

Woche 1: *Einführung*

"Diskrete Strukturen"

???

Diskrete Strukturen

Analysis, lineare Algebra.

Fokus auf unendlichen, oft überabzählbaren Objekten wie z.B. die reellen oder komplexen Zahlen und **kontinuierliche** Abbildungen.

Stellt viele wichtige Methoden bereit um z.B. Funktionen über den reellen oder komplexen Zahlen analysieren zu können.

Diskrete Mathematik/Diskrete Strukturen.

diskret ist hier im Sinne von "trennbar" gemeint.

Der Schwerpunkt liegt hier oft auf endlichen oder abzählbaren Objekten, z.B. endlichen Graphen oder algebraischen Strukturen

Auch gehört die **Kombinatorik** zur diskreten Mathematik, also die Kunst des richtigen Zählens.

Die diskrete Mathematik liefert viele wichtige **mathematische Modelle** („Datenstrukturen“) ebenso wie Methoden, die z.B. für die Laufzeitanalyse von Algorithmen wichtig sind.

1.1 Inhalt

Inhalt der Vorlesung

Inhaltsübersicht.

- **Kombinatorik**
 - Zählprobleme: Urnenmodelle, Permutationen, Binomialsatz, ...
 - Grundlegende Beweismethoden
 - Catalan und Stirling-Zahlen
- **Graphentheorie**
 - Grundlagen, Bäume, Kreise, Grad eines Knoten
 - Zusammenhang in Graphen, Euler-Touren, Mehrfachzusammenhang, Schnittknoten und der Block-Graph
 - Flüsse und der Satz von Menger
 - Matchings
 - planare Graphen und Färbungen
- **Modulare Arithmetik und Zahlentheorie**
 - Modulare Arithmetik, das Rechnen mit großen Zahlen
 - Primzahlen und der Algorithmus von Euklid
 - das RSA System
- **Algebraische Strukturen**
 - Äquivalenzrelationen, Ordnungen, Monoide

Und warum machen wir das?

Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



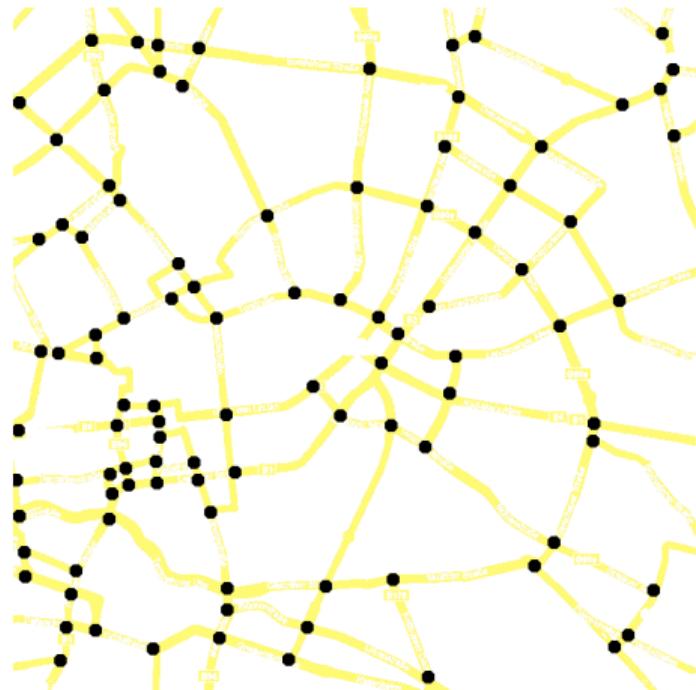
Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



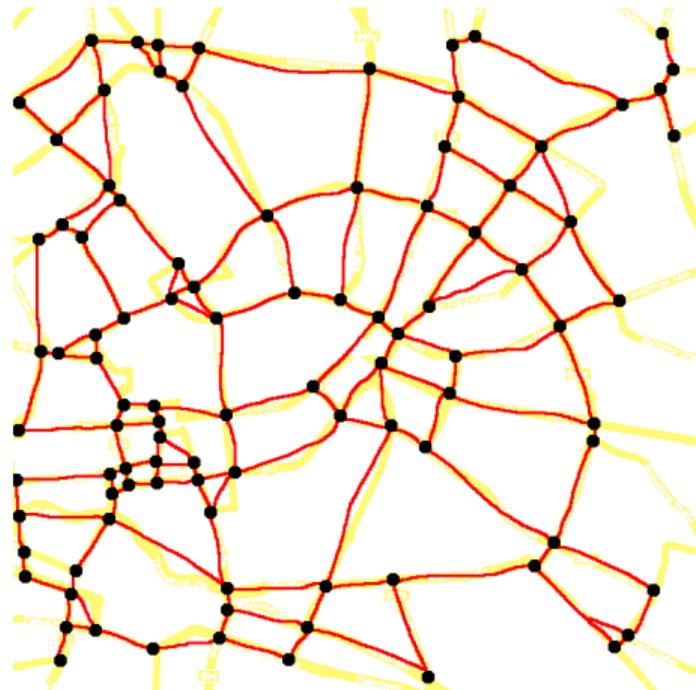
Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



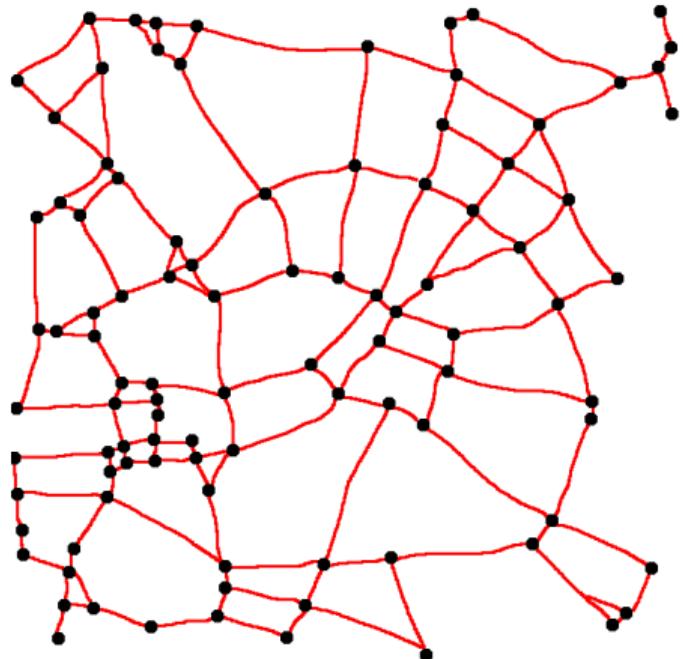
Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



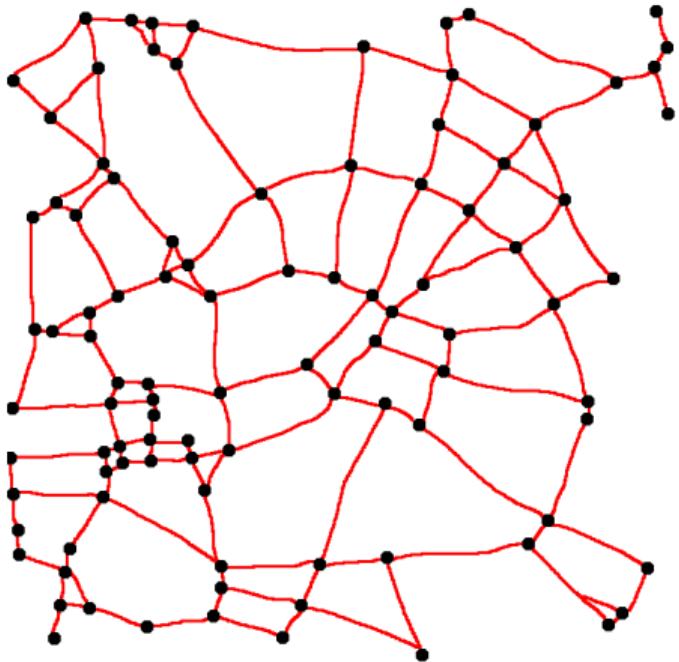
Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



Beispiel: Routen finden

Vorlesung „Diskrete Strukturen“. Do 12-14 Uhr im HE 101.



Modellierung als „Graph“. $G := (V, E)$

Knotenmenge $V := \{v_0, \dots, v_k\}$

Kantenmenge $E := \{\{v_0, v_17\}, \dots\}$

Knoten entsprechen Kreuzungen.

Kanten entsprechen Straßen.

Modellierung und Abstraktion

Abstraktion und Modellierung.

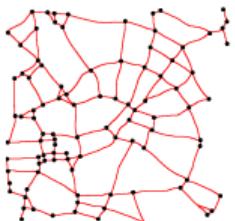
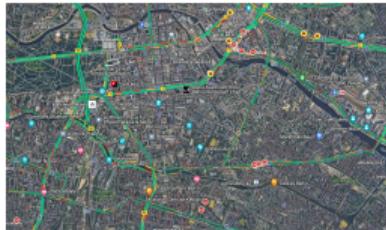
Wir haben also eine Straßenkarte in einen abstrakten Graph überführt.

Der Graph dient uns als *Modell* der wirklichen Situation auf der Straße.

Diese *Abstraktion* erlaubt es uns, leichter Algorithmen zum Finden des kürzesten Weges zu entwickeln:

- Abstraktion auf das „*wesentliche*“
- Alle für die Aufgabe relevanten Informationen bleiben erhalten, alles andere entfällt
- Dies erleichtert es auch, die entwickelten Algorithmen in anderen Anwendungsfällen einzusetzen.

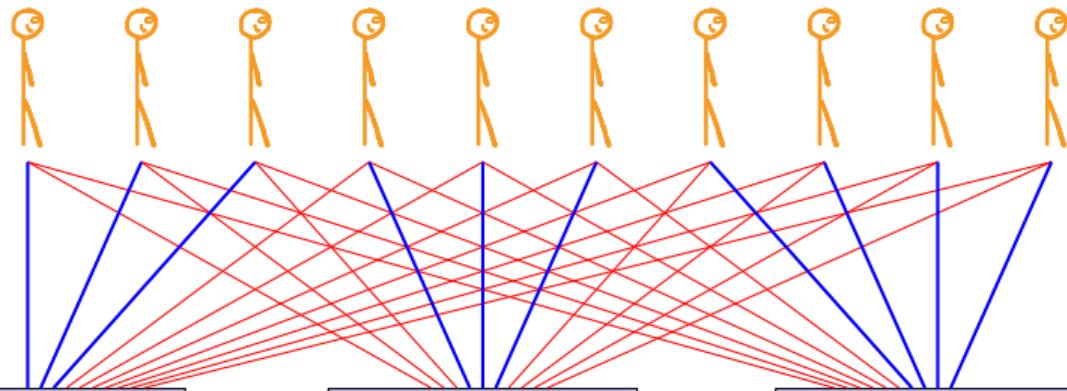
Mathematische Modelle bilden die Basis guter Datenstrukturen.



Beispiel 2: Zuordnungen

Tutorien „Diskrete Strukturen“. Es gibt

ca. 670 Studierende

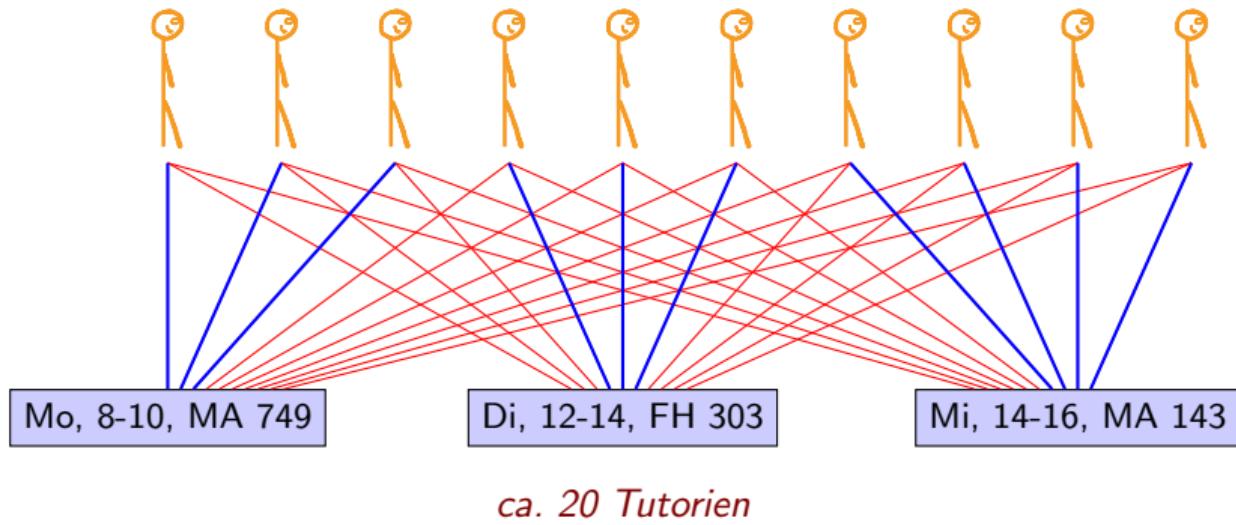


ca. 20 Tutorien

Beispiel 2: Zuordnungen

Tutorien „Diskrete Strukturen“. Es gibt

ca. 670 Studierende



Modellierung als „Graph“.

$$G := (V, E) \text{ bipartit}$$

Knotenmenge $V := S \cup T$

S : Studierende

T : Tutorien

Kantenmenge:

$$E := \{\{s_i, t_j\}, \dots\}$$

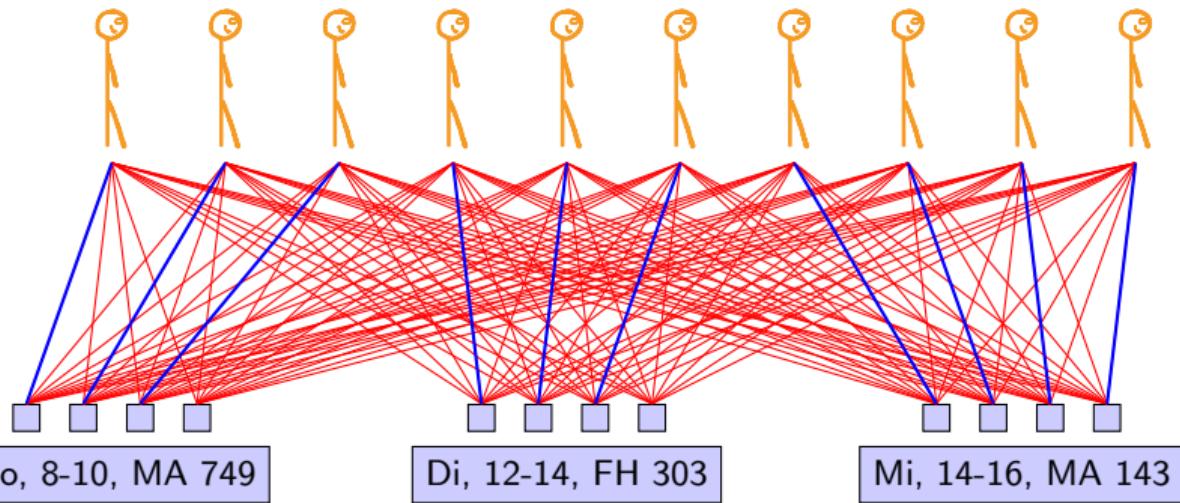
Kante $\{s_i, t_j\}$:

Stud. i kann in Tutorium j .

Beispiel 2: Zuordnungen

Tutorien „Diskrete Strukturen“. Es gibt

ca. 670 Studierende



ca. 20 Tutorien à p Plätze

Matching: Zuordnung, die Stud. einen eindeutigen Platz zuordnet.

Modellierung als „Graph“.

$$G := (V, E) \text{ bipartit}$$

Knotenmenge

$$V := S \cup (T \times \{1, \dots, p\})$$

S : Studierende

(t, p) : Platz p in Tut. t

Kantenmenge:

$$E := \{\{s_i, (t_j, p_j)\}, \dots\}$$

Kante $\{s_i, (t_j, p_j)\}$:

Stud. i kann in Tutorium j .

Vorteile der Abstraktion

Graphen. Wichtiges mathematisches Modell in der Informatik.

Modellierung. Wir haben gesehen, dass wir

- *routing-Probleme* wie das Finden kürzester Wege
- *Zuordnungsprobleme* wie die Tutorieneinteilung

mit Hilfe von Graphen modellieren können, obschon die Probleme erst einmal sehr verschieden aussehen.

Vorteile.

- Gemeinsamkeiten verschiedener Probleme sind leichter zu erkennen.
- Lösungen für ein Problem lassen sich auf andere übertragen.
- Methoden und Algorithmen für Graphen lassen sich auf mehrere Probleme anwenden.

Beispiel. *Maximale matchings* lassen sich effizient mit Hilfe von *routing*-Algorithmen ausrechnen.

Inhalt der Vorlesung

Inhaltsübersicht.

- **Kombinatorik**
 - Zählprobleme: Urnenmodelle, Permutationen, Binomialsatz, ...
 - Grundlegende Beweismethoden
 - Catalan und Stirling-Zahlen
- **Graphentheorie**
 - Grundlagen, Bäume, Kreise, Grad eines Knoten
 - Zusammenhang in Graphen, Euler-Touren, Mehrfachzusammenhang, Schnittknoten und der Block-Graph
 - Flüsse und der Satz von Menger
 - Matchings
 - planare Graphen und Färbungen
- **Modulare Arithmetik und Zahlentheorie**
 - Modulare Arithmetik, das Rechnen mit großen Zahlen
 - Primzahlen und der Algorithmus von Euklid
 - das RSA System
- **Algebraische Strukturen**
 - Äquivalenzrelationen, Ordnungen, Monoide

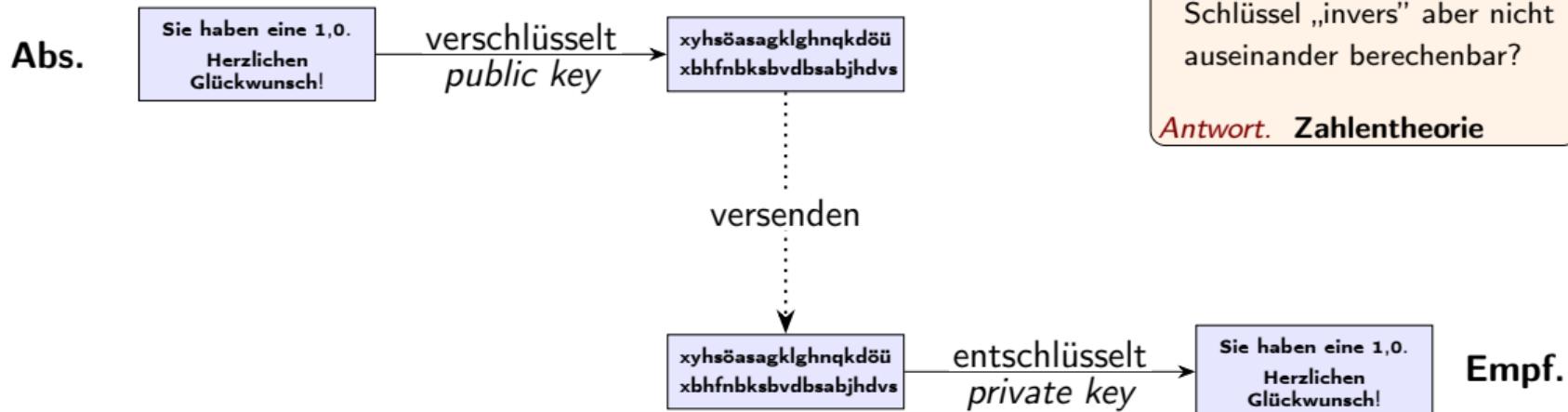
Beispiel 3: Public-Key Kryptographie

Prüfung. Irgendwann werden Sie in dem Modul auch geprüft.

Prüfungsergebnisse sollen vertraulich behandelt werden.

Zum Beispiel sollten Ergebnisse Ihnen per EMail nur verschlüsselt mitgeteilt werden.

Verschlüsselung von EMails. Wie funktioniert EMail-Verschlüsselung?



Public-key Kryptographie.

Schlüsselpaar: (*pub, priv*)

Text = *priv*(*pub*(Text))

Frage. Woher bekommt man so ein Schlüsselpaar?

Schlüssel „invers“ aber nicht auseinander berechenbar?

Antwort. Zahlentheorie

Inhalt der Vorlesung

Inhaltsübersicht.

- **Kombinatorik**
 - Zählprobleme: Urnenmodelle, Permutationen, Binomialsatz, ...
 - Grundlegende Beweismethoden
 - Catalan und Stirling-Zahlen
- **Graphentheorie**
 - Grundlagen, Bäume, Kreise, Grad eines Knoten
 - Zusammenhang in Graphen, Euler-Touren, Mehrfachzusammenhang, Schnittknoten und der Block-Graph
 - Flüsse und der Satz von Menger
 - Matchings
 - planare Graphen und Färbungen
- **Modulare Arithmetik und Zahlentheorie**
 - Modulare Arithmetik, das Rechnen mit großen Zahlen
 - Primzahlen und der Algorithmus von Euklid
 - das RSA System
- **Algebraische Strukturen**
 - Äquivalenzrelationen, Ordnungen, Monoide

Und die Kombinatorik?

Kombinatorik. Die Kombinatorik behandelt unter anderem Methoden um Dinge *abzählen* zu können.

Wie viele maximale matchings zwischen Studierenden und Tutorien gibt es?

Dies ist z. B. wichtig um die Laufzeit von Algorithmen abschätzen zu können.

Diskrete Strukturen

Diskrete Mathematik

Definiert und untersucht viele der für die Informatik wichtigen mathematischen Modelle:

- *Graphen*: Analyse und Modellierung von **Netzwerk-artigen Strukturen** (und eigentlich auch sonst allem)
- *Zahlentheorie*: moderne Kryptographie
- *Kombinatorik*: Analyse und Entwurf von Algorithmen
- ...

Modellierung und Abstraktion

Rolle der Theorie in der Informatik.

- Stellt geeignete *mathematische Modelle* zur Verfügung.
- Analysiert die Eigenschaften dieser Modelle und liefert allgemeine Lösungsverfahren auf Basis dieser Modelle.
- *Abstraktion* erlaubt es zu verstehen, welche Informationen "*mindestens*" für einen Algorithmus zur Verfügung stehen müssen.
- Bei abstrakten Modellen sieht man leichter, was man noch hinzunehmen muss, um bestimmte Aufgaben lösen zu können.

Beispiel. Erweiterung von endlichen Automaten zu push-down-Automaten um nicht-reguläre Sprachen zu erkennen

Aber. Die "theoretisch-mathematische" Modellierung reduziert konkrete Probleme auf ihren abstrakten *Kern* und bietet allgemeine Lösungen an.

Dies ist nur sinnvoll, wenn diese Lösungen allgemeine Gültigkeit haben.

Daher: mathematische *Beweise* statt ausführliches Testen.

1.2 Organisation

Organisation

Vorlesungs- und Übungszeiten.

Vorlesung. Donnerstag, 12:00 - 14:00 Uhr
 Raum HE 101

Großübung. Donnerstag, 14:00 - 16:00 Uhr
 Raum A 151

Tutorien. Insgesamt ca. 20 Tutorien
 zu verschiedenen Zeiten

Rolle der VL, Übung und Tutorien.

- In der *Vorlesung* wird der Stoff vermittelt. Alles, was wir hier machen ist prüfungsrelevant und nur das.
- In der *Großübung* wird der Stoff geübt und an Beispielen erläutert.
- Die *Tutorien* bereiten auf das Lösen von (Prüfungs-) Aufgaben vor.
- Die *freiwilligen Hausaufgaben* bieten die Möglichkeit, selbst Aufgaben zu lösen und korrigiert zu bekommen.

Lernräume.

Räume und Zeiten an denen Sie lernen und an den Aufgaben arbeiten können.

Es sind immer Tutor:innen anwesend, die Sie bei Fragen ansprechen können.

Die ISIS-Seite enthält eine Liste der Zeiten.

Prüfungsform: Portfolio

Prüfung. Das Modul wird als Portfolio geprüft.

Insgesamt können 100 Portfoliopunkte erreicht werden.

Prüfungselemente.

Element	PP	Ersttermin	Zweitermin
Hausaufgabe	25 PP	6.6. - 19.6.	
Multiple-Choice Test	25 PP	31.5., 15-17 Uhr	20.9., 11-13 Uhr
schriftliche Leistungskontrolle	50 PP	29.7., 8-10 Uhr	27.9., 12-14 Uhr

Prüfungszeiträume.

Sie müssen nicht alle Elemente im gleichen Zeitraum absolvieren.

Wir empfehlen das aber, da sie sonst nicht im selben Semester die Prüfung wiederholen können.

Notenschlüssel 1.

≥ 86	1,0
≥ 82	1,3
≥ 78	1,7
≥ 74	2,0
≥ 70	2,3
≥ 66	2,7
≥ 62	3,0
≥ 58	3,3
≥ 54	3,7
≥ 50	4,0
< 50	5,0