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

Wintersemester 2011/12
Übungsblatt 9
12. Dezember 2011

Diskrete Strukturen

Abgabetermin: 20. Dezember 2011, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (4 Punkte)

Sei G eine Gruppe mit e als neutralem Element, $g \in G$ mit $\mathrm{ord}(g) < \infty$. Zeigen Sie:

1. Für $d > 0$ gilt:

$$d = \mathrm{ord}(g) \quad \iff \quad g^d = e \text{ und für jedes } n > 0 \text{ mit } g^n = e \text{ gilt } d|n\,.$$

2. Für $n > 0$ gilt:

$$\mathrm{ord}(g^n) = \frac{\mathrm{ord}(g)}{\mathrm{ggT}(\mathrm{ord}(g), n)}\,.$$

Hausaufgabe 2 (4 Punkte)

Wir betrachten die Symmetrische Gruppe S_n aller Permutationen einer Teilmenge $[n]$ der natürlichen Zahlen mit der Komposition von Abbildungen als Gruppenverknüpfung.

1. Falls S_n zyklisch ist, dann gilt $n \leq 2$. Beweis!

2. Bestimmen Sie die größte Zahl k mit der Eigenschaft, dass es ein Element $p \in S_7$ gibt mit der Ordnung k, d. h. $\mathrm{ord}(p) = k$.

   Begründen Sie Ihre Herleitung und geben Sie eine entsprechende Permutation p an.

Hausaufgabe 3 (4 Punkte)

Wir betrachten die Gruppen $G = \langle \mathbb{Z}_6, +_6, 0\rangle$ und $H = \langle \mathbb{Z}_9^*, \cdot_9, 1\rangle$, wobei $\mathbb{Z}_n = \{0, \ldots, n-1\}$ und $\mathbb{Z}_n^* = \{p \in \mathbb{Z}_n; ggT(n,p) = 1\}$ gilt. Die Verknüpfungen $+_n$ und $\cdot_n$ bezeichnen die Addition bzw. die Multiplikation modulo n.

1. Geben Sie die Mengen $\mathbb{Z}_6$ und $\mathbb{Z}_9^*$ extensional an und bestimmen Sie zu jedem Element aus G und H jeweils das entsprechende Inverse bezglüglich $+_6$ bzw. $\cdot_9$.

2. Geben Sie zu jedem Element aus G und H jeweils die Ordnung an und begründen Sie kurz, wieso G und H isomorph sind.

3. Zwischen G und H existiert ein Isomorphismus $h : \mathbb{Z}_6 \to \mathbb{Z}_9^*$ mit $h(1) = 5$. Bestimmen Sie $h(0), h(2), h(3), h(4)$ und $h(5)$.

Hausaufgabe 4 (4 Punkte)

Bestimmen Sie Polynome $a(x), b(x), c(x)$ über den komplexen Zahlen mit imaginärer Einheit i und $\mathrm{grad}(a) \leq 1$, $\mathrm{grad}(b) = 0$, $\mathrm{grad}(c) = 0$, so dass gilt:

$$\frac{2x^3 - 13x^2 + 18x - 4}{(x-3)^2(x+2i)(x-2i)} = \frac{a(x)}{(x-3)^2} + \frac{b(x)}{(x+2i)} + \frac{c(x)}{(x-2i)}\,.$$

Hausaufgabe 5 (4 Punkte)

1. Zeigen Sie für alle $m, n \in \mathbb{N}$ mit $m < n$, dass $\frac{x^{2^n}-1}{x^{2^m}+1}$ ein Polynom ist.

2. Man zeige: Die 6 rationalen Funktionen x, $\frac{1}{x}$, $1-x$, $\frac{1}{1-x}$, $\frac{x}{x-1}$, $\frac{x-1}{x}$ bilden eine Gruppe bezüglich der Komposition $f \circ g$.

Zusatzaufgabe (Für Interessierte)

Abgaben bitte in der ZÜ an die Übungsleitung!

Irreduzible Polynome über endlichen Körpern spielen in mannigfacher Weise eine bedeutende Rolle. Wir wollen uns einen Überblick verschaffen über die Menge aller irreduziblen Polynome über $\mathbb{Z}_2$ höchstens vom Grad 5.

1. Versuchen Sie zunächst durch möglichst weitreichende hinreichende Bedingungen für die Reduzibilität der betreffenden Polynome die gesuchte Menge möglichst einzuschränken.

2. Für die verbleibende Menge von Polynomen entwerfe man einen systematischen Test auf Irreduzibilität. Führen Sie diesen Test aus.

   Welche Kardinalität besitzt die gesuchte Menge?

Hinweis: Machen Sie sich u. a. mit den Maple-Funktionen `Irreduc` und `Factor` vertraut in Zusammenhang mit den Varianten der Funktionen `mod` und `RootOf`.

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

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

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

Tutoraufgabe 1

Beim Cyclic Redundancy Check (CRC) wird eine Nachricht $(a_{n-1}, \dots, a_0)$ von n Bits zusammen mit einer r-Bit-Checksumme $(p_{r-1}, \dots, p_0)$ 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 überpr"uft, 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?

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

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.