Vorkurs Theoretische Informatik

Einführung in die Grundideen und in die Mengenlehre

Arbeitskreis Theoretische Informatik

Montag, 01.10.2018

Fachgruppe Informatik

Übersicht

Allgemeines

Wer sind wir?

- Fachgruppe Informatik
  - Unser Ziel:
    Das Leben der Studierenden während ihres Studiums angenehmer zu gestalten
  - vertreten die studentische Sicht in offiziellen Gremien
  - verleihen Prüfungen aus den früheren Semestern
  - organisieren Veranstaltungen (Spieleabende, Vorkurse, ...)
- AK Theo
  - Teilmenge der Fachgruppe Informatik
  - haben diesen Vorkurs organisiert

Tipps zum Studium

- Nützliche Links:
  - Fachgruppe Informatik:
    `https://fius.informatik.uni-stuttgart.de/`
  - Foliensätze:
    `https://fius.informatik.uni-stuttgart.de/dienste/theo-vorkurs/`
  - Ergänzung Theoretische Informatik 1 (Wintersemester 17/18):
    `www.fmi.uni-stuttgart.de/ti/teaching/w17/eti1/`
- E-Mail der Fachgruppe: fius@informatik.uni-stuttgart.de

Theoretische Informatik

Was ist eigentlich Theoretische Informatik?

- Theoretische Informatik ist die **formale** Herangehensweise an Probleme.
- Diese Probleme befassen sich unter Anderem mit den **formalen** Sprachen.

Anwendung der theoretischen Informatik

- Ist ein bestimmtes Problem lösbar, oder **können** wir gar keine Lösung finden?
- IT-Sicherheit / Kryptographie: Die Sicherheit bestimmter Algorithmen **beweisen**
- Reguläre Ausdrücke
- Künstliche Intelligenz
- Compilerbau
- ...und vieles mehr...

Theoretische Informatik in deinem Studium

Theoretische Informatik I ist Orientierungsprüfung für Informatik, Medieninformatik, Softwaretechnik und Data Science.

- Du musst diese Prüfung spätestens zum Ende des dritten Semester bestanden haben.
- Du musst spätestens zum Ende des zweiten Semesters eine der beiden Orientierungsprüfungen angetreten haben.
- Du kannst die schriftliche Prüfung einmal nachschreiben und hast dann noch einen mündlichen Versuch im selben Semester.

Kennt eure Prüfungsordnung!

Theoretische Informatik in deinem Studium

- Theoretische Informatik I
  Formale Sprachen und Automatentheorie (FSuA)
- Theoretische Informatik II
  Berechenbarkeit und Komplexität (BuK)
- Theoretische Informatik III
  Algorithmen und Diskrete Strukturen (AuDS)

Literatur der Vorlesung

Uwe Schöning: Theoretische Informatik - kurzgefasst [22,99€]

- Die Vorlesung von Prof. Hertrampf richtet sich in weiten Teilen nach diesem Buch.

Boris Hollas: Grundkurs Theoretische Informatik: Mit Aufgaben und Anwendungen [27,99€]

- Weniger formal, dafür intuitiver mit einigen Beispielen und Übungsaufgaben

Dirk W. Hoffmann: Theoretische Informatik

- wird von Joel oft empfohlen

Literatur der Vorlesung

Uwe Schöning: Theoretische Informatik - kurzgefasst [0€]

- Die Vorlesung von Prof. Hertrampf richtet sich in weiten Teilen nach diesem Buch.

Boris Hollas: Grundkurs Theoretische Informatik: Mit Aufgaben und Anwendungen [0€]

- Weniger formal, dafür intuitiver mit einigen Beispielen und Übungsaufgaben

Dirk W. Hoffmann: Theoretische Informatik

- wird von Joel oft empfohlen

Die Bücher sind alle in der Uni-Bib verfügbar, beim Schöning sollte man sich aber beeilen.

Wörter, Sprachen und Mengen

Mengen

- Was ist eine Menge?

Mengen

- Was ist eine Menge?

- Eine Menge
  - ist eine Sammlung von Zeug
  - ist unsortiert
  - enthält keine Duplikate
  - wird mit geschweiften Klammern notiert

Beispiel

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ = Menge der Natürlichen Zahlen
Studenten = {Janette, Julian, Joel, Fabian, ...}
$\{1, 2\} = \{2, 1\} = \{1, 1, 2, 1, 1, 1\}$

Mengen

- Was ist eine Menge?
- Was ist ein Element?

Mengen

- Was ist eine Menge?
- Was ist ein Element?

- Ein Element ist ein Ding aus einer Menge.

Beispiel

1 ist ein Element der **Natürlichen Zahlen**
$1 \in \mathbb{N}$

Janette ist ein Element aus der Menge der **Studenten**
Janette $\in$ **Studenten**

a ist in der Menge $\{u, v, w\}$ nicht enthalten
$a \notin \{u, v, w\}$

Mengen

- Was ist eine Menge?
- Was ist ein Element?
- Was ist eine Teilmenge?

Mengen

- Was ist eine Menge?
- Was ist ein Element?
- Was ist eine Teilmenge?

- Eine Teilmenge ist eine spezielle Auswahl von Elementen einer Menge.

Beispiel

$\{1, 2, 3\}$ ist eine Teilmenge der Natürlichen Zahlen
$\{1, 2, 3\} \subseteq \mathbb{N}$

{Janette} ist eine Teilmenge der **Studenten**
{Janette} $\subseteq$ **Studenten**

Ein paar Definitionen

Eine nichtleere Menge einstelliger Symbole nennen wir Alphabet. Es wird oft dargestellt durch den Bezeichner Σ.

Beispiele

- $\Sigma = \{a, b\}$
- $\Sigma = \{0, 1\}$
- $\Sigma = \{\text{Rechts, Links, Vorwärts, Rückwärts, Start, Stopp, Pause}\}$

Mengen - Mal anders

Ein paar Definitionen

Auf einem Alphabet können wir die Operation $\cdot$, genannt Konkatenation, ausüben.
$\rightarrow$ zum Beispiel ist dann $a \cdot b = ab$
Eine beliebig lange Kette an Symbolen aus dem Alphabet nennen wir ein Wort.

Beispiele

- *abba* ist ein *Wort* über dem *Alphabet* $\Sigma = \{a, b\}$
- 10011101 ist ein *Wort* über dem *Alphabet* $\Sigma = \{0, 1\}$
- StartVorwärtsRechtsVorwärtsStopp ist ein Wort über $\Sigma = \{$Rechts, Links, Vorwärts, Rückwärts, Start, Stopp, Pause$\}$

Wortlängen

Wortlänge und das leere Wort

Eine endlich lange Kette an Symbolen aus dem Alphabet nennen wir ein Wort.

- Wort der Länge 3: z.B. $aaa, abc, \ldots$
- Wort der Länge 2: z.B. $aa, ab, \ldots$
- Wort der Länge 1: z.B. $a, b, c, \ldots$
- Wort der Länge 0: ε

Wir schreiben $|w|$ um Länge des Wortes w abzukürzen.

Wortlängen

Wortlänge und das leere Wort

Eine endlich lange Kette an Symbolen aus dem Alphabet nennen wir ein Wort.

- Wort der Länge 3: z.B. $aaa, abc, \ldots$
- Wort der Länge 2: z.B. $aa, ab, \ldots$
- Wort der Länge 1: z.B. $a, b, c, \ldots$
- Wort der Länge 0: ε

ε *("Epsilon")* nennen wir das "leere Wort".

- Vergleich: Es ist vergleichbar mit einem leerem String,
  also: "" $= \epsilon$
- Achtung: Das leere Wort kann kein Teil eines Alphabets sein,
  da es nicht einstellig ist.

neutrales Element der Konkatenation

Achtung

Wir können bei der Konkatenation auch das leere Wort anhängen. Es verhält sich hierbei als das neutrale Element.
d.h. für ein beliebiges Wort a, ist $a \cdot \epsilon = \epsilon \cdot a = a$

Vergleich

- Bei der Addition von Zahlen ist die 0 das neutrale Element
  $a + 0 = 0 + a = a$
- Bei der Multiplikation von Zahlen ist die 1 das neutrale Element
  $a * 1 = 1 * a = a$

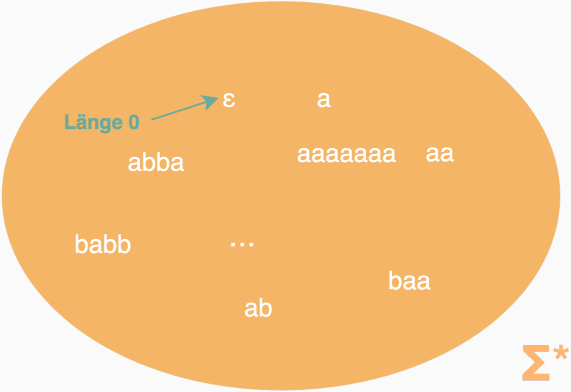

Abbildung 1: Menge von allen Kombinationen der Elemente von Σ heißt Σ^*

Das heißt...

Sei $\Sigma = \{a, b\}$ unser Alphabet.
Wir beschreiben die Menge, die alle Möglichkeiten enthält Elemente aus Σ zu *konkatenieren* mit $\Sigma^* = \{\varepsilon, a, b, ab, ba, aab, aba, \dots\}$.

Das heißt...

Sei $\Sigma = \{a, b\}$ unser Alphabet.
Wir beschreiben die Menge, die alle Möglichkeiten enthält Elemente aus Σ zu *konkatenieren* mit $\Sigma^* = \{\varepsilon, a, b, ab, ba, aab, aba, \ldots\}$.

Achtung

M^* über einer beliebigen Menge M enthält immer das leere Wort ε!
Sogar wenn $M = \{\} = \emptyset$.

Denkpause

Aufgaben

Nenne jeweils 5 der kürzesten Elemente aus Σ^* für die folgenden Alphabete Σ:

Normal

- $\Sigma = \{a\}$
- $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Etwas schwerer

- $\Sigma = \{0, \text{x}, \text{Bieber}\}$
- $\Sigma = \{☺, ☹\}$

Lösungen

Mögliche Lösungen sind …

- $\varepsilon, a, aa, aaa, aaaa \in \{a\}^*$

Lösungen

Mögliche Lösungen sind ...

- $\varepsilon, a, aa, aaa, aaaa \in \{a\}^*$
- $\varepsilon, 0, 1, 2, 3 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^*$

Lösungen

Mögliche Lösungen sind …

- $\varepsilon, a, aa, aaa, aaaa \in \{a\}^*$
- $\varepsilon, 0, 1, 2, 3 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^*$
- $\varepsilon, 0, x, Bieber, xBieber \in \{0, x, Bieber\}^*$

Lösungen

Mögliche Lösungen sind …

- $\varepsilon, a, aa, aaa, aaaa \in \{a\}^*$
- $\varepsilon, 0, 1, 2, 3 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^*$
- $\varepsilon, 0, x, Bieber, xBieber \in \{0, x, Bieber\}^*$
- ε, ☺, ☹, ☺☺, ☺☹ $\in$ {☺, ☹}*

Alphabete und Σ^*

Verständnisabfrage

Denke kurz über folgende Aufgabe nach...

Schwer

Welche Wörter sind in M^* enthalten, wenn $M = \emptyset$ gilt?

- In $M^* = \{\ \}^*$ ist **nur** das leere Wort ε enthalten.

Sprachen

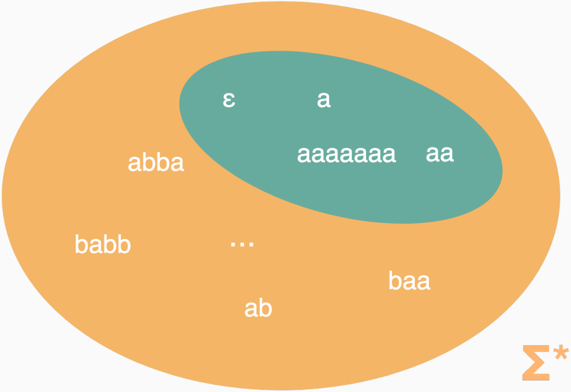

Abbildung 2: Teilmengen unserer Obermenge nennen wir Sprachen

Sprachen beschreiben

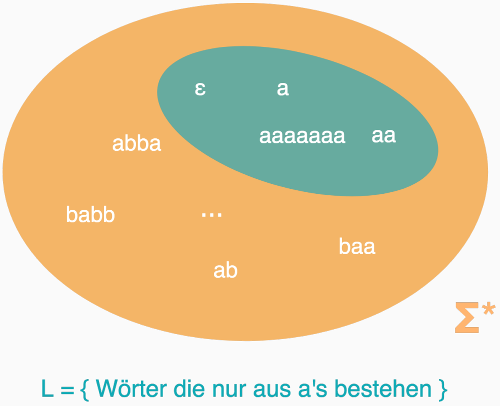

Abbildung 3: Manche Sprachen können wir mit Regeln beschreiben

Sprachen beschreiben

Beispiele für Sprachen in Mengenschreibweise

- $L_1 = \{a^n \mid n \in \mathbb{N}\}$
- $L_2 = \{a^n \mid n \equiv 0 \bmod 2, n \in \mathbb{N}\}$
- $L_3 = \{uv \mid u \in \{a, b\}^*,\ v \in \{a\}\}$
- $L_4 = \{w \mid |w|_a = 3\}$

Was soll das alles? Mehr dazu nach der Pause :)

Murmelpause

Mengenschreibweise

Wie sprechen wir das?

$L_2 = \{a^n \mid n \in \mathbb{N}\}$
Die Sprache L_2 enthält alle Wörter a^n, für die gilt: n stammt aus der Menge der natürlichen Zahlen.

Achtung

In der theoretischen Informatik enthält $\mathbb{N}$ ($\mathbb{N}$ ist die Menge der natürlichen Zahlen) die Zahl 0.

Wie schreiben wir das?

Viele Zeichen hintereinander (konkateniert) können auch einfacher geschrieben werden.

$$
\begin{aligned}
a^0 &= \epsilon \\
a^1 &= a \\
a^2 &= a \cdot a = aa \\
a^3 &= a \cdot a \cdot a = aaa \\
&\vdots \\
a^n &= \underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{n-mal}}
\end{aligned}
$$

Wie schreiben wir das?

- $L_1 = \{0, 2, 4, 6, 8, \dots\} = \{x \mid \text{x ist gerade}\}$
  $L_1 = \{x \mid \text{Es gibt eine Zahl } k \in \mathbb{N} : 2k = x\}$
- $L_2 = \{a^n \mid n \in \mathbb{N}\} = \{\epsilon, a, aa, aaa, aaaa, \dots\}$
- $L_3 = \{a^n b^n \mid n \in \mathbb{N}\} = \{\epsilon, ab, aabb, aaabbb, aaaabbbb, \dots\}$
- $L_4 = \{a^n w \mid n \in \mathbb{N}, w = bccb\} = \{bccb, abccb, aabccb, \dots\}$
  L_4 endet nach einer beliebigen Anzahl von a's immer mit bccb
- $L_5 = \{w \mid |w| = 2, w \in \{a, b\}^*\} = \{aa, bb, ab, ba\}$
  Wörter der Länge 2 aus $\{a, b\}^*$
- $L_6 = \{w \mid |w|_a = 2, w \in \{a, b\}^*\}$
  Wörter mit genau 2 a's aus $\{a, b\}^*$

Denkpause

Aufgaben

Findet Wörter aus den folgenden Sprachen

Normal

- $L_1 = \{a\}$
- $L_2 = \{uv \mid u \in \{a, b\}^*,\ v \in \{c, d\}\}$
- $L_3 = \{w \mid |w| = 3, w \in \{a, b, c\}^*\}$

Etwas Schwerer

- $L_4 = \{a^n \mid n \equiv 1 \bmod 3, n \in \mathbb{N}\}$
- $L_5 = \{w \mid |w|_a = 3, |w|_b = 1, w \in \{a, b, c\}^*\}$
- $L_6 = \{uv \mid u \in \{◀, ▲, ▶, ▼\}^*,\ v \in \{\text{🛑}\}\}$
- $L_7 = \{w \mid |w| = 2, w \in \{a, b\}\}$

Anmerkung: $x \bmod y \equiv z \iff x \div y = w$ Rest z, mit $w, x, y, z \in \mathbb{Z}$

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, …
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, …
  v ist entweder c oder d!

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, ...
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, ...
  v ist entweder c oder d!
- L_3: enthält alle Wörter der Länge 3, deren Buchstaben nur a, b oder c sind.
  $\rightarrow$ aaa, aab, aba, abb, abc, acb, acc, baa, bab, ...

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, ...
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, ...
  v ist entweder c oder d!
- L_3: enthält alle Wörter der Länge 3, deren Buchstaben nur a, b oder c sind.
  $\rightarrow$ aaa, aab, aba, abb, abc, acb, acc, baa, bab, ...
- $L_4 = \{a, aaaa, aaaaaaa, \ldots\}$
  Wörter deren Länge durch 3 geteilt den Rest 1 ergeben.

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, …
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, …
  v ist entweder c oder d!
- L_3: enthält alle Wörter der Länge 3, deren Buchstaben nur a, b oder c sind.
  $\rightarrow$ aaa, aab, aba, abb, abc, acb, acc, baa, bab, …
- $L_4 = \{a, aaaa, aaaaaaa, \ldots\}$
  Wörter deren Länge durch 3 geteilt den Rest 1 ergeben.
- $L_5 = \{caaba, cccbaaa, abaca, aaab, \ldots\}$
  genau 3 a's, genau 1 b, beliebig viele c's, keine Sortierung

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, …
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, …
  v ist entweder c oder d!
- L_3: enthält alle Wörter der Länge 3, deren Buchstaben nur a, b oder c sind.
  $\rightarrow$ aaa, aab, aba, abb, abc, acb, acc, baa, bab, …
- $L_4 = \{a, aaaa, aaaaaaa, \dots\}$
  Wörter deren Länge durch 3 geteilt den Rest 1 ergeben.
- $L_5 = \{caaba, cccbaaa, abaca, aaab, \dots\}$
  genau 3 a’s, genau 1 b, beliebig viele c’s, keine Sortierung
- L_6 = {🛑, ◀🛑, ▲🛑,… , ▼◀▼🛑,…}

Lösungen

- L_1: Enthält **nur** das einzelne Wort a!
- L_2: z.B. c, d, ac, bc, aaac, abababad, ...
  Wort besteht aus zwei Teilen: u z.B. ε, a, b, ababa, ...
  v ist entweder c oder d!
- L_3: enthält alle Wörter der Länge 3, deren Buchstaben nur a, b oder c sind.
  $\rightarrow$ aaa, aab, aba, abb, abc, acb, acc, baa, bab, ...
- $L_4 = \{a, aaaa, aaaaaaa, \dots\}$
  Wörter deren Länge durch 3 geteilt den Rest 1 ergeben.
- $L_5 = \{caaba, cccbaaa, abaca, aaab, \dots\}$
  genau 3 a's, genau 1 b, beliebig viele c's, keine Sortierung
- L_6 = {🛑, ◀🛑, ▲🛑,... , ▼◀▼🛑,...}
- L_7: Enthält **gar kein** Wort!

Mengenoperationen

Mengenoperationen - Schnitt

Schnitt - $A \cap B$
Gegeben zwei Mengen A und B.
In der Schnittmenge liegt alles,
das in Menge A **und** in Menge B ist.

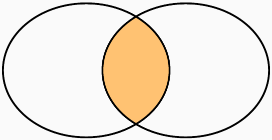

Abbildung 4: Veranschaulichung der Schnittmenge

Vereinigung - $A \cup B$

Gegeben zwei Mengen A und B.
In der Vereinigung liegt alles, das nur in A, nur in B **oder** in beiden Mengen liegt.

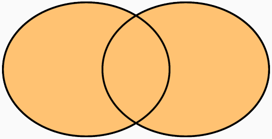

Abbildung 5: Veranschaulichung der Vereinigung

Mengenoperationen - Komplement

Komplement - $\bar{A}$

Gegeben sei eine Menge A.
Im Komplement der Menge A liegen alle Elemente, die in Σ^*, aber nicht in der Menge A selbst liegen.

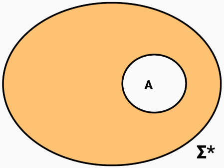

Abbildung 6: Veranschaulichung des Komplements

Komplement - $\bar{A}$

Gegeben sei eine Menge A.
Im Komplement der Menge A liegen alle Elemente, die in Σ^*, aber nicht in der Menge A selbst liegen.

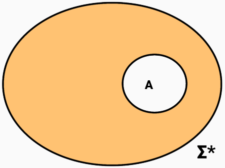

Abbildung 6: Veranschaulichung des Komplements

Anmerkung: Kann auch geschrieben werden als $\Sigma^* \setminus A$.
(gesprochen Σ^* *"ohne"* A)

Mengenoperationen

Berechne folgende Mengen

Normal

- M_1: $\{a\} \cup \{b\}$
- M_2: $\{\} \cap \{u, v, w\}$
- M_3: $\mathbb{N} \cup \mathbb{Z}$
- M_4: $\overline{\{a^n | n \text{ ist gerade}\}}$, über dem Alphabet $\{a\}$

Schwer bis sehr schwer

- M_5: $\{a, b, c\} \cap \{a, \{b, c\}\}$
- M_6: $\{u \mid |u| \equiv 0 \mod 2, u \in \{a, b\}^*\}$
  $\cup \{v \mid |v| \equiv 0 \mod 4, v \in \{a, b\}^*\}$
- M_7: $\overline{\{a^n | n \text{ ist gerade}\}}$, über dem Alphabet $\{a, b\}$

Lösungen

- $M_1 = \{a, b\}$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$
- $M_3 = \mathbb{Z}$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$
- $M_3 = \mathbb{Z}$
- $M_4 = \{a^n \mid \text{n ist ungerade}\},$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$
- $M_3 = \mathbb{Z}$
- $M_4 = \{a^n \mid \text{n ist ungerade}\}$,
- $M_5 = \{a\}$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$
- $M_3 = \mathbb{Z}$
- $M_4 = \{a^n \mid \text{n ist ungerade}\}$,
- $M_5 = \{a\}$
- $M_6 = \{u \mid |u| = 0 \bmod 2, u \in \{a, b\}^*\}$

Lösungen

- $M_1 = \{a, b\}$
- $M_2 = \emptyset$
- $M_3 = \mathbb{Z}$
- $M_4 = \{a^n \mid \text{n ist ungerade}\}$,
- $M_5 = \{a\}$
- $M_6 = \{u \mid |u| = 0 \text{ mod } 2, u \in \{a, b\}^*\}$
- M_7: $\{a^n | n \text{ ist ungerade}\} \cup \{w | w \in \{a, b\}, |w|_b > 1\}$

Wiederholung

Das können wir jetzt beantworten

Einführung

- Theoretische Informatik ist ganz schön wichtig…
- …für mein Studium.

Das können wir jetzt beantworten

Mengen, Sprachen, Elemente

- Was ist eine Menge?
- Was ist eine Sprache?
- Was sind Elemente einer Sprache/Menge?

Das können wir jetzt beantworten

Alphabete, Σ^*

- Was ist ein Alphabet?, Was ist ein Wort?
- Wie funktioniert die Konkatenation?
- Was ist der Unterschied zwischen Σ und Σ^*?
- Das leere Wort: Welches ist das *kleinste* Alphabet, mit $\varepsilon \in \Sigma^*$?
- Bilden von Σ^* für gegebenes Alphabet Σ

Das können wir jetzt beantworten

Operationen auf Mengen

- Wie funktionieren Vereinigung, Schnitt und Komplement?
- Wie bilde ich Vereinigungen oder Schnittmengen zweier Mengen?
- Wie bilde ich das Komplement einer Menge?
- Wie kann ich Sprachen formal beschreiben?
- Hantieren mit verschiedenen seltsamen Mengen und den Verknüpfungen

Noch Fragen?

Glossar

Abk.	Bedeutung	Was?!
$\mathbb{N}$	natürliche Zahlen (mit 0)	In der theoretischen Informatik enthält $\mathbb{N}$ die 0: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	ganze Zahlen	
$\mathbb{Q}$	rationale Zahlen	können als Bruch dargestellt werden
Σ	Sigma	mit diesem Zeichen wird oft das Alphabet (die Menge an verwendbaren Symbolen) repräsentiert
Σ^*	Sigma Stern	Menge aller Möglichkeiten Elemente aus Σ hintereinander zu schreiben
$\emptyset$	{}	leere Menge
:	sodass	z.B. $\forall a, b \in \mathbb{Z}$:a teilt b