Technische Universität München **Winter 2016/17**
Prof. H. J. Bungartz / Dr. M. Luttenberger, J. Bräckle, K. Röhner

HA-Lösung

Diskrete Strukturen – Nachholklausur 22.04.2017

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

Aufgabe 1 — 6P

Gegeben ist die folgende aussagenlogische Formel F in den Variabeln A, B, C:

$$F = \neg(((\neg A \vee B) \wedge (A \vee \neg B)) \vee \neg C)$$

(a) Überführen Sie F in eine semantisch äquivalente aussagenlogische Formel K_F in KNF unter Verwendung des Verfahrens aus der Vorlesung basierend auf semantischen Äquivalenzen. Es reicht in jedem Schritt des Verfahrens einmal die verwendeten Äquivalenzen anzugeben.

(b) Stellen Sie das KV-Diagramm zu $\neg F$ auf und leiten Sie hiermit eine zu $\neg F$ semantisch äquivalente aussagenlogische Formel $D_{\neg F}$ in DNF her, in welcher höchstens 3 Disjunktionen vorkommen.
Verwenden Sie für das KV-Diagramm folgende Vorlage (**nicht ausfüllen!**):

	$\neg C$	C	C	$\neg C$
$\neg B$	?	?	?	?
B	?	?	?	?
	A	A	$\neg A$	$\neg A$

Lösung

(a) 1. Negation nach unten schieben vor die Variablen mittels De Morgan:

$$F \equiv \neg((\neg A \vee B) \wedge (A \vee \neg B)) \wedge \neg\neg C \equiv (\neg(\neg A \vee B) \vee \neg(A \vee \neg B)) \wedge \neg\neg C \equiv ((\neg\neg A \wedge \neg B) \vee (\neg A \wedge \neg\neg B)) \wedge \neg\neg C$$

2. Entfernen doppelter Negationen:

$$\ldots \equiv ((A \wedge \neg B) \vee (\neg A \wedge B)) \wedge C$$

3. Disjunktion im Syntaxbaum unter Konjunktion schieben mittels Distributivität:

$$\ldots \equiv ((A \wedge \neg B) \vee (\neg A \wedge B)) \wedge C \equiv ((A \vee (\neg A \wedge B)) \wedge (\neg B \vee (\neg A \wedge B))) \wedge C \equiv (((A \vee \neg A) \wedge (A \vee B)) \wedge ((\neg B \vee \neg A) \wedge (\neg B \vee B))) \wedge C$$

4. (nicht verlangt) Tautologien entfernen:

$$\ldots \equiv ((A \vee B) \wedge (\neg B \vee \neg A)) \wedge C$$

(b) KV-Diagramm zu $\neg F \equiv (\neg A \wedge \neg B) \vee (B \wedge A) \vee \neg C$

	$\neg C$	C	C	$\neg C$
$\neg B$	1	0	1	1
B	1	1	0	1
	A	A	$\neg A$	$\neg A$

Aufgabe 2 — 6P

Gegeben ist die folgende Klauselmenge in den aussagenlogischen Variablen A, B, C:

$$K = \{\{A, C\}, \{\neg A, \neg C\}, \{A, B, \neg C\}, \{\neg A, B, C\}, \{\neg B\}\}$$

(a) Zeigen Sie mittels aussagenlogischer Resolution, dass die Klauselmenge K *unerfüllbar* ist. Es reicht, eine Resolution der leeren Klausel graphisch entsprechend der Vorlesung darzustellen.

(b) Wenden Sie zum Vergleich den DPLL-Algorithmus aus der Vorlesung (mit *one-literal rule*, ohne *pure-literal rule*) auf die Klauselmenge an.
Halten Sie sich an die Literalordnung $A \prec \neg A \prec B \prec \neg B \prec C \prec \neg C$

Lösung

(a) (i) $\{a, \neg c\}$ aus $\{a, b, \neg c\}$ und $\{\neg b\}$.
(ii) $\{a\}$ aus $\{a, \neg c\}$ und $\{a, c\}$.
(iii) $\{\neg a, c\}$ aus $\{\neg a, b, c\}$ und $\{\neg b\}$.
(iv) $\{\neg a\}$ aus $\{\neg a, c\}$ und $\{\neg a, \neg c\}$
(v) $\{\}$ aus $\{a\}$ und $\{\neg a\}$.

(b) OLR mit $\neg b$:

$$\{\{a, c\}, \{\neg a, \neg c\}, \{a, \neg c\}, \{\neg a, c\}\}$$

Fallunterscheindung nach a:

(i) Fall a (OLR mit a):

$$\{\{\neg c\}, \{c\}\}$$

OLR mit c

$$\{\{\}\}$$

unerfüllbar, Backtracking.

(ii) Fall $\neg a$ (OLR mit $\neg a$):

$$\{\{\neg c\}, \{c\}\}$$

OLR mit c

$$\{\{\}\}$$

unerfüllbar, Backtracking.

K ist unerfüllbar.

Aufgabe 3 — 6P

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

$$A_0 = 2 \quad A_1 = 1 \quad A_2 = 2 \quad A_{n+3} = A_{n+2} - A_{n+1} + A_n$$

Sei $f\colon \mathbb{N}_0 \to \mathbb{N}_0$ definiert durch

$$f(n) := \begin{cases} 2 & \text{falls } n \text{ gerade} \\ 2 - (-1)^{\frac{n-1}{2}} & \text{falls } n \text{ ungerade} \end{cases}$$

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

$$A_n = f(n)$$

Der Induktionsbeweis muss entsprechend der Vorlesung und den Tutorübungen gegliedert werden!

Lösung Behauptung: $A_n = f(n)$ gilt für alle $n \in \mathbb{N}_0$.

- Induktionsbasis:
  $A_0 = 2$ nach Definition; $f(0) = 2$.
  $A_1 = 1$ nach Definition; $f(1) = 2 - (-1)^{\frac{1-1}{2}} = 2 - 1 = 1$.
  $A_2 = 2$ nach Definition; $f(2) = 2$.
- Induktionsschritt: Sei $n \in \mathbb{N}_0$ beliebig fixiert.
  - Induktionsannahme:
    Es gilt $A_k = f(k)$ für $k \in \{n, n+1, n+2\}$.
  - Induktionsbehauptung:
    Es gilt $A_{n+3} = f(n+3)$.
  - Beweis der Induktionsbehauptung:
    Nach Definition von A_{n+3} gilt:

    $$A_{n+3} = A_{n+2} - A_{n+1} + A_n$$

    Nach Induktionsannahme folgt daher:

    $$A_{n+3} = f(n+2) - f(n+1) + f(n)$$

    Falls $n = 2k$ gerade, dann gilt nach Definition von $f(\cdot)$:

    $$A_{n+3} = f(2k+2) - f(2k+1) + f(2k) = 2 - (2 - (-1)^k) + 2 = 2 - (-1)^{k+1} = 2 - (-1)^{\frac{2k+3-1}{2}} = f(2k+3) = f(n+3)$$

    Falls $n = 2k+1$ ungerade:

    $$A_{n+3} = f(2k+3) - f(2k+2) + f(2k+1) = 2 - (-1)^{k+1} - 2 + 2 - (-1)^k = 2 - (-1)^{k+1} - 2 + 2 - (-1)^k = 2 + ((-1)^k - (-1)^k) = 2 = f(2n+4)$$

    Damit gilt in allen Fällen $A_{n+3} = f(n+3)$, womit bewiesen ist, dass die Induktionsbehauptung aus der Induktionsannahme für das gewählte n logisch folgt, womit der Induktionsschritt $\forall n \in \mathbb{N}_0 \colon (A_n = f(n) \wedge A_{n+1} = f(n+1) \wedge A_{n+2} = f(n+2)) \to A_{n+3} = f(n+3)$ gültig ist.

Da die Induktionsbasis $A_0 = f(0) \wedge A_1 = f(1) \wedge A_2 = f(2)$ und der Induktionsschritt gültige Behauptungen sind, ist auch $\forall n \in \mathbb{N}_0 \colon A_n = f(n)$ gültig.

Aufgabe 4 — 4P

Wir betrachten ein Gewinnspiel, bei dem jedes Los einem 6-Tupel $(x_1, x_2, x_3, x_4, x_5, x_6) \in [5]^6$ mit Einträgen aus $[5] = \{1, 2, 3, 4, 5\}$ entspricht. Die *höchste* Zahl, welche *mindestens drei Mal* auf einem gegebenen Los vorkommt, entspricht dem Gewinn; kommt jede Zahl aus [5] höchstens zwei Mal auf dem Los vor, dann ist der Gewinn 0.

Beispiel: Das Los $(2, 3, 4, 3, 5, 3)$ hätte den Gewinn 3, das Los $(1, 2, 3, 4, 5, 5)$ den Gewinn 0.

(a) Bestimmen Sie die Anzahl aller Lose mit Gewinn 5.

(b) Bestimmen Sie die Anzahl aller Lose mit Gewinn 0.

Hinweis: Es reicht, die gesuchten Zahlenwerte als arithmetische Terme unter Verwendung der in der Vorlesung behandelten kombinatorischen Zählkoeffizienten anzugeben. Die Terme müssen jedoch ausführliche begründet und vereinfacht werden.

Erinnerung: In den Tutorübungen haben Sie gesehen, dass es genau $\frac{n!}{\lambda_1!\lambda_2!\cdots\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\cdots(n!)^{\lambda_n}}$ Äquivalenzrelationen über $[n]$ mit genau λ_i Äquivalenzklassen der Größe i gibt, falls $\sum_{i=1}^{n} i\lambda_i = n$ gilt.

Lösung

(a) Es muss mindestens drei Mal die 5 im Tupel vorkommen, die restlichen Einträge spielen dann keine Rolle mehr, da 5 das Maximum in der gegebenen Grundmenge ist. Man partitioniert daher nach der Anzahl k der Vorkommen von 5 im Tupel und wählt die entsprechende Anzahl an Positionen aus den 5 möglichen Positionen im Tupel:

$$\sum_{k=3}^{6} \binom{6}{k} 4^{6-k}$$

(b) Jede Zahl darf höchstens zwei Mal im Tupel auftreten. Minimal muss dabei mindestens eine Zahl doppelt auftreten, maximal können drei Zahlen doppelt im Tupel vorkommen. Man kann daher die Positionen anhand denen ihnen zugewiesenen Werte in Äquivalenzklassen partitionieren und nachträglich den Äquivalenzklassen ohne Wiederholung einen konkreten Wert aus [5] zuweisen:

$$\frac{6!}{4!1!(1!)^4(2!)^1} \cdot 5^{\underline{5}} + \frac{6!}{2!2!(1!)^2(2!)^2} \cdot 5^{\underline{4}} + \frac{6!}{3!(2!)^3} \cdot 5^{\underline{3}}$$

Aufgabe 5 — 3P

Mit *Graph* sei im Weiteren ein Tupel $G = (V, E)$ mit V eine endliche Menge und $E \subseteq \binom{V}{2} := \{\{u, v\} \subseteq V \mid u \neq v\}$ 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) es einen planaren Graphen mit Gradfolge $(2, 4, 4, 4, 5, 5)$ gibt.

(b) jeder Graph mit Gradfolge $(1, 1, 1, 1, 2, 2, 2, 4)$ ein Baum ist.

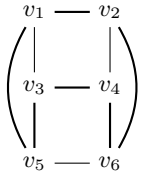
(c) es einen planaren Graph mit Gradfolge $(3, 3, 3, 3, 3, 3)$ gibt, der einen Hamilton-Kreis enthält.

Lösung

(a) Nein, die Knoten v_5, v_6 müssen zwingend mit allen Knoten (außer sich selbst jeweils) verbunden sein. Damit hat v_1 bereits Grad 2, womit v_2, v_3, v_4 noch verbunden sein müssen. Damit ist der durch $\{v_2, v_3, v_4, v_5, v_6\}$ induzierte Teilgraph isomorph zum K_5.

(b) Nein, z.B. der Baum $(1, 1, 1, 1, 4)$ und der C_3.

(c) Z.B.



mit Hamilton-Kreis $v_1, v_2, v_6, v_4, v_3, v_5, v_1$.

Aufgabe 6 — 6P

In dieser Aufgabe sind wir ausschließlich an Graphen $G = (V, E)$ interessiert, welche *alle* folgenden Eigenschaften besitzen:

- $|V| \geq 2$ ist ein positives Vielfaches von 3 und
- $E \subseteq \binom{V}{2}$ und
- je ein Drittel der Knoten hat den Grad d bzw. $2d$ bzw. $3d$ und
- G ist zusammenhängend und planar.

Zeigen Sie:

(a) Sei F die Menge der Flächen, in die G die Ebene unterteilt (inkl. der umschließenden Fläche).
Dann gilt $|F| = 2 + (d-1)\,|V|$.

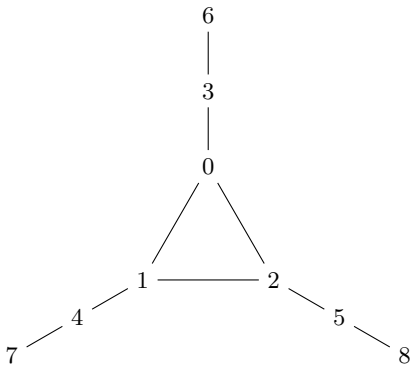
(b) Geben Sie für $|V| = 9$ und $d = 1$ einen solchen Graphen an. Es reicht, den Graphen zu zeichnen.

(c) Zeigen Sie, dass es für $d \notin \{1, 2\}$ *keinen* solchen Graphen geben kann.

Lösung

(a) Allgemein: $|E| = \frac{1}{2}\sum_{v \in |V|} \mathsf{deg}(v) = \frac{|V|}{6}(d + 2d + 3d) = d\,|V|$.
Da G zusammenhängend und planar gilt die EPF: $|F| - |E| + |V| = 2$, also $|F| = 2 + |E| - |V| = 2 + (d-1)\,|V|$.

(b) Blub:



(c) Für $d = 0$ kann der Graph nur zusammenhängend sein, wenn $|V| = 1$, was allerdings kein positives Vielfaches von 3 ist.
Es muss also $d \in \mathbb{N}$ gelten.
Da G planar: $|E| \leq 3\,|V| - 6$
Also: $d\,|V| = |E| \leq 3\,|V| - 6$ bzw. $d \leq 3 - \frac{6}{|V|}$
Mit $|V| \in 3\mathbb{N}$ gilt $\frac{6}{|V|} \in (0, 6/3]$, womit $\lfloor 3 - 6/\,|V| \rfloor \in \{1, 2\}$ und damit auch $d \in \{1, 2\}$ folgt.

Aufgabe 7 — 8P

Sei $N = 32$.

(a) Bestimmen Sie $\varphi(N)$.

(b) Bestimmen Sie die Untergruppen $\langle 3\rangle$, $\langle 29\rangle$ und $\langle 15\rangle$ bzgl. der multiplikativen Gruppe $\langle \mathbb{Z}_N^*, \cdot_N, 1\rangle$ modulo N.

(c) Bestimmen Sie das Inverse von 15 in $\langle \mathbb{Z}_N^*, \cdot_N, 1\rangle$ **mittels des erweiterten euklidischen Algorithmus**.
Hinweis: Halten Sie sich an das in den Übungen und der Vorlesung verwendete Format:

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

(d) Geben Sie eine zu $\langle \mathbb{Z}_5^*, \cdot_5, 1\rangle$ isomorphe Untergruppe der $\langle \mathbb{Z}_N^*, \cdot_N, 1\rangle$ an zzgl. entsprechendem Isomorphismus.

Lösung

(a) $\varphi(32) = 16$ – die Hälfte der Zahlen in [32] ist ungerade.

(b) Es gilt

$$\begin{aligned} 3^1 &\equiv_N 3 \\ 3^2 &\equiv_N 9 \\ 3^3 &\equiv_N 27 \equiv_N -5 \\ 3^4 &\equiv_N -15 \equiv_N 17 \\ 3^5 &\equiv_N 2 \cdot 17 + 17 \equiv_N 2 + 17 \equiv_N 19 \\ 3^6 &\equiv_N 2 \cdot 19 + 19 \equiv_N 6 + 19 \equiv_N 25 \equiv_N -7 \\ 3^7 &\equiv_N -21 \equiv_N 11 \\ 3^8 &\equiv_N 33 \equiv_N 1 \end{aligned}$$

also

$$\langle 3 \rangle = \{3, 9, 27, 17, 19, 25, 11, 1\}$$

Mit $-3 \equiv_N 29 \notin \langle 3 \rangle$ ergibt sich $\langle 29 \rangle$ aus obiger Rechnung, indem man bei den ungeraden Potenzen das Vorzeichen umdreht:

$$\langle 29 \rangle = \{29, 9, 5, 17, 13, 25, 21, 1\}$$

Weiter:

$$\begin{aligned} 15^1 &\equiv_N 15 \\ 15^2 &\equiv_N 225 \equiv_N 1 \end{aligned}$$

(c)

a	b	$\lfloor b/a \rfloor$	α	β
15	32	2	15	-7
2	15	7	-7	1
1	2	–	1	0

Also $1 = \mathsf{ggT}(15, 32) = 15 \cdot 15 - 7 \cdot 32$. Damit ist 15 sein eigenes Inverses modulo $N = 32$, was man ja in (b) bereits gesehen haben sollte.

(d) Die $\mathbb{Z}_5^*$ ist zyklisch und hat Ordnung $\varphi(5) = 4$. Sie ist damit zur additiven Gruppe $\langle \mathbb{Z}_4, +_4, 0 \rangle$ isomorph nach Vorlesung. Auch ist $\langle 3^2 \rangle$ eine zyklische Untergruppe der $\langle \mathbb{Z}_N^*, \cdot_N, 1 \rangle$ der Ordnung 4, welche somit ebenfalls zur $\langle \mathbb{Z}_4, +_4, 0 \rangle$ isomorph ist. Somit sind z.B. auch $\langle 9 \rangle \leq \mathbb{Z}_N^*$ und $\mathbb{Z}_5^*$ isomorph. Für den Isomorphismus muss man nur einen Erzeuger der $\mathbb{Z}_5^*$ auf einen Erzeuger der $\langle 9 \rangle$ (was trivialerweise z.B. 9 ist) abbilden, der Rest ergibt sich dann sofort. Da $\mathbb{Z}_4$ additiv gerade $\varphi(4) = 2$ Erzeuger hat, hat auch $\mathbb{Z}_5^*$ zwei Erzeuger. Trivial sind 1 und $-1 \equiv_5 4$ keine Erzeuger, somit sind sowohl 2 als auch 3 Erzeuger. Damit folgt:

$\mathbb{Z}_5^*$	$\to$	$\langle 9 \rangle \leq \mathbb{Z}_{32}^*$
$1 \equiv_5 2^0$	$\mapsto$	$1 \equiv_{32} 9^0$
$2 \equiv_5 2^1$	$\mapsto$	$9 \equiv_{32} 9^1$
$4 \equiv_5 2^2$	$\mapsto$	$17 \equiv_{32} 9^2$
$3 \equiv_5 2^3$	$\mapsto$	$25 \equiv_{32} 9^3$

Aufgabe 8 — 1P

Sei p eine Primzahl. Zeigen Sie: $\sum_{k=1}^{p-1} k^{p-1} \equiv_p -1$.

Erinnerung: $a \equiv_n b$ gdw. $(a \bmod n) = (b \bmod n)$.

Lösung In $\langle \mathbb{Z}_p^*, \cdot_p, 1 \rangle$ gilt $a^{p-1} \equiv_p 1$, da (1) $\left|\mathbb{Z}_p^*\right| = p - 1$ für p prim und (2) $\forall a \in \mathbb{G}\colon a^{|\mathbb{G}|} = 1$ in jeder endlichen Gruppe $\langle \mathbb{G}, \cdot, 1 \rangle$.

Damit $\sum_{k=1}^{p-1} k^{p-1} \equiv_p p - 1 \equiv_p -1$ für alle Primzahlen.