Grundstrukturen

120 Minuten

Die Prüfung besteht aus 8 MC-Aufgaben zu je 2 Punkten und aus 4 offenen Fragen zu je 8 Punkten. Bei den MC-Aufgaben ist jeweils eine Antwort richtig. Bei den offenen Fragen gibt es natürlich auch Punkte für richtige Zwischenschritte und bei Berechnungen muss die Rechnung klar ersichtlich sein.

---

1. formale Logik. Sei $\mathbf{M}$ ein Modell einer $\mathscr{L}$-Theorie T und sei σ ein $\mathscr{L}$-Satz.
Welche der folgenden Aussagen ist *falsch*?

√ (a) Aus $\mathbf{M} \models \sigma$ folgt $\mathsf{T} \vdash \sigma$.

(b) Aus $\mathsf{T} \vdash \sigma$ folgt $\mathbf{M} \models \sigma$.

(c) Aus $\mathbf{M} \models \neg\sigma$ folgt $\mathsf{T} \nvdash \sigma$.

(d) Aus $\mathsf{T} \vdash \neg\sigma$ folgt $\mathbf{M} \not\models \sigma$.

Lösung: (a) ist die korrekte Antwort, denn die Aussage (a) ist falsch: Es gibt beispielsweise Modelle von Gruppen bei denen der Satz, "Jedes Element ist selbstinvers.", wahr ist. Er kann jedoch nicht aus der Gruppentheorie bewiesen werden, da er nicht für alle Modelle von Gruppen stimmt.

---

2. Ordinalzahlen. Welche der folgenden Aussagen sind *wahr*?

(I) $\omega \cup \{\omega\} \cup \big\{\omega \cup \{\omega\}\big\}$ ist eine Ordinalzahl.

(II) $\omega \cup \bigcup \omega$ ist eine Ordinalzahl.

(III) $\omega \cup \bigcup \{\omega\}$ ist eine Ordinalzahl.

√ (a) (I), (II), (III)

(b) (I), (II)

(c) (II), (III)

(d) (I), (III)

Lösung: (a) ist richtig, da (I), (II) und (III) wahr sind: Es ist ω eine Ordinalzahl und somit auch $\omega \cup \{\omega\} = \omega + 1$ sowie $\omega \cup \{\omega\} \cup \big\{\omega \cup \{\omega\}\big\} = \omega \cup \{\omega\} + 1$. Ausserdem ist $\bigcup \omega = \omega$, $\bigcup\{\omega\} = \omega$ und daraus folgt die Aussage.

---

3. Kardinalzahlen. Für Mengen A, B sei ${}^{A}B$ die Menge aller Funktionen $f : A \to B$ und $\mathfrak{c} = |\mathbb{R}|$.

Welche der folgenden Aussagen ist *falsch*?

✓ (a) $\left|{}^{\omega}\mathfrak{c}\right| = |\mathscr{P}(\mathfrak{c})|$

(b) $\mathfrak{c} = |\mathscr{P}(\omega)|$

(c) $\left|{}^{\omega}\omega\right| = \mathfrak{c}$

(d) $\left|{}^{\mathfrak{c}}\mathfrak{c}\right| = 2^{2^{\omega}}$

Lösung: Die korrekte Antwort ist (a), da diese Aussage falsch ist. Denn nach dem Satz von Cantor gilt $|\mathfrak{c}| < |\mathscr{P}(\mathfrak{c})|$ *und weiter ist*

$$\left|{}^{\omega}\mathfrak{c}\right| = \mathfrak{c}^{\omega} = (2^{\omega})^{\omega} = 2^{\omega\cdot\omega} = 2^{\omega} = |\mathbb{R}| = \mathfrak{c}.$$

---

4. chromatische Zahl. Sei $G = (V, E)$ der ungerichtete Graph mit $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$ und

$$\{a, b\} \in E \iff a \neq b \wedge \exists x, y \in V\, (x + y = a \wedge x \cdot y = b)\,.$$

Welche der folgenden Aussagen ist *richtig*?

✓ (a) $\chi(G) = 3$

(b) $\chi(G) = 2$

(c) $\chi(G) = 4$

(d) $\chi(G) = 5$

Lösung: (a) ist richtig, denn die Zahlen $6, 7, 8$ *bilden ein Dreieck, woraus folgt* $\chi(G) \geq 3$. *Alle anderen Kanten sind von der Form* $\{n, n+1\}$ *für* $n = 1, 2, 3, 4, 5$. *Man sieht sofort, dass G mit drei Farben färbbar ist, sodass keine zwei Elemente in* V *durch eine Kante verbunden sind.*

---

5. zyklische Gruppen. Die Gruppe

$$C_{84} \times C_{330}$$

ist isomorph zur Gruppe:

✓ (a) $C_{42} \times C_{660}$

(b) $C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \times C_7 \times C_{11}$

(c) $C_2 \times C_6 \times C_6 \times C_{25} \times C_{11}$

(d) $C_{72} \times C_{385}$

Es ist 84 *durch* 4 *teilbar und* 330 *durch* 2. *Das heisst,* $C_{84} \times C_{330}$ *ist isomorph zu einem Produkt von zyklischen Gruppen, bei denen genau eine Gruppenordnungen durch* 4 *teilbar ist und dann noch eine weitere Gruppenordnung durch* 2, *aber nicht durch* 4. *Dies wird nur von Aussage (a) erfüllt.*

---

6. endliche Körper. Welche der folgenden Aussagen ist *richtig*?

√ (a) Das Polynom $f = X^2 + 1 \subset \mathbb{F}_3[X]$ ist irreduzibel.

(b) Das Ideal $I = (X^3 + 1) \in \mathbb{F}_7[X]$ ist maximal.

(c) Sei $g = X^2 + 1 \in \mathbb{F}_5[X]$, dann ist $\mathbb{F}_5[X]/(g)$ ein Körper.

(d) Das Ideal $I = (X^3 + 1) \subset \mathbb{F}_2[X]$ ist maximal.

Lösung: Die Antwort (a) ist die korrekte Lösung, da das Polynom $X^2 + 1$ in $\mathbb{F}_3[X]$ keine Nullstellen hat und somit nicht in zwei Faktoren mit nicht-verschwindendem Grad zerlegbar ist. Alle anderen obigen Polynome haben Nullstellen, weshalb die daraus erzeugten Ideal nicht maximal sein können.

---

7. Ringe. Welche der folgenden Aussagen sind *richtig*?

(I) $51\mathbb{Z} \subset \mathbb{Z}$ ist ein maximales Ideal.

(II) Die multiplikative Gruppe von $\mathbb{Z}_9$ ist zyklisch.

(III) $12^{49} \equiv 12 \pmod{17}$

(VI) $7^{49} \equiv 7 \pmod{8}$

√ (a) (II), (III), (IV)

(b) (I), (II), (III)

(c) (II), (IV)

(d) (III), (IV)

Lösung: Die Aussage (a) ist richtig, denn $51 = 3 \cdot 17$ ist keine Primzahl und somit ist das von 51 erzeugte Ideal in $\mathbb{Z}$ nicht maximal, da $\mathbb{Z}/51\mathbb{Z}$ kein Körper ist. Die zyklische Gruppe von $\mathbb{Z}_9$ besteht aus den Elementen $1, 2, 4, 5, 7, 8$ und wird durch 2 und 5 erzeugt. Die beiden Kongruenzen folgen aus dem Euler'schen Satz, da $12, 17$ sowie $7, 8$ teilerfremd sind und $\varphi(17) = 16$ sowie $\varphi(8) = 4$ gilt.

---

8. formale Potenzreihen. Welche der folgenden Gleichungen ist *falsch*?

✓ (a) $D_{\log}\left(\frac{1-z^2}{1-z}\right) = \frac{-1}{1+z}$

(b) $D_{\log}\left(\sum_{n\in\mathbb{N}} z^n\right) = \sum_{n\in\mathbb{N}} z^n$

(c) $D_{\log}\left(\prod_{k\in\mathbb{N}} (1+z^{2^k})\right) = \sum_{n\in\mathbb{N}} z^n$

(d) $\frac{1-z^2}{(1+z)^2} = 1 + 2\cdot\sum_{n\in\mathbb{N}} (-z)^{n+1}$

Lösung: Die Aussage (a) ist die korrekte Lösung, da diese Aussage falsch ist. Denn es gilt

$$D_{\log}\left(\frac{1-z^2}{1-z}\right) = D_{\log}(1+z) = \frac{1}{1+z}$$

Die anderen Identitäten sind alle wahr (vergleiche auch mit den Lösungen der Probeprüfung).

9. *Logik.* Sei $\mathscr{L} = \{\mathtt{c}, \mathtt{R}\}$ eine Signatur, wobei $\mathtt{c}$ ein Konstantensymbol und $\mathtt{R}$ ein 2-stelliges Relationssymbol ist. Weiter sei T eine $\mathscr{L}$-Theorie, welche wie folgt definiert ist:

$$\mathsf{T} = \Big\{ \forall x \forall y \Big(\mathtt{R}xy \to \big(x = y \vee (x = \mathtt{c} \wedge y \neq \mathtt{c}) \big) \Big) \Big\}$$

(a) *(4 Punkte)* Konstruiere ein Modell $\mathbf{M} \models \mathsf{T}$ mit einem 4-elementigen Bereich, sodass gilt:

$$\mathbf{M} \models \forall x \forall y \big(\mathtt{R}xy \to y = \mathtt{c} \big)$$

(b) *(4 Punkte)* Konstruiere (bis auf Isomorphie) alle Modelle $\mathbf{M} \models \mathsf{T}$ mit einem 3-elementigen Bereich, für die gilt:

$$\mathbf{M} \models \forall x \forall y \big(\mathtt{R}xy \to \mathtt{R}yx \big)$$

Lösung:

(a) Seien $\mathtt{c}^{\mathbf{M}}, \alpha, \beta, \gamma$ die 4 verschiedenen Elemente des Bereichs eines Modells $\mathbf{M}$. Betrachte zuerst zwei verschiedene Elemente $x, y \in \{\mathtt{c}^{\mathbf{M}}, \alpha, \beta, \gamma\}$. Da $x = \mathtt{c}^{\mathbf{M}} \wedge y \neq \mathtt{c}^{\mathbf{M}}$ und $y = \mathtt{c}^{\mathbf{M}}$ nicht gleichzeitig gelten können, gilt also $\neg \mathtt{R}xy$, wenn $x \neq y$. Und falls $x = y$, so gilt wegen $y = \mathtt{c}^{\mathbf{M}}$ und der Transitivität des logischen Symbols Gleichheit auch $x = \mathtt{c}^{\mathbf{M}}$. Somit können höchstens die zwei Modelle $\mathbf{M}_1$ und $\mathbf{M}_2$ mit den jeweiligen Relationen $\mathtt{R}_1, \mathtt{R}_2$ und ihren Relationstabellen

$\mathtt{R}_1$	$c^{\mathbf{M}_1}$	α_1	β_1	γ_1
$c^{\mathbf{M}_1}$				
α_1				
β_1				
γ_1				

$\mathtt{R}_2$	$c^{\mathbf{M}_2}$	α_2	β_2	γ_2
$c^{\mathbf{M}_2}$	$\times$			
α_2				
β_2				
γ_2				

existieren. Tatsächlich gilt $\mathbf{M}_i \models \mathsf{T}$ und $\mathbf{M}_i \models \forall x \forall y \big(\mathtt{R}xy \to y = \mathtt{c} \big)$ für $i = 1, 2$.

(b) Sei $c^{\mathbf{M}_i}, \alpha_i, \beta_i$ der Bereich von $\mathbf{M}_i$ mit Relationssymbol $\mathtt{R}_i$, wobei die Elemente $c^{\mathbf{M}_i}, \alpha_i, \beta_i$ paarweise verschieden sind. Dann bedeutet $\mathbf{M}_i \models \forall x \forall y \big(\mathtt{R}_i xy \to \mathtt{R}_i yx \big)$, dass $\mathtt{R}_i$ symmetrisch sein muss. Da die Bedingung $x = \mathtt{c} \wedge y \neq \mathtt{c}$ nicht symmetrisch ist, kann $\mathtt{R}_i xy$ für $x, y \in \{c^{\mathbf{M}_i}, \alpha_i, \beta_i\}$ nur gelten, wenn $x = y$ gilt. Wir finden somit die folgenden nicht-isomorphen Modelle $\mathbf{M}_i$:

$\mathtt{R}_1$	$c^{\mathbf{M}_1}$	α_1	β_1
$c^{\mathbf{M}_1}$			
α_1			
β_1			

$\mathtt{R}_2$	$c^{\mathbf{M}_2}$	α_2	β_2
$c^{\mathbf{M}_2}$	$\times$		
α_2			
β_2			

$\mathtt{R}_3$	$c^{\mathbf{M}_1}$	α_3	β_3
$c^{\mathbf{M}_1}$			
α_3		$\times$	
β_3			

$\mathtt{R}_4$	$c^{\mathbf{M}_2}$	α_4	β_4
$c^{\mathbf{M}_2}$	$\times$		
α_4		$\times$	
β_4			

$\mathtt{R}_5$	$c^{\mathbf{M}_1}$	α_5	β_5
$c^{\mathbf{M}_1}$			
α_5		$\times$	
β_5			$\times$

$\mathtt{R}_6$	$c^{\mathbf{M}_2}$	α_6	β_6
$c^{\mathbf{M}_2}$	$\times$		
α_6		$\times$	
β_6			$\times$

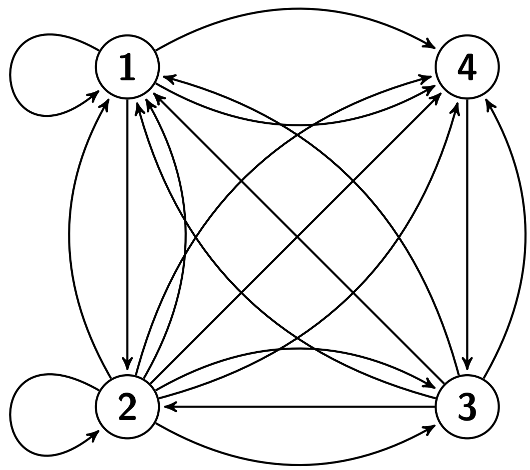
,

Ausserdem gilt $\mathbf{M}_i \models \mathsf{T}$ und $\mathbf{M}_i \models \forall x \forall y \big(\mathtt{R}_i xy \to \mathtt{R}_i yx \big)$ für $i = 1, 2, 3, 4, 5, 6$.

---

10. *Graphentheorie.*

(a) *(4 Punkte)* Gegeben sei der folgende Digraph G:



Wie viele verschiedene Pfeilfolgen der Länge 4 gibt es vom Knoten 3 zum Knoten 1?

(b) *(4 Punkte)* Ergänze die folgende (unvollständige) zyklische Folge zu einer De Bruijn-Folge der Länge 16, und zwar auf alle möglichen Arten:

$$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad . \quad . \quad . \quad . \quad . \quad .$$

Lösung:

(a) *Die Adjazenzmatrix von G ist*

$$A = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & 2 & 3 \\ 3 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Die Anzahl Kanten vom Knoten 3 *zum Knoten* 1 *entspricht dem Koeffizient* $a := a_{31}^{[4]} \in \mathbb{N}$. *Damit wir diesen Koeffizienten von* A^4 *bestimmen können, gehen wir wie folgt vor: Wir berechnen zuerst die dritte Zeile und die erste Spalte von* A^2*:*

$$\begin{pmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & 2 & 3 \\ 3 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & 2 & 3 \\ 3 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & * & * & * \\ 10 & * & * & * \\ 5 & 4 & 3 & 9 \\ 3 & * & * & * \end{pmatrix}$$

Wenn wir nun das Skalarprodukt vom dritten Zeilenvektor von A^2 *mit dem ersten Spaltenvektor von* A^2 *berechnen, dann bekommen wir schliesslich die Gleichung*

$$a_{31}^{[4]} = 5 \cdot 3 + 4 \cdot 10 + 3 \cdot 5 + 9 \cdot 3 = 97.$$

Also gibt es genau 97 *Pfeilfolgen vom Knoten* 3 *zum Knoten* 1.

(b) *Bei dieser Aufgabe gibt es verschiedene Möglichkeiten, wie man vorgehen kann. Beispielsweise können wir diese mit Graphentheorie lösen: Sei* $G_4 = (V, E)$ *mit*

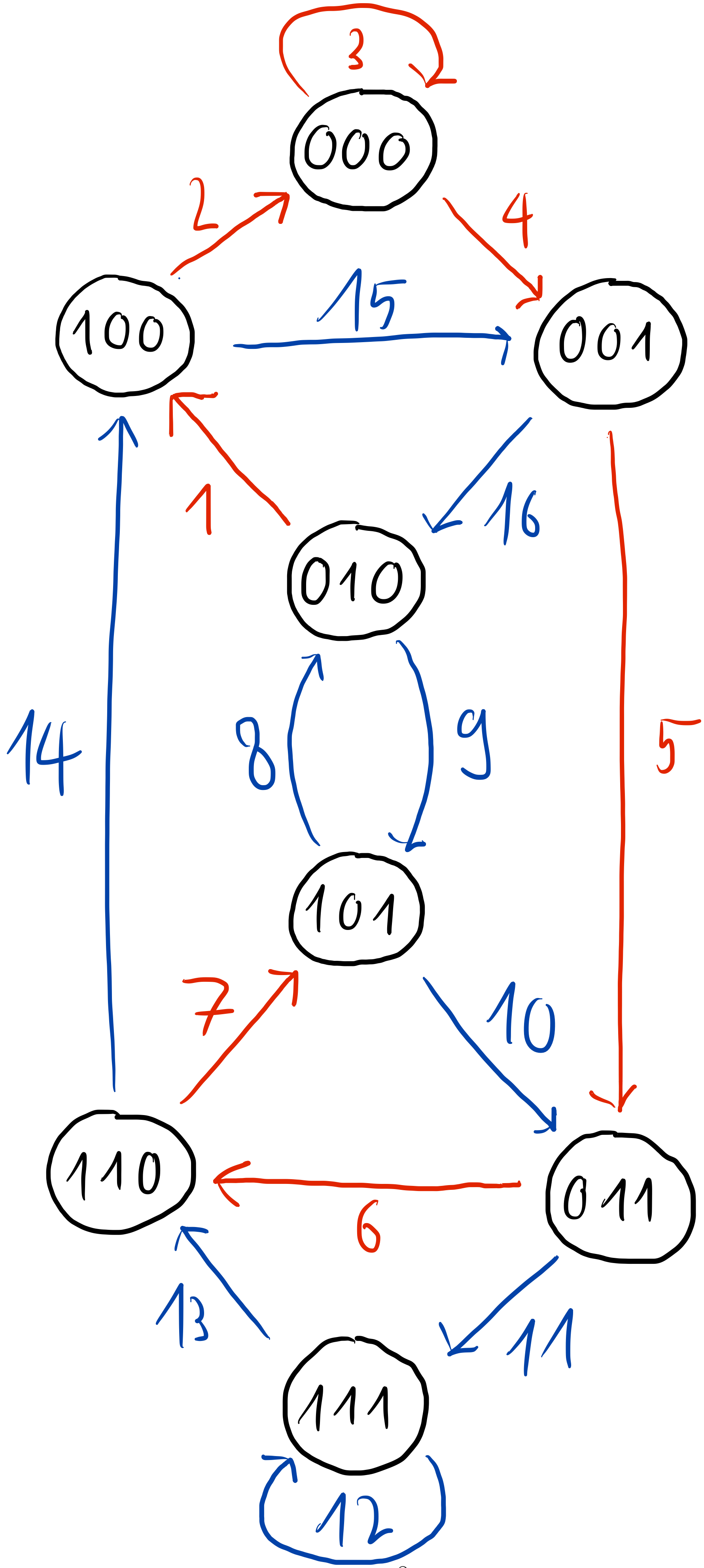
$$\begin{aligned} V &:= \{\langle b_1, b_2, b_3 \rangle : b_i \in \{0, 1\}\}, \\ E &:= \big\{\big\langle \langle b_1, b_2, b_3 \rangle, \langle b_2, b_3, b_4 \rangle \big\rangle : \langle b_1, b_2, b_3 \rangle, \langle b_2, b_3, b_4 \rangle \in V\big\} \end{aligned}$$

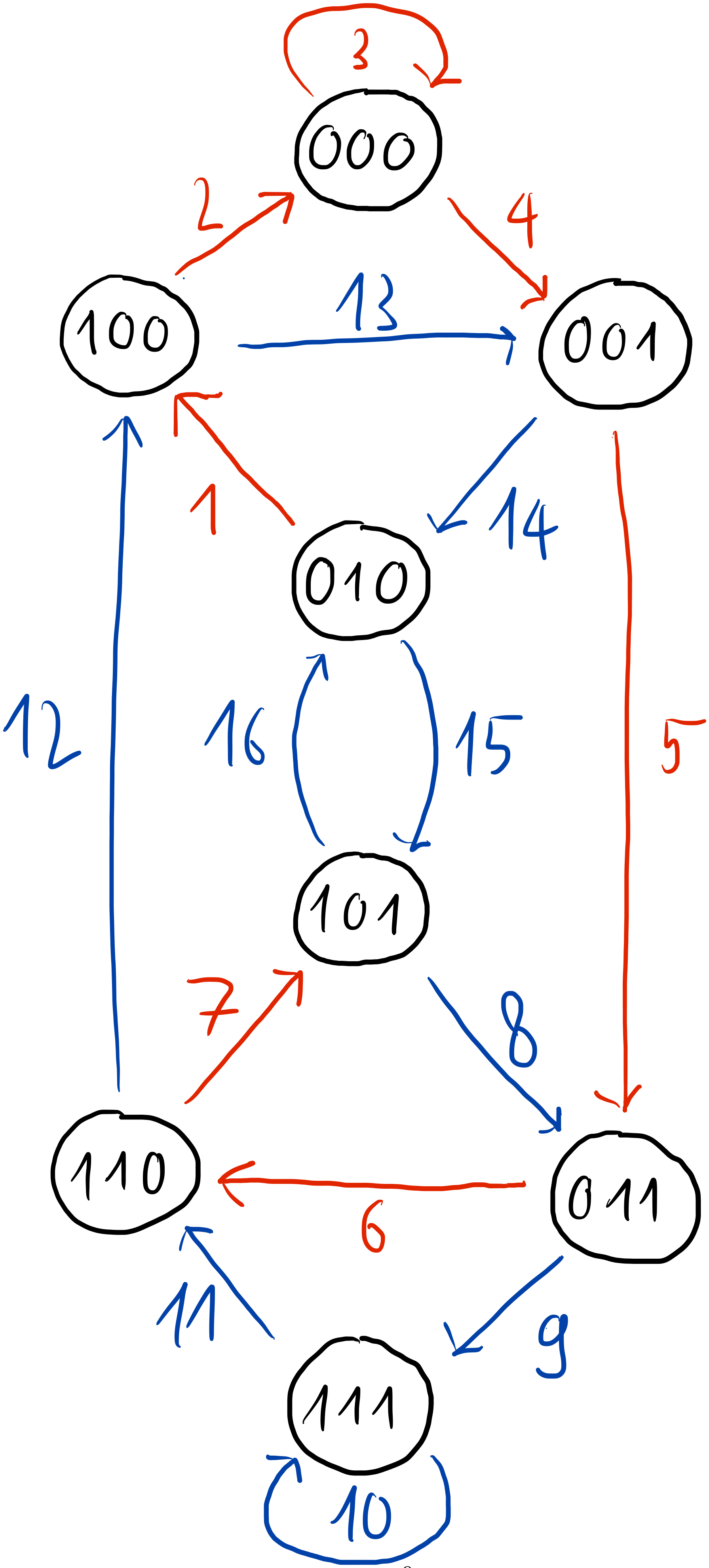
Aus der Vorlesung wissen wir, dass alle De Bruijn-Folgen der Länge 2^4 *einem eindeutigen Euler'schen Pfeilzug in* G_4 *entsprechen. Da wir die ersten* 10 *Ziffern der De Bruijn-Folge bereits kennen, wissen wir, dass der Weg in den Bildern unten rot eingezeichnet sicher im zugehörigen Euler'schen Pfeilzug vorkommen muss. Des Weiteren sehen wir sehr schnell, dass es genau zwei Möglichkeiten gibt, wie wir den Pfeilzug vervollständigen können. Somit gibt es genau die zwei Lösungen wie unten in den Bildern:*

$$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0$$

und

$$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1$$


000
100
001
010
101
110
011
111
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16


000
100
001
010
101
110
011
111
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

Alternativ kann man diese Aufgabe auch mit logischem Schlussfolgern lösen. Dazu sei $(a_n)_{n=1,\ldots 16}$ die gegebene De Bruijn-Folge. Wir können nun wie folgt vorgehen, um die weiteren Folgenglieder zu finden:

- *Es muss gelten $a_{13} = 1$, denn sonst kommt die Sequenz $\langle 1, 1, 1, 1\rangle$ nirgends vor.*

  $$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad . \quad . \quad \color{red}{1} \quad . \quad . \quad .$$

  Es muss auch gelten $a_{12} = 1$. Denn falls $a_{12} = 0$, dann muss die Sequenz $\langle 1, 1, 1, 1\rangle$ bei den letzten vier Ziffern vorkommen und da es genau 8 Nullen und Einsen in der Bruijn-Folge gibt, wäre dann auch $a_{11} = 0$. Das geht aber nicht, da die Sequenz $\langle 0, 1, 0, 0\rangle$ dann doppelt in der De Bruijn-Folge vorkommen würde. Wir haben also

  $$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad . \quad \color{red}{1} \quad 1 \quad . \quad . \quad .$$

- *Nimm nun an $a_{11} = 0$, dann muss gelten $a_{14} = 1$ und $a_{15} = 1$, damit $\langle 1, 1, 1, 1\rangle$ einmal in der De Bruijn-Folge vorkommt. Dann enthält die unvollständige De Bruijn-Folge bisher genau 8 Einsen und 7 Nullen. Folglich muss für die letzte fehlende Zahl der De Bruijn-Folge gelten $a_{16} = 0$ und somit haben wir den Lösungskandidaten:*

  $$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad \color{red}{0} \quad 1 \quad 1 \quad \color{red}{1} \quad \color{red}{1} \quad \color{red}{0}$$

- *Falls $a_{11} = 1$, dann wäre $a_{14} = 0$, denn sonst würde die Folge $\langle 1, 1, 1, 1\rangle$ zweimal vorkommen. Da die Folge $\langle 1, 1, 0, 0\rangle$ noch nicht vorkommt, muss gelten $a_{15} = 0$ und schlussendlich $a_{16} = 1$, damit die De Bruijn-Folge dieselbe Anzahl Einsen und Nullen hat. Wir erhalten also noch einen zweiten Lösungskandidaten:*

  $$0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad \color{red}{1} \quad 1 \quad 1 \quad \color{red}{0} \quad \color{red}{0} \quad \color{red}{1}$$

  Wir sehen, dass die beiden obigen Kandidaten die einzigen möglichen Vervollständigungen der gegebenen De Bruijn-Folge sind. Folglich haben wir alle Lösungen gefunden.

---

11. *Modulorechnen.* Finde mit dem verallgemeinerten Euklid'schen Algorithmus eine ganze Zahl m mit $1 \leq m \leq 155$ für die gilt:

$$(113^m)^{13} \equiv 113^{14} \pmod{155}$$

Lösung: Da $155 = 5 \cdot 31$ *mit* $5 \nmid 113$ *und* $31 \nmid 113$ *sind* 113 *und* 155 *teilerfremd. Ausserdem gilt* $\varphi(155) = \varphi(5) \cdot \varphi(31) = 4 \cdot 30 = 120$*. Das heisst, mit dem Euler'schen Satz folgt* $113^{120} \equiv 1 \pmod{155}$*. Das impliziert, dass die obere Kongruenz sicher dann erfüllt ist, wenn gilt*

$$13 \cdot m \equiv 14 \pmod{120}.$$

Diese Kongruenz ist äquivalent zu

$$13 \cdot m' \equiv 1 \pmod{120}$$

für $m' = m - 1$*. Wir verwenden nun den* vEA*:*

$$\begin{aligned} 120 &= 9 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

		9	*4*	*3*
0	**1**	*9*	*37*	*120*
1	**0**	*1*	*4*	*13*

Es gilt also $13 \cdot 37 - 120 \cdot 4 = 1$*. Also gilt auch* $13 \cdot 37 \equiv 1 \pmod{120}$*. Wähle also* $m' = 37$ *und somit ergibt sich* $m = 38$*. Somit erfüllt* $m = 38$ *auch* $(113^m)^{13} \equiv 113^{14} \pmod{155}$ *mit* $1 \leq m \leq 155$*.*

---

12. ***endliche Geometrie.*** Die 49 Elemente $\langle x, y\rangle \in \mathbb{F}_7 \times \mathbb{F}_7$ seien die Punkte der *endlichen Koordinatenebene* E_{49}.
Für alle $a, b, c \in \mathbb{F}_7$ mit $a \neq 0$ definiert die Menge

$$g(b, c) := \big\{\langle x, y\rangle \in E_{49} : y = bx + c\big\}$$

eine *Gerade* und

$$p(a, b, c) := \big\{\langle x, y\rangle \in E_{49} : y = ax^2 + bx + c\big\}$$

eine *Parabel* in E_{49}.

(a) *(1 Punkt)* Wie viele Punkte hat die Parabel $p(\bar{2}, \bar{3}, \bar{5})$?

(b) *(3 Punkte)* Berechne die Schnittpunkte der Parabel $p(\bar{2}, \bar{3}, \bar{5})$ mit der Geraden $g(\bar{4}, \bar{1})$.

(c) *(4 Punkte)* Gibt es eine Gerade oder eine Parabel, welche durch die 3 Punkte $(\bar{2}, \bar{0}), (\bar{1}, \bar{3}), (\bar{6}, \bar{2})$ geht? Begründen Sie Ihre Antwort.

Lösung:

(a) Für $a, b, c \in \mathbb{F}_7$ gibt es für jede Wahl von $x \in \mathbb{F}_7$ ein wohldefiniertes $y = ax^2 + bx + c$. Das heisst, jede Parabel $p(a, b, c)$ besitzt genau 7 Punkte.

(b) Der Schnittpunkt $\langle x, y\rangle$ von $p(\bar{1}, \bar{2}, \bar{3})$ und $g(\bar{4}, \bar{1})$ muss die beiden Gleichungen

$$\begin{aligned} y &= \bar{2}x^2 + \bar{3}x + \bar{5} \\ y &= \bar{4}x + \bar{1} \end{aligned}$$

erfüllen. Setzt man y der zweiten Gleichung in die erste ein (oder umgekehrt), so erhält man

$$\bar{2}x^2 + \bar{3}x + \bar{5} = \bar{4}x + \bar{1}.$$

Multipliziert man mit $\bar{4}$ und subtrahiert danach $\bar{2}x + \bar{4}$ auf beiden Seiten der obigen Gleichung, so erhält man

$$x^2 + \bar{3}x + \bar{2} = 0.$$

Da $x^2 + \bar{3}x = (x + \bar{5})^2 - \bar{4}$, können wir auf beiden Seiten der oberen Gleichung mit $\bar{2}$ addieren und erhalten

$$(x + \bar{5})^2 = \bar{2}.$$

Nun hat $\bar{2}$ in $\mathbb{F}_7$ die Wurzeln $\bar{3}$ und $\bar{4}$, also erhalten wir die beiden Gleichungen

$$\begin{aligned} x + \bar{5} &= \bar{3} \\ x + \bar{5} &= \bar{4}. \end{aligned}$$

Daraus lässt sich nun $x_1 = \bar{5}$ und $x_2 = \bar{6}$ berechnen. Setzt man diese Werte für x in die Geradengleichung von $g(\bar{4}, \bar{1})$ ein, so bekommt man $y_1 = \bar{0}$ und $y_2 = \bar{4}$. Das heisst, die Schnittpunkte von $p(\bar{1}, \bar{2}, \bar{3})$ und $g(\bar{4}, \bar{1})$ sind $\langle \bar{5}, \bar{0}\rangle$ und $\langle \bar{6}, \bar{4}\rangle$.

(c) Wir setzten die drei Punkte in die allgemeine Parabelgleichung $y = ax^2 + bx + c$ ein und erhalten drei verschiedene lineare Gleichungen mit $a, b, c \in \mathbb{F}_7$:

$$\begin{aligned} \bar{4}a + \bar{2}b + c &= \bar{0} \\ a + b + \bar{c} &= 3 \\ a + \bar{6}b + \bar{c} &= 2 \end{aligned}$$

Subtrahiert man die zweite von der dritten Gleichung, so erhält man $\bar{5}b = \bar{2} - \bar{3} = \bar{6}$*, wobei wir mit* $\bar{3}$ *multiplizieren können und dann bekommen wir* $b = \bar{4}$*. Subtrahieren wir die zweite von der ersten Gleichung und setzten dort* $b = \bar{4}$ *ein, so erhalten wir* $\bar{3}a + \bar{4} = -\bar{3}$*. Addieren wir auf beiden Seiten dieser Gleichung mit* $\bar{3}$*, so erhalten wir* $\bar{3}a = \bar{0}$ *und somit auch* $a = \bar{0}$*. Subtrahieren wir nun von der ersten Gleichung* $\bar{4}a + \bar{2}b$ *und setzten wir* $a = \bar{0}$ *und* $b = \bar{4}$ *ein, so erhalten wir schliesslich* $c = -\bar{2} \cdot \bar{4} = \bar{6}$*. Da* $a = \bar{0}$ *gilt, gibt es also keine Parabel, die durch die obigen drei Punkte geht. Hingegen liegen die drei Punkte offenbar auf der Geraden* $g(\bar{4}, \bar{6})$*.*