Grundbegriffe der Informatik

Einheit 4: Wörter
(und vollständige Induktion)

Thomas Worsch

Universität Karlsruhe, Fakultät für Informatik

Oktober 2008

Überblick

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.

Das Leerzeichen

- man benutzt es heutzutage (jedenfalls z. B. in europäischen Schriften) ständig, aber
- früher nicht!
- Für uns ist es ein Zeichen wie alle anderen auch; der Deutlichkeit wegen manchmal explizit ␣ geschrieben.
- Folge: z. B. `Hallo␣Welt` ist *eine* Folge von Zeichen, also nur *ein* Wort (und nicht zwei)

Eine 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

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

- 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

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

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
  - den Fall des sogenannten leeren Wortes ε mit Länge $n = 0$ betrachten wir 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 Wörtern vorteilhaft
  - manchmal vertraute Auffassung Wörtern vorteilhaft
  - wir wechseln hin und her

Menge aller Wörter

- A^*: *Menge aller Wörter* über einem Alphabet A: alle Wörter, die nur Zeichen aus A enthalten

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

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`, `b`

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`, `b`
  - `aa`, `ab`, `ba`, `bb`

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, b
  - aa, ab, ba, bb
  - aaa, aab, aba, abb, baa, bab, bba, bbb

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, b
  - aa, ab, ba, bb
  - aaa, aab, aba, abb, baa, bab, bba, bbb
  - und so weiter

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, b
  - aa, ab, ba, bb
  - aaa, aab, aba, abb, baa, bab, bba, bbb
  - und so weiter
  - und außerdem ε
    dieses merkwürdige (?) leere Wort (kommt gleich)

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`, `b`
  - `aa`, `ab`, `ba`, `bb`
  - `aaa`, `aab`, `aba`, `abb`, `baa`, `bab`, `bba`, `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!

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, b
  - aa, ab, ba, bb
  - aaa, aab, aba, abb, baa, bab, bba, 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 $B \subseteq A$.

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. Deshalb „sieht man es so schlecht“.
  - 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.

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

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

- Also ist sozusagen

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

aber diese Pünktchen sind nicht schön ...

- Bessere Schreibweise:

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

immer diese Pünktchen ...

- 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*!

Konkatenation von Wörtern: anschaulich

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

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

  oder

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

- Beachte: Reihenfolge ist wichtig!

$$\texttt{SCHRANKSCHLÜSSEL} \neq \texttt{SCHLÜSSELSCHRANK}$$

Konkatenation von Wörtern: formal

- zwei 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!
  - bei Abbildungen prüfen: wird 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:

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

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

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

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

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

- 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.
  - – $w_1 \cdot w_2 : \mathbb{G}_{m+n} \longrightarrow A_1 \cup A_2$ 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 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“ Alphabet A aus, über das man keinerlei Annahmen macht.
- Frage: Wie beweist man die Behauptung für alle $w \in A^*$?
- Eine Möglichkeit: Man geht von einem beliebigen Wort w aus, über das man keinerlei 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

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

- 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: $\varepsilon \cdot w = w$.

Eigenschaften der Konkatenation

- schon gesehen: Reihenfolge ist wichtig

$$\texttt{SCHRANKSCHLÜSSEL} \neq \texttt{SCHLÜSSELSCHRANK}$$

  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

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.
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 $w^1 = w$:

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

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

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

    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 $M = \mathbb{N}_0$.

Vollständige Induktion: Beweis des Lemmas

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:

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

Vollständige Induktion: Beweis des Lemmas

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 $n \longrightarrow n + 1$:

- 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 $n \longrightarrow n+1$: zwei Teile:

- für ein beliebiges aber festes n trifft man die Induktionsannahme oder Induktionsvoraussetzung:
$$|w^n| = n|w|.$$
- 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:

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

Vollständige Induktion: das Prinzip

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

es gilt	$\mathcal{A}(0)$
und es gilt	$\forall n \in \mathbb{N}_0 : (\mathcal{A}(n) \Rightarrow \mathcal{A}(n+1))$

dann gilt auch:

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

Vollständige Induktion: eine kleine Variante

ein kleiner Trick:

- Es sei $\mathcal{B}(n)$ eine Aussage, die von einer Zahl $n \in \mathbb{N}_0$ abhängt.
- Wollen beweisen: $\forall n \in \mathbb{N}_0 : \mathcal{B}(n)$
- Definiere Aussage $\mathcal{A}(n)$ als $\mathcal{B}(n) \wedge \mathcal{B}(n+1)$.
- Beweise $\forall n \in \mathbb{N}_0 : \mathcal{A}(n)$: das reicht!

Vollständige Induktion: eine kleine Variante

ein kleiner Trick:

- Es sei $\mathcal{B}(n)$ eine Aussage, die von einer Zahl $n \in \mathbb{N}_0$ abhängt.
- Wollen beweisen: $\forall n \in \mathbb{N}_0 : \mathcal{B}(n)$
- Definiere Aussage $\mathcal{A}(n)$ als $\mathcal{B}(n) \wedge \mathcal{B}(n+1)$.
- Beweise $\forall n \in \mathbb{N}_0 : \mathcal{A}(n)$: das reicht!
- Induktionsbeweis für $\forall n \in \mathbb{N}_0 : \mathcal{A}(n)$:

  Induktionsanfang $n = 0$: Man muss zeigen:
  $\mathcal{A}(0)$, also $\mathcal{B}(0) \wedge \mathcal{B}(1)$, also $\mathcal{B}(0)$ und $\mathcal{B}(1)$.

  Induktionsschritt $n \to n+1$:

  Induktionsannahme: es gilt $\mathcal{A}(n)$, also $\mathcal{B}(n) \wedge \mathcal{B}(n+1)$,
  also $\mathcal{B}(n)$ und $\mathcal{B}(n+1)$

  Induktionsschluss: zu zeigen: es gilt $\mathcal{A}(n+1)$,
  also $\mathcal{B}(n+1) \wedge \mathcal{B}(n+2)$, also $\mathcal{B}(n+1)$ und $\mathcal{B}(n+2)$
  – $\mathcal{B}(n+1)$: trivial
  – $\mathcal{B}(n+2)$: hier muss man was tun,
  aber man kann $\mathcal{B}(n)$ und $\mathcal{B}(n+1)$ benutzen

Binäre Operationen

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

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

- üblich: Infixschreibweise mit „Operationssysmbol“ 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:

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

Zusammenfassung

Wir haben gesehen

- was ein *Wort* ist
  - Der Begriff *formale Sprache* wirdin der nächsten Einheit folgen.
- induktive Definitionen
  - erlauben, Pünktchen zu vermeiden ...
- *vollständige Induktion*
  - gaaaanz wichtiges Beweisprinzip
  - passt z. B. bei induktiven Definitionen