Technische Universität München
Fakultät für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr
Dr. Werner Meixner

Wintersemester 2011/12
Übungsblatt 10
19. Dezember 2011

Diskrete Strukturen

Abgabetermin: 10. Januar 2012, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (4 Punkte)

Sei $p(x) \in \mathbb{C}[x]$ ein Polynom vom Grad $n-1$ mit den Koeffizienten $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$, d. h.

$$p(x) = P_{\vec{a}}(x)\,.$$

Wir betrachten speziell $n = 8$, $\vec{a} = (2, 1, 2, 1, 2, 1, 2, 1)$ und $\omega = e^{\frac{2\pi i}{8}}$.
Berechnen Sie die Fouriertransformierte

$$\mathcal{F}_{n,\omega}(\vec{a}) = (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1}))$$

durch Ausführung des Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$.

Hausaufgabe 2 (4 Punkte)

1. Seien K ein Körper und $p \in K[x]$ ein Polynom über K mit Unbestimmter x vom Grad 1. Man zeige, dass die Restklassenalgebra $K[x]/(p)$ isomorph zu K ist.
2. Gegeben sei das Polynom $p(x) = x^2 + 1$ über dem Körper der reellen Zahlen $\mathbb{R}$. Man zeige:
   (a) $p(x)$ ist irreduzibel in $\mathbb{R}[x]$.
   (b) Die Restklassenalgebra $\mathbb{R}[x]/(p)$ ist isomorph zum Körper $\mathbb{C}$ der komplexen Zahlen.

Hausaufgabe 3 (4 Punkte)

Wir betrachten den Polynomring $\mathbb{Z}_3[x]$ über dem Körper $\mathbb{Z}_3$.

1. Geben Sie alle irreduziblen, normierten Polynome aus $\mathbb{Z}_3[x]$ vom Grad 2 an. Ein Polynom ist normiert, wenn der Leitkoeffizient (Koeffizient des enthaltenen Monoms mit höchstem Grad) gleich 1 ist.
2. Zeigen Sie, dass das Polynom $x^4 + 1$ aus $\mathbb{Z}_3[x]$ reduzibel ist.

Hausaufgabe 4 (4 Punkte)

Sei K ein endlicher Körper, wobei $q = |K|$ ungerade sei. $K[x]$ sei die Menge der Polynome über K in der Variablen x. Zeigen Sie

1. $x^{q-1} - 1 = \prod_{a \in K^*}(x - a)$.
2. $\sum_{a \in K} a = 0$.

Hausaufgabe 5 (4 Punkte)

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$ aller Polynome über einer Variablen x mit Koeffizienten aus dem Körper $\langle \mathbb{Z}_3, +_3, \cdot_3 \rangle$ der ganzen Zahlen modulo 3. Sei $\pi \in \mathbb{Z}_3[x]$ das Polynom $\pi(x) = x^3 + 2$. Zeigen Sie für Polynome aus $\mathbb{Z}_3[x]$:

1. $(x^3 + 2)^3 = x^9 + 2$.
2. Es gilt $x^8 \equiv x^2 \,(\bmod\, \pi)$, d. h. x^8 ist kongruent zu x^2 modulo $\pi(x)$.
   Hinweis: Bestimmen Sie den Rest bei Division von x^8 durch $\pi(x)$.
3. Der Restklassenring $\langle \mathbb{Z}_3[x]/(\pi), +, \cdot \rangle$ ist kein Körper.

Hausaufgabe 6 (4 Punkte)

Sei $R = \mathbb{Z}_3[x]$ der Ring aller Polynome über dem Körper $\langle \mathbb{Z}_3, +_3, \cdot_3 \rangle$.

Sei $b \in R$ gegeben durch $b(x) = x^3 + x^2 + 1$. Wir betrachten den Ring $R_b = \mathbb{Z}_3[x]_{\mathrm{grad}(b)}$ der Polynome aus R modulo $b(x)$.

1. Zeigen Sie $x^8 \equiv 1 \,(\bmod\, b)$.
2. Geben Sie in R_b das inverse Element von x^2 an.

Zusatzaufgabe (Für Interessierte)

Das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir und Adleman) ist ein Public-Key-Kryptoverfahren, bei dem ein öffentlicher Schlüssel bekanntgegeben werden kann, mit dem Nachrichten verschlüsselt werden, bei dem aber nur der Besitzer des geheimen Schlüssels diese Nachrichten mit vertretbarem Rechenaufwand entschlüsseln kann.

Verfahren:
Man wählt zwei „sehr große“ Primzahlen p, q, berechnet $n = p \cdot q$ und bestimmt dann natürliche Zahlen k, l mit $\mathrm{ggT}(k, \varphi(n))$ und $k \cdot l \equiv 1 \pmod{\varphi(n)}$ (dabei bezeichnet φ die eulersche Phi-funktion). Der öffentliche Schlüssel ist das Paar (k, n), der geheime Schlüssel ist das Paar (l, n).
Eine Nachricht m mit $m < n$ wird wie folgt verschlüsselt:

Verschlüsseln: $m' = m^k \mod n$.

Entschlüsseln: $m'' = (m')^l \mod n$.

Das RSA-Verfahren ist korrekt, d. h., dass $m = m''$ gilt.

Wir kodieren nun Buchstaben durch Zahlen nach folgendem Schema:
Jedem Buchstaben wird eine Zahl zwischen 1 und 26 zugeordnet, die seiner Ordnung im Alphabet entspricht. Zu dieser Zahl wird dann noch 1 addiert (der Buchstabe C wird z. B. durch die Zahl 4 kodiert) und die erhaltene Zahl mit dem RSA-Verfahren verschlüsselt.

Nehmen Sie an, dass der öffentliche Schlüssel $(29, 35)$ und die Nachricht 24, 20, 32 sei. Knacken Sie den Kode!

Hinweis: *Auf den Übungsblättern in diesem Semester wird es grundsätzlich die drei Aufgabentypen Vorbereitungsaufgabe, Tutoraufgabe und Hausaufgabe geben. Die als Vorbereitung bezeichneten Aufgaben dienen der häuslichen Vorbereitung der Tutoraufgaben. Tutoraufgaben werden in den Übungsgruppen bearbeitet. Dabei wird die Lösung der Vorbereitungsaufgaben vorausgesetzt. Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

In der Vorlesung wurde mit der folgenden Tabelle die Basis für eine Klassifizierung kombinatorischer Aufgabenstellungen und Lösungen geschaffen. Die Formeln der Tabelle gelten für alle $n, r \in \mathbb{N}_0$. Wir schreiben für Mengen oder Multimengen X jeweils $X\{\neq\}$ bzw. $X\{=\}$, falls X aus unterscheidbaren (ungleichen) bzw. nicht unterscheidbaren (gleichen) Elementen besteht.

$N \longrightarrow R$ $\lvert N\rvert = n,\ \lvert R\rvert = r$	1 beliebig	2 injektiv	3 surjektiv	4 bijektiv ($r=n$)
$A:$ $N\{\neq\} \longrightarrow R\{\neq\}$	r^n	$r^{\underline{n}}$	$r!S_{n,r}$	$r! = n!$
$B:$ $N\{=\} \longrightarrow R\{\neq\}$	$\frac{r^{\overline{n}}}{n!}$	$\frac{r^{\underline{n}}}{n!} = \binom{r}{n}$	$\binom{n-1}{r-1}$	1
$C:$ $N\{\neq\} \longrightarrow R\{=\}$	$\sum_{i=0}^{r} S_{n,i}$	1 oder 0	$S_{n,r}$	1
$D:$ $N\{=\} \longrightarrow R\{=\}$	$\sum_{i=0}^{r} P_{n,i}$	1 oder 0	$P_{n,r}$	1

1. Bestimmen Sie für die Vorbereitungsaufgaben 1 bis 3 von Übungsblatt 9, mit welchen Formeln der Tabelle diese Aufgaben gelöst werden können.

   Begründen Sie die Zuordnung, indem Sie jeweils Multimengen N und R in Verbindung mit dem entprechenden Abbildungstyp angeben.

2. Sei $N = N_1 \uplus N_2$ eine Multimenge mit $|N| = n$, so dass die Elemente von N_1 bzw. N_2 nicht unterscheidbar sind und alle Paare $x_1 \in N_1$ und $x_2 \in N_2$ unterscheidbar sind. Sei R mit $|R| = r$ eine Menge mit unterscheidbaren Elementen und a die Anzahl der Möglichkeiten der injektiven Zuordnung $N \to R$. Man zeige die folgende Verallgemeinerung der Formeln A_2 und B_2 der Tabelle.

$$a = \binom{r}{n_1} \cdot \binom{r - n_1}{n_2}.$$

3. Man klassifiziere die Tutoraufgaben 2 und 3.1 von Übungsblatt 9 entsprechend.

Vorbereitung 2

Am Montagabend wählen sich n Studenten auf m Rechnern rayhalle1, rayhalle2 bis rayhalle m ein, um die neuen Übungsaufgaben zu lesen. Wie viele Möglichkeiten gibt es dafür, wenn darauf geachtet wird,

1. welcher Student auf welchem Rechner eingeloggt ist,

2. wie viele Studenten auf welchem Rechner eingeloggt sind,
3. welche Studenten gemeinsam auf dem gleichen Rechner eingeloggt sind,
4. wie viele Studenten gemeinsam auf dem gleichen Rechner eingeloggt sind,

und wie hängen die Antworten jeweils davon ab, ob auf jedem Rechner

- höchstens
- mindestens
- genau

ein Student eingeloggt ist.

Vorbereitung 3

Wie viele Stellungen gibt es bei dem Spiel TIC TAC TOE nach 4 Zügen (d. h., wenn jeder Spieler zweimal gesetzt hat)? Der erste Zug sei beliebig.
(siehe auch `http://de.wikipedia.org/wiki/Tic_Tac_Toe`)

Vorbereitung 4

In einem Rangierbahnhof gibt es 30 parallel laufende Gleise, auf denen Schwertransporte zusammengestellt werden. Wegen der übermäßigen Breite der Ladung können keine zwei Züge auf benachbarten Gleisen plaziert werden.

Wie viele Möglichkeiten gibt es, 9 (nicht unterscheidbare) Züge auf die Gleise so zu verteilen, dass sich die Züge nicht behindern?

Tutoraufgabe 1

4 Studenten erhalten 12 Tafeln Schokolade. Wie viele Möglichkeiten gibt es jeweils, stets ganze Tafeln auf die 4 Studenten aufzuteilen?
Beantworten Sie diese Frage für die folgenden zwei Fälle und führen Sie dabei Ihre Antwort auf die Lösungen in der Tabelle der Vorbereitung 1 zurück.

1. Die 12 Tafeln sind nicht unterscheidbar und die Studenten sind unterscheidbar (es ist also nicht egal, wer wie viele bekommt).

2. Die 12 Tafeln sind unterscheidbar und die Studenten sind nicht unterscheidbar. Aber es soll jeder Student genau 3 Tafeln bekommen.

Tutoraufgabe 2

Beantworten Sie die folgenden Fragen und führen Sie dabei Ihre Antwort auf die Lösungen in der Tabelle der Vorbereitung 1 zurück.

1. Wie viele Möglichkeiten gibt es, 4 nicht unterscheidbare Gegenstände in 3 nicht unterscheidbare Schachteln zu legen?

2. Wie viele Möglichkeiten gibt es, in 5 nicht unterscheidbare Pakete 15 gleiche Äpfel zu verteilen, wenn in jedem Paket mindestens 1 Apfel enthalten sein soll?

Tutoraufgabe 3

Beweisen Sie für alle $n, k \in \mathbb{N}_0$ die folgende Formel für die Stirling-Zahlen zweiter Art.

$$S_{n+1,k+1} = \sum_{i=0}^{n} \binom{n}{i} S_{i,k}\,.$$

Tutoraufgabe 4

Wir betrachten die Stirling-Zahlen erster Art $s_{n,k}$ für $n, k \in \mathbb{N}_0$, also die Anzahl verschiedener Permutationen einer n-elementigen Menge mit k nichtleeren, paarweise disjunkten Zyklen.

1. Begründen Sie kurz die folgenden Spezialfälle.

$$s_{0,0} = 1, \quad s_{n,n} = 1. \quad s_{n,k} = 0, \text{ falls } k > n. \quad s_{n,0} = 0, \text{ falls } n > 0\,.$$

2. Beweisen Sie mit Hilfe kombinatorischer Argumente, dass die folgende Gleichung gilt:

$$s_{n,n-2} = \frac{1}{24} n(n-1)(n-2)(3n-1)\,.$$