Technische Universität München (I7)
Prof. J. Esparza / Dr. M. Luttenberger

Winter 2013/14

LÖSUNG

Diskrete Strukturen – Endterm

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

Aufgabe 1 — 4P

Zeigen Sie mit Hilfe aussagenlogischer Resolution, dass folgende Formel F **gültig** ist:

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

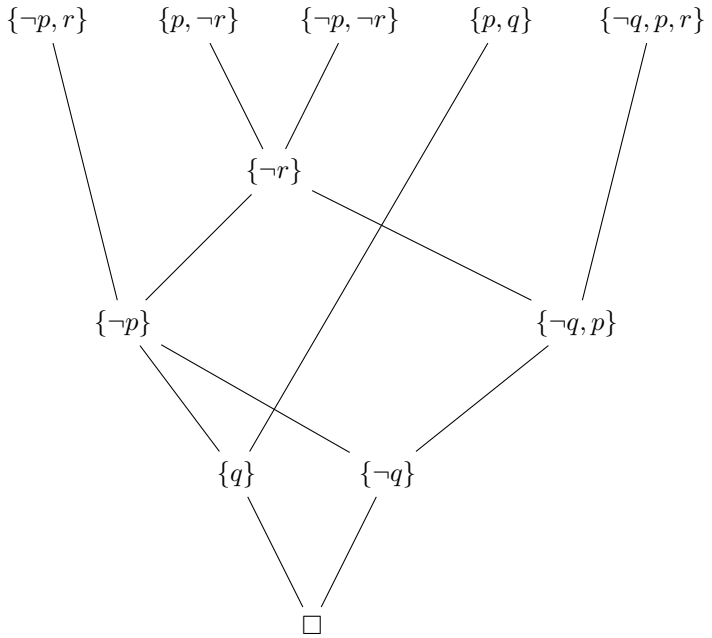
Lösung:

$$\begin{aligned} F &= (p \leftrightarrow \neg r) \vee (p \wedge r) \vee (\neg p \wedge \neg q) \vee \neg(q \rightarrow (p \vee r)) \\ &\equiv (p \wedge \neg r) \vee (\neg p \wedge \neg\neg r) \vee (p \wedge r) \vee (\neg p \wedge \neg q) \vee \neg(\neg q \vee p \vee r) \\ &\equiv (p \wedge \neg r) \vee (\neg p \wedge \neg\neg r) \vee (p \wedge r) \vee (\neg p \wedge \neg q) \vee (q \wedge \neg p \wedge \neg r) \\ \neg F &\equiv \neg((p \wedge \neg r) \vee (\neg p \wedge \neg\neg r) \vee (p \wedge r) \vee (\neg p \wedge \neg q) \vee (q \wedge \neg p \wedge \neg r)) \\ &\equiv (\neg p \vee r) \wedge (p \vee \neg r) \wedge (\neg p \vee \neg r) \wedge (p \vee q) \wedge (\neg q \vee p \vee r) \end{aligned}$$

Klauselmengendarstellung:

$$\{\{\neg p, r\}, \{p, \neg r\}, \{\neg p, \neg r\}, \{p, q\}, \{\neg q, p, r\}\}$$

Eine mögliche Resolution:



Damit ist $\neg F$ unerfüllbar, also F gültig.

Aufgabe 2 — 3P

Zeigen Sie mit Hilfe der Äquivalenzregeln aus der Vorlesung, dass $F \equiv G$ gilt.

Markieren Sie bei jedem Umformungsschritt die betroffene Teilformel. Innerhalb eines Umformungsschritt darf beliebig häufig die Assoziativität, Kommutativität und eine weitere Äquivalenz (z.B. DeMorgan) angewendet werden.

$$F := \forall x \neg \forall y \Big(\big(\neg P(x,y) \wedge \neg Q(y)\big) \vee \neg \forall z P(x,z) \Big) \qquad G := \big(\forall x \exists y P(x,y) \vee \exists y Q(y)\big) \wedge \forall x \forall z P(x,z)$$

Lösung:

$$
\begin{aligned}
F &= \forall x \neg \forall y \underline{\Big(\big(\neg P(x,y) \wedge \neg Q(y)\big) \vee \neg \forall z P(x,z) \Big)} \\
&\equiv \forall x \exists y \neg \underline{\Big(\big(\neg P(x,y) \wedge \neg Q(y)\big) \vee \neg \forall z P(x,z) \Big)} \\
&\equiv \forall x \exists y \Big(\neg \big(\neg P(x,y) \wedge \neg Q(y)\big) \wedge \underline{\neg \neg \forall z P(x,z)} \Big) \\
&\equiv \forall x \exists y \Big(\neg \big(\neg P(x,y) \wedge \neg Q(y)\big) \wedge \forall z P(x,z) \Big) \\
&\equiv \forall x \exists y \Big(\underline{\neg \big(\neg P(x,y) \wedge \neg Q(y)\big)} \wedge \forall z P(x,z) \Big) \\
&\equiv \forall x \exists y \Big(\big(\underline{\neg \neg P(x,y)} \vee \underline{\neg \neg Q(y)}\big) \wedge \forall z P(x,z) \Big) \\
&\equiv \forall x \exists y \underline{\Big(\big(P(x,y) \vee Q(y)\big) \wedge \forall z P(x,z) \Big)} \\
&\equiv \forall x \underline{\Big(\exists y \big(P(x,y) \vee Q(y)\big) \wedge \forall z P(x,z) \Big)} \\
&\equiv \forall x \underline{\exists y \big(P(x,y) \vee Q(y)\big)} \wedge \forall x \forall z P(x,z) \\
&\equiv \underline{\forall x \big(\exists y P(x,y) \vee \exists y Q(y)\big)} \wedge \forall x \forall z P(x,z) \\
&\equiv \big(\forall x \exists y P(x,y) \vee \exists y Q(y)\big) \wedge \forall x \forall z P(x,z) \\
&= G
\end{aligned}
$$

Aufgabe 3 **1P+2P+1P=4P**

Sei R ein 2-stelliges Prädikatensymbol, und f ein 1-stelliges Funktionensymbol. Weiter gelte:

$$F := \forall x \, \neg R(x,x) \; \wedge \; \forall x \, \forall y \, \forall z \, \big((R(x,y) \wedge R(y,z)) \rightarrow R(x,z) \big) \; \wedge \; \forall x \, R(x, f(x))$$

(a) Geben Sie eine zu F passende Struktur S_1 mit $[F](S_1) = 0$ an.

(b) Geben Sie eine zu F passende Struktur S_2 mit $[F](S_2) = 1$ an.

Sei nun:

$$G := F \wedge \exists x \, \exists y \, \forall z \, \neg (R(z,x) \vee R(z,y))$$

(c) Geben Sie eine zu G passende Struktur S_3 mit $[G](S_3) = 1$ an.

Lösung: *Vorbemerkung*: Am einfachsten fasst man R wie üblich als Kantenrelation eines gerichteten Graphen auf (Kante von x nach y, falls $(x,y) \in R$):

- die erste Bedingung (R irreflexiv) bedeutet dann, dass der Graph keine Schleifen besitzen darf;
- die zweite Bedingung (R transitiv) besagt, dass es zu jedem Pfad der Länge ≥ 2 eine Kante vom Start- zum Zielknoten des Pfades geben muss; insbesondere muss der Graph somit kreisfrei sein.
- f muss jedem Knoten x einen seiner Nachfolger bzgl. R zuordnen; insbesondere muss also jeder Knoten eine ausgehende Kante haben.
- Insgesamt muss es unendlich viele Knoten geben: in jede endliche Knotenmenge würde f einen Kreis induzieren, womit auf Grund der Transitivität auch eine Schleife existieren müsste, was aber der Irreflexivität widersprechen würde.

(a) Passende Struktur $S_1 = (U_1, I_1)$, unter der sich F nicht zu wahr auswertet:

Möglichkeiten: Endliches Universum; Schleifen; nicht transitiv; f bildet nicht auf Nachfolger bzgl. R ab; usw. Beispiele:

- $U_1 = \{a\}$, $R_1 = \{(a,a)\}$, $f_1(a) = a$.
- $U_1 = \mathbb{N}$, $R_1 = \{(x,x) \mid x \in \mathbb{N}\}$, $f(x) = x$.

(b) Passende Struktur $S_2 = (U_2, I_2)$, unter der sich F zu wahr auswertet:

Einfachste Möglichkeit: Man wählt $U_1 = \mathbb{N}$, $R_1 = \{(x,y) \in \mathbb{N}^2 \mid x < y\}$, $f(x) = x + 1$.

(c) Die zusätzliche Forderung $\exists x \, \exists y \, \forall z \, \neg (R(z,x) \vee R(z,y))$ besagt, es soll Elemente x und y geben, welche bzgl. R keinen Vorgänger (keine eingehende Kante) haben; es wird allerdings nicht verlangt, dass x und y verschieden sind; insofern reduziert sich die Anforderung zu $\exists x \forall z \neg R(z,x)$.

Die oben angegebene Lösung aus (b) ist also auch eine Lösung für (c).

Aufgabe 4 **3P+1P=4P**

Sei $f\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ eine Funktion mit

- $f(n,1)=f(1,m)=1$ für alle $n,m\geq 1$.
- $f(m,n)\leq f(m,n-1)+f(m-1,n)$ für alle $n,m>1$.

(a) Zeigen Sie durch eine geeignete Induktion: $f(m,n)\leq\binom{m+n-2}{m-1}$ für alle $n,m\geq 1$.

Hinweis: Unterscheiden Sie genau zwischen Induktionsbasis und Induktionsschritt. Geben Sie im Induktionsschritt die Induktionsvoraussetzung explizit an. Für die Induktion gibt es mehrere Möglichkeiten. Z.B. können Sie (müssen jedoch nicht) verwenden, dass die Relation $\prec\subseteq\mathbb{N}^2\times\mathbb{N}^2$ mit $(a,b)\prec(c,d)\leftrightarrow a\leq c\wedge b\leq d\wedge(a,b)\neq(c,d)$ wohlfundiert ist.

(b) Verwenden Sie $n!\in\Omega((n/e)^n)$ und $n!\in O(n(n/e)^n)$, um $f(m,m)\in O(m2^{2m})$ zu zeigen.

Lösung:

(a)
- Induktion nach $K:=m+n$:
  - Induktionsbeginn: Es gelte $K=2$, d.h. $m=n=1$ (da $0\notin\mathbb{N}$).

    Nach Aufgabentext gilt $f(1,1)=1$, womit sofort $f(1,1)\leq\binom{1+1-2}{1-1}=\binom{0}{0}=1$ folgt.
  - Induktionsschritt $K\to K+1$:

    Induktionsvoraussetzung: Für alle $m,n\in\mathbb{N}$ mit $m+n<K+1$ gelte $f(m,n)\leq\binom{m+n-2}{m-1}$.

    Nach Aufgabentext gilt $f(m,n)\leq f(m-1,n)+f(m,n-1)$, falls $m>1\wedge n>1$; ansonsten (d.h. $m=1\vee n=1$) gilt $f(m,n)=1$.

    Der Fall $m=1\vee n=1$ folgt analog zu Induktionsbeginn: Ohne Einschränkung gelte $m=1$; dann ergibt sich $1=f(1,n)\leq\binom{1+n-2}{0}=1$.

    Im Fall $m>1\wedge n>1$ gilt $m+(n-1)=(m-1)+n=K$, so dass die Induktionsvoraussetzung auf $f(m,n-1)$ und $f(m-1,n)$ angewendet werden kann.

    Mittels der Pascal'schen Identität ($\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$) oder durch explizites Nachrechnen folgt dann:

    $f(m,n)\leq f(m-1,n)+f(m,n-1)=\binom{m-1+n-2}{m-1-1}+\binom{m+n-1-2}{m-1}=\binom{m+n-2}{m-1}$.

    In beiden Fällen folgt somit die Behauptung aus der Induktionsvoraussetzung.
- Induktion mittels $\prec$:

  Man muss

  $$\forall(m,n)\in\mathbb{N}^2\colon\left(\forall(a,b)\prec(m,n)\colon f(a,b)\leq\binom{a+b-2}{a-1}\to f(m,n)\leq\binom{m+n-2}{m-1}\right)$$

  zeigen. Der Induktionsbeginn besteht implizit aus den Paaren $(m,n)\in\mathbb{N}^2$, die bzgl. $\prec$ keinen Vorgänger besitzen. Das ist hier nur $(1,1)$. Ansonsten läuft die Induktion quasi analog zu oben:
  - Induktionsbeginn: Es gelte $m=n=1$.

    Nach Aufgabentext gilt $f(1,1)=1$, womit sofort $f(1,1)\leq\binom{1+1-2}{1-1}=\binom{0}{0}=1$ folgt.
  - Induktionsschritt: Sei $(m,n)\in\mathbb{N}^2$ beliebig. Ohne Einschränkung gelte $(m,n)\neq(1,1)$ (siehe Induktionsbeginn).

    Induktionsvoraussetzung: Für alle $(a,b)\prec(m,n)$ gelte $f(a,b)\leq\binom{a+b-2}{a-1}$.

    Wie oben muss man wieder die Fälle $m>1\wedge n>1$ und $m=1\vee n=1$ unterscheiden, wobei der Fall $m=1\vee n=1$ identisch behandelt wird.

    Im Fall $m>1\wedge n>1$ folgt $(m-1,n)\prec(m,n)$ und $(m,n-1)\prec(m,n)$, so dass die Induktionsvoraussetzung wieder auf $f(m-1,n)$ und $f(m,n-1)$ angewendet werden darf, womit wieder mittels der Pascal'schen Identität die Behauptung folgt.

(b) Nach (a) gilt $f(m,m)\leq\binom{2m-2}{m-1}$. Es reicht somit $\binom{2m-2}{m-1}\in O(m2^{2m})$ zu zeigen.

Zuerst löst man die Landau-Symbole auf (alle Funktionen nehmen nur positive Werte an):

$$n!\in\Omega((n/e)^n):\Leftrightarrow\exists C_0\in(0,\infty)\,\exists N_0\in\mathbb{N}\,\forall n\geq N_0\colon n!\geq C_0\cdot(n/e)^n.$$
$$n!\in O(n(n/e)^n):\Leftrightarrow\exists C_1\in(0,\infty)\,\exists N_1\in\mathbb{N}\,\forall n\geq N_1\colon n!\leq C_1\cdot n(n/e)^n.$$

Damit gilt für alle $n\geq N_2=\max(N_0,N_1)$

$$0<C_0\cdot(n/e)^n\leq n!\leq C_1 n(n/e)^n.$$

Hieraus folgt für alle $n \geq N_2$:

$$\binom{2m}{m} = \frac{(2m)!}{(m!)^2} \leq \frac{C_1(2m)(2m/e)^{2m}}{C_0^2(m/e)^{2m}} = \frac{2C_1}{C_0^2} \cdot m2^{2m}.$$

D.h. es gilt $\binom{2m}{m} \in O(m2^m)$ mit den Konstanten $N_2 := \max(N_0, N_1)$ und $C_2 := \frac{2C_1}{C_0^2}$. Somit gilt also auch $\binom{2m-2}{m-2} \in O\big((m-1)2^{2m-2}\big) \subseteq O(m2^{2m})$.

Aufgabe 5 **3P+1P=4P**

Prof. Evilsparza muss eine Klausur benoten, an der $N = 100$ Studenten teilnehmen. Es sind nur die Noten $1, 2, 3, 4, 5$ möglich.

Wie viele mögliche Notenverteilungen gibt es, wenn Prof. Evilsparza

(a) nur daran interessiert ist, wie häufig eine Note erreicht wurde, wobei mindestens 30 Studenten eine 4 bekommen sollen?

(b) von jedem Studenten die Note explizit wissen möchte, wobei mindestens 30 Studenten eine 4 bekommen sollen?

Die genauen Zahlenwerte müssen nicht angegeben werden. Es reicht in allen Fällen, die gesuchten Werte mit Hilfe bekannter Zählkoeffizienten darzustellen. Die Ausdrücke sollten jedoch möglichst einfach sein, unnötig komplizierte Ausdrücke werden ggf. nicht gewertet.

Lösung:

(a) Man ist an den Zählvektoren $\{(n_1, n_2, n_3, n_4, n_5) \in \mathbb{N}_0^5 \mid n_1 + n_2 + n_3 + n_4 + n_5 = 100 \wedge n_4 \geq 30\}$ interessiert.

Die Menge lässt auch schreiben als $\{(n_1, n_2, n_3, k_4, n_5) \in \mathbb{N}_0^5 \mid n_1 + n_2 + n_3 + k_4 + n_5 = 70\}$.

Durch die übliche unäre Kodierung der Zählvektoren erhält man $\binom{70+5-1}{5-1}$.

(b) Man wählt für $k = 30 \ldots 100$ aus 100 gerade k Personen aus, welche eine 4 bekommen, für den Rest wählt man eine beliebige Note aus den vier verbleibenden Noten $\{1, 2, 3, 5\}$ aus:

$\sum_{k \geq 30} \binom{100}{k} 4^{100-k}$

Aufgabe 6 **3P+1P=4P**

(a) Wie viele reflexive Relationen $R \subseteq [10] \times [10]$ gibt es?

(b) Wie viele antisymmetrische Relationen $R \subseteq [10] \times [10]$ gibt es?

Begründen Sie Ihre Antwort. Die genauen Zahlenwerte müssen nicht angegeben werden. Es reicht in allen Fällen, die gesuchten Werte mit Hilfe bekannter Zählkoeffizienten darzustellen. Die Ausdrücke sollten jedoch möglichst einfach sein, unnötig komplizierte Ausdrücke werden ggf. nicht gewertet.

Lösung:

(a) Von den 100 möglichen Paaren, müssen die 10 Paare aus $\{(i, i) \mid i \in [10]\}$ in R enthalten sein; bei den verbleibenden 90 Paaren hat man freie Wahl: 2^{90}.

(b) Eine antisymmetrische Relation darf reflexiv sein; man muss also für jedes Element $x \in [10]$ entscheiden, ob (x, x) in R liegt; für jedes ungeordnete Paar $\{x, y\}$ $(x \neq y)$ muss man dann noch entscheiden, ob man keines der beiden oder genau eines der beiden geordneten Paare aufnimmt. Insgesamt: $2^{10} \cdot 3^{9 \cdot 10/2}$.

Aufgabe 7 **4P**

Sei X eine endliche, nicht leere Menge, und seien $\{A_1, A_2, \ldots, A_n\}$, $\{B_1, B_2, \ldots, B_n\}$ zwei beliebige Partitionen von X mit der Eigenschaft, dass alle Klassen gleich viele Elemente enthalten ($|A_1| = \ldots = |A_n| = |B_1| = \ldots = |B_n|$).

Zeigen Sie:

Es gibt eine Menge $R \subseteq X$, so dass $\forall i \in [n]\colon\ |A_i \cap R| = 1$ und $\forall i \in [n]\colon\ |B_i \cap R| = 1$.

Hinweis: Definieren Sie einen geeigneten bipartiten Graphen mit Knotenpartition $V_0 = \{A_1, \ldots, A_n\}$, $V_1 = \{B_1, \ldots, B_n\}$, so dass auf diesen Graphen der Heiratssatz aus der Vorlesung angewendet werden kann:

„Jede Frau kann genau dann mit einem ihrer Wunschkandidaten verheiratet werden, wenn je k Frauen zusammen mindestens k Wunschkandidaten haben."

Lösung: Sei $N := |X|$. Dann gilt $|A_i| = |B_j| = N/n$.

Man betrachte den bipartiten Graphen mit Knoten $V_0 = \{A_1, \ldots, A_n\}$ und $V_1 = \{B_1, \ldots, B_n\}$. Es gibt genau dann eine Kanten $\{A_i, B_j\}$, wenn $A_i \cap B_j \neq \emptyset$.

Sei $T \subseteq V_0$ eine beliebige k-elementige Teilmenge. Da $(A_1, \ldots, A_n)$ eine Partition von X ist mit $|A_i| = N/n$, überdecken die Mengen aus T genau $N/n \cdot k$ Elemente aus X. Da auch $(B_1, B_2, \ldots, B_n)$ eine Partition von X mit $|B_j| = N/n$ ist, muss T zu mindestens $|T|$ Knoten aus V_1 benachbart sein – wären höchstens $|T| - 1$ Knoten in der Nachbarschaft von T, so könnten diese nur $(|T| - 1) \cdot N/n$ Knoten überdecken. Damit gibt es nach dem Hereitssatz ein Matching. Zu jeder Paarung (A_i, B_j) des Matchings wählt man ein beliebiges $x \in A_i \cap B_j$ als Repräsentant.

Aufgabe 8 — 3P+1P=4P

(a) Wie viele verschiedene Wurzelbäume gibt es bezüglich der Knotenmenge $[n]$?

(b) Wie viele verschiedene „Wurzelwälder" gibt es bezüglich der Knotenmenge $[n]$?

Bemerkung: Ein Wurzelwald sei ein Wald von Wurzelbäumen.Überlegen Sie sich, wie man jeden Wurzelwald mit Knotenmenge $[n]$ eindeutig mit einem Wurzelbaum mit Knotenmenge $[n+1]$ und Wurzel $n+1$ identifizieren kann.

Lösung:

(a) Es gibt n^{n-2} viele Bäume über $[n]$. Um einen Wurzelbaum zu erhalten, muss man noch die Wurzel wählen: $n \cdot n^{n-2}$.

(b) Jeden Wurzelwald über der Knotenmenge $[n]$ kann man eindeutig zu einem Wurzelbaum über der Knotenmenge $[n+1]$ mit Wurzel $n+1$ machen: Man verbindet einfach $n+1$ mit den Wurzeln der Wurzelbäume des Waldes. Diese Abbildung von den Wurzelwäldern über $[n]$ in die Bäume über $[n+1]$ (bzw. Wurzelbäume mit Wurzel $n+1$) ist offensichtlich injektiv; sie ist auch surjektiv, da wir aus jedem Wurzelbaum über $[n+1]$ mit Wurzel $n+1$ einen Wurzelwald über $[n]$ durch Entfernen von $n+1$ erhalten, wobei die Kinder von $n+1$ die Wurzeln der Wurzelbäume des Wurzelwaldes werden.

Nun gibt es $(n+1)^{n+1-2}$ verschiedene Bäume über $[n+1]$. Da die Wurzel stets $n+1$ ist, gibt es somit auch $(n+1)^{n-1}$ Wurzelbäume über $[n+1]$, die gerade $n+1$ als Wurzel haben, womit wiederum folgt, dass es auch $(n+1)^{n-1}$ viele Wurzelwälder über $[n]$ gibt.

Aufgabe 9 — je 1P = 6P

Sei $G = (V, E)$ ein endlicher, einfacher Graph. Wir nehmen 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 einfachen Graphen mit der Gradfolge $(1, 2, 3, 4, 4, 5)$ gibt.

(b) es einen einfachen Graphen mit der Gradfolge $(2, 2, 3, 5, 5, 5)$ gibt.

(c) es einen Baum mit Gradfolge $(2, 3, 3, 4, 4)$ gibt.

(d) jeder einfache Graph mit Gradfolge $(1, 1, 2, 2, 2, 2)$ ein Baum ist.

(e) es einen planaren einfachen Graphen mit der Gradfolge $(4, 4, 5, 5, 5, 5)$ gibt.

(f) jeder Graph mit Gradfolge $(2, 2, 2, 2, 3, 3, 3, 3)$ 4-färbbar ist.

Lösung:

(a) Es Anzahl der Knoten mit ungeradem Knotengrad muss gerade sein bzw. der Gesamtgrad muss gerade sein.

Alternativ: Verfahren aus den Übungen zur Reduktion der Gradfolgen.

(b) Der Graph soll sechs Knoten besitzen, wobei drei davon mit jedem anderen Knoten verbunden sind. Damit muss jeder Knoten mindestens Grad 3 haben.

Alternativ: Verfahren aus den Übungen zur Reduktion der Gradfolgen.

(c) Jeder Baum hat mindestens ein Blatt, also einen Knoten vom Grad 1.

(d) Nein. Man betrachte z.B. den Graphen, der aus dem C_4 und dem Pfad mit 2 Knoten besteht.

(e) Es gilt: $2|E| = \sum_{i=1}^{6} d_i = 26$, also $|E| = 13$. Weiter gilt $|V| = 6$. Damit ist die notwendige Bedingung $|E| \leq 3|V| - 6$ nicht erfüllt.

(f) Ein solcher Graph kann keinen zu K_5 isomorphen Teilgraph enthalten: Hierfür müsste es mindestens 5 Knoten vom Grad 4 geben.

Weiterhin kann ein solcher Graph auch keinen zu $K_{3,3}$ isomorphen Teilgraph enthalten: Hierfür müsste mindestens 6 Knoten vom Grad 3 geben.

Somit ist jeder Graph mit dieser Gradfolge nach Kuratowski planar und damit auch 4-färbbar.

Alternativ: Jeder Graph mit maximalem Kontengrad D lässt sich mit $1 + D$ Farben färben (Beweis ist nicht verlangt).

Aufgabe 10 — je 1P = 3P

Wir betrachten die multiplikative Gruppe $\langle \mathbb{Z}_N^*, \cdot_N, 1 \rangle$ modulo $N := 97 \cdot 103 = 9991$.

(a) Berechnen Sie $|\mathbb{Z}_N^*|$.

(b) Berechnen Sie das Inverse von 23 in $\langle \mathbb{Z}_N^*, \cdot_N, 1 \rangle$ mit Hilfe des erweiterten euklidischen Algorithmus. Geben Sie alle relevanten Zwischenschritte an.

Hinweis: Sie dürfen $\mathrm{ggT}(5, 9) = 2 \cdot 5 + (-1) \cdot 9$ verwenden.

(c) Berechnen Sie 23^{9791} in $\langle \mathbb{Z}_N^*, \cdot_N, 1 \rangle$.

Lösung:

(a) $\varphi(N) = (97 - 1)(103 - 1) = 9792$.

(b) $a_1 = 23$, $b_1 = 9991$, $k_1 = \lfloor b_1/a_1 \rfloor = 434$.

$a_2 = 9$, $b_2 = 23$, $k_2 = \lfloor b_2/a_2 \rfloor = 2$.

$a_3 = 5$, $b_3 = 9$, $\mathrm{ggT}(5, 9) = 2 \cdot 5 + (-1) \cdot 9 \rightsquigarrow (x_3, y_3) = (2, -1)$.

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} -k_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -k_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} -434 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \end{pmatrix} = \begin{pmatrix} 2172 \\ -5 \end{pmatrix}$$

Somit $\mathrm{ggT}(a_1, b_1) = a_1 \cdot x_1 + b_1 \cdot y_1 = 23 \cdot 2172 + 9991 \cdot (-5) = 1$.

Somit $23^{-1} \equiv_N 2172$.

(c) $23^{9791} \equiv_N 23^{9791 \bmod \varphi(N)} \equiv_N 23^{-1} \equiv_N 2172$.