb kann man dies tun? Die Zwischenergebnisse sollten $2p$ nicht überschreiten.
Formulieren Sie in Verallgemeinerung dieses Beispiels nun ein Prinzip zur Berechnung von $H_p(P)$, bei dem Zwischenergebnisse nie größer als $2p$ sind.

(c) Man kann $H_p(T_1)$ und jedes andere $H_p(T_r)$ nach derselben Methode berechnen. Es gibt allerdings einen einfachen Trick $H_p(T_r)$ aus $H_p(T_{r-1})$ für $r > 1$ effizient auszurechnen. Wie?
Damit hat man eine Methode gefunden, ein Fenster der Länge des Suchmusters über den Text zu schieben, an jeder Stelle die Fingerprints zu vergleichen und dies als Kriterium zum Pattern Matching zu benutzen.