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

Wintersemester 2012/13
Übungsblatt 10
17. Dezember 2012

Diskrete Strukturen

Abgabetermin: 8. Januar 2013, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (4 Punkte)

Wir notieren ein Polynom $p(x) \in \mathbb{C}[x]$ vom Grad $n-1$ mit den Koeffizienten $\vec{a} = (b_0, a_1, \ldots, a_{n-1})$ durch $p(x) = P_{\vec{a}}(x)$.
Wir betrachten im Folgenden $n = 8$ und $\omega = e^{\frac{2\pi i}{8}}$.

1. Wir benützen die Bezeichnungen

$$\begin{aligned} \mathcal{F}_{4,i}((1,-1,1,-1)) &= (e_0, e_1, e_2, e_3), \\ \mathcal{F}_{2,-1}((1,1)) &= (c_0, c_1) \qquad \text{und} \\ \mathcal{F}_{2,-1}((-1,-1)) &= (d_0, d_1)\,. \end{aligned}$$

   Berechnen Sie die Fouriertransformierte $\mathcal{F}_{4,i}((1,-1,1,-1))$.

2. Berechnen Sie mit $\vec{a} = (2,1,-2,-1,2,1,-2,-1)$ die Fouriertransformierte

$$\mathcal{F}_{8,\omega}(\vec{a}) = (P_{\vec{a}}(\omega^0), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^7))$$

   durch Ausführung des ersten rekursiven Aufrufs im Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$. Sie dürfen die Ergebnisse aus Teilaufgabe 1 benutzen bzw. entsprechend anpassen.

Hausaufgabe 2 (4 Punkte)

Seien $\mathbb{Z}_2[x]$ der Ring der Polynome in x über dem Körper $\mathbb{Z}_2$ und R der Restklassenring von $\mathbb{Z}_2[x]$ modulo p mit $p = x^{15} + x^{14}$. Wir stellen R als Ring der Reste bei Division durch p und Operationen modulo p dar, d. h. $R = \langle \mathbb{Z}_2[x]_{15}, +_p, \cdot_p \rangle$, und bezeichnen den Rest $r \in R$ bei Division eines Polynoms $q \in \mathbb{Z}_2[x]$ durch p mit $r = q \bmod p$.

1. Zeigen Sie mit vollständiger Induktion für alle $n \in \mathbb{N}$ die folgende Gleichung für entsprechende Polynome aus $\mathbb{Z}_2[x]$:

$$x^{14+n} \bmod p \;=\; x^{14} \bmod p\,.$$

2. Berechnen Sie $q = (x^9 +_p 1) \cdot_p (x^8 +_p 1) \cdot_p x^5 \in R$ als Polynom mit $\text{grad}(q) \leq 14$.

   Ist q ein Nullteiler in R? Beweisen Sie Ihre Antwort!

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)

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 5 (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 4 (Für Interessierte)

Beim Cyclic Redundancy Check (CRC) wird eine Nachricht $(a_{n-1}, \ldots, a_0)$ von n Bits zusammen mit einer r-Bit-Checksumme $(p_{r-1}, \ldots, p_0)$ übertragen. Sowohl die Nachricht als auch die Checksumme werden als Polynome $a(x) = \sum_{i=0}^{n-1} a_i x^i$ bzw. $p(x) = \sum_{i=0}^{r-1} p_i x^i$ im Ring $\mathbb{Z}_2[x]$ aufgefasst. Die Checksumme wird aus der Nachricht mit Hilfe eines fest vorgegebenen Generatorpolynoms $g(x) \in \mathbb{Z}_2[x]$ mit $\mathrm{grad}(g) = r$ wie folgt berechnet:
$p(x)$ ist der Divisionsrest bei Division von $a(x)x^r$ durch $g(x)$, es gilt also

$$a(x)x^r = g(x) \cdot q(x) + p(x) \quad \text{bzw.} \quad a(x)x^r + p(x) = g(x) \cdot q(x)\,,$$

denn wir rechnen in $\mathbb{Z}_2$. Bei Empfang der Nachricht wird überprüft, ob $a(x)x^r + p(x)$ durch $g(x)$ teilbar ist. Falls dies nicht gilt, so ist ein Fehler aufgetreten.

1. Zeigen Sie, dass 1-Bit-Fehler (d. h. ein Bit a_i ist durch $1 - a_i$ ersetzt worden) immer erkannt werden, wenn das Generatorpolynom $g(x) \neq x^r$ ist.

2. Welche Bedingungen muss man an das Generatorpolynom $g(x)$ stellen, damit alle 2-Bit-Fehler erkannt werden?

3. Wir nehmen an, dass $n = 6,\ r = 3$ und $g(x) = x^3 + x^2 + x + 1$ gilt. Sie erhalten als Nachricht $a(x) = x^5 + x^2 + x$.

   Überprüfen Sie, ob die Checksumme $p(x) = x$ zur Nachricht passt!
   Welche Fehler könnten aufgetreten sein?

Hinweis: *Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

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

Begründen Sie Ihre Antworten.

Vorbereitung 2

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

1. Listen Sie alle Äquivalenzrelationen über M auf!
2. Wie viele Partitionen gibt es über M?
3. Gibt es eine Äquivalenzrelation über der leeren Menge?
4. Wie viele surjektive Abbildungen f von M auf $M' = \{1, 2\}$ gibt es?
5. Wie viele injektive Operationen $f : M \to M$ gibt es?
6. Geben Sie alle k-Permutationen (Variationen) von M an!

Begründen Sie Ihre Antworten.

Vorbereitung 3

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?

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.

Vorbereitung 4

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, 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 1.1 entsprechend.

Vorbereitung 5

Die Stirling-Zahlen zweiter Art $S_{n,k}$ für $n, k \in \mathbb{N}_0$ sind definiert als die Anzahl der verschiedenen Partitionen einer n-elementigen Menge in k nicht leere, paarweise disjunkte Teilmengen.

1. Begründen Sie die Gültigkeit der folgenden Gleichungen für alle $n, k \in \mathbb{N}_0$.

   (a) $S_{0,0} = 1$, (b) $S_{n,n} = 1$, (c) $S_{n,k} = 0$, falls $k > n$, (d) $S_{n,0} = 0$, falls $n > 0$.

2. Bekanntlich gilt die Rekursion $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$ für alle $n, k \in \mathbb{N}$. Stellen Sie die Rekursion bis $n + k = 8$ nach Art des Pascalschen Dreiecks dar.

Tutoraufgabe 1

1. Sei M eine Menge mit n Elementen und $k \in \mathbb{N}_0$. Wie viele Multiteilmengen von M mit höchstens k Elementen gibt es, wenn man $n = 6$ und $k = 3$ annimmt. Leiten Sie zunächst eine Formel ab für beliebiges n und k.

2. Bestimmen Sie den Koeffizienten von t^4xy^3z in $(x + y + z + t)^9$.

   Berechnen Sie das Ergebnis durch sukzessive Klammerung und Bestimmung von Binomialkoeffizienten.

Tutoraufgabe 2

1. Wie viele verschiedene Ergebnisse („Wurfkonstellationen“) kann es geben, wenn man mit 4 Würfeln gleichzeitig würfelt? Unterscheiden Sie dabei zwischen folgenden Szenarien:

   (a) Die Würfel sind alle verschiedenfarbig und damit unterscheidbar.

   (b) Die Würfel sind alle gleichfarbig.

   (c) Zwei Würfel sind blau und zwei Würfel sind grün.

2. Wie viele verschiedene Buchstabenfolgen kann man aus den Buchstaben des Wortes *ABRAKADABRA* bilden, wenn jeder Buchstabe genauso oft wie im Ursprungswort vorkommen soll? (Z. B. muss das A genau fünfmal vorkommen.)

Tutoraufgabe 3

Wir betrachten die Stirling-Zahlen zweiter Art $S_{n,k}$ für $n, k \in \mathbb{N}_0$, d. h. die Anzahl verschiedener Partitionen einer n-elementigen Menge in k nicht leere, paarweise disjunkte Teilmengen.

1. Zeigen Sie durch direkte kombinatorische Überlegungen (d. h. ohne vollständige Induktion) für alle $n \geq 1$: $\quad S_{n,n-1} = \binom{n}{2}$.

2. Seien P bzw. Q eine 5-elementige bzw. eine 3-elementige Menge. Wie viele surjektive Abbildungen von P auf Q gibt es?

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:

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