WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011WS/ds/uebung/

14. Dezember 2011

ZÜ IX

Übersicht:

1. Übungsbetrieb

2. Thema: Kryptographie:
   RS (Reed, Solomon)
   CRC (Cyclic Redundancy Code)
   RSA (Rivest, Shamir, Adleman)

3. Vorbereitung: auf TA Blatt 9:
   Zählen von Relationen (VA1)
   Zählen von Abbildungen (VA2)
   Zählen von Wörtern (VA3)
   Binomialkoeffizienten (VA4)

1. Übungsbetrieb

Fragen?

Nächsten Mittwoch: Resümee Zusatzaufgabe von Blatt 6

2. Thema: Kryptographie

RS	(Reed, Solomon):	Vorlesung
CRC	(Cyclic Redundancy Code):	TA 1, Blatt 9
RSA	(Rivest, Shamir, Adleman):	Zusatzaufgabe Blatt 10 siehe Buch Steger

3. Vorbereitung auf TA's Blatt 9

3.1 VA 1, Zählen von Relationen und Mengen

Sei $M = \{1, 2, \ldots, m\}$. Wir betrachten die Menge aller Relationen $R \subseteq M \times M$.

1. Wie viele Relationen über M gibt es?

Lösung:

Die Anzahl $\text{anz}_{Rel}(M)$ der Relationen über M ist gleich der Anzahl der Teilmengen von $M \times M$.

Wegen $|M \times M| = m^2$ gilt

$$\text{anz}_{Rel}(M) = |\mathcal{P}(M \times M)| = 2^{m^2}.$$

2. Wie viele Relationen über M mit $k \in \mathbb{N}_0$ Elementen gibt es?

Lösung:

Die Frage ist,
wie viele Teilmengen mit k Elementen besitzt $M \times M$,
d. h., welchen Wert besitzt $|\{R \in \mathcal{P}(M \times M) \; ; \; |R| = k\}|$?

Nach Vorlesung besitzt jede Menge mit m Elementen genau

$$\binom{m}{k} = \frac{m!}{(m-k)!k!}$$

k-elementige Teilmengen.

Damit gilt für $k \leq m^2$ (und auch für $k > m^2$)

$$|\{R \in \mathcal{P}(M \times M) \; ; \; |R| = k\}| \; = \; \binom{m^2}{k} .$$

3. Wie viele reflexive Relationen über M gibt es?

Lösung:

Zur Konstruktion einer reflexiven Relation über M entfernt man zunächst aus $M \times M$ alle m Paare (x, x) der Identität Id_M,

nimmt dann eine Teilmenge der Restmenge und

fügt anschließend alle Paare der Identität wieder hinzu.

Man beachte, dass das abschließende Hinzufügen der Identität eine injektive Operation darstellt.

Entsprechend erhält man die
Anzahl anz_{refRel} der reflexiven Relationen über M wie folgt.

$$\mathsf{anz}_{refRel}(M) = |\mathcal{P}\left((M \times M) \setminus \mathsf{Id}_M\right)| = 2^{m^2-m}\,.$$

4. Sei A eine n-elementige Menge und
es sei B eine m-elementige Teilmenge von A.

   Wie viele Teilmengen C von A gibt es, die B enthalten, für den Fall $n = 5$ und $m = 2$?

   Geben Sie eine Formel für den allgemeinen Fall $n, m \in \mathbb{N}_0$ an und begründen Sie diese Formel.

Lösung:

Sei $B \subseteq A$.
Seien $A' := A \setminus B$ und $[B, A] := \{C \subseteq A \; ; \; B \subseteq C \subseteq A\}$.

Dann ist $f : [B, A] \to \mathcal{P}(A')$ mit $f(C) = C \setminus B$
eine bijektive Abbildung von $[B, A]$ auf $\mathcal{P}(A')$.

Es gilt wegen $|A'| = n - m$

$$|\mathcal{P}(A')| = 2^{n-m} .$$

Für $n = 5$ und $m = 2$ ergibt sich $|\mathcal{P}(A')| = 2^3 = 8$.

3.2 VA 2, Zählen von Abbildungen

Sei $M = \{0, 1, 2\}$.

1. Listen Sie alle Äquivalenzrelationen über M auf!

Lösung:

Äquivalenzrelationen sind durch
die Menge ihrer zugeordneten Äquivalenzklassen bestimmt.

Über der Grundmenge M mit 3 Elementen gibt es

Äquivalenzrelationen mit 3 Klassen,

mit 2 Klassen und

mit einer einzigen Klasse.

Die Menge der zugeordneten Klassen bildet eine Partition P der Grundmenge M.

Äquivalenzrelationen mit
1 Klasse: $P_{1,1} = \{\{0, 1, 2\}\}$.

Äquivalenzrelationen mit
2 Klassen: $P_{2,1} = \{\{0\}, \{1, 2\}\}$.
$P_{2,2} = \{\{1\}, \{0, 2\}\}$.
$P_{2,3} = \{\{2\}, \{1, 0\}\}$.

Äquivalenzrelationen mit
3 Klassen: $P_{3,1} = \{\{1\}, \{2\}, \{0\}\}$.

2. Wie viele Partitionen gibt es über M?

Lösung:

Die Partitionen entsprechen eineindeutig den Äquivalenzrelationen.

Also gibt es 5 Partitionen über M.

3. Gibt es eine Äquivalenzrelation über der leeren Menge?

Lösung:

Falls $M = \emptyset$,
dann ist $R = \emptyset$ eine Äquivalenzrelation über M.

Aus $\emptyset \times \emptyset = \emptyset$ folgt,
dass $\emptyset$ die einzige Relation über $\emptyset$ ist.

Die Menge der Klassen dieser Relation R ist leer.
Damit entspricht die leere Menge von Klassen in diesem Fall einer (einzigen) Partition von M.

4. Wie viele surjektive Abbildungen f von M auf $M' = \{1, 2\}$ gibt es?

Lösung:

Damit f surjektiv ist, muss $\{k_1, k_2\}$ mit $k_1 := f^{-1}(1)$ und $k_2 := f^{-1}(2)$ eine 2-elementige Partition über M bilden.

Also kommen nur
die Partitionen $P_{2,1}$, $P_{2,2}$ und $P_{2,3}$ für $\{k_1, k_2\}$ in Frage.

Für die Zuordnung der Urbildklassen k_1, k_2 zu den Klassen der Partitionen $P_{i,j}$ gibt es nun stets 2 Möglichkeiten.

Deshalb erhalten wir insgesamt 6 surjektive Abbildungen.

5. Wie viele injektive Operationen $f : M \to M$ gibt es?

Lösung:

Eine injektive Operation über einer endlichen Menge M ist gleichzeitig surjektiv und damit bijektiv.

Für die Abbildung von 0 gibt es 3 Möglichkeiten.

Für jede dieser Möglichkeiten gibt es dann 2 Möglichkeiten der Abbildung des Elementes 1.

Damit erhalten wir $2 \cdot 3 = 6$ injektive Operationen über M.

6. Geben Sie alle Variationen von M an!

In der Vorlesung haben wir dafür k-Permutation gesagt.
D.h., die Begriffe k-Variation und k-Permutation sind synonym.

Lösung:

Eine k-Variation (k-Permutation) einer Menge A wurde als Sequenz $q_1, q_2, \ldots, q_k$ der Länge k von paarweise verschiedenen Elementen q_i aus A definiert.

Eine k-Variation mit $k = |A|$ wird Permutation von A genannt.

Wir ordnen jeder Variation $q_1, q_2, \ldots, q_k$ über einer endlichen Menge A in eineindeutiger Weise eine bijektive Abbildung $f : [1, k] \to A$ wie folgt zu

$$f(i) = q_i \,.$$

Fall $k = 3$ (Permutationen):

Wir erhalten die folgenden 6 Abbildungen $f_1, f_2, \ldots, f_6$.

	1	2	3
f_1	0	1	2
f_2	0	2	1
f_3	1	0	2
f_4	1	2	0
f_5	2	0	1
f_6	2	1	0

Fall $k = 2$:

Wir erhalten die folgenden 6 Abbildungen $r_1, r_2, \ldots, r_6$.

	1	2
r_1	0	1
r_2	0	2
r_3	1	0
r_4	1	2
r_5	2	0
r_6	2	1

Fall $k = 1$:

Wir erhalten die folgenden 3 Abbildungen s_1, s_2, s_3. (gespiegelte Liste).

	s_1	s_2	s_3
1	0	1	2

Fall $k = 0$:

Wir erhalten die leere Sequenz bzw. leere Abbildung als einzige Variation der Länge 0.

3.3 VA 3, Zählen von Wörtern

1. Ein Dominostein besteht aus zwei Quadraten. In jedem Quadrat sei eine Zahl zwischen 1 und 7 durch Punkte dargestellt.
   Wie viele verschiedene Dominosteine dieser Art gibt es?

Lösung:

Die Punktezahlen auf den beiden Quadraten eines Dominosteines bilden eine 2-elementige Multiteilmenge der Menge $[7] \in \mathbb{N}$.

Nach Formel für die Anzahl $\text{anz}_M M(2,7)$ von 2-elementigen Multiteilmengen einer 7-elementigen Menge gilt

$$\text{anz}_{MM}(2,7) = \binom{7+2-1}{7-1} = \binom{8}{6} = \binom{8}{2} = 28\,.$$

2. Bestimmen Sie die Anzahl aller Wörter, die sich aus den Buchstaben des Wortes

MINIMALISIERUNG

bilden lassen.

Dabei darf und muss jedes Vorkommen eines Buchstaben des o. g. Wortes genau einmal verwendet werden.

Lösung:

Das gegebene Wort hat 15 Buchstabenvorkommen mit den folgenden Vielfachheiten:
A - 1, E - 1, G - 1, I - 4, L - 1, M - 2, N - 2, R - 1, S - 1, U - 1.

Würden alle Buchstabenvorkommen zu verschiedenen Buchstaben gehören (d. h. unterscheidbar sein), dann gäbe es $15!$ verschiedene Wörter.

Allerdings sind jeweils $4! \cdot 2! \cdot 2!$ der Wörter gleich, weil sie sich nur durch Vertauschung gleicher Buchstabenvorkommen zu I, M bzw. N ergeben.

Damit ergibt sich die Anzahl der verschiedenen Wörter mit

$$\frac{15!}{4!2!2!} = 13621608000\,.$$

3.4 VA 4, Binomialkoeffizienten

Bestimmen Sie die Binomialkoeffizienten von $x^3y^2z^2$ und x^2z^3 in $(x + xy + z)^5$.

Lösung:

Wir führen eine Klammerung ein und benutzen die Binomische Formel.

$$(x + xy + z)^5 = ((x + xy) + z)^5 = \sum_{k=0}^{5} \binom{5}{k} (x + xy)^{5-k} \cdot z^k$$

Koeffizient von $x^3y^2z^2$:

Es ist der Summand für $k = 2$ zu betrachten.

$$\binom{5}{2}(x+xy)^3z^2 \quad = \quad \binom{5}{2}z^2 \cdot \sum_{i=0}^{3}\binom{3}{i}x^{3-i}(xy)^i$$

Der gesuchte Koeffizient C ergibt sich aus dem Summanden für $i = 2$ wie folgt.

$$C = \binom{5}{2} \cdot \binom{3}{2} = 30\,.$$

Koeffizient von x^2z^3:

Es ist der Summand für $k = 3$ zu betrachten.

$$\binom{5}{3}(x+xy)^2z^3 \quad = \quad \binom{5}{3}z^3 \cdot \sum_{i=0}^{2}\binom{2}{i}x^{2-i}(xy)^i$$

Der gesuchte Koeffizient C ergibt sich aus dem Summanden für $i = 0$ wie folgt.

$$C = \binom{5}{3} \cdot \binom{2}{0} = 10\,.$$