Technische Universität München **Winter 2017/18**
Prof. J. Esparza / Dr. M. Luttenberger, S. Sickert

Diskrete Strukturen – Klausur 14.02.2018

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

Aufgabe 1 **5P**

Gegeben sind die beiden folgenden aussagenlogischen Formeln F_1 und F_2:

$$F_1 := (p \oplus r) \wedge (q \rightarrow (p \wedge r)) \qquad F_2 := p \rightarrow (q \leftrightarrow r)$$

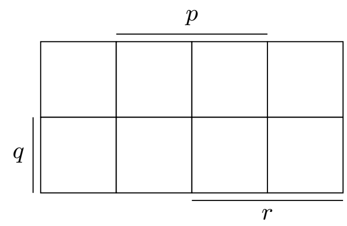
(a) Zeichnen Sie zu beiden Formeln den zugehörigen Syntaxbaum.

(b) Tabellieren Sie beide Formeln entsprechend der Vorlesung in Wahrheitstabellen. Halten Sie sich strikt an das folgende Format (sonst Punktabzug bzw. 0 Punkte):

p	q	r	$\dots$
0	0	0	$\dots$
0	0	1	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$

Entsprechend den Übungen reicht es in jeder Zeile für jede Teilformel H, nur ihre linke Teilformel auszuwerten, falls sich der Wahrheitswert von H hierdurch bereits eindeutig ergibt.

(c) Stellen Sie sowohl F_1 als auch F_2 als KV-Diagramme dar. Halten Sie sich strikt an das folgende Format (sonst Punktabzug bzw. 0 Punkte):



(d) Überführen Sie F_1 nur unter Verwendung semantischer Äquivalenzen entsprechend dem Verfahren aus der Vorlesung in eine semantisch äquivalente Formel in KNF.

Neben Kommutativität, Assoziativität und Distributivität von $\wedge$ und $\vee$, den Regeln nach de Morgan und das Entfernen von Doppelnegationen dürfen nur die folgenden Äquivalenzen benutzt werden:

$$F \rightarrow G \equiv \neg F \vee G \qquad F \leftrightarrow G \equiv (F \vee \neg G) \wedge (\neg F \vee G) \qquad F \oplus G \equiv (F \vee G) \wedge \neg(F \wedge G)$$

(e) Stellen Sie eine zu F_2 erfüllbarkeitsäquivalente Formel F_2' in KNF auf, indem Sie entsprechend der Vorlesung geeignet Hilfsvariablen einführen.

Zeigen Sie explizit, dass $F_3 := (F_2 \leftrightarrow F_2')$ erfüllbar, aber nicht gültig ist.

Erinnerung: In der Vorlesung und den Übungen haben Sie folgende Äquivalenzen hergeleitet:

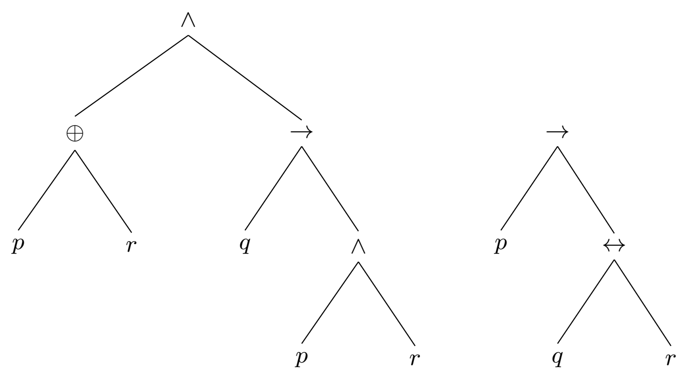
$$(A \leftrightarrow (B \rightarrow C)) \equiv (A \vee B) \wedge (A \vee \neg C) \wedge (\neg A \vee \neg B \vee C)$$

und

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

Solution

(a) Syntaxbäume:

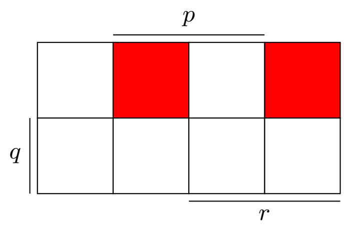


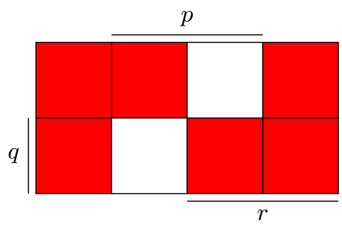
(b) Wahrheitstabellen:

p	q	r	$((p$	$\oplus$	$r)$	$\wedge$	$(q$	$\to$	$(p$	$\wedge$	$r)))$
0	0	0		0		0		1		0	
0	0	1		1		1		1		0	
0	1	0		0		0		0		0	
0	1	1		1		0		0		0	
1	0	0		1		1		1		0	
1	0	1		0		0		1		1	
1	1	0		1		0		0		0	
1	1	1		0		0		1		1	

p	q	r	$(p$	$\to$	$(q$	$\leftrightarrow$	$r))$
0	0	0		1		1	
0	0	1		1		0	
0	1	0		1		0	
0	1	1		1		1	
1	0	0		1		1	
1	0	1		0		0	
1	1	0		0		0	
1	1	1		1		1	

(c) KV-Diagramme:





(d) KNF zu F:

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

(e) Einführen von Hilfsvariablen X_1, X_2 für die inneren Knoten des Syntaxbaums:

$$F_2 \equiv_e X_1 \wedge (X_1 \leftrightarrow (p \to X_2)) \wedge (X_2 \leftrightarrow (q \leftrightarrow r))$$

Umformen mit den zwei gegebenen Äquivalenzen ergibt:

$$F_2 \equiv_e X_1 \wedge (X_1 \vee p) \wedge (X_1 \vee \neg X_2) \wedge (\neg X_1 \vee \neg p \vee X_2) \wedge (X_2 \vee q \vee r) \wedge (\neg X_2 \vee q \vee \neg r) \wedge (\neg X_2 \vee \neg q \vee r) \wedge (X_2 \vee \neg q \vee \neg r) =: F_2'$$

Erfüllende Belegung zu $F_2 \leftrightarrow F_2'$: $\beta(p) = \beta(q) = \beta(r) = 0, \beta(X_1) = \beta(X_2) = 1$

Nicht erfüllende, aber passende Belegung: $\beta(p) = \beta(q) = \beta(r) = 0, \beta(X_1) = \beta(X_2) = 0$

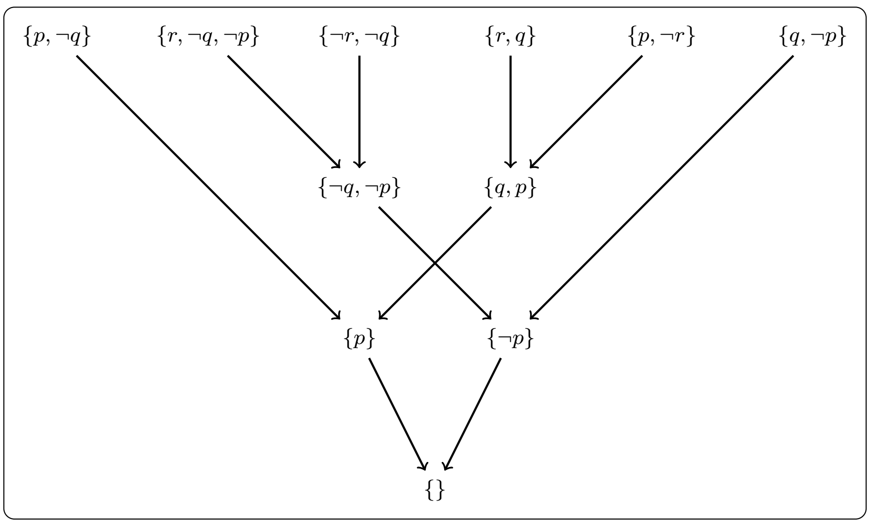
Aufgabe 2 — 3P

Verwenden Sie aussagenlogische Resolution, um zu entscheiden, ob folgende Klauselmenge unerfüllbar ist.

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

Sollte sich die leere Klausel ableiten lassen, reicht es, eine Resolution graphisch entsprechend der Vorlesung darzustellen.

Solution



Aufgabe 3 — 4P

Sei $\mathcal{G}$ die Menge der zusammenhängenden planaren Graphen, in denen alle Knoten Grad 3 haben und jede Fläche (auch die äußere Fläche) von genau 5 Kanten umrandet ist.

Zeigen Sie, dass alle Graphen in $\mathcal{G}$ dieselbe Anzahl α an Flächen haben, und bestimmen Sie diese Anzahl α.

Solution Sei $G = (V, E)$ ein solcher Graph und sei f die Anzahl der Flächen von G. Da alle Knoten Grad 3 haben gilt $2|E| = \sum_{v \in V} \mathsf{deg}(v) = 3\,|V|$. Da alle Flächen von genau 5 Kanten umrandet sind, gilt $2|E| = 5f$ und so $|V| = \frac{5f}{3}$. Damit gilt

$$f - |E| + |V| = f - \frac{5f}{2} + \frac{5f}{3} = \frac{f}{6}$$

Nach der Eulerschen Polyederformel gilt für einen planaren zusammenhängenden Graphen

$$f - |E| + |V| = 2$$

Somit gilt $\frac{f}{6} = 2$ und $\alpha = f = 12$.

Aufgabe 4 **6P**

Begründen Sie jeweils kurz (z.B. durch Angabe eines passenden konkreten Gegenbeispiels oder durch Nennung und Verwendung eines Resultats aus der Vorlesung), ob

(a) **jeder** einfache Graph mit Gradfolge $(3, 3, 3, 3, 4, 4)$ einen Hamilton-Kreis besitzt.

(b) **jeder** einfache Graph mit Gradfolge $(1, 1, 1, 2, 2, 2, 3)$ ein Baum ist.

(c) **jeder** einfache Graph mit Gradfolge $(2, 2, 2, 2, 2, 2, 6)$ dreifärbbar ist.

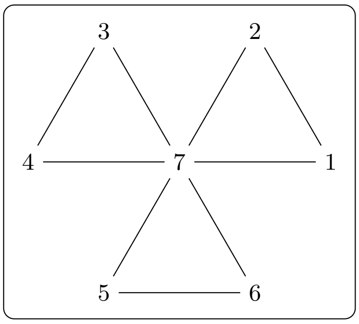
Beachten Sie, dass eine Begründung verlangt ist. Ein einfaches „ja“ oder „nein“ wird mit 0 Punkten bewertet. Sie dürfen annehmen, dass jede der genannten Gradfolgen realisierbar ist.

Solution

(a) **Ja**, da laut Vorlesung (Abschnitt: Hamiltonkreise) ein Hamilton-Kreis existiert, falls (1) $|V| \geq 3$ und (2) $\forall v \in V \colon \mathsf{deg}(v) \geq \frac{|V|}{2}$ gilt. Die gegebene Gradfolge erfüllt dieses Kriterium, da $|V| = 6$ und $\forall v \in V \colon \mathsf{deg}(v) \geq 3$, und somit hat jeder Graph mit der gegebenen Gradfolge einen Hamilton-Kreis.

(b) **Nein**, da der perfekte Ternärbaum der Höhe 1 neben einem ungerichtetem Kreis C_3 die gegebene Gradfolge hat, aber kein Baum ist.

(c) **Ja**, da alle Graphen, die die Gradfolge realisieren, zu dem folgenden Graphen isomorph sind, da der Knoten vom Grad 6 mit jedem anderen Knoten verbunden sein muss und damit dann je zwei der verbleibenden Knoten benachbart sein müssen. Man erhält also einen dreiblättriges Kleeblatt, das man direkt mit drei Farben färben kann, indem man die Knoten $\{1, 3, 5\}$ mit 1, $\{2, 4, 6\}$ mit 2 und 7 mit 3 färbt.



Aufgabe 5 **6P**

Zum Valentinstag haben Sie m Valentinskarten für Ihre n Lebensabschnittsentitäten gekauft mit $m \geq n$.

Sie sind natürlich daran interessiert, wie viele verschiedene Möglichkeiten es gibt, diese m Karten auf diese n Entitäten zu verteilen (jede Karte kann natürlich nur einmal verwendet werden; wir interessieren uns nur dafür, welche Karte schließlich bei welcher Entität landet).

Geben Sie jeweils einen möglichst einfachen arithmetischen Ausdruck (zzgl. kurzer Begründung) für die Anzahl der Möglichkeiten unter Verwendung der in der Vorlesung eingeführten Zählkoeffizienten (Binomialkoeffizienten, Stirlingzahlen, etc.) an, wenn

(a) jede Entität mindestens eine Karte erhalten soll und alle Karten versendet werden sollen und
   (i) nur Karten unterschieden werden, Entitäten jedoch ununterscheidbar sind.
   (ii) nur Entitäten unterschieden werden, Karten jedoch ununterscheidbar sind.

(b) jede Entität mindestens eine Karte erhalten soll, jedoch nicht alle Karten versendet werden müssen und nur Entitäten unterschieden werden, Karten jedoch ununterscheidbar sind.

(c) jede Entität mindestens zwei Karten erhalten soll und alle Karten versendet werden sollen und nur Karten unterschieden werden, Entitäten jedoch ununterscheidbar sind. Nehmen Sie in diesem Fall an, dass Sie $m = 17$ Valentinskarten für Ihre $n = 7$ Lebensabschnittsentitäten gekauft haben.

Erinnerung: In den Übungen haben Sie gesehen, dass die Anzahl der Äquivalenzrelationen über $[N]$, welche genau λ_i viele i-elementige Äquivalenzklassen besitzen, gerade durch $\frac{N!}{\lambda_1!\lambda_2!\cdots\lambda_N!(1!)^{\lambda_1}(2!)^{\lambda_2}\cdots(N!)^{\lambda_N}}$ gegeben ist.

Solution Jede Entität soll mindestens eine Karte erhalten (*d.h. eine Zuorndung* $f\colon [m] \hookrightarrow [n]$ *muss surjektiv sein*) und

(a) alle Karten versendet werden soll und
d.h. eine Zuorndung $f\colon [m] \to [n]$ *muss total sein*

(i) nur Karten unterschieden werden, Entitäten jedoch ununterscheidbar sind.
D.h. die Bilder sind egal, es wird nur die durch die Zuordnung f *induzierte Äquivalenzrelation auf* $[m]$ *(da total) betrachtet, welche genau* n *Klassen (da surjektiv) besitzt.*

$$\left|\left\{\{f^{-1}(1),\ldots,f^{-1}(n)\}\colon f\colon [m]\to[n] \text{ surj.}\right\}\right| = S_{m,n}$$

(ii) nur Entitäten unterschieden werden, Karten jedoch ununterscheidbar sind.
D.h. die genauen Urbilder sind egal, es wird nur die Anzahl der an jede Entität verteilten Karten gezäht (insgesamt m*, da total), d.h. man betrachtet verteilt* m *Striche auf* n *Kategorien, welche mit* $n-1$ *Kommata getrennt werden, wobei auf jede Kategorie mindestens ein Strich verteilt werden muss (da surjektiv), womit man noch effektiv* $m-n$ *Striche mit* $n-1$ *Kommata trennen muss.*

$$\left|\left\{(|f^{-1}(1)|,\ldots,|f^{-1}(n)|)\colon f\colon [m]\to[n] \text{ surj.}\right\}\right| = \left|\left\{(s_1+1,\ldots,s_n+1)\in\mathbb{N}^n\colon s_1+\ldots+s_n = m-n\right\}\right|$$
$$= \binom{m-n+n-1}{n-1} = \binom{m-1}{n-1}$$

(b) jede Entität mindestens eine Karte erhalten soll, jedoch nicht alle Karten versendet werden müssen und
D.h. nur noch partielle, aber surjektive Zuordnungen $f\colon [m]\hookrightarrow[n]$

(i) nur Entitäten unterschieden werden, Karten jedoch ununterscheidbar sind.
D.h. man zählt wieder nur, wie viele Karten jede Entität erhält, wobei man wegen der Surjektivität mindestens n *Karten/Striche, maximal jedoch* m *verteilen muss; fügt man entsprechend den Folien eine* $n+1$ *Kategorie „nicht verwendet" ein, so muss man insgesamt noch* $m-n$ *Striche auf* $n+1$ *Kategorien verteilen, welche durch* n *Kommata getrennt werden.*

$$\left|\left\{(|f^{-1}(1)|,\ldots,|f^{-1}(n)|)\colon f\colon A\to[n] \text{ surj.}, A\subseteq[m]\right\}\right| = \left|\left\{(s_1+1,\ldots,s_n+1,s_{n+1})\in\mathbb{N}_0^{n+1}\colon s_1+\ldots+s_n+s_{n+1} = m-n\right\}\right|$$
$$= \binom{m-n+(n+1-1)}{(n+1-1)} = \binom{m}{n}$$

Macht man alternativ eine Fallunterscheidung nach der Anzahl $n+k := |A| \geq n$ *der verwendeten Karten, so erhält man die folgende Summe*

$$\left|\left\{(|f^{-1}(1)|,\ldots,|f^{-1}(n)|)\colon f\colon A\to[n] \text{ surj.}, A\subseteq[m]\right\}\right| = \sum_{k=0}^{m-n}\binom{k+(n-1)}{n-1} = \binom{m-n+n}{n} = \binom{m}{n}$$

unter Verwendung der Identität aus den Folien (F41).

(c) jede Entität mindestens 2 Karten erhalten soll und alle Karten versendet werden sollen und

(i) nur Karten unterschieden werden, Entitäten jedoch ununterscheidbar sind.
Da man jeder Entität mindestens zwei Karten zuteilen soll, zählt man abweichend von (a-i) nun nur noch die Äquilanzrelationen auf $[m]$ *mit* n *Klassen, welche in jeder Klasse mindestens 2 Elemente liegen. Da die Reihenfolge der Klassen egal ist, führt dies auf die Typen* $(0,6,0,0,1,0,\ldots)$ *(d.h. 6 zweielementige, eine fünfelementige Klasse),* $(0,5,1,1,0,\ldots)$*,* $(0,4,3,0,\ldots)$

$$\frac{17!}{6!1!(2!)^6(5!)^1} + \frac{17!}{5!1!1!(2!)^5(3!)^1(4!)^1} + \frac{17!}{4!3!(2!)^4(3!)^3}$$

Anmerkung: Zunächst sieben zweielementige Klassen zu konstruieren, um dann die verbleibenden drei Karten auf die sieben Klassen zu verteilen, ist in diesem Fall problematisch, da man Klassen derselben Größe beliebig umsortieren kann, da man sie nicht unterscheidet, wofür man jedoch die genaue Anzahl λ_i an i-elementigen Klassen kennen muss.

Aufgabe 6 **8P**

Wir betrachten die zyklische Gruppe $\langle \mathbb{Z}_{47}^*, \cdot_{47}, 1\rangle$ mit der Primzahl $p = 47$.

(a) Bestimmen Sie die Ordnung von 2 und 5 in dieser Gruppe.
Hinweis: $2^{10} \equiv_p 37$ und $5^{10} \equiv_p 12$

(b) Bestimmen Sie das Inverse von 5 in $\langle \mathbb{Z}_{47}^*, \cdot_{47}, 1\rangle$ mittels des erweiterten Euklidischen Algorithmus (EEA).
Halten Sie sich strikt an das Format aus der Vorlesung, um den EEA zu tabellieren (sonst Punktabzug bzw. 0 Punkte):

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

(c) Berechnen Sie 113^{90} mod 47.

Solution

(a) Es gilt $|\mathbb{Z}_{47}^*| = \varphi(47) = 46 = 2 \cdot 23$. Somit können die Ordnungen von 2 und 5 nur $2, 23$ und 46 sein.
- Offensichtlich gilt $2^2 = 4 \not\equiv_{47} 1$.
  Da $2^{23} = 2^{10} \cdot 2^{10} \cdot 8 \equiv_{47} 37 \cdot 37 \cdot 8 \equiv_{47} (-10) \cdot (-10) \cdot 8 = 100 \cdot 8 \equiv_{47} 6 \cdot 8 = 48 \equiv_{47} 1$, hat 2 die Ordnung 23.
- Offensichtlich gilt $5^2 = 25 \not\equiv_{47} 1$.
  Da $5^{23} = 5^{10} \cdot 5^{10} \cdot 125 \equiv_{47} 12 \cdot 12 \cdot 31 \equiv_{47} 144 \cdot (-16) \equiv_{47} 3 \cdot (-16) = -48 \equiv_{47} -1 \not\equiv_{47} 1$, hat 5 die Ordnung 46.

(b)

a	b	k	s	t
5	47	9	19	-2
2	5	2	-2	1
1	2	$-$	1	0

Also ist 19 das multiplikative Inverse von 5 modulo 47, was man leicht direkt überprüft: $5 \cdot 19 = 95 = 2 \cdot 47 + 1 \equiv_{47} 1$.

(c) $113^{90} \equiv_{47} (113 \bmod 47)^{90} = 19^{90} \equiv_{47} 5^{-90} \equiv_{47} 5^{-90 \bmod 46} \equiv_{47} 5^2 = 25$.

Aufgabe 7 4P

(a) Sei P ein einstelliges Prädikatensymbol, a, b Konstantensymbole und f ein einstelliges Funktionssymbol.
Seien F, G die folgenden prädikatenlogischen Formeln mit Gleichheit:

$$F := P(a) \land \neg P(b) \land \forall x(P(x) \leftrightarrow P(f(x))) \qquad G := \forall x \forall y(f(x) = f(y) \to x = y)$$

Geben Sie zwei passende Strukturen $\mathcal{S}$ und $\mathcal{S}'$ mit unendlichem Universum an, so dass:

$$\mathcal{S} \models F \land G \qquad\qquad \mathcal{S}' \models F \land \neg G$$

(b) Geben Sie eine prädikatenlogische Formel H mit Gleichheit an, die die folgenden zwei Eigenschaften erfüllt:
- Für jedes gerade $i \in \mathbb{N}$ gibt es ein Modell von H, dessen Universum genau i Elemente hat.
- Für jedes ungerade $i \in \mathbb{N}$ gibt es kein Modell von H, dessen Universum genau i Elemente hat.

Geben Sie auch ein Modell $\mathcal{S}$ von H mit $|U_{\mathcal{S}}| = 4$ an.

Solution

(a)
- $\mathcal{S} = (\mathbb{N}_0, I)$ mit $P^{\mathcal{S}} = \{0\}$, $a^{\mathcal{S}} = 0$, $b^{\mathcal{S}} = 1$ und $f^{\mathcal{S}}(x) = x^2$.
- $\mathcal{S}' = (\mathbb{Z}, I)$ mit $P^{\mathcal{S}'} = \{0\}$, $a^{\mathcal{S}'} = 0$, $b^{\mathcal{S}'} = 1$ und $f^{\mathcal{S}'}(x) = x^2$.

(b)
- $H = \forall x((f(f(x)) = x) \land \neg(f(x) = x))$
- $\mathcal{S} = (\{a, b, c, d\}, I)$ mit $f^{\mathcal{S}}(a) = b, f^{\mathcal{S}}(b) = a, f^{\mathcal{S}}(c) = d, f^{\mathcal{S}}(d) = c$.

Erklärung: Die erste Bedingung besagt gerade, dass f selbstinvers, damit insbesondere bijektiv und damit eine Permutation von $U_{\mathcal{S}}$ mit Zykellänge ≤ 2 ist (Erinnerung an Algebra: Ordnung einer Permutation ist das kgV der Zykellängen, hier steht, dass die Ordnung maximal 2 ist, womit für die Zykellängen nur noch 1 (Fixpunkte) und 2 in Frage kommt). Die zweite Bedingung fordert, dass f keine Fixpunkte hat, insbesondere also nicht Ordnung 1 hat (also auch nicht die Identität sein kann). Damit zerfällt f in Zykel der Länge genau 2 und partitioniert $U_{\mathcal{S}}$ damit in zweielementige Äquivalenzklassen.

Aufgabe 8 4P

Wir definieren induktiv die Folge $(a_n)_{n \in \mathbb{N}_0}$ von natürlichen Zahlen mittels

$$a_0 := 2,\ a_1 := 4,\ a_2 := 7, \ \text{ und } \ a_{n+3} := 4a_{n+2} - 5a_{n+1} + 2a_n \text{ für } n \in \mathbb{N}_0.$$

Zeigen Sie durch geeignete Induktion, dass für jedes $n \in \mathbb{N}_0$ gilt:

$$a_n = 2^n + n + 1$$

Solution Beweis mittels Induktion über $n \in \mathbb{N}_0$.

Induktionsbasis:

Sei $n = 0$. Der Term $2^n + n + 1$ wertet sich zu $2^0 + 0 + 1 = 1 + 0 + 1 = 2$ aus und nach Definition $a_0 = 2$. Die Behauptung gilt für $n = 0$.
Sei $n = 1$. Der Term $2^n + n + 1$ wertet sich zu $2^1 + 1 + 1 = 2 + 1 + 1 = 4$ aus und nach Definition $a_1 = 4$. Die Behauptung gilt für $n = 1$.
Sei $n = 2$. Der Term $2^n + n + 1$ wertet sich zu $2^2 + 2 + 1 = 4 + 2 + 1 = 7$ aus und nach Definition $a_2 = 7$. Die Behauptung gilt für $n = 2$.

Induktionsschritt: Sei $n \in \mathbb{N}_0$ beliebig fixiert.
Induktionsannahme: Für alle $m \in \mathbb{N}_0$ mit $m < n + 3$ gilt die Behauptung, d.h. $a_m = 2^m + m + 1$.
Induktionsbehauptung: Es gilt auch $a_{n+3} = 2^{n+3} + (n + 3) + 1$.

Beweis der Induktionsbehauptung:

Nach Definition von a_{n+3} gilt:

$$a_{n+3} = 4a_{n+2} - 5a_{n+1} + 2a_n$$

Anwenden der Induktionsannahme auf a_{n+2}, a_{n+1}, a_n führt zu:

$$a_{n+3} = 4(2^{n+2} + n + 2 + 1) - 5(2^{n+1} + n + 1 + 1) + 2(2^n + n + 1)$$

Vereinfachen:

$$a_{n+3} = 16 \cdot 2^n + 4n + 12 - 10 \cdot 2^n - 5n - 10 + 2 \cdot 2^n + 2n + 2$$
$$a_{n+3} = 8 \cdot 2^n + n + 4 = 2^{n+3} + (n+3) + 1$$

was zu zeigen war. Damit folgt die Induktionsbehauptung aus der Induktionsannahme, womit der Induktionsschritt bewiesen ist, und damit $a_n = 2^n + n + 1$ für alle $n \in \mathbb{N}_0$ gilt.