HA-Lösung

Diskrete Strukturen – Endterm

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

Aufgabe 1 **6P**

Wir betrachten die folgenden Formeln über den aussagenlogischen Variablen A, B, C:

$$F_1 := (\neg A \vee (\neg B \oplus A))$$
$$F_2 := (((B \to A) \leftrightarrow (B \vee C)) \wedge \neg(C \to A))$$

(a) Zeichnen Sie zu den Formeln F_1 und F_2 jeweils den entsprechenden Syntaxbaum.

(b) Stellen Sie Wahrheitstabellen für beide Formeln auf.

- Auf die Wiederholung der Wahrheitswerte unter den Variablen der Formel kann verzichtet werden.
- Es müssen Teilformeln nur soweit ausgewertet werden, dass sich der Wahrheitswert der gegebenen Formel eindeutig aus der Wahrheitstabelle ergibt (entsprechend den Tutorübungen).
- Ihre Tabellen müssen dem Format aus den Übungen entsprechen:

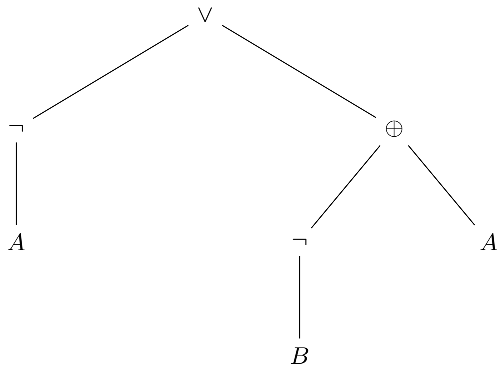
A	B	$(\neg A \vee (\neg B \oplus A))$
0	0	?
0	1	?
⋮	⋮	⋮
1	1	?

bzw.

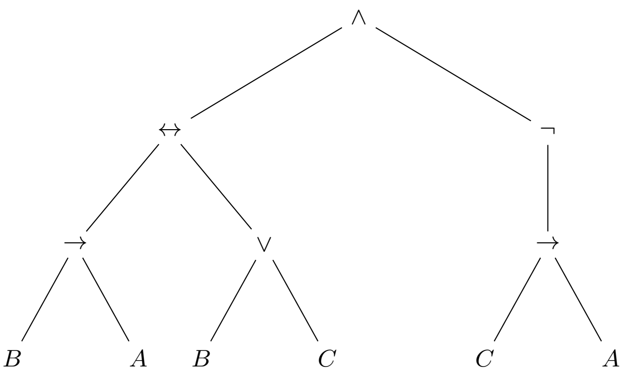
A	B	C	$(((B \to A) \leftrightarrow (B \vee C)) \wedge \neg(C \to A))$
0	0	0	?
0	0	1	?
⋮	⋮	⋮	⋮
1	1	1	?

(c) Geben Sie zu beiden Formeln jeweils eine möglichst einfache semantisch äquivalente Formel in KNF an.

Lösung



A	B	$(\neg$	A	$\vee$	$(\neg$	B	$\oplus$	$A))$
0	0	1		1	1		1	
0	1	1		1	0		0	
1	0	0		0	1		0	
1	1	0		1	0		1	



A	B	C	$(((B$	$\rightarrow$	$A)$	$\leftrightarrow$	$(B$	$\vee$	$C))$	$\wedge$	$\neg$	$(C$	$\rightarrow$	$A))$
0	0	0		1		0		0		0	0		1	
0	0	1		1		1		1		1	1		0	
0	1	0		0		0		1		0	0		1	
0	1	1		0		0		1		0	1		0	
1	0	0		1		0		0		0	0		1	
1	0	1		1		1		1		0	0		1	
1	1	0		1		1		1		0	0		1	
1	1	1		1		1		1		0	0		1	

KNF: $F_1 \equiv (\neg A \vee B)$ (nur eine Klausel)

KNF: $F_2 \equiv \neg A \wedge \neg B \wedge C$

Aufgabe 2 **5P**

Gegeben sei die folgende aussagenlogische Formel als Klauselmenge:

$$\{\{A, \neg B, \neg C\}, \{A, B, D\}, \{A, \neg C, \neg D\}, \{\neg A, B\}, \{\neg A, \neg B\}\}$$

(a) Wenden Sie den DPLL-Algorithmus aus *den Folien* (mit OLR, aber ohne PLR) an, um eine erfüllende Belegung für obige Formel zu berechnen.

(b) Beschreiben Sie die PLR („pure-literal rule", vgl. Übungsblatt 6) und markieren Sie in Ihrer Lösung zu (a) den ersten Zeitpunkt, in welchem die PLR angewendet werden würde.

Erinnerung: Die OLR hat stets höchste Priorität, die Fallunterscheidung stets niedrigste Priorität.

Beachten Sie: Hat der DPLL-Algorithmus die Wahl zwischen mehreren Literalen, so soll stets das Literal gewählt werden, das bzgl. der Ordnung $\prec$ vor allen anderen zur Auswahl stehenden Literalen kommt, wobei gelten soll:

$$A \prec \neg A \prec B \prec \neg B \prec C \prec \neg C \prec D \prec \neg D$$

Lösung

- Fallunterscheidung nach A: Annahme A ist wahr
  - OLR mit $\{A\}$ anwenden:
    $$\{\{B\}, \{\neg B\}\}$$
  - OLR mit $\{B\}$:
    $$\{\{\}\}$$
    also unerfüllbar, backtracking.
- Fallunterscheidung nach A – Annahme A ist falsch
  - OLR mit $\{\neg A\}$ anwenden:
    $$\{\{\neg B, \neg C\}, \{B, D\}, \{\neg C, \neg D\}\}$$
  - Fallunterscheidung nach B – Annahme B ist wahr.
    * OLR mit $\{B\}$:
      $$\{\{\neg C\}, \{\neg C, \neg D\}\}$$
    * OLR mit $\{\neg C\}$
      $$\{\}$$
      also erfüllbar, gib Belegung $\beta(A) = 0, \beta(B) = 1, \beta(C) = 0, \beta(D) \in \{0, 1\}$ zurück.

PLR: Falls eine Variable entweder nur als positives oder nur als negatives Literal vorkommt, setze entsprechendes Literal auf wahr und entferne entsprechend alle Klauseln, welches das Literal enthalten. Die PLR würde hier gleich zu Beginn C auf 0 setzen und damit die Formel auf $\{\{A, B, D\}, \{\neg A, B\}, \{\neg A, \neg B\}\}$ reduzieren.

Aufgabe 3 **5P**

Die Anzahl A_n der Zwuggelmeerschweinchen zum Zeitpunkt $n \in \mathbb{N}_0$ ist durch folgende Rekursionsgleichung gegeben:

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

Zeigen Sie mittels geeigneter Induktion, dass für alle $n \in \mathbb{N}_0$ gilt:

$$A_n = \frac{1}{2}(n^2 + n + 2)$$

Hinweis: Geben Sie explizit die Induktionsbasis an und gliedern Sie den Induktionsschritt in Induktionsannahme, Induktionsbehauptung und Beweis der Induktionsbehauptung. Werten Sie jeweils linke und rechte Seite unabhängig voneinander aus.

Lösung

- IBasis: $n \in \{0, 1\}$
  - $n = 0$: linke Seite: $A_0 = 1$; rechte Seite $\frac{1}{2}(0^2 + 0 + 2) = 1$
  - $n = 1$: linke Seite: $A_1 = 2$; rechte Seite: $\frac{1}{2}(1^2 + 1 + 2) = 2$
- ISchritt: Sei $n \in \mathbb{N}_0$ beliebig fixiert.
  - IAnnahme: Es gilt für das fixierte n: $A_n = \frac{1}{2}(n^2 + n + 2)$ und $A_{n+1} = \frac{1}{2}((n+1)^2 + (n+1) + 2)$.
  - IBehauptung: Es gilt für das fixierte n: $A_{n+2} = \frac{1}{2}((n+2)^2 + (n+2) + 2)$
  - Beweis:
    * Rechte Seite ausmultiplizieren:
    $$\frac{1}{2}((n+2)^2 + n + 2 + 2) = \frac{1}{2}n^2 + \frac{5}{2}n + 4$$
    * Linke Seite nach Definition:
    $$A_{n+2} \stackrel{\text{Def.}}{=} 2A_{n+1} - A_n + 1 \stackrel{\text{IAnn.}}{=} ((n+1)^2 + n + 1 + 2) - \frac{1}{2}(n^2 + n + 2) + 1$$
    $$= n^2 + 2n + 1 + n + 3 - \frac{1}{2}n^2 - \frac{1}{2}n - 1 + 1 = \frac{1}{2}n^2 + \frac{5}{2}n + 4$$

Damit gilt $A_n = \frac{1}{2}(n^2 + n + 2)$ für alle $n \in \mathbb{N}_0$, was zu zeigen war.

Aufgabe 4 **3P**

Mit *Graph* sei im Weiteren ein Tupel $G = (V, E)$ mit $|V| < \infty$ und $E \subseteq \binom{V}{2}$ gemeint. Wir nehmen weiterhin an, dass die Knoten $V = \{v_1, v_2, \ldots, v_n\}$ 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 $(\deg(v_1), \deg(v_2), \ldots, \deg(v_n))$.

Begründen Sie jeweils kurz, ob

(a) jeder Graph mit Gradfolge $(2, 2, 2, 2, 4, 4, 4, 4, 4)$ einen Euler-Kreis enthält.

(b) es einen planaren zusammenhängenden Graphen mit Gradfolge $(1, 1, 2, 2, 3, 3, 4)$ gibt, der die Ebene in genau 2 (umschließende und eingeschlossene) Flächen unterteilt.

(c) es einen 2-färbbaren Graphen mit Gradfolge $(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4, 4, 4)$ (12 Knoten vom Grad 1, 5 Knoten vom Grad 4) gibt.

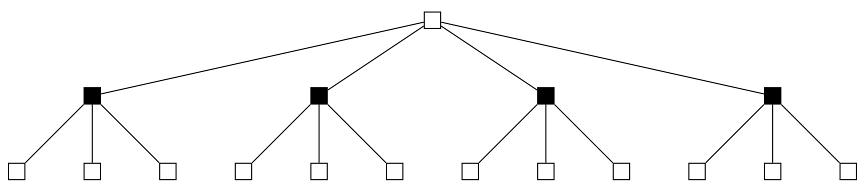
Lösung

(a) Nein, z.B. die disjunkte Vereinigung des C_4 mit dem K_5, welche nicht zusammenhängend ist.

(b) Sollte es einen planaren Graphen mit dieser Gradfolge geben, dann müsste $|F| - |E| + |V| = 1 + k$ gelten (mit k die Anzahl der Zusammenhangskompenten).

Mit der Annahme $|F| = 2$ und den gegebenen Werten $|V| = 7$ und $|E| = 8$ müsste also $2 - 8 + 7 = 1 + k$, also $k = 0$ gelten. Jeder Graph hat aber mindestens eine Zusammenhangskomponente. Also kann es keinen solchen planaren Graphen geben (inbesondere keinen zusammenhängenden, für den dann $k = 1$ gesetzt werden darf).

(c) Z.B.



Aufgabe 5 **6P**

Wir betrachten den Graphen $G_n = (V_n, E_n)$ mit $V_n = 2^{[n]}$ und $E_n = \{\{A, B\} \mid A \subseteq [n], B \subseteq [n], A \cap B = \emptyset, A \neq B\}$.

(a) Zeichnen Sie G_3.

(b) Welchen Grad hat $\emptyset$ in G_n?

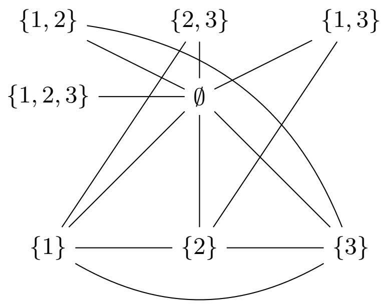
(c) Zeigen Sie: Ist A eine k-elementige, nicht leere Teilmenge von $[n]$, dann gilt $\mathsf{deg}(A) = 2^{n-k}$ in G_n.

(d) Bestimmen Sie $|E_n|$. Geben Sie einen möglichst einfachen Ausdruck an.
Hinweis: Sie dürfen für diese Teilaufgabe $3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$ ohne Beweis verwenden.

(e) Beweisen Sie den Hinweis zu (d), d.h. zeigen Sie, dass $3^n = \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$ für belieibges $n \in \mathbb{N}_0$.

Lösung

(a) Graph (oder so ähnlich):



(b) $\mathsf{deg}(\emptyset) = 2^n - 1$: $\emptyset$ ist disjunkt zu jeder anderen Teilmenge von $[n]$, also zu allen $2^n - 1$ Teilmengen benachbart.

(c) Sei $A \subseteq [n]$ eine Menge mit $k > 0$ Elementen. Dann ist B ein Nachbar von A, falls $B \subseteq [n] \setminus A$. Damit hat A Grad 2^{n-k}.

(d) Nach Vorlesung:

$$2\,|E| = \sum_{A \subseteq [n]} \mathsf{deg}(A) = 2^n - 1 + \sum_{k=1}^{n} \binom{n}{k} 2^{n-k} = -1 + \sum_{k=0}^{n} \binom{n}{k} 1^k 2^{n-k} = 3^n - 1$$

Also $|E| = \frac{3^n - 1}{2}$.
Alternativ: Sei $\{A, B\}$ eine Kante von G_n. Dann gilt $A \cap B = \emptyset$ und $A \cup B \subseteq [n]$. D.h. $A \uplus B$ definiert eine Abbildung $f\colon [n] \to \{a, b, c\}$. Von diesen Abbildungen gibt es 3^n. Die Abbildung, die jedes Element aus $[n]$ auf c abbildet, beschreibt dabei keine Kante, da es in einem ungerichteten Graphen keine Schleifen gibt. Die verbleibenden $3^n - 1$ Abbildung beschreiben jede Kante doppelt (Vertauschen von a und b verändert Kante nicht). Insofern gibt es $\frac{3^n - 1}{2}$ Kanten.

(e) Nach der binomischen Formel gilt: $(x + y)^n = \sum_{k=0}^{n} \binom{n}{y} x^k y^{n-k}$. Mit $x = 1$ und $y = 2$ folgt die Behauptung.

Aufgabe 6 **8P**

(a) Bestimmen Sie $\varphi(83) = |\mathbb{Z}_{83}^*|$. *Hinweis*: 83 ist eine Primzahl.

(b) Berechnen Sie $38 \cdot_{83} 38$.

(c) Zeigen Sie, dass 5 ein Erzeuger von $\langle \mathbb{Z}_{83}^*, \cdot_{83}, 1 \rangle$, d.h. zeigen Sie, dass $\langle 5 \rangle = \mathbb{Z}_{83}^*$ gilt.
Hinweis: Verwenden Sie geeignet, dass $5^{10} \bmod 83 = 11$ gilt (nicht zu zeigen).

(d) Bestimmen Sie das Inverse von 15 in $\langle \mathbb{Z}_{83}^*, \cdot_{83}, 1 \rangle$ mittels des erweiterten euklidischen Algorithmus (EEA).
Hinweis: Halten Sie sich an das in den Übungen und der Vorlesung verwendete Format für die Tabellierung des EEA:

a	b	$\lfloor b/a \rfloor$	α	β
?	?	?	?	?

(e) Berechnen Sie $(264^{245}) \bmod 83$.

Lösung $p := 83$

(a) $\varphi(p) = p - 1 = 82$, da $p = 83$ prim.

(b) $38 \cdot 38 \equiv_p 38 \cdot 2 \cdot 19 \equiv_p 76 \cdot 19 \equiv_p -7 \cdot 19 \equiv_p -133 \equiv_p 33$

(c) Die möglichen Ordnungen von 5 sind die Teiler von $82 = 2 \cdot 41$, also $1, 2, 41, 82$.
Man muss daher zeigen, dass $5^k \not\equiv_{83} 1$ für $k \in \{1, 2, 41\}$, was für $k = 1, 2$ offensichtlich ist.
Bleibt $5^{41} \equiv_p (5^{10})^4 \cdot 5 \equiv_p 11^4 \cdot 5 \equiv_p 121 \cdot 121 \cdot 5 \equiv_p 38 \cdot 38 \cdot 5 \equiv_p 33 \cdot 5 \equiv_p 186 \equiv_p -1 \equiv_p 82$

(d)

a	b	$\lfloor b/a \rfloor$	α	β
15	83	5	-11	2
8	15	1	2	-1
7	8	1	-1	1
1	7	–	1	0

Also ist $-11 \equiv_{83} 72$ das multiplikative Inverse von 15 modulo 83.

(e) $264^{245} \equiv_p (264 \bmod p)^{245 \bmod p-1} \equiv_p 15^{-1} \equiv_p 72$.

Aufgabe 7 **7P**

Wie viele Möglichkeiten gibt es, 42 Studenten 8 Tutoren zuzuordnen, wenn

jedem Tutor mindestens fünf Studenten zugeordnet werden sollen und weiterhin

(a) Studenten *nicht unterschieden* werden,
   (i) Tutoren ebenfalls *nicht unterschieden* werden.
   (ii) Tutoren jedoch *unterschieden* werden.

(b) Studenten *unterschieden* werden,
   (i) Tutoren jedoch *nicht unterschieden* werden.
   (ii) Tutoren ebenfalls *unterschieden* werden.

Erinnerung: In den Tutorübungen haben Sie gesehen, dass die Anzahl aller Äquivalenzrelationen über $[n]$, welche genau λ_i Äquivalenzklassen der Größe i besitzen, gerade durch $\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\cdots(n!)^{\lambda_n}}$ gegeben ist.

In (b) reicht es, das Ergebnis als arithmetisch Ausdruck unter Verwendung der in Vorlesung behandelten Zählkoeffizienten anzugeben. Der arithmetische Ausdruck muss jedoch begründet werden!

Für (a) muss entsprechend (b) verfahren werden, es ist aber *zusätzlich* der explizite Zahlenwert anzugeben.

Lösung

(a) (i) Man ist an der Anzahl der ungeordneten Partitionen von 42 in 8 Summanden, jeder davon größer gleich 5, interessiert:

$$x_1 + x_2 + \ldots + x_7 + x_8 = 42 \text{ mit } 5 \leq x_1 \leq x_2 \ldots \leq x_8$$

Subtrahiert man von jedem x_i genau 4, dann erhält man genau die ungeordneten Partition von $42 - 8 \cdot 4 = 10$ in 8 positive ganze Zahlen, wovon es gerade $P_{10,8} = 2$ viel gibt, nämlich $(1, 1, 1, 1, 1, 1, 1, 3)$ und $(1, 1, 1, 1, 1, 1, 2, 2)$.

(ii) Man ist an den Zählvektoren $(n_1, \ldots, n_8) \in \mathbb{N}_0^8$ mit $\sum_i n_i = 42$ und $n_i \geq 5$ interessiert (n_i Anzahl der Studenten, die Tutor i zugeordnet werden), d.h. an der Anzahl der Zählvektoren $(n_1, \ldots, n_8) \in \mathbb{N}_0^8$ und $\sum_i n_i = 2$, also $\binom{2+8-1}{2} = \frac{9!}{2!7!} = 36$.

(b) (i) (Siehe TA 10.1)

Man muss [42] in 8 Mengen partitionieren, wobei jede Menge mindestens 5 Elemente enthält.

D.h. man ist an den Äquivalenzrelationen über [42] interessiert, die nur Äquivalenzklassen mit mindestens 5 Elementen besitzen, also den Typ $(\lambda_1, \lambda_2, \ldots, \lambda_{42})$ mit $\lambda_1 = \ldots = \lambda_4 = 0$, $\sum_i \lambda_i = 8$ und $\sum_i i\lambda_i = 42$ haben – (siehe Hinweis) von diesen Vektoren $\vec{\lambda}$ gibt es nach (a) gerade $P_{10,8} = 2$ viele, konkret $\lambda_5 = 7, \lambda_7 = 1$ (was in (a) $(5, 5, 5, 5, 5, 5, 5, 7)$ entspricht) und $\lambda_5 = 6, \lambda_6 = 2$ (in (a) $(5, 5, 5, 5, 5, 5, 6, 6)$).

Damit ergibt sich

$$\frac{42!}{7!(5!)^7(7!)} + \frac{42!}{6!2!(5!)^6(6!)^2}$$

(ii) Wie in (b), nur muss man jeder Teilmenge noch einen Tutor zuordnen, also (siehe auch HA 11.3)

$$\left(\frac{42!}{7!(5!)^7(7!)} + \frac{42!}{6!2!(5!)^6(6!)^2}\right) \cdot 8!$$