Fachbereich Mathematik
Prof. Dr. Martin Otto
Alexander Kartzow
Alexander Kreuzer
Benno van den Berg

TECHNISCHE
UNIVERSITÄT
DARMSTADT

SS 2010
21.04.2010

2. Übungsblatt zu FGdI 1

Gruppenübung

Aufgabe G1

Für $a, b, n \in \mathbb{N}$ kann man $a^b \bmod n$ mit dem folgenden Algorithmus effizient berechnen. Sei $b = \sum_{i=0}^{k} b_i 2^i$ mit $b_i \in \{0, 1\}$ (d.h. $b_k b_{k-1} \dots b_0$ ist die Binärdarstellung von b).

```
ModExp(a, b, n)
erg := 1
quad := a mod n

FOR i = 0, ..., k DO
  IF b_i = 1 THEN erg := (erg · quad) mod n
  quad := (quad · quad) mod n
OD
RETURN erg;
```

Machen Sie sich an Hand von Beispielen klar, dass der Algorithmus funktioniert. Für feste Werte von a und n können die Variablen *quad* und *erg* nur endlich viele Werte annehmen. In diesem Fall kann man den Algorithmus durch ein endliches Transitionsystem modellieren.

(a) Modellieren Sie die Berechnung von $6^b \bmod 7$ als endliches Transitionssystem. Wieviele Stellen der Binärdarstellung von b müssen Sie kennen, um den Wert von $6^b \bmod 7$ zu bestimmen?

Hinweis. Fassen Sie die Werte von *erg* und *quad* als die Zustände des Transitionssystems auf und modellieren Sie einen Durchlauf der FOR-Schleife als einen Übergang.

(b) Modellieren Sie die Berechnung von $2^b \bmod 7$ als Transitionssystem. Wieviele Stellen der Binärdarstellung von b müssen Sie in diesem Fall kennen, um den Wert von $2^b \bmod 7$ zu bestimmen?

Aufgabe G2

Sei $z = \sum_{i=0}^{k} z_i 10^i$ mit $z_i \in \{0, 1, \dots, 9\}$ (d.h. $z_k z_{k-1} \dots z_0$ ist die Dezimaldarstellung von z). Die *Quersumme* von z ist die Zahl

$$q(z) = \sum_{i=0}^{k} z_i.$$

(a) Beweisen Sie, dass $z \equiv_9 q(z)$ und dass deshalb die Zahl z genau dann durch 9 teilbar ist, wenn ihre Quersumme dies ist.

Hinweis. Zeigen Sie mit Induktion, dass $10^n - 1$ für jedes $n \in \mathbb{N}$ durch 9 teilbar ist.

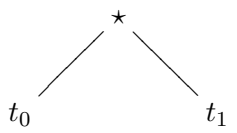
(b) Zeigen Sie, dass die Zahl z genau dann durch 11 teilbar ist, wenn ihre alternierende Quersumme

$$\sum_{i=0}^{k} (-1)^i z_i = z_0 - z_1 + z_2 - \ldots + (-1)^k z_k$$

dies ist.

Aufgabe G3

Wir betrachten folgende Operation zur Erzeugung binärer Bäume: Sind t_0 und t_1 (binäre) Bäume, so sei $f(t_0, t_1)$ der (binäre) Baum, welcher aus der disjunkten Vereinigung von t_0 und t_1 durch Hinzufügen einer neuen Wurzel entsteht.

$f(t_0, t_1) =$ 

Mit $\star$ bezeichnen wir den Baum, welcher aus einem einzigen Knoten ohne Kante besteht. Für einen Baum t bezeichne $\alpha(t)$, $\beta(t)$ und $\gamma(t)$ die Anzahl der *Knoten, Kanten,* bzw. *Blätter* (Knoten ohne Nachfolger) von t.
Beweisen Sie die folgenden Gleichungen für jeden Baum t, der sich mit Hilfe der Operation f aus dem Baum $\star$ erzeugen lässt.

(a) $\gamma(t) = \dfrac{\beta(t)}{2} + 1$

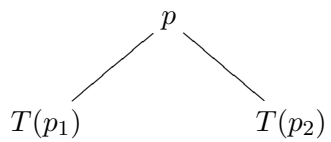
(b) $\beta(t) = 2\alpha(t) - 2\gamma(t)$

Hinweis. Beweisen Sie die Aussagen per Induktion über den Erzeugungsprozess.

Hausübung

Aufgabe H1 (6 Punkte)

Wir betrachten ein Spiel, in dem zwei Spieler abwechselnd ziehen. In diesem Spiel endet jeder regelkonforme Spielverlauf nach einer endlichen Anzahl von Zügen und es gibt dann einen eindeutigen Gewinner. In dieser Aufgabe wird bewiesen, dass jedes solche Spiel *determiniert* ist, d.h., dass es eine Gewinnstrategie für einen der beiden Spieler gibt.
Zur Vereinfachung betrachten wir "endliche" Spiele, in denen es nur endlich viele Spielpositionen insgesamt gibt, und zur weiteren Vereinfachung nehmen wir an, dass es in jeder Spielposition entweder genau 2 verschiedene mögliche Züge gibt oder dass das Spiel in dieser Position endet.
Zum Beweis sollen Sie Induktion über sogenannte *Spielbäume* benutzen. Der Spielbaum zu einer Position p, an der das Spiel endet, ist ein Baum mit nur einem Knoten p. Für jede Spielposition p, an der das Spiel nicht endet, gibt es Spielpositionen p_1 und p_2, die der aktive Spieler mit einem Zug erreichen kann. Wir bezeichnen mit $T(p_i)$ den Spielbaum zur Position p_i für $i \in \{1, 2\}$. Der Spielbaum zur Position p ist dann definiert als der Baum



Beweisen Sie durch Induktion über den Aufbau der Spielbäume, dass jede Position entweder eine Gewinnposition oder eine Verlustposition ist (in einer Gewinnposition hat der Spieler, der am Zug ist, eine Gewinnstrategie, in einer Verlustposition sein Gegenspieler).
Bemerkung. Eine Verallgemeinerung dieses Satzes wurde von Ernst Zermelo bewiesen und 1913 in einem Artikel mit dem Titel "*Über eine Anwendung der Mengenlehre auf die Theorie des Schachspiels*" veröffentlicht.
Zusatz. Das Schokoladenspiel von Blatt 1 (H1) ist ein Beispiel für ein endliches Spiel. Für jede Rechteckgröße hat also einer der Spieler eine Gewinnstrategie. Man kann zeigen: Wenn das Rechteck aus mindestens 2 Stücken besteht, ist es nicht der zweite Spieler (Wie?).

Aufgabe H2 (6 Punkte)

Betrachte die Menge $M = \{a, b, c, d, e, f, g, h, i\}$ und Teilmengen A, B, C von M gegeben durch:

$$\begin{aligned} A &= \{c, f, h\}, \\ B &= \{d, e, f, h\}, \\ C &= \{g, h, i\}. \end{aligned}$$

Wir betrachten die Elemente von M als Einträge in einer Datenbank. Diese Datenbank hat die folgende Abfragesprache (*query language*): man kann abfragen, welche Elemente von M Elemente von A, B und C sind. Man kann Abfragen (*queries*) auch mit AND, OR und NEG verknüpfen: falls X, Y Abfragen sind, kann man mittels X AND Y abfragen, welche Elemente sowohl die Eigenschaften X als auch die Eigenschaft Y haben; mittels X OR Y, welche Elemente mindestens eine der beiden Eigenschaften haben und mittels NEG X, welche Elemente die Eigenschaft X nicht haben. Sei S die Klasse von Teilmengen von M, die man als Antworten auf Abfragen bekommen kann.

(a) Zeigen Sie, dass S sowohl die leere Menge als auch M enthält und unter Vereinigung, Durchschnitt und Komplement (in M) abgeschlossen ist. Folgern Sie daraus, dass S eine Boolesche Algebra bildet.

(b) Seien

$$\begin{aligned} X_1 &:= \overline{A} \cap \overline{B} \cap \overline{C} = \{a, b\} \\ X_2 &:= \overline{A} \cap \overline{B} \cap C = \{g, i\} \\ X_3 &:= \overline{A} \cap B \cap \overline{C} = \{d, e\} \\ X_4 &:= A \cap \overline{B} \cap \overline{C} = \{c\} \\ X_5 &:= A \cap B \cap \overline{C} = \{f\} \\ X_6 &:= A \cap B \cap C = \{h\} \end{aligned}$$

Beweisen Sie, dass man jede Menge in S als eine Vereinigung geeigneter X_i bekommen kann und dass diese Darstellung eindeutig ist. Man nennt solche X_i auch Atome der Booleschen Algebra.

(c) Sei $L := \{1, 2, 3, 4, 5, 6\}$. Beweisen Sie, dass die Abbildungen

$$\begin{array}{rccl} f: & \mathcal{P}(L) & \to & S \\ & P & \mapsto & f(P) := \bigcup_{i \in P} X_i \end{array} \qquad \begin{array}{rccl} g: & S & \to & \mathcal{P}(L) \\ & Q & \mapsto & g(Q) := \{i \in L : X_i \subseteq Q\} \end{array}$$

Homomorphismen von Booleschen Algebren sind und dass sie Umkehrfunktionen voneinander sind. Wie viele Elemente hat S also?