D-MATH PRÜFUNG FS 2022
Prof. Dr. Lorenz Halbeisen

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 T eine $\mathscr{L}$-Theorie und sei σ ein $\mathscr{L}$-Satz.
Welche der folgenden Aussagen ist *falsch*?

√ (a) Gilt $\mathsf{T} \nvdash \sigma$ und $\mathsf{T} \nvdash \neg\sigma$, so ist T inkonsistent.

(b) Gilt $\mathsf{T} \nvdash \sigma$, so existiert immer ein Modell $\mathbf{M} \models \mathsf{T}$ mit $\mathbf{M} \models \neg\sigma$.

(c) Gilt $\mathsf{T} \vdash \sigma$ und $\mathsf{T} \vdash \neg\sigma$, so existiert kein Modell $\mathbf{M} \models \mathsf{T}$.

(d) Gilt $\mathsf{T} \nvdash \neg\sigma$, so gibt es ein Modell $\mathbf{M} \models \mathsf{T} + \sigma$.

Lösung: (a) ist die korrekte Antwort, denn die Aussage (a) ist falsch: Wäre T inkonsistent, so gäbe es eine $\mathscr{L}$-Formel φ, sodass $\mathsf{T} \nvdash \varphi \wedge \neg\varphi$. Daraus könnte man mit $\mathsf{L}_3, \mathsf{L}_4, \mathsf{L}_9$ und Modus Ponens auch zeigen, dass $\mathsf{T} \nvdash \sigma$ und $\mathsf{T} \nvdash \neg\sigma$ gilt.

---

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

(I) Sind α und β Ordinalzahlen und gilt $\alpha \in \beta$, so ist $\alpha \subseteq \beta$.

(II) $\{\emptyset, \{\{\emptyset\}, \emptyset\}\}$ ist eine Ordinalzahl.

(III) $\bigcup(\omega \cup \{\omega\}) = \omega$

(IV) Ist α eine Ordinalzahl, so ist $\bigcap \alpha = \emptyset$.

√ (a) (II)
(b) (III)
(c) (I), (III)
(d) (II), (IV)

Lösung: (a) ist richtig, da (II) falsch und (IV) wahr ist. Die Menge bei (II) ist nämlich nicht transitiv. Hingegen ist der Durchschnitt einer Ordinalzahl leer, da die Ordinalzahl entweder selbst leer ist oder die leere Menge als Element enthält.

---

3. Kardinalzahlen. Für Mengen A, B sei ${}^{A}B$ die Menge aller Funktionen $f : A \to B$ und $\mathscr{P}(A)$ bezeichnet die Potenzmenge von A.

Welche der folgenden Aussagen ist *falsch*?

√ (a) $\left|{}^{\mathbb{Q}}\mathbb{R}\right| = |\mathscr{P}(\mathbb{R})|$

(b) $|\mathbb{R}| = |\mathscr{P}(\mathbb{Q})|$

(c) $\left|{}^{\mathbb{N}}\mathbb{N}\right| = |\mathscr{P}(\mathbb{N})|$

(d) $\left|{}^{\mathbb{R}}\mathbb{R}\right| = |\mathscr{P}(\mathbb{R})|$

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

$$\left|{}^{\mathbb{Q}}\mathbb{R}\right| = \left|{}^{\mathbb{N}}\mathbb{R}\right| = |\underbrace{\mathbb{R} \times \mathbb{R} \times \ldots}_{\omega-\text{mal}}| = \mathfrak{c}^{\omega} = (2^{\omega})^{\omega} = 2^{\omega\cdot\omega} = 2^{\omega} = |\mathbb{R}|.$$

---

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

$$\{a, b\} \in E \iff \text{ggT}(a, b) = 1.$$

Welche der folgenden Aussagen ist *richtig*?

√ (a) $\chi(G) = 4$

(b) $\chi(G) = 3$

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

(d) $\chi(G) = 6$

Lösung: (a) ist richtig, denn die Zahlen $1, 2, 3, 5$ *sind alle paarweise teilerfremd und somit gilt* $\chi(G) \geq 4$. *Da* $2, 4, 6$ *alle paarweise nicht teilerfremd sind, können wir dieselbe "Farbe" für diese Zahlen wählen. Es gilt also* $\chi(G) = 4$.

---

5. zyklische Gruppen. Die Gruppe

$$C_{210} \times C_{900}$$

ist *nicht* isomorph zur Gruppe:

√ (a) $C_5 \times C_7 \times C_{60} \times C_{90}$

(b) $C_6 \times C_{25} \times C_{35} \times C_{36}$

(c) $C_4 \times C_5 \times C_6 \times C_7 \times C_9 \times C_{25}$

(d) $C_{30} \times C_{6300}$

Lösung: 25 *teilt* 900 *aber keine Ordnung der Gruppen* C_5, C_7, C_{60}, C_{90}. *Somit kann* $C_{210} \times C_{900}$ *nicht zu* $C_5 \times C_7 \times C_{60} \times C_{90}$ *isomorph sein und die Aussage (a) ist falsch, also ist sie die korrekte Antwort.*

---

6. endliche Körper. Welche der folgenden Aussagen sind *falsch*?

(I) $\mathbb{F}_{23}^*$ hat 22 Elemente und ist zyklisch.

(II) Ist $f \in \mathbb{F}_{31}[X]$ ein irreduzibles Polynom über dem Körper $\mathbb{F}_{31}$ mit $\deg(f) = 13$, so ist $\mathbb{F}_{31}[X]/(f)$ ein Körper mit 31^{12} Elementen.

(III) Für $f = X^3 + 3X^2 + 5X + 1 \in \mathbb{F}_7[X]$ ist $\mathbb{F}_7[X]/(f)$ ein Körper.

(VI) Für $g = X^3 + 2X^2 + 1 \in \mathbb{F}_5[X]$ ist $\mathbb{F}_5[X]/(g)$ ein Körper mit 125 Elementen.

√ (a) (II), (III)

(b) (III), (IV)

(c) (I), (III)

(d) (I), (II)

Lösung: Die Antwort (a) ist die korrekte Lösung, da sowohl (II) als auch (III) falsch sind: Bei (II) hätte man einen Körper mit 31^{13} *Elementen und bei (III) ist* f *nicht irreduzibel, da* f *eine Nullstelle bei* 3 *hat.*

---

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

√ (a) $24^{121} \equiv 24 \pmod{35}$

(b) $7^{120} \equiv 1 \pmod{35}$

(c) Die multiplikative Gruppe von $\mathbb{Z}_{16}$ ist zyklisch.

(d) Die multiplikative Gruppe von $\mathbb{Z}_8$ ist zyklisch.

Lösung: Die Aussage (a) ist richtig, denn nach dem Euler'schen Satz gilt $24^{24} \equiv 1 \pmod{35}$*, also auch* $24^{121} \equiv 24 \pmod{35}$*.*

---

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

√ (a) $D_{\log}\big(1 + z^2\big) = 2 \cdot \sum_{n \in \mathbb{N}} z^{2n+1}$

(b) $D\Big(\sum_{n \in \mathbb{N}} n z^n\Big) = \sum_{n \in \mathbb{N}} (n+1)^2 \cdot z^n$

(c) $\prod_{k \in \mathbb{N}} (1 + z^{3^k} + z^{2 \cdot 3^k}) = \sum_{n \in \mathbb{N}} z^n$

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

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

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

---

9. *Logik.* Sei $\mathscr{L} = \{\mathtt{c}, \mathtt{R}_1, \mathtt{R}_2\}$ eine Signatur, wobei $\mathtt{c}$ ein Konstantensymbol ist und $\mathtt{R}_1$ und $\mathtt{R}_2$ zwei 2-stellige Relationssymbole sind. Weiter sei T eine $\mathscr{L}$-Theorie, welche wie folgt definiert ist:

$$\mathsf{T} = \Big\{\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx),\ \forall x\forall y\big(\mathtt{R}_2 xy \to (\mathtt{R}_2 yx \wedge \neg\mathtt{R}_1 xy)\big),$$
$$\forall x\neg\mathtt{R}_2 xx,\ \exists x\mathtt{R}_2\mathtt{c}x,\ \exists x\exists y(\mathtt{R}_1\mathtt{c}x \wedge \mathtt{R}_1 y\mathtt{c})\Big\}$$

(a) *(4 Punkte)* Begründe mit Hilfe des Gödel'schen Vollständigkeitssatzes, dass folgendes gilt:

$$\mathsf{T} \vdash \exists x_1\exists x_2\exists x_3\exists x_4\big(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_1 \neq x_4 \wedge x_2 \neq x_3 \wedge x_2 \neq x_4 \wedge x_3 \neq x_4\big)$$

(b) *(4 Punkte)* Sei σ der folgende $\mathscr{L}$-Satz:

$$\exists x\exists y\big(x \neq y \wedge \mathtt{R}_1 x\mathtt{c} \wedge \mathtt{R}_2 xy \wedge \mathtt{R}_1 y\mathtt{c}\big)$$

Zeige, dass gilt:

(i) $\mathsf{T} \nvdash \sigma$ *(2 Punkte)*

(ii) $\mathsf{T} \nvdash \neg\sigma$ *(2 Punkte)*

Lösung:

(a) Nach dem Gödel'schen Vollständigkeitssatz reicht es zu zeigen, dass es kein Modell von T gibt, das weniger als 4 Elemente enthält. Dabei kann es kein Modell von T mit 0 Elementen geben, da die Konstante $\mathtt{c}$ in diesem Modell interpretiert werden muss.

- *Falls ein Modell $\mathbf{M}_1 \models \mathsf{T}$ mit genau einem existieren würde, so müsste wegen $\exists x\exists y(\mathtt{R}_1\mathtt{c}x \wedge \mathtt{R}_1 y\mathtt{c})$ gelten $\mathtt{R}_1^{\mathbf{M}_1}\mathtt{c}^{\mathbf{M}_1}\mathtt{c}^{\mathbf{M}_1}$. Wegen $\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx)$ müsste dann aber auch $\neg\mathtt{R}_1^{\mathbf{M}_1}\mathtt{c}^{\mathbf{M}_1}\mathtt{c}^{\mathbf{M}_1}$ gelten, was ein Widerspruch wäre, da in einem Modell niemals eine Aussage und deren Negation gleichzeitig wahr sein kann.*
- *Sei $\mathbf{M}_2 \models \mathsf{T}$ ein Modell, dessen Bereich aus den zwei verschiedenen Elementen $\mathtt{c}^{\mathbf{M}_2}$ und α besteht. Nach $\exists x\exists y(\mathtt{R}_1\mathtt{c}x \wedge \mathtt{R}_1 y\mathtt{c})$ müsste also gelten $\mathtt{R}_1^{\mathbf{M}_2}c^{\mathbf{M}_2}\alpha$ und $\mathtt{R}_1^{\mathbf{M}_2}\alpha c^{\mathbf{M}_2}$, weil wegen $\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx)$ weder $\mathtt{R}_1^{\mathbf{M}_2}c^{\mathbf{M}_2}c^{\mathbf{M}_2}$ noch $\mathtt{R}_1^{\mathbf{M}_2}\alpha\alpha$ gelten kann. Dann wäre aber $\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx)$ nicht erfüllt, was ein Widerspruch wäre.*
- *Sei $\mathbf{M}_3 \models \mathsf{T}$ ein Modell bestehend aus den drei verschiedenen Elementen $c^{\mathbf{M}_3}, \alpha, \beta$. Dann können wir ohne Einschränkung annehmen, dass gilt $\mathtt{R}_2^{\mathbf{M}_3}\mathtt{c}^{\mathbf{M}_3}\alpha$ wegen $\forall x\neg\mathtt{R}_2 xx$ und $\exists x\mathtt{R}_2\mathtt{c}x$. Dann folgt aber mit zweimaliger Anwendung von $\forall x\forall y\big(\mathtt{R}_2 xy \to (\mathtt{R}_2 yx \wedge \neg\mathtt{R}_1 xy)\big)$, dass $\neg\mathtt{R}_1\mathtt{c}^{\mathbf{M}_3}\alpha$ und $\neg\mathtt{R}_1\alpha\mathtt{c}^{\mathbf{M}_3}$. Da $\neg R_1^{\mathbf{M}_3}\mathtt{c}^{\mathbf{M}_3}\mathtt{c}^{\mathbf{M}_3}$ gilt, wegen $\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx)$, muss auch $R_1^{\mathbf{M}_3}\mathtt{c}^{\mathbf{M}_3}\beta$ und $R_1^{\mathbf{M}_3}\beta\mathtt{c}^{\mathbf{M}_3}$ gelten wegen $\exists x\exists y(\mathtt{R}_1\mathtt{c}x \wedge \mathtt{R}_1 y\mathtt{c})$. Dies ist jedoch ein Widerspruch zu $\forall x\forall y(\mathtt{R}_1 xy \to \neg\mathtt{R}_1 yx)$.*

Die Aussage folgt nun mit der Umkehrung des Gödel'schen Vollständigkeitssatzes.

(b) (i) Betrachte das Modell $\mathbf{M}_4 \models \mathsf{T}$, wessen Bereich aus den vier verschiedenen Elementen $c^{\mathbf{M}_4}, \alpha, \beta, \gamma$ bestehen und dessen Relationen sich durch die beiden Tabellen

$\mathtt{R}_1$	$c^{\mathbf{M}_4}$	α	β	γ
$c^{\mathbf{M}_4}$		$\times$		
α				
β	$\times$			
γ				

$\mathtt{R}_2$	$c^{\mathbf{M}_4}$	α	β	γ
$c^{\mathbf{M}_4}$				$\times$
α				
β				
γ	$\times$			

beschreiben lassen. Dabei bedeutet ein Kreuz in der Tabelle "... in der linken Spalte ist in Relation mit ... aus der oberen Zeile" und kein Kreuz heisst, "... von der linken Spalte ist nicht in Relation mit ... von der oberen Zeile". Dann sieht man schnell, dass der Satz σ in diesem Modell nicht wahr ist, da keine zwei verschiedenen Elemente von $\mathbf{M}_4$ die Relation $\mathtt{R}_2$ erfüllen. Wendet man die Umkehrung des Korrektheitssatzes an, dann muss offenbar gelten $\mathsf{T} \nvdash \sigma$.

(ii) Betrachte das Modell $\mathbf{M}_5 \models \mathsf{T}$, wessen Bereich aus den fünf verschiedenen Elementen $c^{\mathbf{M}_4}, \alpha, \beta, \gamma, \delta$ besteht und dessen Relationen sich durch die beiden Tabellen

$\mathtt{R}_1$	$c^{\mathbf{M}_5}$	α	β	γ	δ
$c^{\mathbf{M}_5}$				$\times$	
α	$\times$				
β	$\times$				
γ					
δ					

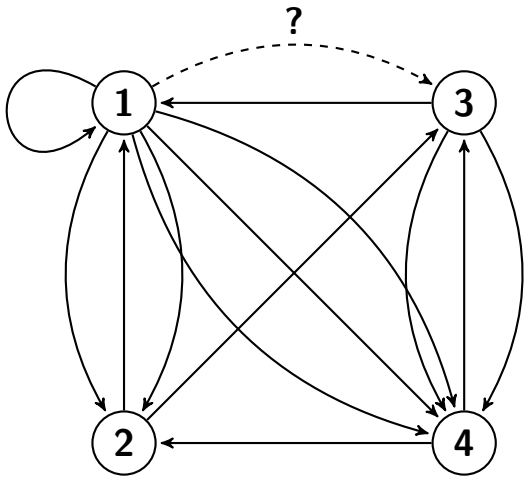
$\mathtt{R}_1$	$c^{\mathbf{M}_5}$	α	β	γ	δ
$c^{\mathbf{M}_5}$					$\times$
α			$\times$		
β		$\times$			
γ					
δ	$\times$				

beschreiben lassen (wie oben). Dann kann man nachprüfen, dass der Satz σ in diesem Modell wahr ist, denn es gilt $\alpha \neq \beta$, $R_1^{\mathbf{M}_5} \alpha \mathsf{c}^{\mathbf{M}_5}$, $R_1^{\mathbf{M}_5} \beta \mathsf{c}^{\mathbf{M}_5}$ und $R_2^{\mathbf{M}_5} \alpha\beta$. Wendet man wieder die Umkehrung des Korrektheitssatzes an, dann muss offenbar gelten $\mathsf{T} \nvdash \neg\sigma$.

---

10. *Graphentheorie.*

(a) *(4 Punkte)* Gegeben sei der folgende Digraph G, bei dem die Kanten vom Knoten 1 zum Knoten 3 fehlen:



Die Adjazenzmatrix A des Digraphen G ist

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

Wie viele Kanten vom Knoten 1 zum Knoten 3 muss es geben, damit genau 22 verschiedene Pfeilfolgen der Länge 3 vom Knoten 1 zum Knoten 3 existieren?

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

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

Lösung:

(a) *Sei* $a := a_{13}^{[1]} \in \mathbb{N}$ *die Anzahl Kanten vom Knoten* 1 *zum Knoten* 3. *Da es genau* 22 *verschiedene Pfeilfolgen der Länge* 3 *vom Knoten* 1 *zum Knoten* 3 *existieren, ist* $a_{13}^{[3]} = 22$. *Wir berechnen nun die erste Zeile von* A^2*:*

$$\begin{pmatrix} 1 & 2 & a & 3 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & a & 3 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} a+3 & 5 & a+5 & 2a+3 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$$

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

$$22 = a_{13}^{[3]} = a^2 + 5a + 8.$$

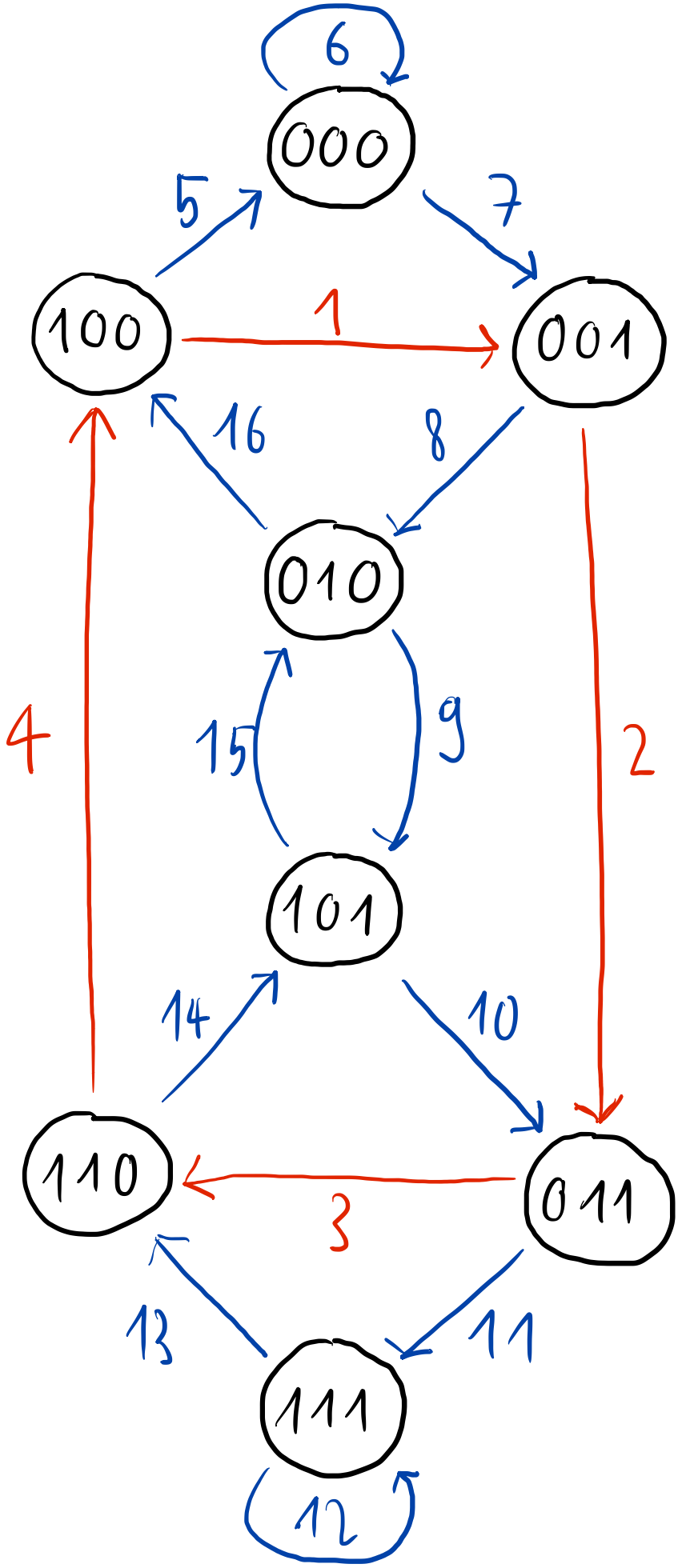
Also können wir die quadratische Gleichung $a^2 + 5a - 14 = 0$ *nach* a *auflösen und bekommen die Lösungen* $-7, 2$. *Da* a *jedoch eine natürliche Zahl sein muss, ist* $a_{13}^{[1]} = 2$.

(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*

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

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* 7 *Ziffern der De Bruijn-Folge bereits kennen, wissen wir, dass der Weg im Bild unten rot eingezeichnet sicher im zugehörigen Euler'schen Pfeilzug vorkommen muss. Desweitern sehen wir sehr schnell, dass sich die Reihenfolge der restlichen Wege von selbst ergibt, da wir keine andere Wahl haben, wenn wir alle Wege im Bild unten ablaufen müssen. Somit gibt es genau eine Möglichkeit, wie wir die De Bruijn-Folge vervollständigen können:*

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


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

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

- *Es muss gelten* $a_8 = 0$*, denn sonst kommt die Folge* $\langle 1, 0, 0, 1\rangle$ *zweimal vor. Dasselbe Agrument liefert uns auch* $a_{16} = 0$*, denn ansonsten kommt die Folge* $\langle 1, 1, 0, 0\rangle$ *zweimal vor (Achtung: die De Bruijn-Folge ist zyklisch!).*

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

- *Da jede mögliche* $0-1$*-Folge der Länge* 4 *genau einmal in der De Bruijn-Folge vorkommen muss, muss die Anzahl von* 0 *und* 1 *in der ganzen Folge gleich sein. Folglich können wir noch genau zwei* 0 *auf die leeren Plätze der De Bruijn-Folge verteilen. Daraus können wir schliessen, dass* $a_9 = 0$ *gelten muss, denn sonst ist es unmöglich, dass* $\langle 0, 0, 0, 0\rangle$ *in der De Bruijn-Folge vorkommt. Ausserdem würde* $\langle 0, 0, 0, 0\rangle$ *zweimal in der Folge vorkommen, wenn nicht* $a_{10} = 1$ *gelten würde.*

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

- *Falls* $a_{15} = 0$*, dann hätte die Bruijn-Folge keine weiteren* 0 *mehr und jede* 0 *hätte minsdestens einen Nachbaren, der auch* 0 *ist, also gäbe es keine Folgen der Form* $\langle 1, 0, 1, *\rangle$ *oder* $\langle *, 1, 0, 1\rangle$ *in der Bruijn-Folge, was ein Widerspruch wäre. Folglich ist* $a_{15} = 1$*.*

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

  Weiter muss auch gelten $a_{12} = 1$ *und* $a_{13} = 1$*, denn sonst kommt* $\langle 1, 1, 1, 1\rangle$ *nicht in der De Bruijn-Folge vor.*

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

  Die Folge $\langle 1, 0, 1, 0\rangle$ *würde zweimal in der De Bruijn-Folge vorkommen, wenn* $a_{14} = 1$ *wäre. Somit muss* $a_{14} = 0$ *und* $a_{11} = 1$ *sein, da wir in der ganzen Folge gleich viele* 0 *und* 1 *haben müssen, damit jeder* $0-1$*-Folge der Länge* 4 *genau einmal vorkommt. Somit sehen wir, dass es eine eindeutige Lösung gibt:*

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

  .

---

11. *Modulorechnen.* Berechne mit dem verallgemeinerten Euklid'schen Algorithmus die kleinste positive, ganze Zahl n für die gilt

$$\begin{aligned} n &\equiv 3 \pmod 5 \\ n &\equiv 2 \pmod 7 \\ n &\equiv 1 \pmod{12} \end{aligned}$$

Lösung: Für die ersten zwei Bedingungen muss gelten $n = 5k + 3$ *und* $n = 7l + 2$. *Also gilt auch* $7l - 5k = 1$. *Wir suchen nun die Zahlen* k, l, *welche wir mit dem* vEA *erhalten können:*

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

		1	*2*	*2*
0	**1**	*1*	*3*	*7*
1	**0**	*1*	*2*	*5*

Wir sehen also, dass wir $k = -3$ *und* $l = -2$ *wählen können, sodass* $7l - 5k = 1$ *gilt. Somit gilt für jedes* n, *welches* $n \equiv -12 \pmod{35}$ *erfüllt, auch die beiden Bedingungen* $n \equiv 3 \pmod 5$ *und* $n \equiv 2 \pmod 7$.

Somit reicht es, wenn wir das kleinste $n' \in \mathbb{N}$ *finden, sodass die Bedingungen* $n' \equiv -12 \pmod{35}$ *und* $n' \equiv 1 \pmod{12}$ *erfüllt sind. Wir suchen also wieder ein* k', l' *sodass* $n' = 35k' - 12 = 12l' + 1$ *gilt. Daraus folgt* $35k' - 12l' = 13$. *Mit dem* vEA *können wir nun* $k'', l'' \in \mathbb{Z}$ *suchen, sodass* $35k'' - 12l'' = 1$ *erfüllt ist:*

$$\begin{aligned} 35 &= 2 \cdot 12 + 11 \\ 12 &= 1 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

		2	*1*	*11*
0	**1**	*2*	*3*	*35*
1	**0**	*1*	*1*	*12*

Somit ist $k'' = -1$ *und* $l'' = -3$ *sowie* $k' = 13k'' = -13$ *und* $l' = 13l'' = -39$. *Die Zahl* $n' = -467$ *erfüllt nun alle Bedingungen. Allgemein erfüllen somit alle Zahlen* $5 \cdot 7 \cdot 12t - 467$ *die Bedingungen für* $t \in \mathbb{Z}$ *beliebig. Die kleinste positive Zahl , welche alle Bedingungen erfüllt, ist* 373 *(für* $t = 2$*).*

---

12. *endliche Geometrie.* Die 121 Elemente $\langle x, y\rangle \in \mathbb{F}_{11} \times \mathbb{F}_{11}$ seien die Punkte der *endlichen Koordinatenebene* E_{121}.
Für alle $a, b \in \mathbb{F}_{11}$ definiert die Menge

$$g(a,b) := \big\{\langle x, y\rangle \in E_{121} : y = ax + b\big\}$$

eine *Gerade* in E_{121}.

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

(b) *(2 Punkte)* Berechne den Schnittpunkt der beiden Geraden $g(\bar{3}, \bar{5})$ und $g(\bar{5}, \bar{2})$.

(c) *(2 Punkte)* Bestimme die Gleichung $y = ax + b$ der Geraden, welche durch die beiden Punkte $\langle \bar{4}, \bar{4}\rangle$ und $\langle \bar{1}, \bar{7}\rangle$ geht.

(d) *(3 Punkte)* Bestimme alle Punkte $\langle x, y\rangle \in E_{121}$, welche folgende Gleichung erfüllen:

$$x^2 + y^2 = \bar{3}$$

Lösung:

(a) Für beliebige $a, b \in \mathbb{F}_{11}$ gibt es für jede Wahl von $x \in \mathbb{F}_{11}$ ein wohldefiniertes $y = ax + b$. Das heisst, jede Gerade $g(a, b)$ besitzt genau 11 Punkte.

(b) Der Schnittpunkt $\langle x, y\rangle$ von $g(\bar{3}, \bar{5})$ und $g(\bar{5}, \bar{2})$ muss die beiden Gleichungen

$$y = \bar{3}x + \bar{5}$$
$$y = \bar{5}x + \bar{2}$$

erfüllen. Subtrahiert man die erste Gleichung von der zweiten, so erhält man $\bar{0} = \bar{2}x - \bar{3}$, wobei wir auf beiden Seiten mit $\bar{3}$ addieren und mit $\bar{6}$ multiplizieren können. Wir erhalten schliesslich $x = \bar{7}$ und durch Einsetzten in einer von den beiden oberen Gleichungen $y = \bar{4}$. Somit ist $\langle \bar{7}, \bar{4}\rangle$ der Schnittpunkt von $g(\bar{3}, \bar{5})$ und $g(\bar{5}, \bar{2})$.

(c) Da die beiden Punkte $\langle \bar{4}, \bar{4}\rangle$ und $\langle \bar{1}, \bar{7}\rangle$ auf einer Gerade $g(a, b)$ liegen, erhalten wir die folgenden Gleichungen für die Koeffizienten a, b:

$$\bar{4} = \bar{4}a + b$$
$$\bar{7} = a + b$$

Subtrahiert man die zweite von der ersten Gleichung, so erhält man $-\bar{3} = \bar{3}a$, was wir mit $\bar{4}$ multiplizieren können und dann bekommen wir $a = -\bar{1} = 10$. Subtrahieren wir a von der zweiten Gleichung, so erhalten wir schliesslich $b = \bar{7} - \bar{10} = \bar{8}$. Somit geht die Gerade $g(\bar{10}, \bar{8})$ durch die beiden Punkte $\langle \bar{4}, \bar{4}\rangle$ und $\langle \bar{1}, \bar{7}\rangle$.

(d) Falls $x, y \in \mathbb{F}_{11}$, so sieht man mit ausprobieren schnell, dass $x^2, y^2 \in M := \{\bar{0}, \bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$ sein muss. Da $x^2 + y^2 = \bar{3}$ sein soll, können wir nun Elemente $a, b \in M$ suchen, sodass $a + b = \bar{3}$ gilt. Beachte, dass $b = \bar{3} - a$ für jede Wahl von $a \in M$ eindeutig definiert ist. Dann gibt es für a und b bis auf Vertauschung nur die folgenden Lösungen:

$$\bar{0} + \bar{3} = \bar{3}$$
$$\bar{5} + \bar{9} = \bar{3}$$

Nun hat jede von diesen Zahlen maximal 2 Wurzeln in $\mathbb{F}_{11}$, wobei beide umgekehrtes Vorzeichen haben. Es gilt:

$$\begin{aligned}\bar{0}^2 &= \bar{0}\\ \bar{3}^2 = \bar{8}^2 &= \bar{9}\\ \bar{4}^2 = \bar{7}^2 &= \bar{5}\\ \bar{5}^2 = \bar{6}^2 &= \bar{3}\end{aligned}$$

Damit bekommt man, dass die Punkte $\langle x, y\rangle \in E_{121}$, welche die Gleichung $x^2 + y^2 = \bar{3}$ erfüllen, von der folgenden Form sein müssen:

$$\langle 0,5\rangle, \langle 5,0\rangle, \langle 0,6\rangle, \langle 6,0\rangle, \langle 3,4\rangle, \langle 4,3\rangle, \langle 3,7\rangle, \langle 7,3\rangle, \langle 8,4\rangle, \langle 4,8\rangle, \langle 8,7\rangle, \langle 7,8\rangle$$
