Vorlesung Diskrete Strukturen
Rechnen mit 0 und 1

Bernhard Ganter

Institut für Algebra
TU Dresden
D-01062 Dresden
bernhard.ganter@tu-dresden.de

WS 2009/10

Zur Erinnerung

Eine *n*-**stellige Operation** auf einer Menge A (auch n-stellige **Verknüpfung** genannt) ist eine Abbildung

$$f : A^n \longrightarrow A,$$

also eine Abbildung, die jedem n-Tupel von Elementen der **Trägermenge** A ein Element aus A zuordnet.

Zur Erinnerung

Eine *n*-**stellige Operation** auf einer Menge A (auch n-stellige **Verknüpfung** genannt) ist eine Abbildung

$$f : A^n \to A,$$

also eine Abbildung, die jedem n-Tupel von Elementen der **Trägermenge** A ein Element aus A zuordnet.

Die Anzahl der n-stelligen Operationen auf A ist $|A|^{(|A|^n)}$.

Im Fall, dass A zweielementig ist, gibt es also 2^{2^n} n-stellige Operationen auf A:

n	0	1	2	3	4	...
2^{2^n}	2	4	16	256	65536	...

Triviale Operationen

Wenig aufregend sind die **konstanten** Operationen, das sind solche, für die es ein Element $c \in A$ gibt mit $f(a_0, \ldots, a_{n-1}) = c$ für alle $a_0, \ldots, a_{n-1} \in A$. Man bezeichnet sie oft einfach mit dem Namen der Konstanten c und lässt die Angabe ihrer Stelligkeit weg.

Dazu gehören alle nullstelligen Operationen.

Triviale Operationen

Wenig aufregend sind die **konstanten** Operationen, das sind solche, für die es ein Element $c \in A$ gibt mit $f(a_0, \ldots, a_{n-1}) = c$ für alle $a_0, \ldots, a_{n-1} \in A$. Man bezeichnet sie oft einfach mit dem Namen der Konstanten c und lässt die Angabe ihrer Stelligkeit weg.

Dazu gehören alle nullstelligen Operationen.

Ebenfalls harmlos sind die **Projektionen** e_i^n, die jedem n-Tupel seine i-te Komponente zuordnen, also mit

$$e_i^n(a_0, \ldots, a_{n-1}) := a_i \qquad \text{für alle } a_0, \ldots, a_{n-1} \in A.$$

Rechnen mit zwei Elementen

Das Rechnen mit nur zwei Elementen ist nur auf den ersten Blick einfach. Tatsächlich ist es nach heutiger Technologie die Grundlage aller elektronische Datenverarbeitung.

Es ist unwichtig, welche zweielementige Trägermenge betrachtet wird. Gängige Bezeichnungen sind $A = \{T, F\}$, $A = \{\perp, \top\}$ und $A = \{0, 1\}$.

Rechnen mit zwei Elementen

Das Rechnen mit nur zwei Elementen ist nur auf den ersten Blick einfach. Tatsächlich ist es nach heutiger Technologie die Grundlage aller elektronische Datenverarbeitung.

Es ist unwichtig, welche zweielementige Trägermenge betrachtet wird. Gängige Bezeichnungen sind $A = \{T, F\}$, $A = \{\bot, \top\}$ und $A = \{0, 1\}$.

Wir haben bereits Möglichkeiten kennen gelernt, auf der zweielementigen Menge $\{0, 1\}$ zu rechnen. Dazu bietet uns der zweielementige Körper GF(2) vielfältige Möglichkeiten. Gibt es weitere, und bringen die etwas neues?

Einstellige Operationen auf $\{0,1\}$

Wir wissen bereits, dass es auf der Menge $\{0,1\}$ genau

2 nullstellige, 4 einstellige und 16 zweistellige

Operationen gibt.

Mit einigen davon haben wir bereits gerechnet. Nun schauen wir nach, ob weitere interessante Rechenoperationen darunter sind.

Einstellige Operationen auf $\{0, 1\}$

Wir wissen bereits, dass es auf der Menge $\{0, 1\}$ genau

2 nullstellige, 4 einstellige und 16 zweistellige

Operationen gibt.

Mit einigen davon haben wir bereits gerechnet. Nun schauen wir nach, ob weitere interessante Rechenoperationen darunter sind.

Die beiden nullstelligen und zwei der einstelligen Operationen sind konstant. Es bleibt nur eine interessante einstellige Operation, $\neg$.

x	0	1
0	0	0

x	0	1
$e_1^1(x)$	0	1

x	0	1
$\neg x$	1	0

x	0	1
1	1	1

Zweistellige Operationen auf $\{0,1\}$

Von den sechzehn zweistelligen Operationen auf $\{0,1\}$ ...

0	0	1
0	0	0
1	0	0

	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

e_1^2	0	1
0	0	0
1	1	1

	0	1
0	0	1
1	0	0

e_2^2	0	1
0	0	1
1	0	1

	0	1
0	0	1
1	1	0

	0	1
0	0	1
1	1	1

	0	1
0	1	0
1	0	0

	0	1
0	1	0
1	0	1

	0	1
0	1	0
1	1	0

	0	1
0	1	0
1	1	1

	0	1
0	1	1
1	0	0

	0	1
0	1	1
1	0	1

	0	1
0	1	1
1	1	0

1	0	1
0	1	1
1	1	1

Zweistellige Operationen auf $\{0, 1\}$

... bleiben ohne Konstante und Projektionen noch 12, von denen zwei **wesentlich einstellig** sind ...

	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

	0	1
0	0	1
1	0	0

	0	1
0	0	1
1	1	0

	0	1
0	0	1
1	1	1

	0	1
0	1	0
1	0	0

	0	1
0	1	0
1	0	1

$\neg e_2^2$	0	1
0	1	0
1	1	0

	0	1
0	1	0
1	1	1

$\neg e_1^2$	0	1
0	1	1
1	0	0

	0	1
0	1	1
1	0	1

	0	1
0	1	1
1	1	0

Zweistellige Operationen auf $\{0, 1\}$

...es sind also noch 10 Operationen zu untersuchen. Zwei davon sind uns vom Rechnen modulo 2 vertraut:

$\cdot$	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

	0	1
0	0	1
1	0	0

$+$	0	1
0	0	1
1	1	0

	0	1
0	0	1
1	1	1

	0	1
0	1	1
1	1	0

	0	1
0	1	1
1	0	1

	0	1
0	1	0
1	1	1

	0	1
0	1	0
1	0	1

	0	1
0	1	0
1	0	0

Zusammengesetzte zweistellige Operationen auf $\{0, 1\}$

Die übrigen lassen sich daraus und der 1 zusammensetzen:

$x \cdot y$

$\cdot$	0	1
0	0	0
1	0	1

$x + x \cdot y$

	0	1
0	0	0
1	1	0

$y + x \cdot y$

	0	1
0	0	1
1	0	0

$x + y$

$+$	0	1
0	0	1
1	1	0

$x + y + x \cdot y$

	0	1
0	0	1
1	1	1

$1 + x \cdot y$

	0	1
0	1	1
1	1	0

$1 + x + x \cdot y$

	0	1
0	1	1
1	0	1

$1 + y + x \cdot y$

	0	1
0	1	0
1	1	1

$1 + x + y$

	0	1
0	1	0
1	0	1

$(1 + x) \cdot (1 + y)$

	0	1
0	1	0
1	0	0

Zweistellige Junktoren auf $\{0,1\}$

In der Aussagenlogik spricht man von **Junktoren** und verwendet andere Symbole.

$\wedge$	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

	0	1
0	0	1
1	0	0

	0	1
0	0	1
1	1	0

$\vee$	0	1
0	0	1
1	1	1

	0	1
0	1	1
1	1	0

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftarrow$	0	1
0	1	0
1	1	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

	0	1
0	1	0
1	0	0

Zweistellige Junktoren auf $\{0, 1\}$

Alle zweistelligen Junktoren lassen sich aus der **Konjunktion** $\wedge$ und der Negation $\neg$ zusammensetzen:

$x \wedge y$

$\wedge$	0	1
0	0	0
1	0	1

$x \wedge \neg y$

	0	1
0	0	0
1	1	0

$y \wedge \neg x$

	0	1
0	0	1
1	0	0

$\neg(x \Leftrightarrow y)$

	0	1
0	0	1
1	1	0

$\neg(\neg x \wedge \neg y)$

$\vee$	0	1
0	0	1
1	1	1

$\neg(x \wedge y)$

	0	1
0	1	1
1	1	0

$\neg(x \wedge \neg y)$

$\Rightarrow$	0	1
0	1	1
1	0	1

$\neg(\neg x \wedge y)$

$\Leftarrow$	0	1
0	1	0
1	1	1

$x \Leftrightarrow y$

$\Leftrightarrow$	0	1
0	1	0
1	0	1

$\neg x \wedge \neg y$

	0	1
0	1	0
1	0	0

Dabei ist $x \Leftrightarrow y = \neg(x \wedge \neg y) \wedge \neg(\neg x \wedge y)$

Zweistellige Junktoren auf $\{0,1\}$

Übersichtlicher ist es, die Junktoren aus der Konjunktion $\wedge$, der **Disjunktion** $\vee$ und der Negation $\neg$ zusammenzusetzen:

$x \wedge y$

$\wedge$	0	1
0	0	0
1	0	1

$x \wedge \neg y$

	0	1
0	0	0
1	1	0

$y \wedge \neg x$

	0	1
0	0	1
1	0	0

$\neg(x \Leftrightarrow y)$

	0	1
0	0	1
1	1	0

$\neg(\neg x \wedge \neg y)$

$\vee$	0	1
0	0	1
1	1	1

$\neg(x \wedge y)$

	0	1
0	1	1
1	1	0

$\neg x \vee y$

$\Rightarrow$	0	1
0	1	1
1	0	1

$x \vee \neg y$

$\Leftarrow$	0	1
0	1	0
1	1	1

$x \Leftrightarrow y$

$\Leftrightarrow$	0	1
0	1	0
1	0	1

$\neg(x \vee y)$

	0	1
0	1	0
1	0	0

Dabei ist $x \Leftrightarrow y = (\neg x \wedge \neg y) \vee (x \wedge y)$

Logikgatter

Aus sogenannten **Gattern** werden kombinatorische Logikschaltungen zusammengestellt.

AND	0	1
0	0	0
1	0	1

	0	1
0	0	0
1	1	0

	0	1
0	0	1
1	0	0

XOR	0	1
0	0	1
1	1	0

OR	0	1
0	0	1
1	1	1

NAND	0	1
0	1	1
1	1	0

	0	1
0	1	1
1	0	1

	0	1
0	1	0
1	1	1

	0	1
0	1	0
1	0	1

NOR	0	1
0	1	0
1	0	0

Peirce-Operator und Sheffer-Strich

Wegen $\neg x = \text{NAND}(x, x)$ und

$$x \wedge y = \text{NAND}(\text{NAND}(x, y), \text{NAND}(x, y))$$

lassen sich alle zweistelligen Operationen auf $\{0, 1\}$ aus der NAND-Operation zusammensetzen. Das Gleiche gilt für NOR.

Peirce-Operator und Sheffer-Strich

Wegen $\neg x = \textsc{nand}(x, x)$ und

$$x \wedge y = \textsc{nand}(\textsc{nand}(x, y), \textsc{nand}(x, y))$$

lassen sich alle zweistelligen Operationen auf $\{0, 1\}$ aus der NAND-Operation zusammensetzen. Das Gleiche gilt für NOR.

Man nennt die Operation

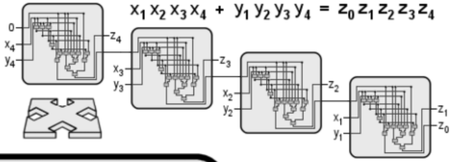
NAND auch den **Sheffer-Strich** und

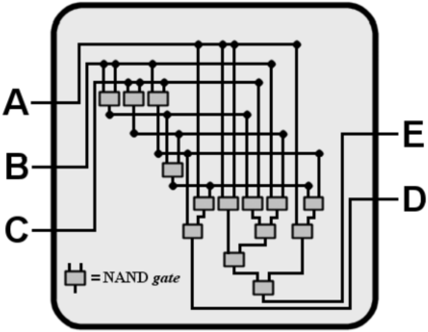
NOR die **Peirce-Funktion**.

Wie wir noch beweisen werden, kann man aus jeder dieser beiden Funktionen *alle* Operationen auf $\{0, 1\}$ zusammensetzen.

Ein Beispiel (aus Wikipedia)

Schematische Darstellung eines 4Bit-Addierers unter ausschließlicher Verwendung von NAND-Gates:





A	B	C	D	E
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

LiLiuS 2005

Etwas Theoriesprache: Signatur

Eine **Signatur** (auch **Rangalphabet** genannt) $\Sigma := (F, \sigma)$ besteht aus einer Menge F und einer Abbildung $\sigma : F \to \mathbb{N}$. Man nennt die Elemente aus F gern **Operationssymbole** und nennt $\sigma(f)$ die **Stelligkeit** des Operationssymbols $f \in F$.

Beispiel: $(\{+, \cdot, 0, 1\}, \{(+, 2), (\cdot, 2), (0, 0), (1, 0)\})$ ist eine Signatur mit den Operationssymbolen $F := \{+, \cdot, 0, 1\}$, deren Stelligkeiten durch die Abbildung

f	$+$	$\cdot$	0	1
$\sigma(f)$	2	2	0	0

gegeben sind.

Achtung: Zwischen Operationen und Operationssymbolen wird unterschieden!

Terme zu einer Signatur

Es sei $\Sigma := (F, \sigma)$ eine Signatur und X eine zu F disjunkte Menge, deren Elemente wir **Variablen**(symbole) nennen.

Dann sind die **Terme** zur Signatur Σ in den Variablen aus X genau die Ausdrücke, die induktiv durch folgende Regeln entstehen:

- Jede Variable $x \in X$ ist ein Term.
- Ist $f \in F$ ein n-stelliges Operationssymbol und sind $t_0, \ldots, t_{n-1}$ Terme, dann ist auch $f(t_0, \ldots, t_{n-1})$ ein Term.
  (Das schließt den Fall $n = 0$ mit ein: Ist f ein nullstelliges Operationssymbol, dann ist f ein Term.)

Die Menge aller Terme wird mit $T_\Sigma(X)$ bezeichnet.

Vereinfachte Schreibweise

Terme werden selten genau so benutzt, wie sie definiert sind. Um besser rechnen zu können, vereinbart man oft abweichende Schreibweisen.

Beispiel: Ein Term in den Variablen $\{x, y\}$ zu der oben angegebenen Signatur ist

$$\cdot(+(1, x), +(1, \cdot(x, y))).$$

Man schreibt dies lesbarer in **Infixnotation** so:

$$(1 + x) \cdot (1 + x \cdot y).$$

Für allgemeine Überlegungen ist die Standardform aber besser geeignet.

Allgemeine Algebra

Eine **allgemeine Algebra** (A, F_A) zur Signatur $\Sigma := (F, \sigma)$ besteht aus einer **Trägermenge** A zusammen mit einer Folge $(f_A \mid f \in F)$ von Operationen auf A (den **fundamentalen Operationen** der Algebra) mit der Eigenschaft, dass die zum Operationssymbol $f \in F$ gehörende Operation f_A jeweils $\sigma(f)$-stellig ist.

Zu jedem n-stelligen Operationssymbol f der Signatur muss also die Algebra eine n-stellige fundamentale Operation f_A auf der Trägermenge A haben.

Die algebraischen Strukturen, die in dieser Vorlesung behandelt wurden (Verbände, Gruppen, Ringe, Körper, Vektorräume, ...), fallen unter diesen Begriff.

Termauswertung

Eine **Belegung** der Variablen aus X in einer Menge A ist eine Abbildung $\beta : X \to A$.

Ist (A, F_A) eine Algebra zur Signatur Σ, dann kann jede Variablenbelegung $\beta : X \to A$ auf natürliche Weise zu einer Abbildung $\overline{\beta} : T_\Sigma(X) \to A$ erweitert werden, und zwar durch **algebraische Induktion**:

- Ist $x \in X$ eine Variable, dann ist $\overline{\beta}(x) := \beta(x)$.
- Ist $t \in T_\Sigma(X)$ ein Term der Form $t := f(t_0, \ldots, t_{n-1})$ für ein n-stelliges Operationssymbol $f \in F$, dann ist

$$\overline{\beta}(t) := f_A(\overline{\beta}(t_0), \ldots, \overline{\beta}(t_{n-1})).$$

Man spricht von der **Auswertung** des Terms t an der Stelle β.

Termoperationen

Ist $X := \{x_0, x_1, \ldots, x_{n-1}\}$, dann wird jedem n-Tupel $a := (a_0, \ldots, a_{n-1}) \in A^n$ eine Variablenbelegung $\beta_a : X \to A$ zugeordnet durch

$$\beta_a(x_i) := a_i \qquad \text{für } i := 0, \ldots, n-1.$$

Ist nun $t \in T_\sigma(\{x_0, \ldots, x_{n-1}\})$ ein Σ-Term und $\underline{A} := (A, F_A)$ eine Algebra der Signatur Σ, dann erhalten wird die **Termoperation** $\overline{t}$ zu t von $\underline{A}$ durch

$$\overline{t}(a) := \overline{\beta}_a(t) \qquad \text{für alle } a \in A.$$

Die Termoperationen sind genau diejenigen Operationen, die sich aus den fundamentalen Operationen von $\underline{A}$ zusammensetzen lassen.

Gleichungen

Eine **Gleichung** ist ein Paar (s,t) von Termen $s,t \in T_\Sigma(X)$.

Eine Gleichung (s,t) **gilt** in einer Σ-Algebra $\underline{A}$, wenn die beiden Termoperationen $\overline{s}$ und $\overline{t}$ identisch sind. Man schreibt dann gern $s = t$ und meint damit $\overline{s} = \overline{t}$.

Gleichungen

Eine **Gleichung** ist ein Paar (s, t) von Termen $s, t \in T_\Sigma(X)$.

Eine Gleichung (s, t) **gilt** in einer Σ-Algebra $\underline{A}$, wenn die beiden Termoperationen $\overline{s}$ und $\overline{t}$ identisch sind. Man schreibt dann gern $s = t$ und meint damit $\overline{s} = \overline{t}$.

In der zweielementigen **Booleschen Algebra** $(\{0, 1\}, \wedge, \vee, \neg, 0, 1)$ gelten z.B. die **Gesetze von de Morgan**

$$\begin{aligned} \neg(x \wedge y) &= \neg x \vee \neg y \\ \neg(x \vee y) &= \neg x \wedge \neg y, \end{aligned}$$

wie man leicht durch Vergleich der Termoperationen feststellt.

Operational vollständig

Wir wollen nun zeigen, dass die zweielementige Boolesche Algebra und der zweielementige Körper GF(2) **operational vollständig** sind (Synonym: **primal**), was bedeutet, dass *jede* Abbildung

$$f : \{0,1\}^n \to \{0,1\}$$

in beiden Algebren als Termoperation dargestellt werden kann.

Das gilt insbesondere für die Fundamentaloperationen der jeweils anderen Algebra. Man hat

$$x \wedge y = x \cdot y, \quad x \vee y = x + y + x \cdot y, \quad \neg x = 1 + x$$

und

$$x \cdot y = x \wedge y, \quad x + y = (x \wedge \neg y) \vee (\neg x \wedge y).$$