

Zentrale Begriffe (Vorlesung vom 16.10.2015)

Kondition eines Problems:

Kleine Ursache, große Wirkung (Orkan Lothar, Moleküldynamik).

Stabilität eines Algorithmus:

Keine Äquivalenz von Multiplikation und mehrfacher Addition.

Komplexität eines Problems

Effizienz eines Algorithmus

Die natürlichen Zahlen (anschaulich)

$0, 1, 2, 3, \dots$

- kennt jedes Kind
- beginnen mit 0 oder 1
- gut geeignet zum Abzählen
- keine Schulden, keine Tortenstücke
- ...

Die natürlichen Zahlen (axiomatisch)

Definition: \mathbb{N} ist die Menge mit den folgenden Eigenschaften:

- Es gibt ein ausgezeichnetes Element $0 \in \mathbb{N}$.

- Es gibt eine Abbildung $S : \mathbb{N} \rightarrow \mathbb{N}$ mit

(S1) S ist injektiv (d.h. $S(n) \neq S(m)$ falls $n \neq m$)

(S2) $0 \notin S(\mathbb{N}) = \{S(n) \mid n \in \mathbb{N}\}$

(S3) Ist $M \subset \mathbb{N}$ und gilt $0 \in M$ und $S(M) \subset M$ so gilt $M = \mathbb{N}$.

Die natürlichen Zahlen (axiomatisch)

Definition: \mathbb{N} ist die Menge mit den folgenden Eigenschaften:

- Es gibt ein ausgezeichnetes Element $0 \in \mathbb{N}$.

- Es gibt eine Abbildung $S : \mathbb{N} \rightarrow \mathbb{N}$ mit

(S1) S ist injektiv (d.h. $S(n) \neq S(m)$ falls $n \neq m$)

(S2) $0 \notin S(\mathbb{N}) = \{S(n) \mid n \in \mathbb{N}\}$

(S3) Ist $M \subset \mathbb{N}$ und gilt $0 \in M$ und $S(M) \subset M$ so gilt $M = \mathbb{N}$.

Anschaulich:

Jede natürlichen Zahl n hat genau einen **Nachfolger** $S(n)$.

Rechnen mit natürlichen Zahlen

Definition der Addition:

$$(A1) \quad n + 0 = n$$

$$(A1) \quad n + S(m) = S(n + m)$$

Rechnen mit natürlichen Zahlen

Definition der Addition:

$$(A1) \quad n + 0 = n$$

$$(A1) \quad n + S(m) = S(n + m)$$

Nachweis der Rechenregeln:

$$\text{Assoziativitat: } k + (n + m) = (k + n) + m$$

$$\text{Kommutativitat: } n + m = m + n$$

Rechnen mit natürlichen Zahlen

Definition der Addition:

$$(A1) \quad n + 0 = n$$

$$(A1) \quad n + S(m) = S(n + m)$$

Nachweis der Rechenregeln:

$$\text{Assoziativität: } k + (n + m) = (k + n) + m$$

$$\text{Kommutativität: } n + m = m + n$$

Folgerung: Wir können mit natürlichen Zahlen rechnen.

Rechnen mit natürlichen Zahlen

Definition der Addition:

$$(A1) \quad n + 0 = n$$

$$(A1) \quad n + S(m) = S(n + m)$$

Nachweis der Rechenregeln:

$$\text{Assoziativität: } k + (n + m) = (k + n) + m$$

$$\text{Kommutativität: } n + m = m + n$$

Folgerung: Wir können mit natürlichen Zahlen rechnen.

Aber: Bevor wir die Summe zweier natürlicher Zahlen **ausrechnen** können muss jede natürliche Zahl genau einen **Namen** haben!

Ziffernketten

Problem:

unendlich viele natürliche Zahlen \Leftrightarrow unendlich viele Namen

Ziffernketten

Problem:

unendlich viele natürliche Zahlen \Leftrightarrow unendlich viele Namen

Lösung:

Ziffernketten: $z_1 z_2 z_3 \dots z_k$, $z_i \in \mathcal{Z}$, $i = 1, \dots, k$

endliche Ziffernmengemenge \mathcal{Z}

Ziffernketten

Problem:

unendlich viele natürliche Zahlen \Leftrightarrow unendlich viele Namen

Lösung:

Ziffernketten: $z_1 z_2 z_3 \dots z_k$, $z_i \in \mathcal{Z}$, $i = 1, \dots, k$

endliche Ziffernmengen \mathcal{Z}

Interpretation:

- Systematische Konstruktion unterschiedlicher Symbole
- Bilden von Worten aus einem Alphabet

Ziffersysteme

Satz: Sei \mathcal{Z} eine endliche Ziffernmenge und

$$\mathcal{D}(\mathcal{Z}) = \{z_1 z_2 \dots z_k \mid k \in \mathbb{N}, z_i \in \mathcal{Z}, i = 1, \dots, k\}$$

die Menge aller Ziffernketten.

Dann existiert eine bijektive Abbildung $\varphi : \mathbb{N} \rightarrow \mathcal{D}(\mathcal{Z})$.

Definition: Die Ziffernmenge \mathcal{Z} und die Zuordnung φ erzeugen ein **Ziffersystem** zur Darstellung von \mathbb{N} .

Ziffersysteme

Satz: Sei \mathcal{Z} eine endliche Ziffernmenge und

$$\mathcal{D}(\mathcal{Z}) = \{z_1 z_2 \dots z_k \mid k \in \mathbb{N}, z_i \in \mathcal{Z}, i = 1, \dots, k\}$$

die Menge aller Ziffernketten.

Dann existiert eine bijektive Abbildung $\varphi : \mathbb{N} \rightarrow \mathcal{D}(\mathcal{Z})$.

Definition: Die Ziffernmenge \mathcal{Z} und die Zuordnung φ erzeugen ein **Ziffersystem** zur Darstellung von \mathbb{N} .

Definition: Eine Menge M , für die ein bijektives $\varphi : \mathbb{N} \rightarrow M$ existiert (die sich durchnummerieren lässt), heißt **abzählbar**.

Beispiele für Ziffernsysteme

römische Zahlen: $\mathcal{Z} = \{I, V, X, L, C, D, M\}$

Beispiele für Ziffernsysteme

römische Zahlen: $\mathcal{Z} = \{I, V, X, L, C, D, M\}$

kein Ziffernsystem!

Beispiele für Ziffersysteme

römische Zahlen: $\mathcal{Z} = \{I, V, X, L, C, D, M\}$

kein Ziffersystem!

Unärsystem:

nur eine Ziffer: $\mathcal{Z} = \{|\}$

Ziffernketten: $\mathcal{D}(\mathcal{Z}) = \{|\, , \|\, , \|\|\, , \dots\}$

Zuordnung: $\varphi(0) = \text{ , } \varphi(1) = |\, , \varphi(n + 1) = \varphi(n)|$

Beispiel: $\varphi(4) = \|\|\|\|$

Praktische Anwendungen

...vor 15000-20000 Jahren im Kongo:



Praktische Anwendungen

...vor 15000-20000 Jahren im Kongo:



...heute:



Potenzzerlegung zur Basis q

Satz: Sei $q \in \mathbb{N}$, $q > 1$ fest gewählt.

Dann lässt sich jede Zahl $n \in \mathbb{N}$ als Potenzzerlegung

$$n = \sum_{i=0}^k r_i q^i,$$

darstellen.

Dabei sind die Koeffizienten $r_i \in \{0, \dots, q - 1\} \subset \mathbb{N}$ eindeutig bestimmt.

Positionssystem zur Basis q

Definition:

Ziffernmenge: $\mathcal{Z} = \{z_0, z_1, \dots, z_{q-1}\}$

Zuordnung:

$$n \mapsto \varphi(n) = z_n, \quad n = 0, \dots, q-1,$$

und im Falle $n > q-1$

$$n \mapsto \varphi(n) = z_{r_k} z_{r_{k-1}} \dots z_{r_0} \quad \text{mit} \quad n = \sum_{i=0}^k r_i q^i, \quad 0 \leq r_i \leq q-1$$

Diese Zifferndarstellung heißt **q -adische Darstellung**.

Beispiele

Dezimalsystem: $\mathcal{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

q -adische Systeme mit $q \leq 36$: Erweiterung um $\{A, B, C, \dots, Z\}$

Konventionen:

- keine Unterscheidung zwischen Darstellung und Zahl:

$$z_k z_{k-1} \dots z_0 q = \sum_{i=0}^k z_i q^i, \quad z_i \in \mathcal{Z} = \{0, 1, \dots, q-1\}.$$

- kein Index q , falls $q = 10$
- den Index i von z_i nennt man **Stelle**, $z_k z_{k-1} \dots z_0 q$ eine **k -stellige Zahl**

Positionssystem zur Basis $q = 2$: Dualsystem

Ziffernmenge $\mathcal{Z} = \{0, 1\}$

Ideal für die technische Umsetzung:

1 Binärstelle \Leftrightarrow 1 Bit

Alle modernen Rechenmaschinen arbeiten mit dem Dualsystem.

Zahlenbereich: Im Dualsystem lassen sich mit N Stellen alle Zahlen $n \in \mathbb{N}$ mit

$$0 \leq n \leq 2^N - 1$$

darstellen.

Historische Rechenmaschinen I

- Abakus
- mechanische Zählräder
- 1623 Wilhelm Schickard, 1642 Blaise Pascal, 1673 Gottfried Wilhelm von Leibniz: Rechenmaschinen mit dekadischem System
- 1679 Leibniz: Dualsystem
- 1935 - 1938 Konrad Zuse (Berlin):
erster frei programmierbarer Rechner Z1 (mechanisch)

Rechenmaschinen II

- 1941 Konrad Zuse: elektromechanisch (Relais): Z3
- 1944 Cambridge: rein elektronisch (Elektronenröhren): COLOSSOS
- 1947 John Bardeen, Walter Brattain, William Shockley: Transistor
- 1971 Mikroprozessor: Intel
- 2000 Pentium 4: 42 Millionen Transistoren auf 217 mm^2
- 2007 Dual-Core Itanium 2: 1200 Millionen Transistoren auf 596 mm^2
- ...

Technische Realisierung

- kleinste Einheit (0 oder 1): Bit
- Bits werden in festen Längen zusammengefaßt.
- 8 Bits = 1 Byte mit $2^8 = 256$ verschiedene Zuständen
- feste Anzahl Bytes für Zahlendarstellung
- üblich: 1, 2, 4, 8 Bytes bzw. 8, 16, 32, 64 Bits
- Bezeichnungen: BYTE, WORD, DWORD, QWORD (nicht einheitlich)
- Bereich von 64-Bit Zahlen:

$$0 \leq z \leq 2^{64} - 1 > 18 \cdot 10^{18} = 18 \text{ Trillionen}$$

Die ganzen Zahlen (anschaulich)

$\dots, -2, -1, 0, +1, +2, \dots$

- kennt (fast) jedes Kind
- beginnen nirgends
- es gibt positive und negative Zahlen
- Schulden, aber keine Tortenstücke

Die ganzen Zahlen (konstruktiv)

Problem:

Ist $n > m$, so hat $x + n = m$ keine Lösung $x \in \mathbb{N}$

Ausweg:

Erweitere \mathbb{N} um $x = (m, n)$ (wir schreiben $m-n$)

Neues Problem:

nicht eindeutig: $x+2 = 1$ und $x+1 = 0$ hätten verschiedene Lösungen

Neuer Ausweg:

Äquivalenzklassen (siehe Skript, Analysis I, Lineare Algebra I, ...)

Zifferndarstellung: Vorzeichenbit

Darstellung der positiven Zahlen:

$$z_k z_{k-1} \dots z_0 q = \sum_{i=0}^k z_i q^i, \quad z_i \in \mathcal{Z} = \{0, 1, \dots, q-1\}.$$

zusätzliches Symbol: „-“

Darstellung der negativen Zahlen:

$$-z_k z_{k-1} \dots z_0 q = - \sum_{i=0}^k z_i q^i, \quad z_i \in \mathcal{Z} = \{0, 1, \dots, q-1\}.$$

technische Realisierung: Vorzeichenbit

Dualdarstellung ganzer Zahlen mit Vorzeichenbit

$$\mathbb{Z} = \{\dots, 111_2, 110_2, 11_2, 00_2, 01_2, 010_2, 011_2, \dots\}$$

Dualdarstellung ganzer Zahlen mit Vorzeichenbit

$$\mathbb{Z} = \{\dots, 111_2, 110_2, 11_2, 00_2, 01_2, 010_2, 011_2, \dots\}$$

Eindeutigkeit bei endlich vielen Stellen: 1. Stelle: Vorzeichenbit

Dualdarstellung ganzer Zahlen mit Vorzeichenbit

$$\mathbb{Z} = \{\dots, 111_2, 110_2, 11_2, 00_2, 01_2, 010_2, 011_2, \dots\}$$

Eindeutigkeit bei endlich vielen Stellen: 1. Stelle: Vorzeichenbit

Nachteile:

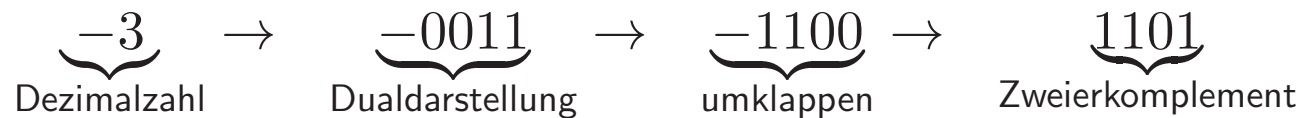
- Keine eindeutig bestimmte Darstellung der Null: $0 = 00_2 = 10_2$
- Addition natürlicher und ganzer Zahlen grundsätzlich verschieden

Dualdarstellung ganzer Zahlen mit Zweierkomplement

Kochrezept: Das Zweierkomplement von $n < 0$ erhält man durch

Dualdarstellung, Umklappen und 1 addieren

Beispiel: $N = 4$ Bits vorhanden und $n = -3$



Einfaches Rechnen mit dem Zweierkomplement

Grundsätzlich keine Subtraktion nötig: $a-b=a+(-b)$

Addition direkt auf negative Zahlen im Zweierkomplement erweiterbar:

Beispiel: $3 - 3 = 3 + (-3)$ im 4-Bit-Zweierkomplement lautet:

$$\begin{array}{r} 0 | 0 1 1 \\ + 1 | 1 0 1 \\ \hline 0 | 0 0 0 \end{array}$$

Was steckt dahinter?

komplementäre Potenzzerlegung:

$$\boxed{1 \mid z_{N-2} \cdots z_0} \hat{=} - \left(1 + \sum_{i=0}^{N-2} (1 - z_i) 2^i \right)$$

eindeutig bestimmte Darstellung der Null: $0 = 0000_2$

asymmetrischer Zahlenbereich:

$$z_{\min} \leq -2^{N-1} \leq z \leq 2^{N-1} - 1 = z_{\max}$$

Nicht verwechseln mit Overflow ...

Beispiel $N = 3$

-1	1 1 1
-2	1 1 0
-3	1 0 1
-4	1 0 0
3	0 1 1
2	0 1 0
1	0 0 1
0	0 0 0

Nicht verwechseln mit Overflow ...

Beispiel $N = 3$

-1	1 1 1
-2	1 1 0
-3	1 0 1
-4	1 0 0
3	0 1 1
2	0 1 0
1	0 0 1
0	0 0 0

Overflow-Desaster: Ariane 5 (4. Juni 1996)

Andere Möglichkeiten...

Asymmetrie des Zweierkomplements:

1000, 1001, ..., 1101, 1110, 1111, 0000, 0001, 0010, 0011, ..., 0111

Andere Möglichkeiten...

Asymmetrie des Zweierkomplements:

1000, 1001, ..., 1101, 1110, 1111, 0000, 0001, 0010, 0011, ..., 0111

exotische Alternative: $q = 3, z_0 = \underline{1}, z_1 = 0, z_2 = 1$

symmetrisch:

1111, ..., 0010, 0011, 0001, 0000, 0001, 0011, 0010, ..., 1111

technische Realisierung: Sowjetunion (S.L. Sobolev, 1958)