Grundbegriffe der Informatik

Einheit 3: Alphabete, Abbildungen, Aussagenlogik

Prof. Dr. Tanja Schultz

Karlsruher Institut für Technologie, Fakultät für Informatik

Wintersemester 2012/2013

- *„Die Abbildung* $U : A_U \to \mathbb{N}_0$ *ist injektiv."*
  Das ist eine Aussage. Sie ist *wahr*.
- *„Die Abbildung* $U : A_U \to \mathbb{N}_0$ *ist surjektiv."*
  Das ist auch eine Aussage. Sie ist *falsch*.
- Aussagen sind Sätze, die „objektiv" wahr oder falsch sind.
  Dazu braucht man eine Interpretation der Zeichen, aus denen die zu Grunde liegende Nachricht zusammengesetzt ist.
- Wir bauen ganz massiv darauf, dass es keine Missverständnisse durch unterschiedliche Interpretationsmöglichkeiten gibt.
  Was ist $\mathbb{N}$? Enthält es die 0?
- Manche umgangssprachlichen Sätze sind nicht wahr oder falsch, sondern sinnlos:

  > *„Ein Barbier ist ein Mann, der genau die Männer rasiert, die sich nicht selbst rasieren."*

  Rasiert sich ein Barbier selbst . . . ?

Häufig setzt man aus einfachen Aussagen ($\mathcal{A}$ und $\mathcal{B}$) kompliziertere Aussagen auf eine der folgenden Arten zusammen:

logische Negation: „Nicht $\mathcal{A}$“
kurz $\neg\mathcal{A}$.

logisches Und: „$\mathcal{A}$ und $\mathcal{B}$“
kurz $\mathcal{A} \wedge \mathcal{B}$.

logisches Oder: „$\mathcal{A}$ oder $\mathcal{B}$“
kurz $\mathcal{A} \vee \mathcal{B}$.

logische Implikation: „Wenn $\mathcal{A}$, dann $\mathcal{B}$“
kurz $\mathcal{A} \Rightarrow \mathcal{B}$.

- Ob eine so zusammengesetzte Aussage wahr oder falsch ist, hängt dabei *nicht* vom konkreten Inhalt der Aussagen ab!
- Wesentlich ist nur, welche Wahrheitswerte die Aussagen $\mathcal{A}$ und $\mathcal{B}$ haben.

Wahrheitswerte aussagenlogischer Formeln

- *aussagenlogische Formel*
  - nach obigen Regeln zusammengesetzt und
  - statt elementarer Aussagen einfach *Aussagevariablen*,
  - die als Werte „wahr“ oder „falsch“ annehmen können.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	wahr	wahr
wahr	falsch	falsch	falsch	wahr	falsch
wahr	wahr	falsch	wahr	wahr	wahr

Wahrheitswerte aussagenlogischer Formeln

- *aussagenlogische Formel*
  - nach obigen Regeln zusammengesetzt und
  - statt elementarer Aussagen einfach *Aussagevariablen*,
  - die als Werte „wahr“ oder „falsch“ annehmen können.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	wahr	wahr
wahr	falsch	falsch	falsch	wahr	falsch
wahr	wahr	falsch	wahr	wahr	wahr

Wahrheitswerte aussagenlogischer Formeln

- *aussagenlogische Formel*
  - nach obigen Regeln zusammengesetzt und
  - statt elementarer Aussagen einfach *Aussagevariablen*,
  - die als Werte „wahr“ oder „falsch“ annehmen können.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	wahr	wahr
wahr	falsch	falsch	falsch	wahr	falsch
wahr	wahr	falsch	wahr	wahr	wahr

- *aussagenlogische Formel*
  - nach obigen Regeln zusammengesetzt und
  - statt elementarer Aussagen einfach *Aussagevariablen*,
  - die als Werte „wahr“ oder „falsch“ annehmen können.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	wahr	wahr
wahr	falsch	falsch	falsch	wahr	falsch
wahr	wahr	falsch	wahr	wahr	wahr

- *aussagenlogische Formel*
  - nach obigen Regeln zusammengesetzt und
  - statt elementarer Aussagen einfach *Aussagevariablen*,
  - die als Werte „wahr“ oder „falsch“ annehmen können.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$
falsch	falsch	wahr	falsch	falsch	wahr
falsch	wahr	wahr	falsch	wahr	wahr
wahr	falsch	falsch	falsch	wahr	falsch
wahr	wahr	falsch	wahr	wahr	wahr

- Das “Logische Oder“ $\vee$ ist „inklusiv“ (und nicht „exklusiv“):
  Wenn A und B beide wahr sind, dann auch $A \vee B$.
- Man kann für komplizierte Aussagen anhand der Tabellen „ausrechnen“, wann sie wahr und wann sie falsch sind.
  - einfaches Rechnen bzw. scharfes Hinsehen:
    die Aussagen $\neg(A \vee B)$ und $(\neg A) \wedge (\neg B)$ immer gleichzeitig wahr bzw. falsch sind.
  - Gleiches gilt für $\neg\neg A$ und A.
  - Solche Aussagen nennt man *äquivalent*.

A	B	$\neg A$	$\neg B$	$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$
falsch	falsch	wahr	wahr		
falsch	wahr	wahr	falsch		
wahr	falsch	falsch	wahr		
wahr	wahr	falsch	falsch		

Bindungsstärke von $\neg$, $\wedge$, $\vee$ und $\Rightarrow$

- Um Klammern zu sparen, legt man z. B. in der Arithmetik Vorrangregeln fest:

$$x \cdot y + z \qquad \text{bedeutet} \qquad (x \cdot y) + z$$

- Analog in der Aussagenlogik:

Was soll $\qquad \neg A \wedge B \vee C \Rightarrow D \qquad$ bedeuten?

- wir vereinbaren:
  - $\neg$ bindet am stärksten
  - $\wedge$ bindet weniger stark
  - $\vee$ bindet noch schwächer
  - $\Rightarrow$ bindet am schwächsten

Bindungsstärke von $\neg$, $\wedge$, $\vee$ und $\Rightarrow$

- Um Klammern zu sparen, legt man z. B. in der Arithmetik Vorrangregeln fest:

$$x \cdot y + z \qquad \text{bedeutet} \qquad (x \cdot y) + z$$

- Analog in der Aussagenlogik:

Was soll $\neg A \wedge B \vee C \Rightarrow D$ bedeuten?

das $(\,(\,(\neg A) \wedge B) \vee C\,) \Rightarrow D$

- wir vereinbaren:
  - $\neg$ bindet am stärksten
  - $\wedge$ bindet weniger stark
  - $\vee$ bindet noch schwächer
  - $\Rightarrow$ bindet am schwächsten

Definition der logischen Implikation $\Rightarrow$

- Beobachtung: Bei $A \wedge B$ und $A \vee B$ hängt der Wahrheitswert der ganzen Formel
  - nur von den Wahrheitswerten von A und B ab, und
  - nicht davon, worum es in den Aussagen A und B geht.
- Ziel: Für die logische Implikation $A \Rightarrow B$ wollen wir das auch
- Der Wahrheitswert von $A \Rightarrow B$ („wenn A, dann B") soll nur von den Wahrheitswerten von A und B abhängen!
- relativ unstrittig (?) ist, was sein soll, wenn A wahr ist:
  - wenn A wahr ist und B falsch, dann soll $A \Rightarrow B$ falsch sein
  - wenn A und B wahr sind, dann soll auch $A \Rightarrow B$ wahr sein

A	B	$A \Rightarrow B$
falsch	falsch	
falsch	wahr	
wahr	falsch	falsch
wahr	wahr	wahr

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil" von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg\neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

Definition der logischen Implikation $\Rightarrow$ (2)

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg \neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg \neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

Definition der logischen Implikation $\Rightarrow$ (2)

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg\neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

Definition der logischen Implikation $\Rightarrow$ (2)

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg\neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

Definition der logischen Implikation $\Rightarrow$ (2)

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg\neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg\neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

- Um die restlichen beiden Fälle der logischen Implikation $A \Rightarrow B$ zu klären, nähern wir uns aus einem anderen Blickwinkel. Die Implikation $A \Rightarrow B$ wird vielleicht auch so noch etwas klarer:
  - Was ist denn das „Gegenteil“ von $A \Rightarrow B$?
  - Doch wohl $A \wedge \neg B$.
  - Also ist $A \Rightarrow B$ äquivalent zu $\neg(A \wedge \neg B)$
  - Das ist äquivalent zu $(\neg A) \vee (\neg \neg B)$ und
  - das ist äquivalent zu $(\neg A) \vee B$.

A	B	$A \wedge \neg B$	$A \Rightarrow B$
falsch	falsch	falsch	wahr
falsch	wahr	falsch	wahr
wahr	falsch	wahr	falsch
wahr	wahr	falsch	wahr

- Auswirkung auf Beweise
  - Man muss nur etwas tun, wenn A wahr ist.

- Eine nützliche Notation aus der *Prädikatenlogik*:

  Allquantor $\forall$ *Existenzquantor* $\exists$

- In der puren Form hat eine quantifizierte Aussage eine der Formen
$$\forall x\ A(x) \qquad \text{oder} \qquad \exists x\ A(x)$$
- Dabei soll $A(x)$ eine Aussage sein, die von einer Variablen x abhängt (oder jedenfalls abhängen kann). A kann weitere Quantoren enthalten.
- $\forall x\ A(x)$ ist zu lesen als: „Für alle x gilt: $A(x)$“.
- $\exists x\ A(x)$ ist zu lesen als: „Es gibt ein x mit: $A(x)$“.
- Zum Beispiel:
$$\forall x\ (x \in \mathbb{N}_0 \Rightarrow \exists y\ (y \in \mathbb{N}_0 \wedge y = x + 1))$$

Allquantor und Existenzquantor (2)

- noch mal dieses Beispiel:

$$\forall x\ (x \in \mathbb{N}_0 \Rightarrow \exists y\ (y \in \mathbb{N}_0 \land y = x + 1))$$

- Das hat man oft: Eine Aussage gilt nicht für alle x, sondern nur für alle x aus einer gewissen (Teil-)Menge M.
- Abkürzung: Statt

$$\forall x\ (x \in M \Rightarrow B(x))$$

schreibt man einfach

$$\forall x \in M :\ B(x)$$

- Doppelpunkt sinnvoll, wenn Lesbarkeit dadurch verbessert
- Obiges Beispiel wird zu:

$$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y = x + 1$$

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

Allquantor und Existenzquantor: weitere Beispiele

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

Allquantor und Existenzquantor: weitere Beispiele

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

Allquantor und Existenzquantor: weitere Beispiele

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

Allquantor und Existenzquantor: weitere Beispiele

$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : x \leq y$	ist wahr
$\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist falsch
$\neg\exists x \in \mathbb{N}_0 : \forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \neg\forall y \in \mathbb{N}_0 : y \leq x$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : \neg(y \leq x)$	ist wahr
$\forall x \in \mathbb{N}_0 : \exists y \in \mathbb{N}_0 : y > x$	ist wahr

Bindungsstärke von Quantoren

Vereinbarung: die Quantoren binden *schwächer* als die binären aussagenlogischen Operatoren.
Also bedeutet

$$\forall x \in M : A(x) \Rightarrow B(x)$$

das gleiche wie

$$\forall x \in M : (A(x) \Rightarrow B(x))$$

Was ist wichtig

Das sollten Sie mitnehmen:

- *Alphabete*
  - ASCII und Unicode sind wichtige Beispiele
- *binäre Relationen*
- *Abbildungen*
  - Spezialfälle: injektiv, surjektiv, bijektiv, partiell
- *Aussagenlogik*
- *Existenz- und Allquantor*

Das sollten Sie üben:

- Benutzung der Begriffe Alphabet, Relation, Abbildung
- Hinschreiben logischer Formeln
- Umgang mit $\Rightarrow$

Grundbegriffe der Informatik

Einheit 4: Wörter und vollständige Induktion

Prof. Dr. Tanja Schultz

Karlsruher Institut für Technologie, Fakultät für Informatik

Wintersemester 2012/2013

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Ein *Wort über einem Alphabet A* ist eine Folge von Zeichen aus A.

`Apfelmus`

Ein *Wort über einem Alphabet A* ist eine Folge von Zeichen aus A.

`Milchreis`

Symbole dürfen mehrfach vorkommen.

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Das Leerzeichen

- man benutzt es heutzutage (jedenfalls z. B. in der deutschen Schrift) ständig, aber
- ... in vielen Schriftsystemen allerdings gar nicht (z. B. Chinesisch) oder nicht konsistent mit Worteinheiten (z. B. Thai, Vietnamesisch)

Vietnamesisch in Quốc Ngữ	**in Hán Nôm**
Tất cả mọi người sinh ra đều được tự do và bình đẳng về nhân phẩm và quyền. Mọi con người đều được tạo hoá ban cho lý trí và lương tâm và cần phải đối xử với nhau trong tình bằng hữu.	畢哿每𠊛生𠚢調得自由吧平等術人品吧權。每猑𠊛調得造化班朱理智吧良心吧懃沛對處佘饒𥪝情朋友。

- Für uns ist es ein Zeichen wie alle anderen auch; der Deutlichkeit wegen manchmal explizit ␣ geschrieben.
- Konsequenz: z. B. `Hallo␣Welt` ist *eine* Folge von Zeichen, also nur *ein* Wort (und nicht zwei)

Eine formale Definition von Wörtern

- Formale Definition von Wörtern:
- Sinn der Übung
  - an harmlosem Beispiel Dinge üben, die später wichtig werden
  - aber nicht: eine einfache Sache möglichst kompliziert darzustellen
- das Wesentliche an einer „Folge“ oder „Liste“ (von Zeichen)?
- Reihenfolge; deutlich gemacht z. B. durch Nummerierung:

0	1	2	3	4	5	6	7	8
M	i	l	c	h	r	e	i	s

- definiere für jede natürliche Zahl $n \geq 0$ die Menge der n kleinsten nichtnegativen ganzen Zahlen

$$\mathbb{G}_n = \{i \in \mathbb{N}_0 \mid 0 \leq i \wedge i < n\}$$

- Beispiele: $\mathbb{G}_4 = \{0, 1, 2, 3\}$, $\mathbb{G}_1 = \{0\}$ und $\mathbb{G}_0 = \{\}$

Eine formale Definition von Wörtern

- Formale Definition von Wörtern:
- Sinn der Übung
  - an harmlosem Beispiel Dinge üben, die später wichtig werden
  - aber nicht: eine einfache Sache möglichst kompliziert darzustellen
- das Wesentliche an einer „Folge“ oder „Liste“ (von Zeichen)?
- Reihenfolge; deutlich gemacht z. B. durch Nummerierung:

0	1	2	3	4	5	6	7	8
M	i	l	c	h	r	e	i	s

- definiere für jede natürliche Zahl $n \geq 0$ die Menge der n kleinsten nichtnegativen ganzen Zahlen

$$\mathbb{G}_n = \{i \in \mathbb{N}_0 \mid 0 \leq i \wedge i < n\}$$

- Beispiele: $\mathbb{G}_4 = \{0, 1, 2, 3\}$, $\mathbb{G}_1 = \{0\}$ und $\mathbb{G}_0 = \{\}$

Eine formale Definition von Wörtern

- Formale Definition von Wörtern:
- Sinn der Übung
  - an harmlosem Beispiel Dinge üben, die später wichtig werden
  - aber nicht: eine einfache Sache möglichst kompliziert darzustellen
- das Wesentliche an einer „Folge“ oder „Liste“ (von Zeichen)?
- Reihenfolge; deutlich gemacht z. B. durch Nummerierung:

0	1	2	3	4	5	6	7	8
`M`	`i`	`l`	`c`	`h`	`r`	`e`	`i`	`s`

- definiere für jede natürliche Zahl $n \geq 0$ die Menge der n kleinsten nichtnegativen ganzen Zahlen

$$\mathbb{G}_n = \{i \in \mathbb{N}_0 \mid 0 \leq i \land i < n\}$$

- Beispiele: $\mathbb{G}_4 = \{0, 1, 2, 3\}$, $\mathbb{G}_1 = \{0\}$ und $\mathbb{G}_0 = \{\}$

Eine formale Definition von Wörtern

- Formale Definition von Wörtern:
- Sinn der Übung
  - an harmlosem Beispiel Dinge üben, die später wichtig werden
  - aber nicht: eine einfache Sache möglichst kompliziert darzustellen
- das Wesentliche an einer „Folge“ oder „Liste“ (von Zeichen)?
- Reihenfolge; deutlich gemacht z. B. durch Nummerierung:

0	1	2	3	4	5	6	7	8
`M`	`i`	`l`	`c`	`h`	`r`	`e`	`i`	`s`

- definiere für jede natürliche Zahl $n \geq 0$ die Menge der n kleinsten nichtnegativen ganzen Zahlen

$$\mathbb{G}_n = \{i \in \mathbb{N}_0 \mid 0 \leq i \wedge i < n\}$$

- Beispiele: $\mathbb{G}_4 = \{0, 1, 2, 3\}$, $\mathbb{G}_1 = \{0\}$ und $\mathbb{G}_0 = \{\}$

Eine formale Definition von Wörtern

- Formale Definition von Wörtern:
- Sinn der Übung
  - an harmlosem Beispiel Dinge üben, die später wichtig werden
  - aber nicht: eine einfache Sache möglichst kompliziert darzustellen
- das Wesentliche an einer „Folge“ oder „Liste“ (von Zeichen)?
- Reihenfolge; deutlich gemacht z. B. durch Nummerierung:

0	1	2	3	4	5	6	7	8
`M`	`i`	`l`	`c`	`h`	`r`	`e`	`i`	`s`

- definiere für jede natürliche Zahl $n \geq 0$ die Menge der n kleinsten nichtnegativen ganzen Zahlen

$$\mathbb{G}_n = \{i \in \mathbb{N}_0 \mid 0 \leq i \land i < n\}$$

- Beispiele: $\mathbb{G}_4 = \{0, 1, 2, 3\}$, $\mathbb{G}_1 = \{0\}$ und $\mathbb{G}_0 = \{\}$

Eine formale Definition von Wörtern

- Ein *Wort* ist eine *surjektive* Abbildung $w : \mathbb{G}_n \to A$.
  - Beispiel: Wort $w = \texttt{hallo}$
  - wird formal zur Abbildung $w : \mathbb{G}_5 \to \{\texttt{a}, \texttt{h}, \texttt{l}, \texttt{o}\}$ mit $w(0) = \texttt{h}$, $w(1) = \texttt{a}$, $w(2) = \texttt{l}$, $w(3) = \texttt{l}$ und $w(4) = \texttt{o}$.
- Wir machen uns klar, dass $w : \mathbb{G}_n \to A$ eine Abbildung ist
  - In der letzten Vorlesung haben wir gelernt, dass *Abbildungen* solche Relationen $R \subseteq A \times B$ sind, die linkstotal und rechtseindeutig sind (Schreibweise $R : A \to B$).
  - Linkstotal: für jedes $a \in A$ existiert ein $b \in B$ mit $(a, b) \in R$.
  - Rechtseindeutig: für kein $a \in A$ gibt es zwei $b_1, b_2 \in B$ mit $b_1 \neq b_2$, so dass sowohl $(a, b_1) \in R$ als auch $(a, b_2) \in R$ ist.
- Wir machen uns klar, dass $w : \mathbb{G}_n \to A$ eine *surjektive* Abbildung ist
  - $R \subseteq A \times B$ heißt rechtstotal oder surjektiv, wenn für jedes $b \in B$ ein $a \in A$ existiert, für das $(a, b) \in R$ ist.

Eine formale Definition von Wörtern

- Ein *Wort* ist eine *surjektive* Abbildung $w : \mathbb{G}_n \to A$.
- n heißt die *Länge eines Wortes*, geschrieben $|w|$

- Sie denken erst einmal an Wortlängen $n \geq 1$?
  - ist in Ordnung
  - das leere Wort ε (mit Länge 0) kommt gleich noch
- Beispiel:
  - Wort $w = \texttt{hallo}$ wird
  - formal zur Abbildung $w : \mathbb{G}_5 \to \{\texttt{a}, \texttt{h}, \texttt{l}, \texttt{o}\}$ mit $w(0) = \texttt{h}$, $w(1) = \texttt{a}$, $w(2) = \texttt{l}$, $w(3) = \texttt{l}$ und $w(4) = \texttt{o}$.
- Ist *das umständlich!*
  - ja, aber
  - manchmal formalistische Auffassung von Wörtern vorteilhaft
  - manchmal vertraute Auffassung von Wörtern vorteilhaft
  - wir wechseln erst einmal hin und her

Eine formale Definition von Wörtern

- Ein *Wort* ist eine *surjektive* Abbildung $w : \mathbb{G}_n \to A$.
- n heißt die *Länge eines Wortes*, geschrieben $|w|$

- Sie denken erst einmal an Wortlängen $n \geq 1$?
  - ist in Ordnung
  - das leere Wort ε (mit Länge 0) kommt gleich noch
- Beispiel:
  - Wort $w = \mathtt{hallo}$ wird
  - formal zur Abbildung $w : \mathbb{G}_5 \to \{\mathtt{a}, \mathtt{h}, \mathtt{l}, \mathtt{o}\}$ mit $w(0) = \mathtt{h}$, $w(1) = \mathtt{a}$, $w(2) = \mathtt{l}$, $w(3) = \mathtt{l}$ und $w(4) = \mathtt{o}$.
- Ist *das umständlich!*
  - ja, aber
  - manchmal formalistische Auffassung von Wörtern vorteilhaft
  - manchmal vertraute Auffassung von Wörtern vorteilhaft
  - wir wechseln erst einmal hin und her

Eine formale Definition von Wörtern

- Ein *Wort* ist eine *surjektive* Abbildung $w : \mathbb{G}_n \to A$.
- n heißt die *Länge eines Wortes*, geschrieben $|w|$

- Sie denken erst einmal an Wortlängen $n \geq 1$?
  - ist in Ordnung
  - das leere Wort ε (mit Länge 0) kommt gleich noch
- Beispiel:
  - Wort $w = \mathtt{hallo}$ wird
  - formal zur Abbildung $w : \mathbb{G}_5 \to \{\mathtt{a}, \mathtt{h}, \mathtt{l}, \mathtt{o}\}$ mit $w(0) = \mathtt{h}$, $w(1) = \mathtt{a}$, $w(2) = \mathtt{l}$, $w(3) = \mathtt{l}$ und $w(4) = \mathtt{o}$.
- Ist *das umständlich!*
  - ja, aber
  - manchmal formalistische Auffassung von Wörtern vorteilhaft
  - manchmal vertraute Auffassung von Wörtern vorteilhaft
  - wir wechseln erst einmal hin und her

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A:
  alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - a und b
  - aa, ab, ba und bb
  - aaa, aab, aba, abb, baa, bab, bba und bbb
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen
  $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- *A^*: Menge aller Wörter* über einem Alphabet A:
  alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - a und b
  - aa, ab, ba und bb
  - aaa, aab, aba, abb, baa, bab, bba und bbb
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen
  $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - `a` und `b`
  - `aa`, `ab`, `ba` und `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba` und `bbb`
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - a und b
  - aa, ab, ba und bb
  - aaa, aab, aba, abb, baa, bab, bba und bbb
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A:
  alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - a und b
  - aa, ab, ba und bb
  - aaa, aab, aba, abb, baa, bab, bba und bbb
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen
  $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - `a` und `b`
  - `aa`, `ab`, `ba` und `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba` und `bbb`
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - `a` und `b`
  - `aa`, `ab`, `ba` und `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba` und `bbb`
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\texttt{a}, \texttt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - `a` und `b`
  - `aa`, `ab`, `ba` und `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba` und `bbb`
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A:
  alle Wörter, die nur Zeichen aus A enthalten
- Beispiel: $A = \{\mathtt{a}, \mathtt{b}\}$.
  Dann enthält A^* zum Beispiel die Wörter
  - `a` und `b`
  - `aa`, `ab`, `ba` und `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba` und `bbb`
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)
  - Beachte: es gibt unendlich viele Wörter
    die aber alle *endliche* Länge haben!
- A^* formalistisch: die Menge aller surjektiven Abbildungen
  $w : \mathbb{G}_n \to B$ mit $n \in \mathbb{N}_0$ und $B \subseteq A$.

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

- Zählen
  - man fängt erst mal mit eins an
  - später: oh, die Null ist auch nützlich
- Analogon bei Wörtern: das leere Wort
  - Es besteht aus 0 Symbolen.
  - Damit man es nicht übersieht, *schreiben wir* ε dafür
  - erfordert ein bisschen Abstraktionsvermögen
- vielleicht hilft die formalistische Definition:

$$\varepsilon : \mathbb{G}_0 \to \{\} \qquad \text{also} \qquad \varepsilon : \{\} \to \{\}$$

  - Stört Sie der leere Definitionsbereich oder/und der Zielbereich?
  - Denken Sie an Abbildungen als spezielle Relationen
  - Es gibt nur eine Relation $R \subseteq \{\} \times \{\} = \{\}$, nämlich $R = \{\}$.
  - Sie ist linkstotal und rechtseindeutig, also Abbildung
  - und sogar rechtstotal, also surjektiv.
  - Also ist es richtig von *dem* leeren Wort zu sprechen.

Das leere Wort

- Zählen
  - man fängt erst mal mit eins an
  - später: oh, die Null ist auch nützlich
- Analogon bei Wörtern: das leere Wort
  - Es besteht aus 0 Symbolen.
  - Damit man es nicht übersieht, *schreiben wir ε* dafür
  - erfordert ein bisschen Abstraktionsvermögen
- vielleicht hilft die formalistische Definition:

$$\varepsilon : \mathbb{G}_0 \to \{\} \qquad \text{also} \qquad \varepsilon : \{\} \to \{\}$$

  - Stört Sie der leere Definitionsbereich oder/und der Zielbereich?
  - Denken Sie an Abbildungen als spezielle Relationen
  - Es gibt nur eine Relation $R \subseteq \{\} \times \{\} = \{\}$, nämlich $R = \{\}$.
  - Sie ist linkstotal und rechtseindeutig, also Abbildung
  - und sogar rechtstotal, also surjektiv.
  - Also ist es richtig von *dem* leeren Wort zu sprechen.

- Zählen
  - man fängt erst mal mit eins an
  - später: oh, die Null ist auch nützlich
- Analogon bei Wörtern: das leere Wort
  - Es besteht aus 0 Symbolen.
  - Damit man es nicht übersieht, *schreiben wir ε* dafür
  - erfordert ein bisschen Abstraktionsvermögen
- vielleicht hilft die formalistische Definition:

$$\varepsilon : \mathbb{G}_0 \to \{\} \qquad \text{also} \qquad \varepsilon : \{\} \to \{\}$$

  - Stört Sie der leere Definitionsbereich oder/und der Zielbereich?
  - Denken Sie an Abbildungen als spezielle Relationen
  - Es gibt nur eine Relation $R \subseteq \{\} \times \{\} = \{\}$, nämlich $R = \{\}$.
  - Sie ist linkstotal und rechtseindeutig, also Abbildung
  - und sogar rechtstotal, also surjektiv.
  - Also ist es richtig von *dem* leeren Wort zu sprechen.

Das leere Wort als Element von Mengen

- Das leere Wort ist „etwas“.
- Die Kardinalität der Menge $\{\varepsilon, \texttt{abaa}, \texttt{bbbababb}\}$ ist

$$|\{\varepsilon, \texttt{abaa}, \texttt{bbbababb}\}| = 3$$

- Die Kardinalität der Menge $\{\varepsilon\}$ ist

$$|\{\varepsilon\}| = 1$$

  Das ist nicht die leere Menge!
- Die Kardinalität der Menge $\{\}$ ist

$$|\{\}| = 0$$

  Das ist die leere Menge.

Überblick

Wörter
- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern
- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Wörter einer festen Länge n

- *A^n: Menge aller Wörter der Länge n* über dem Alphabet A
- Beispiel: Ist $A = \{\mathtt{a}, \mathtt{b}\}$, dann ist

$$
\begin{aligned}
A^0 &= \{\varepsilon\} \\
A^1 &= \{\mathtt{a}, \mathtt{b}\} \\
A^2 &= \{\mathtt{aa}, \mathtt{ab}, \mathtt{ba}, \mathtt{bb}\} \\
A^3 &= \{\mathtt{aaa}, \mathtt{aab}, \mathtt{aba}, \mathtt{abb}, \mathtt{baa}, \mathtt{bab}, \mathtt{bba}, \mathtt{bbb}\}
\end{aligned}
$$

- Also ist sozusagen die Menge A^* aller Wörter über dem Alphabet A

$$A^* = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \cdots$$

aber diese Pünktchen „...“ sind nicht schön
- Bessere Schreibweise:

$$A^* = \bigcup_{i=0}^{\infty} A^i$$

- berechtigte Frage: Was soll denn

$$\bigcup_{i=0}^{\infty} M_i$$

  genau bedeuten?
- Das hier:

$$\bigcup_{i=0}^{\infty} M_i = \{x \mid \exists i : x \in M_i\}$$

  also alle Elemente, die in mindestens einem M_i enthalten sind.
- Das ∞-Zeichen in obiger Schreibweise ist gefährlich. Beachte:
  - i kann nicht „den Wert Unendlich" annehmen.
  - i durchläuft die unendlich vielen Werte aus $\mathbb{N}_0$.
  - Aber jede dieser Zahlen ist *endlich*!
  - d. h. es gibt unendlich viele Wörter, aber alle sind von endlicher Länge

Überblick

Wörter
- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern
- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Konkatenation von Wörtern: anschaulich

- ganz einfach: die Hintereinanderschreibung zweier Wörter
- Operationssymbol üblicherweise der Punkt „$\cdot$“, den man wie bei der Multiplikation manchmal weglässt
- Beispiel:

$$\mathtt{SCHRANK} \cdot \mathtt{SCHLÜSSEL} = \mathtt{SCHRANKSCHLÜSSEL}$$

oder

$$\mathtt{SCHLÜSSEL} \cdot \mathtt{SCHRANK} = \mathtt{SCHLÜSSELSCHRANK}$$

- Beachte: Reihenfolge ist wichtig!

$$\mathtt{SCHRANKSCHLÜSSEL} \neq \mathtt{SCHLÜSSELSCHRANK}$$

Konkatenation von Wörtern: formal

- Wörter als Listen von Zeichen, genauer
- surjektive Abbildungen $w : \mathbb{G}_n \to A$
- Beispiel

$$
\begin{array}{cccccccccc}
 & 0 & 1 & 2 & 3 & 4 & & 0 & 1 & 2 \\
 & \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \cdot & \mathtt{M} & \mathtt{U} & \mathtt{S}
\end{array}
$$

$$
\begin{array}{ccccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
= & \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \mathtt{M} & \mathtt{U} & \mathtt{S}
\end{array}
$$

- definiere

$$
\begin{aligned}
w_1 \cdot w_2 : \mathbb{G}_{m+n} &\to A_1 \cup A_2 \\
i &\mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}
\end{aligned}
$$

Konkatenation von Wörtern: formal

- Wörter als Listen von Zeichen, genauer
- surjektive Abbildungen $w : \mathbb{G}_n \to A$
- Beispiel

$$
\begin{array}{ccccccccccc}
 & 0 & 1 & 2 & 3 & 4 & & 0 & 1 & 2 \\
 & \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \cdot & \mathtt{M} & \mathtt{U} & \mathtt{S}
\end{array}
$$

$$
\begin{array}{ccccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
= & \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \mathtt{M} & \mathtt{U} & \mathtt{S}
\end{array}
$$

- definiere

$$
w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2
$$

$$
i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \le i < m \\ w_2(i-m) & \text{falls } m \le i < m+n \end{cases}
$$

- Wörter als Listen von Zeichen, genauer
- surjektive Abbildungen $w : \mathbb{G}_n \to A$
- Beispiel

$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & & 0 & 1 & 2 \\ \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \cdot & \mathtt{M} & \mathtt{U} & \mathtt{S} \end{array}$$

$$\begin{array}{ccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ = & \mathtt{A} & \mathtt{P} & \mathtt{F} & \mathtt{E} & \mathtt{L} & \mathtt{M} & \mathtt{U} & \mathtt{S} \end{array}$$

- definiere

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$

$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

Definition

- beliebige Wörter $w_1 : \mathbb{G}_m \to A_1$ und $w_2 : \mathbb{G}_n \to A_2$ gegeben
- definiere

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Was muss man tun, wenn man so etwas vorgesetzt bekommt?
  - Nicht abschrecken lassen!
  - Abbildung: für *alle* Argumente ein Funktionswert definiert?
  - bei Fallunterscheidungen: widerspruchsfrei?
  - Hat das Definierte die erforderlichen Eigenschaften?
  - Verstehen!
- Man sieht übrigens:
  $\forall w_1 \in A^* \; \forall w_2 \in A^* : |w_1 w_2| = |w_1| + |w_2|$.

Definition

- beliebige Wörter $w_1 : \mathbb{G}_m \to A_1$ und $w_2 : \mathbb{G}_n \to A_2$ gegeben
- definiere

$$
\begin{aligned}
w_1 \cdot w_2 : \mathbb{G}_{m+n} &\to A_1 \cup A_2 \\
i &\mapsto \begin{cases} w_1(i) & \text{falls } 0 \le i < m \\ w_2(i-m) & \text{falls } m \le i < m+n \end{cases}
\end{aligned}
$$

- Was muss man tun, wenn man so etwas vorgesetzt bekommt?
  - Nicht abschrecken lassen!
  - Abbildung: für *alle* Argumente ein Funktionswert definiert?
  - bei Fallunterscheidungen: widerspruchsfrei?
  - Hat das Definierte die erforderlichen Eigenschaften?
  - Verstehen!
- Man sieht übrigens:
  $\forall w_1 \in A^* \; \forall w_2 \in A^* : |w_1 w_2| = |w_1| + |w_2|$.

Definition

- beliebige Wörter $w_1 : \mathbb{G}_m \to A_1$ und $w_2 : \mathbb{G}_n \to A_2$ gegeben
- definiere

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Was muss man tun, wenn man so etwas vorgesetzt bekommt?
  - Nicht abschrecken lassen!
  - Abbildung: für *alle* Argumente ein Funktionswert definiert?
  - bei Fallunterscheidungen: widerspruchsfrei?
  - Hat das Definierte die erforderlichen Eigenschaften?
  - Verstehen!
- Man sieht übrigens:
  $\forall w_1 \in A^* \; \forall w_2 \in A^* : |w_1 w_2| = |w_1| + |w_2|$.

Konkatenation von Wörtern: formal

- definiert:

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Überprüfung:
  - $w_1(i)$ für $0 \leq i < m$ und $w_2(i-m)$ für $m \leq i < m+n$ sind stets definiert.
  - die Funktionswerte stammen aus dem Bereich $A_1 \cup A_2$: $w_1(i) \in A_1$ und $w_2(i-m) \in A_2$.
  - Die Fallunterscheidung ist widerspruchsfrei.
  - $w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$ ist surjektiv:
    Für jedes $a \in A_1 \cup A_2$ gilt eine der Möglichkeiten:
    - $a \in A_1$: da w_1 surjektiv ist, existiert $i_1 \in \mathbb{G}_m$ mit $w_1(i_1) = a$. Also ist $(w_1 w_2)(i_1) = w_1(i_1) = a$.
    - $a \in A_2$: da w_2 surjektiv ist, existiert $i_2 \in \mathbb{G}_n$ mit $w_2(i_2) = a$. Also ist $(w_1 w_2)(m + i_2) = w_2(i_2) = a$.

Konkatenation von Wörtern: formal

- definiert:

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Überprüfung:
  - ✓ $w_1(i)$ für $0 \leq i < m$ und $w_2(i-m)$ für $m \leq i < m+n$ sind stets definiert.
  - die Funktionswerte stammen aus dem Bereich $A_1 \cup A_2$: $w_1(i) \in A_1$ und $w_2(i-m) \in A_2$.
  - Die Fallunterscheidung ist widerspruchsfrei.
  - $w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$ ist surjektiv:
    Für jedes $a \in A_1 \cup A_2$ gilt eine der Möglichkeiten:
    - $a \in A_1$: da w_1 surjektiv ist, existiert $i_1 \in \mathbb{G}_m$ mit $w_1(i_1) = a$. Also ist $(w_1 w_2)(i_1) = w_1(i_1) = a$.
    - $a \in A_2$: da w_2 surjektiv ist, existiert $i_2 \in \mathbb{G}_n$ mit $w_2(i_2) = a$. Also ist $(w_1 w_2)(m + i_2) = w_2(i_2) = a$.

Konkatenation von Wörtern: formal

- definiert:

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Überprüfung:
  - ✓ $w_1(i)$ für $0 \leq i < m$ und $w_2(i-m)$ für $m \leq i < m+n$ sind stets definiert.
  - ✓ die Funktionswerte stammen aus dem Bereich $A_1 \cup A_2$: $w_1(i) \in A_1$ und $w_2(i-m) \in A_2$.
  - – Die Fallunterscheidung ist widerspruchsfrei.
  - – $w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$ ist surjektiv:
    Für jedes $a \in A_1 \cup A_2$ gilt eine der Möglichkeiten:
    - $a \in A_1$: da w_1 surjektiv ist, existiert $i_1 \in \mathbb{G}_m$ mit $w_1(i_1) = a$. Also ist $(w_1 w_2)(i_1) = w_1(i_1) = a$.
    - $a \in A_2$: da w_2 surjektiv ist, existiert $i_2 \in \mathbb{G}_n$ mit $w_2(i_2) = a$. Also ist $(w_1 w_2)(m + i_2) = w_2(i_2) = a$.

Konkatenation von Wörtern: formal

- definiert:

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$

- Überprüfung:
  - ✓ $w_1(i)$ für $0 \leq i < m$ und $w_2(i-m)$ für $m \leq i < m+n$ sind stets definiert.
  - ✓ die Funktionswerte stammen aus dem Bereich $A_1 \cup A_2$: $w_1(i) \in A_1$ und $w_2(i-m) \in A_2$.
  - ✓ Die Fallunterscheidung ist widerspruchsfrei.
  - – $w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$ ist surjektiv:
    Für jedes $a \in A_1 \cup A_2$ gilt eine der Möglichkeiten:
    - $a \in A_1$: da w_1 surjektiv ist, existiert $i_1 \in \mathbb{G}_m$ mit $w_1(i_1) = a$.
      Also ist $(w_1 w_2)(i_1) = w_1(i_1) = a$.
    - $a \in A_2$: da w_2 surjektiv ist, existiert $i_2 \in \mathbb{G}_n$ mit $w_2(i_2) = a$.
      Also ist $(w_1 w_2)(m + i_2) = w_2(i_2) = a$.

Konkatenation von Wörtern: formal

- definiert:

$$w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$$
$$i \mapsto \begin{cases} w_1(i) & \text{falls } 0 \le i < m \\ w_2(i-m) & \text{falls } m \le i < m+n \end{cases}$$

- Überprüfung:
  - ✓ $w_1(i)$ für $0 \le i < m$ und $w_2(i-m)$ für $m \le i < m+n$ sind stets definiert.
  - ✓ die Funktionswerte stammen aus dem Bereich $A_1 \cup A_2$: $w_1(i) \in A_1$ und $w_2(i-m) \in A_2$.
  - ✓ Die Fallunterscheidung ist widerspruchsfrei.
  - ✓ $w_1 \cdot w_2 : \mathbb{G}_{m+n} \to A_1 \cup A_2$ ist surjektiv:
    Für jedes $a \in A_1 \cup A_2$ gilt eine der Möglichkeiten:
    - $a \in A_1$: da w_1 surjektiv ist, existiert $i_1 \in \mathbb{G}_m$ mit $w_1(i_1) = a$. Also ist $(w_1 w_2)(i_1) = w_1(i_1) = a$.
    - $a \in A_2$: da w_2 surjektiv ist, existiert $i_2 \in \mathbb{G}_n$ mit $w_2(i_2) = a$. Also ist $(w_1 w_2)(m + i_2) = w_2(i_2) = a$.

Überblick

Wörter

Wörter

Das leere Wort

Mehr zu Wörtern

Konkatenation von Wörtern

Konkatenation mit dem leeren Wort

Binäre Operationen

Eigenschaften der Konkatenation

Beispiel: Aufbau von E-Mails

Iterierte Konkatenation

Vollständige Induktion

Konkatenation mit dem leeren Wort

- bei den Zahlen:

$$\forall x \in \mathbb{N}_0 : x + 0 = x \wedge 0 + x = x$$

  Die Null ist das *neutrale Element* bezüglich der Addition.

- Analog bei Wörtern:
  Lemma. Für jedes Alphabet A gilt:

$$\forall w \in A^* : w \cdot \varepsilon = w \wedge \varepsilon \cdot w = w \; .$$

- Anschaulich klar: Wenn man an ein Wort w hinten der Reihe nach noch alle Symbole des leeren Wortes „klebt", also gar keine, dann „ändert sich an w nichts".
- Aber wir können das auch formal beweisen ...

Das leere Wort ist neutrales Element bezüglich Konkatenation

- Frage: Wie beweist man das für alle denkbaren Alphabete A?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen“ Alphabet A aus, über das man keine Annahmen macht.
- Frage: Wie beweist man die Behauptung für alle $w \in A^*$?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen“ Wort w aus, über das man keine Annahmen macht.
- Also:
  - Es sei A ein Alphabet und $w \in A^*$, d. h. eine surjektive Abbildung $w : \mathbb{G}_m \to B$ mit $B \subseteq A$.
  - Außerdem ist $\varepsilon : \mathbb{G}_0 \to \{\}$.
  - berechne $w' = w \cdot \varepsilon$ anhand der formalen Definition:
  - w' ist eine Abbildung $w' : \mathbb{G}_{m+0} \to B \cup \{\}$, also $w' : \mathbb{G}_m \to B$.

Das leere Wort ist neutrales Element bezüglich Konkatenation

- Frage: Wie beweist man das für alle denkbaren Alphabete A?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen" Alphabet A aus, über das man keine Annahmen macht.
- Frage: Wie beweist man die Behauptung für alle $w \in A^*$?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen" Wort w aus, über das man keine Annahmen macht.
- Also:
  - Es sei A ein Alphabet und $w \in A^*$, d. h. eine surjektive Abbildung $w : \mathbb{G}_m \to B$ mit $B \subseteq A$.
  - Außerdem ist $\varepsilon : \mathbb{G}_0 \to \{\}$.
  - berechne $w' = w \cdot \varepsilon$ anhand der formalen Definition:
  - w' ist eine Abbildung $w' : \mathbb{G}_{m+0} \to B \cup \{\}$, also $w' : \mathbb{G}_m \to B$.

Das leere Wort ist neutrales Element bezüglich Konkatenation

- Frage: Wie beweist man das für alle denkbaren Alphabete A?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen" Alphabet A aus, über das man keine Annahmen macht.
- Frage: Wie beweist man die Behauptung für alle $w \in A^*$?
- Eine Möglichkeit: Man geht von einem „beliebigen aber festen" Wort w aus, über das man keine Annahmen macht.
- Also:
  - Es sei A ein Alphabet und $w \in A^*$, d. h. eine surjektive Abbildung $w : \mathbb{G}_m \to B$ mit $B \subseteq A$.
  - Außerdem ist $\varepsilon : \mathbb{G}_0 \to \{\}$.
  - berechne $w' = w \cdot \varepsilon$ anhand der formalen Definition:
  - w' ist eine Abbildung $w' : \mathbb{G}_{m+0} \to B \cup \{\}$, also $w' : \mathbb{G}_m \to B$.

Das leere Wort ist neutrales Element bezüglich Konkatenation (2)

- für $i \in \mathbb{G}_m$ gilt

$$w'(i) = \begin{cases} w_1(i) & \text{falls } 0 \leq i < m \\ w_2(i-m) & \text{falls } m \leq i < m+n \end{cases}$$
$$= \begin{cases} w(i) & \text{falls } 0 \leq i < m \\ \varepsilon(i-m) & \text{falls } m \leq i < m+0 \end{cases}$$
$$= w(i)$$

- Also
  - w und w' haben gleichen Definitionsbereich
  - w und w' haben gleichen Zielbereich
  - w und w' haben für alle Argumente die gleichen Funktionswerte.
  - Also ist $w' = w$.
- Ganz analog zeigt man: $\varepsilon \cdot w = w$.

Überblick

Wörter
- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern
- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

- Eine *binäre Operation* auf einer Menge M ist eine Abbildung

$$f : M \times M \to M$$

- üblich: Infixschreibweise mit „Operationssymbol“ wie z. B. Pluszeichen oder Multiplikationspunkt
  - Statt $+(3, 8) = 11$ schreibt man $3 + 8 = 11$.
- Eine binäre Operation $\diamond : M \times M \to M$ heißt genau dann *kommutativ*, wenn gilt:

$$\forall x \in M \;\; \forall y \in M : \;\; x \diamond y = y \diamond x \; .$$

- Eine binäre Operation $\diamond : M \times M \to M$ heißt genau dann *assoziativ*, wenn gilt:

$$\forall x \in M \;\; \forall y \in M \;\; \forall z \in M : \;\; (x \diamond y) \diamond z = x \diamond (y \diamond z) \; .$$

Überblick

Wörter
- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern
- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

- schon gesehen: Reihenfolge ist wichtig

$$\mathtt{SCHRANKSCHLÜSSEL} \neq \mathtt{SCHLÜSSELSCHRANK}$$

Konkatenation ist *nicht kommutativ*.

- Bei Zahlen gilt: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Bei Wörtern analog:

Lemma. Für jedes Alphabet A und alle Wörter w_1, w_2 und w_3 aus A^* gilt:

$$(w_1 \cdot w_2) \cdot w_3 = w_1 \cdot (w_2 \cdot w_3) \ .$$

Konkatenation ist *assoziativ*.

- Beweis: einfach nachrechnen (Hausaufgabe Oktober 2009)

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

RFC

- Struktur von E-Mails in einem sogenannten RFC festgelegt
- RFC ist die Abkürzung für *Request For Comment*.
- alle RFCs zum Beispiel unter
  `http://tools.ietf.org/html/`

- aktuelle Fassung der E-Mail-Spezifikation in RFC 2822
  `http://tools.ietf.org/html/rfc2822`
- im folgenden einige Zitate aus Abschnitt 2.1 des RFC 2822 und Kommentare dazu

E-Mails, RFC 2822 (1)

- *„This standard specifies that messages are made up of characters in the US-ASCII range of 1 through 127.“*
- Das Alphabet, aus dem die Zeichen stammen müssen, die in einer E-Mail vorkommen, ist der US-ASCII-Zeichensatz mit Ausnahme des Zeichens mit der Nummer 0.

E-Mails, RFC 2822 (2)

- *„Messages are divided into lines of characters. A line is a series of characters that is delimited with the two characters carriage-return and line-feed; that is, the carriage return (CR) character (ASCII value 13) followed immediately by the line feed (LF) character (ASCII value 10). (The carriage-return/line-feed pair is usually written in this document as "CRLF".)"*
- Eine Zeile (*line*) ist
  - eine Folge von Zeichen, also ein Wort,
  - das mit den „nicht druckbaren" Symbolen $\boxed{\texttt{CR}}$ $\boxed{\texttt{LF}}$ endet.
  - Line Feed $\boxed{\texttt{LF}}$: Zeilenvorschub (Schreibmaschine)
  - Carriage Return $\boxed{\texttt{CR}}$: Wagenrücklauf (Schreibmaschine)

  - an anderer Stelle:
    - als Zeile sind nicht beliebige Wörter zulässig, ...
    - ... sondern nur solche, deren Länge kleiner oder gleich 998 ist.

E-Mails, RFC 2822 (3)

- *A message consists of*
  - *[...] the header of the message [...] followed,*
  - *optionally, by a body."*
- eine E-Mail (*message*) ist die Konkatenation von
  - Kopf (*header*) der E-Mail und
  - Rumpf (*body*) der E-Mail.
- Rumpf optional,
  - darf also sozusagen fehlen,
  - d.h. der Rumpf darf auch das leere Wort sein.

Das ist noch nicht ganz vollständig. Gleich anschließend wird der RFC genauer:

E-Mails, RFC 2822 (4)

-
  - *„The header is a sequence of lines of characters with special syntax as defined in this standard.*
  - *The body is simply a sequence of characters that follows the header and*
  - *is separated from the header by an empty line (i.e., a line with nothing preceding the CRLF). [...]"*
- also:
  - Kopf einer E-Mail ist die Konkatenation (mehrerer) Zeilen.
  - Rumpf einer E-Mail ist die Konkatenation von Zeilen.
    - (an anderer Stellen spezifiziert)
    - Es können aber auch 0 Zeilen oder 1 Zeile sein.
  - Eine Leerzeile (*empty line*) ist das Wort $\boxed{\texttt{CR}}$ $\boxed{\texttt{LF}}$.
  - Eine Nachricht ist die Konkatenation von
    - Kopf der E-Mail,
    - einer Leerzeile und
    - Rumpf der E-Mail.

Überblick

Wörter

- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern

- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Iterierte Konkatenation: Potenzen von Wörtern

- bei Zahlen: Potenzschreibweise x^3 für $x \cdot x \cdot x$ usw.
- Ziel: analog für Wörter so etwas wie

$$w^n = \underbrace{w \cdot w \cdot \cdots \cdot w}_{n \text{ mal}}$$

- wieder diese Pünktchen ...
- Wie kann man die vermeiden?
  - Was ist mit $n = 1$?
    (immerhin stehen da ja drei w auf der rechten Seite)
  - Was soll man sich für $n = 0$ vorstellen?
- Möglichkeit: eine *induktive Definition*
- für *Potenzen von Wörtern* geht das so:

$$w^0 = \varepsilon$$
$$\forall n \in \mathbb{N}_0 : \; w^{n+1} = w^n \cdot w$$

Iterierte Konkatenation: Potenzen von Wörtern

- definiert:

$$w^0 = \varepsilon$$
$$\forall n \in \mathbb{N}_0 : \; w^{n+1} = w^n \cdot w$$

- Damit kann man ausrechnen, was w^1 ist:

$$w^1 = w^{0+1} = w^0 \cdot w = \varepsilon \cdot w = w$$

- Und dann:

$$w^2 = w^{1+1} = w^1 \cdot w = w \cdot w$$

- Und dann:

$$w^3 = w^{2+1} = w^2 \cdot w = (w \cdot w) \cdot w$$

- Und so weiter.

Ein einfaches Lemma

Lemma: Ein Satz, der als Zwischenschritt eine Bedeutung im Beweis eines wichtigeren Satzes hat

Lemma.
Für jedes Alphabet A, jedes Wort $w \in A^*$ und jedes $n \in \mathbb{N}_0$ gilt:

$$|w^n| = n|w| \ .$$

- Wie kann man das beweisen?
- Immer wenn in einer Aussage „etwas" eine Rolle spielt, das induktiv definiert wurde, sollte man in Erwägung ziehen, für den Beweis *vollständige Induktion* zu benutzen.

Ein einfaches Lemma

- erst mal ein paar einfache Fälle als Beispiele:
  - $n = 0$: Das ist einfach: $|w^0| = |\varepsilon| = 0 = 0 \cdot |w|$.
  - $n = 1$: Man kann ähnlich rechnen wie bei $w^1 = w$:

    $$\begin{aligned} |w^1| = |w^{0+1}| &= |w^0 \cdot w| \\ &= |w^0| + |w| \\ &= 0|w| + |w| && \text{siehe Fall } n = 0 \\ &= 1|w| \end{aligned}$$

    Da die Behauptung für $n = 0$ richtig war, konnten wir sie auch für $n = 1$ beweisen.
  - $n = 2$: Wir gehen analog zu eben vor:

    $$\begin{aligned} |w^2| = |w^{1+1}| &= |w^1 \cdot w| \\ &= |w^1| + |w| \\ &= 1|w| + |w| && \text{siehe Fall } n = 1 \\ &= 2|w| \end{aligned}$$

    Da die Behauptung für $n = 1$ richtig war, konnten wir sie auch für $n = 2$ beweisen.

Vollständige Induktion

- allgemeines Muster:
  - Weil w^{n+1} mit Hilfe von w^n definiert wurde,
  - folgt aus der Richtigkeit der Behauptung für $|w^n|$ die für $|w^{n+1}|$.
- Also: Wenn wir mit M die Menge aller natürlichen Zahlen n bezeichnen, für die die Behauptung $|w^n| = n|w|$ gilt, dann wissen wir also:
  1. $0 \in M$
  2. $\forall n \in \mathbb{N}_0 : \ (n \in M \Rightarrow n+1 \in M)$
- Faktum aus der Mathematik:
  Wenn eine Menge M
  - nur natürliche Zahlen enthält
  - Eigenschaft 1 hat und
  - Eigenschaft 2 hat,

  dann ist $M = \mathbb{N}_0$.

Nun im wesentlichen noch einmal das Gleiche wie oben in der für Induktionsbeweise üblichen Form:

Induktionsanfang $n = 0$: Zu zeigen ist: $|w^0| = 0 \cdot |w|$.
Das geht so:

$$\begin{aligned} |w^0| &= |\varepsilon| \qquad \text{nach Defintion von } w^0 \\ &= 0 = 0 \cdot |w| \ . \end{aligned}$$

Induktionsschritt $n \to n + 1$:

- Zu zeigen ist: Für jedes n gilt: wenn $|w^n| = n|w|$, dann $|w^{n+1}| = (n + 1)|w|$.
- Wie kann man zeigen, dass diese Aussage für *alle* natürlichen Zahlen n gilt?
- Möglichkeit: Man gehe von einem „beliebigen, aber festen“ n aus und zeige für „dieses“ n: $|w^n| = n|w| \Rightarrow |w^{n+1}| = (n + 1)|w|$.

Nun im wesentlichen noch einmal das Gleiche wie oben in der für Induktionsbeweise üblichen Form:

Induktionsanfang $n = 0$: Zu zeigen ist: $|w^0| = 0 \cdot |w|$.
Das geht so:

$$\begin{aligned} |w^0| &= |\varepsilon| && \text{nach Defintion von } w^0 \\ &= 0 = 0 \cdot |w| \ . \end{aligned}$$

Induktionsschritt $n \to n + 1$:

- Zu zeigen ist: Für jedes n gilt: wenn $|w^n| = n|w|$, dann $|w^{n+1}| = (n + 1)|w|$.
- Wie kann man zeigen, dass diese Aussage für *alle* natürlichen Zahlen n gilt?
- Möglichkeit: Man gehe von einem „beliebigen, aber festen" n aus und zeige für „dieses" n: $|w^n| = n|w| \Rightarrow |w^{n+1}| = (n + 1)|w|$.

Vollständige Induktion: Beweis des Lemmas

Induktionsschritt $n \to n+1$: zwei Teile:

- für ein beliebiges aber festes n trifft man die Induktionsvoraussetzung oder Induktionsannahme:
$$|w^n| = n|w|.$$
- Zu leisten ist nun mit Hilfe dieser Annahme der Nachweis, dass auch $|w^{n+1}| = (n+1)|w|$. Das nennt man den Induktionsschluss: In unserem Fall:

$$\begin{aligned}
|w^{n+1}| &= |w^n \cdot w| \\
&= |w^n| + |w| \\
&= n|w| + |w| && \text{nach Induktionsvoraussetzung} \\
&= (n+1)|w|
\end{aligned}$$

Überblick

Wörter
- Wörter
- Das leere Wort
- Mehr zu Wörtern

Konkatenation von Wörtern
- Konkatenation mit dem leeren Wort
- Binäre Operationen
- Eigenschaften der Konkatenation
- Beispiel: Aufbau von E-Mails
- Iterierte Konkatenation

Vollständige Induktion

Vollständige Induktion: das Prinzip

- Grundlage
  - Wenn man für eine Aussage $\mathcal{A}(n)$, die von einer Zahl $n \in \mathbb{N}_0$ abhängt, weiß

$$\begin{array}{rc} \text{es gilt} & \mathcal{A}(0) \\ \text{und es gilt} & \forall n \in \mathbb{N}_0 : (\mathcal{A}(n) \Rightarrow \mathcal{A}(n+1)) \end{array}$$

  - dann gilt auch:

$$\forall n \in \mathbb{N}_0 : \ \mathcal{A}(n) \ .$$

- Struktur des Beweises im einfachsten Fall:

  Induktionsanfang: zeige: $\mathcal{A}(0)$ gilt.

  Induktionsvoraussetzung:

  für beliebiges aber festes $n \in \mathbb{N}_0$ gilt: $\mathcal{A}(n)$.

  Induktionsschluss: zeige: auch $\mathcal{A}(n+1)$ gilt.

Was ist wichtig

Das sollten Sie mitnehmen:

- ein *Wort* ist eine Folge von Symbolen
  - *Formale Sprachen* werden in der nächsten Einheit folgen.
- induktive Definitionen
  - erlauben, Pünktchen zu vermeiden ...
- *vollständige Induktion*
  - gaaaanz wichtiges Beweisprinzip

    Induktionsanfang
    Induktionsvoraussetzung
    Induktionsschluss
  - passt z. B. bei induktiven Definitionen

Das sollten Sie üben:

- vollständige Induktion
- „Rechnen" mit Wörtern