

Lösung

HA-Lösung

LÖSUNG

Diskrete Strukturen – Endterm

Beachten Sie: Soweit nicht anders angegeben, ist stets eine Begründung bzw. der Rechenweg anzugeben!

Aufgabe 1

2P

Wir definieren 1m breite, 2m hohe und 12cm dicke Holztüren mit Plastikgriffen (kurz: HTPGs). HTPGs gibt es in verschiedenen Preisklassen:

- \emptyset ist die einzige HTPG der Preisklasse 0.
- X ist eine HTPG der Preisklasse $k + 1$, wenn
 - jedes $x \in X$ eine HTPG der Preisklasse $\leq k$ ist (mit $k \in \mathbb{N}_0$) und
 - es **genau** ein $x \in X$ gibt, das eine HTPG der Preisklasse k ist.
- X ist eine HTPG, wenn es ein $k \in \mathbb{N}_0$ gibt, so dass X eine HTPG der Preisklasse k ist; ansonsten gibt es keine weiteren HTPGs.

Bestimmen Sie, wie viele HTPGs der Preisklassen 1 bis 5 es jeweils gibt. Geben Sie die genauen Zahlenwerte als 2er-Potenz, d.h. in der Form 2^n mit $n \in \mathbb{N}_0$ an.

Lösung: Sei A_k die Anzahl der HTPG der Preisklasse k . Nach Definition gilt $A_0 := 1$.

Im Allgemeinen gilt nun für A_{k+1} , dass man genau eine HTPG der Preisklasse k auswählen muss (A_k Möglichkeiten), und ansonsten aus jeder Preisklasse $j < k$ eine beliebige Teilmenge von HTPGs der Preisklasse j (jeweils 2^{A_j} Möglichkeiten für $j = 0, \dots, k - 1$). Insgesamt somit:

$$A_{k+1} = A_k \cdot 2^{\sum_{j=0}^{k-1} A_j}.$$

Damit ergibt sich $A_1 = 1$, $A_2 = 1 \cdot 2^1 = 2$, $A_3 = 2 \cdot 2^{1+1} = 8$, $A_4 = 8 \cdot 2^{2+1+1} = 2^7 = 128$ und $A_5 = 128 \cdot 2^{8+2+1+1} = 2^{19} = 524288$.

Beispiele:

HTPGs der Preisklasse 0

$$\emptyset$$

HTPGs der Preisklasse 1

$$\{\emptyset\}$$

HTPGs der Preisklasse 2

$$\{\{\emptyset\}, \{\{\emptyset\}, \emptyset\}$$

HTPGs der Preisklasse 3

$$\{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}, \emptyset\}, \{\{\{\emptyset\}\}, \{\emptyset\}\}, \{\{\{\emptyset\}\}, \emptyset, \{\emptyset\}\}, \{\{\{\emptyset\}\}, \emptyset\}, \{\{\{\emptyset\}, \emptyset\}\}, \{\{\{\emptyset\}, \emptyset\}, \emptyset\}, \{\{\{\emptyset\}, \emptyset\}, \{\emptyset\}\}, \{\{\{\emptyset\}, \emptyset\}, \emptyset, \{\emptyset\}\},$$

usw.

Aufgabe 2

je 1P=4P

Wir betrachten folgende aussagenlogische Formel über den aussagenlogischen Variablen p, q, r :

$$F = (((p \rightarrow q) \wedge \neg(q \leftrightarrow r)) \vee \neg(\neg p \vee \neg q))$$

- (a) Geben Sie den Syntaxbaum von F an.
 (b) Stellen Sie die *vollständig* ausgefüllte Wahrheitstabelle zu F auf.

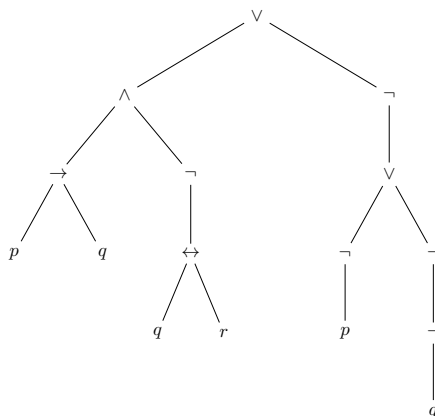
Die Spalten für die Belegungen müssen von links nach rechts mit pqr beschriftet sein.

- (c) Stellen Sie das KV-Diagramm zu $\neg F$ auf. Halten Sie sich *genau* an folgende Vorlage (nicht auf Aufgabenblatt eintragen!):

	$\neg r$	r	r	$\neg r$
$\neg q$				
q				
	p	p	$\neg p$	$\neg p$

- (d) Geben Sie eine aussagenlogische Formel G in KNF mit $G \equiv F$ an.

Lösung: $((p \rightarrow q) \wedge \neg(q \leftrightarrow r)) \vee \neg(\neg p \vee \neg q)$



p	q	r	$((p \rightarrow q) \wedge \neg(q \leftrightarrow r)) \vee \neg(\neg p \vee \neg q)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

	$\neg r$	r	r	$\neg r$
$\neg q$	0	0	0	1
q	0	1	1	0
	p	p	$\neg p$	$\neg p$

KNF zu F : $F \equiv (\neg q \vee \neg r) \wedge (p \vee q \vee r) =: G$.

Aufgabe 3

3P

Notation: Ist L ein Literal, so bezeichnet \bar{L} das Literal mit $\bar{L} \equiv \neg L$.

Sei K eine Klauselmeng und L ein Literal, so dass \bar{L} in keiner Klausel aus K vorkommt (kurz: $\forall C \in K: \bar{L} \notin C$).

Zeigen Sie unter dieser Voraussetzung:

K ist erfüllbar genau dann, wenn $K' := \{C \mid C \in K \wedge L \notin C\}$ erfüllbar ist.

Lösung: Zunächst macht man sich klar, dass

$$K = K' \uplus \{C \in K \mid L \in C\}$$

gilt. Insbesondere gilt somit $K' \subseteq K$. Weiter kommt weder L noch \bar{L} in einer Klausel aus K' vor.

Damit ist K' trivialerweise erfüllbar, wenn K erfüllbar ist: Gilt $\beta \models K$, dann nach Definition der Semantik der Konjunktion $\beta \models C$ für jede Klausel $C \in K$ und damit auch $\beta \models C$ für jede Klausel $C \in K' \subseteq K$, also $\beta \models K'$.

Sei K' erfüllbar und β' eine entsprechende erfüllende Belegung. Erweitert man daher β' zu $\beta := \beta'[L \rightarrow 1]$, so bleibt β ein Modell von K' , da nur der Wahrheitswert von L umdefiniert wird, welcher für K' keine Rolle spielt, da weder L noch \bar{L} und damit auch nicht die zugehörige Variable in K' auftritt. β ist aber trivialerweise in Modell für jede Klausel aus $\{C \in K \mid L \in C\}$. Damit ist β auch ein Modell von K , d.h. K ist erfüllbar.

Aufgabe 4

2P

Zeigen Sie, dass folgende Formel F der Prädikatenlogik 1. Stufe erfüllbar, aber nicht gültig ist. Geben Sie hierfür entsprechend zwei passende Strukturen $\mathcal{S}_0, \mathcal{S}_1$ mit $[F](\mathcal{S}_0) = 0$ und $[F](\mathcal{S}_1) = 1$ und Universum $U_{\mathcal{S}_0} = U_{\mathcal{S}_1} = \{a, b, c\}$ an:

$$F = \forall x \exists y \forall z (P(x, f(z)) \rightarrow \neg P(y, f(y)))$$

Lösung: Man kann die Formel vereinfachen zu:

$$F \equiv \forall x \exists y \forall z (\neg P(x, f(z)) \vee \neg P(y, f(y))) \equiv \forall x \forall z \neg P(x, f(z)) \vee \exists y \neg P(y, f(y))$$

(a) $f^{\mathcal{S}_1}(d) := a, P^{\mathcal{S}_1} = \{\}$ ist ein Modell.

(b) $f^{\mathcal{S}_0}(d) := d, P^{\mathcal{S}_0} = \{(a, a), (b, b), (c, c)\}$ ist kein Modell.

Alternativ: Für $P^{\mathcal{S}} = \emptyset$ ist die Hypothese der Implikation stets unerfüllbar, somit die Implikation trivial für jede Wahl von x, y, z erfüllt. Damit ist jede Struktur mit $P^{\mathcal{S}} = \emptyset$ und einer passenden Interpretation von f ein Modell.

Ergibt sich mit $P^{\mathcal{S}} = U_{\mathcal{S}}^2$ und jeder beliebigen passenden Interpretation von f eine passende Struktur, welche kein Modell ist.

Aufgabe 5

3P

Die Anzahl der Panzerkaninchen A_n im Jahr $n \in \mathbb{N}_0$ folgt folgender Gesetzmäßigkeit:

$$A_0 = 2 \quad A_1 = 6 \quad A_{n+2} = 4A_{n+1} - 4A_n$$

Zeigen Sie mittels geeigneter Induktion, dass $A_n = 2^n(n+2)$ für alle $n \in \mathbb{N}_0$ gilt.

Geben Sie explizit Induktionsbasis und Induktionsschritt an. Unterscheiden Sie weiterhin im Induktionsschritt explizit nach Induktionssannahme, der im Induktionsschritt zu zeigenden Behauptung und deren Beweis.

Lösung: Induktionsbasis $n \in \{0, 1\}$:

Für $n = 0$: $2^n(n+2) = 2^0(0+2) = 2 = A_0$

Für $n = 1$: $2^n(n+2) = 2^1(1+2) = 6 = A_1$

Induktionsschritt: Sei $n \in \mathbb{N}_0$ beliebig fixiert.

Annahme: Für $m \in \{n, n+1\}$ gilt $A_m = 2^m(m+2)$.

Zu zeigen: $A_{n+2} = 2^{n+2}(n+4)$

Beweis:

$$A_{n+2} \stackrel{\text{nDef}}{=} 4A_{n+1} - 4A_n \stackrel{\text{IA n}}{=} 4 \cdot 2^{n+1}(n+3) - 4 \cdot 2^n(n+2) = 2^{n+2}(2n+6-n-2) = 2^{n+2}(n+4)$$

Aufgabe 6

2P+2P+2P+3P=9P

Sei $\Sigma = \{a, b, c\}$ ein Alphabet bestehend aus drei verschiedenen Zeichen. Für $w \in \Sigma^*$ und $x \in \Sigma$ sei $|w|_x$ die Anzahl der Vorkommen von x in w , z.B. $|abac|_a = 2$. Die Länge von w wird wie üblich mit $|w|$ bezeichnet, z.B. $|abac| = 4$.

Bestimmen Sie jeweils die Anzahl der Wörter, welche folgenden Anforderungen genügen:

- $|w| = 11$ **und** stets steht jedes a links von jedem b , **und** jedes b links von jedem c .
- $|w| = 7$ **und** $|w|_a \leq |w|_b \leq |w|_c$ **und** stets steht jedes a links von jedem b , **und** jedes b links von jedem c .
- $|w| = 5$ **und** $|w|_a \leq |w|_b \leq |w|_c$.
- $|w| = 9$ **und** $|w|_a = 5$ **und** das Wort cb kommt in w **nicht** als zusammenhängendes Teilwort vor (z.B. nicht $aaaaacbbb$).

Neben dem Rechenweg sind jeweils die genauen Zahlenwerte verlangt.

Lösung:

- Jedes solche Wort hat die Form $a^{k_1}b^{k_2}c^{k_3}$ mit $(k_1, k_2, k_3) \in \mathbb{N}_0^n$ und $k_1 + k_2 + k_3 = 11$ oder ist ein beliebiges Wort aus $\{a, c\}^{11}$. Vom ersten Typ gibt es nach VL genau $\binom{11+3-1}{11} = \binom{11+3-1}{3-1} = \frac{13!}{2!11!} = 78$ viele. Vom zweiten Typ genau 2^{11} . In beiden Klassen liegen die Wörter der Form $a^k c^l$ mit $k+l=11$, wo von es $\binom{11+2-1}{11} = 12$ gibt. Insgesamt gibt es somit $78 + 2048 - 12 = 2114$ solcher Wörter.
- Jedes solche Wort hat die Form $a^{k_1}b^{k_2}c^{k_3}$ mit $(k_1, k_2, k_3) \in \mathbb{N}_0^n$, $k_1 \leq k_2 \leq k_3$ und $k_1 + k_2 + k_3 = 7$. Jedes Wort ist somit eindeutig mit dem Vektor (k_1, k_2, k_3) (plus Nebenbedingungen) identifiziert. Von diesen gibt es nach VL/TA11.1 genau $P_{7+3,3} = 8$ Stück (konkret $(0, 0, 7), (0, 1, 6), (0, 2, 5), (0, 3, 4), (1, 1, 5), (1, 2, 4), (1, 3, 3), (2, 2, 3)$ bzw. $P_{7,0} = 0, P_{7,1} = 1, P_{7,2} = 3, P_{7,3} = P_{4,0} + P_{4,1} + P_{4,2} + P_{4,3} = 0 + 1 + 2 + 1 = 4$).
- Im Gegensatz zu (b) muss man nicht nur Wörter der Form $a^{k_1}b^{k_2}c^{k_3}$ mit $(k_1, k_2, k_3) \in \mathbb{N}_0^n$, $k_1 \leq k_2 \leq k_3$ und $k_1 + k_2 + k_3 = \text{const}$ zählen, sondern muss ihre möglichen Anordnungen noch beachten: Ein Vektor (k_1, k_2, k_3) lässt sich dabei zu $\frac{5!}{k_1!k_2!k_3!}$ vielen verschiedenen Wörtern umordnen.

Konkret hat man folgende Vektoren (k_1, k_2, k_3) : $(0, 0, 5), (0, 1, 4), (0, 2, 3), (1, 1, 3), (1, 2, 2)$ ($P_{8,3} = P_{5,1} + P_{5,2} + P_{5,3} = 5$)

Damit erhält man

$$\frac{5!}{5!} + \frac{5!}{4!} + \frac{5!}{2!3!} + \frac{5!}{3!} + \frac{5!}{2!2!} = 1 + 5 + 10 + 20 + 30 = 66$$

Möglichkeiten.

- Jedes solche Wort hat die Form $b^{k_1}c^{l_1}ab^{k_2}c^{l_2}ab^{k_3}c^{l_3}ab^{k_4}c^{l_4}ab^{k_5}c^{l_5}ab^{k_6}c^{l_6}$ mit $k_1+l_1+\dots+k_6+l_6 = 4$ und $(k_1, \dots, k_6), (l_1, \dots, l_6) \in \mathbb{N}_0^n$. Damit muss man die verbleibenden 4 Zeichen auf b und c verteilen, und anschließend die entsprechenden Vektoren wieder zählen. Sei $j = |w|_b = k_1 + \dots + k_6$. Dann:

$$\sum_{j=0}^4 \binom{j+5}{5} \binom{4-j+5}{5} = \binom{5}{5} \cdot \binom{9}{5} + \binom{6}{5} \cdot \binom{8}{5} + \binom{7}{5} \cdot \binom{7}{5} + \binom{8}{5} \cdot \binom{6}{5} + \binom{9}{5} \cdot \binom{5}{5} = 1365$$

Alternative Rechnung:

Wörter der Länge 9 mit genau 5 as : $\binom{9}{5} \cdot 2^4 = 2016$.

(Wähle Positionen der as , dann die Positionen der bs , Rest sind cs)

Wörter der Länge 9 mit genau 5 as und mind. einmal cb : $\binom{8}{1} \binom{7}{5} 2^2 = 672$ – das stimmt dann noch nicht, da $a^k c b a^l c b a^n$ doppelt gezählt werden. Muss also um $\binom{5+3-1}{3-1} = \binom{7}{2} = 21$ korrigiert werden.

Insgesamt also: $2016 - 672 + 21 = 1365$.

Aufgabe 7

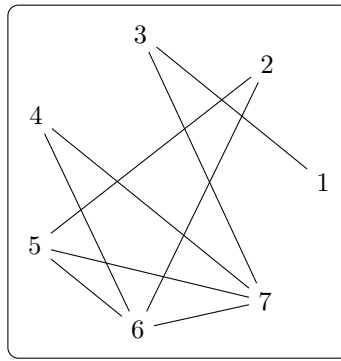
2P

Sei $d = (d_1, \dots, d_7) = (1, 2, 2, 2, 3, 4, 4)$.

Konstruieren Sie mit dem Verfahren aus den Übungen einen einfachen ungerichteten Graphen $G = ([7], E)$ mit $\deg(v_i) = d_i$.

Lösung: Mittels des Algorithmus aus den Tutorübungen erhält man z.B.:

(Die Reduktion der Gradfolge samt Permutationen wird erwartet.)



Aufgabe 8

2P+2P+2P+2P=8P

Mit Graph ist im Folgenden stets ein einfacher ungerichteter Graph gemeint.

Sei $G = (V, E)$ ein Graph. Wir nehmen an, dass die Knoten $V = \{v_1, v_2, \dots, v_n\}$ nach aufsteigendem Knotengrad aufgezählt werden, d.h. $\deg(v_i) \leq \deg(v_j)$ für $1 \leq i < j \leq n$. Dann ist die Gradfolge von G gerade die Sequenz $(\deg(v_1), \deg(v_2), \dots, \deg(v_n))$.

Begründen Sie jeweils,

- (a) ob es einen planaren Graphen mit der Gradfolge $(4, 4, 4, 4, 5, 5)$ gibt?
- (b) ob jeder zusammenhängende Graph mit Gradfolge $(1, 1, 1, 1, 2, 4)$ ein Baum ist?
- (c) ob jeder Graph mit Gradfolge $(3, 3, 3, 3, 4, 4, 4)$ einen Hamiltonkreis enthält?
- (d) ob jeder Graph mit Gradfolge $(2, 2, 2)$ eine Euler-Tour enthält?

Lösung:

- (a) Es gilt $|E| = 13$ und $|V| = 6$, also $|E| > 3|V| - 6$. Somit kann es keinen planaren Graphen mit dieser Gradfolge geben.
- (b) Wenn G zusammenhängend sein soll, dann folgt mit $2|E| = \sum d_i = 10 = 2|V| - 2$, dass ein solcher Graph ein Baum sein muss. Dass es überhaupt einen Baum mit dieser Gradfolge gibt, überprüft man leicht.
- (c) Nein, z.B. enthält der $K_{3,4}$ keinen Hamiltonkreis, siehe TA.
- (d) Gibt nur einen Graphen mit dieser Gradfolge, den C_3 , und der ist eulersch.

Aufgabe 9

2P+2P+2P+1P=7P

Sei $p = 107 = 2 \cdot 53 + 1$ mit $q = 53$. Sowohl p als auch q sind prim.

- (a) Berechnen Sie $5^q \pmod p$ und $3^q \pmod p$.
Hinweise: Es gilt $3^9 \equiv_p 102$, $5^5 \equiv_p 22$, $3^5 \equiv_p 29$ und $22^{10} \equiv_p 101$.
- (b) Entscheiden Sie jeweils, ob 3 bzw. 5 ein Erzeuger von $\langle \mathbb{Z}_p^*, \cdot, 1 \rangle$ ist.
- (c) Bestimmen Sie das multiplikative Inverse von 32 modulo p . Verwenden Sie hierfür den erweiterten euklidischen Algorithmus und protokollieren Sie die Teilergebnisse in einer Tabelle der folgenden Gestalt:

a	b	k	s	t
32	107
...

Insbesondere sollte in jeder Zeile stets $0 \leq a < b$, $k = \lfloor b/a \rfloor$ und $\text{ggT}(a, b) = as + bt$ gelten.

- (d) Berechnen Sie $32^{105} \pmod p$.

Lösung:

- (a) $3^{53} = (3^9)^5 \cdot 3^8 \equiv 102^5 \cdot 102/3 \equiv_p (-5)^5 \cdot 34 = -5^5 \cdot 34 \equiv_p -22 \cdot 34 = -748 \equiv_p 1$
 $5^{53} = (5^5)^{10} \cdot 5^3 \equiv_p 22^{10} \cdot 125 \equiv_p 101 \cdot 18 \equiv_p -6 \cdot 18 = -108 \equiv_p -1 \equiv_p 106$.
- (b) 3 ist kein Erzeuger, da die Ordnung wegen $3^{53} \equiv_p 1$ höchstens 53 sein kann.
5 ist ein Erzeuger: nach (a) gilt $5^{53} \equiv_p -1$, weiter gilt offensichtlich $5^2 \not\equiv_p 1$, und somit erst $5^{106} \equiv_p 1$, da als mögliche Ordnung von 5 nur die Teiler von 106, also 2 und 53 in Frage kommen.

(c)

a	b	k	s	t
32	107	3	-10	3
11	32	2	3	-1
10	11	1	-1	1
1	10	-	1	0

Damit ist $-10 \equiv_{107} 97$ das multiplikative Inverse von 32 modulo 107.

(d) In jeder endlichen Gruppe gilt $a^{|G|} = 1$ bzw. $a^{|G|-1} = a^{-1}$. Nun ist $|G| = 106$, also folgt $32^{105} \equiv_{107} 32^{-1} \equiv_{107} 97$.