

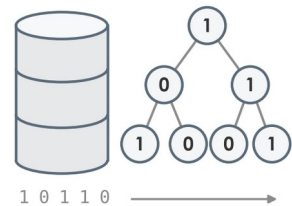
Informatik Klasse 12

Thema: Übung zum Abitur – Algorithmen, Datenbanken, Automaten

Name: _____ Datum: _____

Punkte: _____ / 42 Note: _____

Unterschrift: _____



Viel Erfolg!

1 Algorithmen: Sortieren und Suchen

Die Prozedur sortiere ordnet ein Feld A mit n Zahlen (Indizes 0 bis n – 1) aufsteigend.

- a) Die Prozedur wird mit A = [6, 2, 8, 4, 1] aufgerufen. **Geben** Sie den Inhalt von A jeweils nach einem Durchlauf der äußeren Schleife **an**.

```
prozedur sortiere(A)
  für i ← 1 bis n – 1
    x ← A[i]
    j ← i – 1
    solange j ≥ 0 und A[j] > x
      A[j + 1] ← A[j]
      j ← j – 1
    A[j + 1] ← x
```

	[0]	[1]	[2]	[3]	[4]
i = 1					
i = 2					
i = 3					
i = 4					

- b) Welches Verfahren ist das?
Kreuzen Sie **an**.

- ☐ Sortieren durch Auswahl
☐ Sortieren durch Einfügen
☐ Bubblesort
☐ Quicksort

- c) Laufzeit im schlechtesten Fall?
Kreuzen Sie **an**.

- ☐ O(n)
☐ O(n · log n)
☐ O(n²)
☐ O(2ⁿ)

- d) **Begründen** Sie, warum die Prozedur für ein bereits sortiertes Feld nur eine lineare Laufzeit benötigt.

Die binäre Suche vergleicht den Suchwert mit dem Element an der Stelle mitte = (links + rechts) div 2 und sucht dann in der passenden Hälfte weiter:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
3	8	11	15	19	24	27	31	36	40	44	52	57	63	70

- e) **Geben** Sie der Reihe nach die Elemente **an**, mit denen der Suchwert 12 verglichen wird, und das Ergebnis der Suche.

2 Datenstrukturen: Stapel, Schlange, binärer Suchbaum

Ein Stapel S (Stack) und eine Schlange Q (Queue) sind zu Beginn leer. pop() und dequeue() entfernen ein Element und geben es aus.

```
S: push(4); push(7); push(2); pop();
   push(9); pop(); pop()
Q: enqueue(4); enqueue(7); enqueue(2); dequeue();
   enqueue(9); dequeue(); dequeue()
```

- a) **Geben** Sie jeweils die Ausgaben in ihrer Reihenfolge und den Inhalt am Ende **an**.

	Ausgaben (in Reihenfolge)	Inhalt am Ende
Stapel S		
Schlange Q		

- b) **Kreuzen** Sie jeweils die passende Datenstruktur **an**.

Anwendung	Stapel	Schlange
Rückgängig-Funktion eines Texteditors	☐	☐
Druckaufträge an einen Netzwerkdrucker	☐	☐
Zurück-Taste eines Webbrowsers	☐	☐

- c) **Fügen** Sie die Zahlen 41, 23, 67, 15, 30, 52, 80, 27 in dieser Reihenfolge in einen leeren binären Suchbaum **ein**. **Zeichnen** Sie den entstandenen Baum.

- d) **Geben** Sie für diesen Baum die Inorder- und die Preorder-Traversierung **an**.

Inorder: _____

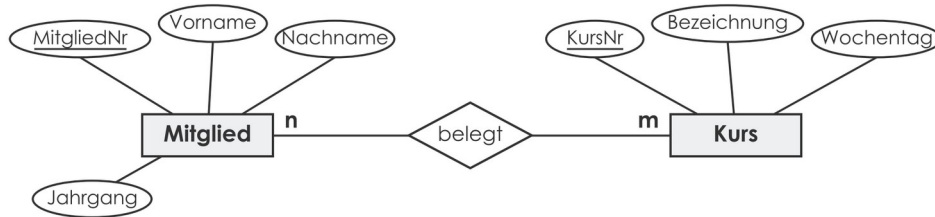
Preorder: _____

- e) **Erläutern** Sie, wovon die Laufzeit der Suche in einem binären Suchbaum abhängt.

3 Datenbanken: ER-Modell und SQL

Ein Sportverein verwaltet seine Mitglieder und Kurse in einer relationalen Datenbank. M1 zeigt das ER-Modell, M2 einen Ausschnitt der Tabellen.

M1 ER-Modell



M2 Tabellen (Ausschnitt)

Mitglied

MitgliedNr	Vorname	Nachname	Jahrgang
1	Lea	Brandt	2007
2	Jonas	Ehlers	2009
3	Mira	Kaya	2006
4	Tim	Vogt	2008
5	Sina	Albers	2007
6	Paul	Jansen	2010

Kurs

KursNr	Bezeichnung	Wochentag
K1	Klettern	Montag
K2	Volleyball	Mittwoch
K3	Schach	Freitag

Belegung

MitgliedNr	KursNr
1	K1
1	K3
2	K2
3	K1
4	K2
5	K1
5	K2
6	K3

- a) **Erläutern** Sie die Kardinalität n:m im Sachzusammenhang. **Begründen** Sie, warum für „belegt“ eine eigene Tabelle nötig ist, und **geben** Sie Primär- und Fremdschlüssel von Belegung **an**.

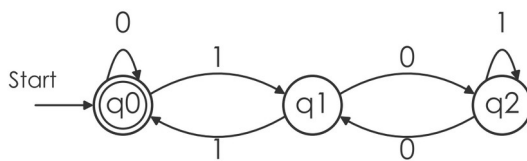
- b) **Formulieren** Sie eine SQL-Abfrage, die Vor- und Nachnamen aller Mitglieder ausgibt, die den Kurs „Klettern“ belegt haben.

- c) **Formulieren** Sie eine SQL-Abfrage, die für jeden Kurs mit mindestens drei Teilnehmenden die Bezeichnung und die Anzahl der Teilnehmenden ausgibt.

4 Endliche Automaten

Der deterministische endliche Automat A (M3) liest Wörter über $\{0, 1\}$.

M3 Automat A



a) Akzeptiert A das Wort?
Kreuzen Sie an.

Wort	ja	nein
110	☐	☐
111	☐	☐
1001	☐	☐
1100	☐	☐
10101	☐	☐

b) **Beschreiben** Sie die von A akzeptierte Sprache. **Erläutern** Sie die Zustände.

c) **Entwerfen** und **zeichnen** Sie einen DEA über $\{a, b\}$, der genau die Wörter akzeptiert, die auf **ab** enden.

___ / 8

5 Kryptographie und Netzwerke

a) Caesar-Verfahren, Verschiebung um 3 nach rechts (nach Z folgt A):
Entschlüsseln Sie GDWHQ VFKXHWCHQ.

b) RSA mit $p = 5$, $q = 11$ und $e = 3$: **Berechnen** Sie n und $\phi(n)$ und **zeigen** Sie, dass $d = 27$ der private Exponent ist.

c) **Verschlüsseln** Sie $m = 4$ mit dem öffentlichen Schlüssel (e, n) .

d) **Kreuzen** Sie **an**: richtig oder falsch?

Aussage	richtig	falsch
Bei RSA ist (e, n) öffentlich, d bleibt geheim.	☐	☐
Ein DNS-Server verschlüsselt Webseiten.	☐	☐

___ / 7

Lösung: Informatik Klasse 12 – Übung zum Abitur – Algorithmen, Datenbanken, Automaten

Insgesamt sind 42 Punkte erreichbar, halbe Punkte sind möglich.

Note 1	Note 2	Note 3	Note 4	Note 5	Note 6
42–38 P.	37,5–34 P.	33,5–27,5 P.	27–21 P.	20,5–13 P.	12,5–0 P.

1 Algorithmen: Sortieren und Suchen

Die Prozedur sortiere ordnet ein Feld A mit n Zahlen (Indizes 0 bis n – 1) aufsteigend.

- a) Die Prozedur wird mit A = [6, 2, 8, 4, 1] aufgerufen. **Geben** Sie den Inhalt von A jeweils nach einem Durchlauf der äußeren Schleife **an**.

```

prozedur sortiere(A)
  für i ← 1 bis n – 1
    x ← A[i]
    j ← i – 1
    solange j ≥ 0 und A[j] > x
      A[j + 1] ← A[j]
      j ← j – 1
    A[j + 1] ← x
  
```

	[0]	[1]	[2]	[3]	[4]
i = 1	2	6	8	4	1
i = 2	2	6	8	4	1
i = 3	2	4	6	8	1
i = 4	1	2	4	6	8

- b) Welches Verfahren ist das?
Kreuzen Sie **an**.

- ☐ Sortieren durch Auswahl
☒ Sortieren durch Einfügen
☐ Bubblesort
☐ Quicksort

- c) Laufzeit im schlechtesten Fall?
Kreuzen Sie **an**.

- ☐ $O(n)$
☐ $O(n \cdot \log n)$
☒ $O(n^2)$
☐ $O(2^n)$

- d) **Begründen** Sie, warum die Prozedur für ein bereits sortiertes Feld nur eine lineare Laufzeit benötigt.

- Bei sortiertem Feld gilt in jedem Durchlauf $A[i - 1] \leq x$, die Bedingung der solange-Schleife ist sofort falsch.
- Die innere Schleife verschiebt nichts; pro Durchlauf nur ein Vergleich, insgesamt $n - 1$ Vergleiche $\rightarrow O(n)$.

Die binäre Suche vergleicht den Suchwert mit dem Element an der Stelle mitte = (links + rechts) div 2 und sucht dann in der passenden Hälfte weiter:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
3	8	11	15	19	24	27	31	36	40	44	52	57	63	70

- e) **Geben** Sie der Reihe nach die Elemente **an**, mit denen der Suchwert 12 verglichen wird, und das Ergebnis der Suche.

- Vergleiche mit 31 (Index 7), 15 (Index 3), 8 (Index 1), 11 (Index 2); danach ist links > rechts: 12 ist nicht enthalten.

2 Datenstrukturen: Stapel, Schlange, binärer Suchbaum

Ein Stapel S (Stack) und eine Schlange Q (Queue) sind zu Beginn leer. pop() und dequeue() entfernen ein Element und geben es aus.

```
S: push(4); push(7); push(2); pop();
   push(9); pop(); pop()
Q: enqueue(4); enqueue(7); enqueue(2); dequeue();
   enqueue(9); dequeue(); dequeue()
```

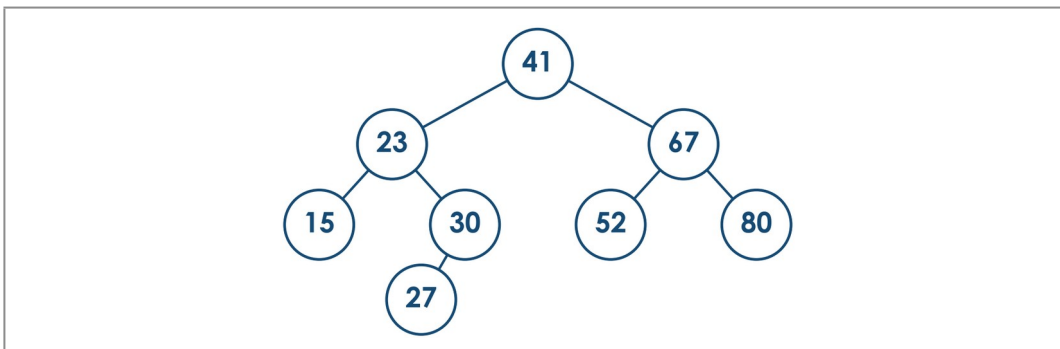
- a) **Geben** Sie jeweils die Ausgaben in ihrer Reihenfolge und den Inhalt am Ende **an**.

	Ausgaben (in Reihenfolge)	Inhalt am Ende
Stapel S	2, 9, 7	4
Schlange Q	4, 7, 2	9

- b) **Kreuzen** Sie jeweils die passende Datenstruktur **an**.

Anwendung	Stapel	Schlange
Rückgängig-Funktion eines Texteditors	☒	☐
Druckaufträge an einen Netzwerkdrucker	☐	☒
Zurück-Taste eines Webbrowsers	☒	☐

- c) **Fügen** Sie die Zahlen 41, 23, 67, 15, 30, 52, 80, 27 in dieser Reihenfolge in einen leeren binären Suchbaum **ein**. **Zeichnen** Sie den entstandenen Baum.



- d) **Geben** Sie für diesen Baum die Inorder- und die Preorder-Traversierung **an**.

- Inorder: 15, 23, 27, 30, 41, 52, 67, 80 (aufsteigend sortiert)
- Preorder: 41, 23, 15, 30, 27, 67, 52, 80

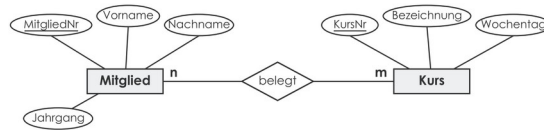
- e) **Erläutern** Sie, wovon die Laufzeit der Suche in einem binären Suchbaum abhängt.

- Die Anzahl der Vergleiche entspricht höchstens der Höhe des Baums. Ausgeglichener Baum: Höhe $\approx \log_2 n$, also $O(\log n)$.
- Werden die Werte sortiert eingefügt, entartet der Baum zu einer Liste: Höhe n , also $O(n)$.

3 Datenbanken: ER-Modell und SQL

Ein Sportverein verwaltet seine Mitglieder und Kurse in einer relationalen Datenbank. M1 zeigt das ER-Modell, M2 einen Ausschnitt der Tabellen.

M1 ER-Modell



M2 Tabellen (Ausschnitt)

Mitglied

MitgliedNr	Vorname	Nachname	Jahrgang
1	Lea	Brandt	2007
2	Jonas	Ehlers	2009
3	Mira	Kaya	2006
4	Tim	Vogt	2008
5	Sina	Albers	2007
6	Paul	Jansen	2010

Kurs

KursNr	Bezeichnung	Wochentag
K1	Klettern	Montag
K2	Volleyball	Mittwoch
K3	Schach	Freitag

Belegung

MitgliedNr	KursNr
1	K1
1	K3
2	K2
3	K1
4	K2
5	K1
5	K2
6	K3

- a) **Erläutern** Sie die Kardinalität n:m im Sachzusammenhang. **Begründen** Sie, warum für „belegt“ eine eigene Tabelle nötig ist, und **geben** Sie Primär- und Fremdschlüssel von Belegung **an**.

- n:m: Ein Mitglied belegt mehrere Kurse, ein Kurs hat mehrere Mitglieder. Ein Fremdschlüssel in Mitglied oder Kurs könnte nur einen Partner speichern.
- Primärschlüssel: (MitgliedNr, KursNr) zusammengesetzt;
Fremdschlüssel: MitgliedNr → Mitglied, KursNr → Kurs.

- b) **Formulieren** Sie eine SQL-Abfrage, die Vor- und Nachnamen aller Mitglieder ausgibt, die den Kurs „Klettern“ belegt haben.

```
SELECT M.Vorname, M.Nachname
FROM Mitglied M
JOIN Belegung B ON M.MitgliedNr = B.MitgliedNr
JOIN Kurs K ON B.KursNr = K.KursNr
WHERE K.Bezeichnung = 'Klettern';
```

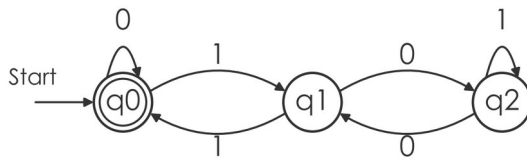
- c) **Formulieren** Sie eine SQL-Abfrage, die für jeden Kurs mit mindestens drei Teilnehmenden die Bezeichnung und die Anzahl der Teilnehmenden ausgibt.

```
SELECT K.Bezeichnung, COUNT(*) AS Anzahl
FROM Kurs K
JOIN Belegung B ON K.KursNr = B.KursNr
GROUP BY K.KursNr, K.Bezeichnung
HAVING COUNT(*) >= 3;
```

4 Endliche Automaten

Der deterministische endliche Automat A (M3) liest Wörter über $\{0, 1\}$.

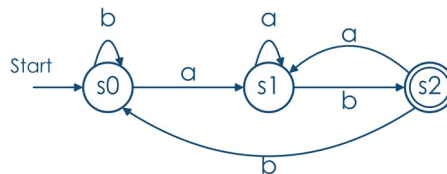
M3 Automat A



a) Akzeptiert A das Wort?
Kreuzen Sie an.

Wort	ja	nein
110	☒	☐
111	☐	☒
1001	☒	☐
1100	☒	☐
10101	☒	☐

- b) **Beschreiben** Sie die von A akzeptierte Sprache. **Erläutern** Sie die Zustände.
- A akzeptiert genau die Binärzahlen, deren Wert durch 3 teilbar ist (dazu das leere Wort).
 - Zustand q_r bedeutet: Der bisher gelesene Wert w hat bei Division durch 3 den Rest r . Ein neues Bit b ergibt $2 \cdot w + b$.
- c) **Entwerfen** und **zeichnen** Sie einen DEA über $\{a, b\}$, der genau die Wörter akzeptiert, die auf **ab** enden.



8 / 8

5 Kryptographie und Netzwerke

- a) Caesar-Verfahren, Verschiebung um 3 nach rechts (nach Z folgt A):
Entschlüsseln Sie GDWHQ VFKXHWCHQ.
- DATEN SCHUETZEN
- b) RSA mit $p = 5$, $q = 11$ und $e = 3$: **Berechnen** Sie n und $\phi(n)$ und **zeigen** Sie, dass $d = 27$ der private Exponent ist.
- $n = p \cdot q = 55$; $\phi(n) = (p - 1) \cdot (q - 1) = 4 \cdot 10 = 40$; $\text{ggT}(3, 40) = 1$
 - $e \cdot d = 3 \cdot 27 = 81 = 2 \cdot 40 + 1$, also $e \cdot d \equiv 1 \pmod{40}$: $d = 27$ passt.
- c) **Verschlüsseln** Sie $m = 4$ mit dem öffentlichen Schlüssel (e, n) .
- $c = m^e \pmod{n} = 4^3 \pmod{55} = 64 \pmod{55} = 9$ (Probe: $9^{27} \pmod{55} = 4$)
- d) **Kreuzen** Sie **an**: richtig oder falsch?

Aussage	richtig	falsch
Bei RSA ist (e, n) öffentlich, d bleibt geheim.	☒	☐
Ein DNS-Server verschlüsselt Webseiten.	☐	☒

Zu 2: DNS übersetzt Domainnamen in IP-Adressen.

7 / 7