ARITHMETISCHE DARSTELLUNG DER FORMALEN LOGIK

II. Arithmetische Grundlagen

Peter Jaenecke

Die Restklassenarithmetik Modulo 2 wird über die Axiome des kommutativen Rings und über spezielle, die Restklassenarithmetik charakterisierende Axiome eingeführt. Aus diesen Axiomen werden elementare Sätze hergeleitet, mit denen sich die logischen Berechnungen erheblich vereinfachen lassen.

Ex nihilo unum omnia ducit.
Leibniz

1 Einleitung

Im ersten Teil der *Arithmetischen Logik* wurden die wichtigsten logischen Grundbegriffe eingeführt; sie bezogen sich auf die junktorielle Darstellung der Logik, die dadurch gekennzeichnet ist, dass die logischen Ausdrücke aus Aussagen bestehen, die durch Junktoren verknüpft sind. Jetzt geht es um die Grundlagen für ihre arithmetische Darstellung, bei der arithmetische Operatoren die Aufgabe der Junktoren übernehmen. Beide Darstellungen müssen gleichwertig sein, d.h. es muss sowohl eine Transformation als auch eine inverse Transformation geben, mit denen es möglich ist, von einer Darstellung in die jeweils andere zu wechseln.

Kapitel 2 behandelt den Übergang von der junktoriellen zur arithmetischen Darstellung auf der Basis der Wahrheitswertetabellen (Tabelle I.4): Zunächst wird die Restklassenarithmetik Modulo 2, kurz RK_2 – Arithmetik, eingeführt und anschließend gezeigt, dass jeder Junktor eineindeutig einem in dieser Arithmetik definierten ŽEGALKIN Polynom zugeordnet werden kann; dieses Polynom ist die gesuchte arithmetische Darstellung des Junktors. Die Eineindeutigkeit ist zugleich der Beweis, dass junktorielle und arithmetische Darstellung strukturgleich sind.

In *Kapitel 3* geht es darum, den arithmetischen Ausdruck für einen Junktor zu berechnen: Gegeben ist seine Wahrheitswertetabelle, gesucht ist sein ŽEGALKIN Polynom. Die Berechnung erfolgt über einen Koeffizientenvergleich; dieser liefert ein Gleichungssystem und dessen Lösungen ergeben die Koeffizienten des ŽEGALKIN Polynoms. Mit der gleichen Methode lassen sich Junktoren ineinander umrechnen.

Die Aussagenlogik ist hochredundant, insbesondere gibt es zu einem logischen Ausdruck unendlich viele andere logische Ausdrücke, die mit ihm äquivalent sind. In *Kapitel 4* geht es daher um die Frage, wie man am besten einen logischen Ausdruck vereinfachen kann. Gegeben sei also ein junktorenlogischer Ausdruck $\mathbf{Z}_1$, gesucht ist ein junktorenlogischer Ausdruck $\mathbf{Z}_2$ so, dass

(a) Inhalt($\mathbf{Z}_1$) = Inhalt ($\mathbf{Z}_2$) und

(b) $\mathbf{Z}_2$ ist einfacher als $\mathbf{Z}_1$

gilt. Hintergrund solch einer Vereinfachung ist die Frage, ob es sich bei einem gegebener Ausdruck um eine Tautologie, um eine Kontradiktion oder um einen neutralen Ausdruck handelt. Bei einer Tautologie ist $\mathbf{Z}_2$ = wahr, bei einer Kontradiktion ist $\mathbf{Z}_2$ = falsch. In diesen beiden Fällen ist es offensichtlich, dass $\mathbf{Z}_1$ nicht mehr weiter vereinfacht werden kann. Bei einem neutralen Ausdruck legen wir bei der Relation ‚einfacher als' ein intuitives Verständnis von Einfachheit zugrunde.

Hauptanwendungsgebiet der Vereinfachung ist die Optimierung einer elektronischen Schaltung. Bekanntlich muss jedes Programm in einen aussagenlogischen Ausdruck umgewandelt werden, damit es auf einer digitalen Recheneinheit ausgeführt werden kann. Solche Ausdrücke können mehrere Tausend Junktoren enthalten; sie können also sehr umfangreich sein, und deshalb ist es zur Verringerung des Rechenaufwandes von großem Interesse, sie möglichst klein zu halten. In *Kapitel 5* werden zunächst die herkömmlichen, auf Normalformen aufbauenden Vereinfachungsverfahren beschreiben und mit der arithmetischen Vereinfachungsmethode vergleichen.

2 Restklassenarithmetik Modulo 2 (RK_2-Arithmetik)

Die RK_2-Arithmetik bildet den kommutativen Ring

$$R = <\{0, 1\}, +, \cdot>,$$

dessen Axiome zunächst angegeben werden. Aus diesen Axiomen leiten wir dann anschließend einige elementare Sätze ab, die wir im Verlauf der Untersuchungen zur Vereinfachung der Berechnungen verwenden werden. Danach führen wir Restklassenausdrücke und Restklassenfunktionen ein und leiten den Fundamentalsatz über Restklassengleichungen her.

2.1 Axiome der RK_2-Arithmetik

Die Axiome der RK_2-Arithmetik wurden in Tabelle 1 zusammengestellt.[1]

Es gelte für alle $a, b, c, e_0, e_1 \in \mathbb{U}$:

Ringaxiome:

R_1	$a + b = b + a$	(kommutatives Gesetz der Addition)
R_2	$(a + b) + c = a + (b + c)$	(assoziatives Gesetz der Addition)
R_3	$a + e_0 = a$	(neutrales Element der Addition)
R_4	$a \cdot b = b \cdot a$	(kommutatives Gesetz der Multiplikation)
R_5	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	(assoziatives Gesetz der Multiplikation)
R_6	$a \cdot (b + c) = a \cdot b + a \cdot c$	(distributives Gesetz)
R_7	$a \cdot e_1 = a$	(neutrales Element der Multiplikation)

Spezielle Axiome der RK_2-Arithmetik:

R_+	$a + a = 0$	(Restklassenaddition Modulo 2)
$R_\cdot$	$a \cdot a = a$	(Idempotenz)

Tabelle 1: Axiome der RK_2-Arithmetik.

[1] S. auch BERNSTEIN (1936): *Postulates for Boolean algebra*, p. 318.

Diese wenigen Axiome bilden das Fundament für die gesamte formale Aussagenlogik. Die Axiome $R_1 - R_7$ definieren die allgemeinen Eigenschaften der Operationen '+' und '·'. Die folgenden zwei Axiome R_+ und $R_\cdot$ betreffen die RK_2-Arithmetik. $\mathbb{U}$ ist der Definitionsbereich der Axiome. Über die Axiome R_+ und $R_\cdot$ erhalten die Operationen '+' und '·' zusätzliche, die RK_2-Arithmetik charakterisierende Eigenschaften.

Neben den Operationen '+' und '·' kommt in den Axiomen noch das Gleichheitszeichen vor, dessen Handhabung durch die in Tabelle 2 angegebenen Ersetzungsregeln festgelegt wird. Von diesen Regeln werden wir im Folgenden Gebrauch machen, ohne besonders darauf hinzuweisen.

(A) $A =_{abk} T(x_1, x_2, ..., x_n)$

(F) $T_1(x_1, x_2, ..., x_n) = T_2(x_1, x_2, ..., x_n) \curvearrowright$
$oT_1(x_1, x_2, ..., x_n) = oT_2(x_1, x_2, ..., x_n)$, o inhaltsneutrale Operation

(E) $y = x_i \curvearrowright T(x_1, x_2, ..., x_i, ..., x_n) = T(x_1, x_2, ..., y, ..., x_n)$

(G_1) $\lambda \curvearrowright x = x$, λ ist das leere Zeichen

(G_2) $x = y \curvearrowright y = x$

Tabelle 2: Liste $R_=$ von allgemeinen Rechenregeln für gleichheitsbewahrende Umformungen. Es handelt sich um die Einführung einer Abkürzung (A), um die operationale Erweiterung einer Gleichung (F), um die Ersetzung gleicher Ausdrücke (E) sowie um zwei Regeln (G_1, G_2) für die Gleichheitsrelation. Das Zeichen ‚A $\curvearrowright$ B' bedeutet ‚A ist ersetzbar durch B'.

Regel (A) besagt lediglich, es dürfen Abkürzungen eingeführt werden, und die Kurzform ist per Definition mit der Langform gleichbedeutend.

Regel (F) sagt aus, dass die Gleichheit erhalten bleibt, wenn man auf beiden Seiten die gleiche inhaltsneutrale Operation o ausführt. Ob eine Operation inhaltsneutral ist, muss von Fall zu Fall geprüft werden. Inhaltsverändernd sind alle sinnlosen Operationen, denn sie führen Unsinn in die Berechnungen ein. So ist es z.B. unzulässig, beide Seiten einer Gleichung durch Null zu dividieren; auch eine Division durch $(x - 1)$ kann unzulässig sein, wenn der Fall $x = 1$ möglich ist. Hat man bisher nur mit reellen Zahlen gerechnet, so darf man auf beiden Seiten einer

Gleichung die Wurzel ziehen. Reelle Zahlen können aber auch negativ sein, und die Wurzel aus einer negativen Zahl ergibt eine aus dem Bereich der reellen Zahlen herausführende imaginäre Zahl. Das kann gewollt sein, es kann sich aber auch um eine unzulässige Inhaltserweiterung handeln.

Regel (E) bezieht sich auf die von LEIBNIZ stammende Ersetzbarkeit und besagt: kommt irgendwo in einem Term T ein x_i vor und gilt außerdem $x_i = y$, dann darf überall in dem Term T das x_i durch y ersetzt werden. Hier sichert die Gleichheit von x_i und y die logische Synonymität von $T(...,x_i,...)$ und $T(...,y,...)$.

Die Regeln G_1 und G_2 entsprechen den ersten beiden Axiomen für die Gleichheitsrelation; sie wurden aber hier als Ersetzungsregeln dargestellt. G_1 drückt die Identität aus, sie hat hier die Funktion einer Startregel für eine Gleichung. G_2 besagt, dass die Gleichheitsrelation kommutativ ist. Im Allgemeinen wird als drittes Axiom noch die Transitivität

$$a=b \wedge b=c \rightarrow a=c$$

angegeben, doch sie ist hier nur ein Theorem, das unmittelbar aus der Ersetzungsregel (E) folgt.

Zwischen den als wahr vorausgesetzten Axiomen und ihrem Definitionsbereich $\mathbb{U}$ besteht ein „Dualismus“: Entweder man wählt einen bestimmten Definitionsbereich, dann ist man nicht mehr frei in der Wahl der Axiome, oder man legt, wie im vorliegenden Fall, die Axiome fest, dann wird durch sie ihr Definitionsbereich eingeschränkt. Es gilt der folgende

Satz:

Wenn die Axiome der RK_2-Arithmetik als wahr vorausgesetzt werden, dann ist ihr Definitionsbereich gegeben durch

(1) $\mathbb{U} = \{e_0, e_1\}$.

Vereinfachter Beweis:

Der vereinfachte Beweis erfolgt in zwei Schritten:

(a) Es ist zu zeigen, dass die im Axiomensystem der RK_2-Arithmetik charakterisierten Operationen nicht aus dem Definitionsbereich $\mathbb{U}$ herausfallen.

(b) Es ist zu zeigen, dass ein Definitionsbereich mit mehr als zwei Elementen nicht mit dem Axiomensystem der RK_2-Arithmetik zu vereinbaren ist.

Beweis von (a):

(i) a + b führt nicht zu Werten, die außerhalb von $\mathbb{U} = \{e_0, e_1\}$ liegen:

$a = b$ führt wegen R_+ auf $a + a = e_0$, $a \in \mathbb{U}$;

$a \neq b$ führt auf $e_1 + e_0$ oder $e_0 + e_1$; beides ergibt nach R_3 und R_1 den Wert e_1.

(ii) a · b führt nicht zu Werten, die außerhalb von $\mathbb{U} = \{e_0, e_1\}$ liegen:

$a = b$ führt wegen $R_\cdot$ auf $a \cdot a = a$, $a \in \mathbb{U}$;

$a \neq b$ führt auf $e_1 \cdot e_0$ oder $e_0 \cdot e_1$; beides ergibt nach R_7 und R_4 den Wert e_0.

Addition und Multiplikation der Elemente aus $\mathbb{U}$ ergeben wieder Elemente aus $\mathbb{U}$. □

Beweis von (b):

Der Definitionsbereich enthalte die drei unterschiedlichen Elemente $\{e_0, e_1, e_2\}$. Welche Werte kann dann die Summe $e_1 + e_2$ annehmen?

(i) $e_1 + e_2 = e_2$. Also gilt auch $e_1 + (e_2 + e_2) = (e_2 + e_2)$ und wegen R_+ gilt außerdem $e_1 + e_0 = e_0$, im Widerspruch zu R_3.

(ii) $e_1 + e_2 = e_1$. Also gilt auch $e_2 + (e_1 + e_1) = (e_1 + e_1)$ und wegen R_+ gilt außerdem $e_2 + e_0 = e_0$, im Widerspruch zu R_3, es sei denn $e_2 = e_0$; das steht aber im Widerspruch zur Annahme.

(iii) $e_1 + e_2 = e_0$. Also gilt auch $e_1 + (e_2 + e_2) = e_0 + e_2$ und wegen R_+ gilt außerdem $e_1 + e_0 = e_0 + e_2$, im Widerspruch zu R_3, es sei denn $e_1 = e_2$; das steht aber im Widerspruch zur Annahme.

Ein dreielementiger Definitionsbereich ist nicht mit den Axiomen vereinbar. Entsprechendes gilt für einen Definitionsbereich mit mehr als drei Elementen, denn dieser Fall lässt sich durch $e_2' = e_2 + e_3 + \ldots$ auf den dreielementigen zurückführen. □

Die RK_2-Arithmetik lässt sich somit als mathematische Struktur

$$S = < \mathbb{U}, +, \cdot, = >$$

darstellen, wobei die Arithmetikaxiome von Tabelle 1 die beiden Operationen '+' und '·' und die Ersetzungsregeln aus Tabelle 2 die Gleichheitsrelation charakterisieren.

Welche Werte für die Symbole e_0 und e_1 stehen sollen, darüber sagen die Axiome nichts aus; e_0 wird auch als ‚Nullelement' und e_1 als ‚Einselement' bezeichnet. Ohne die Allgemeinheit einzuschränken, wählen wir daher $e_0 = 0$ und $e_0 = 1$, d.h. wir legen im Folgenden für die RK_2-Arithmetik den Definitionsbereich

$$\mathbb{U} = \{0, 1\} \qquad (2)$$

zugrunde.

Durch diese Wahl beschreiben die obigen Axiome in exakter Weise vertraute arithmetische Operationen, denn es gelten auch in der RK_2-Arithmetik alle aus der Schulmathematik bekannten arithmetischen Rechenregeln mit Ausnahme derjenigen, die sich aus den Axiomen R_+ und $R_\cdot$ ergeben; diese tragen allerdings in erheblichem Maß zur Vereinfachung der Berechnungen bei.

Dies zeigt sich bereits bei den elementaren, in Tabelle 3 zusammengestellten, aus den Axiomen der Restklassenarithmetik abgeleiteten Sätzen, die wir – ohne es eigens zu erwähnen – bei unseren Berechnungen zugrundelegen. Die Sätze $RS_1 - RS_4$ kommen häufig bei Umformungen zum Einsatz, während die Sätze RS_5 und RS_6 als elementare Schlussfolgerungen angesehen werden können.

Es gelte für alle $a, b, c \in \mathbb{U}$ die Sätze:

RS_1	wenn $x + a = b$, dann $x = a + b$ und umgekehrt
RS_2	$a \cdot 0 = 0$
RS_3	$a \cdot (a + 1) = 0$
RS_4	$a \cdot (b + a \cdot c) = a \cdot (b + c)$
RS_5	aus $a \cdot b = 1$, folgt $a = 1$ und $b = 1$
RS_6	aus $a + b + a \cdot b = 0$, folgt $a = 0$ und $b = 0$

Tabelle 3: Elementare Sätze der RK_2-Arithmetik.

Satz RS_1 betrifft das Umformen von Gleichungen; er besagt in umgangssprachlicher Fassung: man darf eine additiv verknüpfte Größe von einer Seite der Gleichung auf die andere bringen. Ein Vorzeichenwechsel, wie man es sonst in der Arithmetik gewohnt ist, erfolgt nicht, denn es gibt keine negativen Zahlen:[2]

$$\begin{aligned} &x + a = b, \\ &x + a + a = a + b && \text{(Addition mit } a\text{)}, \\ &x + 0 = a + b && (R_+), \\ &x = a + b && (RS_1). \end{aligned}$$

Eine entsprechende Umformungsmöglichkeit für eine multiplikative Verknüpfung gibt es nicht.

[2] ŽEGALKIN (1927): *Über die Technik der Berechnung von Sätzen in der symbolischen Logik*, p. 13.

RS_2 behauptet $a \cdot 0 = 0$; dies folgt aus der Beweiskette

$$\begin{aligned} a \cdot 0 &= a \cdot (a + a) &&= && (R_+) \\ &= a \cdot a + a \cdot a &&= && (R_6) \\ &= a + a &&= && (R_\bullet) \\ &= 0 && && (R_+). \end{aligned}$$

RS_3 ist, wie wir später sehen werden, das arithmetische Gegenstück zum sogenannten Satz des ausgeschlossenen Widerspruchs.

Den Satz RS_4, $a \cdot (b + a \cdot c) = a \cdot (b + c)$, könnte man als Ausklammerungsregel bezeichnen.[3] Er erweist sich als sehr hilfreich zur Vereinfachung von Ausdrücken, denn er besagt: man darf im Inneren einer Klammer jeden Faktor streichen, wenn er schon als Faktor vor der Klammer vorkommt, und zwar unabhängig davon, welche Faktoren bei den anderen Ausdrücken in der Klammer stehen; insbesondere gilt

$$a \cdot (b + a) = a \cdot (b + 1).$$

Er lässt sich durch die folgende Beweiskette beweisen:

$$\begin{aligned} a \cdot (b + a \cdot c) &= \\ &= a \cdot b + a \cdot a \cdot c = && (R_6) \\ &= a \cdot (b + c) && (R_\bullet, R_6). \end{aligned}$$

Die Axiome R_+ und $R_\bullet$ sowie die Sätze $RS_1 - RS_4$ vereinfachen die Berechnungen erheblich; wir werden ausführlich von ihnen Gebrauch machen.

Beweis von RS_5: Sei $a \neq b$, also $a = b + 1$ und somit $(b + 1) \cdot b = 1$, im Widerspruch zu RS_3; also muss $a = b$ gelten, d.h. $a = b = 1$ wegen der Idempotenz $R_\bullet$.

Es bleibt der Beweis für RS_6. Multipliziert man $a + b + a \cdot b = 0$ mit a durch ergibt sich wegen $R_\bullet$: $a + a \cdot b + a \cdot b = 0$, also $a = 0$. Entsprechend erhält man $b = 0$, wenn man mit b durchmultipliziert.

[3] Der Satz findet sich bereits bei ŽEGALKIN (1927): *Über die Technik der Berechnung von Sätzen in der symbolischen Logik*, p. 12f.

2.2 Restklassenausdrücke und -funktionen

Nicht jede Kombination arithmetischer Zeichen ist sinnvoll, d.h. stellt einen korrekten arithmetischen Ausdruck dar. Die Menge der wohlformulierten arithmetischen Ausdrücke wird meist umgangssprachlich durch eine induktive Definition festgelegt. Die Menge bildet eine formale Sprache: Gestützt auf die Vokabulare

$$\mathbb{V} = \{a_1, a_2, ..., a_n\}$$
$$\mathbb{J} = \{+, \cdot\},$$
$$\mathbb{V}_{\text{technische Zeichen}} = \{(,), [,], \{, \}\}$$

lässt sich daher die induktive Definition unmittelbar in die reguläre Grammatik

$$G_{RK} = < \mathbb{V}_{\text{Nichtterminale}}, \mathbb{V}_{\text{Terminale}}, S, \mathbb{R} >$$

übertragen, wobei

$$\mathbb{V}_{\text{Nichtterminale}} = \{S, Z\},$$
$$\mathbb{V}_{\text{Terminale}} = \mathbb{V} \cup \mathbb{J} \cup \mathbb{V}_{\text{technische Zeichen}}$$
$S \in \mathbb{V}_{\text{Nichtterminale}}$ ist das Startsymbol und steht für ‚logischer Ausdruck'

$\mathbb{R}$ ist die Regelmenge

(1)	$S \Rightarrow a_i \quad a_i \in \mathbb{V}$,
(2)	$S \Rightarrow Z$,
(3a – 3c)	$Z \Rightarrow (Z) \mid [Z] \mid \{Z\}$
(4a – 4b)	$Z \Rightarrow a_i \circledast_j Z \mid Z \circledast_j a_i \quad a_i \in \mathbb{V}, \circledast_j \in \mathbb{J}$
(5)	$Z \Rightarrow a_i \quad a_i \in \mathbb{V}$

Beispiel: Es ist der Ausdruck $a_1 \cdot (a_2 + a_3)$ aus G_{RK} zu erzeugen. Für diesen Fall ist $\mathbb{V} = \{a_1, a_2, a_3\}$, $\mathbb{J} = \{+, \cdot\}$ und $\mathbb{V}_{\text{technische Zeichen}} = \{(,), [,]\}$. Im Folgenden werden die Herleitungsschritte angegeben; links erscheint jeweils die Nummer der verwendeten Regel:

(2) Z

(4a) $a_1 \cdot (Z)$

(4a) $a_1 \cdot (a_2 + Z)$

(5) $a_1 \cdot (a_2 + a_3)$.

Eine Zeichenkette ist danach genau dann ein arithmetischer Ausdruck, wenn sie bezüglich der regulären Grammatik G_{RK} grammatisch korrekt ist; ob dies zutrifft, kann man daher für jede Zeichenkette stets in endlich vielen Schritten entscheiden.

Restklassenfunktionen führen wir – dem bekannten mathematischen Vorbild folgend – über arithmetische Ausdrücke ein:

Definition: k – stellige Restklassenfunktion

Eine k – stellige Restklassenfunktion $\mathbf{f}$ mit $k = 1, 2, ...,$ dem Definitionsbereich $\mathbb{D}$ und dem Wertebereich $\mathbb{U}$ ist eine Vorschrift, die jedem k -Tupel $(\mathrm{x_1}, \mathrm{x_2}, ..., \mathrm{x_k}) \in \underbrace{\mathbb{D} \times \mathbb{D} \times ... \times \mathbb{D}}_{k-\textit{faches kartesisches Produkt}}$ einen Wert $w \in \mathbb{U}$ zuordnet. Die Zuordnungsvorschriften werden durch Restklassenausdrücke beschrieben.

Für die Restklassenfunktionen übernehmen wir die in der Mathematik übliche Schreibweise und schreiben z.B.

$$f(\mathbf{a}, \mathbf{b}, \mathbf{c}) = (\mathbf{a} + \mathbf{b}) \cdot \mathbf{c}\,.$$

Wir lassen eine beliebige endliche Anzahl von unabhängigen Variablen zu. Da Definitions- und Wertebereich endlich sind, lässt sich jede Restklassenfunktion eindeutig durch eine Wertetabelle charakterisieren.

2.3 Fundamentalsatz über Restklassengleichungen

Unter einer Restklassengleichung (RK-Gleichung) verstehen wir eine implizit definierte Funktion:

Definition: Restklassengleichung

Sei $\mathbf{f}$ eine k – stellige Restklassenfunktion, dann ist $\mathbf{f}$ implizit definiert durch die Gleichung $\mathbf{f}(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}) = w$, wobei $\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n} \in \mathbb{D}^n, w \in \mathbb{U}$; w ist eine Konstante.

RK-Gleichungen kann man entweder vereinfachen oder lösen. Dabei spielen die Rechenregeln von Tabelle 2 eine große Rolle. Sie sind so definiert, dass sie bei ihrer Verwendung die Gleichheit bewahren. Aber Gleichungen besitzen auch eine Lösungsmenge; man muss daher untersuchen, ob sie auch die Lösungsmenge unverändert lassen. Das ist im Allgemeinen nicht der Fall:

Satz über die Erhaltung der Lösungsmenge

Eine Ersetzungsregel lässt die Lösungsmenge unverändert, wenn die Ersetzung rückgängig gemacht werden kann.

Wenn die Ersetzungsregel rückgängig gemacht werden kann, dann kann dies an irgendeiner Stelle geschehen, spätestens also in der Lösungsmenge selbst.

Die Regeln (A), (E), (G_1) und (G_2) haben, wie sich leicht zeigen lässt, keinen Einfluss auf die Lösungsmenge. Die Regel (F) kann sie jedoch verändern; das ist bereits aus der herkömmlichen Arithmetik bekannt. So bleibt z.B. die Gleichheit erhalten, wenn man beide Seiten einer Gleichung quadriert; man kann dies auch wieder rückgängig machen, allerdings nur auf Kosten von Vorzeichenproblemen.

Eine Veränderung der Lösungsmenge ist auch in der RK_2-Arithmetik bei Anwendung der Regel (F) zu erwarten. Ausgangspunkt sind die beiden Operatoren

(3) $\{T(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n) +, T(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n)\bullet\}$;

dabei ist T ein beliebiger n-stelliger logischer an eine arithmetische Operation gekoppelter Ausdruck; durch diese Kopplung wird der Ausdruck zu einem Operator. Gegeben seien ferner zwei beliebige logische Ausdrücke T_1 und T_2; es gelte $T_1 = T_2$; dann ergibt sich für

$T(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n) +$:

$$T(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n) + T_1(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n) = T(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n) + T_2(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n);$$

wiederholt man diese Operation, erhält man

$$(T + T) + T_1 = (T + T) + T_2 \text{ bzw.}$$
$$e_0 + T_1 = e_0 + T_2,$$

und daraus folgt wegen R_3 wieder die Ausgangsgleichung $T_1 = T_2$. Die erste Operation aus der Menge (3) verändert die Lösungsmenge nicht. Das ist ein sehr wichtiges Ergebnis, denn nur mit Hilfe dieser Operation ist es möglich, einen Term von der einen Seite einer Gleichung auf die andere zu bringen.

Mit Vorsicht hingegen ist die zweite Operation, das Durchmultiplizieren einer Gleichung mit einem Term, zu gebrauchen, denn das Durchmultiplizieren lässt sich nicht rückgängig machen. Sie führt zwar wiederum auf eine Gleichung, und, da man mit beliebig vielen Termen durchmultiplizieren kann, lassen sich aus einer Gleichung beliebig viele neue Gleichungen erzeugen. Da man dabei aber nichts Neues gewinnt, macht das Durchmultiplizieren nur dann Sinn, wenn man dadurch Terme gewinnt, die man in Gleichungen einsetzen und sie dadurch vereinfachen kann.

Während in der herkömmlichen Arithmetik das Durchmultiplizieren im Allgemeinen zu komplizierteren Ausdrücken führt, verhindern bei Restklassengleichungen die Idempotenz (Axiom R•) und die Addition Modulo 2 (Axiom R+) nicht nur die Zunahme an Komplexität, sondern bewirkt oft auch ihre Vereinfachung. Multipliziert man z.B. $(\mathbf{x} + \mathbf{xy})$ mit $\mathbf{y}$ durch, so erhält man 0. Bei Restklassengleichungen ist also Durchmultiplizieren durchaus sinnvoll; mehr noch: es ist, wie wir sehen werden, ein hochwirksames Beweisinstrument. Dass man allerdings dabei behutsam umgehen muss, zeigt die folgende Behauptung:

Wenn $\mathbf{a} + \mathbf{b} = 1$ gilt, dann gilt auch $\mathbf{a} \cdot \mathbf{b} = 0$.

Multipliziert man $\mathbf{a} + \mathbf{b} = 1$ mit $\mathbf{a}$ oder mit $\mathbf{b}$ durch, so ergibt sich mit Axiom R• unmittelbar die Behauptung. Aber die *gültige* Gleichung $\mathbf{a} \cdot \mathbf{b} = 0$ ist inhaltlich nicht gleichwertig mit der Ausgangsgleichung $\mathbf{a} + \mathbf{b} = 1$, denn sie lässt auch die *ungültige* Lösung $\mathbf{a} = \mathbf{b} = 0$ zu. Das ist ein wichtiges Ergebnis: Das Durchmultiplizieren liefert zwar eine zulässige Gleichung, die z.B. an irgendeiner Stelle in einem Gleichungssystem eingesetzt werden darf, aber sie ersetzt nicht die Gleichung, welche durchmultipliziert wurde; diese darf nicht weggelassen werden. Sei z.B.

$$\mathbf{x} + \mathbf{xy} = 1.$$

Mit $\mathbf{y}$ durchmultipliziert, ergibt unmittelbar $\mathbf{y} = 0$. Damit erhalten wir zwar eine Lösung der Gleichung, aber es geht durch das Durchmultiplikation die Information über $\mathbf{x}$ verloren. Allerdings darf man, da beim Durchmultiplizieren die Gleichheit erhalten bleibt, die gewonnene Lösung in die Ausgangsgleichung einsetzen; das führt dann auf die Lösung $\mathbf{x} = 1$. Das Ergebnis fassen wir zusammen in dem

Fundamentalsatz für Restklassengleichungen

Gegeben seien beliebige Restklassenfunktionen g_1, $\mathbf{g}_2$, ..., $\mathbf{g}_n$ sowie eine Menge von m k–Tupeln $\mathbb{D}_m{}^k = \{(\mathbf{x}_1{}^1, \mathbf{x}_2{}^1, ..., \mathbf{x}_k{}^1), ..., (\mathbf{x}_1{}^m, \mathbf{x}_2{}^m, ..., \mathbf{x}_k{}^m)\} \subseteq \mathbb{D}^k$, dabei ist $\mathbb{D}^k$ der Definitionsbereich einer Ausgangsfunktion $\mathbf{f}$ und $\mathbb{D}_m{}^k$ die Lösungsmenge der Ausgangsgleichung $\mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) = w$, $w \in \mathbb{U}$, d.h. für alle $(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) \in \mathbb{D}_m{}^k$ gelte diese Gleichung. Dann besitzt das Gleichungssystem

$$\mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) = w$$
$$\mathbf{g}_1 \cdot \mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) = w \cdot \mathbf{g}_1$$
$$\mathbf{g}_2 \cdot \mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) = w \cdot \mathbf{g}_2$$
$$...$$
$$\mathbf{g}_n \cdot \mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_k) = w \cdot \mathbf{g}_n$$

ebenfalls die Lösungsmenge $\mathbb{D}_m{}^k$.

Der Fundamentalsatz lässt sich unmittelbar auf ein System von Ausgangsgleichungen erweitern.

Beweis:

(a) Sei $w = 1$. Dann gilt für alle Lösungen aus der Lösungsmenge $\mathbb{D}_m{}^k$: $\mathbf{g_i} = w\ \mathbf{g_i}$ ($i = 1, 2, ..., n$); diese Gleichung ist erfüllt für alle Elemente aus dem Definitionsbereich $\mathbb{D}^k$, d.h. das Durchmultiplizieren der Funktionen $\mathbf{g_i}$ erweitert zunächst die Lösungsmenge. Da jedoch für alle Elemente $\mathbb{D}^k \setminus \mathbb{D}_m{}^k$ die Gleichung $\mathbf{f}(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_k}) = 0$ gilt, wird die erweiterte Lösungsmenge wieder auf die ursprüngliche eingeschränkt. (b) Ein entsprechendes Ergebnis erhält man für $w = 0$.

Der Fundamentalsatz besagt, dass es *zusätzlich* zur Ausgangsgleichung weitere Gleichungen gibt, die sich aus dem Durchmultiplizieren der Ausgangsgleichung mit irgendeinem Term erzeugen lassen. Die zusätzlich gewonnenen Gleichungen haben den Status von Hilfsgleichungen; sie führen auf keine neuen Lösungen, sind aber weniger informativ als die Ausgangsgleichung. Deswegen können sie nicht die Ausgangsgleichung ersetzen, aber sie können dazu verwendet werden, die Ausgangsgleichung zu vereinfachen.

Der Fundamentalsatz lässt auch zu, dass eine Gleichung, die bereits mit einem Term durchmultipliziert wurde, mit einem weiteren durchmultipliziert werden darf. In der RK_2-Arithmetik ist die Zahl der zusätzlichen Gleichungen begrenzt, wenn man nur mit Termen durchmultipliziert, welche aus Variablen bestehen, die auch in der Ausgangsgleichung vorkommen, denn dann führen irgendwann die beiden Axiome R_+ und $R_\bullet$ auf die Gleichung $0 = 0$ oder auf die Ungleichung $0 = 1$.

Beispiele

Beispiel 1

(1*) $\quad \mathbf{x_1} + \mathbf{x_2} + \mathbf{x_3} + \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} = 1$

Gleichung (1*) z.B. mit $\mathbf{x_1}$ durchmultipliziert, ergibt

$$\mathbf{x_1} + \mathbf{x_1}\mathbf{x_2} + \mathbf{x_1}\mathbf{x_3} + \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} = \mathbf{x_1} \quad \text{bzw.} \quad \mathbf{x_1}\mathbf{x_2} + \mathbf{x_1}\mathbf{x_3} + \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} = 0$$

Im nächsten Schritt wird die letzte Gleichung mit $\mathbf{x_3}$ durchmultipliziert; das führt auf

$$\mathbf{x_1}\mathbf{x_2}\mathbf{x_3} + \mathbf{x_1}\mathbf{x_3} + \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} = 0$$

und damit auf

$$\mathbf{x_1}\mathbf{x_3} = 0 \quad \text{und somit auch auf} \quad \mathbf{x_1}\mathbf{x_2}\mathbf{x_3} = 0,$$

so dass die Ausgangsgleichung (1*) die einfache Form

(1*′) $\quad \mathbf{x_1} + \mathbf{x_2} + \mathbf{x_3} = 1$

annimmt, d.h. die beiden Gleichungen (1*) und (1*′) sind inhaltsgleich, aber Gleichung (1*′) ist einfacher als Gleichung (1*).

Beispiel 2

Reduktionssatz:

Seien $\mathbf{x}$ und $\mathbf{A}$ zwei beliebige Ausdrücke mit $\mathbf{x} \neq 0$, $\mathbf{A} \neq 0$ und $\mathbf{A} \neq 1$, wenn $\mathbf{x} \neq 1$; es gelte ferner $\mathbf{x} = \mathbf{A}\mathbf{x}$. Dann gilt auch $\mathbf{A} = \mathbf{x}$.

Beweis:

Unter den genannten Voraussetzungen ist $\mathbf{x} = \mathbf{Ax}$ nur dann allgemein erfüllt, wenn die Idempotenz ins Spiel kommt, denn sie führt auf die allgemeine Gleichung $\mathbf{x} = \mathbf{x}$.

Beispiel 3

Gesucht ist die Lösungsmenge für die Ausgangsgleichung

(2*) $\mathbf{ab}(1+\mathbf{c})+\mathbf{a}+\mathbf{b}=0$ bzw. für $\mathbf{ab}+\mathbf{abc}+\mathbf{a}+\mathbf{b}=0$.

Durchmultiplizieren mit **a** führt auf

(2*$_1$) $\mathbf{a}=\mathbf{abc}$.

Setzt man dieses Ergebnis in die Gleichung (2*) ein, so ergibt sich

(2*′) $\mathbf{b}=\mathbf{ab}$,

bzw. Letzteres in Gleichung (2*$_1$) eingesetzt, $\mathbf{a} = \mathbf{bc}$. Gleichung (2*$_1$) ist eine Zusatzgleichung zu Gleichung (2*); Gleichung (2*′) ist ihre vereinfachte Form. Die Lösungsmenge lässt sich einfach durch die Fallunterscheidung $\mathbf{a} = 0$ und $\mathbf{a} = 1$ ermitteln:

Fall 1: $\mathbf{a} = 0$; daraus folgt $\mathbf{bc} = 0$.

Fall 2: $\mathbf{a} = 1$; daraus folgt $\mathbf{c} = 1$ und $\mathbf{b} = 1$.

Die Lösungsmenge lautet daher: $\mathbb{L}=\{\underbrace{(0,0,0),(0,0,1),(0,1,0)}_{\text{Fall 1}},\underbrace{(1,1,1)}_{\text{Fall 2}}\}$.

Beispiel 4

Durchmultiplizieren kann einen Beweis merklich vereinfachen, wie der folgende Fall zeigt:

Satz:

Wenn sowohl $\mathbf{a}(\mathbf{b}+1)=0$ als auch $\mathbf{b}(\mathbf{c}+1)=0$ gilt, dann gilt auch $\mathbf{a}(\mathbf{c}+1)=0$.

Beweis: Multipliziert man die Gleichung $\mathbf{b}(\mathbf{c}+1)=0$ mit **a** durch, so erhält man $\mathbf{ab}(\mathbf{c}+1)=0$. Aus $\mathbf{a}(\mathbf{b}+1)=0$ folgt $\mathbf{ab}=\mathbf{a}$ und somit die Behauptung.

2.4 Entwicklungssatz

Sei

$$\mathbf{t}^{\mathbf{k}}=(\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_{\mathbf{k}})$$

ein $k-$Tupel von Variablen ($k>1$),

$$\mathbf{f}(\mathbf{t}^{\mathbf{k}})=_{abk}\mathbf{f}(\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_{\mathbf{k}})$$

eine k – stellige RK_2-Funktion und

$$\mathbf{t}^{\mathbf{k}}\setminus\mathbf{x}_{\mathbf{i}},\ i=1,2,...,k.$$

ein $(k-1)-$Tupel von Variablen, bei der die Variable $\mathbf{x}_{\mathbf{i}}$, $i=1,2,...,k$ fehlt; $\mathbf{t}^{\mathbf{0}}=\mathbf{t}^{1}\setminus\mathbf{x}_1$ ist ein leeres Tupel, die Funktion $\mathbf{f}(\mathbf{t}^{0})=a$ ist eine Konstante. Dann gilt der folgende

Entwicklungssatz:

Gegeben sei eine beliebige $k-$stellige logische Funktion $\mathbf{f}(\mathbf{t}^{\mathbf{k}})$ mit $k>1$. Dann gibt es zwei Tupel von Variablen, $\mathbf{t}_1$ und $\mathbf{t}_2$, mit

(4) $\mathbf{f}(\mathbf{t}^{\mathbf{k}})=\mathbf{f}_1(\mathbf{t}_1\setminus\mathbf{x}_{\mathbf{i}})+\mathbf{x}_{\mathbf{i}}\cdot\mathbf{f}_2(\mathbf{t}_2\setminus\mathbf{x}_{\mathbf{i}}),\ \mathbf{t}_1,\mathbf{t}_2\subset\mathbf{t}^{\mathbf{k}},\ i=1,2,...,k.$

Beweis

Die Funktion f kann man zerlegen in einen Anteil $\mathbf{f_1}$, in dem $\mathbf{x_i}$ nicht vorkommt sowie in einen Anteil $\mathbf{f_2^*}$, in dem $\mathbf{x_i}$ vorkommt. Aus $\mathbf{f_2^*}$ kann man daher $\mathbf{x_i}$ herausziehen, so dass

$$\mathbf{f}_2^{\,*}(\mathbf{t}_2) = \mathbf{x_i} \cdot \mathbf{f}_2(\mathbf{t}_2 \setminus \mathbf{x_i}),$$

d.h.

$$f(\mathbf{t^k}) = f_1(\mathbf{t}_1 \setminus \mathbf{x_i}) + \mathbf{x_i} \cdot f_2(\mathbf{t}_2 \setminus \mathbf{x_i}).$$

Satz:

Sei $\mathbf{f}$ ein $k-$ stelliges analytisches Gesetz, d.h. es gelte $\mathbf{f}(\mathbb{D}^k) = w,\ w \in \mathbb{W}$. Dann lässt sich dieses Gesetz ebenfalls nach einer ihren Variablen entwickeln, d.h.

$$\mathbf{f(t^k)} = \mathbf{f}_1(\mathbf{t}_1 \setminus \mathbf{x_i}) + \mathbf{x_i} \cdot \mathbf{f}_2(\mathbf{t}_2 \setminus \mathbf{x_i}) + w = 0,\ \mathbf{t}_1, \mathbf{t}_2 \subset \mathbf{t^k},\ i = 1,2,...,k,$$

und es gilt

$$(5) \qquad \mathbf{f}_1(\mathbf{t}_1 \setminus \mathbf{x_i}) = w,\ \mathbf{f}_2(\mathbf{t}_2 \setminus \mathbf{x_i}) = 0,\quad \mathbf{t}_1, \mathbf{t}_2 \subset \mathbf{t^k},\ i = 1,2,...,k.$$

Der Beweis folgt aus dem Entwicklungssatz.

Einsetzungssatz 1:

Sei $\mathbf{f}$ ein $k-$ stelliges analytisches Gesetz, d.h. es gelte $\mathbf{f}(\mathbf{t^k}) = w,\ w \in \mathbb{W}$ und sei $\mathbf{g}(\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y_m})$ eine beliebige RK_2 - Funktion. Dann gilt:

$$\mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, \mathbf{g}, \mathbf{x}_{i+1}, ..., \mathbf{x_n}) = w,\ w \in \mathbb{W}.$$

Beweis:

Nach dem Entwicklungssatz gilt $f(\mathbf{t}^k) = f_1(\mathbf{t}_1 \setminus \mathbf{x_i}) + \mathbf{x_i} \cdot f_2(\mathbf{t}_2 \setminus \mathbf{x_i}) + w$; da $\mathbf{f}$ nach Voraussetzung ein analytisches Gesetz ist, gilt wegen der Beziehungen (5) stets $\mathbf{f}(\mathbf{t}^k) = w + \mathbf{x_i} \cdot 0 + w = 0$ und damit auch $\mathbf{f}(\mathbf{t}^k) = w + g \cdot 0 + w = 0$.

Einsetzungssatz 2:

Gegeben seien die RK_2 - Funktionen

$$\mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, g, \mathbf{x}_{i+1}, ..., \mathbf{x_n}) =$$
$$= \mathbf{f}_1(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, ..., \mathbf{x_n}) + \mathbf{g} \cdot \mathbf{f}_2(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, ..., \mathbf{x_n}),$$

$\mathbf{g}(\mathbf{x}_{j_1}, \mathbf{x}_{j_2}, ..., \mathbf{x}_{j_m})$ und $\mathbf{h}(\mathbf{x}_{j_1}, \mathbf{x}_{j_2}, ..., \mathbf{x}_{j_m})$ mit $j_1, ..., j_m \in \{1, ..., n\}$;

es sei $\mathbf{g}(\mathbf{x}_{j_1}, \mathbf{x}_{j_2}, ..., \mathbf{x}_{j_m}) = \mathbf{h}(\mathbf{x}_{j_1}, \mathbf{x}_{j_2}, ..., \mathbf{x}_{j_m})$.

Dann gilt auch

$$\mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, g, \mathbf{x}_{i+1}, ..., \mathbf{x_n}) = \mathbf{f}(\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_{i-1}, h, \mathbf{x}_{i+1}, ..., \mathbf{x_n}).$$

Beweis:

Nach dem Entwicklungssatz gilt $\mathbf{f}(\mathbf{t^k}) = \mathbf{f}_1(\mathbf{t}^{\mathbf{k}_1} \setminus \mathbf{x_i}) + \mathbf{g} \cdot \mathbf{f}_2(\mathbf{t}^{\mathbf{k}_2} \setminus \mathbf{x_i})$; daraus folgt

$$\mathbf{f}(\mathbf{t^k}) = \mathbf{f}_1(\mathbf{t}^{\mathbf{k}_1} \setminus \mathbf{x_i}) + \underbrace{\mathbf{g} \cdot \mathbf{f}(\mathbf{t}^{\mathbf{k}_2} \setminus \mathbf{x_i}) + \mathbf{h} \cdot \mathbf{f}_2(\mathbf{t}^{\mathbf{k}_2} \setminus \mathbf{x_i})}_{=0} + \mathbf{h} \cdot \mathbf{f}_2(\mathbf{t}^{\mathbf{k}_2} \setminus \mathbf{x_i})$$

und somit die Behauptung.

In diesem Kapitel wurden die Mittel zusammengestellt, um mit Ausdrücken und Gleichungen aus der RK_2-Arithmetik bequem rechnen zu können. Um diese bequeme Rechenweise auch auf die zweiwertige Junktorenlogik zu übertragen, muss nun eine Verbindung zwischen dieser Logik und der RK_2-Arithmetik hergestellt werden. Dies soll im folgenden Kapitel geschehen.

3 Arithmetische Darstellung der zweiwertigen Aussagenlogik

Die Aussagenlogik lässt sich sowohl junktoriell als auch arithmetisch darstellen. Im ersten Abschnitt beschreiben wir die Transformationen, mit denen der Wechsel von einer Darstellung in die andere vollzogen werden kann. Beide Darstellungen müssen inhaltsgleich sein, d.h. ihre Strukturen müssen identisch sein; wir drücken dies durch den Satz über Strukturidentität aus, der im zweiten Abschnitt über die ŽEGALKIN Polynome bewiesen wird, indem gezeigt wird, dass jedem Junktor umkehrbar eindeutig ein ŽEGALKIN Polynom zugeordnet werden kann. Der dritte Abschnitt beschäftigt sich mit der Aufgabe, an Hand der Wertetabellen für jeden Junktor das zugehörige ŽEGALKIN Polynom zu berechnen.

3.1 Transformationen zwischen zweiwertiger Aussagenlogik und RK$_2$-Arithmetik

Die zweiwertige Aussagenlogik ist durch den Wahrheitswertebereich $\mathbb{W}=\{w_1, w_2\}$ gekennzeichnet. Der Ausdruck 'zweiwertig' zeigt an, dass nur zwei Wahrheitswerte zugelassen sind, und zwar w_1 und w_2. Darüber hinaus gibt es in der Junktorenmenge $\mathbb{J}$ 16 Junktoren, mit denen bestimmte Variablen aus einer Variablenmenge $\mathbb{P}$ zu einem aussagenlogischen Ausdruck verknüpft werden können (Tabelle 4 a).

Variablenmenge:	$\mathbb{P}=\{\mathbf{p},\mathbf{q},\mathbf{r},...\}$	$\mathbb{P}=\{\mathbf{p},\mathbf{q},\mathbf{r},...\}$
Wertebereich der Variablen:	$\mathbb{W}=\{wahr, falsch\}$	$\mathbb{U}=\{1,0\}$
Menge der Junktoren/Operatoren:	$\mathbb{J}=\{\neg, \wedge, \vee, \rightarrow, ...\}$	$\mathbb{O}=\{\cdot, +\}$
	(a)	(b)

Tabelle 4: Gegenüberstellung von junktorieller Darstellung der zweiwertigen Aussagenlogik (a) und RK$_2$-Arithmetik (b).

Die RK$_2$-Arithmetik ist ebenfalls zweiwertig; sie hat den Wertebereich $\mathbb{U}=\{1,0\}$. Ihre Operationsmenge $\mathbb{O}$ enthält allerdings nur zwei Operatoren, mit denen mit den Variablen aus einer Variablenmenge $\mathbb{P}$ arithmetische Ausdrücke aufgebaut werden können (Tabelle 4 b). Wir werden im Folgenden ständig zwischen den beiden Darstellungen hin und her wechseln. Um die Schreibweise zu vereinfachen, legen wir fest:

(i) Wir führen für logische Wahrheitswerte und arithmetische Werte keine unterschiedlichen Variablensymbole ein, da aus den Operationszeichen immer hervorgeht, welche Werte gemeint sind, so dass keine Verwechselungsgefahr besteht. Dies wurde bereits in der Gegenüberstellung in Tabelle 4 berücksichtigt; dort wurde für beide Darstellungen die gleiche Variablenmenge $\mathbb{P}$ vorgesehen.

(ii) Der Übergang von einem Ausdruck der RK$_2$-Arithmetik zu ihrem logischen Gegenpart oder der von einem logischen zu einem arithmetischen Ausdruck wird durch eine symmetrische, d.h. in beide Richtungen geltende Transformationsbeziehung beschrieben, die wir durch '$=_T$' symbolisieren. Repräsentiert die eine Seite der Beziehung einen junktorenlogischen Ausdruck, dann repräsentiert die andere sein arithmetisches Gegenstück und umgekehrt.

Strukturidentitätssatz:

Zwischen der RK$_2$-Arithmetik und der zweiwertigen Aussagenlogik besteht eine Strukturidentität, wenn festgelegt wird, dass folgende, in beiden Richtungen ausführbare Transformationen vereinbart werden:

$$wahr =_T 1,\ falsch =_T 0,$$
$$\mathbb{J}=\{\wedge, \veebar\} =_T \mathbb{O}=\{\cdot, +\}.$$

Der Strukturidentitätssatz kann entweder über die junktorenlogischen Wahrheitswertetafeln und den ŽEGALKIN Polynomen oder – wie wir im III. Teil der *Arithmetischen Darstellung* zeigen werden – aus geeigneten Axiomensystemen hergeleitet werden. Wir wählen zunächst den Beweisweg über die ŽEGALKIN Polynome.

3.2 Beweis des Strukturidentitätssatzes über die ŽEGALKIN Polynome

Jede Funktion in der RK_2-Arithmetik lässt sich algebraisch nach einem Polynom entwickeln, das auch als 'ŽEGALKIN Polynom' bezeichnet wird.[4] Das ŽEGALKIN Polynom für zweistellige Funktionen lautet

$$(6) \qquad \mathbf{f}(\mathbf{p},\mathbf{q};a_0,a_1,a_2,a_3) = a_0 + a_1\mathbf{p} + a_2\mathbf{q} + a_3\mathbf{pq}\,, \quad \mathbf{p},\mathbf{q},a_0,a_1,a_2,a_3 \in \{0,1\}\,.$$

Höhere Potenzen entfallen, weil die Restklassenmultiplikation idempotent ist (Axiom $R_\bullet$).

Die vier Koeffizienten kann man sich als eine vierstellige Binärzahl geschrieben denken. Es gibt genau 16 Binärzahlen 0000, 0001, ..., 1111 und folglich 16 verschiedene Koeffizientensätze für ein zweistelliges ŽEGALKIN Polynom. Jeder Koeffizientensatz definiert genau ein ŽEGALKIN Polynom; es gibt somit genau 16 unterschiedliche zweistellige ŽEGALKIN Polynome. Andererseits gibt es auch genau 16 verschiedene Junktoren. Folglich lässt sich jeder vierstelligen Binärzahl umkehrbar eindeutig ein ŽEGALKIN Polynom und jedem ŽEGALKIN Polynom umkehrbar eindeutig ein Junktor der zweiwertigen Aussagenlogik zuordnen.

Damit wurde der Strukturidentitätssatz bewiesen: Für alle 16 Junktoren der zweistelligen Aussagenlogik lassen sich umkehrbar eindeutig arithmetische Ausdrücke angeben. Im nächsten Abschnitt wird berechnet, welcher Junktor zu welchem ŽEGALKIN Polynom gehört.

3.3 Berechnung der ŽEGALKIN Polynome aus den Wertetabellen der Junktoren

Im Folgenden gehen wir davon aus, dass ein Junktor durch seine als bekannt vorausgesetzte Wahrheitswertetafel definiert ist. Sein arithmetisches Gegenstück sei das ŽEGALKIN Polynom

$$(7) \qquad \mathbf{f}(\mathbf{p},\mathbf{q};a_0,a_1,a_2,a_3) = a_0 + a_1\mathbf{p} + a_2\mathbf{q} + a_3\mathbf{pq}\,, \quad \mathbf{p},\mathbf{q},a_0,a_1,a_2,a_3 \in \{0,1\}\,.$$

Die Aufgabe besteht darin, die Koeffizienten a_0,a_1,a_2,a_3 des Polynoms aus der Wahrheitswertetafel zu berechnen, indem man die zu einem Junktor gehörenden Angaben aus seiner Wahrheitswertetafel auf ein Gleichungssystem zurückführt und dieses dann löst.

[4] ŽEGALKIN (1928): p. 324ff.

Wir betrachten zunächst den Sonderfall der einstelligen Junktoren; für sie haben die ŽEGALKIN Polynome die allgemeine Form

$$(8) \qquad \mathbf{f}(\mathbf{p};a_0,a_1) = a_0 + a_1\mathbf{p} \quad \mathbf{p},a_0,a_1 \in \{0,1\}\,,$$

bzw.

$$\mathbf{f}(\mathbf{q};a_0,a_2) = a_0 + a_2\mathbf{q} \quad \mathbf{q},\, a_0,a_2 \in \{0,1\}\,.$$

Sie gehen aus dem ŽEGALKIN Polynom (6) hervor, indem man dort a_3 sowie entweder a_1 oder a_2 Null setzt, so dass im Polynom immer nur eine Variable auftreten kann. Das ergibt die in Tabelle 5 angegebenen sechs möglichen einstelligen ŽEGALKIN Polynome.

a_0	a_1	a_2	a_3	**ŽEGALKIN Polynom**
1	1	0	0	$1+1\cdot\mathbf{p}$
0	1	0	0	$1\cdot\mathbf{p}$
1	0	1	0	$1+1\cdot\mathbf{q}$
0	0	1	0	$1\cdot\mathbf{q}$
1	0	0	0	1
0	0	0	0	0

Tabelle 5: Die in der zweiwertigen Aussagenlogik möglichen sechs einstelligen ŽEGALKIN Polynome.

Zweistellige Junktoren sind dadurch gekennzeichnet, dass sie zwei Aussagen **p** und **q** miteinander verknüpfen. Ihre arithmetische Darstellung können also nur aus solchen ŽEGALKIN Polynomen bestehen, die sowohl von **p** als auch von **q** abhängen. Im einfachsten Fall bedeutet dies: nur a_3 ist verschieden von Null; im kompliziertesten Fall sind alle Koeffizienten verschieden von Null (Tabelle 6). Als ŽEGALKIN Polynom muss daher die allgemeine Form (7) angesetzt werden, in der alle vier Koeffizienten vorkommen.

a_0	a_1	a_2	a_3	ŽEGALKIN Polynom
0	0	0	1	$1\cdot\mathbf{pq}$
0	1	1	0	$1\cdot\mathbf{p} + 1\cdot\mathbf{q}$
0	1	0	1	$1\cdot\mathbf{p} + 1\cdot\mathbf{pq}$
0	0	1	1	$1\cdot\mathbf{q} + 1\cdot\mathbf{pq}$
0	1	1	1	$1\cdot\mathbf{p} + 1\cdot\mathbf{q} + 1\cdot\mathbf{pq}$
1	0	0	1	$1 + 1\cdot\mathbf{pq}$
1	1	1	0	$1 + 1\cdot\mathbf{p} + 1\cdot\mathbf{q}$
1	1	0	1	$1 + 1\cdot\mathbf{p} + 1\cdot\mathbf{pq}$
1	0	1	1	$1 + 1\cdot\mathbf{q} + 1\cdot\mathbf{pq}$
1	1	1	1	$1 + 1\cdot\mathbf{p} + 1\cdot\mathbf{q} + 1\cdot\mathbf{pq}$

Tabelle 6: Die in der zweiwertigen Aussagenlogik möglichen zehn zweistelligen ŽEGALKIN Polynome.

Es folgen einige Beispiele.

Negation

Die Verneinung ist ein einstelliger Junktor; es genügt daher vom ŽEGALKIN Polynom (8) auszugehen, denn die Koeffizienten a_2 und a_3 sind Null und damit bereits bekannt. Die Wahrheitswertetafel der Verneinung führt auf das Gleichungssystem

$$\begin{aligned} \neg w &= f \qquad a_0 + a_1 \cdot 1 = 0 \\ \neg f &= w \qquad a_0 + a_1 \cdot 0 = 1;\ a_0 = 1 \end{aligned}$$

d.h. es gilt $a_0 = a_1 = 1$ bzw.

$$\neg\mathbf{p} =_T 1 + \mathbf{p}\,.$$

Konjunktion

Aus der Wahrheitswertetafel der Konjunktion ergeben sich die Gleichungen

$$\begin{aligned} w \wedge w &= w \qquad a_0 + a_1 + a_2 + a_3 = 1 \\ w \wedge f &= f \qquad a_0 + a_1 = 0 \\ f \wedge w &= f \qquad a_0 + a_2 = 0 \\ f \wedge f &= f \qquad a_0 = 0 \end{aligned} \quad ;$$

aus ihnen folgt $a_0 = a_1 = a_2 = 0$ und $a_3 = 1$ bzw.

$$\mathbf{p} \wedge \mathbf{q} =_T f(\mathbf{p}, \mathbf{q}; 0, 0, 0, 1) = \mathbf{pq}.$$

Exklusives Oder

Die Wahrheitswerttafel vom exklusiven Oder liefert die Gleichungen

$$\begin{aligned} w \,Y w &= f \qquad a_0 + a_1 + a_2 + a_3 = 0 \\ w \,Y f &= w \qquad a_0 + a_1 = 1 \\ f \,Y w &= w \qquad a_0 + a_2 = 1 \\ f \,Y f &= f \qquad a_0 = 0 \end{aligned} \quad ;$$

Daraus folgen die Koeffizienten $a_0 = a_3 = 0$ und $a_1 = a_2 = 1$, d.h. es gilt

$$\mathbf{p}\,Y\,\mathbf{q} =_T \mathbf{p} + \mathbf{q}\,.$$

Wie aus den obigen Beispielen zu erkennen ist, bleibt die linke Seite der Gleichungen für alle Junktoren gleich; Unterschiede treten nur auf der rechte Seite bei den Konstanten auf, d.h. es gilt jeweils das Gleichungssystem

$$\begin{aligned} a_0 + a_1 + a_2 + a_3 &= w_1 \\ a_0 + a_1 &= w_2 \\ a_0 + a_2 &= w_3 \\ a_0 &= w_4 \end{aligned}$$

zu lösen. Dieses Gleichungssystem hat immer eine eindeutige Lösung, ganz gleich, welche Werte die Konstanten $w_1, ..., w_4$ annehmen; die Lösung lautet:

$$
\begin{aligned}
a_0 &= w_4 \\
a_1 &= w_2 + w_4 \\
a_2 &= w_3 + w_4 \\
a_3 &= w_1 + w_2 + w_3 + w_4
\end{aligned}
\qquad (9)
$$

mit

$$w_1, ..., w_4 \in \{0,1\}.$$

Alternative

Für die Alternative lautet die Wahrheitswertetabelle

$$
\begin{array}{ll}
w \vee w = w & w_1 = 1 \\
w \vee f = w & w_2 = 1 \\
f \vee w = w & w_3 = 1 \\
f \vee f = f & w_4 = 0
\end{array},
$$

aus der über das Gleichungssystem (9) $a_0 = 0$ sowie $a_1 = a_2 = a_3 = 1$ bzw.

$$\mathbf{p} \vee \mathbf{q} =_T \mathbf{p} + \mathbf{q} + \mathbf{pq}$$

folgt.

Implikation

Die Wahrheitswerttafel der Implikation lautet

$$
\begin{array}{ll}
w \rightarrow w = w & w_1 = 1 \\
w \rightarrow f = f & w_2 = 0 \\
f \rightarrow w = w & w_3 = 1 \\
f \rightarrow f = w & w_4 = 1
\end{array}.
$$

In das Gleichungssystem (9) eingesetzt, ergeben sich die Koeffizienten $a_0 = a_1 = a_3 = 1$ und $a_2 = 0$ und somit die arithmetische Entsprechung

$$\mathbf{p} \rightarrow \mathbf{q} =_T 1 + \mathbf{p} + \mathbf{pq}.$$

Auf die gleiche Weise können auch alle übrigen ŽEGALKIN Polynome über die Wahrheitswertetafeln berechnet werden (Tabelle 7, Tabelle 8). Damit lässt sich das gesamte formale Wissen der zweiwertigen Aussagenlogik durch 16 ŽEGALKIN Polynome darstellen. Die in Tabelle 8 angegebene Zuordnung zwischen den Junktoren und ihren ŽEGALKIN Polynomen stellt eine bidirektionale Verbindung zwischen junktorieller und arithmetischer Welt her, d.h. man kann einen Junktor in seinen arithmetischen Ausdruck transformieren und einen arithmetischen Ausdruck wieder zurück in eine junktorielle Darstellung bringen. Setzt man diese Tafeln als gegeben voraus, dann handelt es sich bei der Zuordnung von einem Junktor zu einem ŽEGALKIN Polynom jeweils um ein Theorem, denn die Zuordnung lässt sich beweisen.

Die Wahrheitswertetafeln haben den gleichen Status wie herkömmliche Wertetabellen für Funktionen reeller Zahlen. Doch während sich die Polynomkoeffizienten *eindeutig* aus den Wahrheitswertetabellen bestimmen lassen, ist es bei Funktionen über reelle Zahlen meist nur möglich, etwa durch eine Regressionsanalyse, eine Näherungsfunktion zu berechnen.

	Verneinen (Negation)	Unverändertlassen (Identität)	Wahrmachen (Tautologie)	Falschmachen (Kontradiktion)
p	**¬p**	**÷p**	**◊p**	**#p**
w	f	w	w	f
f	w	f	w	f
	p + 1	p	1	0

Tabelle 7: Wahrheitswertetafeln der einstellige Junktoren und ihr arithmetisches Gegenstück.

Bezeichnung **logische**	**technische**	**Sym bol**	**p** **q**	w w	w f	f w	f f	Arithmetische Operation
Einsfunktion, Tautologie		◊		w	w	w	w	1
Alternative, Disjunktion (Oder)	OR	∨		w	w	w	f	**p** + q + p • q
Gegenimplikation, Replikation		←		w	w	f	w	q + p • q
Transferfunktion **p**		÷		w	w	f	f	p
Implikation (wenn-dann)		→		w	f	w	w	p + p • q + 1
Transferfunktion **q**		÷		w	f	w	f	q
Äquivalenz	XNOR	↔		w	f	f	w	p + q + 1
Konjunktion (und)	AND	∧		w	f	f	f	p • q
SHEFFER Strich	NAND	|, ↑		f	w	w	w	p • q + 1
Exklusives Oder, Antivalenz, Autfunktion	XOR	Y		f	w	w	f	p + q
Negation **q**	NOT	¬		f	w	f	w	q + 1
Rehibition (**q**, aber nicht **p**)		⊥		f	w	f	f	p + p • q
Negation **p**	NOT	¬		f	f	w	w	p + 1
Inhibition (**p**, aber nicht **q**)		T		f	f	w	f	q + p • q + 1
NICOD Funktion, PEIRCE Funktion (weder-noch)	NOR	↓		f	f	f	w	p + q + p • q + 1
Nullfunktion, Kontradiktion		#		f	f	f	f	0

Tabelle 8: Wertetabellen der zweistellige Junktoren und ihr arithmetisches Gegenstück.

3.4 Zurückführung von drei- und mehrstelligen Junktoren auf zweistellige

Ein dreistelliger Junktor verknüpft drei Aussagen miteinander, so dass seine Wahrheitswertetabelle die acht mögliche Eingangszustände

p q r	**Wahrheitswert**
0 0 1	w_1
0 1 0	w_2
0 1 1	w_3
1 0 0	w_4
1 0 1	w_5
1 1 0	w_6
1 1 1	w_7
0 0 0	w_8

berücksichtigen muss. Diese Tabelle erfasst 2^8 verschiedene dreistellige Junktoren. Es gilt nun zu zeigen, dass sich diese Junktoren eindeutig durch die 2^8 ŽEGALKIN Polynome

$$\mathbf{f(p,q,r)} = a_0 + a_1\mathbf{p} + a_2\mathbf{q} + a_3\mathbf{r} + a_4\mathbf{pq} + a_5\mathbf{pr} + a_6\mathbf{qr} + a_7\mathbf{pqr}$$

darstellen lassen. Man muss also nachweisen, dass für jeden dreistelligen Junktor die Koeffizienten a_0, ..., a_7 eindeutig aus seiner Wertetabelle berechnet werden können. Dazu verwenden wir die gleiche Methode, die bereits bei den zweistelligen Junktoren zum Erfolg führte: Aus jeder Zeile der Tabelle stellen wir eine Bestimmungsgleichung auf; insgesamt erhalten wir das Gleichungssystem

$$a_0 = w_8$$
$$a_0 + a_3 = w_1$$
$$a_0 + a_2 = w_2$$
$$a_0 + a_1 = w_4$$
$$a_0 + a_2 + a_3 + a_6 = w_3$$
$$a_0 + a_1 + a_3 + a_5 = w_5$$
$$a_0 + a_1 + a_2 + a_4 = w_6$$
$$a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = w_7\,,$$

mit der Lösung

$$a_0 = w_8$$
$$a_1 = w_4 + w_8$$
$$a_2 = w_2 + w_8$$
$$a_3 = w_1 + w_8$$
$$a_4 = w_2 + w_4 + w_6 + w_8$$
$$a_5 = w_1 + w_4 + w_5 + w_8$$
$$a_6 = w_1 + w_2 + w_3 + w_8$$
$$a_7 = \sum_{n=1}^{8} w_n$$

Damit konnte jeder Koeffizient eindeutig als Funktion der Wahrheitswerte bestimmt werden, d.h. jeder dreistellige Junktor ist auf einen Ausdruck der zweistelligen Junktoren $\wedge$ und Y zurückführbar. Entsprechendes gilt für Junktoren, die mehr als drei Stellen haben. Wir brauchen daher nur Ausdrücke mit höchstens zweistelligen Junktoren zu betrachten.

4 Rechnen mit aussagenlogischen Ausdrücken

Die Aussagenlogik ist hochredundant; dies zeigt sich unter anderem daran, dass es viele Möglichkeiten gibt, eine junktorielle Verknüpfung in eine andere umzurechnen. Der *erste* Abschnitt beschäftigt sich daher mit den arithmetischen Möglichkeiten für solche Umrechnungen. Wenn es möglich ist, junktorielle Verknüpfungen in andere junktorielle Verknüpfungen umzurechnen, so stellt sich die Frage, ob nicht ein bestimmter Satz von Junktoren, gewissermaßen als eine Junktorenbasis, ausreicht, um alle anderen Verknüpfungen darzustellen? Mit dieser Frage setzt sich der *zweite* Abschnitt auseinander; es wird angegeben, wie sich arithmetisch solch eine Basis berechnen lässt.

Literatur

Siehe: *Arithmetische Darstellung der formalen Logik: Gesamtliteraturverzeichnis*