WS 2009/10

Diskrete Strukturen

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2009WS/ds/uebung/

27. Januar 2010

ZÜ XII Blatt 12, VA1 bis VA4

1. Blatt 12, VA 1

Beweisen oder widerlegen Sie:

Jeder Baum enthält höchstens ein einziges perfektes Matching.

Antwort:

Die Aussage ist wahr.

Beweis:
Wie folgt.

Sei $G = (V, E)$ ein Graph.

Eine Teilmenge M der Kanten von G, $M \subseteq E$, ist ein Matching von G, falls keine zwei Kanten aus M einen Knoten gemeinsam haben; formal:

$$\forall e, f \in M : e \cap f = \emptyset\,.$$

Ein Matching M ist perfekt, falls alle Knoten mit einer Kante aus M inzidieren;
formal:

$$\forall v \in V :\ \exists e \in M : v \in e\,.$$

Man sagt auch, dass ein perfektes Matching alle Knoten überdeckt.

Beispiel:

Seien V die Menge aller Anwesenden im Hörsaal
und E gegeben durch die Nachbarschaft in einer Reihe.

Wir erzeugen (zufällig) ein Matching:

Handschlag: Jeder gibt, wenn möglich, einem Nachbarn die Hand.

Können noch weitere Handschläge gemacht werden,
oder ist das Matching maximal?

Wie viele Knoten sind nicht überdeckt? Hand heben!

Ist das Matching perfekt?

Können wir das Matching durch ein Brücke perfekt machen?

Fortsetzung Beweis:

Jedes perfekte Matching M von G ist maximal bezüglich der Matching-Eigenschaft, d. h., dass es keine echte Obermenge M' von M gibt, die auch ein Matching von G ist.

Daraus folgt, dass für zwei verschiedene perfekte Matchings M_1, M_2 von G es eine Kante e gibt mit

$$e \in M_1 \setminus M_2 \,.$$

Jedes perfekte Matching M von G definiert eine involutorische Abbildung $\;m : V \to V\;$ von V auf sich mit

$$m(u) = v \;\Leftrightarrow\; \{u, v\} \in M \,.$$

Wir beweisen die Aussage nun durch Widerspruch
und nehmen an, dass M_1, M_2 zwei verschiedene perfekte Matchings von G seien mit $e = \{u_0, v_0\} \in M_1 \setminus M_2$.

Dann ist

$$v_0,\, m_1(v_0),\, (m_2 \circ m_1)(v_0),\, \ldots,\, (m_2 \circ m_1)^n(v_0) \;=\; v_{2n}$$

für jedes n ein Weg in G, wobei mindestens
v_0, v_1 und v_2 paarweise verschieden sind.

Es gilt $v_k \neq v_{k+2}$ für alle $k \geq 0$, weil aufeinanderfolgende Kanten nicht aus dem Durchschnitt $M_1 \cap M_2$ sein können.

Da aber jeder Weg endliche Länge hat, gibt es ein erstes k, so dass $v_k = v_j$ gilt mit $j < k - 2$. Damit gibt es einen Kreis in G.

Widerspruch! Denn ein Baum ist kreisfrei.

2. Blatt 12, VA 2

Zeigen Sie, dass im Folgenden
Algebren $A = \langle S, \circ \rangle$ definiert werden, die bezüglich des binären Operators $\circ$ eine kommutative Gruppe bilden.

1. Sei $S = \mathbb{R} \setminus \{-1\}$ und für alle $x, y \in S$

$$x \circ y = x + y + xy.$$

Beweis:

- Zunächst ist zu prüfen, ob durch die Gleichung $x \circ y = x + y + x \cdot y$ tatsächlich eine Operation von $S \times S$ in S definiert ist.

  Seien $x, y \in \mathbb{R} \setminus \{-1\}$.
  Es gilt offenbar $x \circ y \in \mathbb{R} \setminus \{-1\}$, denn wir können zeigen, dass $-1 = x + y + x \cdot y$ einen Widerspruch ergibt und deswegen $x, y \in \mathbb{R} \setminus \{-1\}$ gelten muss.

$$\begin{aligned} -1 = x + y + x \cdot y \quad &\Rightarrow \quad -1 - y = x(1+y) \\ &\Rightarrow \quad x = \frac{-1-y}{1+y} \\ &\Rightarrow \quad x = -1\,. \end{aligned}$$

- Wir zeigen die Assoziativität von $\circ$:

$$
\begin{aligned}
x \circ (y \circ z) &= x + (y \circ z) + x \cdot (y \circ z) \\
&= x + (y + z + y \cdot z) + x \cdot (y + z + y \cdot z) \\
&= x + y + z + y \cdot z + x \cdot y + x \cdot z + x \cdot y \cdot z \\
&= (x + y + x \cdot y) + z + (x + y + x \cdot y) \cdot z \\
&= (x \circ y) + z + (x \circ y) \cdot z \\
&= (x \circ y) \circ z\,.
\end{aligned}
$$

- $x = 0$ ist das Einselement (neutrales Element) bezüglich $(x \circ y)$.

$$0 \circ y = 0 + y + 0 \cdot y = y\,.$$

Das linke Einselement ist offensichtlich auch rechtes Einselement, d. h. Einselement.

- Wir zeigen, dass zu einem Element $x \in S$ das Inverse gegeben ist durch

$$x^{-1} = -\frac{x}{1+x}\,.$$

Es gilt

$$\begin{aligned} x \circ y = 0 \quad &\Leftrightarrow \quad x + y + x \cdot y = 0 \\ &\Leftrightarrow \quad y = -\frac{x}{1+x}\,. \end{aligned}$$

Die Existenz eines rechten Inversen ist damit bewiesen.

Allein schon aus der offensichtlichen Kommutativität folgt hier, dass jedes rechte auch linkes Inverses ist.

Es sei aber bemerkt, dass
die Beziehung zwischen linken und rechten Inversen
auch ohne Kommutativität ganz allgemein in Gruppen untersucht werden kann. Es genügt, allein die Existenz der linken Inversen nachzuweisen.

Ergebnis:
Damit ist der Nachweis erbracht, dass A eine Gruppe ist.
Die Kommutativität gilt aufgrund der Kommutativität von $+$ und $\cdot$.

Weiter: Gruppeneigenschaft von $A = (S, \circ)$.

2. Sei S gleich der Potenzmenge $\mathcal{P}(X)$ $(= 2^X)$ einer beliebigen Menge X und sei $\circ$ für $A, B \subseteq X$ gegeben durch

$$A \circ B = (A \cup B) \setminus (A \cap B).$$

Beweis:

Die Mengenoperation, die hier betrachtet wird, nennt man die Bildung der symmetrischen Mengendifferenz.

Wir führen zunächst die Bildung der einfachen Mengendifferenz auf die Komplementbildung innerhalb X zurück,
d. h. $A \setminus B = A \cap \overline{B}$ mit $\overline{Y} = X \setminus Y$.

Damit sind die De Morganschen Gesetze anwendbar und es gilt

$$\begin{aligned} A \circ B &= (A \cup B) \cap (\overline{A \cap B}) \\ &= (A \cup B) \cap (\overline{A} \cup \overline{B}) \\ &= (A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup (B \cap \overline{B}) \\ &= (A \cap \overline{B}) \cup (B \cap \overline{A}), \end{aligned}$$

und

$$\overline{A \circ B} = (A \cap B) \cup (\overline{A} \cap \overline{B}).$$

- Offensichtlich ist durch die Gleichung
  $A \circ B = (A \cup B) \setminus (A \cap B)$ eine Operation von $S \times S$ in S definiert,
  denn die gesamte Potenzmenge von X ist als Bildbereich der Verknüpfung zugelassen.

- Nachweis der Assoziativität:

Die Bildung einer mehrfachen symmetrischen Mengendifferenz läßt sich mit drei Mengen A, B, C gut veranschaulichen. Es werden genau jene Elemente erhalten, die entweder in genau einer der Mengen A, B, C sind oder die im Durchschnitt aller 3 Mengen enthalten sind.

Dies wird durch folgende Rechnung bestätigt:

$$
\begin{aligned}
&(A \circ B) \circ C \\
&\quad = \quad (A \circ B) \cap \overline{C} \cup (\overline{A \circ B}) \cap C \\
&\quad = \quad [(B \cap \overline{A}) \cup (A \cap \overline{B})] \cap \overline{C} \cup [(A \cap \overline{B}) \cup (B \cap \overline{A})] \cap C \\
&\quad = \quad (A \cap \overline{B} \cap \overline{C}) \cup (B \cap \overline{A} \cap \overline{C}) \cup (C \cap \overline{A} \cap \overline{B}) \cup (A \cap B \cap C).
\end{aligned}
$$

Substituiert man (zyklisch) B für A, C für B und A für C, dann erhält man einerseits den Ausdruck $(B \circ C) \circ A$ und andererseits die gleiche Formel wie oben,
denn die rechte Seite der Formel ist invariant gegenüber der genannten Permutation von Variablen.

Also gilt wegen Kommutativität

$$(A \circ B) \circ C = (B \circ C) \circ A = A \circ (B \circ C)\,.$$

- Das Einselement der symmetrischen Mengendifferenz ist offensichtlich die leere Menge.

$$A \circ \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A\,.$$

- Die Inverse von A ist A selbst. Es gilt

$$A \circ A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset\,.$$

Damit ist der Nachweis erbracht, dass G eine Gruppe ist.

3. Blatt 12, VA 3

1. Sei $S' = \langle S, \circ \rangle$ eine Halbgruppe. Dann nennen wir ein Element $x \in S$ vertauschbar in S', falls gilt

   $$(\forall a \in S)\,[\,a \circ x = x \circ a\,]\,.$$

   Es sei $V(S')$ die Menge aller in S' vertauschbaren Elemente von S.
   Zeigen Sie, dass $V(S')$ eine Unterhalbgruppe von S' erzeugt.

Beweis:

Seien $x, y \in V(S')$.
Zu zeigen ist $x \circ y \in V(S')$, d. h.

$$(\forall a \in S)\, [a \circ (x \circ y) = (x \circ y) \circ a] \,.$$

Es gilt

$$\begin{aligned} a \circ (x \circ y) &= (a \circ x) \circ y \\ &= (x \circ a) \circ y \\ &= x \circ (a \circ y) \\ &= x \circ (y \circ a) \\ &= (x \circ y) \circ a \,. \end{aligned}$$

2. Sei $M = \langle S, \circ \rangle$ ein Monoid mit neutralem Element 1. Wir nehmen an, dass für alle $x \in S$ gilt $x \circ x = 1$.

   Zeigen Sie, dass M eine abelsche Gruppe ist.

Beweis:

Nach Definition ist offenbar jedes Element zu sich selbst invers.
Wir zeigen die Vertauschbarkeit wie folgt:

$$\begin{aligned} x \circ y &= 1 \circ (x \circ y) \circ 1 \\ &= (y \circ y) \circ x \circ y \circ (x \circ x) \\ &= y \circ ((y \circ x) \circ (y \circ x)) \circ x = y \circ 1 \circ x \\ &= y \circ x \,. \end{aligned}$$

4. Blatt 12, VA 4

1. Zeigen Sie, dass gilt

$$\{(7k) \bmod 12 \mid k \in \mathbb{N}\} = \mathbb{Z}_{12}\,.$$

Man könnte k von 1 bis 12 durchlaufen und nachsehen, ob modulo 12 alle Zahlen aus $\mathbb{Z}_{12}$ erscheinen.

Tatsächlich ist das auch der Fall.

Man beweist aber eleganter wie folgt.

Beweis:

Wegen $ggT(7, 12) = 1$
gibt es $m, n \in \mathbb{Z}$, so dass $7m + 12n = 1$.
(Siehe Vorlesung nächste Woche, euklidscher Algorithmus.)

Man kann m positiv wählen, wenn man die Gleichung nur modulo 12 zu lösen braucht.

Damit folgt

$$7mx + 12nx \ = \ x \, .$$

Für jedes $x \in \mathbb{Z}_{12}$ gibt es deshalb ein $k \in \mathbb{N}$ und ein $l \in \mathbb{Z}$, so dass

$$7k + 12l \ = \ x$$

und damit

$$7k \ \equiv \ x \pmod{12}\,, \quad \text{d.h.} \quad x \ = \ (7k) \bmod 12\,.$$

2. Welche Ordnung besitzt 11 in $\langle \mathbb{Z}_{12}, +_{12} \rangle$?
Beweis!

Anwort: 12 .

Beweis:

Wegen $ggT(11, 12) = 1$ gibt es $m, n \in \mathbb{Z}$, so dass $11m + 12n = 1$.

Es folgt $\{(11k) \bmod 12 \mid k \in \mathbb{N}\} = \{0, 1, 2, \ldots, 11\}$.

Die Ordnung von 11 ist also $|\{(11k) \bmod 12 \mid k \in \mathbb{N}\}| = 12$.