Informatik 1 & 2

Vorlesung von

Professor Wilfried Lex

an der

Technischen Universität Clausthal

1995

Textverarbeitung: Christian Preuße
unterstützt von: Marcus Döring
e-mail: christian.preusse@rz.tu-clausthal.de
Erstellt mit emTEX auf der Basis von LATEX 2_ε.

Inhaltsverzeichnis

Einleitung

Was ist Informatik?

informatio, onis f. (lat.) die Abbildung in der Seele die Vorstellung, der Begriff; — verbi: Darstellung des Begriffes, der in dem Worte liegt.

Informatik 1968 von franz. „l'informatique“: Science de traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications, dans les domaines techniques, économiques et socials.

Computer science computer: Rechner, von (lat.) „computare“ – zusammen-, be-rechnen; „putare“ – reinigen, rechnen, meinen.

Kybernetik Wissenschaft von den Steuerungen, Regelungen; Teilgebiet der Informatik

Aufteilung:

- Theoretische Informatik
- Technische Informatik
- Praktisch–Angewandte Informatik

Kurzer historischer Abriß

ca.–1800 Abakus
In der gesamten Antike waren Algorithmen (Rechenverfahren) bekannt und wurden angewandt. Das Wort ist eine Latinisierung von al–Ḫwārizmī [1].

1202 „Liber abbaci“ des Leonardo Fibonacci von Pisa (ca.1180–ca.1250), Vermittler des indisch-arabischen Positionssystems.

[1] eigentlich Abū ^{c}Abdallah oder Abū Ǧa^{c}far Muḥammad ibn Mūsā al–Ḫwārizmī al–Maǧūsī (ca. 780–846); nicht zu verwechseln mit Abū ^{c}Abdallah Muḥammad ibn Aḥmad ibn Muḥammad Yūsuf al–Ḫwārizmī al–Kātib (der Schreiber), 2. Hälfte 10. Jh., wirkte in Buchara am Hofe der Samaniden-Emire, vermutlich in der Verwaltung, und war Verfasser der „Mafātīḥ al–^{c}ulūm“ (Schlüssel der Wissenschaften), der ersten arabischen Enzyklopädie. Der erste al–Ḫwārizmī war Leiter des „Hauses der Weisheit“, einer Akademie in Bagdad unter dem Abassidenkalifen al–Ma'mūn (813–833) und schrieb u. a. „Al–kitab al–muḫtaṣar fi ḥisāb al–ǧabr wa'l–muqābala“ (Ein kurzgefaßtes Buch über die Rechenverfahren durch Ergänzen und Ausgleichen)[Gleichungslehre]; auf dieses „al–ǧabr“ geht übrigens unser Wort „Algebra“ zurück.

1623 Wilhelm Schick(h)ard(t) (22.IV.1592–23.X.1635), Mathematiker und Orientalist, Professor in Tübingen, erste Rechenmaschine.

1674 Gottfried Wilhelm Leibniz (1.VII.1646–14.XI.1716), Universalgelehrter, Mitglied der Royal Society, konstruierte Rechenmaschine (mit Gleitschlitten und Staffelwalze); darüber hinaus durch Binärsystem, seine „Characteristica universalis“ und Logik von Bedeutung für die Informatik.

1833 Charles Babbage (26.XII.1792–18.X.1871), Professor in Cambridge, entwirft ersten programmgesteuerten Universalrechner: „Analytic Engine“.

ab ca. 1850 Entwicklung der modernen Logik.

1886 Herrmann Hollerith (20.II.1860–17.XI.1929), amerikanischer Bergbauingenieur deutscher Abkunft, Erfinder und Unternehmer, konstruierte eine Lochkartenmaschine zur Auswertung der 11. amerikanischen Volkszählung 1890 (43 Maschinen mit je 1 Helfer 4 Wochen; vorher (1880): 500 Helfer 7 Jahre!).

1938 Konrad Ernst Otto Zuse (*22.VI.1910): erster programmgesteuerter mechanischer Rechner mit Binärtechnik, „Z1“.

1939— „Z2“: elektromechanischer Rechner mit rund 200 Relais.

1941— „Z3“: erste voll arbeitsfähige programmgesteuerte elektromechanische Maschine mit Rechenwerk (600 Relais), 2 parallelen arithmetischen Einheiten für Exponent und Mantisse, Speicher (1400 Relais; 64 Wörter à 22 Bits) und Steuerung (8-Kanal-Lochstreifen); Multiplikation: 3s.

1944 Howard Hathaway Aiken (8.III.1900–14.III.1977), Professor an der Harvard University, danach in Miami, baute „MARK I“, Relaisrechner: 16m lang, 2,5m hoch, 35t schwer, Multiplikation: 6s.

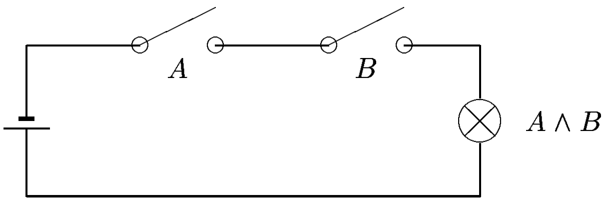
Kapitel 1

Schaltungen, Verbände und Logik

1.1 Schalter und Schaltungen

Beispiel 1 (elektrische, bistabile Schalter)
0 symbolisiere „Strom fließt nicht“ oder „Schalter auf“, 1 „Strom fließt“ oder„Schalter zu“.

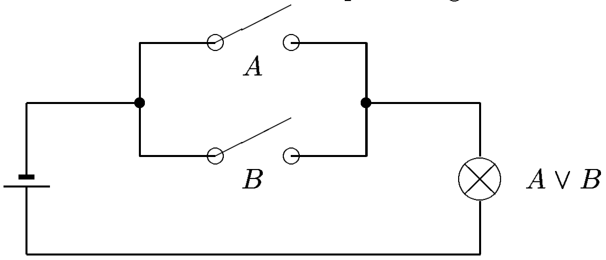
a) Zwei Schalter A und B seien in Reihe (bzw. Serie, seriell oder hintereinander) geschaltet. Das entsprechende Schaltbild sieht wie folgt aus:



A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

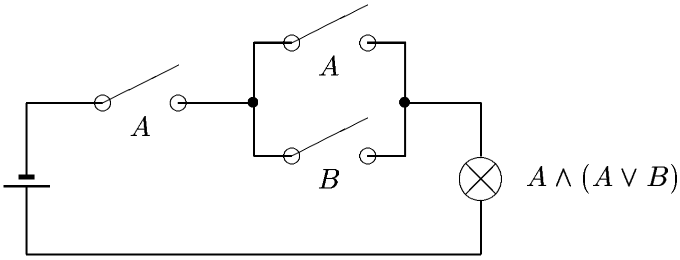
Rechts ist die das Schaltbild beschreibende Tabelle. Dabei verwenden wir 0 und 1 für die entsprechenden Schalterstellungen.

b) Zwei Schalter A und B seien parallel geschaltet. Schaltbild und Wertetabelle:



A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

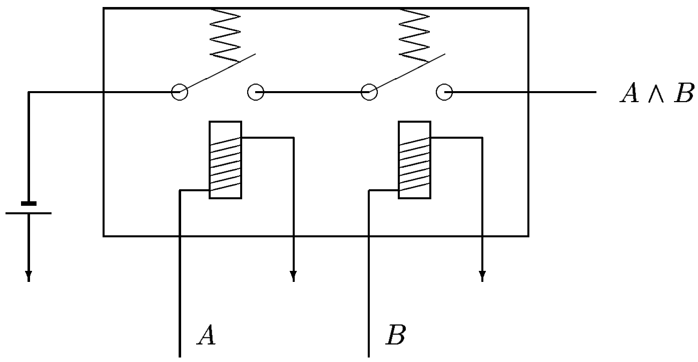
c) Die beiden obigen Schaltungen zusammengefaßt ergibt das folgende Schaltbild:



A	B	$A \wedge (A \vee B)$
0	0	0
0	1	0
1	0	1
1	1	1

Die Wahrheitstafel zeigt, daß $A \wedge (A \vee B) = A$. Gleichheit verstehen wir hier als gleiche Wirkung, und gleiche Bezeichnung zweier Schalter besagt, daß der eine genau dann zu ist, wenn der andere geschlossen ist.

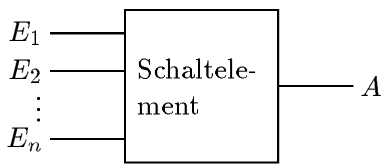
d) Schalter können auch elektrisch betrieben werden:



Für solche und ähnliche Schaltungen gibt es genormte Zeichen, die im Anhang C aufgeführt sind.
Solche elektrischen Schaltungen werden heute durch Transistoren verwirklicht. Diese modernen Schaltelemente haben den Vorteil, daß sie sehr schnell und klein sind. (Näheres siehe Vorlesung „Technische Informatik“, speziell VLSI-Entwurf [Very Large Scale Integration], ca. 10^5 Bauelemente pro Chip; ULSI, SLSI ($> 10^6$))
Andere Realisierungsmöglichkeiten sind Fluidikelemente und Neuronen.

Definition 1 (Schaltelement, $\mathbb{B}$, Schaltungen)

α) Ein **Schaltelement** ist eine technische — oder auch biologische — Vorrichtung mit $n(\in \mathbb{N}_0)$ Eingängen $E_1, \ldots, E_n$ und einem Ausgang A derart, daß das Anliegen bzw. Nichtanliegen eines Signals (etwa Spannung, Luftstrom, etc.), 1 bzw. 0, an jedem der n Eingänge eindeutig das Anliegen bzw. Nichtanliegen eines Signals am Ausgang bedingt.



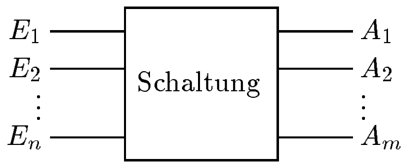
Bei zwei Eingängen A und B kann man speziell unter folgenden Schaltelementen unterscheiden:

Schaltelement	alternative Bezeichnung	Mathematische Zeichen
NON-Gatter	Inverter, Negator	$\overline{A}$, $\neg A$, $\sim A$
AND-Gatter	Konjunktor	$A \wedge B$, $A \& B$, $A \bullet B$, AB
OR-Gatter	Adjunktor, Disjunktor, Alternator, Valenz	$A \vee B$, $A + B$
NAND-Gatter	Negatadjunktor, Sheffer-Strich [stroke]	$\overline{A \wedge B}$, $A \barwedge B$, $A \vert B$, $A \uparrow B$ oder $A \downarrow B$, $A \sqcup B$, $A - B$
NOR-Gatter	Negatkonjunktor, Antialternator, Peirce-Pfeil , Nicod-Funktor, „weder, noch“	$\overline{A \vee B}$, $A \overline{\vee} B$, $A \downarrow B$ oder $A \uparrow B$, $A \sqcap B$, $A \bigtriangledown B$
EXOR-Gatter	Exklusiv-Oder, vollständige Adjunktion, vollständige Disjunktion „entweder, oder“	$A \dot{\vee} B$, $A \bigtriangleup B$, $A \oplus B$, $A \nleftrightarrow B$, $A \nLeftrightarrow B$, $A \curlyvee B$
EXNOR-Gatter	NEXOR-Gatter, Exklusiv-NOR, (Materiale) Äquivalenz, „genau dann, wenn“	$A \equiv B$, $A \leftrightarrow B$, $A \Leftrightarrow B$, $A \curlywedge B$, $A \sim B$

β) Es sei

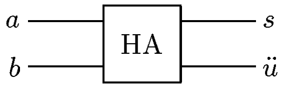
$\mathbb{B}$[1] $\rightleftharpoons \{0,1\}$; (mit $0 \neq 1$)

γ) Eine **Schaltung** ist eine Kombination von $k(\in \mathbb{N})$ Schaltelementen so, daß die Ausgänge gewisser Schaltelemente Eingänge anderer Schaltelemente sind und sich bei $n(\in \mathbb{N}_0)$ Eingängen $m(\in \mathbb{N})$ Ausgänge ergeben.



Beispiel 2 (Halbaddierer)
Ein Halbaddierer ist eine Schaltung gemäß Definition 1γ), die die Summe s mit Übertrag $\ddot{u}$ einstelliger Dualzahlen a und b liefert:

[1] $\mathbb{B}$ wie „binär“ oder nach George Boole



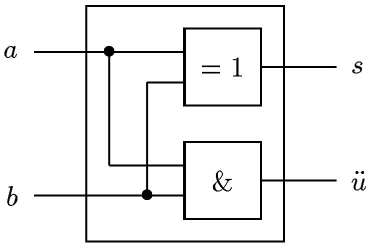
Eine Tabelle dazu lautet:

a	b	$ü$	s	$a \vee b$	$\overline{ü}$
0	0	0	0	0	1
0	1	0	1	1	1
1	0	0	1	1	1
1	1	1	0	1	0

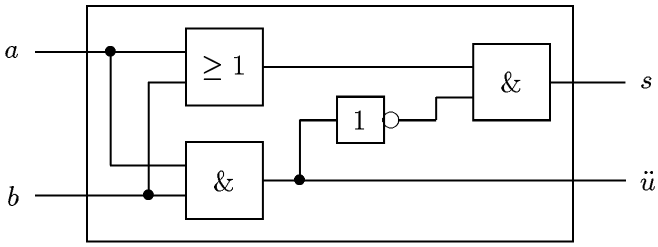
Aus dieser Tabelle folgt:

$$
\begin{aligned}
ü &= a \wedge b \\
s &= a \oplus b = (a \vee b) \wedge \overline{a \wedge b},
\end{aligned}
$$

also



oder



Satz 1
Für $x, y, z \in \mathbb{B}$ gelten:

$x \wedge y = y \wedge x$ $x \vee y = y \vee x$	(Kommutativität)	(1)
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$ $(x \vee y) \vee z = x \vee (y \vee z)$	(Assoziativität)	(2)
$x \wedge x = x$ $x \vee x = x$	(Idempotenz)	(3)
$x \wedge (x \vee y) = x$ $x \vee (x \wedge y) = x$	(Distributivität)	(4)
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	(Absorption)	(5)
$x \wedge 1 = x$ $x \vee 0 = x$	(Existenz von Neutralelementen)	(6)
$x \wedge 0 = 0$ $x \vee 1 = 1$	(Existenz absorbierender Elemente)	(7)
$\overline{\overline{x}} = x$	(Existenz einer Involution)	(8)
$x \wedge \overline{x} = 0$ $x \vee \overline{x} = 1$	(Komplementiertheit, Komplementarität)	(9)

$$\begin{aligned} \overline{x \wedge y} &= \overline{x} \vee \overline{y} \\ \overline{x \vee y} &= \overline{x} \wedge \overline{y} \end{aligned} \qquad \text{(De Morgan)} \tag{10}$$

$$\begin{aligned} x \wedge y = z \wedge y;\ x \wedge \overline{y} = z \wedge \overline{y} \ &\Rightarrow\ x = z \\ x \vee y = z \vee y;\ x \vee \overline{y} = z \vee \overline{y} \ &\Rightarrow\ x = z \end{aligned} \qquad \text{(Kürzungsregeln)} \tag{11}$$

Beweis:
(1) und (3) ergeben sich unmittelbar aus den Definitionen, ebenso (6) bis (9).

(4): siehe Beispiel 1c,d); dual ($\wedge$ und $\vee$ vertauscht!) entsprechend.

(5), (10): Übung!

(11): 0-1-Tabelle!

Eine andere Beweistechnik ist das Anwenden bereits bewiesener Sätze:

$$\begin{aligned} x &\overset{(6)}{=} x \wedge 1 \overset{(9)}{=} x \wedge (y \wedge \overline{y}) \overset{(5)}{=} (x \wedge y) \vee (x \wedge \overline{y}) \overset{\text{Vor.}}{=} (z \wedge y) \vee (z \wedge \overline{y}) \\ &\overset{(5)}{=} z \wedge (y \wedge \overline{y}) \overset{(9)}{=} z \wedge 1 \\ &\overset{(6)}{=} z \end{aligned}$$

Der zweite Teil läßt sich dual beweisen.

(2) beweisen wir durch die Tabelle:

x	y	z	$x \wedge y$	$(x \wedge y) \wedge z$	$y \wedge z$	$x \wedge (y \wedge z)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	0
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	1	0	0	0
1	1	1	1	1	1	1

Die Ausdrücke $(x \wedge y) \wedge z$ und $x \wedge (y \wedge z)$ liefern für jede Binärkombination jeweils die gleichen Werte, d.h. die beiden Ausdrücke sind gleich.
Der Beweis für $(x \vee y) \vee z \ = \ x \vee (y \vee z)$ ist wieder dual möglich.
Auch in diesem Falle ist es möglich, den Satz durch bereits bewiesenes zu beweisen. Aus

$$x \vee ((x \wedge y) \wedge z) \ \overset{(5)}{=} \ (x \vee (x \wedge y)) \wedge (x \vee z) \overset{(4)}{=} x \wedge (x \vee z) \overset{(4)}{=} x \overset{(4)}{=} x \vee (x \wedge (y \wedge z))$$

und

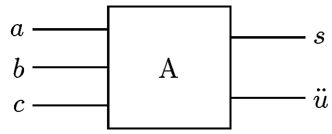
$$\begin{aligned} \overline{x} \vee ((x \wedge y) \wedge z) &\overset{(5)}{=} (\overline{x} \vee (x \wedge y)) \wedge (\overline{x} \vee z) \overset{(5)}{=} ((\overline{x} \vee x) \wedge (\overline{x} \vee y)) \wedge (\overline{x} \vee z) \\ &\overset{(6)}{=} (\overline{x} \vee y) \wedge (\overline{x} \vee z) \overset{(5)}{=} \overline{x} \vee (y \wedge z) \overset{(6)}{=} 1 \wedge (\overline{x} \vee (y \wedge z)) \\ &\overset{(1,7)}{=} (\overline{x} \vee x) \wedge (\overline{x} \vee (y \wedge z)) \\ &\overset{(5)}{=} \overline{x} \vee (x \wedge (y \wedge z)) \end{aligned}$$

ergibt sich (1) und (11) zufolge

$$(x \wedge y) \wedge z = x \wedge (y \wedge z)$$

Dual für $\vee$.

Beispiel 3 (Volladdierer)
Ein Volladdierer ist eine Schaltung, die für die Addition von drei einstelligen Dualzahlen a, b und c die Summe s mit Übertrag $\ddot{u}$ liefert. Eine solche Schaltung ist notwendig, da etwa bei der Addition zweier n-stelliger Dualzahlen mit $n > 1$ auch der Übertrag [carry] zu den beiden Summanden addiert werden muß.



Die zu entwickelnde Schaltung muß folgende Ergebnisse liefern:

			$a+b+c$		$a+b$		s_1+c	
a	b	c	$\ddot{u}$	s	$\ddot{u}$	s_1	$\ddot{u}$	s_2
0	0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0
0	1	0	0	1	0	0	0	1
0	1	1	1	0	0	1	0	1
1	0	0	0	1	0	1	0	1
1	0	1	1	0	0	1	1	0
1	1	0	1	0	1	0	0	0
1	1	1	1	1	1	0	0	1

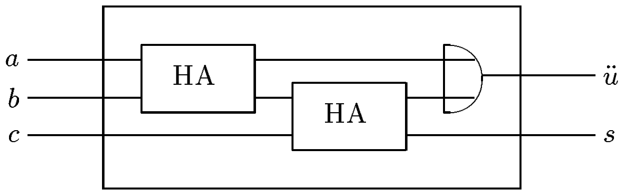
was man auch durch

$$s = s_2 = s_1 \oplus c = (a \oplus b) \oplus c$$

und

$$\ddot{u} = \ddot{u}_1 \vee \ddot{u}_2$$

ausdrücken kann.
Die Schaltung läßt sich also wie in der folgenden Abbildung aufbauen:



HA: Halbaddierer

Bemerkung 1
Wie Beispiel 1, 2, 3 und Definition 1 zeigen, lassen sich Verhaltensweisen von Schaltelementen und Schaltungen durch 0-1-Tabellen beschreiben, oder anders durch Funktionen von

$$\mathbb{B}^n \rightleftharpoons \underbrace{\mathbb{B} \cdot \mathbb{B} \cdot \ldots \cdot \mathbb{B}}_{\text{n-mal}} \qquad \text{in} \qquad \mathbb{B}^m,$$

wobei n die Anzahl der Eingänge und m die Anzahl der Ausgänge darstellt.

Definition 2
Sei $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$:

α) Eine Abbildung von $\mathbb{B}^n$ in $\mathbb{B}^m$ heißt **n-äre** oder n-stellige **Schaltfunktion** oder **Boolesche Funktion** (sie hat also m-Tupel aus Nullen und Einsen als jeweiligen Funktionswert).

Die 0-ären Schaltfunktionen sind per definitionem gerade die Konstanten aus $\mathbb{B}^m$, also m-Tupel aus Nullen und Einsen.

Die Gesamtheit der Schaltfunktionen von $\mathbb{B}^n$ in $\mathbb{B}^m$ werde mit $\mathfrak{B}_n^m$ bezeichnet und es sei speziell

$$\mathfrak{B}_n \rightleftharpoons \mathfrak{B}_n^1$$

also ist $\mathfrak{B}_n^m = \mathbb{B}^{m\mathbb{B}^n}$ und $\mathfrak{B}_n = \mathbb{B}^{\mathbb{B}^n}$

β) Für φ, ψ aus $\mathfrak{B}_n^m$ sei

$$\overline{\varphi} \rightleftharpoons (x_1, \ldots, s_n) \mapsto \overline{\varphi(x_1, \ldots, x_n)}$$

und

$$\varphi \wedge \psi \rightleftharpoons (x_1, \ldots, x_n) \mapsto \varphi(x_1, \ldots, x_n) \wedge \psi(x_1, \ldots, x_n)$$

und entsprechend für andere Verknüpfungen.

Zu φ und ψ aus $\mathfrak{B}^m$ gibt es n-äre Schaltfunktionen $\varphi_1, \ldots, \varphi_m$ und $\psi_1, \ldots, \psi_m$ aus $\mathfrak{B}_n$ mit

$$\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n))$$

und

$$\psi(x_1, \ldots, x_n) = (\psi_1(x_1, \ldots, x_n), \ldots, \psi_m(x_1, \ldots, x_n))$$

für alle $x_1, \ldots, x_n$ aus $\mathbb{B}$, und wir definieren

$$\overline{\varphi(x_1, \ldots, x_n)} \rightleftharpoons (\overline{\varphi_1(x_1, \ldots, x_n)}, \ldots, \overline{\varphi_m(x_1, \ldots, x_n)})$$

und

$$\begin{aligned}\varphi(x_1,\ldots,x_n)\wedge\psi(x_1,\ldots,x_n) \;&\rightleftharpoons\; (\varphi_1(x_1,\ldots,x_n)\wedge\\ &\wedge\psi_1(x_1,\ldots,x_n),\ldots,\varphi_m(x_1,\ldots,x_n)\wedge\\ &\wedge\psi_m(x_1,\ldots,x_n))\end{aligned}$$

bzw.

$$\begin{aligned}\varphi(x_1,\ldots,x_n)\vee\psi(x_1,\ldots,x_n) \;&\rightleftharpoons\; (\varphi_1(x_1,\ldots,x_n)\vee\\ &\vee\psi_1(x_1,\ldots,x_n),\ldots,\varphi_m(x_1,\ldots,x_n)\vee\\ &\vee\psi_m(x_1,\ldots,x_n))\end{aligned}$$

für alle $x_1,\ldots,x_n\in\mathbb{B}$

Beispiel 4

a) Für n-stellige Dualzahlen a und b, etwa $a=a_{n-1}\ldots a_0$ und $b=b_{n-1}\ldots b_0$ mit $a_\nu,b_\nu\in\mathbb{B}$ für $\nu=0,1,\ldots,n-1$, also $a=\sum_{\nu=0}^{n-1}a_\nu 2^\nu$ und $b=\sum_{\nu=0}^{n-1}b_\nu 2^\nu$, suchen wir eine Schaltung, die $c=a+b$ liefert, etwa $c=c_n\ldots c_0$ mit $c_\nu\in\mathbb{B}$ für $\nu=0,1,\ldots,n$.

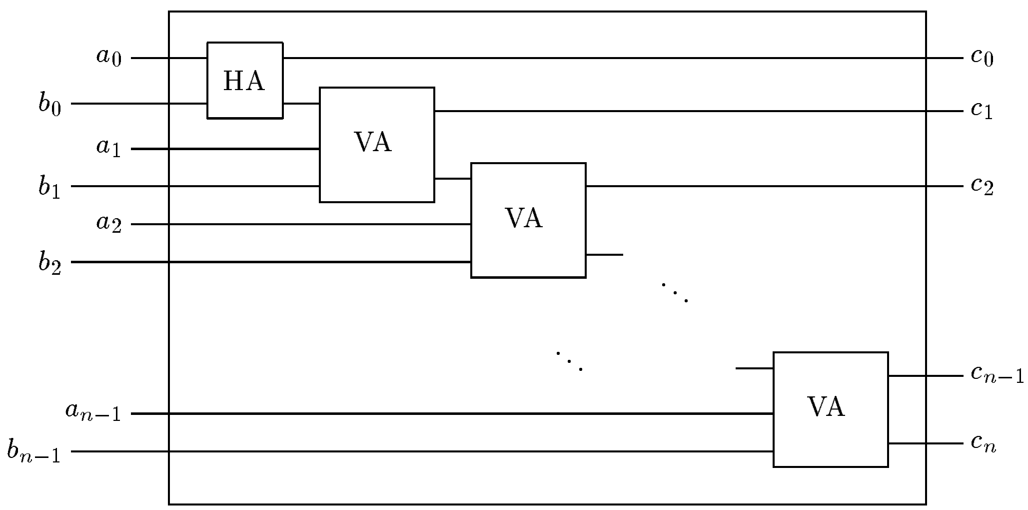
Wie beim schriftlichen Rechnen haben wir

$$\begin{aligned}\ddot{u}_1 &= \ddot{u}(a_0,b_0)\\ \ddot{u}_\nu &= \ddot{u}(a_{\nu-1},b_{\nu-1},\ddot{u}_{\nu-1}) \qquad (\nu=2,3,\cdots,n)\end{aligned}$$

und

$$\begin{aligned}c_0 &= a_0\oplus b_0\\ c_\nu &= a_\nu\oplus b_\nu\oplus\ddot{u}_\nu \qquad (\nu=1,2,\cdots,n-1)\\ c_n &= \ddot{u}_n\end{aligned}$$

Mithin die Schaltung:



Aufwand:	1 Halbaddierer, $n-1$ Addierer.
Vorteil:	Übersichtlichkeit, modulares Prinzip.
Nachteil:	Gewisser Aufwand, aber vor allem langsam: Wenn ein Halbaddierer für eine Addition σ ns braucht und ein Addierer τ ns, so beträgt die Gesamtadditionszeit mehr als $\sigma+(n-1)\tau$ ns; da auf modernen Computern 32, 64 oder 128 bit üblich sind, ist diese Schaltung zu langsam!
Abhilfe:	Etwa vorausberechneter Übertrag (carry look ahead, siehe 40).

b) Problem von a) für n=2: Es seien $s_0 \in \mathfrak{B}_2,\ s_1, s_2 \in \mathfrak{B}_4$ und $s \in \mathfrak{B}_4^3$ mit

$$\begin{aligned}
s_0(a_0,b_0) &\rightleftharpoons c_0,\\
s_1(a_0,b_0,a_1,a_2) &\rightleftharpoons c_1,\\
s_2(a_0,b_0,a_1,a_2) &\rightleftharpoons c_2 \quad \text{und}\\
s(a_1,a_0,b_1,b_0) &\rightleftharpoons (c_2,c_1,c_0)
\end{aligned}$$

für $a_\nu, b_\nu, c_\nu \in \mathbb{B}$ und $\nu = 0,1$ sowie $\mu = 0,1,2$.

Explizit etwa:

$$\begin{aligned}
s_0(a_0,b_0) &= a_0 \oplus x_0 \overset{\text{B2}}{=} (a_0 \vee b_0) \wedge \overline{a_0 \wedge b_0} \overset{(10)}{=} (a_0 \vee b_0) \wedge (\overline{a_0} \vee \overline{b_0})\\
s_1(a_0,b_0,a_1,b_1) &= (a_1 \oplus b_1) \oplus \ddot{u}_1 = ((a_1 \oplus b_1) \vee \ddot{u}_1) \wedge (\overline{a_1 \oplus b_1} \vee \overline{\ddot{u}_1}),
\end{aligned}$$

dazu zunächst

$$\begin{aligned}
\overline{a_1 \oplus b_1} &= \overline{(a_1 \vee b_1) \wedge (\overline{a_1} \vee \overline{b_1})} = (\overline{a_1 \vee b_1}) \vee (\overline{\overline{a_1} \vee \overline{b_1}}) = (\overline{a_1} \wedge \overline{b_1}) \vee (\overline{\overline{a_1}} \wedge \overline{\overline{b_1}})\\
&= (\overline{a_1} \vee a_1) \wedge (\overline{a_1} \vee b_1) \wedge (a_1 \vee \overline{b_1}) \wedge (\overline{b_1} \vee b_1),
\end{aligned}$$

also

$$\begin{aligned}
s_1(a_0,b_0,a_1,b_1) &= (((a_1 \vee b_1) \wedge (\overline{a_1} \vee \overline{b_1})) \vee \ddot{u}_1) \wedge (((\overline{a_1} \vee b_1) \wedge (a_1 \vee \overline{b_1})) \vee \overline{\ddot{u}_1})\\
&= (a_1 \vee b_1 \vee \ddot{u}_1) \wedge (\overline{a_1} \vee \overline{b_1} \vee \ddot{u}_1) \wedge (\overline{a_1} \vee b_1 \vee \overline{\ddot{u}_1}) \wedge (a_1 \vee \overline{b_1} \vee \overline{\ddot{u}_1})\\
&= (a_0 \vee a_1 \vee b_1) \wedge (a_1 \vee b_0 \vee b_1) \wedge (a_0 \vee \overline{a_1} \vee \overline{b_1}) \wedge (\overline{a_1} \vee \overline{b_1} \vee b_0) \wedge\\
&\quad \wedge (\overline{a_0} \vee \overline{a_1} \vee \overline{b_0} \vee b_1) \wedge (\overline{\overline{a_0}} \vee a_1 \vee \overline{\overline{b_0}} \vee \overline{b_1})
\end{aligned}$$

und

$$\begin{aligned}
s_2 &= (a_0,b_0,a_1,b_1) = \ddot{u}(a_1,b_1,\ddot{u}_1) = (a_1 \wedge b_1) \vee ((a_1 \oplus b_1) \vee ((a_1 \oplus b_1) \wedge \ddot{u}_1)\\
&= (a_1 \vee ((a_1 \vee b_1) \wedge (\overline{a_1} \vee \overline{b_1}))) \wedge (a_1 \vee \ddot{u}_1) \wedge (b_1 \vee ((a_1 \vee b_1) \wedge (\overline{a_1} \vee \overline{b_1}))) \wedge (b_1 \vee \ddot{u}_1)\\
&= (a_1 \vee b_1) \wedge (a_1 \vee \overline{a_1} \vee \overline{b_1}) \wedge (a_1 \vee \ddot{u}_1) \wedge (a_1 \vee b_1) \wedge (b_1 \vee \ddot{u}_1)\\
&= (a_1 \vee b_1) \wedge (a_1 \vee \ddot{u}_1) \wedge (a_1 \vee b_1) \wedge (b_1 \vee \ddot{u}_1) = (a_1 \vee b_1) \wedge (a_1 \vee \ddot{u}_1) \wedge (b_1 \vee \ddot{u}_1)\\
&= (a_1 \vee b_1) \wedge (a_0 \vee a_1) \wedge (a_1 \vee b_0) \wedge (a_0 \vee b_1) \wedge (b_0 \vee b_1),
\end{aligned}$$

was insgesamt eine „schnellere“ Schaltung als a) liefert.

Definition 3

α) V sei eine abzählbar unendliche Menge von Variablen mit $V \cap \mathbb{B} = \emptyset$, wobei **Variablen** bedeutungsleere Zeichen, meist Buchstaben oder indizierte Buchstaben seien, die die Stellen kennzeichnen, die mit (Namen von) Dingen besetzt werden können. Gleiche Zeichen verdeutlichen gleiche Dinge. Variablen sind also Platzhalter.

I. $0, 1$ und jedes x aus V ist ein Term.

II. Sind α und β Terme, so auch
$\neg(\alpha)$ oder $\overline{\alpha}$,
$(\alpha \wedge \beta)$,
$(\alpha \vee \beta)$,
$(\alpha \Rightarrow \beta)$ sowie
$(\alpha \leftrightarrow \beta)$. ($x \leftrightarrow y$ ist eine Abkürzung für $\overline{x} \vee y$)

Genau die nach I und II bildbaren Schreibfiguren heißen **(Boolesche) Terme**, **(Boolesche) Ausdrücke**, oder **Formeln**. In Termen kann man Klammern nach dem üblichen Klammersparungsregeln einsparen. So etwa bindet der Operator $\neg$ stärker als die Operatoren $\wedge$ und $\vee$, diese wiederum stärker als $\Rightarrow$, welches wiederum stärker als $\leftrightarrow$ bindet.

Die anderen in Definition 11α) eingeführten Verknüpfungszeichen sind jeweils als Abkürzungen zu verstehen.

β) Jedem Booleschen Ausdruck α ist in natürlicher Weise eine Schaltfunktion φ_α zugeordnet.

Sind $x_1, \ldots, x_n$ die in α vorkommenden Variablen, so ist

$$\varphi_\alpha : \ (x_1, \ldots, x_n) \longmapsto \alpha$$

wobei $\varphi_\alpha(x_1, \ldots, x_n)$ für $(x_1, \ldots, x_n) \in \mathbb{B}^n$ sukzessiv nach Definition 1α) bestimmt wird.

Für Boolesche Ausdrücke α, β schreiben wir „par abus de language“ (durch Sprachmißbrauch), wie üblich, auch $\alpha = \beta$ im Falle $\varphi_\alpha = \varphi_\beta$. Ob diese Gleichheit oder Gleichheit zwischen Termen im engeren Sinne gemeint ist, geht jeweils aus dem Zusammenhang hervor. So sind zum Beispiel die beiden Terme $x \vee y$ und $(x \vee y) \wedge (x \vee \overline{x})$ trotz ihrer gleichen Wirkung im engeren Sinne betrachtet ungleich.

Bemerkung 2
Schön wäre es, wenn auch umgekehrt jeder Schaltfunktion ein Boolescher Ausdruck entspräche. Dies ist nicht selbstverständlich. Über $\mathbb{R}$ etwa gibt es weitaus mehr reelle Funktionen als etwa arithmetische Ausdrücke!

Satz 2
Zu jeder Schaltfunktion φ auf $\mathfrak{B}_n$ gibt es einen Booleschen Ausdruck α mit $\varphi = \varphi_\alpha$ und zwar etwa

$$\begin{aligned} \alpha \quad = \quad & (x_1 \wedge x_2 \wedge \cdots \wedge x_n \wedge \varphi(1, 1, \cdots, 1)) \vee \\ & \vee (\overline{x_1} \wedge x_2 \wedge \cdots \wedge x_n \wedge \varphi(0, 1, \cdots, 1)) \vee \end{aligned}$$

$$\begin{aligned}
&\vee (x_1 \wedge \overline{x_2} \wedge \cdots \wedge x_n \wedge \varphi(1,0,\cdots,1)) \vee \\
&\qquad\qquad\vdots \\
&\vee (x_1 \wedge x_2 \wedge \cdots \wedge \overline{x_n} \wedge \varphi(1,1,\cdots,0)) \vee \\
&\vee (\overline{x_1} \wedge \overline{x_2} \wedge \cdots \wedge x_n \wedge \varphi(0,0,\cdots,1)) \vee \\
&\qquad\qquad\vdots \\
&\vee (x_1 \wedge x_2 \wedge \cdots \wedge \overline{x_{n-1}} \wedge \overline{x_n} \wedge \varphi(1,1,\cdots,0,0)) \vee \\
&\qquad\qquad\vdots \\
&\vee (x_1 \wedge \overline{x_2} \wedge \cdots \wedge \overline{x_n} \wedge \varphi(1,0,\cdots,0)) \vee \\
&\vee (\overline{x_1} \wedge \overline{x_2} \wedge \cdots \wedge \overline{x_n} \wedge \varphi(0,0,\cdots,0)) \\
= &\bigvee_{(y_1,\cdots,y_n)\in\mathbb{B}^n} \Big(\bigwedge_{\nu=1}^{n} (x_\nu \leftrightarrow y_\nu) \wedge \varphi(y_1,\cdots,y_n)\Big)
\end{aligned}$$

wobei

$$(x_\nu \leftrightarrow y_\nu) = (x_\nu \wedge y_\nu) \vee (\overline{x_\nu} \wedge \overline{y_\nu})$$

ist.
Für $y_\nu = 0$ gilt also

$$(x_\nu \wedge 0) \vee (\overline{x_\nu} \wedge \overline{0}) = 0 \vee (\overline{x_\nu} \wedge 1) = 0 \vee \overline{x_\nu} = \overline{x_\nu}$$

und für $y_\nu = 1$ ist

$$(x_\nu \wedge 1) \vee (\overline{x_\nu} \wedge \overline{1}) = x_\nu \vee 0 = x_\nu$$

Beweis:
Mit D_φ als dem Definitionsbereich von φ hat man

$$D_\varphi = \mathbb{B}^n = D_{\varphi_\alpha} \qquad (\varphi \in \mathfrak{B}_n)$$

und für $(z_1,\cdots,z_n) \in \mathbb{B}^n$ wegen $(z_1,\cdots,z_n) \neq (y_1,\cdots,y_n)$

$$\bigwedge_{\nu=1}^{n} (z_\nu \leftrightarrow y_\nu) = 0,$$

ferner nach Definition $3\beta)$

$$\varphi_\alpha(z_1,\ldots,z_n) = \bigvee_{(y_1,\ldots,y_n)\in\mathbb{B}} \Big(\bigwedge_{\nu=1}^{n} (z_\nu \leftrightarrow y_\nu) \wedge \varphi(y_1,\cdots,y_n)\Big) = \varphi(z_1,\cdots,z_n),$$

was $\varphi = \varphi_\alpha$ beweist.

Bemerkung 3
Der Beweis von Satz 2 liefert zugleich ein konstruktives Verfahren, einen Algorithmus zur Bildung eines Booleschen Ausdrucks.

Beispiel 5
Die Bildung eines Booleschen Ausdrucks zeigen wir am Beispiel des Volladdierers, den wir bereits im Beispiel 3 vorgestellt haben.

a	b	c	s_1	s_0
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

Der Boolesche Ausdruck α von s_1 bildet sich wie folgt:

$$\begin{aligned}\alpha &= (a \wedge b \wedge c \wedge 1) \vee (\overline{a} \wedge b \wedge c \wedge 1) \vee (a \wedge \overline{b} \wedge c \wedge 1) \vee (a \wedge b \wedge \overline{c} \wedge 1) \vee \\ &\quad \vee (\overline{a} \wedge \overline{b} \wedge c \wedge 0) \vee (\overline{a} \wedge b \wedge \overline{c} \wedge 0) \vee (a \wedge \overline{b} \wedge \overline{c} \wedge 0) \vee (\overline{a} \wedge \overline{b} \wedge \overline{c} \wedge 0) \\ &= (a \wedge b \wedge c) \vee (\overline{a} \wedge b \wedge c) \vee (a \wedge \overline{b} \wedge c) \vee (a \wedge b \wedge \overline{c})\end{aligned}$$

Der Einzelvergleich mit der Tabelle zeigt die Richtigkeit des so ermittelten Booleschen Ausdrucks. Jetzt formen wir α weiter zu einer „Konjunktion von Adjunktionen“ um:

$$\begin{aligned}\alpha &= ((a \vee \overline{a}) \wedge (a \wedge c)) \vee (a \wedge ((\overline{b} \wedge c) \vee (b \wedge \overline{c}))) \\ &= (b \wedge c) \vee (a \wedge ((\overline{b} \vee b) \wedge (\overline{b} \vee \overline{c}) \wedge (c \vee b) \wedge (c \vee \overline{c}))) \\ &= (b \wedge c) \vee (a \wedge (\overline{b} \vee \overline{c}) \wedge (b \vee c)) \\ &= (b \vee a) \wedge (b \vee \overline{b} \vee \overline{c}) \wedge (b \vee b \vee c) \wedge (c \vee a) \wedge (c \vee \overline{c} \vee \overline{b}) \vee (c \vee b) \\ &= (a \vee b) \wedge (b \vee c) \wedge (c \vee a),\end{aligned}$$

was wiederum durch die Tabelle bestätigt wird.

Korollar A zu Satz 2:
Zu jeder Schaltfunktion φ aus $\mathfrak{B}_n$ gibt es einen Booleschen Ausdruck α mit $\varphi = \varphi_\alpha$, und zwar

$$\alpha = \bigvee_{\substack{(y_1,\cdots,y_n)\in\mathbb{B}^n \\ \varphi(y_1,\cdots,y_n)=1}} \bigwedge_{\nu=1}^{n} x_\nu \leftrightarrow y_\nu$$

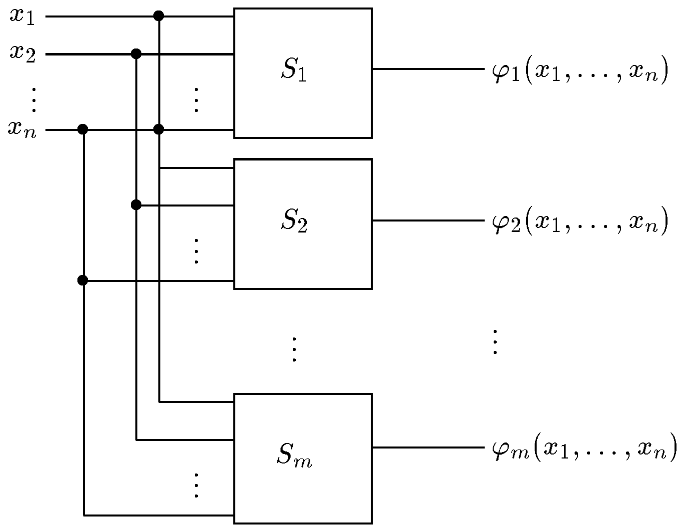
Beweis: folgt unmittelbar aus Satz 2.

Korollar B zu Satz 2:
Jede Schaltfunktion aus $\mathfrak{B}_n^m$ mit $m \in \mathbb{N}$ und $n \in \mathbb{N}_0$ ist durch eine Schaltung realisierbar.

Beweis:
Zu $\varphi \in \mathfrak{B}_n^m$ gibt es $\varphi_1, \varphi_2, \ldots, \varphi_m \in \mathfrak{B}_n$ mit

$$\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \varphi_2(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n))$$

für alle $x_1, \ldots, x_n \in \mathbb{B}$. Zu jedem φ_μ existiert nach Korollar A zu Satz 2 ein Boolescher Ausdruck α_μ mit $\varphi_\mu = \varphi_{\alpha_\mu}$, der unmittelbar in einer Schaltung s_μ – Odergatter von Undgattern mit evtl. vorgeschalteten Invertern! – verwirklicht werden kann für $\mu = 1, \ldots, m$.
Also:



Definition 4

α) I. Jede Variable sowie 0 und 1 heißt ein **Literal**.

II. Wenn λ ein Literal wie unter I. ist, so ist auch $\neg\lambda$ oder $\overline{\lambda}$ ein Literal.

Genau die gemäß I. und II. bildbaren Terme sind Literale.

β) Ein Boolescher Ausdruck α heißt in **konjunktiver** bzw. **adjunktiver Normalform**, falls α eine Konjunktion von Adjunktionen, bzw. eine Adjunktion von Konjunktionen von Literalen ist.

γ) $\mathfrak{V}\in \bigcup_{\nu=0}^{n} \mathfrak{B}_\nu$ heißt **funktional vollständig** oder eine **Basis** für $\mathfrak{B}_n$, falls sich jede Funktion aus $\mathfrak{B}_n$ durch Hintereinanderausführung von Funktionen aus $\mathfrak{V}$ darstellen läßt.

Korollar C zu Satz 2:
Zu jedem Booleschen Ausdruck α gibt es einen Booleschen Ausdruck β in konjunktiver Normalform und einen Booleschen Ausdruck γ in adjunktiver Normalform mit

$$\varphi_\beta = \varphi_\alpha = \varphi_\gamma$$

Beweis:
Die Existenz von γ mit $\varphi_\alpha = \varphi_\gamma$ folgt sofort aus Satz 2 bzw. dem Korollar A zu Satz 2. Durch „Ausmultiplizieren" gemäß (5) kann γ stets in die konjunktive Normalform gebracht werden. (vgl. Beispiel 5, letzter Teil). Der formale Beweis kann etwa durch Induktion nach dem Formelaufbau geleistet werden.

Bemerkung 4
Die konjunktive und adjunktive Normalform sind natürlich nicht eindeutig bestimmt, wie z.B. $x \wedge y = (x \wedge y) \vee (x \wedge y \wedge z)$ zeigt.

Satz 3
Für $\mathfrak{B}_n$ mit $n \in \mathbb{N}_0$ sind funktional vollständig:

a) $\{\neg, \wedge, \vee\}$

b) $\{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \to\}$

c) $\{|\}, \{\downarrow\}$

Beweis:
Seien $x, y \in \mathbb{B}$. Wir beschränken uns auf $n = 2$ (Verallgemeinerung leicht).

a) Sofort aus Satz 2 bzw. Korollar A zu Satz 2.

b) Wegen $x \vee y = \overline{\overline{x} \wedge \overline{x}}$ und a) ist $\{\neg, \wedge\}$ Basis von $\mathfrak{B}_2$.
Für $\{\neg, \vee\}$ – dual.
Wegen $x \vee y = \overline{\overline{x}} \vee y = \overline{x} \to y$ und vorigem ist $\{\neg, \to\}$ funktional vollständig.

c) Wegen

$$\overline{x} = \overline{x} \vee \overline{x} = \overline{x \wedge x} = x|x$$

und

$$x \vee y = \overline{\overline{x}} \vee \overline{\overline{y}} = \overline{\overline{x} \wedge \overline{y}} = \overline{x}|\overline{y} \quad (= (x|x)|(y|y))$$

sowie b) ist $\{|\}$ Basis von $\mathfrak{B}_2$.
Für $\{\downarrow\}$ dual.

1.2 Verbände

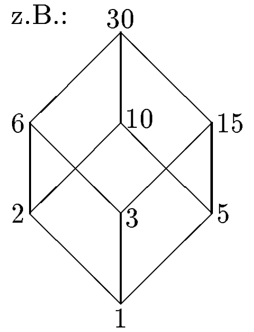
Definition 5 (Verband)
$(V, \wedge, \vee)$ heißt **Verband** (engl. lattice, franz. treillis), wenn $(V, \wedge)$ und $(V, \vee)$ kommutative Halbgruppen sind und das Absorbtionsgesetz $x \wedge (x \vee y) = x$ bzw. $x \vee (x \wedge y) = x$ für alle $x, y \in V$ gilt.

Beispiel 6
Verbände sind

a) $(\mathbb{B}, \wedge, \vee)$, allgemeiner: $(\mathfrak{B}_n^m, \wedge, \vee)$

b) $(P(M), \cap, \cup)$ für eine beliebige Menge M; Potenzmengenverband von M

c) $(T(n), \mathrm{ggT}, \mathrm{kgV})$ mit $T(n) \rightleftharpoons \{x \in \mathbb{N} \mid x|n\}$; Teilerverband von n
für $n = 30$ z.B.:

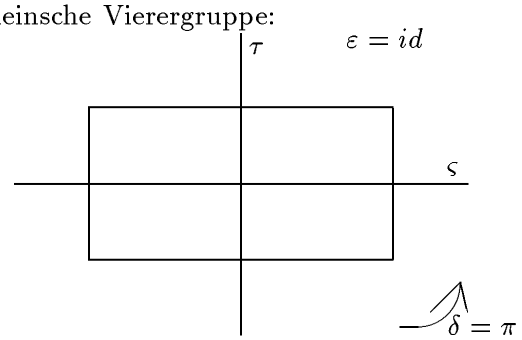


d) $(U(G), \cap, \cup)$ mit
$U(G) \rightleftharpoons \{H \mid (H, \cdot) \subseteq (G, \cdot)\}$; Untergruppenverband von G
Beispiele:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

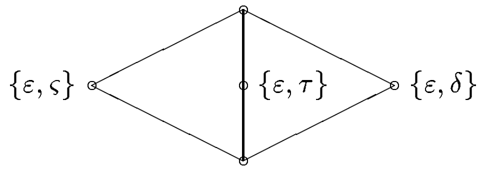
$+_2$	0	1
0	0	1
1	1	0

Kleinsche Vierergruppe:



$\circ$	ε	ς	τ	δ
ε	ε	ς	τ	δ
ς	ς	ε	δ	τ
τ	τ	δ	ε	ς
δ	δ	τ	ς	ε

für $\mathcal{V} = (V, \circ) = \{\varepsilon, \varsigma, \tau, \delta\}$ und z.B.
$\mathcal{U}(\mathcal{V}) = \Big(\Big\{\{\varepsilon\}, \{\varepsilon, \varsigma\}, \{\varepsilon, \tau\}, \{\varepsilon, \delta\}\Big\}, \vee\Big)$:



e) $(\mathbb{N}, \min, \max)$
mit $\min : (x, y) \mapsto \min\{x, y\}$ und $\max : (x, y) \mapsto \max\{x, y\}$

Satz 4
$(V, \wedge, \vee)$ ist genau dann ein Verband, wenn $(V, \wedge)$ und $(V, \vee)$ kommutative idempotente Halbgruppen mit

$$x \wedge y = x \Longleftrightarrow x \vee y = y \tag{12}$$

für alle $x, y \in V$ sind.

Beweis:
Sei $\mathcal{V} \rightleftharpoons (V, \wedge, \vee)$.

a) $\mathcal{V}$ ist ein Verband: Dann folgt die Idempotenz für alle $x \in V$ (siehe kleine Übungen) und mit $x \wedge y = x$ hat man

$$x \vee y = (x \wedge y) \vee y = y \vee (y \wedge x) = y$$

und umgekehrt mit $x \vee y = y$ auch

$$x \wedge y = x \wedge (x \vee y) = x,$$

also (12).

b) Für $\mathcal{V}$ gelte die im Satz genannte Bedingung. Z.z.: Idempotenz
Mit $x \vee y = (x \vee x) \vee y = x \vee (x \vee y)$ ergibt sich (12) zufolge

$$x \wedge (x \vee y) = x$$

und mit $x \wedge y = (x \wedge x) \wedge y = x \wedge (x \wedge y) = (x \wedge y) \wedge x$ auch

$$x \vee (x \wedge y) = (x \wedge y) \vee x = x.$$

Bemerkung 5
Wie die Beispiele aus Beispiel 6 zeigen, scheint ein Verband etwas mit (partiellen) Ordnungen zu tun zu haben. Genauer: „transitiv“ = „identitiv“

Satz 5
$V \neq \emptyset$

a) Ist $(V, \wedge, \vee)$ ein Verband, so ist $\leq$ mit
$x \leq y \rightleftharpoons x \wedge y = x \quad x, y \in V$
eine Ordnung auf V derart, daß $\inf\{x, y\}$ und $\sup\{x, y\}$ für alle $x, y \in V$ existieren.

b) Ist umgekehrt $\leq$ eine (partielle) Ordnung der unter a) genannten Art auf V, so ist $(V, \wedge, \vee)$ mit
$x \wedge y \rightleftharpoons \inf\{x, y\}$ und $x \vee y \rightleftharpoons \sup\{x, y\} \quad x, y \in V$
ein Verband.

c) Führt man die in a) und b) definierten Konstruktionen nacheinander aus, gelangt man jeweils zur Ausgangsgröße zurück.

Beweis:

a) I. Aus der Idempotenz für alle $x \in V$ folgt $x \leq x$, also ist $\leq$ reflexiv.
II. Mit $x \leq y$ (also $x \wedge y = x$) und $y \leq x$ (also $y \wedge x = y$) gilt $x = x \wedge y = y \wedge x = y$, also ist $\leq$ antisymmetrisch.
III. Gilt $x \leq y$ und $y \leq z$, so gilt $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x$, also ist $\leq$ transitiv.

Mithin ist $\leq$ eine Ordnung auf V

Wegen $x = x \wedge (x \vee y)$ und $y = y \wedge (x \vee y)$
gilt $x \leq x \vee y$ und $y \leq x \vee y$,
also ist $x \vee y$ obere Schranke von $\{x, y\}$.
Für jede obere Schranke s von $\{x, y\}$ gilt $x \leq s$ und $y \leq s$,
und damit $(x \vee y) \vee s = x \vee y \vee s \vee s = (x \vee s) \vee (y \vee s) = s$,
also $x \vee y \leq s$; $x \vee y = \sup\{x, y\}$.
Für $\inf\{x, y\}$ entsprechend.

Mithin existieren für alle $x, y \in V$ $\sup\{x, y\}$ und $\inf\{x, y\}$.

b) Übung.

c) Übung.

Beispiel 7
Für $\leq$ gemäß Satz 5a) und Beispiel 6 ergibt sich

a) $\leq$: $0 \leq 1$ — Für $\varphi, \psi \in \mathfrak{B}_n$ entsprechend
$\varphi \leq \psi \iff \varphi(x_1, \ldots, x_n) \leq \psi(x_1, \ldots, x_n)$ für alle $x_1, \ldots, x_n \in \mathbb{B}$
und für $\varphi, \psi \in \mathfrak{B}_n^m$:
$\varphi(x_1, \ldots, x_n) = (\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_m(x_1, \ldots, x_n))$
$\psi(x_1, \ldots, x_n) = (\psi_1(x_1, \ldots, x_n), \ldots, \psi_m(x_1, \ldots, x_n))$
mit $x_1, \ldots, x_n \in \mathbb{B}$ und $\varphi_i, \psi_i \in \mathfrak{B}_n$ für $i = 1, \ldots, m$
schließlich $\varphi \leq \psi \iff \bigwedge_{i=1}^{m} \varphi_i \leq \psi_i$

b) $\subseteq$

c) $|$ („teilt“)

d) $\leq$ im Sinne von $H \leq K \iff (H, \cdot)$ Untergruppe von $(K, \cdot)$

e) $\leq$ im üblichen Sinne

Definition 6 (Nachbar, Hasse-Diagramm, vergleichbar, Kette)

α) Ein Verband $(V, \sqcap, \sqcup)$ bestimmt nach Satz 5 eindeutig eine geordnete Menge $P = (V, \leq)$ und umgekehrt.
Daher wird auch P als Verband bezeichnet.

β) $(M, \leq)$ sei eine (partiell) geordnete Menge, $x, y, z \in M$ und wie üblich sei mit $x < y \rightleftharpoons x \leq y, x \neq y$.
x heißt **unterer Nachbar** von y genau dann, wenn $x \leq y$ und es kein $z \in M$ gibt mit $x < z < y$.
y heißt dann **oberer Nachbar** von x und x, y heißen **Nachbarn**.

γ) Endliche (nicht zu große) Verbände $(V, \leq)$ lassen sich graphisch dadurch darstellen, daß jedem $x \in V$ ein Punkt P_x der (euklidischen) Ebene bijektiv so zugeordnet wird, daß gilt:

- wenn $x \leq y$, dann liegt P_x unterhalb P_y,
- wenn x und y Nachbarn sind, werden P_x und P_y durch eine Strecke verbunden.

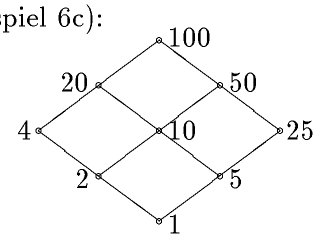
Eine solche Darstellung heißt **Ordnungs-** oder **Hasse-Diagramm**.

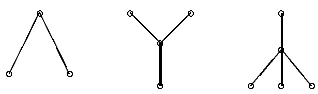
δ) $\mathcal{M} = (M, \leq)$ sei eine geordnete Menge und $x, y \in M$.
x heißt **vergleichbar** mit y, wenn $x \leq y$ oder $y \leq x$.
$\mathcal{M}$ heißt **linear** oder **total geordnet** oder **Kette**, wenn alle $x, y \in M$ vergleichbar sind.

Beispiel 8

a) Hasse-Diagramme wurden schon in den Beispielen 6c),d) und e) benutzt.

b) $T(100)$ gemäß Beispiel 6c):



c) Die durch  gekennzeichneten Ordnungen sind keine Verbände.

Satz 6
$(M, \leq)$ mit der Ordnung $\leq$ ist genau dann eine Kette, wenn entweder $x < y$ oder $x = y$ oder $y < x$ für alle $x, y \in M$ gilt.

Beweis: Übung.

Satz 7
Jede nichtleere Kette ist ein Verband.

Beweis:
$\mathcal{K} = (K, \leq)$ sei eine Kette mit $K \neq \emptyset$ und $x, y \in K$.
Dann ist

$$x \leq y \quad ; \quad \inf\{x,y\} = x \quad ; \quad \sup\{x,y\} = y$$

oder

$$y \leq x \quad ; \quad \inf\{x,y\} = y \quad ; \quad \sup\{x,y\} = x.$$

Daher ist mit Definition 6a) und Satz 5b) $\mathcal{K}$ ein Verband.

Definition 7 (Isomorphie)
Die Verbände $\mathcal{U} = (U, \wedge, \vee)$ und $\mathcal{V} = (V, \sqcap, \sqcup)$ heißen **isomorph** ($\mathcal{U} \simeq \mathcal{V}$), wenn es einen Isomorphismus

$$\varphi : \mathcal{U} \overset{\simeq}{\rightarrowtail\!\!\!\twoheadrightarrow} \mathcal{V},$$

d. h. eine Bijektion von $\mathcal{U}$ auf $\mathcal{V}$ mit

$$\varphi(x \wedge y) = \varphi(x) \sqcap \varphi(y)$$

und

$$\varphi(x \vee y) = \varphi(x) \sqcup \varphi(y)$$

für alle $x, y \in U$ gibt.

Beispiel 9

$$\Big(P(\{1,2,3\}, \cap, \cup\Big) \simeq \Big(T(30), \mathrm{ggT}, \mathrm{kgV}\Big) \simeq (\mathfrak{B}_0^3, \wedge, \vee) \qquad \text{(Nachprüfen!)}$$

Satz 8
$\simeq$ ist eine Äquivalenzrelation auf der Klasse aller Verbände.

Beweis: Übung.

Satz 9 (Dualitätsprinzip für Verbände)
Kann eine Aussage A allein aus den Verbandsaxiomen (etwa (1), (2), (4)) gefolgert werden, so auch die zu A **duale Aussage** A', d.h. diejenige Aussage, bei der in A jedes $\wedge$ durch $\vee$, jedes $\vee$ durch $\wedge$, jedes $\leq$ durch $\geq$ und jedes $\geq$ durch $\leq$ ersetzt wird.

Beweis:
(1), (2) und (4) sind selbstdual, d.h. gehen bei Vertauschung von $\wedge$ und $\vee$ in sich über. Also kann jede Herleitung von A auf A' umgeschrieben werden.

Definition 8 (1_M, distributiver Verband)

α) Für $n \in \mathbb{N}_0$ sei

$$\mathbb{A}_n \rightleftharpoons \{x \in \mathbb{N}; x \leq n\}, \text{ also } \mathbb{A}_0 = \emptyset$$

und

$$\mathbb{U}_n \rightleftharpoons \mathbb{A}_{n-1} \cup \{0\}, \text{ also } \mathbb{U}_1 = \{0\}.$$

β) Für eine Menge M sei 1_M die **identische Abbildung** von (Diagonale von , Identität auf) M, also

$$1_M \rightleftharpoons \{(x, x); x \in M\}.$$

γ) Für $n \in \mathbb{N}$ und $\alpha, \omega \notin \mathbb{A}_n$ mit $\alpha \neq \omega$ sei

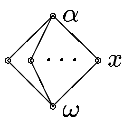
$$M_n \rightleftharpoons \mathbb{A}_n \cup \{\alpha, \omega\}$$

und

$$\preceq \rightleftharpoons 1_M \cup \{(x, \alpha); x \in \mathbb{A}_n\} \cup \{(\omega, x); x \in \mathbb{A}_n\} \cup \{(\omega, \alpha)\},$$

sowie

$\mathcal{M}_n \rightleftharpoons (M_n, \preceq)$:

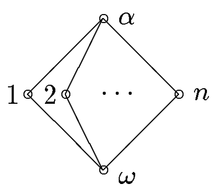


δ) Ein Verband $(V, \wedge, \vee)$ heißt **distributiv**, wenn

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z) \tag{13}$$

für alle $x, y, z \in V$ gilt.

Bemerkung 6
$\mathcal{M}_n$ aus Definition 8c) ist ein Verband:



Wie üblich bezeichnen wir auch jeden zu $\mathcal{M}_n$ isomorphen Verband als $\mathcal{M}_n$, benutzen also $\mathcal{M}_n$ als Bezeichnung für jeden Verband der gesamten Isomorphieklasse.

Satz 10
Für einen Verband $\mathcal{V} = (V, \wedge, \vee)$ sind folgende Aussagen gleichwertig:

a) $\mathcal{V}$ ist distributiv.

b) $\forall x, y, z \in V: \; x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

c) $\forall x, y, z \in V: \; x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

d) $\forall x, y, z \in V: \; x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ und $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

e) $\forall x, y, z \in V: \; x \vee (y \wedge z) \geq (x \vee y) \wedge (x \vee z)$

Beweis: Übung.

Beispiel 10

a) $(\mathbb{B}, \wedge, \vee)$, allgemeiner $(\mathfrak{B}_n^m, \wedge, \vee)$, ist distributiv.

b) $(P(M), \cap, \cup)$ ist distributiv für jede Menge M.

c) $(T(n), \mathrm{ggT}, \mathrm{kgV})$ aus Beispiel 6c) ist für jedes $n \in \mathbb{N}$ distributiv:

$$\mathrm{ggT}\Big(x, \mathrm{kgV}(y, z)\Big) \mid \mathrm{kgV}\Big(\mathrm{ggT}(x, y), \mathrm{ggT}(x, z)\Big).$$

d) $\mathcal{M}_3$ aus Beispiel 6d) ist nicht distributiv, denn
$1 \wedge (2 \vee 3) = 1 \wedge \alpha = 1, \quad (1 \wedge 2) \vee (2 \wedge 3) = \omega \vee \omega = \omega.$

Satz 11 (Dualitätsprinzip für distributive Verbände)
Kann eine Aussage A allein aus den Verbandsaxiomen und (5) gefolgert werden, so auch die zu A duale Aussage. (vgl. Satz 9 S.23)

Beweis: Übung.

Definition 9 (Null, Eins, Komplement)
$\mathcal{V} = (V, \wedge, \vee)$ sei ein Verband und $x \in V$.

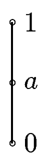
α) $\inf V$ — sofern existent — heißt **Nullelement** von $\mathcal{V}$, kurz 0.
$\sup V$ — sofern existent — heißt **Einselement** von $\mathcal{V}$, kurz 1.

β) Ein $y \in V$ mit $x \wedge y = 0$ und $x \vee y = 1$ heißt **Komplement** von x, falls $\mathcal{V}$ 0 und 1 hat.

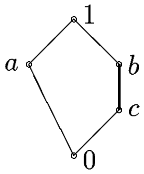
γ) Besitzt $\mathcal{V}$ 0 und 1 und jedes Element aus V mindestens ein Komplement, heißt $\mathcal{V}$ **komplementiert** oder **komplementär**.

Beispiel 11

a) $(\mathbb{N}, \leq)$, nach Satz 7 S.22 ein Verband, hat zwar eine Null, nämlich 1, aber keine Eins.

b) In 

hat a kein Komplement.

c) In 

hat a sowohl c als auch b als Komplement.

Satz 12
Null und Eins existieren in

a) jedem endlichen Verband,

b) $(P(M), \cap, \cup)$ für jede Menge M, und zwar mit $\emptyset$ als Null und M als Eins,

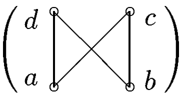
c) $(\mathfrak{B}_n^m, \wedge, \vee)$.

Beweis:

a) $\mathcal{V} = (V, \leq)$ sei ein Verband. Mit $x, y \in V$ existiert $\inf\{x,y\}$ und $\sup\{x,y\}$ und damit auch $\inf E$ und $\sup E$ für jedes endliche $E \subseteq V$. Ist V also endlich, folgt mit $E \rightleftharpoons V$ die Behauptung.

b) Bezüglich $\subseteq$ gilt $\inf P(M) = \emptyset$ und $\sup P(M) = M$

c) Übung.

Bemerkung 7
$c = a \vee b = d$ (

) kann in einem Verband nicht vorkommen.

Satz 13
Für 0 und 1 in einem Verband $(V \wedge, \vee)$ gilt:

$$0 \leq x \text{ und } x \leq 1$$

$$x \wedge 0 = 0 \text{ und } x \wedge 1 = x$$

$$x \vee 0 = x \text{ und } x \vee 1 = 1$$

für jedes $x \in V$.
Je einer der Punkte genügt zur Charakterisierung von Null und Eins.

Beweis:
Es ist $0 = \inf V \leq x \leq \sup V = 1$ für jedes $x \in V$ und damit

$$\begin{array}{ll} x \wedge 0 = \inf\{x,0\} = 0 & x \wedge 1 = \inf\{x,1\} = x \\ x \vee 0 = \sup\{x,0\} = x & x \vee 1 = \sup\{x,1\} = 1. \end{array}$$

Mit $n \in V$ folgt

$$\forall x : n \leq x \Longleftrightarrow n \leq \inf V = 0 \leq n, \text{ also } n = 0,$$

$$\forall x : x \wedge n = n \Longleftrightarrow n = 0 \wedge n = n \wedge 0 = 0, \text{ also } n = 0,$$

$$\forall x : x \vee n = x \Longleftrightarrow n = n \vee 0 = 0 \vee n = 0, \text{ also } n = 0.$$

Für Eins folgt die Charakterisierung dual.

Bemerkung 8
In einem Verband $(V, \wedge, \vee)$ mit 0 und 1 ist das einzige Komplement von 0 bzw. 1 stets 1 bzw. 0:
Aus $0 \wedge 1 = 0$ und $0 \vee 1 = 1$ folgt: 1 ist Komplement von 0.
Für ein Komplement e von 0 muß gelten: $e \vee 0 = 1$, also $e = 1$.
Für 1 dual.

Satz 14 (Dualitätsprinzip für Verbände mit 0 und 1)
Kann eine Aussage nur aus den Verbandsaxiomen und (6) gefolgert werden, so auch die zu A duale Aussage, wobei zudem noch 0 durch 1 und 1 durch 0 zu ersetzen ist.

Beweis: Übung.

Satz 15
In einem distributiven Verband sind die Komplemente jeweils eindeutig bestimmt.

Beweis: Übung.

Definition 10 (Boolescher Verband, Boolesche Algebra)
$\mathcal{V} = (V, \wedge, \vee)$ sei ein Verband.

α) $\mathcal{V}$ heißt **boolesch** oder **Boolescher Verband**, wenn $\mathcal{V}$ distributiv und komplementär ist.

β) $(V, \wedge, \vee, ^{-}, 1, 0)$ heißt **Boolesche Algebra**, wenn $\mathcal{V}$ ein Boolescher Verband mit 1 als Eins und 0 als Null und $^{-}$ als Komplementbildung ist.

Satz 16 (Dualitätsprinzip für Boolesche Verbände)
Kann eine Aussage A nur aus den Axiomen für einen Booleschen Verband gefolgert werden, so auch die zu A duale Aussage.

Beweis: Übung.

Beispiel 12
Boolesche Algebren sind:

a) $(\mathfrak{B}_n^m, \wedge, \vee, ^{-}, \mathbf{1}, \mathbf{0})$

b) $(P(M), \cap, \cup, ^{-}, M, \emptyset)$ für jede Menge M

c) $(E(M) \cup K(M), \cap, \cup, ^{-}, M, \emptyset)$ für jede Menge M mit $E(M)$ als der Menge der finiten (endlichen) Teilmengen von M und $K(M)$ als der Menge der kofiniten (deren Komplement endlich ist) Teilmengen:
$E(M) = \{X \subseteq M \mid |X| \in \mathbb{N}_0\}, \quad K(M) = \{\overline{X} \subseteq M \mid X \in E(M)\}, \quad \overline{X} \rightleftharpoons M \setminus X$

d) $(\mathcal{P}_n, \cap, \cup, ^{-}, \mathbb{Z}, \emptyset)$ mit $\mathcal{P}_n \rightleftharpoons \{X \subseteq \mathbb{Z} \mid (\overset{x}{\in} X + \overset{n}{\in} \mathbb{Z}) \in X\}$

e) $(V, \wedge, \vee, ^{-}, \mathbb{R}, \emptyset)$ mit V als der Menge aller endlichen Vereinigungen von Mengen aus $\{]-\infty, a[\} \cup \{[b, c[\} \cup \{[d, \infty[\}; \quad a, b, c, d \in \mathbb{R}; b < c$

Satz 17
$(V, \wedge, \vee, \overline{\ }, 1, 0)$ ist genau dann eine Boolesche Algebra, wenn für alle $x, y \in V$ gilt:

$$\begin{aligned} x \wedge y &= y \wedge x & \qquad x \vee y &= y \vee x \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) & \qquad x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \\ x \wedge 1 &= x & \qquad x \vee 0 &= 0 \\ x \wedge \overline{x} &= 0 & \qquad x \vee \overline{x} &= 1 \end{aligned}$$

Beweis: Übung.

Satz 18
Ist φ ein Isomorphismus des Booleschen Verbandes $\mathcal{A} = (A, \wedge, \vee)$ auf $\mathcal{B} = (B, \sqcap, \sqcup)$, so ist auch $\mathcal{B}$ ein Boolescher Verband. Für die zugehörigen Booleschen Algebren $\mathcal{A} = (A, \wedge, \vee, \overline{\ }, 1, 0)$ und $\mathcal{B} = (B, \sqcap, \sqcup, \tilde{\ }, \mathbf{1}, \mathbf{0})$ gilt dann:
$\varphi(\overline{x}) = \widetilde{\varphi(x)}$; $\quad \varphi(1) = \mathbf{1}$; $\quad \varphi(0) = \mathbf{0}$

Beweis:
Kommutativität, Assoziativität, Absorption und Distributivität übertragen sich durch φ von $\mathcal{A}$ auf $\mathcal{B}$, so daß auch $\mathcal{B}$ ein distributiver Verband ist.
Zu jedem $y \in B$ gibt es ein $x \in A$ mit $\varphi(x) = y$.
Damit hat man

$$y \sqcap \varphi(0) = \varphi(x) \sqcap \varphi(0) = \varphi(x \wedge 0) = \varphi(0)$$

und

$$y \sqcup \varphi(1) = \varphi(x) \sqcup \varphi(1) = \varphi(x \vee 1) = \varphi(1),$$

was $\varphi(0)$ bzw. $\varphi(1)$ nach Satz 13 als Null bzw. Eins von $\mathcal{B}$ kennzeichnet.
$\mathcal{B}$ ist also Verband mit Null ($\mathbf{0} = \varphi(0)$) und Eins ($\mathbf{1} = \varphi(1)$).
Wegen

$$y \sqcap \varphi(\overline{x}) = \varphi(x) \sqcap \varphi(\overline{x}) = \varphi(x \wedge \overline{x}) = \varphi(0) = \mathbf{0}$$

und

$$y \sqcup \varphi(\overline{x}) = \varphi(x) \sqcup \varphi(\overline{x}) = \varphi(x \vee \overline{x}) = \varphi(1) = \mathbf{1}$$

sowie Satz 15, ist

$$\varphi(\overline{x}) = \widetilde{\varphi(x)},$$

also ist $\mathcal{B}$ komplementär.
Damit ist $\mathcal{B}$ eine Boolesche Algebra.

Definition 11 (Involution, dualer Verband, duale Boolesche Algebra)

α) Eine Abbildung φ von M heißt Involution oder involutorisch, wenn $\varphi \circ \varphi = 1_M$.

β) $(V, \vee, \wedge)$ heißt dualer Verband zu $(V, \wedge, \vee)$.
$(B, \vee, \wedge, \overline{\ }, 0, 1)$ heißt duale Boolesche Algebra zu $(B, \wedge, \vee, \overline{\ }, 1, 0)$.

Satz 19
$\mathcal{A} = (A, \wedge, \vee, \overline{\ }, 1, 0)$ sei eine Boolesche Algebra.
Dann ist $x \longmapsto \overline{x}$ ein involutorischer Isomorphismus von $\mathcal{A}$ auf die zu $\mathcal{A}$ duale Boolesche Algebra, d.h. insbesondere gelten die De-Morgan-Regeln (10).

Beweis: Übung.

Definition 12 (charakteristische Funktion, Boolescher Ring)

α) G sei eine beliebige Menge und $M \subseteq G$. Die charakteristische Funktion oder Indikatorfunktion von M bzgl. G χ_M aus $\mathbb{B}^G$ ist definiert durch

$$\chi_M(x) \rightleftharpoons \begin{cases} 1 & \Leftarrow x \in M \\ 0 & \Leftarrow x \notin M \end{cases} .$$

β) Ein Ring $(R, +, \cdot)$ heißt Boolescher Ring, wenn für alle $x \in R$ $x^2 = x$ gilt.

Beispiel 13

a) $(R, +, \cdot)$ sei ein abelscher monoider Ring und $E \rightleftharpoons \{e \in R; e^2 = e\}$.
Dann ist $(E, \star, \cdot)$ mit $x \star y = x + y - 2xy$ ein monoider Boolescher Ring.

b) $\mathbb{B}$ sei das Galois-Feld $GF(2)$ mit $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ und $\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$.
M sei eine beliebige Menge und $\mathcal{B} \rightleftharpoons \mathbb{B}^M$.
Dann ist $\mathcal{B} = (B, +, \cdot)$ mit

$$\varphi + \psi \rightleftharpoons x \mapsto \varphi(x) + \psi(x)$$

und

$$\varphi \cdot \psi \rightleftharpoons x \mapsto \varphi(x) \cdot \psi(x)$$

für $\varphi, \psi \in \mathcal{B}$ ein Boolescher Ring.
In $P(M)$sei für $X, Y \subseteq M$ definiert:
$X \diamond Y \rightleftharpoons (X \setminus Y) \cup (Y \setminus X)$ und $X * Y \rightleftharpoons X \cap Y$.
Dann ist $\mathcal{P} = (P(M), \diamond, *)$ ein Boolescher Ring und man hat sogar $\chi : \mathcal{P} \overset{\simeq}{\rightarrowtail\!\!\twoheadrightarrow} \mathcal{B}$ mit $\chi(X) = \chi_X$.

Satz 20

a) Ist $(A, \wedge, \vee, \overline{\ }, 1, 0)$ eine Boolesche Algebra, so ist $(A, +, \cdot)$ mit

$$x + y \rightleftharpoons (x \wedge \overline{y}) \vee (\overline{x} \wedge y)$$

und

$$x \cdot y \rightleftharpoons x \wedge y$$

ein monoider Boolescher Ring.

b) Ist $(A, +, \cdot)$ ein monoider Boolescher Ring, so ist $(A, \wedge, \vee, \overline{}, 1, 0)$ mit

$$\wedge \rightleftharpoons \cdot,$$

$$x \vee y \rightleftharpoons x + y + xy$$

und

$$\overline{x} \rightleftharpoons 1 - x$$

sowie 0 als Null von $(A, +)$ eine Boolesche Algebra.

c) Führt man die in a) und b) genannten Konstruktionen hintereinander aus, gelangt man jeweils zum Ausgangspunkt zurück.

Beweis:

a) Seien $x, y, z \in A$.
Da $(A, \wedge) = (A, \cdot)$ idempotente Halbgruppe ist, ist mit
$1 \cdot x = 1 \wedge x = x \wedge 1 = x$ 1 als Eins nachgewiesen.
$+$ ist kommutativ.

$$\begin{array}{rrcl}
\text{Wegen} & (x+y)+z & = & \Big((x+y) \wedge \overline{z}\Big) \vee \Big(\overline{(x \wedge \overline{y}) \vee (\overline{x} \wedge y)} \wedge z\Big) \\
& & = & \Big(\Big((x \wedge \overline{y}) \vee (\overline{x} \wedge y)\Big) \wedge \overline{z}\Big) \wedge \Big((\overline{x} \vee y) \wedge (x \vee \overline{y}) \wedge z\Big) \\
& & = & (x \wedge \overline{y} \wedge \overline{z}) \vee (\overline{x} \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge \overline{y} \wedge z) \vee (x \wedge y \wedge z) \\
& & = & \Big(x \wedge ((\overline{y} \wedge \overline{z}) \vee (y \wedge z))\Big) \vee \Big(\overline{x} \wedge ((y \wedge \overline{z}) \vee (\overline{y} \wedge z))\Big) \\
& & = & \Big(x \wedge ((\overline{y} \vee z) \wedge (\overline{z} \vee y))\Big) \vee \Big(\overline{x} \wedge (y+z)\Big) \\
& & = & (x \wedge \overline{(y \wedge \overline{z}) \vee (z \wedge \overline{y})}) \vee (\overline{x} \wedge (y+z)) \\
& & = & (x \wedge \overline{y+z}) \vee (\overline{x} \wedge (y+z)) \\
& & = & x + (y+z)
\end{array}$$

$$\begin{array}{rrcl}
\text{und} & x + 0 & = & (x \wedge \overline{0}) \vee (\overline{x} \wedge 0) \\
& & = & (x \wedge 1) \vee 0 \\
& & = & x
\end{array}$$

$$\begin{array}{rrcl}
\text{und} & x + x & = & (x \wedge \overline{x}) \vee (\overline{x} \wedge x) \\
& & = & 0 \vee 0 \\
& & = & 0
\end{array}$$

ist $(A,+)$ eine abelsche Gruppe mit 0 als Null.
Da alle $x \in A$ selbstinvers sind, existieren alle Inversen.

$$
\begin{aligned}
\text{Da} \quad x \cdot (y+z) &= x \wedge \Big((y \wedge \overline{z}) \vee (\overline{y} \wedge z) \Big) \\
&= (x \wedge y \wedge \overline{z}) \vee (x \wedge \overline{y} \wedge z) \\
&= (x \wedge y \wedge \overline{x}) \vee (x \wedge y \wedge \overline{z}) \vee (\overline{x} \wedge x \wedge z) \vee (x \wedge \overline{y} \wedge z) \\
&= \Big((x \wedge y) \wedge (\overline{x} \vee \overline{z}) \Big) \vee \Big((\overline{x} \vee \overline{y}) \wedge x \wedge z \Big) \\
&= (x \cdot y \wedge \overline{x \cdot z}) \vee (\overline{x \cdot y} \wedge x \cdot z) \\
&= x \cdot y + x \cdot z
\end{aligned}
$$

ist $(A,+,\cdot)$ distributiv. Damit ist $(A,+,\cdot)$ ein monoider Boolescher Ring.

b) Übung.

c) Übung.

Korollar:
Zu jedem endlichen Booleschen Verband $(A,\wedge,\vee)$ existiert ein $k \in \mathbb{N}_0$ mit $|A| = 2^k$ und umgekehrt existiert zu jedem $k \in \mathbb{N}_0$ ein Boolescher Verband $(A,\wedge,\vee)$ mit $|A| = 2^k$.

Beweis:
Nach Satz 20 gibt es zu einem endlichen Booleschen Verband $(A,\wedge,\vee)$ einen Booleschen Ring $(A,+,\cdot)$.
Der Trivialfall $|A| = 1$ liefert $|A| = 2^0$. Sei also $|A| > 1$.
Die endliche abelsche Gruppe $\mathcal{A} = (A,+)$ ist nach dem zweiten Hauptsatz über endlich erzeugbare abelsche Gruppen isomorph einem äußeren Produkt von zyklischen Gruppen.
Jedes Element $x \in A$ hat die Ordnung 2, denn $x + x = 0$.
Also ist $\mathcal{A}$ isomorph einem äußeren Produkt $\bigotimes_{\kappa=1}^{k} \mathbb{I}_2$ mit $k \in \mathbb{N}_0$, was $|A| = 2^k$ bedingt.
Zu $k \in \mathbb{N}_0$ ist $(P(A_k),\cap,\cup)$ ein Boolescher Verband mit $|P(A_k)| = 2^k$.

Definition 13 (Mengenring, Mengenträger, Atom, atomar, vollständig)

α) M sei eine beliebige Menge und $\mathcal{R} \subseteq P(M)$.
$\mathcal{R}$ heißt
Mengenring, wenn $X, Y \in \mathcal{R} \Longrightarrow X \cap Y, X \cup Y \in \mathcal{R}$ und
Mengenträger, wenn $X, Y \in \mathcal{R} \Longrightarrow X \cap Y, \overline{X} (\rightleftharpoons M \setminus \{X\}) \in \mathcal{R}$
was wegen De-Morgan auch als $\ldots \Longrightarrow X \cup Y, \overline{X} \in \mathcal{R}$ geschrieben werden kann.

β) $\mathcal{V} = (V, \leq)$ sei ein Verband.

I. V habe eine 0: Ein oberer Nachbar von 0 heißt **Atom**, und $\mathcal{V}$ heißt **atomar** (engl. atomic), wenn es zu jedem $x \in V \setminus \{0\}$ ein Atom a mit $a \leq x$ gibt.

II. $\mathcal{V}$ heißt **vollständig**, wenn zu jeder Teilmenge $U \subseteq V$ auch $\inf U$ und $\sup U$ in V existiert.
(Vorsicht: Unterschiede zum Vollständigkeitsbegriff der Analysis!)

Beispiel 14

a) Jeder endliche Verband ist atomar und vollständig.

b) Jeder Potenzmengenverband ist bzgl. $\cap, \cup$ atomar und vollständig; die Atome sind gerade die einelementigen Mengen (engl. singletons).

c) Der Boolesche Verband $(V, \cap, \cup)$ mit $V = E(M) \cup K(M)$ aus Beispiel 12c) ist für jedes M atomar, Atome sind wiederum die „singletons", jedoch i. a. nicht vollständig.
Sei $M = \mathbb{N}$, dann ist $P \rightleftharpoons \{\{p\} \mid p \in \mathbb{P}\} \subseteq E(\mathbb{N}) \subseteq V$,
also $\sup\mathbb{P} = \bigcup\{\{p\} \mid p \in \mathbb{P}\} = \mathbb{P} \notin E(\mathbb{N}) \cup K(\mathbb{N})$, also $\sup\mathbb{P} \notin V$.

d) Es sei $\sim \rightleftharpoons \{(x,y) \in P(\mathbb{N}) \times P(\mathbb{N}) \mid |x \bigtriangleup y| \in \mathbb{N}_0\}$.
Dann ist $\sim$ eine Äquivalenzrelation (sogar Kongruenz) auf $P(\mathbb{N})$ mit

$$\forall x, y, z \in \mathbb{N}: \ (x \sim y \Longrightarrow x \cap z \sim y \cap z) \wedge (x \sim y \Longrightarrow \overline{x} \sim \overline{y}).$$

Mit $\tilde{X}$ bezeichnen wir die Klasse von X bzgl. $\sim$ und wie üblich sei

$$P(\mathbb{N})/_\sim \rightleftharpoons \{\tilde{X}; X \subseteq \mathbb{N}\}.$$

Mit $\tilde{x} \cap \tilde{y} \rightleftharpoons x \tilde{\cap} y$ und $\tilde{x} \cup \tilde{y} \rightleftharpoons x \tilde{\cup} y$ ist dann $(P(\mathbb{N})/_\sim, \cap, \cup)$ ein vollständiger, nicht atomarer Boolescher Verband.
Zum Beweis der Nichtatomarität: Die Annahme der Existenz eines Atoms führt auf $|A| \notin \mathbb{N}_0$ und damit auf die Existenz von $B, C \subseteq \mathbb{N}_0$ mit $|B|, |C| \in \mathbb{N}_0$ sowie $B \cap C = \emptyset$ und $A = B \cup C$, was $\tilde{A} > \tilde{B} > \tilde{\emptyset}$ bedingt.

e) Der Boolesche Verband $(V, \cap, \cup)$ aus Beispiel 12e) ist weder atomar noch vollständig:
Zwar gilt für alle $n \in \mathbb{N}$ $[0, 1/n[\in V$, also $D \rightleftharpoons \{[0, 1/n[\mid n \in \mathbb{N}\} \subseteq V$,
aber $\inf D = \bigcap_{n=1}^{\infty}[0, 1/n[= \{0\} \notin V$.

Satz 21
Ein Boolescher Verband ist genau dann zu einem Potenzmengenverband isomorph, wenn er atomar und vollständig ist.

Beweis:
Für die nichttriviale Richtung sei $\mathcal{B}$ ein atomarer und vollständiger Boolescher Verband und A die Menge seiner Atome. Mit der durch $\varphi(x) \rightleftharpoons \{a \in A; a \leq x\}$ definierten Abbildung hat man $\varphi : \mathcal{B} \overset{\simeq}{\rightarrowtail\!\!\twoheadrightarrow} (P(A), \cap, \cup)$ **Korollar:**
Jeder endliche Boolesche Verband ist zu einem Potenzmengenverband isomorph.

Beweis:
Nach Beispiel 14a) ist jeder endliche Boolesche Verband atomar und vollständig, also nach Satz 21 einem Potenzmengenverband isomorph.

Bemerkung 9
Wegen $|P(M)| = 2^{|M|}$ folgt das Korollar zu Satz 20 auch direkt aus dem Korollar zu Satz 21.

Satz 22 (Satz von Stone)
Jede Boolesche Algebra ist isomorph zu einem Mengenträger.

Beweis:
Man ordne jedem Element b einer Booleschen Algebra $\mathcal{B}$ die Menge derjenigen maximalen Filter F (siehe kleine Übungen) von $\mathcal{B}$ mit $b \in F$ zu.

Satz 23 (Satz von Birkhoff)
Jeder distributive Verband ist isomorph zu einem Mengenring.

Beweis: Ähnlich jenem zu Satz 22.

1.3 Logik

Beispiel 15

a) Beispiele für die Notwendigkeit einer Präzisierung der Umgangssprache:

I. α) Ein Pferd zu haben, ist gut. (Mindestens ein Pferd...)

β) Ein Pferd ist ein Säugetier. (Jedes Pferd...)

γ) Er besitzt ein Pferd. (... genau ein Pferd)

II. α) Anna und Berta sind schön. (Anna ist schön und Berta ist schön.)

β) Anna und Berta sind verwandt. (Anna ist verwandt und Berta ist verwandt.)

III. Durchführungsbestimmungen zur II. Strahlenschutzverordnung:

„*In ... Ingenieurschulen dürfen z.Z. auch noch nicht zugelassene Röntgengeräte benutzt werden.*“

Dieses Zitat kann durch entsprechende „Klammerung“ verschiedene Aussagen verdeutlichen, die Klammerung ist hier eher im mathematischen Sinne zu verstehen:

α) „*In ... Ingenieurschulen dürfen z.Z. (auch noch) (nicht zugelassene) Röntgengeräte benutzt werden.*“

β) „*In ... Ingenieurschulen dürfen z.Z. auch (noch nicht zugelassene) Röntgengeräte benutzt werden.*“

γ) „*In ... Ingenieurschulen dürfen z.Z. (auch noch nicht) zugelassene Röntgengeräte benutzt werden.*“

IV. „*Wer Banknoten nachmacht oder ... oder ... und in Verkehr bringt, wird ... bestraft.*“ Eine mögliche Interpretation wäre: Man wird erst bestraft, wenn man Banknoten nachmacht *und* in den Verkehr bringt. D.h. man kann Banknoten nachmachen und geht straffrei aus, wenn man sie nicht in den Verkehr bringt.

V. *Antinomien*

α) „Der Lügner“ (Eubalides) — „*alle Kretaer sind Lügner und ich bin ein Kretaer.*“

β) „Protagoras“ (Aulus Gelius)

γ) „Dorfbarbier“ (Russell) — Ist der Dorfbarbier Selbstrasierer oder nicht?

b) Beispiele *sprachlicher Gebilde*:

I. La donna é mobile.

II. Have you prayed to··night, Dejdemona?

III. Vae victes!

IV. Staub lieber als ein Weib sein, das nicht reizt.

V. $\Pi < 3$

VI. Ist $\Pi < 3$?

VII. Es gibt ungerade vollkommene Zahlen.

Von diesen sprachlichen Gebilden sind nur V., VII. und I. Aussagen.

Definition 14
Eine **Aussage** ist ein sprachliches Gebilde, von dem es sinnvoll ist zu behaupten, es sei **wahr** (w, $\top$, 1) oder **falsch** (f, $\perp$, 0), ihm komme der Wahrheitswert w oder f zu.
Es gibt also eine Abbildung W der Menge aller (jeweils betrachteten) Aussagen in $\mathbb{B}$.

Beispiel 16

a) Rolle der Buchstaben in der Mathematik oder Informatik:

I. $e < 3$

II. $a + 3b = 5$

III. $\int_0^3 x^2\,dx = 9$

IV. $\int_0^t x^2\,dx = \frac{t^3}{3} = \int_0^t t^2\,dt$ wahre Aussage

V. $1 \leq |\{a, b, c\}| \leq 3$

b) I. Qui desiderat pacem, praeparet bellum. (Si vis pacem, para bellum)

II. $x^2 + 2x = 3$

III. $(a + b)(a - b) = a^2 - b^2$

Definition 15
(Zu Variablen siehe Definition 3α!)

α) Eine **Aussageform** ist eine Aussage oder ein sprachliches Gebilde, das nach Ersetzung von (freien) Variablen durch (Namen von) Gegenständen zu einer Aussage wird.

β) Ist bei jeder (zugelassenen) Interpretation (Ersetzung) von Aussageformen A, B mit der sich aus A ergebende Aussage $\mathfrak{A}$ auch die sich aus B ergebende Aussage $\mathfrak{B}$ wahr, so sagen wir, A **impliziere** B, B **folge aus** A, kurz $A \prec B$.

γ) Aussageformen A, B heißen **äquivalent** (gleichwertig, -bedeutend), kurz $A \prec\!\succ B$, im Fall $A \prec B$ und $B \prec A$.

Beispiel 17

a) Beispiele für Aussageformen wurden schon in Beispiel 15a) Punkt I., II. sowie in Beispiel 15b) Punkt I., V. und VII. genannt.

b) $a = c \wedge b = c \prec a = b$

c) $x \neq 0 \prec x^2 > 0$ (Abhängig vom für x zugelassenen Bereich.)

d) $n \in 2\mathbb{N} \setminus \{2\} \prec \exists p, q \in \mathbb{P} : n = p + q$ (Goldbachsche Verknüpfung)

e) v ist vollkommen $\wedge\ v \in 2\mathbb{N} \prec\!\succ \exists n \left(2^n - 1 \in \mathbb{P} \wedge v = 2^{n-1}\left(2^n - 1\right)\right)$

Definition 16 (Präordnung)
K sei eine beliebige Klasse: Eine transitive und auf K reflexive Relation heiße Präordnung oder Quasiordnung auf K.

Beispiel 18

a) Jede Ordnung ist eine Präordnung.

b) Jede Äquivalenzrelation ist eine Präordnung.

c) Auf der Klasse $\mathfrak{G}$ aller Gruppen ist die Relation

$$\{(\mathcal{G}, \mathcal{H}) \in \mathcal{G} \times \mathcal{G} \mid \mathcal{H} \text{ ist kein Bild von } \mathcal{G}\}$$

eine Präordnung, die weder Ordnung noch Äquivalenzrelation ist.

Satz 24
Ist $\leq$ eine Präordnung auf M, so ist $\leq \cap \geq$ eine Äquivalenzrelation auf M. (Dabei sei $\geq$ die zu $\leq$ inverse oder konverse Relation, also $\geq \rightleftharpoons \leq^{-1}$)

Beweis:
$\leq$ sei Präordnung auf M, $\sim \rightleftharpoons \leq \cap \geq$ und $x, y, z \in M$:

a) $\sim$ ist reflexiv auf M: Wegen $x \leq x$ gilt $x \geq x$ und daher:

$$x \leq x \wedge x \geq x,$$

also ist $x \sim x$ für jedes x.

b) $\sim$ ist symmetrisch: $x \sim y \Rightarrow x \leq y, x \geq y \Rightarrow y \leq x, y \geq x \Rightarrow y \sim x$

c) $\sim$ ist transitiv: $x \sim y, y \sim x \Rightarrow x \leq y, y \leq x, y \leq z, z \leq y \Rightarrow x \leq z, z \leq x \Rightarrow x \sim z$

Satz 25
$\mathcal{A}$ sei die Klasse der jeweils betrachteten Aussageform:

a) $\prec$ ist Präordnung auf $\mathcal{A}$, d.h.

$$A \prec A \tag{14}$$

und

$$A \prec B, B \prec C \Rightarrow A \prec C \qquad \text{Transitivität der Implikation} \tag{15}$$

für alle $A, B, C \in \mathcal{A}$.

b) $\prec\!\succ$ ist Äquivalenzrelation auf $\mathcal{A}$.

Beweis:

a) (14): Da gleiche Variablen durch gleiche Aussagen ersetzt werden müssen, trivial!

(15): Sei $A \prec B$ und $B \prec C$ sowie $\mathfrak{A}$ eine wahre Ersetzung von A, und $\mathfrak{B}$ bzw. $\mathfrak{C}$ eine Ersetzung von B bzw. C, dann ist $\mathfrak{B}$ wahr, also auch $\mathfrak{C}$, und somit gilt $A \prec C$.

b) Direkt aus a) und Satz 24.

Definition 17

α) A, B seien Voraussetzungen für Aussageformen und ι, κ logische Partikel. Bestimmen die Wahrheitswerte von A und B eindeutig den Wahrheitswert von ιA bzw. $A\kappa B$, so heiße ι bzw. κ **ein-** bzw. **zweistelliger Junktor**.

β) Ist α ein Boolscher Ausdruck und sind $v_1, \cdots, v_n$ sämtliche in α vorkommende (freie) Variablen, so heiße $(x_1, \cdots, x_n)$ aus $\mathbb{B}^n$ eine **Belegung** von α.

Jeder Belegung von α ist eindeutig ein Wahrheitswert von α zugeordnet, diese Funktion aus $\mathfrak{B}_n$ wird mit φ_α bezeichnet.

Satz 26
A, B seien Boolsche Ausdrücke und $v_1, \cdots, v_n$ mit $n \in \mathbb{N}_0$ sämtliche sowohl in A, als auch in B vorkommende Variablen:
$A \prec B$ gilt genau dann, wenn es keine Belegung $\mathfrak{x}$ bzw. $\mathfrak{y}$ von A bzw. B so gibt, daß $\varphi_A(\mathfrak{x}) = 1$ und $\varphi_B(\mathfrak{y}) = 0$ ist, und natürlich den $v_1, \cdots, v_n$ in A und B jeweils dieselben Wahrheitswerte zugeordnet werden.

Beispiel 19
In $\mathfrak{B}_1$ können x folgende Wahrheitswerte zugeordnet werden:

x	$\top$	x	$\overline{x}$	$\bot$
1	1	1	0	0
0	1	0	1	0

Satz 27
Es gilt:

$$\overline{\overline{A}} \prec\!\!\succ A \qquad \text{(Doppelte Negation)} \tag{16}$$

für beliebige boolsche Ausdrücke und

$$\overline{\top} \prec\!\!\succ \bot, \overline{\bot} \prec\!\!\succ \top \tag{17}$$

Beweis:

(16): siehe (8).

Satz 28
Für Boolsche Ausdrücke A, B, C gilt:

a)

$$A \wedge B \prec A, A \wedge B \prec B \tag{18}$$
$$A \prec B, A \prec C \Rightarrow A \prec B \wedge C \tag{19}$$

b)

$$A \wedge A \mathrel{\prec\!\!\succ} A \tag{20}$$

Beweis:

a) Wir beweisen Satz 28a) durch Wahrheitstabellen. (Siehe auch Satz 26)

(18):

A	B	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	0

(19):

A	B	C	$B \wedge C$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

b) Zum Beweis haben wir wieder mehrere Möglichkeiten:

- durch die Wahrheitstabelle,
- durch Satz 1 (3) oder
- mit der Methode der Heuristik:

1.	$A \wedge A \prec A$	(18)
2.	$A \prec A$	(14)
3.	$A \prec A$	(14)
4.	$A \prec A \wedge A$	(19)
5.	$A \wedge A \mathrel{\prec\!\!\succ} A$	1, 4

Beispiel 20

a) A: Sie ist schön.
B: Sie ist klug.
C: Sie ist begehrenswert.
Aus der Beziehung $A \wedge B \prec C$ kann man schließen: $A \wedge \overline{C} \prec \overline{B}$ (Kontraposition)

b) Seien $a, b \in \mathbb{R}$ mit $a < b$ und φ eine auf $[a, b]$ stetige reelle Funktion:

- φ differenzierbar auf $]a, b[\ \wedge\ \varphi(a) = \varphi(b) \prec \exists c \in\ ]a, b[: \varphi'(c) = 0$,
- φ differenzierbar auf $]a, b[\ \wedge\ \nexists c \in\ ]a, b[: \varphi'(c) = 0 \prec \varphi(a) \neq \varphi(b)$

Satz 29
Für Boolsche Ausdrücke A, B und C gilt:

$$A \wedge B \prec C \Rightarrow A \wedge \overline{C} \prec \overline{B} \qquad \text{(Kontraposition)} \tag{21}$$
$$A \prec B \Rightarrow \overline{B} \prec \overline{A} \qquad \text{(Kontraposition)} \tag{22}$$
$$A \succ\!\prec B \Rightarrow \overline{a} \succ\!\prec \overline{B} \tag{23}$$

Beweis:

(21): analog zum Beweis von (19).

(22): $\overline{B} \wedge \overline{B} \prec \overline{A}$, also folgt $\overline{B} \wedge A \prec B$

1	$\overline{B} \prec \overline{B} \wedge \overline{B}$	(20)
2	$\overline{B} \wedge A \prec A$	(18)
3	$A \prec B$	(22)
4	$\overline{B} \wedge A \prec B$	(15)
5	$\overline{B} \wedge \overline{B} \prec \overline{A}$	(21)
6	$\overline{B} \prec \overline{A}$	(15) : 1, 5

(23:) Unter Benutzung von (22) lassen sich folgende Beziehungen aufbauen:

- $A \prec B \Rightarrow \overline{B} \prec \overline{A}$
- $B \prec A \Rightarrow \overline{A} \prec \overline{B}$

insgesamt also $A \succ\!\prec B \Rightarrow \overline{A} \succ\!\prec \overline{B}$

Satz 30
Für Boolsche Ausdrücke A, B, C gilt:

$$A \wedge B \succ\!\prec B \wedge A \tag{24}$$
$$(A \wedge B) \wedge C \succ\!\prec A \wedge (B \wedge C) \tag{25}$$
$$A \succ\!\prec B \Rightarrow \begin{cases} A \wedge C \succ\!\prec B \wedge C \\ C \wedge A \succ\!\prec A \wedge B \end{cases} \tag{26}$$

Beweis:

(26): Voraussetzung: $A \succ\!\prec B$
Hier genügt es zu zeigen: $A \wedge C \prec B \wedge C$. (Der Fall $C \wedge A \prec C \wedge B$ ist trivial wegen (24)!)

1	$A \wedge C \prec A$	(18)
2	$A \prec B$	Vor.
3	$A \wedge C \prec B$	(15)
4	$A \wedge C \prec C$	(18)
5	$A \wedge C \prec B \wedge C$	(19)

Satz 31
Ersetzt man in einem Boolschen Ausdruck, der an Junktoren nur $\neg$ und $\wedge$ enthält, Aussageformen durch äquivalente, so erhält man einen äquivalenten Boolschen Ausdruck.

Beweis:
Durch Induktion nach dem Termaufbau unter Berücksichtigung von (23) und (26).

Satz 32
Für Boolsche Ausdrücke A, B, C gilt:

$$A \wedge \overline{A} \prec B \tag{27}$$

$$A \wedge \overline{A} \mathrel{\succ\!\!\!\prec} \bot \qquad \text{(Satz vom Widerspruch)} \tag{28}$$

$$\bot \prec A \qquad \text{(ex falso quodlibet)} \tag{29}$$

$$A \prec \top \qquad \text{(ex quodlibet verum)} \tag{30}$$

$$A \wedge \bot \mathrel{\succ\!\!\!\prec} \bot, \quad A \wedge \top \mathrel{\succ\!\!\!\prec} A \tag{31}$$

$$A \wedge \overline{B} \prec C, \quad A \wedge \overline{B} \prec \overline{C} \Rightarrow A \prec B \qquad \text{(Indirekter Beweis, Widerspruchsbeweis)} \tag{32}$$

Beweis:

	1	$A \wedge \overline{A} \prec \overline{A} \wedge A$	(24)
	2	$A \prec \overline{\overline{A}}$	(16)
	3	$\overline{A} \wedge A \prec \overline{A} \wedge \overline{\overline{A}}$	(26)
	4	$A \wedge \overline{A} \prec \overline{A} \wedge \overline{\overline{A}}$	(15) : 1, 3
(26):	5	$\overline{A} \wedge \overline{B} \prec \overline{A}$	(18)
	6	$\overline{A} \wedge \overline{\overline{A}} \prec \overline{\overline{B}}$	(21)
	7	$\overline{\overline{B}} \prec B$	(16)
	8	$\overline{A} \wedge \overline{\overline{A}} \prec B$	(15)
	9	$A \wedge \overline{A} \prec B$	(15) : 4, 8

Satz 33
Für Boolsche Ausdrücke A, B, C gilt:

$$A \prec A \vee B, \quad B \prec A \vee B \tag{33}$$

$$A \prec C, B \prec C \Rightarrow A \vee B \prec C \tag{34}$$

$$A \vee A \mathrel{\succ\!\!\!\prec} A \tag{35}$$

$$A \vee B \mathrel{\succ\!\!\!\prec} \overline{\overline{A} \wedge \overline{B}} \tag{36}$$

$$A \wedge B \mathrel{\succ\!\!\!\prec} \overline{\overline{A} \vee \overline{B}}$$

Satz 34
Ersetzt man in einem Boolschen Ausdruck, der an Junktoren nur $\neg$, $\wedge$ und $\vee$ enthält, Aussageformen durch äquivalente, so erhält man einen äquivalenten Boolschen Ausdruck.

Beweis: Beachte (36) und Satz 31.

Satz 35 Für Boolsche Ausdrücke A, B, C gilt:

$$A \vee B \divideontimes B \vee A \tag{37}$$
$$(A \vee B) \vee C \divideontimes A \vee (B \vee C) \tag{38}$$
$$A \vee \overline{A} \divideontimes \top \qquad \text{(Tertium non datur)} \tag{39}$$
$$A \vee \top \divideontimes \top, A \vee \bot \divideontimes A \tag{40}$$
$$A \vee (A \vee B) \divideontimes A, A \vee (A \wedge B) \divideontimes A \tag{41}$$
$$\begin{aligned} &A \wedge (B \vee C) \divideontimes (A \wedge B) \vee (A \wedge C) \\ &A \vee (B \wedge C) \divideontimes (A \vee B) \wedge (A \vee C) \end{aligned} \tag{42}$$
$$\begin{aligned} &A \wedge B \prec C \Rightarrow A \prec \overline{B} \vee C \\ &A \prec B \vee C \Rightarrow A \wedge \overline{B} \prec C \end{aligned} \qquad \text{(Transportationsregeln)} \tag{43}$$
$$A \prec B \vee C, A \wedge B \prec C \Rightarrow A \prec C \qquad \text{(Schnittregel)} \tag{44}$$

Beweis:

(37): $A \vee B \overset{(36)}{\divideontimes} \overline{\overline{A} \wedge \overline{B}} \overset{(24)}{\divideontimes} \overline{\overline{B} \wedge \overline{A}} \overset{(36)}{\divideontimes} B \vee A$

(39): $A \vee \overline{A} \overset{(36)}{\divideontimes} \overline{\overline{A} \wedge \overline{\overline{A}}} \overset{(28)}{\divideontimes} \overline{\bot} \overset{(17)}{\divideontimes} \top$

(44): $\left.\begin{array}{l} A \prec A \\ A \prec B \vee C \end{array}\right\} A \prec A \wedge (B \wedge C) \prec (A \wedge B) \vee (A \wedge C) \prec C \vee (A \wedge C) \prec C$

Definition 18
Der Aussageform A werde durch $\{x|A\}$ ein neues Objekt (als Schreibfigur) – die Menge der x mit A – derart zugeordnet, daß für Aussageformen A und B diese Objekte genau dann gleich sind, wenn $A \divideontimes B$ für alle x, also

$$\{x|A\} = \{x|B\} \rightleftharpoons \forall x : A \divideontimes B.$$

Für $M = \{x|A\}$ wird „x ist Element von M" („x aus M", „x gehört zu M" etc.) definiert durch

$$x \in M \rightleftharpoons A.$$

Ferner sei

$$x \notin M \rightleftharpoons \neg(x \in M)$$
$$\emptyset \rightleftharpoons \{x|\bot\} \qquad \text{(leere Menge)}$$
$$U \rightleftharpoons \{x|\top\} \qquad \text{(Universum, Universalmenge)}$$
$$\{a_1, \cdots, a_n\} \rightleftharpoons \left\{x| \quad \bigvee_{\nu=1}^{n} \quad x = a_\nu\right\}$$
$$\exists x \in M : A \rightleftharpoons \exists x : x \in M \wedge A$$
$$\forall x \in M : A \rightleftharpoons \forall x : x \in M \prec A$$
$$\{\mathcal{T}|y \in M\} \rightleftharpoons \{x|\exists y \in M : x = \mathcal{T}\} \qquad (\mathcal{T}\text{: Term, Variablenkollision})$$

Bemerkung 10
Vorsicht! Die zum Aufbau der Mengen zulässigen Bindungen müssen eingeschränkt werden, da sonst ein Widerspruch eintritt: Für $M \rightleftharpoons \{x|x \in x\}$ gilt $M \in M \Leftrightarrow M \notin M$! (Russelsche Antinomie, vgl. Beispiel 15aVγ) — „Der Dorfbarbier“) Genaueres in einer Vorlesung „(Grundlagen der) Mengentheorie“.

Satz 36
Für Mengen M, N gelten:

$$M = \{x|x \in M\} \qquad \text{und} \tag{45}$$
$$M = N \Leftrightarrow \forall x : x \in M \Leftrightarrow x \in N. \tag{46}$$

Beweis:

(45): trivial nach Definition.

(46):

$$\begin{aligned} M = N &\overset{(45)}{\iff} \{x|x \in M\} = \{x|x \in N\} \\ &\overset{\text{Def.}}{\iff} \forall x : x \in M \Leftrightarrow x \in N \end{aligned}$$

Definition 19
M, N seien Mengen und

$\overline{M} \rightleftharpoons \{x\|x \notin M\}$	**Komplement** von M
$M \cap N \rightleftharpoons \{x\|x \in M \wedge x \in N\}$	**Durchschnitt** von M und N
$M \cup N \rightleftharpoons \overline{\overline{M} \cap \overline{N}}$	**Vereinigung** von M und N
$M \setminus N \rightleftharpoons M \cap \overline{N}$	**Differenz** von M und N
$M \triangle N \rightleftharpoons (M \setminus N) \cup (N \setminus M)$	**Symmetrische Differenz** von M und N
$M \subseteq N \rightleftharpoons \forall x : x \in M \prec x \in N$	**Mengeninklusion**
$P(M) \rightleftharpoons \{x\|x \subseteq M\}$	**Potenzmenge** von M

und für eine Menge $\mathfrak{M}$ von Mengen

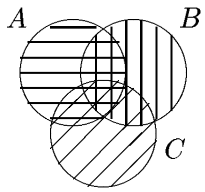
$$\bigcap \mathfrak{M} \rightleftharpoons \{x|\forall M \in \mathfrak{M} : x \in M\}$$

und

$$\bigcup \mathfrak{M} \rightleftharpoons \{x|\exists M \in \mathfrak{M} : x \in M\}$$

im Einklang mit der Definition von $\cap$ und $\cup$.

Bemerkung 11
Mengen lassen sich in bekannter Weise durch (Euler)-Venn-Diagramme darstellen, mengenalgebraische Formeln, durch solch Diagramme sogar *beweisen*, falls nur ein „allgemeiner Fall“ behandelt wird. (siehe auch Anhang E.)



$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (a \cap C)$$

Satz 37
Für Mengen M, N gelten:

$$M = N \Leftrightarrow M \subseteq N \wedge N \subseteq M \tag{47}$$
$$\emptyset \subseteq M \subseteq U. \tag{48}$$

Beweis:

(47):

$$\begin{aligned} M = N &\overset{(46)}{\Longleftrightarrow} \forall x : x \in M \prec\!\!\!\succ x \in N \\ &\Longleftrightarrow \forall x : ((x \in M \prec x \in N) \wedge (x \in N \prec x \in M)) \\ &\Longleftrightarrow \forall x\,(x \in M \prec x \in N) \wedge \forall x\,(x \in N \prec x \in M) \\ &\Longleftrightarrow M \subseteq N \wedge N \subseteq M \end{aligned}$$

(48): ex falso quodlibet:

$$\begin{aligned} \perp \prec x \in M &\Rightarrow \forall x : \perp \prec x \in M \\ &\Rightarrow \forall x : x \in \{x|\perp\} \prec x \in M \\ &\Rightarrow \emptyset \subseteq M. \end{aligned}$$

Definition 20
A, B, M, N seien Mengen:

α) $(a, b) \rightleftharpoons \{\{a\}, \{a, b\}\}$ heiße **Paar** (aus a und b), und

$$\begin{aligned} A \times B &\rightleftharpoons \{(a,b)|a \in A \wedge b \in B\} \\ &\rightleftharpoons \{x|\exists a, b : x = (a,b) \wedge a \in A \wedge b \in B\} \end{aligned}$$

heiße **kartesisches Produkt** aus A und B.

β) Eine Menge von Paaren heißt **(binäre) Relation**. – ϑ sei Relation: Für $(x, y) \in \vartheta$ schreibt man auch $x\vartheta y$.
Gilt

$$x\vartheta y \wedge x\vartheta z \prec y = z,$$

so heiße ϑ **rechtseindeutig**, entsprechend **linkseindeutig**:

$$V_\vartheta \rightleftharpoons \{x | \exists y : x\vartheta y\} \quad \text{heiße } \textbf{Vorbereich(sfeld)} \text{ von } \vartheta$$
$$N_\vartheta \rightleftharpoons \{y | \exists x : x\vartheta y\} \quad \text{heiße } \textbf{Nachbereich(sfeld)} \text{ von } \vartheta$$

und

$$\vartheta|_M \rightleftharpoons \vartheta \cap (M \times N_\vartheta) \quad \text{heiße } \textbf{Einschränkung} \text{ von } \vartheta$$

auf M.

γ) Eine rechtseindeutige (binäre) Relation φ heiße **Funktion** oder **Abbildung** – für $x\varphi y$ schreibt man auch $y = \varphi(x)$. φ heiße Funktion (Abbildung) bzw. **partielle Funktion (Abbildung)** auf (von) M, falls

$$D \rightleftharpoons D_\varphi \rightleftharpoons V_\varphi$$

gilt mit $D = M$ bzw. $D \subseteq M$ und ferner sei

$$\varphi : M \longrightarrow N \rightleftharpoons \ \varphi \text{ ist Funktion auf } M \wedge N_\varphi \subseteq N$$

und man sagt „φ ist Abbildung von M in N“.
(**Kategorischer Funktionsbegriff**:

$$\varphi \text{ ist Funktion } \rightleftharpoons \exists B\gamma : \varphi = (\gamma, B) \wedge \gamma \text{ rechtseindeutige Relation } \wedge N_\varphi \subseteq B.)$$

δ) Eine Funktion φ auf $\mathbb{A}_n$ mit $n \in \mathbb{N}$ heiße **n-Tupel** und man schreibt

$$\varphi = (\varphi(1), \varphi(2), \cdots, \varphi(n)) .$$

Eine **n-äre Relation** ist eine Menge von n-Tupeln.

Satz 38
Seien $\alpha = (a_1, a_2, \ldots, a_n)$ und $\beta = (b_1, b_2, \ldots, b_n)$ irgendwelche n-tupel, so gilt

$$\alpha = \beta \leftrightarrow \bigwedge_{\nu=1}^{n} a_\nu = b_\nu \tag{49}$$

Bemerkung 12
Paare und allgemeine n-tupel können als undefinierte Objekte eingeführt werden, bei denen die Gleichheit durch (49) gegeben ist.

Definition 21
$\mathcal{A}$ sei eine Menge von Aussageformen und $\tilde{A}$ bezeichne die Klasse der zu $A(\in \mathcal{A})$ äquivalenten Aussageformen aus $\mathcal{A}$. Für $A, B \in \mathcal{A}$ sei

$$\overline{\tilde{A}} \rightleftharpoons \tilde{\overline{A}}$$

und

$$\tilde{A} \wedge \tilde{B} \rightleftharpoons \widetilde{A \wedge B} \tilde{A} \vee \tilde{B} \rightleftharpoons \widetilde{A \vee B}$$

(Diese Verknüpfungen sind wohldefiniert!).

Satz 39
$\mathfrak{A}$ sei eine Menge von Klassen äquivalenter Aussageformen und bezüglich $\overline{}$ sowie $\wedge$ abgeschlossen: Dann ist $\mathcal{A} = (\mathfrak{A}, \wedge, \vee)$ ein Boolscher Verband und es gibt eine Menge $\mathfrak{M}$ von Mengen mit $(\mathfrak{M}, \wedge, \vee) \simeq \mathcal{A}$

Beweis:
Sei $\varphi(\tilde{A}) \rightleftharpoons \{x|X\}$ für $X \in \tilde{A} \in \mathfrak{A}$ und geeignetem x (Variablenkollision!), dann ist φ wohldefiniert. Mit $\mathfrak{M} = \varphi\mathfrak{A}$ gilt $\varphi : \mathfrak{A} \rightarrowtail\!\!\!\twoheadrightarrow \mathfrak{M}$ und

$$\varphi(\overline{\tilde{A}}) = \varphi(\tilde{\overline{A}}) = \{x|\overline{A}\} = \overline{\{x|A\}} = \overline{\varphi(\tilde{A})},$$
$$\varphi(\tilde{A} \wedge \tilde{B}) = \varphi(\widetilde{A \wedge B}) = \{x|A \wedge B\} = \{x|A\} \wedge \{x|B\} = \varphi(\tilde{A}) \wedge \varphi(\tilde{B})$$

für alle $\tilde{A}, \tilde{B} \in \mathfrak{A}$; wegen „DEMORGAN“ ist $\mathfrak{A}$ auch bezüglich $\vee$ abgeschlossen, und man hat entsprechend

$$\varphi(\tilde{A} \vee \tilde{B}) = \varphi(\tilde{A}) \vee \varphi(\tilde{B}),$$

also

$$\varphi : \mathcal{A} \overset{\sim}{\rightarrowtail\!\!\!\twoheadrightarrow} (\mathfrak{M}, \cap, \cup).$$

und, da $(\mathfrak{M}, \cap, \cup)$ als Mengenkörper Boolscher Algebra ist, auch $\mathcal{A}$ als Boolscher Algebra.

Definition 22
(vergleiche Definition 3β)
Sind A, B Boolscher Ausdruck, so auch $(A \to B)(\neg, \supset, \Rightarrow, \rhd, : \cdot, \rightsquigarrow, \frown)$, kurz $A \to B$, – „wenn A, dann B“ – die **Subjunktion** ((Nateriale) Implikation) von A und B mit:

$\to$	w	f
w	w	f
f	w	w

Bemerkung 13
„$A \to B$“ ist genau im Falle $a \prec B$ (vergleiche auch Definition 15β und Satz 26) wahr.

Satz 40
Für Boolsche Ausdrücke A, B, C gilt:

$$A \to A \asymp \top \tag{50}$$
$$(A \to B) \wedge (B \to C) \prec A \to C \qquad \text{(Transitivität von } \to) \tag{51}$$
$$A \to B \asymp \overline{A} \vee B \tag{52}$$
$$\bot \to A \asymp \top, A \to \top \asymp \top \tag{53}$$
$$\top \to A \asymp A, A \to \bot \asymp \overline{A}$$
$$A \wedge (A \to B) \prec B \qquad \text{(Modus (ponendo) ponens, Abtrennungsregel)} \tag{54}$$
$$\neg B \wedge (A \to B) \prec \neg A \qquad \text{(Modus (tollendo) tollens, Widerlegungsregel)} \tag{55}$$
$$A \wedge B \prec C \Rightarrow A \prec B \to C \tag{56}$$
$$A \prec B \to C \Rightarrow A \wedge B \prec C$$

Beweis:
(50)–(53), (55), (56) Übung.

(54):

$$
\begin{array}{rcll}
A \to B & \prec & \overline{A} \vee \overline{B} & (52) \\
A \wedge (A \to B) & \prec & A \wedge (\overline{A} \vee B) & (26) \\
A \wedge (\overline{A} \vee B) & \prec & (A \wedge \overline{A}) \vee (A \wedge B) & (42) \\
A \wedge (A \to B) & \prec & (A \wedge \overline{A}) \vee (A \wedge B) & (15) \\
A \wedge \overline{A} & \prec\!\!\!\succ & \bot & (28) \\
(A \wedge \overline{A}) \vee (A \wedge B) & \prec\!\!\!\succ & \bot \vee (A \wedge B) & \text{Satz 31} \\
A \wedge (A \to B) & \prec & \bot \vee (A \wedge B) & (15) \\
\bot \vee (A \wedge B) & \prec & (A \wedge B) \vee \bot & (37) \\
A \wedge (A \to B) & \prec & (A \wedge B) \vee \bot & (15) \\
(A \wedge B) \vee \bot & \prec & A \wedge B & (40) \\
A \wedge (A \to B) & \prec & A \wedge B & (15) \\
A \wedge B & \prec & B & (18) \\
A \wedge (A \to B) & \prec & B & (15)
\end{array}
$$

Bemerkung 14
$A \leftrightarrow B$ (siehe Definition 1αVII) ist genau im Falle $A \prec\!\!\!\succ B$ wahr (vgl. Bemerkung 12).

Satz 41
Für Boolesche Ausdrücke A, B, C gelten:

$$A \leftrightarrow B \prec\!\!\!\succ (A \to B) \wedge (B \to A) \tag{57}$$

$$A \leftrightarrow B \prec\!\!\!\succ (\overline{A} \vee B) \wedge (\overline{B} \vee A) \tag{58}$$

$$A \leftrightarrow B \prec\!\!\!\succ (A \wedge B) \vee (\overline{A} \wedge \overline{B}) \tag{59}$$

$$\top \leftrightarrow A \prec\!\!\!\succ A \prec\!\!\!\succ A \leftrightarrow \top \tag{60}$$

$$\bot \leftrightarrow A \prec\!\!\!\succ \overline{A} \prec\!\!\!\succ A \leftrightarrow \bot$$

$$A \leftrightarrow B \prec\!\!\!\succ B \leftrightarrow A \tag{61}$$

$$(A \leftrightarrow B) \leftrightarrow C \prec\!\!\!\succ A \leftrightarrow (B \leftrightarrow C) \tag{62}$$

Beweis: Übung.

Satz 42
Für Boolesche Ausdrücke A, B, C gelten:

$$A \bigtriangleup B \prec\!\!\!\succ (A \vee B) \wedge \overline{A \wedge B} \tag{63}$$

$$A \bigtriangleup B \prec\!\!\!\succ (A \wedge \overline{B}) \vee (\overline{A} \wedge B) \tag{64}$$

$$A \bigtriangleup B \prec\!\!\!\succ \overline{A \leftrightarrow B} \tag{65}$$

$$A \bigtriangleup B \prec A \vee B \tag{66}$$

$$A \bigtriangleup B \prec\!\!\!\succ B \bigtriangleup A \tag{67}$$

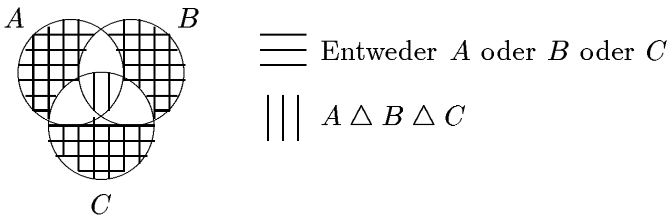
$$(A \bigtriangleup B) \bigtriangleup C \prec\!\!\!\succ A \bigtriangleup (B \bigtriangleup C) \tag{68}$$

$$\top \bigtriangleup B \prec\!\!\!\succ \overline{B} \tag{69}$$

$$\bot \bigtriangleup B \prec\!\!\!\succ B$$

Beweis: Übung.

Bemerkung 15
„$A \bigtriangleup B \bigtriangleup C$“ bedeutet nicht „Entweder A oder B oder C“:



Definition 23
Sind A, B Boolesche Ausdrücke, so auch $A \leftarrow B$, $A \leftharpoondown B$ und $A \rightharpoonup B$, die **konverse Subjunktion**, die **Subtraktion** und die **konverse Subtraktion** mit:

$\leftarrow :=$

A	B	$A \leftarrow B$
0	0	1
0	1	1
1	0	0
1	1	1

, $\leftharpoondown :=$

A	B	$A \leftharpoondown B$
0	0	0
0	1	1
1	0	0
1	1	0

und $\rightharpoonup :=$

A	B	$A \rightharpoonup B$
0	0	0
0	1	0
1	0	1
1	1	0

Beispiel 21

$\bot$	$\overline{\lor}$	$\rightharpoonup$	$\overline{x}$	$\leftharpoondown$	$\overline{y}$	$\bigtriangleup$	$\overline{\land}$	$\land$	$\leftrightarrow$	y	$\rightarrow$	x	$\leftarrow$	$\lor$	$\top$
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Die jeweiligen Negate erhält man durch Spiegelung an der Mittelachse.

Definition 24
A und B seien Boolesche Ausdrücke.
A und B heißen **supplementär**, wenn $A \lor B$ wahr ist.
A und B heißen **konträr** (**kontradiktorisch**), wenn $A \overline{\lor} B$ wahr ist.
A und B heißen **äquivalent**, wenn $A \leftrightarrow B$ wahr ist.
A und B heißen **kontravalent** (**antivalent**), wenn $A \bigtriangleup B$ wahr ist.

Satz 43
Ersetzt man in einem Booleschen Ausdruck Teilausdrücke durch äquivalente, so erhält man einen äquivalenten Booleschen Ausdruck.

Beweis: Übung.

Definition 25
A sei Boolescher Ausdruck.

α) A heißt **allgemeingültig** (**tautologisch**), wenn $A \between \top$.

β) A heißt **inkonsistent** (**antilogisch**, **kontradiktorisch**), wenn $\neg A$ allgemeingültig ist.

γ) A heißt **erfüllbar** (satisfiable), wenn A nicht inkonsistent ist.

Satz 44
A sei ein Boolescher Ausdruck.

a) A allgemeingültig $\Longrightarrow$ A erfüllbar.

b) A inkonsistent $\Longleftrightarrow$ $A \mathrel{-\!\!\ast\!\!-} \bot$.

c) A erfüllbar $\Longleftrightarrow$ A allgemeingültig $\vee\ \exists(x_1,\dots,x_n):\ \varphi_A(x_1,\dots,x_n) =$w.

d) A nicht allgemeingültig $\Longleftrightarrow$ A inkonsistent $\vee\ \exists(x_1,\dots,x_n):\ \varphi_A(x_1,\dots,x_n) =$f.

Beweis:

a) Kontraposition:
A nicht erfüllbar $\Leftrightarrow$ A inkonsistent $\Leftrightarrow$ $\neg A$ allgemeingültig $\Leftrightarrow \neg A \mathrel{-\!\!\ast\!\!-} \top \Leftrightarrow A \mathrel{-\!\!\ast\!\!-} \bot$
$\Rightarrow$ Beh.

b) siehe a)

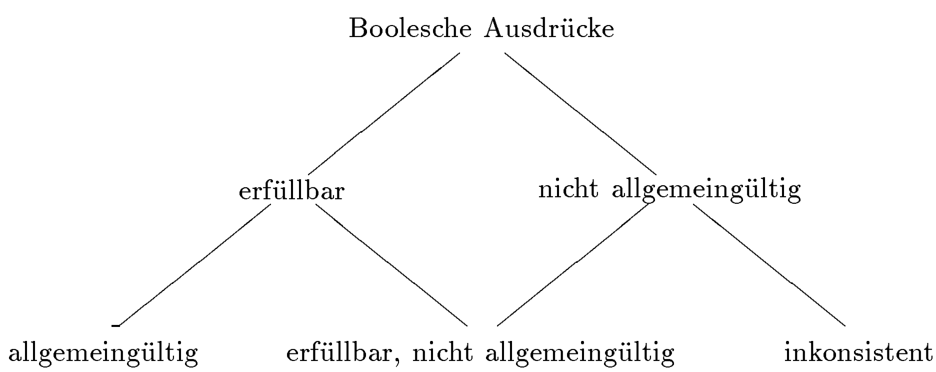
c) A erfüllbar $\overset{\text{b)}}{\Leftrightarrow}$ nicht: $A \mathrel{-\!\!\ast\!\!-} \bot \Leftrightarrow A \mathrel{-\!\!\ast\!\!-} \top \vee \exists(x_1,\dots,x_n):\ \varphi(x_1,\dots,x_n) =$w

d) analog c)

Beispiel 22

$$
\begin{array}{lll}
 & (A \to B) \to ((A \to C) \to (A \to B \wedge C)) & \\
A = \top: & B \to (C \to B \wedge C) & \\
\quad B = \top: & C \to C & \text{erfüllbar} \\
\quad B = \bot: & \top & \text{erfüllbar} \\
A = \bot: & \top \to (\top \to \top) & \text{allgemeingültig}
\end{array}
$$

Bemerkung 16
Arten von Booleschen Ausdrücken:



Satz 45
Ein Boolescher Ausdruck in konjunktiver bzw. adjunktiver Normalform ist genau dann allgemeingültig bzw. inkonsistent, wenn in jeder seiner Ad- bzw. Konjunktionen $\top$ bzw. $\bot$ vorkommt oder mindestens eine Variable zugleich mit ihrem Negat auftritt oder $\top$ und $\bot$ gleichzeitig auftreten.

Beweis:
A sei ein Boolescher Ausdruck in konjunktiver Normalform und

$\Rightarrow$: von der genannten Art. Dann folgt $A \mathrel{-\!\!\ast\!\!-} \top$, also die Allgemeingültigkeit von A.

$\Leftarrow$: allgemeingültig. Sei etwa $A = \bigwedge\limits_{\mu=1}^{m} A_\mu$ mit $m \in \mathbb{A}_n$.
Dann ist A_μ für jedes $\mu = 1, \ldots, m$ allgemeingültig.
Sei $A_\mu = \bigvee\limits_{\nu=1}^{n_\mu} B_{\mu\nu}$ mit $n_\mu \in \mathbb{N}$ und $\mu \in \mathbb{A}_m$.
Wäre $B_{\mu\nu} \neq \top$ für $\nu = 1, \ldots, n\mu$ und gäbe es keine $\lambda, \nu \in \mathbb{A}_\mu$ mit $B_{\mu\nu} = \overline{B}_{\mu\lambda}$, dann gäbe es eine Belegung $(x_1, \ldots, x_{m_\mu})$ von A_μ mit $\varphi_{A_\mu}(x_1, \ldots, x_{m_\mu})$ =f oder es wäre $A_\mu \mathrel{-\!\!\ast\!\!-} \bot$, beides im Widerspruch zur Allgemeingültigkeit von A_μ.

Für A in adjunktiver Normalform entsprechend.

Beispiel 23

$$
\begin{aligned}
&\neg((A \to B \vee C) \to (A \wedge \overline{B} \to C)) \\
&\qquad \mathrel{-\!\!\ast\!\!-} \neg(\overline{\overline{A} \vee B \vee C} \vee \overline{A \wedge \overline{B}} \vee C) \\
&\qquad \mathrel{-\!\!\ast\!\!-} (\overline{A} \vee B \vee C) \wedge A \wedge \overline{B} \wedge \overline{C} && \text{kon. Nf. nicht allgemeingültig} \\
&\qquad \mathrel{-\!\!\ast\!\!-} (\overline{A} \wedge A \wedge \overline{B} \wedge \overline{C}) \vee (A \wedge B \wedge \overline{B} \wedge \overline{C}) \vee (A \wedge \overline{B} \wedge C \wedge \overline{C}) && \text{ad. Nf. inkonsistent}
\end{aligned}
$$

Bemerkung 17
Methoden zur Feststellung der Allgemeingültigkeit, Erfüllbarkeit oder Inkonsistenz eines Booleschen Ausdrucks:

a) Vollständige Tabelle (2^n Ersetzungen) ei n Variablen: selbst mit heutigen Rechnern bei vielen Variablen nicht mehr zu schaffen (bei 30 Variablen mehr als 10^9 Ersetzungen!)

b) Reduziertes, „effektives Probieren“, siehe Beispiel 22

c) Umformen auf Bekanntes

d) Umformen auf konjunktive oder adjunktive Normalform

Definition 26 (vollständige Normalform)
Ein Boolescher Ausdruck α heißt **vollständige konjunktive** bzw. **adjunktive Normalform**, wenn $\alpha = \top$ oder $\alpha = \bot$ oder α in konjunktiver bzw. adjunktiver Normalform ist und α weder $\top$ noch $\bot$ enthält und jede Kon- bzw. Adjunktion von α jede in α vorkommende Variable oder ihr Negat genau einmal enthält.

Beispiel 24

$A \wedge B \to C$

$\divideontimes\quad \overline{A \wedge B} \vee C$

$\divideontimes\quad \overline{A} \vee \overline{B} \vee C$ vollständige konjunktive Normalform (=ad. Nf.)

$\divideontimes\quad (\overline{A} \wedge (B \vee \overline{B})) \vee (\overline{B} \wedge (A \vee \overline{A}) \vee (C \wedge (A \vee \overline{A}))$

$\divideontimes\quad (\overline{A} \wedge B) \vee (\overline{A} \wedge \overline{B}) \vee (\overline{B} \wedge A) \vee (\overline{B} \wedge \overline{A}) \vee (C \wedge A) \vee (C \wedge \overline{A})$

$\divideontimes\quad (\overline{A} \wedge B \wedge C) \vee (\overline{A} \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge \overline{B} \wedge C) \vee (\overline{A} \wedge \overline{B} \wedge \overline{C}) \vee (A \wedge \overline{B} \wedge C)$
$\vee (A \wedge \overline{B} \wedge \overline{C}) \vee (A \wedge B \wedge C)$ vollständige adjunktive Normalform

Satz 46

Jeder Boolesche Ausdruck ist sowohl zu einem Booleschen Ausdruck in vollständiger adjunktiver als auch einem solchen in vollständiger konjunktiver Normalform äquivalent.

Beweis:

α sei ein Boolescher Ausdruck.
Dann gibt es einen zu α äquivalenten Booleschen Ausdruck β in konjunktiver Normalform. Ferner existiert ein Boolescher Ausdruck γ in konjunktiver Normalform mit $\gamma \divideontimes \beta$ derart, daß $\gamma = \top$ oder $\gamma = \bot$ ist oder γ weder $\top$ noch $\bot$ enthält, etwa $\gamma = \bigwedge\limits_{\lambda=1}^{e} \gamma_\lambda$.
Seien $(x_1, \ldots, x_n)$ genau die in γ vorkommenden Variablen und γ nicht in vollständiger konjunktiver Normalform. Dann gibt es ein minimales $m \in \mathbb{A}_e$ so, daß γ_m nicht alle x_ν dieser Art enthält. Sei $k \in \mathbb{A}_n$ der kleinste Index dieser Art.
$\delta \rightleftharpoons \gamma_m \vee (x_k \wedge \overline{x}_k) \divideontimes \gamma_m$
$\delta \divideontimes \delta' \rightleftharpoons (\gamma_m \vee x_k) \wedge (\gamma_m \vee \overline{x}_k)$
$$\gamma' \rightleftharpoons \left(\bigwedge_{\lambda=1}^{m-1} \gamma_\lambda\right) \wedge \delta' \wedge \left(\bigwedge_{\lambda=m+1}^{e} \gamma_\lambda\right)$$
Offensichtlich ist $\gamma \divideontimes \gamma'$ und x_k in beiden Adjunktionen von δ'.
Dieses Verfahren kann wiederholt werden (ν-mal), bis $\gamma^{(\nu)}$ vollständige konjunktive Normalform ist.

Für die vollständige adjunktive Normalform dual.

Definition 27

α) Eine Variable oder ihr Negat heißt **Atom**.

β) Eine Konjunktion von Atomen derart, daß keine Variable zweimal auftritt, heißt **Klausel**.
Für Klauseln κ und λ definieren wir:
$\kappa \subseteq \lambda \rightleftharpoons \forall \text{Atome } \alpha : \ (\alpha \text{ aus } \kappa \Rightarrow \alpha \text{ aus } \lambda$
$\kappa \subset \lambda \rightleftharpoons \kappa \subseteq \lambda \ \wedge \ \exists \text{Atom } \alpha : \ (\alpha \text{ aus } \lambda \wedge \alpha \text{ nicht aus } \kappa)$

γ) Eine Adjunktion von Klauseln heißt **Normalterm**.
Ein Normalterm μ heißt **minimal**, wenn aus μ durch Weglassen eines beliebigen Kon- bzw. Adjunktionsgliedes von μ kein zu μ äquivalenter Normalterm entsteht.

δ) κ und λ seien Klauseln und ν ein Normalterm.
κ heißt **Primimplikant** von ν, wenn $\kappa \prec \nu$ und $\nexists \lambda \subset \kappa : \ \lambda \prec \nu$.
κ heißt **Erweiterung** von λ bezüglich ν, wenn $\lambda \subseteq \kappa$ und in κ und ν genau dieselben Variablen vorkommen.

Satz 47
κ sei Klausel, ν Normalterm.

a) Jeder minimale zu ν äquivalente Normalterm ist eine Adjunktion von Primimplikanten.

b) Jeder Primimplikant von ν enthält nur Variable von ν.

c) ν sei adjunktive Normalform ohne $\top$ und $\bot$ und κ enthält nur Variable von ν. Dann gilt:
$\kappa \prec \nu \Longleftrightarrow$ Alle Erweiterungen von κ bezüglich ν sind Klauseln von ν.

Beweis:

a) Sei μ minimaler Normalterm mit $\mu \mathrel{\prec\!\!\!\!\succ} \nu$ und κ eine Klausel von μ.
Dann gilt $\kappa \prec \mu \prec \nu$ und mithin $\kappa \prec \nu$.
Annahme: κ ist kein Primimplikant von ν.
Dann gibt es $\lambda \subset \kappa$ mit $\lambda \prec \nu \prec \mu$, und es gilt $\lambda \prec \mu$, also ist μ nicht minimal im Widerspruch zur Voraussetzung.
Daher ist κ Primimplikant von ν.

b) Übung.

c) $\Rightarrow$: Kontraposition:
Es gebe eine Erweiterung κ' von κ bzgl. ν die nicht Klausel von ν ist. Dann enthält jede Klausel von ν eine Variable, die in κ' negiert ist oder umgekehrt.
$\varphi_{\kappa'}(x_1, \dots, x_m) = 1$ bedingt $\varphi_\lambda(x_1, \dots, x_m) = 0$ für alle Klauseln λ von ν. Wegen $\kappa' \supseteq \kappa$ gilt
$\varphi_\kappa(x_1, \dots, x_m) = 1 \Longrightarrow \varphi_\kappa(y_1, \dots, y_e) = 1$, also nicht $\kappa \prec \nu$.
$\Leftarrow$: Übung.

Satz 48
α und λ seien Klauseln und ν eine vollständige adjunktive Normalform $\neq \top, \bot$.

κ ist Primimplikant von $\nu \Longleftrightarrow$

a) Alle Variable von κ sind in ν enthalten
b) $\wedge$ Alle Erweiterungen von κ bzgl. ν sind Klauseln von ν
c) $\wedge$ $\nexists \lambda \subset \kappa$: Alle Erweiterungen von λ bzgl. ν sind Klauseln von ν

Beweis:

$\Rightarrow$: κ sei Primimplikant von ν, d. h. $\kappa \prec \nu$ und $\nexists \lambda \subset \kappa : \ \lambda \prec \nu$

Es gilt a) wegen Satz 47b),
b) wegen Satz 47c),
c) , denn gäbe es $\lambda \subset \kappa$ so, daß alle Erweiterungen von λ bzgl. ν Klauseln von ν wären, dann gälte Satz 47c) zufolge $\lambda \prec \nu$ im Widerspruch zu κ als Primimplikant.

$\Leftarrow$: Übung.

Bemerkung 18
Satz 48 liefert ein Verfahren zur Berechnung der Primimplikanten und damit nach Satz 47a) eines zur Minimalisierung von Normaltermen, das sogenannte **Quine-McCluskey-Verfahren**.

Beispiel 25 (Quine-McCluskey)

Normalterm, in jeder Adjunktion kommt jede Variable höchstens einmal vor:

$$\alpha \rightleftharpoons (A \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge C \wedge D) \vee (B \wedge D) \vee (A \wedge C \wedge \overline{D})$$
$$\vee(\overline{A} \wedge \overline{B} \wedge \overline{C} \wedge \overline{D}) \vee (\overline{B} \wedge C \wedge \overline{D})$$

fehlende Variable ergänzen und ausmultiplizieren:

$$\mathrel{-\!\!\!\ast\!\!\!-} (A \wedge B \wedge \overline{C} \wedge D) \vee (A \wedge B \wedge \overline{C} \wedge \overline{D}) \vee (\overline{A} \wedge B \wedge C \wedge D) \vee (\overline{A} \wedge \overline{B} \wedge C \wedge D)$$
$$\vee(A \wedge B \wedge C \wedge D) \vee (\overline{A} \wedge B \wedge C \wedge D) \vee (A \wedge B \wedge \overline{C} \wedge D) \vee (\overline{A} \wedge B \wedge \overline{C} \wedge D)$$
$$\vee(A \wedge B \wedge C \wedge \overline{D}) \vee (A \wedge \overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge \overline{B} \wedge \overline{C} \wedge \overline{D})$$
$$\vee(A \wedge \overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge \overline{B} \wedge C \wedge \overline{D})$$

Überflüssige (doppelt vorhandene) Adjunktionsglieder herausstreichen:

$$\mathrel{-\!\!\!\ast\!\!\!-} (A \wedge B \wedge \overline{C} \wedge D) \vee (A \wedge B \wedge \overline{C} \wedge \overline{D}) \vee (\overline{A} \wedge B \wedge C \wedge D) \vee (\overline{A} \wedge \overline{B} \wedge C \wedge D)$$
$$\vee(A \wedge B \wedge C \wedge D) \vee (\overline{A} \wedge B \wedge \overline{C} \wedge D) \vee (A \wedge B \wedge C \wedge \overline{D}) \vee (A \wedge \overline{B} \wedge C \wedge \overline{D})$$
$$\vee(\overline{A} \wedge \overline{B} \wedge \overline{C} \wedge \overline{D}) \vee (\overline{A} \wedge \overline{B} \wedge C \wedge \overline{D})$$

Umwandeln in eine Liste und untereinander vergleichen, ob sich Elemente nur in einem Atom ($\dot{X}$) unterscheiden, diese Atome entfernen und „Restterm“ in die nächste Liste setzen ($\longrightarrow$):

$\dot{A}BC\dot{D}$	✓		$AB\dot{C}$	✓		AB	$\ast$
$ABC\dot{\overline{D}}$	✓		$\dot{A}B\dot{D}$	✓		BD	$\ast$
$\dot{A}B\overline{C}\dot{D}$	✓		$B\dot{C}D$	✓			
$AB\overline{C}\dot{\overline{D}}$	✓		$AB\dot{\overline{D}}$	✓			
$\dot{A}\overline{B}C\overline{D}$	✓		$AC\overline{D}$	$\ast$			
$\dot{\overline{A}}\dot{B}CD$	✓	$\longrightarrow$	$AB\dot{\overline{C}}$	✓	$\longrightarrow$		
$\dot{\overline{A}}B\overline{C}D$	✓		$B\dot{\overline{C}}D$	✓			
$\overline{A}\dot{\overline{B}}CD$	✓		$\overline{B}C\overline{D}$	$\ast$			
$\dot{\overline{A}}\overline{B}\dot{C}\overline{D}$	✓		$\dot{\overline{A}}BD$	✓			
$\overline{AB}\dot{\overline{C}}\overline{D}$	✓		$\overline{A}CD$	$\ast$			
			$\overline{AB}C$	$\ast$			
			$\overline{ABD}$	$\ast$			

Die mit $\ast$ bezeichneten Ausdrücke (die übriggebliebenen) bilden den vereinfachten, jedoch noch nicht minimalisierten Normalterm:

$$\alpha \mathrel{-\!\!\!\ast\!\!\!-} (A \wedge B) \vee (B \wedge D) \vee (A \wedge C \wedge \overline{D}) \vee (\overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge C \wedge D)$$
$$\vee(\overline{A} \wedge \overline{B} \wedge C) \vee (\overline{A} \wedge \overline{B} \wedge \overline{D})$$

Definition 28
Umfaßt eine Klausel einer vollständigen adjunktiven Normalform nur einen Primimplikanten, so heißt er **Kernimplikant**.
Die Adjunktion der Kernimplikanten heißt Kern und ist die bis auf die Reihenfolge der Adjunktionsglieder eindeutige minimale adjunktive Normalform.

Beispiel 26 (Quine-McCluskey)
Bestimmen des Kerns von α aus Beispiel 25 $K(\alpha)$.
Tabelle aus Primimplikanten und Klauseln:

	AB	BD	$AC\overline{D}$	$\overline{AB}C$	$\overline{ABD}$	$\overline{A}CD$	$\overline{B}C\overline{D}$	Primimplikanten
$ABCD$	×	×						
$ABC\overline{D}$	×		×					
$AB\overline{C}D$	×	×						
$AB\overline{CD}$	×							
$A\overline{B}C\overline{D}$			×				×	
$\overline{A}BCD$		×				×		
$\overline{A}B\overline{C}D$		×						
$\overline{AB}CD$				×		×		
$\overline{AB}C\overline{D}$				×	×		×	
$\overline{ABCD}$					×			

Klauseln der vollständigen adjungierten Normalform

Also $K(\alpha) = (A \wedge B) \vee (b \wedge D) \vee (\overline{A} \wedge \overline{B} \wedge \overline{D})$.

Mit den übrigen Primimplikanten neue Tabelle:

	$AC\overline{D}$	$\overline{AB}C$	$\overline{A}CD$	$\overline{B}C\overline{D}$	Primimplikanten, die nicht im Kern sind
$A\overline{B}C\overline{D}$	×			×	
$\overline{AB}CD$		×	×		

Klauseln der vollst. adj. Nf., die nicht vom Kern abgedeckt werden

Das Verfahren ist damit beendet; minimaler Normalterm von α:

$$\begin{aligned} \alpha \quad \Leftrightarrow \quad & K(\alpha) \vee (A \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge \overline{B} \wedge C) \\ & K(\alpha) \vee (A \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge C \wedge D) \end{aligned}$$

$$K(\alpha) \vee (\overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge \overline{B} \wedge C)$$
$$K(\alpha) \vee (\overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge C \wedge D)$$

Zu weiterführender Literatur zum Quine-McCluskey-Verfahren
siehe Literaturverzeichnis Anhang E.

Bemerkung 19
Die bisherige Logik, Aussagen- oder Junktorenlogik (propositional logik) ist zu schwach, um übliche Mathematik und Informatik zu formalisieren. Aufgrund des Mangels an „für alle“ und „es existiert“ reicht es nicht einmal für die (Aristotelische) Syllogistik.
Daher sei im folgenden ein Abriß der Prädikatenlogik oder Quantorenlogik (quantification theorie) gegeben. Die Formalisierung ist jedoch auch auf andere Weise möglich.

Definition 29
A (häufig Σ) sei eine Menge von Zeichen (Symbolen, Buchstaben), ein sogenannter **Zeichenvorrat.**
$(A, \leq)$ mit einer Wohlordnung $\leq$ heißt **Alphabet**.

α) Endliche Folgen, also n-Tupel über A heißen **Wörter** (Zeichenreihen, Symbolfolgen, Liste etc.) über A inclusive der leeren Folge $\varnothing$.
Statt $(a_1, \ldots, a_n)$ schreibt man meist $a_1 \ldots a_n$ mit $a_\nu \in A$ für $\nu \in \mathbb{A}_n$ und $n \in \mathbb{N}$.
Ein einelementiges Wort wird mit seinem Buchstaben identifiziert.
Die **Länge** $|w|$ eines Wortes w ist die Zahl seiner Glieder, also $|\varnothing| = 0$ und $|a_1 \ldots a_n| = n$, und $|w|_a$ gibt an, wie oft a in w vorkommt.

β) Die Menge der Wörter über A wird mit A^* bezeichnet und es sei $A^+ \risingdotseq A^* \setminus \{\varnothing\}$.

γ) Wörter u, v aus A^* werden **multipliziert**, **verkettet**, **konkateniert** zu $w = uv$ genannt.
Es sei $w = v$ bzw. u im Falle $u = \varnothing$ bzw. $v = \varnothing$, ferner für $u, v \in A^+$, etwa $u = a_1 \ldots a_m$ und $v = b_1 \ldots b_n$ mit $a_\mu, b_\nu \in A$ für $\mu \in \mathbb{A}_m, \nu \in \mathbb{A}_n$ und $m, n \in \mathbb{N}, w = a_1 \ldots a_m b_1 \ldots b_n$.

δ) Ein (algebraisches) Gebilde $(M, \cdot, e)$ heißt **Monoid**, falls $(M, \cdot)$ Halbgruppe und e das neutrale Element ist.

Beispiel 27

a) Mit $D = \{0, 1, 2, \ldots, 8, 9\}$ hat man in D^+ die Menge der nicht-negativen ganzen (Dezimal-)Zahlen mit führenden Nullen.
$(D \setminus \{0\})\, D^* \cup \{0\}$ liefert eine eindeutige Darstellung ohne führende Nullen (jedoch mit Null) von $\mathbb{N}_0$.

b) Für $A = \{|\}$ entspricht $A^+ = \{|, ||, |||, ||||, \ldots\}$ den natürlichen Zahlen.

c) Für $A = \{a, b\}$ mit $a \neq b$ ist A^3 die Menge der Wörter der Länge 3 über A, also $A^3 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$.

d) Monoide sind

I. $(\mathbb{N}_0, +, 0), (\mathbb{N}, \cdot, 1), (\mathbb{R}, +, 0), (\mathbb{R}, \cdot, 1)$;
$(R, +, 0)$ und $(R, \cdot, 1)$ für jeden Ring $(R, +, \cdot)$ mit 0 als Null und 1 als Eins

II. Jede Gruppe $(G, \star, e)$ mit e als neutralem Element von $\star$

III. $(P(M), \cap, M)$ und $(P(M), \cup, \emptyset)$ für jede Menge M; allgemeiner $(V, \wedge, 1)$ und $(V, \vee, 0)$ für jeden Verband $(V, \wedge, \vee)$ mit 1 als Eins und 0 als Null

Satz 49
Für jeden Zeichenvorrat A ist $(A^+, \text{Zeichen für Verkettung?}, \varnothing)$ ein Monoid.

Beweis: Übung!

Definition 30 (Syntax der Prädikatenlogik (quantification theory))
$Z \rightleftharpoons \{o, O, |, *, \neg, \wedge, \forall, \subset, \supset\}$ sei der Zeichenvorrat der Prädikatenlogik.

α) Die Wörter $o|, o||, o|||, \ldots$ heißen **Individuenvariable** und die Wörter
$O*|, O*||, \ldots, O**|, O**||, \ldots, O*** \, |, \ldots$,
die Elemente von $O\{*\}^+\{|\}^+$ heißen **Prädikatenvariable.**
Für eine Prädikatenvariable Π heißt $|\Pi|_*$ **Stellenzahl** von Π.

β) α heißt **Atomformel**, wenn es mit einer Prädikatenvariablen Π beginnt und von $|\Pi|_*$ Individuenvariablen gefolgt wird.

γ) I. Atomformeln sind Formeln.

II. Sind α und β Formeln, so auch $\neg\alpha$ und $(\alpha \wedge \beta)$.

III. Ist α eine Formel und ξ eine Individuenvariable, so ist $\forall\xi\alpha$ eine Formel.

IV. Genau die durch I. bis III. bestimmten Wörter sind Formeln.

Beispiel 28
Formeln sind

a) $\neg(\forall o| \; O*|| \; o| \;\; \wedge \;\; \neg O*|| \; o|)$, oder üblicherweise:
$\neg(\forall\xi \; \Pi\xi \;\; \wedge \;\; \neg\Pi\xi)$
$(\forall\xi \; \Pi\xi \;\; \rightarrow \;\; \Pi\xi)$

b) $\neg\neg\neg\forall o|| \; O**||| \; o||| \; o||$

Bemerkung 20
Als Abkürzungen benutzen wir $(\alpha \rightarrow \beta)$ statt $\neg(\alpha \wedge \neg\beta)$ und $\exists\xi\alpha$ statt $\neg\forall\xi\neg\alpha$.

Definition 31 (Semantik der Prädikatenlogik)

α) Ein **Individuenbereich** ist eine beliebige nichtleere Menge ω. Die Elemente von ω heißen **Individuen.** Ein n-stelliges **Prädikat** P über ω für $n \in \mathbb{N}$ ist eine Menge von n-Tupeln mit Elementen aus ω, also $P \subseteq \omega^n$.

β) Eine **Interpretation** i über ω ist eine Abbildung der Individuenvariablen und Prädikatenvariablen auf Individuen aus ω und Prädikate über ω mit $i(\Pi) \subseteq \omega^{|\Pi|_*}$ für jede Prädikatenvariable Π, also
$i \in \omega \cup P(\omega^+)^{o\{|\}^+ \cup O\{*\}^+\{|\}^+}$
mit $i\left(o\{|\}^+\right) \subseteq \omega$ und $i\left(O\{*\}^+\{|\}^+\right) \subseteq P(\omega^+)$ sowie $i(\Pi) \subseteq \omega^{|\Pi|_*}$ für $\Pi \in O\{*\}^+\{|\}^+$.
$i \stackrel{\xi}{=} j \quad (i = j$ bis auf $\xi)$ bedeutet, daß i und j Interpretationen über demselben Individuenbereich sind und daß sich i und j höchstens für das Argument ξ unterscheiden.

γ) i, j seien Interpretationen über ω, ferner α und β Formeln und ξ eine Individuenvariable.

I. Eine Atomformel $\Pi\xi_1, \ldots, \xi_n$ gilt bei i genau im Falle
$(i(\xi_1), i(\xi_2), \ldots, i(\xi_n)) \in i(\Pi)$.

II. $\neg\alpha$ gilt bei i genau dann, wenn α bei i nicht gilt.

III. $(\alpha \wedge \beta)$ gilt bei i genau dann, wenn α und β bei i gelten.

IV. $\forall\xi\alpha$ gilt bei i genau dann, wenn α bei jedem j mit $i \stackrel{\xi}{=} j$ gilt.

Beispiel 29
Sei $\xi \rightleftharpoons o|$, $\eta \rightleftharpoons o||$, $\Pi \rightleftharpoons O*|$, $\Lambda \rightleftharpoons O{*}{*}|$, $K \rightleftharpoons \{(x,y) \in \mathbb{N} \times \mathbb{N}; x < y\}$ und i eine Interpretation über $\mathbb{N}$, für die insbesondere
$i(\xi) = 17$, $i(\eta) = 100$, $i(\Pi) = P \subseteq \omega$ und $i(\Lambda) = K$.
Bei i gelten dann
$\Pi\xi$,
$\neg\Pi\eta$ und
$\forall\xi\,(\Pi\xi \rightarrow \exists\eta\,(\Pi\eta \wedge \Lambda\xi\eta))$,
das heißt: „Es gibt unendlich viele Primzahlen“, Euklid.

Satz 50
i sei Interpretation.

a) „$(\alpha \rightarrow \beta)$ gilt bei i“ ist äquivalent zu „wenn α bei i gilt, dann auch β“.

b) „$\exists\xi\alpha$ gilt bei i“ ist äquivalent zu „es gibt ein j mit $i \stackrel{\xi}{=} j$ bei dem α gilt“.

Beweis:

a) $\Rightarrow$: Also gelte $(\alpha \rightarrow \beta)$ und α bei i, dann gilt β bei i.
Denn sonst gälte $\neg\beta$, also $(\alpha \wedge \neg\beta)$ im Widerspruch zur Gültigkeit von $\neg(\alpha \wedge \neg\beta) = (\alpha \rightarrow \beta)$.

$\Leftarrow$: Also gelte β, wenn α bei i gilt. Dann gilt $(\alpha \rightarrow \beta)$.
Denn sonst gälte $\neg(\alpha \wedge \neg\beta)$ nicht, also $(\alpha \wedge \neg\beta)$ und daher α und $\neg\beta$ im Widerspruch zur Gültigkeit von β, wenn α gilt.

b) $\exists\xi\alpha$ gilt bei i genau dann,

wenn $\neg\forall\xi\neg\alpha$ bei i gilt,

wenn $\forall\xi\neg\alpha$ bei i nicht gilt, wenn es nicht wahr ist, daß $\neg\alpha$ bei jedem j mit $i \stackrel{\xi}{=} j$ gilt,

wenn es nicht wahr ist, daß α bei j mit $i \stackrel{\xi}{=} j$ nicht gilt,

wenn es (mindestens) ein j gibt mit $i \stackrel{\xi}{=} j$, bei dem α gilt.

Definition 32
α, β seien Formeln und $\mathcal{M}$ eine Menge von Formeln.

α) $\mathcal{M}$ gilt bei i genau dann, wenn jedes Element von $\mathcal{M}$ bei i gilt.

β) α heißt **allgemeingültig**, kurz $\Vdash \alpha$, wenn α bei jeder Interpretation über einem beliebigen Individuenbereich gilt.

γ) α **folgt aus** $\mathcal{M}$, kurz $\mathcal{M} \Vdash \alpha$, wenn α bei jeder Interpretation gilt, bei der $\mathcal{M}$ gilt.
Für $\{\alpha\} \Vdash \beta$ schreiben wir auch $\alpha \Vdash \beta$.

Satz 51
$\mathcal{M}$, $\mathcal{N}$ seien Formelmengen, α, β, γ Formeln und ξ eine Individuenvariable.

a) $\emptyset \Vdash \alpha \Longleftrightarrow \Vdash \alpha$

b) $\alpha \in \mathcal{M} \Longrightarrow \mathcal{M} \Vdash \alpha$

c) $\mathcal{M} \Vdash \alpha \Longrightarrow (\mathcal{M} \cup \mathcal{N}) \Vdash \alpha$

d) $(\alpha \Vdash \beta \ \wedge \ \beta \Vdash \gamma) \Longrightarrow \alpha \Vdash \gamma$

e) $(\mathcal{M} \Vdash \alpha \ \wedge \ \mathcal{N} \Vdash \beta) \Longrightarrow (\mathcal{M} \cup \mathcal{N}) \Vdash (\alpha \wedge \beta)$

f) $(\mathcal{M} \Vdash (\alpha \to \beta) \ \wedge \ \mathcal{N} \Vdash \beta) \Longrightarrow (\mathcal{M} \cup \mathcal{N}) \Vdash (\alpha \wedge \beta)$

g) $\mathcal{M} \Vdash (\alpha \to \beta) \Longleftrightarrow (\mathcal{M} \cup \{\alpha\}) \Vdash \beta$

h) $(\forall \xi \alpha) \Vdash \alpha$

Beweis:

a) – d) Übung (folgt aus Definition)

e) $(\mathcal{M} \cup \mathcal{N})$ gelte bei i.
$$\left.\begin{array}{l}\text{Wegen } \mathcal{M} \Vdash \alpha \text{ gilt } \alpha \text{ bei i} \\ \text{Wegen } \mathfrak{N} \Vdash \beta \text{ gilt } \beta \text{ bei i}\end{array}\right\} \text{ also gilt } (\alpha \wedge \beta) \text{ bei i.}$$

f) $(\mathcal{M} \cup \mathcal{N})$ gelte bei i.
Wegen $\mathfrak{N} \Vdash \alpha$ gilt α bei i und wegen $\mathcal{M} \Vdash (\alpha \to \beta)$ damit β.

g) $\Rightarrow$: $(\mathcal{M} \Vdash (\alpha \to \beta) \ \wedge \ \{\alpha\} \Vdash \alpha) \Longrightarrow (\mathcal{M} \cup \{\alpha\}) \Vdash \beta$
$\Leftarrow$: $(\mathcal{M} \cup \{\alpha\}) \Vdash \beta$ und $\mathcal{M}$ gelte bei i.
Wenn nun α bei i gilt, dann auch β und nach Satz 50a) daher $(\alpha \to \beta)$ bei i.

h) $\forall \xi \alpha$ gelte bei i.
Dann gilt α bei jedem j mit $i \stackrel{\xi}{=} j$, also a fortiori bei i.

Definition 33
α und β seien Formeln und $\mathcal{M}$ eine Formelmenge der Prädikatenlogik sowie ξ und η Individuenvariable.

α)
 I. Ist α Atomformel, kommen alle Individuenvariable von α in α **frei** vor.
 II. η kommt in $\neg\alpha$ frei vor genau dann, wenn η in α frei vorkommt.
 III. η kommt in $(\alpha \wedge \beta)$ frei vor genau dann, wenn η in α und β frei vorkommt.
 IV. η kommt in $\forall\xi\alpha$ frei vor genau dann, wenn η in α frei vorkommt und $\xi \neq \eta$.

β) η kommt in $\mathcal{M}$ frei for, wenn η in wenigstens einem Element von $\mathcal{M}$ frei vorkommt.

γ) Kommt η in α bzw. $\mathcal{M}$ vor, aber nicht frei, so kommt η in α bzw. $\mathcal{M}$ **gebunden** vor.

Beispiel 30
ξ kommt in $\Pi\xi \to \exists\eta\,(\Pi\eta \wedge \Lambda\xi\eta)$ frei
und in $\forall\xi\,(\Pi\xi \to \exists\eta\,(\Pi\eta \wedge \Lambda\xi\eta))$ gebunden vor.

Satz 52
Kommt die Individuenvariable η in der Formel α nicht frei vor und gilt $i \overset{\eta}{=} j$, so gilt α bei i genau dann, wenn α bei j gilt.

Beweis: Induktion über Formelaufbau:

$\Rightarrow$: Wegen $i \overset{\eta}{=} j$ und $\eta \neq \xi_1, \ldots, \xi_n$ — denn sonst käme ja η in α frei vor — ist $i\,(\xi_\nu) = j\,(\xi_\nu)$ für $\nu \in \mathbb{A}_n$ und $i\,(\Pi) = j\,(Pi)$, womit gilt:
$(i\,(\xi_1)\,, i\,(\xi_2)\,, \ldots, i\,(\xi_n)) \in i\,(Pi) \Longleftrightarrow (j\,(\xi_1)\,, j\,(\xi_2)\,, \ldots, j\,(\xi_n)) \in j\,(Pi)$.
Da $\alpha = \Pi\xi_1 \ldots \xi_n$ bei i gilt, gilt α auch bei j.

$\Leftarrow$: Die Behauptung gilt für $\neg\alpha$, wenn sie für α gilt: Kommt η in $\neg\alpha$ nicht frei vor, so auch nicht frei in α. Somit sind äquivalent:
$\neg\alpha$ gilt bei i
α gilt nicht bei i
α gilt nicht bei j
$\neg\alpha$ gilt bei j.

Satz 53
ξ komme in $\mathcal{M} \cup \{\beta\}$ nicht frei vor und es sei $\mathcal{M} \cup \{\alpha\} \Vdash \beta$.
Dann gilt $\mathcal{M} \cup \{\exists\xi\alpha\} \Vdash \beta$.

Beweis: Aufgabe 23.

Definition 34 (Substitution)
$\alpha, \alpha', \beta, \beta', \gamma$ seien Formeln, ξ, η, η' Individuenvariable und $\mathcal{M}$, $\mathfrak{M}'$ Formelmengen der Prädikatenlogik.
Ersetzt man in α überall η, wo η nicht „im Wirkungsbereich" einer Quantifizierung von η vorkommt durch η', und erscheint kein η' „im Wirkungsbereich" einer Quantifizierung von η', so ist das so entstandene α' aus α durch eine **Substitution** von η' für η, kurz $\mathrm{Sub}_{\alpha\eta\eta'\alpha'}$ hervorgegangen. ($\mathrm{Sub}_{\alpha\eta\eta'\alpha'}$ ist eine Aussage!)
Genauer:

α) Ist α Atomformel, so gelte $\mathrm{Sub}_{\alpha\eta\eta'\alpha'}$ genau dann, wenn α' aus α dadurch entsteht, daß in α überall η durch η' ersetzt wird.

β) $\mathrm{Sub}_{\neg\alpha\eta\eta'\beta} \rightleftharpoons \exists\alpha' \; \big(\mathrm{Sub}_{\alpha\eta\eta'\alpha'} \wedge \beta = \neg\alpha'\big)$.

γ) $\mathrm{Sub}_{(\alpha\wedge\beta)\eta\eta'\gamma} \rightleftharpoons \exists\alpha'\beta' \; \big(\mathrm{Sub}_{\alpha\eta\eta'\alpha'} \wedge \mathrm{Sub}_{\beta\eta\eta'\beta'} \wedge \gamma = (\alpha' \wedge \beta')\big)$.

δ) $\begin{array}{ll} \mathrm{Sub}_{(\forall\xi\alpha)\eta\eta'\beta} & \rightleftharpoons \eta \text{ kommt nicht frei in } \forall\xi\alpha \text{ vor } \wedge \; \beta = \forall\xi\alpha \\ & \rightleftharpoons \eta \text{ kommt frei in } \forall\xi\alpha \text{ vor } \wedge \; \eta' \neq \xi \; \wedge \; \exists\alpha' \big(\mathrm{Sub}_{\alpha\eta\eta'\alpha'} \wedge \beta = \forall\xi\alpha'\big) \end{array}$

ε) $\mathrm{Sub}_{\mathcal{M}\eta\eta'\mathcal{M}'} \rightleftharpoons \forall\alpha \in \mathcal{M} \; \exists\alpha' \in \mathcal{M}' \; \big(\mathrm{Sub}_{\alpha\eta\eta'\alpha'} \; \wedge$ jedes Element von $\mathcal{M}$ entsteht so $\big)$

Beispiel 31
(vgl. B 29)
Mit $\alpha \rightleftharpoons \exists\eta \; (\Pi\eta \wedge \Lambda\xi\eta)$, $\beta \rightleftharpoons \exists\eta \; (\Pi\eta \wedge \Lambda\nu\eta)$ und $\gamma \rightleftharpoons \exists\zeta \; (\Pi\zeta \wedge \Lambda\xi\zeta)$ gilt offenbar $\mathrm{Sub}_{\alpha\xi\nu\beta}$, $\mathrm{Sub}_{\alpha\eta\zeta\alpha}$ und $\neg\mathrm{Sub}_{\alpha\eta\zeta\gamma'}$.

Satz 54
Unter den Voraussetzungen

- $\mathrm{Sub}_{\alpha\eta\eta'\alpha'}$,
- $i \overset{\eta}{=} i'$ und
- $i\,(\eta) = i'\,(\eta')$

gilt α bei i genau dann, wenn α' bei i' gilt.

Beweis: Induktion über Formelaufbau; Übung!

Satz 55
$\mathrm{Sub}_{\mathcal{M}\eta\eta'\mathcal{M}'} \;\wedge\; \mathrm{Sub}_{\alpha\eta\eta'\alpha'} \;\wedge\; \mathcal{M} \Vdash \alpha \implies \mathcal{M}' \Vdash \alpha'$

Beweis:
i' sei Interpretation, bei der $\mathfrak{M}'$ gilt und i Interpretation mit $i \overset{\eta}{=} i'$ und $i\,(\eta) = i'\,(\eta')$. Nach Satz 44 gilt $\mathcal{M}$ bzw. α bei i genau dann, wenn $\mathfrak{M}'$ bzw. α' bei i' gilt. Daher nacheinander:

$$\begin{array}{rll} \mathcal{M}' & \text{gilt bei} & i' \\ \mathcal{M} & \text{gilt bei} & i \\ \alpha & \text{gilt bei} & i \quad (\text{ wegen } \mathcal{M} \Vdash \alpha) \\ \alpha' & \text{gilt bei} & i' \end{array}$$

Bemerkung 21
Für die in Definition 30 definierten, gelegentlich durch Konstante, „=“ oder Funktionsvariable angereicherte Prädikatenlogik, deren Semantik in Definition 31 festgelegt wurde, lassen sich (Ableitungs-)**Kalküle** K angeben.
Gewisse Formeln oder Folgen von Formeln der Prädikatenlogik werden als Axiome ausgezeichnet. Durch sogenannte (Ableitungs-, Schluß-)Regeln, etwa dem „modus ponens“, ist vorgeschrieben, wie man von einer Formelmenge $\mathcal{M}$ zu einer Formel α gelangen kann, kurz $\mathcal{M} \overset{K}{\vdash} \alpha$.
K läßt sich so wählen, daß K sowohl **korrekt** (**konsistent**) als auch **vollständig** ist, d. h., daß für

jede Formel α und jede Formelmenge $\mathcal{M}$ gilt:

$$\begin{array}{lcll} \mathcal{M} \overset{K}{\vdash} \alpha & \Longrightarrow & \mathcal{M} \Vdash \alpha & \text{(korrekt)} \\ \mathcal{M} \Vdash \alpha & \Longrightarrow & \mathcal{M} \overset{K}{\vdash} \alpha & \text{(vollständig)} \end{array}$$

Wir geben hier nur kurz ein solches K an, verzichten aber auf den Nachweis von Korrektheit und Vollständigkeit (siehe Gödel 1930).

Definition 35

α) Der —— bedeutet: Sind die über —— stehenden Zeichenreihen schon abgeleitet, darf zu der unter —— stehenden Zeichenreihe übergegangen werden.
$\mathrm{Sub}_{\smile\alpha\xi\nu\frown\beta}$ heiße, daß $\mathrm{Sub}_{\alpha\xi\nu\beta}$ und jedes Glied von $\smile\alpha$ durch Substitution non η für ξ in das entsprechende Glied von $\frown\beta$ übergeht.
$\smile$ und $\frown$ sind endliche Folgen von Formeln, $\smile\alpha$ und $\frown\beta$ solche Folgen, die mit α bzw. β enden.
Definition der Regeln:

I. $\alpha\alpha$

II.
$$\frac{\smile\alpha \quad \frown\beta}{\smile\frown(\alpha\wedge\beta)}$$

III.
$$\frac{\smile\frown(\alpha\wedge\beta)}{\smile\alpha}$$

IV.
$$\frac{\smile\frown(\alpha\wedge\beta)}{\frown\beta}$$

V.
$$\frac{\smile\alpha\beta \quad \frown\neg\alpha\beta}{\smile\frown\beta}$$

VI.
$$\frac{\smile\alpha \quad \frown\neg\alpha}{\smile\frown\beta}, \qquad \text{ex falso quodlibet}$$

VII.
$$\frac{\smile\forall\xi\alpha}{\smile\alpha}$$

VIII.
$$\frac{\smile\alpha}{\smile\forall\xi\alpha}, \qquad \text{falls } \xi \text{ nicht frei in } \smile \text{ vorkommt}$$

IX.
$$\frac{\smile\alpha}{\frown\beta}, \qquad \text{falls } \mathrm{Sub}_{\smile\alpha\xi\eta\frown\beta}$$

β) Ist $\alpha_1\ldots\alpha_t$ mit $t\in\mathbb{N}$ mit den Regeln aus α) ableitbar, schreiben wir $\vdash\alpha_1\ldots\alpha_t$ oder $\alpha_1\ldots\alpha_{t-1}\vdash\alpha_t$ (falls $t>1$).

γ) Für eine Formelmenge $\mathcal{M}$ schreiben wir $\mathcal{M}\vdash\alpha$, falls es $\alpha_1\ldots\alpha_t\in\mathcal{M}$ mit $t\in\mathbb{N}_0$ und $\alpha_1\ldots\alpha_t\vdash\alpha$ gibt.

Beispiel 32

a)

$(\alpha\wedge\neg\alpha)$	$(\alpha\wedge\neg\alpha)$	noch keine inhaltliche Interpretation!
$(\alpha\wedge\neg\alpha)$	α	Übergang auf die Teile der Konjunktion
$(\alpha\wedge\neg\alpha)$	$\neg\alpha$	

Widerspruch, d. h. beliebige Formel herleitbar (ex falso quodlibet):

$(\alpha\wedge\neg\alpha)$	$\neg(\alpha\wedge\neg\alpha)$	$2\times$ die Formel $\frac{\substack{\alpha\beta\\ \neg\alpha\beta}}{\ldots\beta}$
$\neg(\alpha\wedge\neg\alpha)$	$\neg(\alpha\wedge\neg\alpha)$	

also: $\vdash(\alpha\to\neg\alpha)$

b)

$\forall\xi\,(\alpha\wedge\beta)$	$\forall\xi\,(\alpha\wedge\beta)$	
$\forall\xi\,(\alpha\wedge\beta)$	$(\alpha\wedge\beta)$	
$\forall\xi\,(\alpha\wedge\beta)$	α	
$\forall\xi\,(\alpha\wedge\beta)$	$\forall\xi\alpha$	, da ξ nicht frei in $\forall\xi\,(\alpha\wedge\beta)$ vorkommt

also: $\forall\xi\,(\alpha\wedge\beta)\vdash\forall\xi\alpha$

Bemerkung 22
Trotz $\mathcal{M}\Vdash\alpha\iff\mathcal{M}\vdash\alpha$ (siehe Gödel 1930) ist die Prädikatenlogik im Gegensatz zur Aussagenlogik **unentscheidbar**,
d. h. es gibt keinen Algorithmus, mittels dessen man für jede Formel α entscheiden kann, ob sie allgemeingültig ist, also $\Vdash\alpha$ gilt, und nach Satz 51g),a) gibt es daher auch keinen Algorithmus, der für jede endliche Formelmenge $\mathcal{M}$ und α entscheidet, ob $\mathcal{M}\Vdash\alpha$ gilt.
Dennoch gibt es Algorithmen, die genau dann abbrechen, wenn $\mathcal{M}\Vdash\alpha$ gilt, diese sind allerdings sehr zeitaufwendig, vermutlich exponentiell.
In praxi, z. B. in der Artifiziellen Intelligenz (AI) hat man es aber vielfach mit Problemen der Bauart

$$\forall\ldots(\alpha_1\wedge\ldots\wedge\alpha_m\to\beta)\;\Vdash\;\exists\ldots(\gamma_1\wedge\ldots\wedge\gamma_n) \tag{70}$$

mit Atomformeln $\alpha_1,\ldots,\alpha_m,\beta,\gamma_1,\ldots,\gamma_n$ zu tun.
Dazu:

Definition 36
Seien $\alpha_1, \ldots, \alpha_m, \beta, \beta_1, \ldots, \beta_n$ mit $m, n \in \mathbb{N}_0$ Atomformeln der Prädikatenlogik.
Eine Formel $\alpha_1 \wedge \ldots \wedge \alpha_m \to \beta_1 \vee \ldots \vee \beta_n$, kurz
$\bigwedge_{\mu=1}^{m} \alpha_\mu \to \bigvee_{\nu=1}^{n} \beta_\nu$ heißt Gentzenformel,
speziell für $m \leq 1$ Hornformel,
die dazu äquivalente Formel:

$\beta \vee \neg\alpha_1 \vee \ldots \vee \alpha_m$	(kurz $\beta : -\alpha_1, \ldots, \alpha_m$)
β	$(\beta : -)$
$\neg\alpha_1 \vee \ldots \neg\alpha_m$	$(: -\alpha_1, \ldots, \alpha_m)$
$\perp$	$(: -)$

heißt Hornklausel.

Bemerkung 23
Es gibt ein Verfahren, die sogenannte Resolution, die zu jeder endlichen Formelmenge $\mathcal{M}$ der linken Seite von (70) entscheidet, ob $\mathcal{M} \Vdash \alpha$ gilt, wobei α eine Formel der rechten Seite von (70) ist, und überdies Beispiele, d. h. Terme für die Existenz der in α behaupteten Individuen liefert. Das Verfahren ist also in dem in Bemerkung 19 beschriebenen Sinn korrekt und vollständig.
Dabei spielt die sogenannte Unifikation eine entsprechende Rolle, d. h. zu den Atomformeln α und β mit Individuenvariablen ξ und ν ist eine Ersetzung ζ, ϑ zu finden mit
$\mathrm{Sub}_{\alpha\xi\zeta\alpha'}$, $\mathrm{Sub}_{\beta\eta\vartheta\beta'}$ und $\alpha' = \beta'$.
Genaueres siehe Literatur und Spezialvorlesungen.

Kapitel 2

Graphen

2.1 Einführung

Beispiel 33

a) Königsberger Brückenproblem nach Leonhard Euler

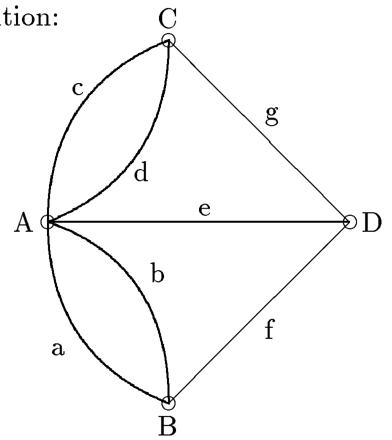
c d C g

A (Kneiphof) e D

a

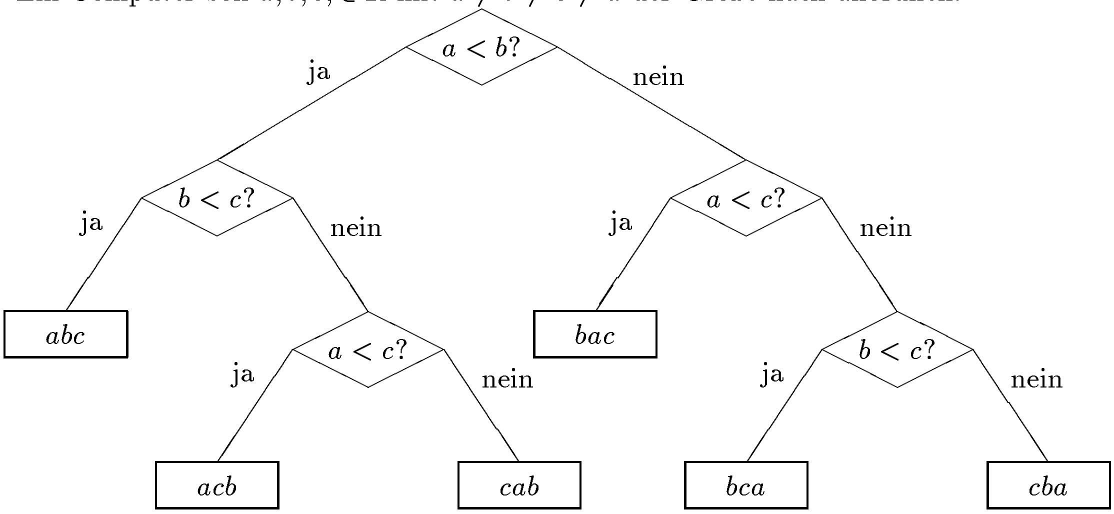
b B f

Ist ein Weg möglich, der jede Brücke genau einmal enthält?
Abstraktion:

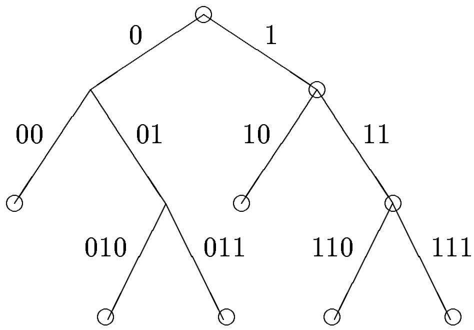


Andere Einkleidungen sind dabei möglich, etwa: „In einem Pipelinesystem soll ein Prüfgerät so zwischen Stationen hin- und hergeschoben werden, daß jede Pipeline genau einmal befahren wird.“

b) Entscheidungsbaum
Ein Computer soll $a, b, c, \in \mathbb{R}$ mit $a \neq b \neq c \neq a$ der Größe nach anordnen:

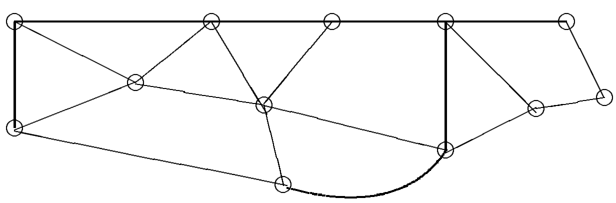


Abstraktion:



Allgemeiner: Jedes Flußdiagramm, jeder Programmlaufplan, auch etwa Material- und Geldströme in der Wirtschaft lassen sich graphentheoretisch behandeln.

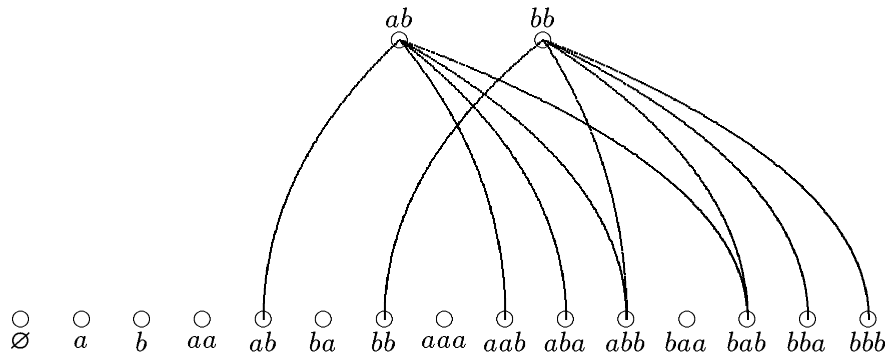
c) Vierfarbensatz
Die Frage eines Studenten an de Morgan, der sie am selben Tag Hamilton mitteilte: Reichen vier Farben aus, um eine Fläche vollständig zu färben, sodaß an jeder Kante ausschließlich verschiedene Farben zusammentreffen?



Drei Farben reichen im allgemeinen nicht aus, jedoch stets vier.
Beweis: K. Appel, W. Haken: „Every planar map is four colorable“ Part 1, Discharging Illinois, J. Math. 21 (1977), S. 429–490; J. Koch ebd. Part 2, Reducibility, ebd. S.

491–567

d) Jede (binäre) Relation, insbesondere jede Funktion, läßt sich (im Prinzip) durch ein Pfeildiagramm darstellen.
Für $u, v \in A^*$, etwa mit $A = \{a, b\}$ und $a \neq b$ sei $u \leq v$ definiert durch $\varnothing \leq v$ und für $v = a_1 \dots a_n$ mit $a_\nu \in A$ für $\nu \in \mathbb{A}_n$ und $n \in \mathbb{N}$ durch
$\exists m \in \mathbb{A}_n \ \exists \nu_1 \dots \nu_m \in \mathbb{A}_n : \ \nu_1 < \nu_2 < \dots < \nu_m \ \wedge \ u = a_{\nu_1} a_{\nu_2} \dots a_{\nu_m}$,
etwa:



Definition 37 (Potenzmenge, Grad, Ecken, Kanten, inzidieren, adjazent, Ordnung, Schlingen, Mehrfachkanten, schlicht)

α) Für eine Menge M sei
$P_n(M) \rightleftharpoons \{X \subseteq M; |X| = n; n \in \mathbb{N}_0\}$ die **Potenzmenge** von M.
Speziell ist also $P_1(M) = \{\{x\}; x \in M\}$ (singletons)
und $P_0(M) = \{\emptyset\}$.

β) Ein Tripel $\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ aus einer Menge $\mathcal{E}$, einer Menge $\mathcal{K}$ und einer Abbildung φ heißt (ungerichteter) **Graph** im Falle
$\mathcal{E} \cap \mathcal{K} = \emptyset$
und
$\varphi \in (P_1(\mathcal{E}) \cup P_2(\mathcal{E}))^{\mathcal{K}}$.

I. Die Elemente von $\varepsilon(\mathcal{G}) \rightleftharpoons \mathcal{E}$ werden **Ecken** oder **Knoten**, Punkte, Elemente (vertices, points, nodes, junctions) von $\mathcal{G}$ genannt und die von $\kappa(\mathcal{G}) \rightleftharpoons \mathcal{K}$ **Kanten**, **Linien** oder Elemente (lines, branches) von $\mathcal{G}$.

II. Seien $E, F \in \mathcal{E}$ und $h, k \in \mathcal{K}$.
Im Falle $E \in \varphi(k)$ sagt man, E **inzidiert** mit k oder E liegt auf oder an k oder E stößt in E.
Für $E, F \in \varphi(k)$ mit $E \neq F$ sagt man, k verbindet E und F, oder E und E sind **Nachbarn**, **adjazent** bzgl. k, kurz: $E \sim_k F$ oder $E \sim F$;
analog im Falle $\varphi(h) \cap \varphi(k) \neq \emptyset$, etwa $E \in \varphi(h) \cap \varphi(k)$ mit $h \neq k$, daß h und k **Nachbarn**, **adjazent** bzgl. E sind, kurz $h \sim_E k$ oder $h \sim k$.
Ferner sei
$\tilde{k} = \varphi(k)$ mit $k \in \mathcal{K}$
und
$\tilde{E} = \{k \in \mathcal{K}; E \in \varphi(k)\}$ mit $E \in \mathcal{E}$.

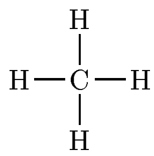
III. $o(\mathcal{G}) \rightleftharpoons |\mathcal{E}|$ heißt die **Ordnung** von $\mathcal{G}$ und $\mathcal{G}$ **endlich** falls $o(\mathcal{G}), |\mathcal{K}| \in \mathbb{N}_0$ sind.

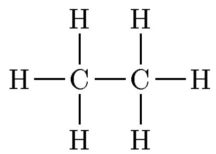
IV. Eine Kante s heißt **Schlinge** (Schleife, loop) von $\mathcal{G}$ im Falle
$|\tilde{s}| = |\varphi(s)| = 1$;
$\sigma(E)$ sei die Menge der Schlingen durch $E \in \mathcal{G}$ und
$\sigma(\mathcal{G}) \rightleftharpoons \bigcup_{E \in \mathcal{G}} (E)$.
Man sagt, $\mathcal{G}$ habe **Mehrfachkanten** (zwischen E und F) im Falle
$\exists E, F \in \mathcal{G} : \ E \neq F \ \wedge \ |\tilde{E} \cap \tilde{F}| = |\varphi^{-1}\{E, F\}| > 1.$

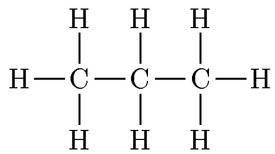
V. Ein schlingenloser Graph ohne Mehrfachkanten heißt **schlicht** (einfach).

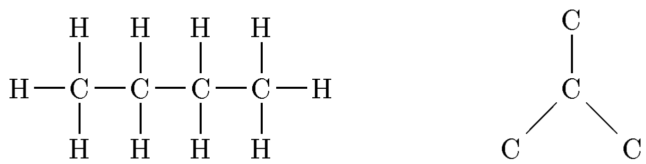
Beispiel 34
Schlichte Graphen sind:

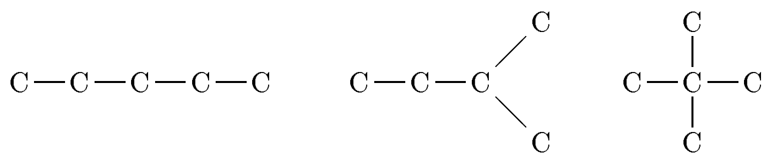
a)

Methan  CH_4

Ethan  C_2H_6

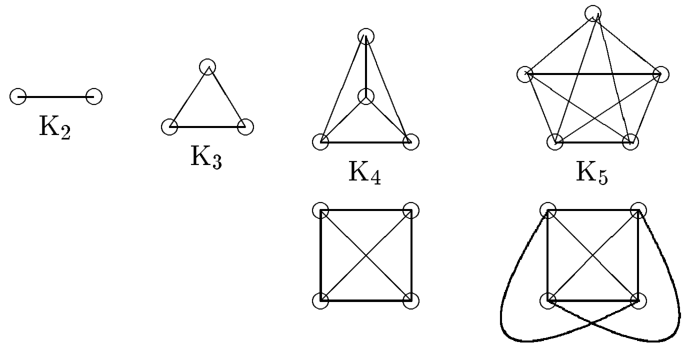
Propan  C_3H_8

Butane  C_4H_{10}

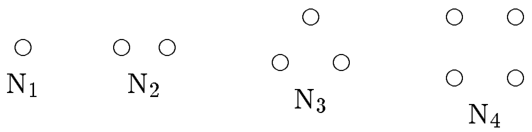
Pentane  C_5H_{12}

Wieviele Isomere gibt es bei C_nH_{2n+2}?
(Programm zur Isomerenbestimmung u. a. von A. Kerber, Softwarepreis 1993.)

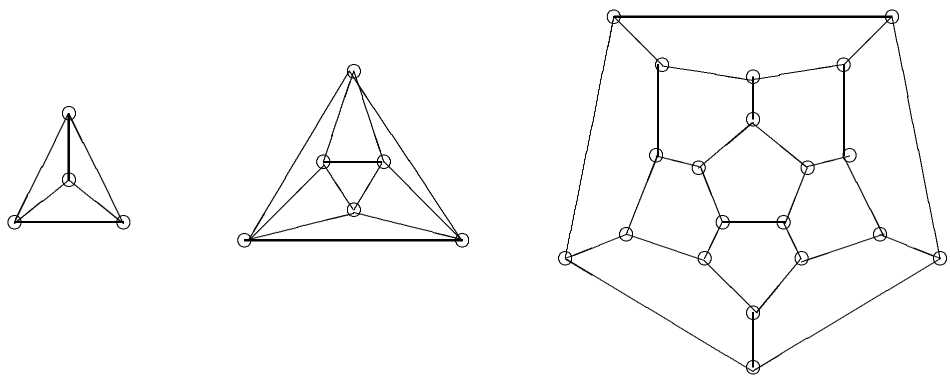
b)



c)



d) Projektion eines regelmäßigen Polyeders:
Tetraeder: Oktaeder: Dodekaeder:



Bemerkung 24
Für einen schlichten Graphen $(\mathcal{E}, \mathcal{K}, \varphi)$ gilt $\varphi: \ \mathcal{K} \rightarrowtail P_2(\mathcal{E})$, weshalb gelegentlich einfach $\mathcal{K} \subseteq P_2(\mathcal{E})$ und damit $\varphi = 1_{\mathcal{K}}$ genommen und $(\mathcal{E}, \mathcal{K})$ statt $(\mathcal{E}, \mathcal{K}, \varphi)$ geschrieben wird.

Satz 56
Für die Kantenzahl k eines schlichten Graphen der Ordnung n (n Ecken) gilt:

$$0 \leq k \leq \binom{n}{2}$$

und für die Ordnung n eines schlichten Graphen der Kantenzahl k entsprechend

$$n \geq \frac{1}{2}(1 + \sqrt{8k+1}).$$

Beweis:
Maximal können irgendzwei Ecken aus $\mathcal{E} = \varepsilon(S)$ eines schlichten Graphen S der Ordnung n durch eine Kante verbunden werden, das sind aber gerade $\binom{n}{2}$ Möglichkeiten.
Andere Variante: Nach Bemerkung 24 kann für $S = (\mathcal{E}, \mathcal{K}, \varphi)$ auch $\mathcal{K} \subseteq P_2(\mathcal{E})$ genommen werden. k ist genau dann maximal, wenn $|\mathcal{K}|$ maximal, also $\mathcal{K} = P_2(\mathcal{E})$ und mithin $|\mathcal{K}| = |P_2(\mathcal{E})| = \binom{n}{2}$ ist.
Rest: Übung.

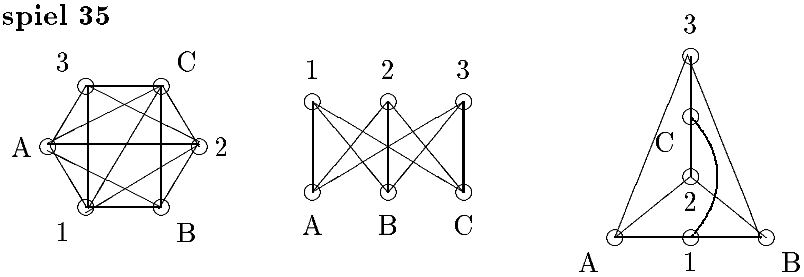
Definition 38
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei ein Graph.

α) Sei $\mathcal{G}' = (\mathcal{E}', \mathcal{K}', \varphi')$ Graph und $h \rightleftharpoons (f, g)$ mit $f : \mathcal{E} \rightarrowtail\!\!\!\twoheadrightarrow \mathcal{E}'$ und $g : \mathcal{K} \rightarrowtail\!\!\!\twoheadrightarrow \mathcal{K}'$.
h heißt **Isomorphismus** von $\mathcal{G}$ auf $\mathcal{G}$', kurz $h : \mathcal{G} \overset{\simeq}{\rightarrowtail\!\!\!\twoheadrightarrow} \mathcal{G}'$ und $\mathcal{G}$ **isomorph** zu $\mathcal{G}$', kurz $\mathcal{G} \simeq \mathcal{G}'$ im Falle

$$\forall E \in \mathcal{E}\ \forall k \in \mathcal{K} :\ E \in \varphi(k) \Longleftrightarrow f(E) \in \varphi'(g(k)).$$

β) Ein Isomorphismus von $\mathcal{G}$ auf $\mathcal{G}$ heißt **Automorphismus** von $\mathcal{G}$, $\mathcal{G}$ ist **automorph** $\mathcal{G}$.

Beispiel 35



Satz 57

a) $\simeq$ ist eine Äquivalenzrelation auf der Klasse aller Graphen.

b) Die Automorphismen eines Graphen $\mathcal{G}$ bilden bzgl. dem Abbildungsprodukt eine Gruppe, die **Automorphismengruppe** von $\mathcal{G}$.

Beweis: Übung.

Definition 39 (Nullgraph, vollständig)
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph.

α) $\mathcal{G}$ heißt **Nullgraph** im Falle $\mathcal{K} = \emptyset$.
Die Isomorphieklasse der Nullgraphen der Ordnung n wird mit N_n bezeichnet (vgl Beispiel 34c)).

β) $\mathcal{G}$ heißt **vollständig**, falls $\mathcal{G}$ schlichter Graph mit maximaler Kantenanzahl ist.
Die Isomorphieklasse der vollständigen Graphen dr Ordnung n wird mit K_n (nach Kuratowski) bezeichnet (vgl. Beispiel 34b)).

2.2 Grade

Definition 40 (Grad, regulär)
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph.

α) Für $E \in \mathcal{E}$ sei

$$\gamma(E) \rightleftharpoons |\tilde{E}| + |\varsigma(E)|$$

der **Grad** (degree, valency) von E.

β) Ist $\mathcal{G}$ schlichter Graph mit $\exists r \ \forall E \in \mathcal{E}: \ \gamma(E) = r$ heißt $\mathcal{G}$ **regulär** vom Grad r oder r-**regulär** und r der Grad von $\mathcal{G}$, kurz $\gamma(\mathcal{G}) = r$.
Ein 2-regulärer Graph wird auch **binär** (bivalent), ein 3-regulärer auch **kubisch** (trivalent) etc. genannt.

Satz 58
Ein endlicher schlichter Graph mit mindestens zwei Ecken hat mindestens zwei Ecken gleichen Grades.

Beweis:
Sei $\mathcal{G}$ schlichter Graph mit $\mathcal{E} = \varepsilon(\mathcal{G})$ und $n \rightleftharpoons |\mathcal{E}| \in \mathbb{N} \setminus \{1\}$.
Dann hat man $\gamma(\mathcal{E}) \in \mathbb{A}_{n-1} \cup \{0\}$ für jedes $E \in \mathcal{E}$. Wegen

$$\exists A \in \mathcal{E}: \ \gamma(A) = 0 \Longrightarrow \forall E \in \mathcal{E}: \ \gamma(E) < n-1$$

gilt somit

$$\forall E \in \mathcal{E}: \ \gamma(E) \in \mathbb{A}_{n-1} \ \vee \ \forall E \in \mathcal{E}: \ \gamma(E) \in \mathbb{A}_{n-2} \cup \{0\}$$

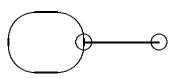
also $|\mathcal{E}| = n$ zufolge

$$\exists A, B \in \mathcal{E}, A \neq B: \ \gamma(A) = \gamma(B).$$

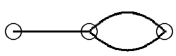
Beispiel 36
Satz 58 liefert: Auf einer Party gibt es stets mindestens zwei Personen, die gleichviele Teilnehmer begrüßt haben.

Bemerkung 25
Die Voraussetzungen der Schlichtheit und Endlichkeit in Satz 58 sind wesentlich:

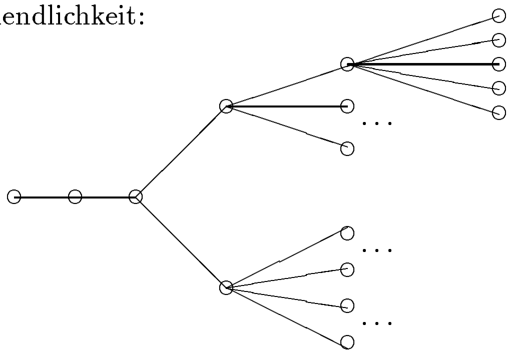
a) Schlingen:



b) Mehrfachkanten:



c) Unendlichkeit:



Satz 59 (Satz von Euler)
$(\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph.

$$\sum_{E\in\mathcal{E}} \gamma(E) = 2|\mathcal{K}|$$

Beweis:

$$\begin{aligned}
|\mathcal{K}| &= |\{h \in \mathcal{K};\ |\varphi(h)| = 1\} \cup \{h \in \mathcal{K};\ |\varphi(h)| = 2\}| \\
&= |\{h \in \mathcal{K};\ |\varphi(h)| = 1\}| + |\{h \in \mathcal{K};\ |\varphi(h)| = 2\}| \\
&= \sum_{E\in\mathcal{E}} |\varsigma(E)| + \frac{1}{2}\sum_{E\in\mathcal{E}} |\tilde{E} \setminus \varsigma(E)|
\end{aligned}$$

also

$$\begin{aligned}
2|\mathcal{K}| &= \sum_{E\in\mathcal{E}} (2|\varsigma(E)| + |\tilde{E}| - |\varsigma(E)|) \\
&= \sum_{E\in\mathcal{E}} \gamma(E).
\end{aligned}$$

Korollar A
Mit $n \rightleftharpoons |\mathcal{E}| \in \mathbb{N}$ gilt:

$$\min_{E\in\mathcal{E}} \gamma(E) \le \frac{2k}{n} \le \max_{E\in\mathcal{E}} \gamma(E),$$

speziell für reguläre Graphen vom Grad r: $rn = 2k$.

Beweis:
Die Behauptung ergibt sich aus Satz 59.

Korollar B (handshaking lemma)
Die Zahl der Ecken ungeraden Grades eines Graphen mit endlich vielen Kanten ist gerade.

Beweis:
Mit $G \rightleftharpoons \{E \in \mathcal{E};\ \gamma(E) \in 2\mathbb{N}_0\}$
und $U \rightleftharpoons \{E \in \mathcal{E};\ \gamma(E) \in 2\mathbb{N} - 1\}$
gilt $G \cup U = \mathcal{E}$ und $G \cap U = \emptyset$ und nach Satz 59 daher

$$\sum_{E\in U} \gamma(E) = 2k - \sum_{E\in G} \gamma(E) \in 2\mathbb{N}_0,$$

also $|U| \in 2\mathbb{N}_0$.

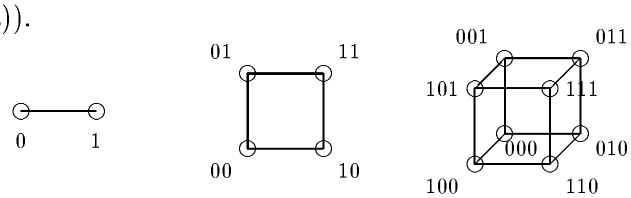
Korollar C
Die Ordnung eines endlichen kubischen Graphen ist gerade.

Beweis:
Die Behauptung folgt sofort aus Korollar A und B.

Beispiel 37

a) Jedes Kohlenwasserstoffmolekül hat eine gerade Anzahl von Wasserstoffatomen (vgl. Beispiel 34a)).

b) Es sei



Q_1 Q_2 Q_3

allgemeiner sei Q_n für $n \in \mathbb{N}$ die Klasse von $(\mathbb{B}^n, \{u,v\};\ u,v \in \mathbb{B}^n;\ h(u,v) = 1\})$, wobei $h(u,v)$ der Hammingabstand von u nach v ist, für $u = u_1 \dots u_n$ und $v = v_1 \dots v_n$ mit $u_\nu, v_\nu \in \mathbb{B}$ für $\nu \in \mathbb{A}_n$ also $h(u,v) \rightleftharpoons |\{\nu \in \mathbb{A}_n;\ u_\nu \neq v_\nu\}|$ (siehe 60).

Was ist $|\kappa(\mathcal{G})|$ für $\mathcal{G} \in Q_n$?
Sei $k \rightleftharpoons |\kappa(\mathcal{G})|$. Da $\mathcal{G}$ offenbar n-regulär ist, folgt aus Korollar A sofort $n2^n = 2k$, also $k = n2^{n-1}$, mithin für $n = 3$ etwa $k = 3 \cdot 2^2 = 12$.

2.3 Gerichtete Graphen

Definition 41

$\mathcal{D} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei ein Tripel aus einer Menge $\mathcal{E}$, einer Menge $\mathcal{K}$ und einer Abbildung φ.

α) $\mathcal{D}$ heißt **gerichteter Graph** oder **Digraph** (directed graph, digraph) im Falle

$$\mathcal{E} \cap \mathcal{K} = \emptyset \quad \wedge \quad \varphi \in (\mathcal{E} \times \mathcal{E})^{\mathcal{K}}.$$

β) Alle für Graphen definierten Redeweisen gelten auch für Digraphen, evtl. mit dem Zusatz „gerichtet“; gerichtete Kanten heißen auch **Pfeile**.

γ) Für $E \in \mathcal{E}$ sei

$$\gamma^+(E) \rightleftharpoons |\{k \in \mathcal{K};\ \exists X \in \mathcal{E}:\ \varphi(k) = (E, X)\}|$$

bzw.

$$\gamma^-(E) \rightleftharpoons |\{k \in \mathcal{K};\ \exists X \in \mathcal{E}:\ \varphi(k) = (X, E)\}|$$

der **Aus-** oder **Außengrad** bzw. **In-** oder **Innengrad** (out- bzw. in-degree).

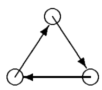
Beispiel 38

a) siehe Beispiel 33b), d)

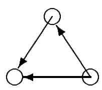
b) Ein **Turnier** (tournament, round robin) sei ein Wettkampf, bei dem jeder Teilnehmer gegen jeden anderen genau einmal kämpft und entweder gewinnt oder verliert:

A B

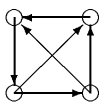
„A schlägt (gewinnt gegen) B“

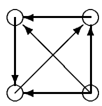


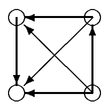
Kein Gewinner

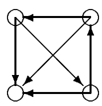


Verlierer Gewinner







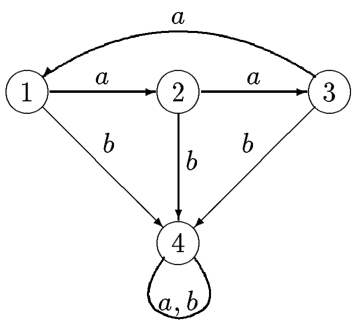


$2 \times \gamma^- = 1$	$1 \times \gamma^- = 0$	$1 \times \gamma^- = 0$	$3 \times \gamma^- = 1$
$2 \times \gamma^- = 2$	$3 \times \gamma^- = 2$	$1 \times \gamma^- = 1$	$1 \times \gamma^- = 3$
		$1 \times \gamma^- = 2$	
		$1 \times \gamma^- = 3$	

Sind das alle Möglichkeiten?
Offensichtlich ja, also: Digraph $(\mathcal{E}, \mathcal{K}, \varphi)$ mit
$\forall X, Y \in \mathcal{E}:\ X \neq Y \Longrightarrow \overset{1}{\exists}\, k \in \mathcal{K}:\ \varphi(k) = (X, Y)\ \vee\ \varphi(k) = (Y, X).$

c) Transitionsdiagramm eines (endlichen deterministischen) Automaten:
A sei ein Zeichenvorrat, $\mathcal{E}$ die Zustandsmenge eines Automaten M und $\mathcal{K}$ derart, daß $\varphi(k) = (X, Y)$ für $k \in \mathcal{K}$ und $X, Y \in \mathcal{E}$, falls es ein $x \in A$ gibt, das, eingelesen, den Übergang von X nach Y bewirkt.
Damit ist ein Digraph $(\mathcal{E}, \mathcal{K}, \varphi)$ definiert. Dabei wird $\forall E \in \mathcal{E} : \ \gamma^+(E) = |A|$ gefordert.

Speziell sei $A = \{a, b\}$ mit $a \neq b$ und $\mathcal{E} = \mathbb{A}_4$ mit



und dem Startzustand 1.
Genau die Wörter a^{3n+2} mit $n \in \mathbb{N}_0$ beweiken einen Übergang von 1 nach 3; mit anderen Worten: M „erkennt“ oder „akzeptiert“ die Sprache (=Menge von Wörtern) $\{a^{3n+2};\ n \in \mathbb{N}_0\}$ über A.

2.4 Darstellung von Graphen

Definition 42 (Adjazenzliste, Adjazenz-, Inzidenzmatrix)

Ein Graph bzw. Digraph $\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ läßt sich darstellen:

α) graphisch: $\mathcal{E}$ wird bijektiv Punkten der Ebene zugeordnet, und $\mathcal{K}$ bijektiv Linien (glatten Kurven) bzw. Pfeilen, die die entsprechenden Punkte verbinden.

β) durch Adjazenzliste: mit $\mathcal{E} = \{E_1, \ldots, E_m\}$ und $m = |\mathcal{E}|$ etwa

$$\begin{array}{ccccc} E_1 & E_2 & & \ldots & E_m \\ \hline X_{11} & X_{21} & & & X_{m1} \\ X_{12} & X_{22} & \vdots & \vdots & X_{m2} \\ \vdots & \vdots & & & \vdots \\ X_{1n_1} & X_{2n_2} & & & X_{mn_m} \end{array}$$

wobei $X_{\mu\nu} \neq X_{\mu\lambda}$ für $\nu \neq \lambda$
und $\exists k : \ \{E_\mu, X_\nu\} = \varphi(k)$
bzw. $\exists k : \ (E_\mu, X_\nu) = \varphi(k)$
gilt und $X_{\mu\nu}$ bei Mehrfachkanten oder Mehrfachschleifen noch von der entsprechenden Anzahl gefolgt wird für $\mu, \nu \in \mathbb{A}_{n_\mu}$ und $\mu \in \mathbb{A}_m$.

γ) durch Matrizen: Dabei seien $\mathcal{E}$ und $\mathcal{K}$ durch M und N indiziert, meist $M = \mathbb{A}_m$ und $N = \mathbb{A}_n$, also etwa $\mathcal{E} = \{E_\mu;\ \mu \in M\}$ und $\mathcal{K} = \{K_\nu;\ \nu \in N\}$:

I. durch eine Inzidenzmatrix $(i_{\mu\nu})_{\substack{\mu \in M \\ \nu \in N}}$ und zwar für $\mathcal{G}$

a) Graph mit

$$i_{\mu\nu} \risingdotseq \left\{ \begin{array}{c} 0 \\ 1 \\ 2 \end{array} \right\}, \text{ falls } k_\nu \left\{ \begin{array}{l} \notin \tilde{E}_\mu \\ \in \tilde{E}_\mu \setminus \varsigma(E_\mu) \\ \in \varsigma(E_\mu) \end{array} \right.$$

b) Digraph mit

$$i_{\mu\nu} \risingdotseq \left\{ \begin{array}{c} 0 \\ 1 \\ -1 \\ -0 \end{array} \right\}, \text{ falls } \left\{ \begin{array}{l} \forall X \in \mathcal{E} :\ (E_\mu, X), (X, E_\mu) \neq \varphi(K_\nu) \\ \exists X \in \mathcal{E} :\ X \neq E_\mu \wedge (E_\mu, X) = \varphi(K_\nu) \\ \exists X \in \mathcal{E} :\ X \neq E_\mu \wedge (X, E_\mu) = \varphi(K_\nu) \\ (E_\mu, E_\mu) = \varphi(K_\nu) \end{array} \right.$$

II. durch eine Adjazenzmatrix $(a_{\mu\nu})_{\mu,\nu \in M}$ und zwar für $\mathcal{G}$

a) Graph mit

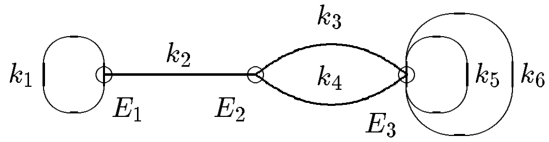
$$a_{\mu\nu} \risingdotseq \left\{ \begin{array}{c} |\tilde{E}_\mu \cap \tilde{E}_\nu| \\ 2|\varsigma(E_\mu)| \end{array} \right\}, \text{ falls } \mu \left\{ \begin{array}{c} \neq \\ = \end{array} \right\} \nu$$

b) Digraph mit

$$a_{\mu\nu} \risingdotseq |\{k \in \mathcal{K};\ \varphi(k) = (E_\mu, E_\nu)\}|$$

Beispiel 39

a)



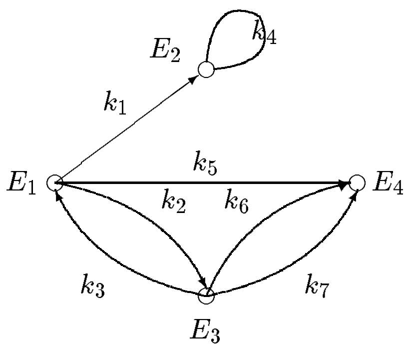
hat die Adjazenzliste

E_1	E_2	$E-3$
E_1	E_1	$E_2 2$
E_2	$E_3 2$	$E_3 2$

die Adiazenzmatrix $\begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 4 \end{pmatrix}$

und die Inzidenzmatrix $\begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \end{pmatrix}$.

b)



hat die Adjazenzliste

E_1	E_2	E_3	E_4
E_2	E_2	E_1	
E_3		$E_4 2$	
E_4			

die Adjazenzmatrix $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

und die Inzidenzmatrix $\begin{pmatrix} 1 & 1 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & -0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 \end{pmatrix}$.

Bemerkung 26

a) Keine der in Definition 42 genannten Darstellungen ist eindeutig!

b) Für die Speicherung einer Adjazenzmatrix eines Graphen der Ordnung n werden wegen der Symmetrie von $A = (a_{\mu\nu})_{\mu,\nu=1,\ldots,n}$, also wegen $a_{\mu\nu} = a_{\nu\mu}$ für $\mu, \nu \in \mathbb{A}_n$ nur

$\frac{n^2-n}{2} + n = \frac{(n+1)n}{2} = \begin{pmatrix} n+1 \\ 2 \end{pmatrix}$
bzw. bei schlichten Graphen nur
$\frac{n^2-n}{2} = \begin{pmatrix} n \\ 2 \end{pmatrix}$
Plätze benötigt.

Trotzdem kann das Arbeiten mit ganz A sinnvoll sein.

c) Vorsicht: Bezeichnungswirrwarr!

Satz 60
$A = (a_{\mu\nu})_{\mu,\nu=1,\dots,n}$ und $I = (i_{\mu\nu})_{\substack{\mu \in M \\ \nu \in N}}$ seien Adjazenzmatrix und Inzidenzmatrix eines Graphen bzw. Digraphen $\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ mit $\mathcal{E} = \{E_1, \dots, E_m\}$ und $\mathcal{K} = \{k_1, \dots, k_n\}$.

a) Ist $\mathcal{G}$ Graph, so ist A eine symmetrische Matrix; speziell für schlichte Graphen eine symmetrische 0-1-Matrix mit Nullen in der Hauptdiagonalen.

b) Die Zeilensummen geben jeweils, außer bei einer Inzidenzmatrix eines Digraphen, die Grade bzw. Außengrade wieder, genauer:

$$\sum_{\nu=1}^{m} a_{\mu\nu} = \sum_{\nu=1}^{n} i_{\mu\nu} = \gamma(E_\mu)$$

bzw.

$$\sum_{\nu=1}^{m} a_{\mu\nu} = \gamma^+(E_\mu)$$

für $\mu \in \mathbb{A}_m$; und die Spaltensummen sind Grade bzw. Innengrade, 2 oder 0, genauer:

$$\sum_{\mu=1}^{m} a_{\mu\nu} = \gamma(E_\nu) \text{ für } \nu \in \mathbb{A}_m \ , \ \sum_{\mu=1}^{m} i_{\mu\nu} = 2 \text{ für } \nu \in \mathbb{A}_n$$

bzw.

$$\sum_{\mu=1}^{m} a_{\mu\nu} = \gamma^-(E_\nu) \text{ für } \nu \in \mathbb{A}_m \ , \ \sum_{\mu=1}^{m} i_{\mu\nu} = 0 \text{ für } \nu \in \mathbb{A}_n.$$

$$\gamma^-(E_\nu) = |\{\nu \in \mathbb{A}_m;\ i_{\mu\nu} \in \{-0, -1\};\ \mu \in \mathbb{A}_M\}|$$

c) Für Digraphen gilt:

$$\sum_{\mu=1}^{m} \gamma^+(E_\mu) = \sum_{\mu=1}^{m} \gamma^-(E_\mu)$$

Beweis:

a) Übung.

b) Übung.

c) Anschaulich klar, oder

$$\sum_{\mu=1}^{m} \gamma^{+}(E_\mu) \overset{b)}{=} \sum_{\mu=1}^{m}\sum_{\nu=1}^{m} a_{\mu\nu} = \sum_{\nu=1}^{m}\sum_{\mu=1}^{m} a_{\mu\nu} \overset{b)}{=} \sum_{\mu=1}^{m} \gamma^{-}(E_\mu)$$

2.5 Wege

Definition 43
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph bzw. Digraph, $A, B \in \mathcal{E}$ und $\mathcal{Z}$ eine endliche Ecken-Kanten-Folge von $\mathcal{G}$ derart, daß aufeinanderfolgende Ecken und Kanten inzidieren; genauer:

$\mathcal{Z} = (E_0, (k_\nu, E_\nu)_{\nu \in \mathbb{A}_n})$ mit

$\{E_{\nu-1}, E_\nu\} = \varphi(k_\nu)$ bzw. $(E_{\nu-1}, E_\nu) = \varphi(k_\nu)$

für $\nu \in \mathbb{A}_n$ und $n \in \mathbb{N}_0$

oder $\mathcal{Z} = \emptyset$.

$\mathcal{Z}$ heißt **Kantenzug** (walk, chemin) von $\mathcal{G}$ der Länge $\lambda(\mathcal{Z} = n$ von E_0 nach E_n., kurz E_0-E_n-Kantenzug und E_0 bzw. E_n **Anfangs-** bzw. **Endecke** von $\mathcal{Z}$.

α) Gilt $E_0 = E_n$, heißt $\mathcal{Z}$ **geschlossen**, anderenfalls **offen**.

β) $\mathcal{Z}$ heißt **Linie** (trail, chemin simple) im Falle

$$\forall \mu, \nu \in \mathbb{A}_n : \ \mu \neq \nu \Longrightarrow k\mu \neq k_\nu$$

und **Weg** (path, chemin élémentaire) im Falle

$$\forall \mu, \nu \in \mathbb{U}_{n+1} : \ \mu \neq \nu \Longrightarrow E_\mu \neq E_\nu.$$

γ) Ein kürzester A-B-Weg heißt **geodätischer Weg** oder **Geodäte** von A nach B oder A-B-Geodätische. Dabei wird ein Kantenzug $\mathcal{W}$ von $\mathcal{G}$ kürzer als $\mathcal{Z}$ genannt, falls $\lambda(\mathcal{W}) < \lambda(\mathcal{Z})$ gilt.

δ) Die **Entfernung** (distance) von A nach B, kurz $\delta(A, B)$ ist definiert durch

$$\delta(A,B) \rightleftharpoons \begin{cases} \lambda(\mathcal{W}) & \Leftarrow \quad \mathcal{W} \text{ ist } A\text{-}B\text{-Geodätische} \\ \infty & \Leftarrow \quad \nexists\ A\text{-}B\text{-Geodätische} \end{cases}$$

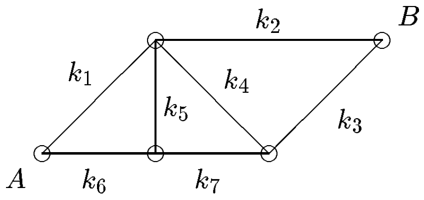
Bemerkung 27

a) Vorsicht: Bzeichnungswirrwarr!

b) Es ist leicht zu sehen: Wenn in einem Kantenzug keine Ecke zweimal vorkommen darf, kann auch keine Kante zweimal vorkommen, also ist jeder Weg auch eine Linie.

c) Da die E_ν aus Definition 43 häufig eindeutig durch $(k_\nu)_{\nu \in \mathbb{A}_n}$ bestimmt sind, wird in diesen Fällen auch $(k_\nu)_{\nu \in \mathbb{A}_n}$ als Kantenzug bezeichnet und gelegentlich mit $k_1 \to k_2 \to \ldots \to k_n$ notiert.

Beispiel 40
In



ist $\delta(A, B) = 2$ und $k_1 \to k_2 \to \ldots \to k_6$ eine geschlossene Linie, aber kein Weg.

Satz 61
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei ein endlicher nichtleerer Graph, bzw. Digraph, etwa mit $\mathcal{E} = \{A_\nu;\ \nu \in \mathbb{A}_n\}$ und $|\mathcal{E}| = n \in \mathbb{N}$
sowie $A = (a_{\mu\nu})_{\mu,\nu \in \mathbb{A}_n}$ die dazugehörige Adjazenzmatrix
und $C = (c_{\mu\nu})_{\mu,\nu \in \mathbb{A}_n}$

$$\text{mit } c_{\mu\nu} \rightleftharpoons \left\{ \begin{matrix} a_{\mu\nu} \\ \frac{a_{\mu\nu}}{2} \end{matrix} \right\} \text{ für } \mu \left\{ \begin{matrix} \neq \\ = \end{matrix} \right\} \nu \text{ im Falle } \mathcal{G} \text{ ist Graph}$$

und $C = A$ im Falle $\mathcal{G}$ ist Digraph.

Dann ist

$$|\{\mathcal{Z};\ \mathcal{Z} \text{ ist } A_\lambda\text{-}A_\nu\text{-Kantenzug der Länge } l\}| = c_{\lambda\nu}^{(l)}$$

$$\text{mit } (c_{\lambda\nu}^{(l)})_{\lambda,\nu \in \mathbb{A}_n} \rightleftharpoons C^l \text{ und } l \in \mathbb{N}_0.$$

Beweis:
Induktion nach l:

IA: $l = 0 \Longrightarrow C^0 = E_n$ ($n \times n$-Einheitsmatrix)

IS: Sei $z_{\lambda\nu}^{(j)} \rightleftharpoons |\mathcal{Z}_{\lambda\nu}^{(j)}|$ mit
$\mathcal{Z}_{\lambda\nu}^{(j)} \rightleftharpoons \{\mathcal{Z};\ \mathcal{Z}$ ist A_λ-A_ν-Kantenzug von $\mathcal{G}$ der Länge $j\}$
für $j \in \mathbb{N}_0$, $\lambda, \nu \in \mathbb{A}_n$ sowie für l bewiesener Behauptung, also
Induktionsvoraussetzung: $z_{\lambda\nu}^{(l)} = c_{\lambda\nu}^{(l)}$ für $\lambda, \nu \in \mathbb{A}_n$.
Dann gilt:

$$\begin{aligned} z_{\lambda\nu}^{(l+1)} &= |\{\mathcal{Z};\ \exists \mu \in \mathbb{A}_n\ \exists k \in \mathcal{K}: \ \mathcal{Z} = (\mathcal{W}, k, A_\nu) \\ &\qquad \wedge\ \mathcal{W} \in \mathcal{Z}_{\lambda\mu}^{(l)} \\ &\qquad \wedge\ \{A_\mu, A_\nu\} = \varphi(k) \text{ bzw. } (A_\mu, A_\nu) = \varphi(k)\}| \\ &= \sum_{\mu \in \mathbb{A}_n} (z_{\lambda\mu}^{(l)} \cdot c_{\mu\nu}) \\ &\overset{\text{IV}}{=} \sum_{\mu=1}^{n} (c_{\lambda\mu}^{(l)} \cdot c_{\mu\nu}) \\ &= c_{\lambda\nu}^{(l+1)}. \end{aligned}$$

Definition 44 (Untergraph, zusammenhängend, Komponente)
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ und $\mathcal{G}' = (\mathcal{E}', \mathcal{K}', \varphi')$ seien Graphen bzw. Digraphen mit $\mathcal{E}' \subseteq \mathcal{E}$ und $\mathcal{K}' \subseteq \mathcal{K}$.

α) $\mathcal{G}'$ heißt **Untergraph** (Teilgraph, subgraph) bzw. -digraph von $\mathcal{G}$, auch: $\mathcal{G}$ enthält $\mathcal{G}'$, kurz $\mathcal{G}' \subseteq \mathcal{G}$, und $\mathcal{G}$ dann **Obergraph** bzw. -digraph von $\mathcal{G}'$, kurz $\mathcal{G} \supseteq \mathcal{G}'$, falls

$$\varphi' = \varphi\lceil_{\mathcal{K}'}$$

ist.

β) $\mathcal{G}$ sei Graph. $\mathcal{G}$ heißt **zusammenhängend** (connected), wenn es zu allen $A, B \in \mathcal{E}$ mit $A \neq B$ einen A-B-Weg gibt, sonst **unzusammenhängend** (disconnected).
Ein maximaler zusammenhängender Untergraph von $\mathcal{G}$ heißt **Zusammenhangskomponente**, kurz **Komponente** von $\mathcal{G}$.

Erinnerung:
(M, δ) heißt **metrischer Raum**, falls M eine Menge und δ eine **Metrik** auf M ist, d. h. es gilt:

$$\delta : \ M \times M \longrightarrow \mathbb{R}_0^+$$

mit $\forall x, y, z \in M$:

$\delta(x, y) = 0 \Leftrightarrow x = y$	(positiv definit)	
$\delta(x, y) = \delta(y, x)$	(symmetrisch)	(vgl. W. Klotz; LA & AG I/II, S. 72)
$\delta(x, y) \leq \delta(x, z) + \delta(z, y)$	(Dreiecksungleichung).	

Satz 62
$(\varepsilon(K), \delta)$ ist für jede Komponente K eines Graphen bzgl. der in Definition 43δ) definierten Entfernung ein metrischer Raum.

Beweis: Übung. Fiolgt direkt aus der Definition.

Satz 63
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei schlichter Graph mit $m \rightleftharpoons |\mathcal{E}| \in \mathbb{N}_0$, $n \rightleftharpoons |\mathcal{K}|$ und k Komponenten. Dann gilt

$$m - k \leq n \leq \binom{m-k+1}{2}.$$

Beweis:

a) Für $m \in \mathbb{N}$, $k \in \mathbb{A}_n$ und $m_1, m_2, \ldots, m_k \in \mathbb{A}_m$ mit $\sum\limits_{\kappa=1}^{k} m_\kappa = m$ zeigen wir

$$(*) \qquad \sum_{\kappa=1}^{k} \binom{m_\kappa}{2} \leq \binom{m-k+1}{2}$$

Sei $A_\kappa \rightleftharpoons P_2(\mathbb{A}_{\sum_{\lambda=1}^{\kappa} m_\lambda - (\kappa-1)} \setminus \mathbb{A}_{\sum_{\lambda=1}^{\kappa-1} m_\lambda - (\kappa-1)})$ für $\kappa \in \mathbb{A}_k$,
speziell wegen $\sum\limits_{\lambda=1}^{1-1} m_\lambda - (1-1) = 0$, also $A_1 = P_2(\mathbb{A}_{m_1}$
und $C \rightleftharpoons P_2(\mathbb{A}_{m-k+1})$ für $\kappa \in \mathbb{A}_k$ ist

$$|\mathbb{A}_{\sum\limits_{\lambda=1}^{\kappa} m_\lambda - (\kappa-1)} \setminus \mathbb{A}_{\kappa-1 \atop \sum\limits_{\lambda=1} m_\lambda - (\kappa-1)}|$$

$$= \left(\sum_{\lambda=1}^{\kappa} m_\lambda - (\kappa-1)\right) - \left(\sum_{\lambda=1}^{\kappa-1} m_\lambda - (\kappa-1)\right)$$

$$= m_\kappa$$

und daher

$$\binom{m_\kappa}{2} = |P_2(\mathbb{A}_{m_\kappa})| = |A_\kappa|;$$

ferner $(\iota \neq \kappa,\ \iota, \kappa \in \mathbb{A}_k \Longrightarrow A_\iota \cap A_\kappa = \emptyset)$
sowie $\bigcup_{\kappa=1}^{k} A_\kappa \subseteq P_2(\mathbb{A}_{\sum_{\lambda=1}^{k} m_\lambda - (k-1)}) = C$
und somit

$$\sum_{\kappa-1}^{k} \binom{\kappa}{2} = \sum_{\kappa=1}^{k} |A_\kappa| = |\bigcup_{\kappa=1}^{k} A_\kappa| \leq |C| = \binom{m-k+1}{2}.$$

(Anderer Beweis von $(*)$ mittels Induktion möglich.)

b) $\mathcal{G}$ habe k Komponenten $K_1, \ldots, K_k$:

I. Durch Induktion zeigen wir

$$(**) \qquad m - k \leq n.$$

IA: $n = 0 \Rightarrow k = m$ (jeder Punkt ist eine Komponente) für $m > 0$
$k = 1$ (leerer Graph als Komponente) für $m = 0$
also $m - k \leq 0 \leq n$.

IS: Induktionsvoraussetzung: $(**)$ sei wahr für ein $n \in \mathbb{N}_0$ und $\mathcal{G}'$ ein schlichter Graph mit $m \in \mathbb{N}_0$ Ecken, $n+1$ Kanten und k Komponenten.
Durch Wegnahme einer Kante aus $\mathcal{G}'$ erhalten wir einen schlichten Graphen S mit m Ecken, n Kanten und k Komponenten mit $k \leq k' + 1$, nach Induktionsvoraussetzung also

$$m - k' \leq m - k + 1 \leq n + 1$$

II. Wir beweisen $n \leq \binom{m-k+1}{2}$.
Für $m = 0$ ist $n = 0$ und die Behauptung richtig.
Sei also $m \in \mathbb{N}$ und m_κ die Ordnung von K_κ für $\kappa \in \mathbb{A}_k$.
Dann gilt $\sum_{\kappa-1}^{k} m_\kappa = m$
und wegen $|\kappa(K_\kappa)| \overset{\text{Satz 56}}{\leq} \binom{m_\kappa}{2}$ für $\kappa \in \mathbb{A}_k$ $(*)$ zufolge

$$n = \sum_{\kappa=1}^{k} |\kappa(K_\kappa)| \leq \sum_{\kappa=1}^{k} \binom{m_\kappa}{2} \leq \binom{m-k+1}{2}.$$

Korollar:
Gilt

$$n > \binom{m-1}{2},$$

ist $\mathcal{G}$ zusammenhängend.

Beweis:
Nach Satz 63 hat man

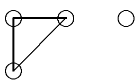
$$\binom{m-1}{2} < \binom{m-k+1}{2}$$

also $m - 1 < m - k + 1$, was $k < 2$, folglich $k = 1$, d. h. $\mathcal{G}$ zusammenhängend, bedingt.

Bemerkung 28

a) Satz 63 ist eine Verallgemeinerung von Satz 56:

$$0 \leq n \leq \binom{m-k+1}{2} \leq \binom{m}{2}.$$

b) Die Schranken in Satz 63 und im Korollar sind optimal; für das Korollar:
Bei  gilt $n = \binom{m-1}{2}$ und $\mathcal{G}$ ist unzusammenhängend.

2.6 Wälder

Definition 45 (Kreis, Wald, Baum, Blätter)
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph bzw. Digraph.

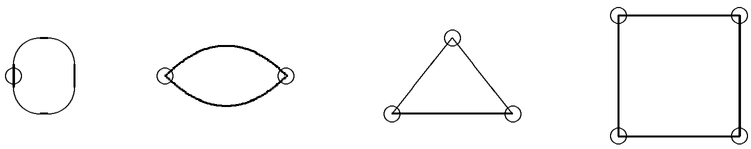
α) $\mathcal{Z}$ sei ein Kantenzug wie in Definition 43:
Ist $n \geq 1$ und $n \neq 2$, $\mathcal{Z}$ geschlossen und $(E_0, (k_\nu, E_\nu)_{\nu \in \mathbb{A}_{n-1}})$ ein Weg oder $\mathcal{Z} = (E_0, k_1, E_1, k_2, E_0)$ mit $k_1 \neq k_2$, so wird $\mathcal{Z}$ und der entsprechende Untergraph **Kreis** (cycle) der Länge n genannt.
Ein Kreis der Länge n, genauer seine Isomorphieklasse, wird mit C_n bezeichnet, ebenso der entsprechende Untergraph.

β) Hat $\mathcal{G}$ keine Kreise, so heißt $\mathcal{G}$ **kreislos** oder **azyklisch**.
Ein azyklischer Graph wird **Wald** (forest) genannt, ein zusammenhängender Wald **Baum** (tree) (im Sinne der Graphentheorie).

γ) Bei einem Baum oder Wald heißen die Ecken vom Grad 1 oder 0 auch **Blätter**, die anderen Ecken **innere Ecken**.

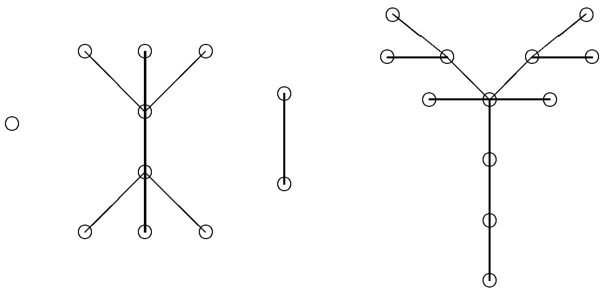
Beispiel 41

a)



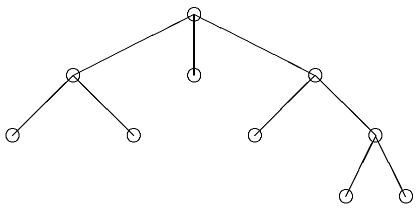
C_1 C_2 $C_3 \equiv K_3$ C_4

b)



ist ein Wald aus vier Bäumen. (Achtung: der isolierte Punkt ist gleichzeitig Baum und Blatt!)

c)



ist ein Baum mit 6 Blättern und vier inneren Ecken.

Satz 64
$\mathcal{G}$ sei Graph.

a)

	I	$\mathcal{G}$ ist Baum
$\Longleftrightarrow$	II	$\mathcal{G}$ ist z̄usammenhängend, schlicht und enthält keine Kreise einer Länge ≥ 3
$\Longleftrightarrow$	III	$\mathcal{G}$ ist zusammenhängend und zerfällt bei Wegnahme einer beliebigen Kante in zwei Komponenten
$\Longleftrightarrow$	IV	Alle Ecken A, B von $\mathcal{G}$ sind durch genau einen A-B-Weg verbunden
$\Longleftrightarrow$	V	$\mathcal{G}$ enthält keine Kreise , aber das Hinzufügen einer beliebigen neuen Kante schafft genau einen Kreis
$\Longleftrightarrow$	VI	$\mathcal{G}$ ist zusammenhängend, nicht vollständig für Ordnung ≥ 2 und nach Hinzufügen einer beliebigen neuen Kante hat der Graph genau einen Kreis

b) n sei die Ordnung von $\mathcal{G}$.

	I	$\mathcal{G}$ ist Baum
$\Longleftrightarrow$	II	$\mathcal{G}$ ist zusammenhängend und hat genau $n-1$ Kanten
$\Longleftrightarrow$	III	$\mathcal{G}$ enthält keine Kreise und hat genau $n-1$ Kanten
$\Longleftrightarrow$	IV	$\mathcal{G}$ ist nicht kantendisjunkte Vereinigung zweier vollständiger schlichter Graphen der Ordnung 3 und der Ordnung 1 bzw. 2

Beweis:
Sei $\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$.

a) II $\overset{\alpha}{\Leftrightarrow}$ I $\overset{\beta}{\Rightarrow}$ III $\overset{\gamma}{\Rightarrow}$ IV $\overset{\delta}{\Rightarrow}$ V $\overset{\varepsilon}{\Rightarrow}$ VI $\overset{\zeta}{\Rightarrow}$ I

α) — δ) Übung.

ε) Wäre $\mathcal{G}$ unzusammenhängend, gäbe es zwei Komponenten K_1, K_2 und eine K_1 mit K_2 verbindende neue Kante würde keinen Kreis schaffen.
Wäre $\mathcal{G}$ vollständig bei einer Ordnung ≥ 2, hätte $\mathcal{G}$ einen Kreis.

ζ) Da $\mathcal{G}$ nicht vollständig bei einer Ordnung ≥ 2, gibt es zwei Ecken A, B mit $A \not\sim B$. Sei $k \notin \mathcal{K}$ mit $A \sim_k B$. Da $\mathcal{G}$ zusammenhängend, gibt es einen A-B-Weg $\mathcal{W}$ in $\mathcal{G}$ und $\mathcal{V} = (\mathcal{W}, k, A)$ ist ein Kreis. Besäße $\mathcal{G}$ einen Kreis $\mathcal{Z}$, müßte $\mathcal{Z}$ bis auf die Reihenfolge gleich $\mathcal{V}$ sein, da k in $\mathcal{V}$ enthalten. Also ist $\mathcal{G}$ kreislos.

b)

I$\Rightarrow$II: $\mathcal{G}$ ist per definitionem zusammenhängend, Rest durch Induktion nach n:

IA: $n = 1$: $\mathcal{G}$ hat genau $n - 1 = 0$ Kanten.

IS: Die Behauptung sei wahr für ein $n \in \mathbb{N}$ und $\mathcal{B}$ ein Baum mit genau $n + 1$ Ecken. Wegen der Endlichkeit von $\mathcal{B}$ gibt es zwei Ecken A, B mit maximalem $\delta(A, B) \eqqcolon m$; dann sind A und B Blätter, denn sonst wäre m nicht maximal oder $\mathcal{B}$ enthielte einen Kreis. Das Entfernrn von A mit der anliegenden Kante liefert einen Baum $\mathcal{B}'$ mit genau n Ecken, der nach Induktionsvoraussetzung genau $n-1$ Kanten besitzt. Also hat $\mathcal{B}$ genau $n - 1 + 1 = (n + 1) - 1$ Kanten.

I$\Leftarrow$II: zu zeigen: $\mathcal{G}$ ist kreislos. Induktion nach n:

IA: $n = 1$: trivial.

IS: Die Behauptung sei wahr für ein $n \in \mathbb{N}$ und $\mathcal{B}$ sei zusammenhängender Graph der Ordnung $n + 1$ mit genau n Kanten.
$\mathcal{B}$ hat eine Ecke A mit $\gamma(A) = 1$, denn des Zusammenhanges von $\mathcal{B}$ ist $\gamma(E) > 0$ für alle $E \in \varepsilon(\mathcal{B})$, und wäre $\gamma(E) \geq 2$ für alle $E \in \varepsilon(\mathcal{B})$, so hätte man Satz 59 zufolge
$2n = \sum\limits_{E\in\varepsilon(\mathcal{B})} \gamma(E) \geq 2(n + 1)$.
Das Entfernen von A mit der anliegenden Kante liefert einen zusammenhängenden Graph $\mathcal{B}'$ der Ordnung n mit genau $n - 1$ Kanten, nach Induktionsvoraussetzung also einen Baum $\mathcal{B}'$. Mithin ist $\mathcal{B}'$ und daher auch $\mathcal{B}$ azyklisch.

Rest: Übung.

Korollar A:
Jeder Baum der Ordnung $n \in \mathbb{N}\setminus\{1\}$ hat mindestens zwei Blätter und höchstens $n-2$ innere Ecken.

Beweis:
Sei $\mathcal{B} = (\mathcal{E}, \mathcal{K}, \varphi)$ Baum mit $n \eqqcolon |\mathcal{E}| \in \mathbb{N} \setminus \{1\}$.
Nach Satz 59 und Satz 64b) gilt $\sum\limits_{E\in\mathcal{E}} \gamma(E) = 2|\mathcal{K}| = 2(n - 1)$,
also gibt es $A, B \in \mathcal{E}$ mit $A \neq B$ und $\gamma(A) = \gamma(B) = 1$.
Da eine Ecke entweder innere Ecke oder Blatt ist, folgt die Behauptung.

Korollar B:
Ein Wald der Ordnung $n \in \mathbb{N}$ mit b Bäumen hat genau $n - b$ Kanten.

Beweis:
Sei n_β die Ordnung des Baumes $\mathcal{B}_\beta$ des Waldes $\mathcal{W}$ der Ordnung n für $\beta = 1, \ldots, b$.
Nach Satz 64b) hat $\mathcal{B}_\beta$ genau $n_\beta - 1$ Kanten, also hat $\mathcal{W}$ genau $\sum\limits_{\beta=1}^{b} (n_\beta - 1) = n - b$ Kanten.

Satz 65
$\mathcal{B} = (\mathcal{E}, \mathcal{K}, \varphi)$ mit $\mathcal{K} \subseteq P_2(\mathcal{E})$ und $\varphi = 1_\mathcal{K}$ sei ein Baum und $W \in \mathcal{E}$.
Dann gibt es genau einen Digraphen $\mathcal{T} = (\mathcal{E}, \mathcal{H}, \psi)$ mit

$\mathcal{H} \in \mathcal{E} \times \mathcal{E}$,

$\psi = 1_\mathcal{H}$ und

$(X, Y) \in \mathcal{H} \iff \{X, Y\} \in \mathcal{K} \ \wedge\ \delta(W, X) < \delta(W, Y)$.

Beweis: Übung.

Bemerkung 29
Jeder Baum läßt sich nach Satz 65 von jenem W, der Wurzel (einer ausgezeichneten Ecke) weg orientieren.

Definition 46
$\mathcal{A} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Digraph.

α) $\mathcal{A}$ heißt **Arboreszenz** oder **Wurzelbaum** (rooted tree), falls

$$\mathcal{E} = \emptyset$$

oder

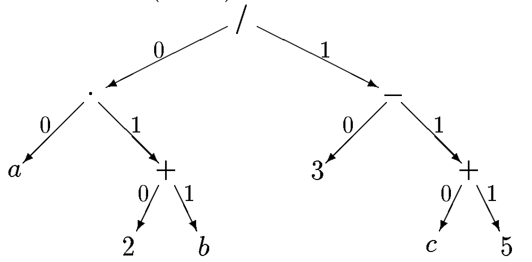
$$\overset{1}{\exists}\, W \in \mathcal{E} : \ \gamma^-(W) = 0 \ \wedge \ \forall E \in \mathcal{E} \setminus \{W\} : \ \gamma^-(E) = 1.$$

W heißt dann **Wurzel** von $\mathcal{A}$ und alle $B \in \mathcal{E}$ mit $\gamma^+(B) = 0$ **Blätter** von $\mathcal{A}$.

β) Ist bei einem Wurzelbaum für jedes $E \in \mathcal{E}$ mit $\gamma^+(E) > 0$ noch eine Reihenfolge der in E startenden Pfeile festgelegt, sprechen wir von einem **geordneten Wurzelbaum** (arborescence) oder kurz von einem **Baum** im Sinne der Informatik.

Beispiel 42
„Aufbrechen" einer Formel in **Infixnotation** (Operand-Operator-Operand) durch einen Compiler führt auf sogenannte **Kantorowitsch-Bäume**, etwa

für $\dfrac{a(2+b)}{3-(c+5)} = a \cdot (2+b)/(3-(c+5))$ auf



Jeder Ecke kann eindeutig ein 0-1-Wort zugeordnet werden, das den Weg von der Wurzel zu dieser Ecke beschreibt, wenn „links" bzw. „rechts" durch 0 bzw. 1 markiert werden (vgl. Beispiel 33b)).
Schreibt man die Eckensymbole in der lexikographischen Ordnung der ihnen zugeordneten Wörter, erhält man eine Preorder-Traversierung des Baumes und so die sogenannte polnische Notation oder Warschauer Normalform nach Łukasiewicz oder **Präfixnotation** (Operator-Operand-Operand) der ursprünglichen Formel:

∅	0	00	01	010	011	1	10	11	110	111
/	·	a	+	2	b	-	3	+	c	5

Entsprechende **Suffixnotation** (Operand-Operand-Operator) oder umgekehrte polnische Notation:

a	2	b	+	·	3	c	5	+	-	/
00	010	011	01	0	10	110	111	11	1	∅

Definition 47 (Sohn, Vater, m-är, Höhe, Tiefe)
$\mathcal{B} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei ein Baum mit Wurzel W, $X, Y \in \mathcal{E}$ und $m \in \mathbb{N}$.

α) Y heißt **Tochter**, **Sohn** oder unmittelbarer Nachfolger von X im Falle

$$(X, Y) \in \varphi(\mathcal{K})$$

und X dann **Mutter**, **Vater** oder unmittelbarer Vorgänger von Y.
Entsprechend lassen sich Schwester (Bruder), Enkel, Base (Vetter), etc. definieren.

β) $\mathcal{B}$ heißt **m-är** im Falle

$$\forall E \in \mathcal{E}: \ \gamma^+(E) \leq m,$$

speziell **binär** bzw. **ternär** für $m = 2$ bzw. $m = 3$.

γ) Das Distanzmaximum von W zu den Blättern heißt **Höhe** oder **Tiefe** von $\mathcal{B}$, kurz

$$h(\mathcal{B}) \rightleftharpoons \max\{\delta(W, B);\ B \in \mathcal{E};\ \gamma^+(B) = 0\}$$

Beispiel 43
Der binäre Baum aus Beispiel 42 hat die Höhe 3.

Satz 66

a) Jeder Baum $\mathcal{B}$ ist entweder leer oder läßt sich eindeutig darstellen als $(W, \mathcal{F})$, wobei W die Wurzel von $\mathcal{B}$ und $\mathcal{F}$ eine (evtl. leere) Folge von nichtleeren Teilbäumen ist, und zwar in der durch die Ordnung gegebenen Reihenfolge.

b) Umgekehrt bestimmt jede rekursive Festlegung der in a) genannten Art eindeutig einen Baum.

So läßt sich der Begriff Baum rekursiv definieren durch:
Ein Baum ist leer oder ein Gebilde $(W, \mathcal{F})$, wobei $\mathcal{F}$ eine eventuell leere Folge nichtleerer Bäume ist.

Beweis: Übung.

Beispiel 44
Der Baum aus Beispiel 42 läßt sich gemäß Satz 66 darstellen als:

$$\Big(/, ((\cdot, ((a, \emptyset), (+_1, ((2, \emptyset), (b, \emptyset))))), (-, ((3, \emptyset), (+_2, ((c, \emptyset), (5, \emptyset))))))\Big).$$

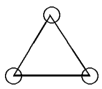
2.7 Euler- und Hamiltongraphen

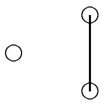
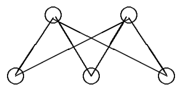
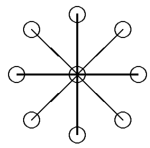
Definition 48
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph.

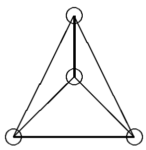
α) Ein Kantenzug von $\mathcal{G}$ heißt **Eulersche Linie** (eulerian trail) von $\mathcal{G}$, wenn er $\mathcal{K}$ enthält.
$\mathcal{G}$ heißt **Eulerscher Graph** (eulerian graph), wenn $\mathcal{G}$ eine geschlossene Eulersche Linie hat, die $\mathcal{E}$ enthält.

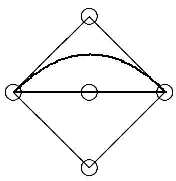
β) Ein Kantenzug von $\mathcal{G}$ heißt **Hamiltonsche Linie** (hamiltonian trail) von $\mathcal{G}$, wenn er $\mathcal{E}$ enthält.
Ist eine Hamiltonsche Linie ein Weg oder Kreis einer Länge ¿2, so heißt sie **Hamiltonscher Weg** (hamiltonian path) oder **Hamiltonscher Kreis** (hamiltonian circuit).
$\mathcal{G}$ heißt **Hamiltonscher Graph**, falls $\mathcal{G}$ einen Hamiltonschen Kreis hat.

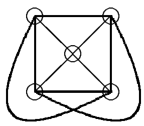
Beispiel 45

a)  K_3 ist Eulerscher und Hamiltonscher Graph.

b)  ,  und  sind weder Eulersche noch Hamiltonsche Graphen.

c)  K_4 ist Hamiltonscher, nicht jedoch Eulerscher Graph.

d)  ist Eulerscher, nicht jedoch Hamiltonscher Graph.

e)  K_5 ist Eulerscher und Hamiltonscher Graph.

Satz 67 (Euler, Veblen)
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph und $m = |\mathcal{E}|$.

I $\mathcal{G}$ ist Eulerscher Graph

$\Longleftrightarrow$ II $\mathcal{G}$ ist zusammenhängend, $m \in \mathbb{N}_0$ und $\forall E \in \mathcal{E}: \ \gamma(E) \in 2\mathbb{N}_0$

$\iff$ III $\mathcal{G}$ ist zusammenhängend und $\mathcal{G}$ ist endliche Vereinigung von Kreisen oder $\mathcal{G} = N_1$

Beweis:
I $\overset{\alpha)}{\Rightarrow}$ II $\overset{\beta)}{\Rightarrow}$ III $\overset{\gamma)}{\Rightarrow}$ I

α) $\mathcal{L}$ sei geschlossene Eulersche Linie, die $\mathcal{E}$ enthält. Da $\mathcal{L}$ per definitionem endlich ist und $\mathcal{E}$ sowie $\mathcal{K}$ enthält, ist $\mathcal{G}$ endlich und zusammenhängend.
Bei jedem „Durchlaufen" von $E \in \mathcal{E}$ längs $\mathcal{L}$ erhöht sich der Beitrag zu $\gamma(E)$ um 2. Da $\mathcal{G}$ endlich, ist $\gamma(E) \in 2\mathbb{N}_0$ für jedes $E \in \mathcal{E}$.

β) , γ) Übung.

Korollar A:

a) $\mathcal{G}$ sei regulärer Graph vom Grad r:
$\mathcal{G}$ ist Eulerscher Graph genau dann, wenn $\mathcal{G}$ endlich, zusammenhängend und $r \in 2\mathbb{N}_0$.

b) C_n ist Eulerscher Graph.

c) K_n ist Eulerscher Graph genau dann, wenn $n \in 2\mathbb{N}$ oder $n = 0$.

d) N_n mit $n \in \mathbb{N} \setminus \{1\}$ ist kein Eulerscher Graph.

Beweis:
Unmittelbar aus der Definition und Satz 67.

Korollar B:
Ein zusammenhängender endlicher Graph hat genau dann eine Eulersche Linie, wenn er höchstens zwei Ecken ungeraden Eckengrades besitzt.

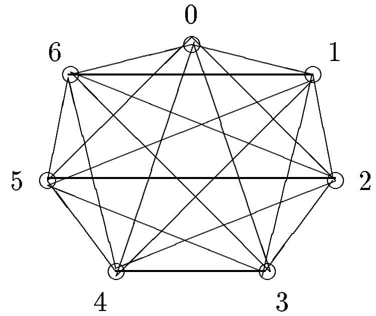
Beweis:
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei zusammenhängender endlicher Graph.

$\Leftarrow$: $\mathcal{L}$ sei Eulersche Linie von $\mathcal{G}$ mit Anfangsecke A und Endecke B.
Für jede Ecke E von $\mathcal{L}$ mit $A \neq E \neq B$ folgt $\gamma(E) \in 2\mathbb{N}$ wie im Beweis von Satz 67.

$\Rightarrow$: Übung.

Beispiel 46

a) Kann aus allen Steinen eines Dominospieles ein Kreis gelegt werden?

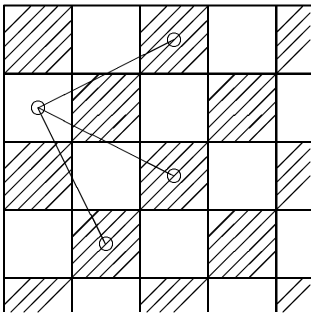


(Kanten entsprechen Steinen)

Ja, denn jede Ecke hat Grad 6, nach Satz 67 ist der Graph also ein Eulerscher Graph.

b) Königsberger Brückenproblem (siehe Beispiel 33a))
Da 3 Ecken vom Grad 3 vorhanden sind, gibt es nach Korollar B zu Satz 67 keine Eulersche Linie.

c) Lassen sich auf einem Schachbrett alle mit einem Springer möglichen Züge so hintereinander machen, daß jeder Zug genau einmal vorkommt?



Es gibt mindestens 8 Ecken ungeraden Grades, nach Korollar B zu Satz 67 ist ein solcher Zug also unmöglich.

Satz 68
$\mathcal{G}$ sei schlichter Graph mit $\mathcal{E} = \varepsilon(\mathcal{G})$ und $m \rightleftharpoons |\mathcal{E}| \in \mathbb{N} \setminus \mathbb{A}_2$.
Dann gilt:

$$\Big(\forall A, B \in \mathcal{E} : \; A \not\sim B \Rightarrow \gamma(A) + \gamma(B) \geq m\Big) \Longrightarrow \; \mathcal{G} \text{ ist Hamiltonscher Graph.}$$

Beweis: Übung.

Korollar A:
Voraussetzung wie in Satz 68.

$$\forall E \in \mathcal{E} : \; \gamma(E) \geq \frac{m}{2} \Longrightarrow \; \mathcal{G} \text{ ist Hamiltonscher Graph.}$$

Beweis:
Unmittelbar aus Satz 68.

Korollar B:
Jeder reguläre endliche Graph der Ordnung $m \geq 3$ von einem Grade $\geq \frac{m}{2}$ ist Hamiltonscher Graph.

Beweis: Spezialisierung von Korollar A.

Bemerkung 30
Daß Satz 68 nicht umkehrbar ist, zeigt schon C_5.

Eine („schöne") hinreichende und notwendige Charakterisierung für Hamiltonsche Graphen ist bisher nicht gefunden worden.

2.8 Petrinetze

Definition 49
$\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ sei Graph bzw. Digraph.

α) $\mathcal{G}$ heißt **paar**, **bipartit** oder **bichromatisch**, falls es τ und ϑ gibt mit $\tau \neq \emptyset \neq \vartheta$ und $\tau \cup \vartheta = \mathcal{E}$ sowie $\tau \cap \vartheta = \emptyset$ und

$$\forall k \in \mathcal{K}\ \exists X \in \tau\ \exists Y \in \vartheta :\ \varphi(k) = \{X, Y\} \text{ bzw. } \varphi(k) \in \{(X, Y), (Y, X)\}.$$

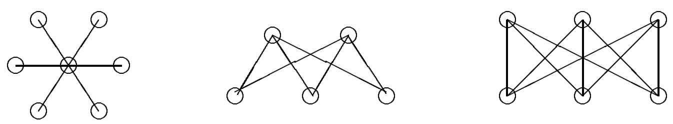
β) $\mathcal{G}$ sei paarer schlichter Graph; die Benennung sei wie in α).
$\mathcal{G}$ heißt **vollständig paarer Graph** im Falle

$$\forall X \in \tau\ \forall Y \in \vartheta\ \exists k \in \mathcal{K} :\ \varphi(k) = \{X, Y\}.$$

Mit $m \eqqcolon |\tau| \in \mathbb{N}$ und $n \eqqcolon |\vartheta| \in \mathbb{N}$ wird die Isomorphieklasse dieser Graphen mit $K_{m,n}$ bezeichnet.

Beispiel 47

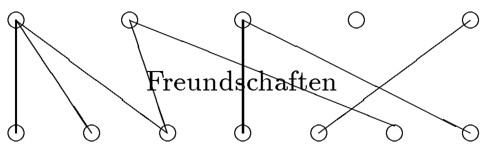
a)



$K_{1,6}$ $K_{2,3}$ $K_{3,3}$

b) „Heirat" ist ein „Matching", die jedes $d \in D$ sättigt, d. h. eine injektive Abbildung $d \longmapsto h$ mit $d \sim h$.

Damen

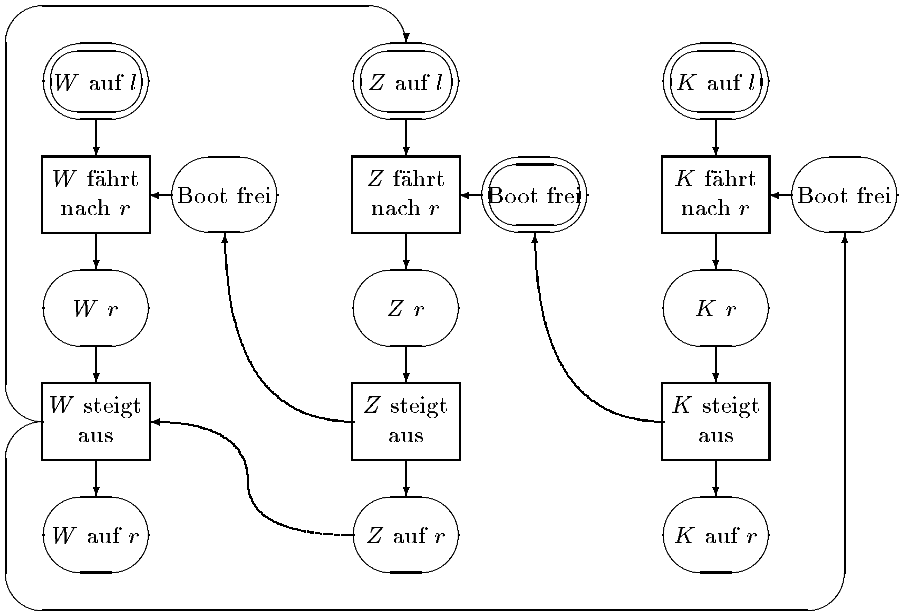


Herren

Notwendige und hinreichende (mathematische) Bedingung für eine Heirat (Heiratssatz von P. Hall, 1935):

$$\forall U \subseteq D :\ |N(U)| \geq |U| \text{ mit } N(U) \eqqcolon \{h \in H;\ \exists u \in U :\ u \sim h\}.$$

c) „Wolf, Ziege, Kohlkopf"
Das Problem geht schon auf Flacus Albinus Alkuin ($\approx$ 735–804), einen Berater Karls des Großen zurück.
W, Z und K sollen vom linken Ufer (l) eines Flusses an das rechte (r) gebracht werden, wobei im Boot außer dem Fährmann nur ein Lebewesen Platz hat. Außerdem muß der Fluß der Nahrungskette verhindert werden: Es darf weder W mit Z noch Z mit K allein bleiben.



Bei gegebenem Anfangszustand (gesetzte Markierungen) entsteht die Dynamik durch das Verschieben der Markierungen:
Sid alle Bedingungen eines Ereignisses erfüllt, kann „geschaltet (gefeuert)“ werden: die Markierungen wandern zu den Nachbedingungen des Ereignisses (die Anzahl der Markierungen braucht dabei nicht konstant zu bleiben).

Definition 50 (Petrinetz)

α) Ein Digraph $\mathcal{N} = (\mathcal{E}, \mathcal{K}, \varphi)$ mit $\mathcal{K} \subseteq \mathcal{E} \times \mathcal{E}$ und $\varphi = 1_{\mathcal{K}}$ heißt **Petrinetz** im Falle

I. $\mathcal{E} = \mathfrak{z} \cup \mathfrak{t}$ mit $\mathfrak{z} \cap \mathfrak{t} = \emptyset$, also $\mathcal{E} = \mathfrak{z} \oplus \mathfrak{t}$.
Die Elemente von $\mathfrak{z}$ heißen **Zustände** (Bedingungen, Stellen, Plätze, S-Elemente) (conditions, places) und werden mit mit „Rundem“, etwa , symbolisiert.
Die Elemente von $\mathfrak{t}$ heißen **Ereignisse** (Transitionen, Aktionen, Hürden, T-Elemente) (events, transitions) und werden mit „Eckigem“, etwa , symbolisiert.

II. $\mathcal{K} \subseteq (\mathfrak{z}, \mathfrak{t}) \cup (\mathfrak{t}, \mathfrak{z})$ heißt auch **Flußrelation**.

Gelegentlich wird noch $\forall S \in \mathfrak{z}\ \forall T \in \mathfrak{t}: \ |\{(S,T),(T,S)\} \cap \mathcal{K}| \leq 1$ gefordert.

III. $\forall E \in \mathcal{E}\ \exists X \in \mathcal{E}: \ (E,X) \in \mathcal{K} \ \vee \ (X,E) \in \mathcal{K}$

β) $(\mathcal{N}, \mu)$ heißt **markiertes Petrinetz** und μ dann **Markierung** von $\mathcal{N}$, falls $\mathcal{N}$ Petrinetz ist und

$$\mu : \ \mathfrak{z} \longrightarrow \{0,1\} \text{ gilt.}$$

γ) Für ein markiertes Petrinetz wie in β) sei $T \in \mathfrak{t}$ ein Ereignis und

$$\bullet T \rightleftharpoons \{S \in \mathfrak{y};\ (S,T) \in \mathcal{K}\} \text{ bzw. } T\bullet \rightleftharpoons \{S \in \mathfrak{y};\ (T,S) \in \mathcal{K}\}$$

der **Vor-** bzw. **Nachbereich** von T.

T heißt **aktiviert** unter μ, falls

$$\mu \bullet T \subseteq \{1\} \ \wedge \ \mu T\bullet \subseteq \{o\} \text{ gilt.}$$

$\mu' \in \{0,1\}$ heißt **Folgemarkierung** von μ unter T im Falle

$$\mu' = \mu\lceil_{\mathfrak{y}\setminus(\bullet T \cup T\bullet)} \cup (\bullet T \times \{0\}) \cup (T \bullet \times \{1\}).$$

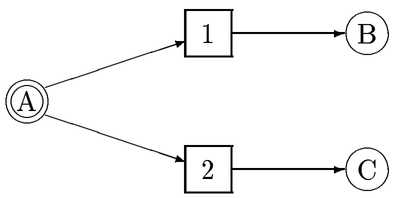
Wir sagen T **schaltet** von μ nach μ', kurz $\mu\langle T\rangle\mu'$, falls T unter μ aktiviert ist und man von μ zur Folgemarkierung μ' von μ unter T übergeht.

Bemerkung 31
In der Theorie der Petrinetze werden auch kompliziertere Konzepte als die in Definition 50 genannten untersucht. So läßt man etwa mehrere unterschiedliche Marken pro S-Element zu und versieht die Kanten mit Kapazitäten. Ferner werden Verfeinerungen und damit auch Vergrößerungen von Petrinetzen behandelt. Auch das Versehen der Kanten mit „Abfragen“, logischen Verzweigungen ist möglich.

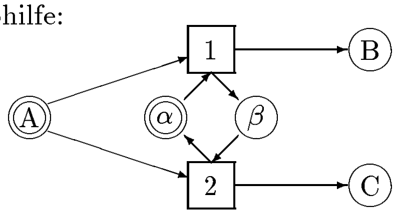
Inzwischen gibt es auch einsetzbare Software für Petrinetze.

Beispiel 48
Konflikte:

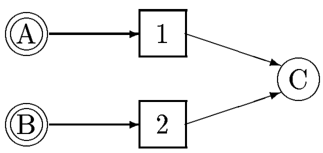
a) **Verzweigungskonflikt** (branch conflict):



Abhilfe:



b) **Wettbewerbskonflikt** (meet conflict):



Abhilfe: ähnlich wie in a)

Kapitel 3

Rechner

3.1 Zahldarstellungen

3.1.1 g-adische Darstellungen

Beispiel 49

1) Zehnersystem (**dekadisch**, dezimal, denär)

   I. „Schriftliches Rechnen“: Grundschule; gilt allgemein für jedes Positionssystem

   II. Teilbarkeitsregeln:

      α) Eine (natürliche) Zahl ist genau dann gerade, wenn sie auf 0, 2, 4, 6 oder 8 endet. Beweis: Übung!

      β) Eine Zahl ist genau dann durch 3 bzw. 9 teilbar, wenn ihre Quersumme durch 3 bzw. 9 teilbar ist. Beweis: Übung!

   III. Dezimalklassifikation

2) Zweiersystem (**dyadisch**, **dual**, binär)
   erstmals in unveröffentlichtem Manuskript (ca. 1605) von Harriot, dann Caramuel und Leibniz

   I. Länge der Noten

   II. Englische Hohlmaße:
   1 tun = 2 pipes = 2^2 hogsheads = 2^3 barrels = 2^4 kilderkins = 2^5 firkins (bushels) = 2^6 demibushels = 2^7 pecks = 2^8 gallons = 2^9 pottles = 2^{10} quarts = 2^{11} pints = 2^{12} chopins = 2^{13} gills

   III. $7 \cdot 13 = 91$

$$
\begin{array}{ccccccccccc}
 & & & 1 & 1 & 0 & 1 & \cdot & 1 & 1 & 1 \\
 & & 1 & 1 & 0 & 1 & & & & & \\
 & 1 & 1 & 0 & 1 & & & & & & \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 1 & & & & \\
64 & & +16 & +8 & & +2 & +1 & = & 91 & &
\end{array}
$$

3) Andere Basen
   Modulare Arithmetiken (soft– oder hardwaremäßig realisiert) in Computern, aber auch in Codes und Kryptographie.

Definition 51
Sei $g \in \mathbb{N} \setminus \{1\}$, die Basis oder Radix,
und seien bzw. $\zeta_0, \zeta_1, \ldots, \zeta_{g-1}$ g verschiedene Ziffern, d. h. (atomare) Zeichen für die Zahlen bzw. $0, 1, \ldots, g-1$,
ferner $Z \rightleftharpoons \{\zeta_\gamma; \gamma \in \mathbb{U}_g\}$,
$Z' \rightleftharpoons Z \setminus \{\zeta_0\}$
und $A \rightleftharpoons Z'Z^* \cup \{\zeta_0\}$ mit der Konvention, daß $\sqcup$ ($\in Z^*$) als Faktor nicht geschrieben wird (ohne führende Nullen)
sowie $\alpha : A \longrightarrow \mathbb{N}_0$ mit

$$\alpha(Z) = \begin{cases} 0 & \Leftarrow Z = \zeta_0 \\ \sum_{\nu=0}^{n} & \Leftarrow Z = \zeta_{a_n}\zeta_{a_{n-1}}\cdots\zeta_{a_0} \end{cases}$$

Satz 69

$$\alpha : A \rightarrowtail\!\!\!\twoheadrightarrow \mathbb{N}_0$$

Beweis: Übung. (siehe auch Lucht, Analysis I, §21)

Beispiel 50

a) Als Basen sind vor allem verbreitet: 2, 3, 4, 8, 10, 12, 16, 20, 60

b) Sechzehnersystem (hexadezimal, semidenarisch, hekkaidekadisch, sexadezimal)
   $g = 16 : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$

Definition 52
Bezeichnungen wie oben.

α) $\alpha^{-1}(a)$ heiße g-adische Darstellung (polyadische Darstellung, Positionssystem mit Basis g) von $a \in \mathbb{N}_0$.

β) Sei $- \notin Z$
   und $B \rightleftharpoons A \cup \{-\} ZZ^*$
   sowie $\beta : B \longrightarrow \mathbb{Z}$ mit

$$\beta(Z) = \begin{cases} \alpha(Z) & \Leftarrow Z \in A \\ -\alpha(Z') & \Leftarrow Z = -Z' \end{cases}$$

Satz 70 $\beta : B \rightarrowtail\!\!\!\twoheadrightarrow \mathbb{Z}$

Beweis:
mit Satz 69 trivial

Satz 71
Sei $g \in \mathbb{N} \setminus \{1\}$ und $G \eqqcolon \mathbb{U}_g$.

a) Für $n \in \mathbb{N}_0$ und $a_\nu \in G \cup -G$ mit $\nu \in \mathbb{U}_{n+1}$ gilt

$$\sum_{\nu=0}^{n} a_\nu g^\nu < g^{n+1} \tag{1}$$

und

$$\sum_{\nu=0}^{n} a_\nu g^\nu = 0 \Leftrightarrow a_0 = a_1 = ldots = a_n = 0. \tag{2}$$

b) $$\forall a \in [0,1[\ \forall n \in \mathbb{N} \overset{1}{\exists} (a_1, \ldots, a_n) \in G^n \overset{1}{\exists} r \in [0, g^{-n}[\ : a = \sum_{\nu=1}^{n} a\nu g^{-\nu} + r.$$

c) Zu jeder nichtnegativen reellen Zahl a und jedem $\varepsilon \in \mathbb{R}^+$ gibt es ein minimales $m \in \ltimes_0$ und ein minimales $n \in \mathbb{N}_0$ mit

$$\overset{1}{\exists} (a_m, a_{m-1}, \ldots, a_1, a_0, a_{-1}, \ldots, a_{-(n-1)}, a_{-n}) \in G^{m+n+1} : 0 \leq a - \sum_{\nu=-n}^{m} a_\nu g^\nu < \varepsilon.$$

(Reelle Zahlen sind beliebig genau und eindeutig, also g-adisch darstellbar.)

Beweis:

a) (70): $\sum_{\nu=0}^{n} a_\nu g^\nu \leq \sum_{\nu=0}^{n} (g-1) g^\nu = (g-1)\frac{g^{n+1}-1}{g-1} < g^{n+1}$

(71): $\Leftarrow$: trivial

$\Rightarrow$: Induktion nach n:

IA: $n = 0 \Rightarrow a_0 g^0 = 0 \Rightarrow a_0 = 0$

IS: $0 = \sum_{\nu=0}^{n+1} a_\nu g^\nu = \sum_{\nu=0}^{n} a_\nu g^\nu + a_{n+1} g^{n+1}$,

mithin $|a_{n+1}| g^{n+1} = |a_{n+1} gn + 1| = |\sum_{\nu=0}^{n} a_\nu g^\nu| \leq \sum_{\nu=0}^{n} |a_\nu| g^\nu \overset{(70)}{<} g^{n+1}$,

daher $|a_{n+1}| < 1$ und somit $a_{n+1} = 0$, was $\sum_{\nu=0}^{n} a_\nu g^\nu = 0$ bedingt,

nach IV also $a_0 = a_1 = \ldots = a_n = 0 = a_{n+1}$.

b) Eindeutigkeit:

Sei $(b_1, \ldots, b_n) \in G^n$ und $s \in [0, g^{-n}[$ mit $\sum_{\nu=1}^{n} b_\nu g^{-\nu} + s = a = \sum_{\nu=1}^{n} a_\nu g^{-\nu} + r$

Mit $c_\nu \eqqcolon a_\nu - b_\nu \in G \cup -G; \nu \in \mathbb{A}_n$

folgt $0 = \sum_{nu=1}^{n} a_\nu g^{-\nu} + r - (\sum_{\nu=1}^{n} b_\nu g^{-\nu} + s) = \sum_{\nu=1}^{n} c_\nu g^{-\nu} + r - s$

und wegen $-g^{-n} < r - s < g^{-n}$ mit $c_0 \eqqcolon 0$

weiter $0 = \sum_{\nu=1}^{n} c_\nu g^{-\nu} + r - s = \underbrace{\sum_{\nu=1}^{n} c_\nu g^{n-\nu}}_{\in \mathbb{Z}} + \underbrace{(r-s) g^n}_{\in]-1,1[}$

also $(r - s) g^n \in \mathbb{Z} \cap \,]-1, 1[$, mithin $r = s$

und daher $\sum_{\nu=0}^{n} c_{n-\nu} g^{\nu} = 0$, nach (71) somit $\forall \nu \in \mathbb{A}_n : 0 = c_\nu = a_\nu - b_\nu$,
also $a_\nu = b_\nu$.
Existenz:
Sei $b \rightleftharpoons \lfloor ag^n \rfloor$, etwa $ag^n = b + s$ mit $s \in [0, 1[$.
Nach Satz 69 gibt es $m \in \mathbb{N}_0$ und $b_\nu \in G$ für $\nu \in \mathbb{A}_m$ mit
$b = \sum_{nu=0}^{m} b_\nu g^\nu$ und $m > 0$, mithin $b_n > 0$,
also $(*)$ $a = \sum_{\nu=0}^{m} b_\nu g^{\nu-n} + sg^{-n}$.
Wegen $m > 0 \Rightarrow g^m \leq \sum_{\nu=0}^{m} b_\nu g^\nu \leq ag^n < g^n$,
$m = 0 \Rightarrow m < n$,
mithin $1 \leq n - m$ und $sg^{-n} \in [0, g^{-n}[$
wird mit $a_1 \rightleftharpoons a_2 \rightleftharpoons \ldots \rightleftharpoons a_{n-m-1} \rightleftharpoons 0$,
der Indexverschiebung $a_{n-m+\lambda} \rightleftharpoons b_{m-\lambda}; \lambda \in \mathbb{A}_m$
und $r \rightleftharpoons sg^{-n}$
aus $(*)$ das Gewünschte erreicht.

c) Sei $a \in \mathbb{R}^+ \cup \{0\}$ und $\varepsilon \in \mathbb{R}^+$ sowie $b \rightleftharpoons \lfloor a \rfloor$, etwa $a = b + c$ mit $c \in [0, 1[$.
Nach Satz 69 gibt es ein minimales $m \in \mathbb{N}_0$ und ein eindeutig bestimmtes $a_\nu \in G$
mit $(**)$ $b = \sum_{\nu=0}^{m} a_\nu g^\nu$
Im Falle $\varepsilon \geq 1$ ist $a - \sum_{\nu=0}^{m} a_\nu g^\nu = a - b = c < 1 \geq \varepsilon$
und mit dem minimalen $n = 0$ ist alles erreicht.
Sei also $\varepsilon < 1$. Dann gilt $1 < \varepsilon^{-1}$,
mithin $0 = \log_g 1 < \log_g \varepsilon^{-1}$
und daher $n \rightleftharpoons \lceil \log_g \varepsilon^{-1} \rceil \in \mathbb{N}$
sowie $\log_g \varepsilon^{-1} \leq n$, also $\varepsilon^{-1} \leq g^n$, damit $g^{-n} \leq \varepsilon$
und n ist aufgrund der Konstruktion minimal mit dieser Eigenschaft.
Nach b) existiert genau dann ein $(a_{-1}, a_{-2}, \ldots, a_{-n}) \in G^n$ und $r \in [0, g^{-n}[\ \subseteq [0, \varepsilon]$
mit $c = \sum_{\nu=-n}^{-1} a_\nu g^\nu + r$,
was

$$\begin{aligned} a - \sum_{\nu=-n}^{m} a_\nu g^\nu &= b + c - \sum_{\nu=-n}^{-1} a_\nu g^\nu - \sum_{\nu=0}^{m} a_\nu g^\nu \\ &\overset{(**)}{=} \underbrace{b - \sum_{\nu=0}^{m} a_\nu g^\nu}_{=0} + \underbrace{c - \sum_{\nu=-n}^{-1} a_\nu g^\nu}_{=r} \\ &= r < \varepsilon \end{aligned}$$

liefert.

Korollar:
Zu jedem $g \in \mathbb{N} \setminus \{1\}$ und jedem nichtnegativen a gibt es genau ein $m \in \mathbb{N}_0$ und genau ein $M \in \{\mathbb{U}_{m+1}\} \cup \mathcal{E} \cup \mathcal{U}$ mit
$\mathcal{E} \rightleftharpoons \{\mathbb{U}_{m+1} \cup -\mathbb{U}_{n+1}; n \in \mathbb{N}\}$
$\mathcal{U} \rightleftharpoons \{\mathbb{U}_{m+1} \cup -\mathbb{N}\}$
und eindeutig bestimmtem $a_\nu \in \mathbb{U}_g$ für $\nu \in M$, so daß $a = \sum_{\nu \in M} a_\nu g^\nu$ mit
$a_m \neq 0$ für $m > 0$,
$a_{\min\{M\}} \neq 0$ für $M \in \mathcal{E}$ und
$\forall k \in \mathbb{N} (\exists \kappa \in \mathbb{N} \setminus \mathbb{A}_k : a_{-\kappa} \neq g - 1 \wedge \exists \lambda \in \mathbb{N} \setminus \mathbb{A}_k : a_{-\lambda} \neq 0)$ für $M \in \mathcal{U}$.

Beweis: Übung.

Definition 53
Bezeichnungen wie oben.
Sei $, \notin Z \cup \{-\}$
und $E \rightleftharpoons \{,\}\, Z^* Z'$,
sowie $C \rightleftharpoons B \cup AE \cup \{-\}\, AE$
und $\gamma : C \longrightarrow \mathbb{Q}$ mit $\gamma_{\lfloor B} \rightleftharpoons \beta$, $\gamma(-Z) = -\gamma(Z)$ und $\gamma(\zeta_{a_n}, \ldots, \zeta_{a_0}, \ldots, \zeta_{a_{-m}}) \rightleftharpoons \sum_{\nu=-m}^{n} a_\nu g^\nu$,
ferner $\Gamma \rightleftharpoons \gamma(C)$.

Satz 72

a) $$\gamma : C \rightarrowtail\!\!\!\twoheadrightarrow \Gamma$$

b) $\Gamma = \{0\} \cup \left\{\frac{a}{b}; a \in \mathbb{Z} \setminus \{0\} \wedge b \in \mathbb{N} \wedge \operatorname{ggT}(a,b) = 1 \wedge \exists k \in \mathbb{N} : b \mid g^k\right\}$

c) $\Gamma \neq \mathbb{Q}$

I. Γ liegt dicht in $\mathbb{R}$, $\mathbb{Q}$ und in sich und ist abzählbar unendlich.

II. $\mathbb{R} \setminus \Gamma$ liegt dicht in $\mathbb{R}$, $\mathbb{Q}$ und in sich und ist überabzählbar.

III. $\mathbb{Q} \setminus \Gamma$ liegt dicht in $\mathbb{R}$, $\mathbb{Q}$ und in sich und ist abzählbar unendlich.

Beweis:

a) $\twoheadrightarrow$: per definitionem
$\rightarrowtail$: Folgt aus Korollar zu Satz 71

b) R sei die rechte Seite der behaupteten Gleichung.

I. Sei $c \in \Gamma$, oBdA $0 \leq c = \sum_{\nu=m}^{n} a_\nu g^\nu$ mit $m, n \in \mathbb{Z}$, $m \leq n$ und $a_\nu \in \mathbb{U}_g$.
Da $c \in \mathbb{Q}$ folgt $c = 0$ oder die Existenz von $a \in \mathbb{Z} \setminus \{0\}$ und $b \in \mathbb{N}$ mit $c = \frac{a}{b}$ und $\operatorname{ggT}(a,b) = 1$.
Sei $c \neq 0$. Wegen $c = \sum_{\nu=m}^{n} a_\nu g^\nu$ gibt es ein $k \in \mathbb{N}$ mit $\frac{a}{b} g^k = c g^k \in \mathbb{N}$
und wegen $\operatorname{ggT}(a,b) = 1$ folgt $b \mid g^k$.
Damit ist $c \in R$, also $\Gamma \subseteq R$.

II. Sei $c \in R$, oBdA $c = \frac{a}{b}$ mit $g^k = tb$ und $a, b, k, t \in \mathbb{N}$.
Dann hat man $c g^k = \frac{a}{b} tb = at \in \mathbb{N}$,
nach Satz 69 also die Existenz von $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in \mathbb{U}_g$ mit $a_n \neq 0$ und $at = \sum_{\nu=0}^{n} a_\nu g^\nu$,
daher $c = atg^{-k} = \sum_{\nu=0}^{n} a_\nu g^{\nu-k}$
und somit nach Beseitigung etwaiger Endnullen ein $z \in C$ mit $\gamma(z) = c$,
was $R \subseteq \Gamma$ beweist.

c) Laut Definition ist $\Gamma \in \mathbb{Q}$ und wegen $g+1 \not| g^k$ für $k \in \mathbb{N}$ hat man b) zufolge $(g+1)^{-1} \in \mathbb{Q} \setminus \Gamma$.

I. Im Falle $x < 0 < y$ $c \rightleftharpoons 0$.
Sei also oBdA $0 \leq x < y$ und $\varepsilon \rightleftharpoons \frac{y-x}{2}$, also $y, \varepsilon \in \mathbb{R}^+$.
Dann gibt es nach Satz 71c) ein $c \in \Gamma$ mit $0 \leq y - \varepsilon - c \leq \varepsilon$,

was $x = y - 2\varepsilon < c \leq y - \varepsilon < y$ bedingt,
woraus $\forall x, y \in \mathbb{R} : x < y \Rightarrow \exists c \in \Gamma : x < c < y$ folgt.
Wegen $\mathbb{Z} = \beta(B) = \gamma(B) \subseteq \gamma(C) = \Gamma \subseteq \mathbb{Q}$ hat man $|\mathbb{N}| = |\mathbb{Z}| \leq |\Gamma| \leq |\mathbb{Q}| = |\mathbb{N}|$, also $|\Gamma| = |\mathbb{N}|$.

II. Übung.

III. Übung.

Bemerkung 32
Für jedes $g \in \mathbb{N} \setminus \{1\}$ ist es für eine beliebige reelle Zahl r ein ganz unwahrscheinlicher Glücksfall, daß sich r durch eine endliche g-adische Entwicklung exakt darstellen läßt. Nach Korollar zu Satz 71 kann r jedoch beliebig genau approximiert werden.
Bei Implementation, wo es auf den genauen Umgang mit rationalen Zahlen ankommt, muß daher ein $r \in \mathbb{Q}$ als Paar (a, b), etwa aus $\mathbb{Z} \times \mathbb{Z}$, behandelt werden (siehe etwa D. Knuth „The Art of Computer Programming II", 213 ff oder H. Isselhorst „Ein Beitrag zur Verwendung rationaler Zahlen in Public-Key Kryptosystemen", Heidelberg 1988).

Definition 54
Bezeichnungen wie oben.

α) $\gamma^{-1}(a)$ heißt g-adische Darstellung (polyadische Darstellung, Darstellung im g-er System, Positionssystem zur Basis g, zur Radix g) von $a \in \Gamma$.

β) Entsprechend für unendliche Folgen gemäß dem Korollar zu Satz 71.

Beispiel 51 (Umrechnung nach (Ruffini-) Horner-Schema)
Horner-Schema: Polynomauswertung, Berechnung eines Funktionswertes einer ganzrationalen Funktion durch sukzessives Ausklammern des Argumentes:

		Zahl der Multiplikationen	allgemein für Grad n
$(54321)_6$	$=$		
	$= 1 + 2 \cdot 6 + 3 \cdot 6^2 + 4 \cdot 6^3 + 5 \cdot 6^4$	$\frac{4 \cdot 5}{2}$	$\binom{n}{2}$
	$= (((5 \cdot 6 + 4) \cdot 6 + 3) \cdot 6 + 2) \cdot 6 + 1$	4	n
	$= 7465$		

Das Horner-Schema ist leicht zu programmieren und in gewisser Weise optimal (siehe Belaga et al. 1961).

Satz 73
Sei $a \in \mathbb{N}_0$ und $\sum_{\nu=0}^{n} a_\nu g^\nu$ die g-adische Darstellung von a. Der folgende Algorithmus berechnet zu gegebenem a die Größen n und a_ν, dabei stehe A, G, N, M für a, g, n, m mit $a < g^m$:

```
program GAD (input,output);          {G-ADISCHE DARSTELLUNG}
const   M=
var     A, G, I, N, R: integer;
        P: array[0...M] of integer;
begin
    readln(G,A);
    R:=A; I:=0;
    repeat
```

```
        P(I):=R mod G;
        R:=R div G;
        I:=I+1
    until R=0;
    N:=I-1;
    writeln(N);
    for I:=N downto 0 do
        writeln(P(I))
end.
```

Beweis:
Aus $a = \sum_{\nu=0}^{n}$ folgt für den nichttrivialen Fall $k \neq 0$ sofort

$$ag^{-k} = \underbrace{\sum_{\nu=0}^{k-1} a_\nu g^{\nu-k}}_{<1} + a_k + \underbrace{\sum_{\nu=k+1}^{n} a_\nu g^{\nu-k}}_{\in\mathbb{N}_0}$$

also $a \operatorname{div} g^k = \underbrace{g \sum_{\nu=k+1}^{n} a_\nu g^{\nu-(k+1)}}_{\in\mathbb{N}_0} + \underbrace{a_k}_{<g}$

mithin $a_k = (a \operatorname{div} g^k) \bmod g$.

Entsprechend ergibt sich $a = \underbrace{g^{k+1} \sum_{\nu=k+1}^{n} a_\nu g^{\nu-(k+1)}}_{\in\mathbb{N}_0} + \underbrace{\sum_{\nu=0}^{k} a_\nu g^\nu}_{<g^{k+1}}$

somit $a \bmod g^{k+1} = a_k g^k + \underbrace{\sum_{\nu=0}^{k-1} a_\nu g^\nu}_{\overset{(70)}{<} g^k}$

ferner $(a \bmod g^{k+1}) g^{-k} = a_k + \underbrace{\sum_{\nu=0}^{k-1} a_\nu g^{\nu-k}}_{<1}$

und daher $a_\nu = (a \bmod g^{k+1}) \operatorname{div} g^k$.
Die Verifikation des angegebenen Programmes folgt dann aus
$a_k = (a \operatorname{div} g^k) \bmod g = (a \bmod g^{k+1}) \operatorname{div} g^k$.

Beispiel 52 (Umrechnung vom dekadischen in das binäre System)

7465	
3732	R1
1866	
933	
466	R1
233	
116	R1
58	
29	
14	R1
7	
3	R1
1	R1
0	R1

also $(7465)_{10} = (1\,110\,100\,101\,001)_2$

3.1.2 Gleitkommazahlen

Beispiel 53
In einem binär arbeitenden Computer (32-Bit-Prozessor) sollen zur Speicherung von Zahlen je 4 Byte verwandt werden. Benutzt man ein Bit als Vorzeichen und repräsentiert man die die Zahlen in Dualdarstellung, wobei das Komma an einer festen Stelle gedacht sei (**Festkommadarstellung**, fixed-point representation), kann man an nichtnegativen etwa darstellen
alle ganzen Zahlen 0, ..., 2^{31}-1=2 147 483 647
oder alle rationalen Zahlen 2^{-15}=0,000 030 517 578 125, ..., 2^{16}=65536 im Abstand von 2^{-15}.
Für Anwendungen in Natur, Technik, Verwaltung, Mathematik ist das jedoch oft vielfach zu wenig.
Eine Abhilfe könnten geeignete Faktoren schaffen.

Definition 55

$\alpha)$ Ein Paar (m, e) heißt **Gleitkommadarstellung** oder **Fließkommadarstellung** (floating-point representation) von mB^e im Falle $m \in]-1, 1[$ (üblicherweise als Festkommazahl), $e \in \mathbb{Z}$ (üblicherweise als Festkommazahl) und $B \in \mathbb{N} \setminus \{1\}$.

$\beta)$ m wird auch **Mantisse** (fixed-point part), e **Exponent** (exponent) und B **Basis** (radix) genannt.

$\gamma)$ $G \rightleftharpoons]-1, 1[\times \mathbb{Z}$
$\gamma_B \rightleftharpoons (m, e) \mapsto m \cdot B^e$ mit $D_{\gamma_B} \rightleftharpoons G$.

Satz 74
$\forall B \in \mathbb{N} \setminus \{1\} : \gamma_B : G \twoheadrightarrow \mathbb{R}$

Beweis:
$\gamma_B : G \longrightarrow \mathbb{R}$ per definitionem.
Mit $n \in \mathbb{N}$ ist $\gamma_B(B^{-n}, n) = B^{-n}B^n = 1$, γ_B nicht injektiv.
Sei $a \in \mathbb{R}$.
Im Falle $a = 0$ gilt: $\gamma_B(0, e) = a$ für jedes $e \in \mathbb{Z}$.
Für $a \neq 0$ gibt es Satz 71c) zufolge $n \in \mathbb{Z}$ mit
$(*)$ $B^{n-1} \leq |a| < B^n$,

damit folgt $|aB^{-n}| = |a|B^{-n} < 1$ und $\gamma_B(aB^{-n}, n) = aB^{-n}B^n = a$,
mithin die Surjektivität von γ_B auf $\mathbb{R}$.
Um Injektivität von γ_B auf $\mathbb{R}$ zu erhalten, legt man fest:

Definition 56

α) Die Gleitkommazahl (m, e) heißt normalisiert im Falle
$m = e = 0$ oder $B^{-1} \leq |m| < 1$.

β) N_B sei die Menge der bezüglich B normalisierten Gleitkommazahlen.

γ) $\beta_B \rightleftharpoons \gamma_{B\lfloor N_B}$

Satz 75

$$\beta_B : N_B \rightarrowtail\!\!\!\twoheadrightarrow \mathbb{R}$$

Beweis:
$\beta_B : N_B \longrightarrow \mathbb{R}$ per definitionem.

$\twoheadrightarrow$: Sei $a \in \mathbb{R}$.
Für $a = 0$ ist $(0, 0) \in \gamma_B^{-1}(a) \cap N_B$.
Im Falle $a \neq 0$ gibt es dem Beweis von Satz 74 zufolge $n \in \mathbb{Z}$ mit $B^{n-1} \leq |a| < B^n$
und daher $B^{-1} \leq |a|B^{-n} < 1$,
mithin $(aB^{-n}, n) \in \gamma_B^{-1}(a) \cap N_B$.

$\rightarrowtail$: Sei $\beta \rightleftharpoons \beta_B$ und $(m, e), (m', e') \in N_B$ sowie

a) $0 = \beta(0, 0) = \beta(m, e) = mB^e$, also ist $m = 0$ und daher $e = 0$.

b) $m \neq 0$ und $mB^e = \beta(m, e) = \beta(m', e') = m'B^{e'}$,
mithin gilt $B^{-1} \leq |m| = |m'|B^{e'-e} < 1$
und weiter $-1 \leq \underbrace{\log_B |m'|}_{>-1} + e' - e < 0$, also $-1 < e' - e < 1$,
wegen $e', e \in \mathbb{Z}$ aber $e' = e$ und damit auch $m' = m$.

Definition 57
$\nu_B \rightleftharpoons \beta_B^{-1} g_B$ heißt Normalisierungsfunktion mit $g_B \rightleftharpoons (m, e) \mapsto mB^e$ und $D_{g_B} \rightleftharpoons \mathbb{R} \times \mathbb{Z}$.

Satz 76

a) $\nu_B : \mathbb{R} \times \mathbb{Z} \twoheadrightarrow N_B$

b) $\forall (m, e) \in \mathbb{R} \times \mathbb{Z} : g_B(\nu_B(m, e)) = g_B(m, e)$

c) $\nu_B^2 = \nu_B$

Beweis:

a)
$$\begin{tikzcd}
\mathbb{R} \times \mathbb{Z} \arrow[rr, "\nu"] \arrow[dr, "g", "\text{Satz 74}"'] & & N \arrow[dl, bend left, two heads, "\beta", "\text{Satz 75}"'] \\
& \mathbb{R} \arrow[ur, bend left, tail, two heads, "\beta^{-1}"] &
\end{tikzcd}$$

b) Folgt aus $g\nu = \beta\beta^{-1}g = g$

c) Nach b) gilt $g\nu = g$, also $\nu^2 = \beta^{-1}g\nu = \beta^{-1}g = \nu$

Definition 58
Für $(m, e), (m', e') \in \mathbb{R} \times \mathbb{Z}$ sei

$$\begin{aligned}
(m, e) + (m', e') &\rightleftharpoons \nu(m + m'B^{e'-e}, e) \\
(m, e) - (m', e') &\rightleftharpoons \nu(m - m'B^{e'-e}, e) \\
(m, e) \cdot (m', e') &\rightleftharpoons \nu(m \cdot m', e + e') \\
\frac{(m, e)}{(m', e')} &\rightleftharpoons \nu(\frac{m}{m'}, e - e'))
\end{aligned}$$

Satz 77
Sei $* \in \{+, -, \cdot, \div\}$.

a) $\nu_B : (\mathbb{R} \times \mathbb{Z}, *) \overset{\sim}{\twoheadrightarrow} (N_B, *)$

b) $\beta_B : (N_B, *) \overset{\sim}{\rightarrowtail\!\!\!\twoheadrightarrow} (\mathbb{R}, *)$

c) $g_B : (\mathbb{R} \times \mathbb{Z}, *) \overset{\sim}{\twoheadrightarrow} (\mathbb{R}, *)$

Beweis:

a) Übung.

b) Übung.

c) ohne Index B:
$$\begin{tikzcd}
\mathbb{R} \times \mathbb{Z} \arrow[rr, two heads, "\nu \quad \overset{a)}{\sim}"] \arrow[dr, "g"'] & & N \arrow[dl, bend left, two heads, "\beta", "\overset{b)}{\sim}"'] \\
& \mathbb{R} &
\end{tikzcd}$$

Beispiel 54
In je einem 1-Byte-Register sollen $x = (m, e)$ und $y = (m', e')$ aus N_2 gespeichert werden. Dabei habe die Mantisse bzw. der Exponent 5 bzw. 3 Stellen inklsive einer Vorzeichenstelle, der jeweils ersten, und beide Größen sollen als duale Festkommazahlen dargestellt werden. Speziell sei

$$\begin{array}{l} x = 01\,001\,010 \\ y = 01\,000\,011 \end{array} \text{, also } \begin{array}{l} \beta_2(x) = \left(\frac{1}{2} + \frac{1}{16}\right) 2^2 = 2 + \frac{1}{4} = 2,25 \\ \beta_2(y) = \frac{1}{2} 2^3 = 4 \end{array}$$

mithin $\beta_2(x) + \beta_2(y) = 6,25$.
In Gleitkommarechnung:
$x + y = \nu(m + m' 2^{e'-e}, e) = \nu\left(\frac{1}{2} + \frac{1}{16} + \frac{1}{2}2, 2\right) = \beta_2^{-1} g_2\left(\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{32}\right), 2\right)$
$= \beta_2^{-1}\left(\left(\frac{1}{2} + \frac{1}{4} + \frac{1}{32}\right) 2^3\right)$
$\hat{=}\ 01\,100\,011 = 6$, oder
$\hat{=}\ 01\,101\,011 = 6,5$.

Bemerkung 33

a) Wie Beispiel 54 zeigt, gibt es bei der Gleitkommadarstellung im Rechner Intervalllücken, in die, schon bei der Addition, im Gegensatz zur Festkomma-Arithmetik, ein Rechenergebnis fallen kann, das dann gerundet und damit verfälscht wird.

b) Diese Lücken sind im allgemeinen nicht äquidistant.

c) Sowohl bei Festkomma- wie auch bei Gleitkomma-Arithmetik können Operationen, auch außerhalb dieser Lücken, aus dem Bereich der darstellbaren Zahlen herausführen, nach oben als Überlauf, nach unten als Ünterlauf bezeichnet.

d) Die unter a) und c) genannten Fakten führen dazu, daß für die im Rechner darstellbaren Zahlen, etwa $Z \subseteq \mathbb{Z}$ (integer) und $R \subseteq \mathbb{R}$ (real) die üblichen Rechengesetze für den Ring $(\mathbb{Z}, +, \cdot)$ und den Körper $(\mathbb{R}, +, \cdot)$ nicht mehr gelten.
Die Operationen $+, -, \cdot, \div$ sind lediglich partielle Funktionen in Z bzw. R, sogar die Assoziativität von $+$ gilt deshalb nicht mehr.

e) Exponenten werden gelegentlich in der Darstellung um die Hälfte des zulässigen Bereichs verschoben (**Charakteristik**), um Vorzeichen zu sparen.

f) Die **Rundungsfehlerproblematik** sollte schon bei der Hardware des Prozessors und des floating-point prozessor's berücksichtigt werden. Sonst muß dies wenigstens bei der Software geschehen!

g) Ergebnisse messender Wissenschaften sind prinzipiell fehlerhaft, hinzu kommen Rundungs- und formale Fehler. Eine Abhilfe schafft dabei eine sorgfältige Intervallmathematik.

3.1.3 Tetradencodes

Bemerkung 34
Vielfach muß „Information“ codiert, d. h. anders als ursprünglich dargestellt werden, etwa aus technischen Gründen (Binärsystem) oder zum Zwecke der Fehlererkennung, -korrektur, Verschleierung (Kryptologie) oder Datenkompression (Bildverarbeitung) etc.
Hier nur die allereinfachsten Anfänge zu üblichen Codierungen im Rechner.

Definition 59
A und B seien endliche, nichtleere Zeichenvorräte.

α) $c : A \rightarrowtail B^+ \rightleftharpoons B^* \setminus \{\sqcup\}$ heißt A-B-Codierung.

β) $C \rightleftharpoons c(A)$ wird Code über B genannt und die Element von C Codewörter w über B.

γ) Ein Code bzw. eine Codierung über B heißt q-när im Falle $|B| = q$, insbesondere für $q = 1, 2, 3, 4$ bzw. unär, binär, ternär, quaternär.

δ) Für $w \in C$, allgemeiner für $w \in B^*$, bezeichne wie üblich $|w|$ die Länge von w.
Gilt $\exists l \in \mathbb{N} \forall w \in C : |w| = l$ heißt C Blockcode der Länge l.

Beispiel 55
Sei $Z = \{0, 1, \ldots, 9\}$.

a) Zahlcodierung (altes Telefonsystem) $t : Z \rightarrowtail \mathbb{B}^+$ gemäß:

Z	$t(Z)$
1	L0
2	LL0
3	LLL0
⋮	⋮
9	LLLL LLLLL0
0	LLLLL LLLLL0

Vorteil: einfache technische Realisierung
Nachteil: Weder fehlererkennend noch -korrigierend

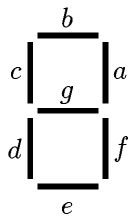
b) 1-aus-10-Code (allgemeiner: 1-aus-n-Code mit $n \in \mathbb{N} \setminus \{1\}$):

0	00000 0000L
1	00000 000L0
2	00000 00L00
⋮	⋮
9	L0000 00000

wird auch Kettencode genannt.

c) Zifferndarstellung auf Leuchtschirmen:
Sei $A \rightleftharpoons \{a, b, c, d, e, f, g\}$ wie im Bild
und $\Gamma \rightleftharpoons \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$ mit

$$\begin{aligned}
\alpha &\eqqcolon ab\\
\beta &\eqqcolon be\\
\gamma &\eqqcolon cf\\
\delta &\eqqcolon de\\
\varepsilon &\eqqcolon g\\
\zeta &\eqqcolon fa
\end{aligned}$$



mit l_1 bzw. l_2 die Injektion von 2 in A^+ bzw. Γ^+ gemäß:

I.	0	$abcdef$	6	bzw. II.	$\alpha\gamma\delta$	3
	1	af	2		ζ	1
	2	$abdeg$	5		$\alpha\delta\varepsilon$	3
	3	$abefg$	5		$\beta\varepsilon\gamma$	3
	4	$acfg$	4		$\gamma\varepsilon\zeta$	3
	5	$bcefg$	5		$\beta\gamma\varepsilon$	3
	6	$cdefg$	5		$\gamma\delta\varepsilon$	3
	7	abf	3		$\alpha\zeta$	2
	8	$abcdefg$	7		$\alpha\gamma\delta\varepsilon$	4
	9	$abcfg$	5		$\alpha\gamma\varepsilon$	3
		Länge:	47		Länge:	28

D_ν sei die Durchschnittslänge eines Codewortes aus $l_\nu 2$ für $\nu = 1, 2$.

Also ist $D_\nu = \frac{1}{|Z|} \sum\limits_{z \in \mathbb{Z}} |l_\nu(Z)|$,

$D_1 = \frac{1}{10} 47 = 4,7$ und $D_2 = \frac{1}{10} 28 = 2,8$, d. h. l_2 ist wesentlich sparsamer in der technischen Realisierung als l_1.

d) Z soll in einem binären Blockcode C der Länge l, etwa über $\mathbb{B}$, codiert werden. Wegen $C \subseteq \{w \in \mathbb{B}^+; |w| = l\} = B^l$ folgt $|10| = |Z| = |C| \leq 2^l$,
wegen $2^3 < 10 < 2^4$ also $l \geq 4$.

Definition 60 (Hamming-Abstand, Hamming-Zahl)
B sei Zeichenvorrat mit $|B| \in \mathbb{N}$, sowie $x, y \in B^n$, etwa $x = x_1 \ldots x_n$ und $y = y_1 \ldots y_n$, ferner C ein Blockcode der Länge n.

α) $h(x, y) \eqqcolon |\{\nu \in \mathbb{A}_n; x_\nu \neq y_\nu\}|$ heißt Hamming-Abstand von x nach y.

β) Im Falle $|C| \neq 1$ heißt $h_C \eqqcolon \min\{h(x, y); x, y \in C \wedge x \neq y\}$ Hamming-Zahl oder Minimalabstand von C.

Beispiel 56

a) Für einen 1-aus-n-Code (siehe Beispiel 55b)) gilt $h_C = 2$.

b) C sei wie in Beispiel 55d) mit $l = 4$.
Annahme: $h_C = 2$

Dann gibt es $x = x_1x_2x_3x_4$ und $y = y_1y_2y_3y_4$ aus C mit $h(x,y) = 2$.
Sei daher $k \in \mathbb{A}_4$ mit $x_k \neq y_k$ und C' der aus C dadurch entstehende Code, daß in jedem Codewort von C das k-te Zeichen entfernt wird. C' ist also ein Blockcode der Länge 3 und injektiv, weil verschiedene Stellen gestrichen wurden.
Daraus folgt $10 = |C| = |C'| \leq |\mathbb{B}^3| = 2^3 = 8$ als Widerspruch.
Mithin gilt $h_C \neq 2$ und wegen der leicht zu verifizierenden Unmöglichkeit von $h_C > 2$ sogar $h_C = 1$.

Satz 78
Mit B als endlichem nichtleerem Zeichenvorrat, $n \in \mathbb{N}$ und n als Hamming-Abstand auf B^n ist (B^n, h) ein metrischer Raum.

Beweis: Übung.

Definition 61
Werden zu einer Codierung c von $Z = \{0, 1, \ldots, 9\}$ bzw. Tetraden, Pentaden, Hexaden, etc. , d. h. Elemente bzw. aus $\mathbb{B}^4$, $\mathbb{B}^5$, $\mathbb{B}^6$, etc. , benutzt, spricht man bzw. von **Tetraden-**, **Pentaden-**, **Hexaden-**, etc. **codes**.
Die Elemente aus $\mathbb{B}^n \setminus c(Z)$ mit bzw. $n = 4, 5, 6$, etc. heißen auch bzw. Pseudotetraden, -pentaden, -hexaden, etc.

Beispiel 57
Sei $Z = \{0, 1, \ldots, 9\}$.

a) **Tetradencodes:**

Tetraden	d	s	a	g	m
0000	0		0	0	
000L	1		1	1	
00L0	2		2	3	0
00LL	3	0	3	2	
0L00	4	1	4	7	4
0L0L	5	2		6	3
0LL0	6	3		4	1
0LLL	7	4		5	2
		—	—		
L000	8	5			
L00L	9	6			
L0L0		7			9
L0LL		8	5		
LL00		9	6	8	5
LL0L			7	9	6
LLL0			8		8
LLLL			9		7

I. *D*irekter Code, BCD-Code (binary coded decimals), 8-4-2-1-Code (ein Stellenwert-code)
(∗) Es gilt $d(x) + d(9-x) = L00L = d(9)$ für jedes $x \in Z$.

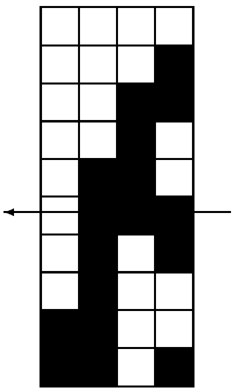
II. *S*tibitz-Code, 3-Exzeß-Code
3-Exzeß, da $s(Z) = d(Z) + 00LL$.
(∗∗) Wegen $s(x)+s(9-x) = d(x)+00LL+d(9-x)+00LL \overset{(*)}{=} L00L+0LL0 = LLLL$ leichte Bildung des Neunerkomplementes, denn mit $\bar{\mathfrak{x}} \rightleftharpoons \left\{ \begin{matrix} L \\ 0 \end{matrix} \right\}$, falls $\mathfrak{x} = \left\{ \begin{matrix} 0 \\ L \end{matrix} \right\}$ und $s(x) = \alpha\beta\gamma\delta$ hat man (∗∗) zufolge $s(9-x) = \overline{\alpha}\overline{\beta}\overline{\gamma}\overline{\delta}$ für alle $x \in Z$.
Solche Codes werden auch **symmetrisch** genannt (siehe Tabelle —).
Dies bedingt, daß bei Rundungen ≥ 5 nur die 1. Dualstelle zu berücksichtigen ist, der Dezimalübertrag bewirkt den Tetradenübertrag.

III. *A*iken-Code, 2-4-2-1-Code (ein Stellenwertcode)
Wegen $a(x) = \left\{ \begin{array}{ll} d(x) & \Leftarrow x \leq 4 \\ d(x) + 0LL0 & \Leftarrow x < 4 \end{array} \right.$ gilt (∗∗) entsprechend:

$$a(x) + a(9-x) = \left\{ \begin{array}{l} d(x) + d(9-x) + 0LL0 \\ d(x) + 0LL0 + d(x) \end{array} \right\} = L00L + 0LL0 = LLLL$$

d. h. a ist symmetrisch (siehe Tabelle —).

IV. *G*ray-Code (einschrittiger, progressiver Code)
Da sich beim Übergang von $x \in Z \setminus \{9\}$ zu $z+1$ nur eine Binärstelle beim entsprechenden Übergang von $g(x)$ zu $g(x+1)$ ändert, also $h(g(x), g(x+1)) = 1$, ist dieser Code wegen der Stetigkeit besonders gut geeignet für AD-Wandler (Analog-Digital-Wandler) (!reizvolle mathematische Theorie: Die Anzahl der möglichen Gray-Codes für $\mathbb{A}_n$ ist die Anzahl gewisser Hamiltonwege auf einem k-dimensionalen Würfel!)
Konstruktion:



	00		0L		LL		L0
00	0	→	1	→	2	→	3
							↓
0L	7	←	6	←	5	←	4
	↓						
LL	8	→	9				
L0							

V. Gray-Stibitz.Code, ge*m*ischter Code (progressiver Code)
Wegen $m(x) + L000 = m(9-x)$ ist die Berechnung des Neunerkomplementes hier sehr leicht.

$$\begin{array}{c|ccccccc} & 00 & & 0L & & LL & & L0 \\ \hline 00 & & & & & & & 0 \\ & & & & & & & \downarrow \\ 0L & 4 & \leftarrow & 3 & \leftarrow & 2 & \leftarrow & 1 \\ & \downarrow & & & & & & \\ LL & 5 & \rightarrow & 6 & \rightarrow & 7 & \rightarrow & 8 \\ & & & & & & & \downarrow \\ L0 & & & & & & & 9 \end{array}$$

Nachteil der Tetradencodes: Fehleranfälligkeit.
Daher:

b) **Pentaden-Hexadencodes:**

	p	f	c	b
0	00LL0	LL000	0LL0L	000 00L
1	0L00L	000LL	LLL0L	000 0L0
2	0L0L0	00L0L	LL00L	000 L00
3	0LL00	00LL0	L0000	00L 000
4	0LLLL	0L00L	0L0L0	0L0 000
5	L000L	0L0L0	0000L	L00 00L
6	L00L0	0LL00	L0L0L	L00 0L0
7	L0L00	L000L	LLL00	L00 L00
8	L0LLL	L00L0	0LL00	L0L 000
9	LL000	L0L00	000LL	LL0 000

I. p: Stibitz-Code mit Paritätsbit
$s(x)$ aus a)II. mit $x \in Z$ wird durch eine Dualstelle am Ende so erweitert, daß die Zahl der L in jeder Pentade gerade ist, also
$\forall x \in Z\ \exists b \in \mathbb{B} : p(x) = s(x)b \quad \wedge \quad h(p(x), 00000) = 0 \bmod 2$.

II. f: 2-aus-5-Code: Fehlererkennung leicht möglich.

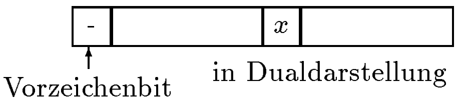
III. c: CCITT-Code (Comité Consultatif International Télégraphique et Téléphonique), Fernschreibcode, Boudot-Code
1932 eingeführt, geht zurück auf Boudot 1874 und basiert im wesentlichen auf Anregungen von Gauß und Weber 1833.

IV. b: Biquinärer Code: Leichte Fehlererkennung.

3.2 Rechnen

3.2.1 Subtraktion

Bemerkung 35
$x \in -\mathbb{N}$ — Beschränkung auf ganze Zahlen unerheblich — wird üblicherweise als $-|x|$ dargestellt, also mit Vorzeichen, was sich unmittelbar im Rechner realisieren läßt, etwa:



Nachteil: Spezielle Vorzeichenrechnung und relativ kompliziertes Rechenwerk, das sowohl addieren als auch subtrahieren kann, da lästige Fallunterscheidungen erfolgen müssen. Folgen sind Zeitverlust, Kosten und Anfälligkeit.
Daher ist eine Zurückführung der Subtraktion auf die Addition oder umgekehrt durch Komplementbildung: $\overline{y} \rightleftharpoons c - y; c \in \mathbb{N}, y \in \mathbb{Z} : x - y = x + \overline{y} - c$ sinnvoll,
wobei sowohl $y \mapsto \overline{y}$ als auch $x \mapsto x - c$ (Reduktion mod c) leicht realisierbar sein müssen.
Im folgenden sind die B-adische Darstellung ($B \in \mathbb{N} \setminus \{1\}$) und Rechenwörter der Länge $n \in \mathbb{N}$, etwa $x = x_{n-1} \dots x_1 x_0$ mit $x_\nu \in \mathbb{U}_B; \nu \in \mathbb{U}_n$, vorausgesetzt.

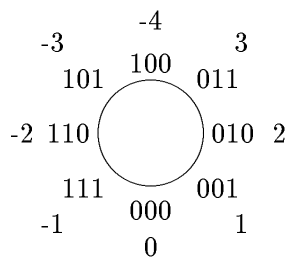
Definition 62 (B-Komplement)
Positive Zahlen: $0w$ mit $w \in \mathbb{U}_B^{n-1}$, also $0 \dots 0$, d. h. Null ist positiv
Negative Zahlen: $(B-1)w$ mit $w \in \mathbb{U}_B^{n-1}$

Beispiel 58

a) Negative Zahlen für $B = 2$:

$$\begin{array}{rl} \text{-1:} & 11\dots111 \\ \text{-2:} & 11\dots110 \\ \text{-3:} & 11\dots101 \\ \vdots & \vdots \\ -(2^{n-1}-1): & 10\dots001 \\ -2^{n-1}: & 10\dots000 \end{array}$$

b) „Zahlenring" (B=2, n=3):



Also $|x|$ für $\begin{matrix}\text{pos.}\\ \text{neg.}\end{matrix}$ x maximal $\begin{matrix}B^{n-1}-1\\ B^{n-1}\end{matrix}$.

Bemerkung 36
Für das B-Komplement von $x \in \mathbb{Z}$ gilt

$$\begin{aligned}
\overline{x} &= B^n - x = B^n - 1 - x + 1 \\
&= (B-1)(B-1)\ldots(B-1) - x_{n-1}x_{n-2}\ldots x_1x_0 + 1 \\
&= \tilde{x}_{n-1}\tilde{x}_{n-2}\ldots\tilde{x}_1\tilde{x}_0 + 1
\end{aligned}$$

mit $\tilde{x}_\nu \rightleftharpoons (B-1) - x_\nu$ für $\nu \in \mathbb{U}_{n-1}$
also Komplementation durch stellenweise $(B-1)$-Komplementation, bei $B = 2$ also Inversion $\{(0,1),(1,0)\}$ und anschließender Addition von 1.
Ferner ist $x - c = x_{n-1}\ldots x_0 - \underbrace{10\ldots0}_{n} \equiv_{B^n} x_{n-1}\ldots x_0 = x$,
es entfällt also die Reduktion mod c.

Beispiel 59

a) $B = 2, n = 6, x = 13, y = 7$; zu berechnen: $x - y$:

$$\begin{array}{lrcl}
 & y & = & 000\,111 \\
\hookrightarrow & \tilde{y} & = & 111\,000 \\
\hookrightarrow & \overline{y} & = & 111\,001 \\
 & x & = & 001\,101 \\
\hookrightarrow & x + \overline{y} & = & 000\,110
\end{array}$$

also $x - y = x + \overline{y} - c \equiv_c 000\,110 \mathrel{\hat{=}} 6$.

b) $B = 2, n = 6, x = -8, y = -11$; zu berechnen: $x - y$:

$$\begin{array}{lrcl@{\qquad}lrcl}
 & x & = & 001\,000 & & \overline{y} & = & 001\,011 \\
\hookrightarrow & \tilde{x} & = & 110\,111 & \hookrightarrow & \tilde{\overline{y}} & = & 110\,100 \\
\hookrightarrow & \overline{x} & = & 111\,000 & \hookrightarrow & y & = & 110\,101 \\
 & y & = & 110\,101 & & & & \\
\hookrightarrow & \overline{x} + y & = & 000\,011 & & & &
\end{array}$$

also $x - y = 000\,011 \mathrel{\hat{=}} 3$.

c) Schieben (shift) nach links für $B = 2, n = 4$:
$\underbrace{0101}_{5} \longrightarrow \underbrace{1010}_{-6}$ oder $\underbrace{1011}_{-5}$
aber:
$\underbrace{0011}_{3} \longrightarrow \underbrace{0110}_{6}$ oder $\underbrace{0111}_{7}$

Bemerkung 37 (Nachteile des B-Komplementes)
Asymmetrie bzgl. 0 und damit Überlauf bei $x \mapsto |x|$ möglich
Schieben um eine Stelle nach links nicht immer Ver-B-fachung, für $B = 2$ Verdopplung

Definition 63 ((B-1)-Komplement)
Positive Zahlen: $0w$ mit $w \in \mathbb{U}_B^{n-1}$
Negative Zahlen: $(B-1)w)$ mit $w \in \mathbb{U}_B^{n-1}$

„Positive“ Null: $\underbrace{00\ldots00}_{\text{n-mal}}$

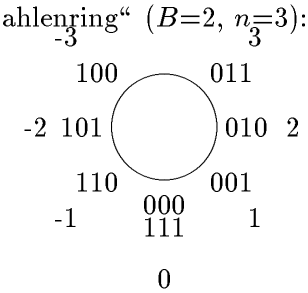
„Negative“ Null: $\overbrace{(B-1)(B-1)\ldots(B-1)(B-1)}$

Beispiel 60

a) Negative Zahlen für $B = 2$:

0:	$11\ldots111$
-1:	$11\ldots110$
-2:	$11\ldots101$
$\vdots$	$\vdots$
$-(2^{n-1}-2)$:	$10\ldots001$
$-(2^{n-1}-1)$:	$10\ldots000$

b) „Zahlenring“ (B=2, n=3):



Also $|x|$ für $\begin{matrix}\text{pos.}\\\text{neg.}\end{matrix}$ x maximal $B^{n-1}-1$.

Bemerkung 38

a) Für das $(B-1)$-Komplement von $x \in \mathbb{Z}$ gilt

$$\begin{aligned}\overline{x} &= B^n - 1 - x = (B-1)\ldots(B-1) - x_{n-1}\ldots x_0\\ &= \tilde{x}_{n-1}\ldots\tilde{x}_0\end{aligned}$$

mit $\tilde{x}_\nu = (B-1) - x_\nu$ für $\nu \in \mathbb{U}_{n-1}$
also Komplementation durch stellenweise $(B-1)$-Komplementation.

b) Sei $(*)$ $d = x - y = x + \overline{y} - c = x + (c-y) - c$ für $x, y \in \mathbb{N}$ zu berechnen und

I. $x > y$: Dann ist $d \geq 1$ und
$x + (c-y) = c + d \geq c + 1 = B^n - 1 + 1 = B^n$.
An der fiktiven $(n+1)$-ten Stelle ergibt sich also eine 1, deren Wegfall einer Subtraktion von B^n entspricht. Es soll aber $(*)$ zufolge $B^n - 1$ subtrahiert werden, was daher eine Addition von 1 bedingt, den sogenannten Einer-Rücklauf.

II. $x \leq y$: Dann ist $d \leq 0$ und
$c - |d| = c - (-d) = c + d = c + x + \overline{y} - c = x + \overline{y}$,
da ja $x + \overline{y} = x + (c - y) = c + d \leq c = B^n - 1$, also kein Überlauf entsteht.

Aus I. und II. ergibt sich für die Reduktion nach c:
Entsteht bei der Addition eine 1 in der $(n+1)$-ten Stelle, muß noch eine 1 addiert werden (Einer-Rücklauf). Also ist naheliegend, die $(n+1)$-te Stelle wie einen Übertrag zur 1. Stelle zu addieren.

Beispiel 61

a) $B = 10, n = 4, x = 496, y = 1$; zu berechnen: $x - y$:

$$\begin{array}{rr} y & 0001 \\ \overline{y} & 9998 \\ x & +0496 \\ \hline & 10494 \\ \text{Einer-Rücklauf} & \longrightarrow 1 \\ \hline & 495 \end{array}$$

b) $B = 2, n = 5, x = 9, y = 0$; zu berechnen: $x - y$:

I.
$$\begin{array}{rr} y & 00000 \\ \overline{y} & 11111 \\ x & +01001 \\ \hline & 101000 \\ \text{Einer-Rücklauf} & \longrightarrow 1 \\ \hline & 01001 \end{array}$$

II.
$$\begin{array}{rr} \overline{y} & 11111 \\ y & 00000 \\ x & +01001 \\ \hline & 01001 \end{array}$$

c) Schieben (nach links) für $B = 2, n = 4$ (siehe Beispiel 59c)):
$\underbrace{0101}_{5} \longrightarrow \underbrace{1010}_{-5}$ oder $\underbrace{1011}_{-4}$
aber:
$\underbrace{0011}_{3} \longrightarrow \underbrace{0110}_{6}$ oder $\underbrace{0111}_{7}$

Bemerkung 39

a) Trotz verschiedener Darstellungen sind die Operationen mit Null beim $(B-1)$-Komplement eindeutig (vgl. Beispiel 61b)). Es genügt, dies für die Addition zu zeigen, da andere Operationen darauf reduzierbar sind.
Für „positive“ Null gilt: $x + 0 = x_{n-1} \dots x_0 + 0 \dots 0 = x_{n-1} \dots x_0 = x$.
Für „negative“ Null gilt:

I. $x_0 \geq 1$:

$$\begin{array}{ccccccc} & x_{n-1} & x_{n-2} & \dots & x_2 & x_1 & x_0 \\ + & B-1 & B-1 & \dots & B-1 & B-1 & B-1 \\ \hline 1 & x_{n-1} & x_{n-2} & \dots & x_2 & x_1 & x_0 - 1 \\ \longrightarrow & & & & & & 1 \\ \hline & x_{n-1} & x_{n-2} & \dots & x_2 & x_1 & x_0 \end{array}$$

II. $x_0 = 0$: ($+_B \stackrel{\wedge}{=}$stellenweise Addition unter Berücksichtigung des Restes)
Entweder: $\forall \nu \in \mathbb{A}_{n-1} : \ x_\nu = 0$
Dann ist $x + 0 = 0 \ldots 0 + (B-1) \ldots (B-1) = (B-1) \ldots (B-1) = x$.
Oder: $\exists \nu \in \mathbb{A}_{n-1} : \ x_\nu \neq 0$
Dann gibt es ein minimales ν mit dieser Eigenschaft, etwa m, und für $s_{n-1} \ldots s_0 \rightleftharpoons x + (B-1) \ldots (B-1)$ erhält man zunächst
$s'_\mu = 0 +_B (B-1) = B-1$ für $\mu = 0, \ldots, m-1$
$s'_m = x_m +_B (B-1) = x_m - 1$
$s'_\mu = x_\mu +_B (B-1) + 1 = x_\mu$ wie I. für $\mu = m+1, \ldots, n-1$
und dann durch Einer-Rücklauf
$s_\mu = s'_\mu +_B 1 = (B-1) +_B 1 = 0$ für $\mu = 0, \ldots, m-1$
$s_m = s'_m +_B 1 = (x_m - 1) +_B 1 = x_m$
$s_\mu = s'_\mu +_B 0 = x_\mu$ für $\mu = m+1, \ldots, n-1$
also $x + 0 = s_{n-1} \ldots s_0 = x_{n-1} \ldots x_m 0 \ldots 0 = x$.

b) Nachteile des $(B-1)$-Komplementes:
Doppelte Darstellung der Null, bei Abfragen, etwa bedingten Sprungbefehlen lästig
Schieben siehe Beispiel 61c) und Bemerkung 37

c) Beide Komplemente sind verbreitet und erlauben homogene Rechenwerksstrukturen: Beim B-Komplement ist die Reduktion besonders einfach, beim $(B-1)$-Komplement die Komplementbildung.

d) Bei der obigen Behandlung war ein zeitliches Moment — Abfolge von Operationen — unübersehbar, dessen Realisierung dient u. a. ein Flip-Flop (bistabile Kippschaltung, bistabiler Trigger), das zur Speicherung eines Bits dient und bei einem Taktimpuls Information weitergibt.

3.2.2 Addierwerke

Bemerkung 40
Problem: Addition von Dualzahlen (vgl. Beispiel 4)
Sei $n \in \mathbb{N}$, $a = a_{n-1} \ldots a_0$ der Angend und $b = b_{n-1} \ldots b_0$ der Addend mit $a_\nu, b_\nu \in \mathbb{B}$ sowie $s_n \ldots s_0 = s \rightleftharpoons a + b$ mit $s_\nu \in \mathbb{B}$ die Summe.
Dann gilt gemäß Beispiel 4 mit $\ddot{u}_0$
$\ddot{u}_\nu \rightleftharpoons \ddot{u}(\ddot{u}_{\nu-1}, a_{\nu-1} +_2 b_{\nu-1}) \ \vee \ \ddot{u}(a_{\nu-1}, b_{\nu-1})$
$s_\nu \rightleftharpoons \ddot{u}_\nu +_2 a_\nu +_2 b_\nu$ mit $\nu \in \mathbb{A}_n$.
Die Schaltelemente brauchen Zeit, die sogenannte Schaltzeit oder Gatterlaufzeit τ, definiert als diejenige Zeit, die vergeht, bis das Ausgangssignal von 10% auf 90% angewachsen ist. Heutige Gatter haben eine Schaltzeit von 10ps bis 100ns. Unter Vernachlässigung der Inversion benötigt ein Halbaddierer (unserer Bauart, siehe Beispiel 2) für die Summe rund 2τ, für den Übertrag (carry) τ, ein Addierer (unserer Bauart, siehe Beispiel 3) daher für die Summe und den Übertrag je 4τ.
Eine Realisierung gemäß Beispiel 4, Addierer mit durchlaufendem Übertrag (ripple carry adder) (gehört zur Klasse asynchroner, d. h. nicht getakteter Paralleladdierer) braucht zur Gewinnung von s_n also $4\tau + \underbrace{2\tau + \ldots + 2\tau}_{\text{(n-2)-mal}} = 2n\tau$, $2n$ Gatterlaufzeiten. Bei $n = 64$ und $\tau = 10ns$ macht das $1,28\mu s$, was zu langsam ist. Jedoch sind der geringe Aufwand (1 Halbaddierer, n-1

Addierer) und die Übersichtlichkeit aufgrund des modularen Prinzips ein Vorteil.

Nächster Versuch: Addierer mit minimaler Übertragsverzögerung
Es gilt
$s_0 \;=\; \ddot{u}_0 +_2 a_0 +_2 b_0 = (a_0 \vee b_0) \wedge (\overline{a}_0 \vee \overline{b}_0),$
für $n = 1$:
$s_1 \;=\; a_0 \wedge b_0,$
und für $n = 2$:

$$\begin{aligned} s_1 &= (a_0 \vee a_1 \vee b_1) \wedge (a_1 \vee b_0 \vee b_1) \wedge (a_0 \vee \overline{a}_1 \vee b_1) \wedge (\overline{a}_1 \vee b_0 \vee b_1) \\ &\quad \wedge (\overline{a}_0 \vee a_1 \vee \overline{b}_0 \vee b_1) \wedge (\overline{a}_0 \vee a_1 \vee \overline{b}_0 \vee b_1) \\ s_2 &= (a_0 \vee a_1) \wedge (a_0 \vee b_1) \wedge (a_1 \vee b_0) \wedge (a_1 \vee b_1) \wedge (b_0 \vee b_1) \end{aligned}$$

Bedarf:

Stellen	AND-Gatter	OR-Gatter	Gatter insgesamt
1	2	2	4
2	3	13	16
n	Übung.		

Das ist selbst bei heutiger Mikrotechnik zu viel. Ganz abgesehen von der begrenzten Zahl der Eingänge, etwa ≤ 20.

Ein Kompromiß zwischen beiden Fehlschlägen sind Addierer mit vorausberechnetem Übertrag (carry-look-ahead-adder):
Für je k Stellen werden die $k-1$ Überträge der niedrigeren Stellen zusammengefaßt, bevor die entsprechenden Summen berechnet werden.
Berechnung der ν-ten Stellensumme mittels Halbaddierer:
Nach der Zeit τ steht fest, ob ein Übertrag erzeugt wird (carry generate), also bei $g_\nu = 1$ mit $g_\nu \rightleftharpoons a_\nu \wedge b_\nu$ für $\nu \in \mathbb{U}_n$.
Nach der Zeit 2τ steht fest, ob ein von der $(\nu-1)$-ten Stelle ankommender Übertrag weitergegeben wird (carry propagate), also bei $p_\nu = 1$ mit $p_\nu \rightleftharpoons a_\nu +_2 b_\nu$ für $\nu \in \mathbb{U}_n$.
Für konkrete Schaltungen, sei etwa $k = 4$, für welche Gruppe wir G_m bzw. P_m für Erzeugung bzw. Weiterleitung des Gruppenübertrages ermitteln.
Dabei gelte: $k \mid n$ und $m \in \mathbb{A}_n$ mit $m \equiv_k -1$.
Offenbar ist
$G_m = g_m \vee (g_{m-1} \wedge p_m) \vee (g_{m-2} \wedge p_{m-1} \wedge p_m) \vee (g_{m-3} \wedge p_{m-2} \wedge p_{m-1} \wedge p_m)$
und
$P_m = p_{m-3} \wedge p_{m-2} \wedge p_{m-1} \wedge p_m.$
Die technische Umsetzung findet sich auf Seite 119.

Aus dieser Schaltung ist zu ersehen, daß schon nach der Zeit 2τ bzw. τ bekannt ist, ob eine Vierergruppe einen Übertrag erzeugt ($G_m = 1$) oder einen einlaufenden Übertrag weiterleitet ($P_m = 1$; das heißt nicht, daß ein solcher weiterzuleitender Übertrag auch vorhanden sein muß).
Ein Vergleich zwischen RCA (ripple carry adder) und CLAA (carry look ahead adder) zeigt:

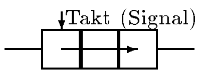
	Zeit für Gesamtsumme	Aufwand	
		1 HA	3 Gatter
RCA	$2 \cdot 4\tau = 8\tau$	3 A	$3(2 \cdot 3 + 1)$ Gatter
			24 Gatter
		$2 \cdot 4$ HA	$8 \cdot 3$ Gatter
CLAA	$\underbrace{2\tau + 2\tau}_{2\text{ HA}} + 2\tau = 6\tau$	Übertrag	14 Gatter
			38 Gatter

Es ergibt sich also bei geringem Mehraufwand (58%) eine Zeitersparnis von 25%. Der Aufbau des CLAA beweist seine Überlegenheit jedoch bei der Iteration des Prinzips, wie in der Schaltung auf Seite 120 realisiert.

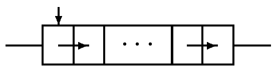
Allgemein entsteht bei einer Stufe eine Additionszeit von $2\tau + 16 \cdot 2\tau + 2\tau = 36\tau$ gegenüber $2 \cdot 64\tau = 128\tau$ beim RCA, jedoch 14τ bei drei Stufen (eingezeichnetes Signal).

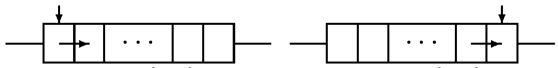
Weitere Lösungen:

- Synchrone Paralleladdierer siehe Literaturverzeichnis Anhang E
- Synchrone Serienaddierer
  Verzögerungsglied:

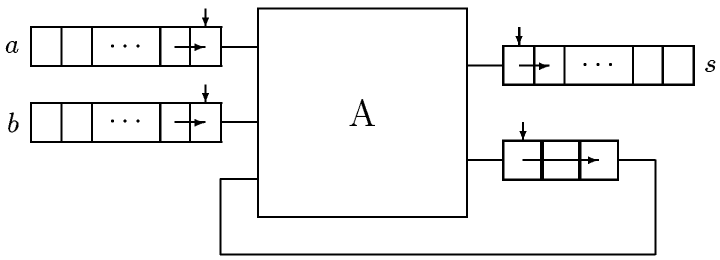


  Schieberegister:



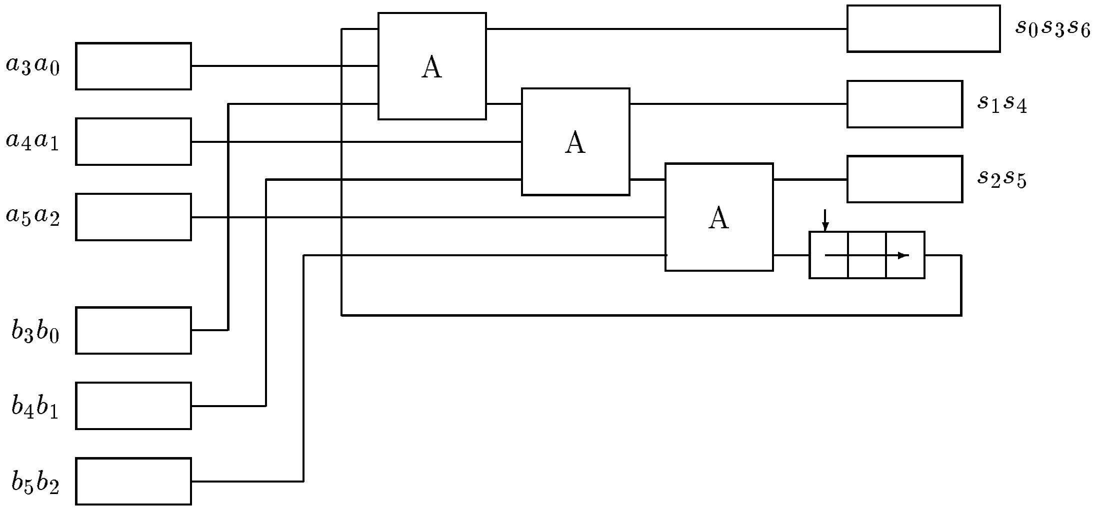


Hineinschieben Herausschieben



  Aufwand: 1 Addierer, 1 Verzögerungsglied, 3 Schieberegister
  Laufzeit: $(n+1)\sigma$ mit Taktzeit σ (heute im ps- bis ns- Bereich; dabei $\sigma > 4\tau$!)
  Auch das ist zu langsam!

- Kombination: Serien-Paralleladdierer
  Für $n = 6$ (oder allgemeiner $n = 3k$) ist mit
  Aufwand: 3 Addierer, 1 Verzögerungsglied, 8 Schieberegister à $2k$ Stellen, 1 Schieberegister à $3(k+1)$ Stellen
  Laufzeit: 3σ $((k+1)\sigma$; dabei $\sigma > 4\tau + 2\tau + 2\tau = 8\tau)$
  eine mögliche Realisierung die folgende Schaltung:

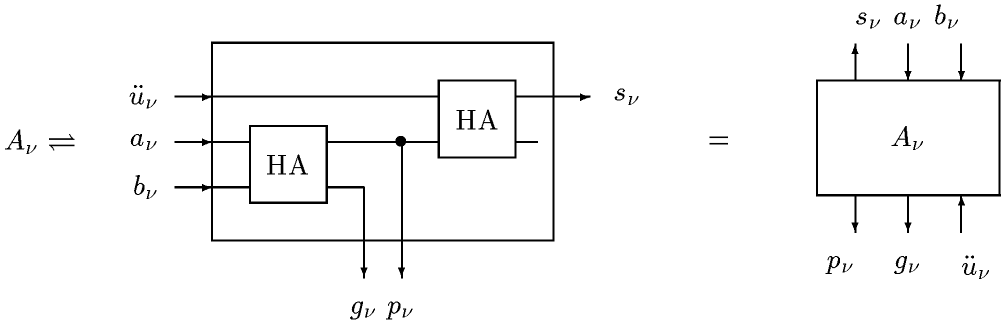


3.2.3 Multiplikation und andere Operationen

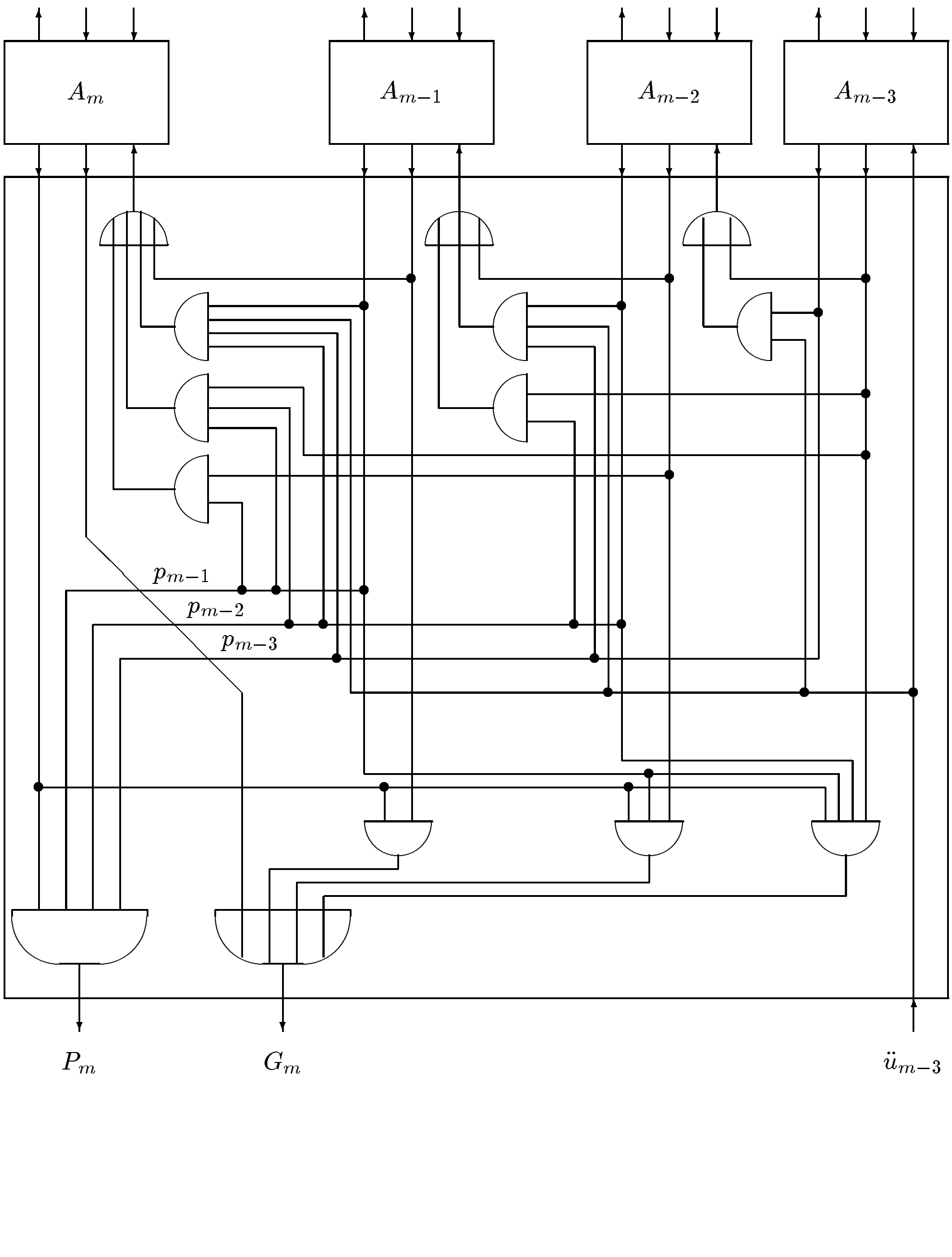
Bemerkung 41
Hier sei nur auf die gesonderte Vorlesung „Rechnerarchitektur“ und die Literatur Anhang E verwiesen.

Addierer mit vorausberechnetem Übertrag:

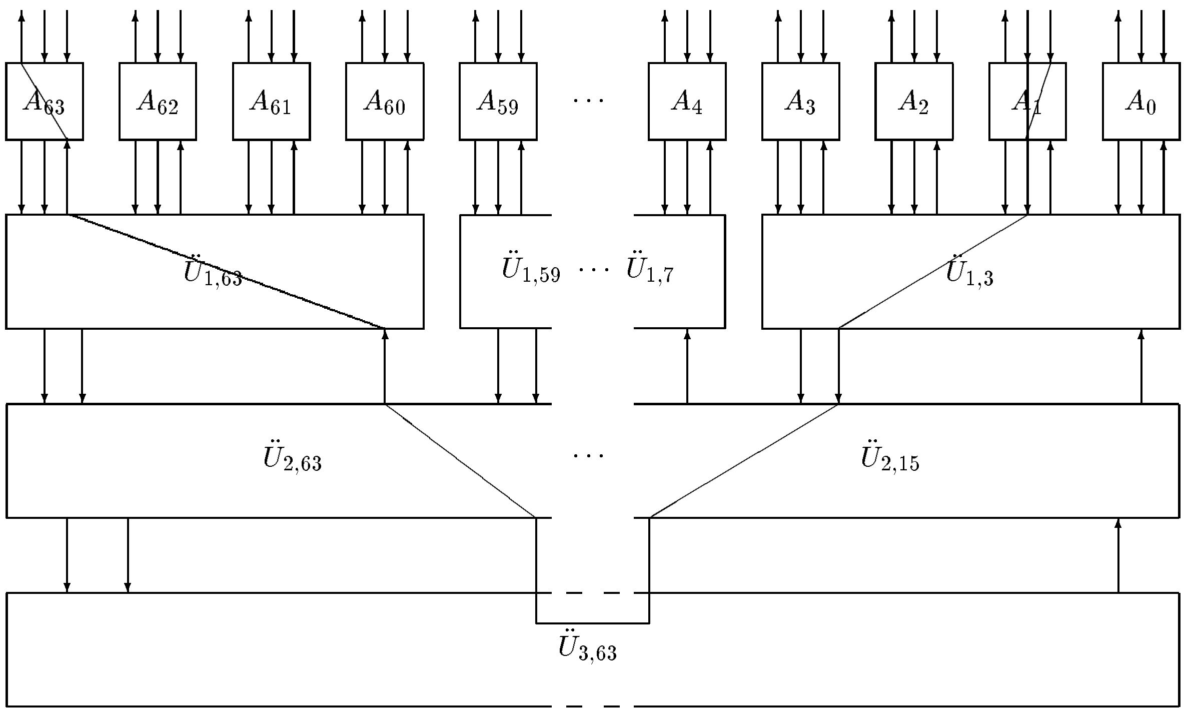
Mit



ist die folgende Schaltung möglich:



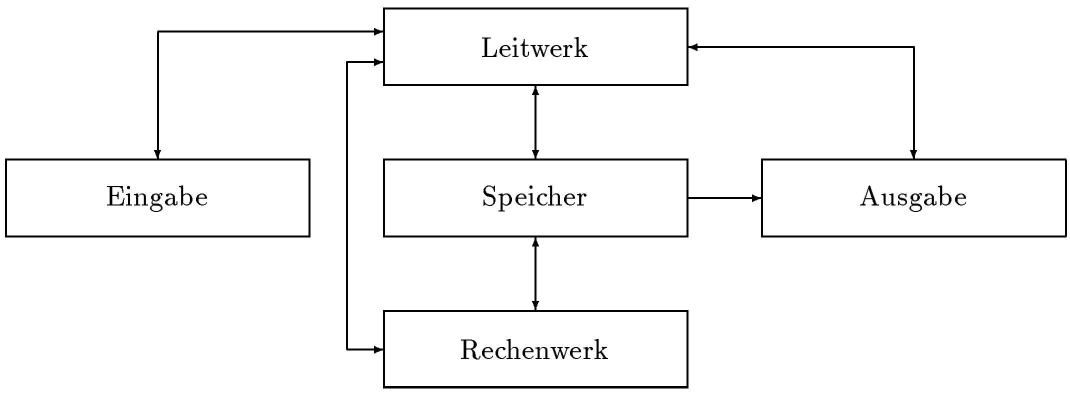
Iteration eines CLAA:



3.3 Rechnerarchitektur

3.3.1 Von-Neumann-Rechner

Definition 64
Der klassische, auf von Neumann zurückgehende Universalrechner (Von-Neumann-Rechner) ist nach folgendem Schema aufgebaut:



Er ist vom Prinzipiellen her auch heute noch wichtig und genügt folgender Kennzeichnung:

α) Der Rechner hängt in seiner Struktur nicht von dem zu bearbeitenden Problem ab. Für jede Aufgabe wird eine geeignete Bearbeitungsvorschrift, ein Programm, das sich aus einzelnen Befehlen zusammensetzt, eingegeben und im Speicher aufbewahrt (sogenannte speicherprogrammierte Rechner).

β) Befehle und Daten werden in einem einheitlichen Speicher, dem Hauptspeicher abgelegt.

γ) Die Speicherzellen sind mittels Zahlen, den Adressen durchnumeriert. Auf den jeweiligen Zelleninhalt kann mittels der zugehörigen Adresse zugegriffen werden.

δ) Das Programm ist im Speicher unter den Adressen $a, a+1, \ldots$ deponiert und wird in der Regel der Reihe nach abgearbeitet. Zum Holen des nächsten Befehls muß dann die Adresse nur um 1 erhöht werden. Von dieser Reihenfolge wird nur abgewichen, wenn ein sogenannter Sprungbefehl vorliegt, d. h. nach Ausführung des Befehls mit der Adresse s (des Sprungbefehls) wird der Befehl mit einer Adresse $t \neq s+1$ fortgefahren. Man erreicht dadurch eine enorme Flexibilität.

ε) Verwendung des Dualsystems.

Zu den einzelnen Bestandteilen:

1. Rechenwerk
   Das Rechenwerk dient zur Ausführung arithmetischer $(+, -, \cdot, \div)$ und logischer $(\wedge, \vee, \neg)$ Operationen. Zur Zwischenspeicherung hat es mindestens 3 sogenannte Register (Kleinstspeicher)

a) Akkumulator-Register (AR)
b) Operanden-Register (OR)
c) Übertragsregister (ÜR)

für je ein Rechnerwort (Zelleninhalt)

2. Speicher
Der Speicher besteht aus gleichartigen, adressierbaren Zellen, deren Inhalt als Rechnerwort bezeichnet wird und dient zur Speicherung des Programms, der Eingabedaten, der Zwischenergebnisse und der Endresultate.

3. Ein-/Ausgabe
Das Eingabe- bzw. Ausgabewerk bringt Eingabedaten und Programme in den Speicher bzw. Ergebnisse vom Speicher nach außen. Ein Eingabe- bzw. Ausgabebefehl transportiert je ein Wort.

4. Leitwerk
Das Leitwerk bewirkt die Ausführung der im gespeicherten Programm niedergelegten Arbeitsvorgänge und besitzt dazu je ein(en)

   a) Befehlsregister (BR)
   b) Befehlszähler (BZ)

Programmablauf:
Das Programm sei schon, etwa durch ein handgesteuertes Leseprogramm im Speicher ab Adresse a abgelegt mit der Startadresse a. Zunächst wird a in den Befehlszähler (BZ) übernommen, sodann kommt der in a stehende Befehl in das Befehlsregister (BR) und wird ausgeführt durch entsprechende Signale an den Speicher, das Rechenwerk oder Ein/Ausgabe. Gleichzeitig wird der Befehlszähler um 1 erhöht, usw.
Dieses Schema wird nur durchbrochen, wenn im Befehlsregister ein Sprungbefehl steht. Dann wird lediglich die im Sprungbefehl stehende Adresse in den Befehlszähler übernommen und wie oben weiterverfahren.
Zum Beenden des Programmablaufs dient ein Stoppbefehl. Kommt ein Wort, das ihn enthält, in das Befehlsregister, wird die Arbeit des Leitwerks beendet und kein Befehl mehr geholt.
Befehlsaufbau:
Ein Befehlswort, außer Sprung- und Stoppbefehlen, ist ein Tripel (O, A, R), wobei O die auszuführende Operation, A die Adresse eines Operanden und R ein Register bezeichnet, das (in der Regel) als Akkumulator ausgezeichnet wird.
Ist die Länge der Teilwörter o, a bzw. r und die Länge eines Wortes n, so gilt $o + a + r = n$ und es gibt maximal 2^o mögliche Operationen, 2^a ansprechbare Adressen und 2^r Register. Solche Rechner werden **Einadreßmaschinen** genannt.
Können zwei bzw. drei Adressen im Befehlswort stehen, spricht man von **Zwei-** bzw. **Dreiadreßmaschinen**. Wegen der Wortlängenbegrenzung wurden hauptsächlich Ein- und Zweiadreßmaschinen gebaut.
Nebenspeicher:
Viele Rechner besitzen außer dem Speicher mit schnellem Zugriff aus Kosten- und technischen Gründen noch einen oder mehrere sogenannte Externspeicher (Trommeln, Bänder, Platten), mit denen vermöge eines weiteren Ein-/Ausgabewerkes kommuniziert wird.

Bemerkung 42
In den Speicherzellen mit den Adressen a, b, c stehen bzw. die Zahlen x, y, z. Es soll $x(y+z)$ berechnet und nach d, e (doppelte Wortlänge) gespeichert werden. Dabei sei die Länge von $x+y$ höchstens gleich der Wortlänge.

Hole	b, AR	y nach AR
Add	c, AR	z nach OR
		$y+z$ nach AR
Mult	a, AR	x nach OR
		$x(y+z)$ nach AR und ÜR
Bring	d, ÜR	
		$x(y+z)$ nach d, e
Bring	e, AR	

3.3.2 Modernere Konzepte

Einprozessor-Systeme

Definition 65

α) Unter dem Rechnerkern oder Prozessor (DIN 44 300), häufig auch CPU (central processing unit), versteht man die zentralen Werke eines Rechners, also i. w. eine Rechenanlage ohne Speicher und ohne Ein-/Ausgabegeräte. Bei dem in Definition 64 skizzierten von-Neumann-Rechner besteht der Rechnerkern also aus Leit- und Rechenwerk.

β) Einprozessor-Systeme oder Monoprozessoren verfügen lediglich über einen Prozessor, etwa sogenannte Mikroprozessoren, hochintegrierte Schaltkreise, die wesentliche oder sämtliche Teile eines Rechners in sich vereinigen.

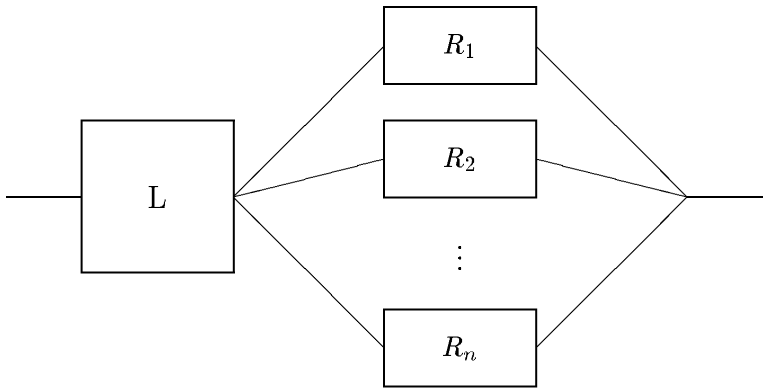
Mehrprozessor-Systeme

Bemerkung 43
Zur Steigerung der Rechenleistung (dies muß und kann präzisiert werden) kann man bei gegebenen technischen Voraussetzungen versuchen, zu „parallelisieren", d. h. möglichst viele „Arbeiten" des Rechners gleichzeitig ablaufen zu lassen.
Dies ist heute eine sehr intensive und erfolgreiche Aktivität von der Forschung bis zur Praxis und kann auf allen Ebenen geschehen: Programm (Sprache), Compiler, Leitwerk, Prozessor.

Definition 66
Mehrprozessor-Systeme oder Multiprozessoren (Bezeichnungen uneinheitlich!) sind Rechner, die nicht nur ein Leitwerk und ein Rechenwerk besitzen. Man unterscheidet

α) Feldrechner
Rechner mit mehreren parallelen (nebenläufigen) Rechenwerken R_ν mit $\nu \in \mathbb{A}_n$ und

hinreichen großem $n \in \mathbb{N}$, die jedoch durch ein gemeinsames Leitwerk L gesteuert werden:

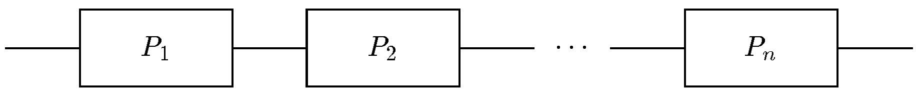


Beispiele:

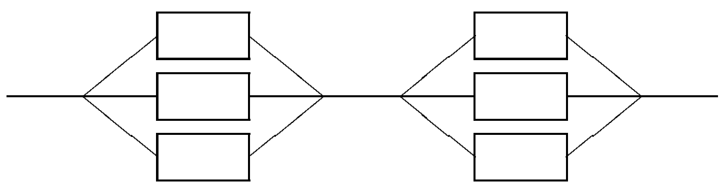
a) ILLIAC IV (1966–72, 1975; statt geplanten 1000 MFlops „nur“ 15 MFlops (Mega Floating Point Operations per Second))

b) Assoziativrechner (Rechner mit Assoziativspeicher, inhaltsadressiertem Speicher (CAM — content adressable memory), d. h. gespeicherte Information wird nicht über die Adresse gefunden, sondern über Teile der die Information tragenden Teile selbst.)
z. B. STARAN B (1972), STARAN E (1977)

β) Pipeline-Rechner
Rechner mit Fließbandverarbeitung: $n \in \mathbb{N} \setminus \{1\}$ Prozessoren $P_1, \ldots, P_n$ arbeiten in Serie verschiedene oder gleiche Teilaufgaben ab:



Nebenläufige Pipeline:

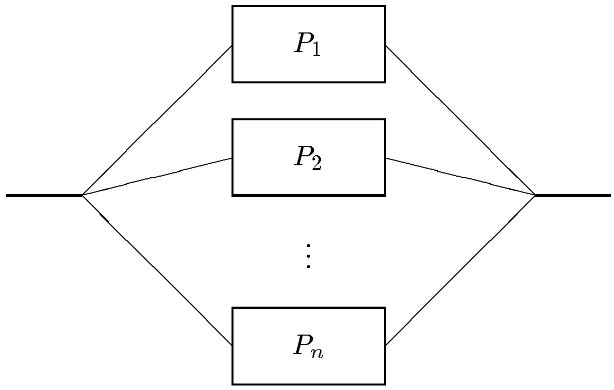


Beispiele:

a) Vektorrechner, d. h. Rechner mit arithmetischem Pipelining, z. B. CDC STAR 100 (1977; 100 MFlops theoretischer Maximalwert)

b) Rechner mit Befehls-Pipelining, z. B. CRAY–1 (1980; Grundtakt 12,5 ns; 200 MFlops; $\approx$ 9 Mio. \$), CRAY–1/S (1981; $\approx$ 18 Mio. \$), CYBER 205 (1982; 800 MFlops; $\approx$ 18 Mio. \$)

γ) Multiprozessoren
im eigentlichen Sinne Systeme von mehreren Prozessoren $P_1, \ldots, P_n$ mit eigenen Speichern, die weitgehend unabhängig voneinander arbeiten, d. h. gleichzeitig werden mehrere unterschiedliche Programme auf den verschiedenen Prozessoren ausgeführt:



Beispiel: EGPA (Erlanger General Purpose Array, 1975)

3.4 Programmiersprachen

Definition 67 (Programmiersprachen)
Programmiersprachen sind formale Sprachen P, also $P \subseteq A^*$ über einem Zeichenvorrat A, die zur Formulierung von anweisungen an einen Computer dienen.
Man unterscheidet (auch allgemeiner bei Sprachen)

α) Syntax: Die genaue Festlegung von P, etwa durch

  I. Aufzählung: insbesondere, wenn P endlich, jedoch selten

  II. Grammatiken: (genaue Definition in Theoretische Informatik I/II) oder Ähnlichem, etwa Automaten, Backus-Naur-Formalismus, Syntaxdiagramme

β) Semantik: Festlegung der Bedeutung von P

  I. Operationale Semantik: Bedeutung als Abläufe auf einer realen oder virtuellen Maschine

  II. Funktionale Semantik: Bedeutung als Funktion zwischen Eingaben und Ausgaben

γ) Progmatik: „reale“ Sicht von P, etwa Zielsetzung, Realisierung, Nutzung, Wirkung, Nebenwirkungen, …, speziell:

  I. Lebenszyklus von P: Entwurf, Implementation, Wartung, Standardisierung, Verbreitung, etc.

  II. Sprachfamilien: z. B. PASCAL, MODULA, , OBERON

  III. Erlernen von P

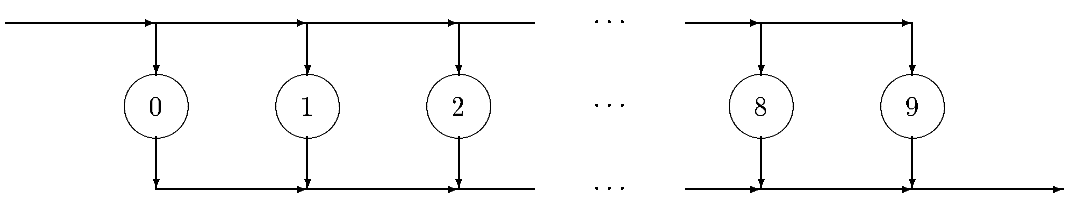
  IV. Implementationsprobleme: (genauer in der Vorlesung „Compilerbau“)

Beispiel 62

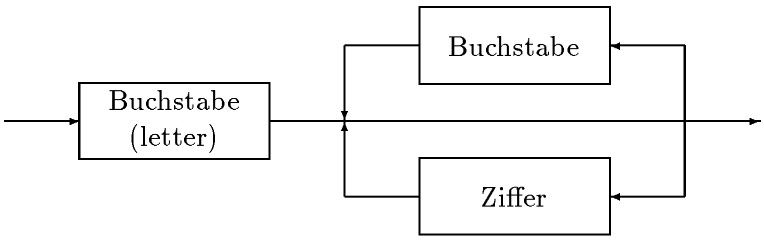
a) Syntaxdiagramme: Digraphen ohne Überkreuzungen (plättbare Graphen).

Knoten: ○, ▢: Terminale Zeichen
□, ▭: Nichtterminales, Definiendum
• : Verzweigungen

  I. Ziffern (digit) in ALGOL, PASCAL u. a.:

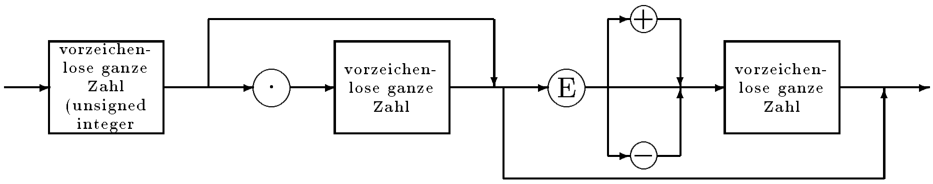


II. Name oder Bezeichner (identifier):



z. B. $JB007$

III. vorzeichenlose Zahl (unsigned number) in PASCAL u. a.:



z. B. 8128 oder $6 \cdot 626\ E - 34$

b) Backus-Naur-Formalismus (Backus normal term) (von J. W. Backus 1959 für ALGOL 60 entwickelt):
Metasymbole im Backus-Naur-Formalismus sind

::= bedeutet $\rightleftharpoons$
| bedeutet $\vee$
Nichtterminalsymbole werden in $\langle\ \rangle$ gesetzt

I. $\langle$Ziffer$\rangle$ ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

II. $\langle$Name$\rangle$ ::= $\langle$Buchstabe$\rangle$ | $\langle$Name$\rangle\langle$Buchstabe$\rangle$ | $\langle$Name$\rangle\langle$Ziffer$\rangle$
z. B. $JB007$

III. vgZ: vorzeichenlose ganze Zahl

$$\begin{aligned}\langle \text{vgZ}\rangle \quad ::= \quad & \langle \text{vgZ}\rangle | \langle \text{vgZ}\rangle \text{ E}\langle \text{vgZ}\rangle \\ & |\langle \text{vgZ}\rangle \text{ E} + \langle \text{vgZ}\rangle \mid \langle \text{vgZ}\rangle \text{ E} - \langle \text{vgZ}\rangle \\ & |\langle \text{vgZ}\rangle \cdot \langle \text{vgZ}\rangle \mid \langle \text{vgZ}\rangle \cdot \langle \text{vgZ}\rangle \text{ E}\langle \text{vgZ}\rangle \\ & |\langle \text{vgZ}\rangle \cdot \langle \text{vgZ}\rangle \text{ E} + \langle \text{vgZ}\rangle \mid \langle \text{vgZ}\rangle \cdot \langle \text{vgZ}\rangle \text{ E} - \langle \text{vgZ}\rangle\end{aligned}$$

z. B. 8128 oder $6 \cdot 6\ E - 34$

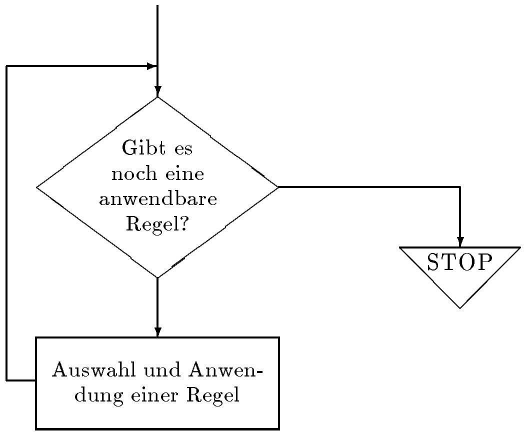
Definition 68
Wir sprechen von einem programmiersprachlichen Paradigma eine Programmiersprache P, wenn es Modellvorstellungen für die Abarbeitung eines Programmes in P gibt und diese die Einzelheiten von P bestimmen, i. w. die folgenden:

α) imperative (prozedurale) Programmiersprachen:
Das Programm besteht aus einer Folge von Befehlen (instructions) wie Wertzuweisungen, Sprungbefehle oder Addition von 1 etc.

Eingabewerte werden in Variablen gespeichert und weiterverarbeitet.
P spiegelt die Struktur eines Von-Neumann-Rechners wieder.
Beispiele: ADA, ALGOL, BASIC, C, COBOL, COMAL, ELAN, FORTRAN, MODULA-2, PL/1, PASCAL, SIMULA, SNOBOL, etc.

β) funktionale (applikative) Programmiersprachen:
Programme werden als Funktionen von Mengen von Eingabewerten (Parametern) in Mengen von Ausgabewerten aufgefaßt.
In rein funktionalen Programmiersprachen werden die Funktionen durch Zusammensetzung aus einfacheren definiert, wobei Grundfunktionen vorgegeben sind.
In applikativen Programmiersprachen wird dagegen eine Funktion durch Anwendung von Funktionen auf Parameter definiert, wobei als Parameter wieder Funktionen auftreten können.
Programme sind ein System von Funktionsdefinitionen, Parallelität wird leicht durch mehrstellige Funktionen erreicht.
Wissenschaftlich entwickelt werden sie aber kaum in der Praxis eingesetzt.
Beispiele: LISP, FP, HOPE, ML, LOGO, MIRANDA, etc.

γ) regelbasierte Programmiersprachen:
Voraussetzung: aktueller Datenbestand, sogenannte Datenbasis. Dieser wird durch Regelanwendungen verändert.
Ein Programm besteht aus einer Menge von Regeln, deren Abarbeitung i. a. nicht determiniert erfolgt (sog. Reagnize-Act-Cycle):



I. a. haben Regeln die Form „wenn ⟨Bedingung⟩ gilt, dann ⟨Aktion⟩ ausführen“.
Beispiele: STRIPS, OPS 5, PROLOG, INTRAN, etc.

δ) logikbasierte Programmiersprachen:
Spezialfall von γ).
Jeder Einzelschritt ist eine Anwendung einer logischen Schlußregel, deren Reihenfolge sich aus den Methoden der logischen Beweisverfahren ergibt.
Ein Programm ist eine Menge logischer Formeln (Tautologien) und einer Anfrage, d. h. der Eingabe eines Spezialfalles, einer zu bearbeitenden Formel.
Beispiele: PROLOG, PROLOG III

ε) objektorientierte Programmiersprachen:

Informationen (Daten und Regeln) werden als „Objekte“ aufgefaßt, die durch Senden von „Nachrichten“ Information austauschen. Jedes Objekt, z. B. „ganze Zahlen“, gehört zu einer Klasse, etwa „Ringe“, durch die festgelegt ist, welche Nachricht, etwa „multiplizieren“, es versteht und wie es auf diese reagiert.
Entwicklung noch im Anfang!
Beispiele: C++, SMALLTALK, EIFFEL, etc.

Beispiel 63 (LISP)
LISP (List Processing Language) (John McCarthy 1959) basiert auf dem Listenkonzept und dem λ-Kalkül (Morzo Church 1941), daher Klammern.

$$V \rightleftharpoons \{x, y, z, \ldots, f, g, h, \ldots\}$$

sei eine (abzählbare) Menge von Variablen und

$$S \rightleftharpoons \{(,), \lambda, =\}$$

die Menge der Symbole mit $V \cap S = \emptyset$. Für $u = v$ mit $u, v \in V \cup S$ wird $u \equiv v$ geschrieben.

1. Für $x \in V$ ist x ein Term. x ist frei in x.
2. Ist $x \in V$ und t Term, so ist auch $(\lambda x\ t)$ Term. $y \in V$ ist genau dann frei in $(\lambda x\ t)$, wenn y frei in t und $y \not\equiv x$ ist.
3. Sind s, t Terme, so ist auch $(s\ t)$ ein Term, wobei s Operator- und t Operandenteil von $(s\ t)$ heißt. x ist genau dann frei in $(s\ t)$, wenn x frei in s oder frei in t ist.

Statt $(\ldots((t_1\ t_2)t_3)\ldots t_n)$ wird auch $(t_1\ t_2\ldots t_n)$ geschrieben, Klammern können weggelassen werden, wenn keine Unklarheiten entstehen.

Seien $x \in V$ ind r, s, t Terme über V. Dann heißt S_u^x Substitution, falls $S_u^x t$ wie folgt definiert ist:

1. Ist $t \in V$, so
$$S_u^x t \rightleftharpoons \left\{ \begin{array}{c} u \\ t \end{array} \right\}, \text{ falls } t \left\{ \begin{array}{c} \equiv \\ \not\equiv \end{array} \right\} x.$$
2. Ist $t \equiv (r\ s)$, so
$$S_u^x t \rightleftharpoons (S_u^x r\ S_u^x s).$$
3. Ist $t \equiv (\lambda y\ r)$, so
$$S_u^x t \rightleftharpoons \left\{ \begin{array}{c} (\lambda u\ S_u^x r) \\ (\lambda y\ S_u^x r) \end{array} \right\}, \text{ falls } y \left\{ \begin{array}{c} \equiv \\ \not\equiv \end{array} \right\} x.$$

Beispiel, was bei einer fehlenden Fallunterscheidung in 1., 3. entsteht:
$(\lambda x\ (x\ \lambda x\ (x\ y)))$ geht bei Ersetzung aller x durch $(u\ v)$ in
$(\lambda(u\ v)\ ((u\ v)\ \lambda(u\ v)\ ((u\ v)\ y)))$ über, was natürlich kein Term ist!

Sind $x, y \in V$ und t, u Terme, so gibt es folgende Ableitungsregeln:

1. β-Reduktion (Auswertung, Elimination des λ-Operators)

   $$((\lambda x\ t)\ u) \Longrightarrow S^x_u t,$$

   wenn t keine gebundene Variable x enthält.
   Enthält t die gebundene Variable x, so muß zunächst gemäß 2. umbenannt werden.

2. α-Konversion (Umbenennung von Variablen)

   $$((\lambda x\ t)\ u) \Longrightarrow S^x_y((\lambda y\ t)\ u),$$

   wenn y nicht in t vorkommt.

Beispiel:

a) $(\lambda x\ x(y\ z)) \overset{1.}{\Rightarrow} S^x_{yz} x \equiv (y\ z)$

b) $(\lambda x\ (x\ y)\ \lambda z\ z) \equiv ((\lambda x\ (x\ y))\ \lambda z\ z)$
$\overset{1.}{\Rightarrow} S^x_{\lambda z\ z}(x\ y) \equiv S^x_{\lambda z\ z} x\ S^x_{\lambda z\ z} y \equiv ((\lambda z\ z)\ y)$
$\overset{1.}{\Rightarrow} S^z_y z \equiv y$

c) $((\lambda x\ y)\ x) \overset{2.}{\Rightarrow} S^x_{x'}((\lambda x'\ y)\ x) \equiv (S^x_{x'}(\lambda x'\ y)\ S^x_{x'} x) \equiv (\lambda x'\ S^x_{x'}(y\ x)) \equiv (\lambda x'\ y)\ x$
$\overset{1.}{\Rightarrow} S^x_{x'} y \equiv y$

$\top \rightleftharpoons (\lambda x\ (\lambda y\ x))$

$\bot \rightleftharpoons (\lambda x\ (\lambda y\ y))$

Damit: $(\top x)\ y \equiv \ldots \equiv x$
$(\bot x)\ y \equiv \ldots \equiv y$

bedingte Ausdrücke: $(Px)\ y$ entspricht „**if** P **then** x **else** y **fi**",
wobei P eine Funktion ist, die $\top$ oder $\bot$ liefert.

logische Ausdrücke: AND $\rightleftharpoons (\lambda x\ \lambda y\ ((x\ y)\ \bot))$
OR $\rightleftharpoons (\lambda x\ \lambda y\ ((x\ \top)\ y))$
NOT $\rightleftharpoons (\lambda x\ ((x\ \bot)\ \top))$

Kern-LISP (pure LISP)

Kern-LISP besteht aus S-Ausdrücken (syntactic expressions) und auf S-Ausdrücken definierten Funktionen.

S-Ausdrücke: (in Backus-Naur-Formalismus)
NIL entspricht dem logischen $\bot$, T dem logischen $\top$.

⟨Ziffer⟩ ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

⟨Buchstabe⟩ ::= ⟨Buchstabe⟩ | ⟨Atom⟩⟨Buchstabe⟩ | ⟨Atom⟩⟨Ziffer⟩ | NIL | T

⟨S-Ausdruck⟩ ::= ⟨Atom⟩ | (⟨S-Ausdruck⟩.⟨S-Ausdruck⟩)

Listen sind genau die folgenden S-Ausdrücke:

1. Das Atom NIL,
2. Jeder S-Ausdruck, in dem die als rechte Teile vorkommenden Atome gleich NIL sind.

Beispiele für Listen:
(ABC) für $(A.(B.(C.NIL)))$,
$((AB)C)$ für $((A.(B.NIL)).(C.NIL))$

Funktionen: S-Menge der S-Ausdrücke

$$\text{CONS}: \; S \times S \longrightarrow S \;\; \text{mit} \;\; (\text{CONS } S_1 S_2) \equiv (S_1 \cdot S_2)$$

$$\text{CAR}: \; S \longrightarrow S \;\; \text{mit} \;\; (\text{CAR } S) \equiv \begin{cases} \text{linker Teil eines zusammengesetzten S-Ausdruk-} \\ \text{kes, also das erste Element einer Liste} \end{cases}$$

$$\text{CDR}: \; S \longrightarrow S \;\; \text{mit} \;\; (\text{CDR } S) \equiv \begin{cases} \text{rechter Teil des S-Ausdruckes, also der Rest der} \\ \text{Liste} \end{cases}$$

$$\text{ATOM}: \; S \longrightarrow \text{NIL}, \text{T} \;\; \text{mit} \;\; (\text{ATOM } S) \equiv \begin{cases} \text{T, wenn } S \text{ Atom ist} \\ \text{NIL sonst} \end{cases}$$

$$\text{EQ}: \; S \times S \longrightarrow \text{NIL}, \text{T} \;\; \text{mit} \;\; (\text{EQ } S_1 S_2) \equiv \begin{cases} \text{T, wenn } S_1, S_2 \text{ gleiche Atome sind} \\ \text{NIL sonst} \end{cases}$$

Näheres siehe Literaturverzeichnis Anhang E.

Anhang A

Aufgaben

Aufgabe 1

Natürliche Zahlen x und y zwischen 5 und 10, jeweils inklusive, lassen sich wie folgt mit Hilfe der Finger multiplizieren:
Man strecke $x-5$ bzw. $y-5$ Finger der rechten bzw. linken Hand (Daumen jeweils eingeschlossen und fünffingrige Hände vorausgesetzt!) und beuge jeweils die restlichen Finger. Sodann multipliziere man die Zahl der gebeugten Finger der rechten Hand mit der Zahl der gebeugten Finger der linken Hand, addiere das Ergebnis zum Zehnfachen der Summe der Zahlen der gestreckten Finger und erhält so xy [1].

a) Man begründe dieses Verfahren ausführlich!

b) Wie läßt sich dieser Algorithmus ausweiten?

Aufgabe 2

Zur Multiplikation natürlicher Zahlen x, y mit $x \leq y$ bilde man sukzessive

$$\begin{array}{rlrl} x_0 &\leftrightharpoons x, & y_0 &\leftrightharpoons y, \\ x_{\nu+1} &\leftrightharpoons \left\lfloor \frac{x_\nu}{2} \right\rfloor, & y_{\nu+1} &\leftrightharpoons 2y_\nu, \end{array} \qquad (\text{für } \nu = 0, 1, \ldots, n)$$

$$(\text{wobei } \lfloor r \rfloor \leftrightharpoons \max\{z \in \mathbb{Z} \mid z \leq r\} \text{ für } r \in \mathbb{R})$$

bis $x_n = 1$, d. h. n ist der kleinste Index ν mit $x_\nu = 1$, und hat dann

$$xy = \sum_{\substack{\nu = 0 \\ x_\nu \text{ ungerade}}}^{n} y_\nu .$$ [2]

(Beispiel: $43 \cdot 57 = 2451$ erhält man so

[1] Diese Fingermultiplikation wurde bereits beschrieben u. a. von Nicolas Chuquet (≈1445–≈1488), Pariser Bakkalaureus der Medizin, 1484 in seinem „Le Triparty en la science des nombres“ und von Bahā' al-Dīn Muḥammad ibn al-Ḥusain al-ᶜAmilī (⋆1547 Baalbeck, †1622 Isfahan).

[2] Das Verfahren wurde in modifizierter Form schon im alten Ägypten angewandt und wird gelegentlich als Russische- oder Türkische -Bauern-Methode oder einfach als Bauernmethode bezeichnet, da ja außer Halbieren und Verdoppeln eine Beherrschung des „Einmaleins“ hinfällig wird.

$$\begin{array}{rrl} 43 & 57 & * \\ 21 & 114 & * \\ 10 & \cancel{228} & \\ 5 & 456 & * \\ 2 & \cancel{912} & \\ 1 & \underline{+1824} & * \\ & 2451 & .) \end{array}$$

Man beweise dies etwa mittels Dualdarstellung!

Aufgabe 3

a) Man entwerfe eine Schaltung zur Berechnung von x^2, falls x eine

- 1-stellige Dualzahl,
- 2-stellige Dualzahl,
- 3-stellige Dualzahl

ist.

b) Die vorletzte Binärstelle von x^2 läßt sich besonders einfach darstellen. Diese Beobachtung ist für n-stelliges x mit $n \in \mathbb{N} \setminus \{1\}$ zu verallgemeinern und zu beweisen.

Aufgabe 4

Man deduziere Satz 1, (10), also die De-Morganschen Regeln ohne Rückgriff auf die ursprüngliche Bedeutung von $\wedge$, $\vee$ und $\bar{\ }$ allein aus den übrigen Regeln (1)–(9) und (11).

Aufgabe 5

Sei $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$:

a) Man bestimme die Zahl der Schaltfunktionen aus $\mathfrak{B}_n^m$.

b) Die Zahl der in ihrer Wirkung wesentlich voneinander verschiedenen Schaltungen mit n Eingängen und höchstens m Ausgängen ist zu berechnen.

c) Wieviele wesentlich verschiedene Schaltungen mit höchstens 3 Eingängen und höchstens 3 Ausgängen gibt es? (Das Ergebnis ist selbstverständlich explizit als natürliche Zahl anzugeben und zu begründen.)

Aufgabe 6

Ein Ventil V soll in Abhängigkeit von drei 0-1-Eingangssignalen a, b und c gesteuert werden, und zwar soll V genau dann geöffnet werden, wenn entweder genau eins der Signale a und c den Wert 1 hat oder wenn c den Wert 0 hat, falls a oder b den Wert 1 hat.

a) Man entwerfe und begründe eine Schaltung, die V wunschgemäß steuert.

b) Ein Boolescher Ausdruck in konjunktiver und in adjunktiver Normalform ist anzugeben, der die Steuerung beschreibt.

Aufgabe 7

Man zeige: Ist $\leq$ eine partielle Ordnung auf einer nichtleeren Menge V derart, daß $\inf\{x, y\}$ und $\sup\{x, y\}$ für alle $x, y \in V$ existieren, so ist $(V, \wedge, \vee)$

$$\text{mit} \quad \begin{array}{l} x \wedge y = \inf\{x, y\} \\ x \vee y = \sup\{x, y\} \end{array} \qquad \text{für } x, y \in V$$

ein Verband.

Aufgabe 8

Man skizziere die Diagramme aller wesentlich voneinander verschiedenen Verbände mit höchstens 6 Elementen.

Aufgabe 9

Man zeige: Jede nichtleere Kette ist ein distributiver Verband.

Aufgabe 10

Zu beweisen ist: In einem distributiven Verband sind die Komplemente jeweils eindeutig bestimmt.

Aufgabe 11

T_n sei der Teilerverband von $n \in \mathbb{N}$. Man charakterisiere n für den Fall, daß T_n

a) [r eine Kette

* b) ein Boolescher Verband

ist.

Aufgabe 12

Man beweise: $(B, \wedge, \vee, \overline{}, 1, 0)$ ist genau dann eine Boolesche Algebra, wenn

$$\begin{array}{rl} x \wedge y = y \wedge x, & x \vee y = y \vee x, \\ x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), & x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \\ x \wedge 1 = x, & x \vee 0 = x, \\ x \wedge \overline{x} = 0, & x \vee \overline{x} = 1 \end{array}$$

für alle $x, y, z \in B$ gelten.

Aufgabe 13

Eine nichtleere Teilmenge F von B, wobei $\mathcal{B} = (\mathcal{B}, \wedge, \vee, \overline{\ }, \infty, \prime)$ eine Boolesche Algebra sei, heiße Filter auf $\mathcal{B}$, falls $0 \notin F$ und

$$x, y \in F \Longrightarrow x \wedge y \in F$$

sowie

$$x \in F,\ y \in B,\ x \leq y \Longrightarrow y \in F$$

gelten.
Als Filter sind nachzuweisen:

a) Für $a \in B \setminus \{0\}$ die Menge $[a) \rightleftharpoons \{x \in B \mid a \leq x\}$.

b) Für $\mathcal{B} = (\mathcal{P}(\mathbb{N}), \cap, \cup, \overline{\ }, \mathbb{N}, \emptyset)$ die Menge K der kofiniten Teilmengen von $\mathbb{N}$, also

$$K = \{X \subseteq \mathbb{N} \mid |\overline{X}| \in \mathbb{N}_0\}.$$

Aufgabe 14

Man zeige die Gültigkeit von

$$A \wedge \overline{B} \prec C, \quad A \wedge \overline{B} \prec \overline{C} \Longrightarrow A \prec B$$

für Boolesche Ausdrücke A, B und C mittels einer formalen Ableitung aus schon bewiesenen Regeln.

Aufgabe 15

Aus einem Mathematikbuch für die 7. Klasse:

Herr König stürzt aus seinem Laden.
„*Wer von Euch hat mir meine Fensterscheibe eingeworfen?*“ donnert er die Kinder an, die verdattert vor seinem Laden stehen.
Benno sagt:„*Hans war es*“.
Hans sagt:„*Otto hat es getan*“.
Jutta sagt:„*Ich war es nicht*“.
Otto sagt:„*Hans hat gelogen*“.
Ja, wer war es nun, wenn

a) nur ein Kind gelogen hat,

b) nur ein Kind die Wahrheit gesagt hat?

Aufgabe 16

Die Transportationsregeln, also

$$A \wedge B \prec C \Longrightarrow A \prec \overline{B} \vee C \quad \text{und} \quad A \prec B \vee C \Longrightarrow A \wedge \overline{B} \prec C$$

für Boolesche Ausdrücke A, B und C sind aus schon bewiesenen Regeln formal herzuleiten.

Aufgabe 17

Forschungsminister Glanzhäuser hat es schwer. Er muß entscheiden, welches der folgenden wissenschaftlichen Großprojekte verwirklicht werden soll und welches nicht: die Pionenschleuder GABY, das Mikrometer-Teleskop LAUSCHI, die Riesensternwarte GUCKI, das Satellitenprojekt SAUSI, der Fusionsreaktor PLASMI und der Supercomputer DENKI. (Diese Namen sind natürlich Abkürzungen für hochwissenschaftliche Bezeichnungen.)
In seiner Entscheidungsnot beruft Minister Glanzhäuser ein Gutachter-Gremium aus lauter gelehrten Männern. Dessen Vorsitzender, Professor Müller-Bahlsen, legt schließlich nach langen Beratungen diese Entscheidung der Koryphäe vor:

a) GABY soll verwirklicht werden, jedoch weder SAUSI noch DENKI.

b) Keinesfalls dürfen sowohl LAUSCHI als auch GUCKI errichtet werden.

c) LAUSCHI und DENKI sollen gebaut werden, nicht jedoch GUCKI.

d) Falls DENKI, dann auch PLASMI.

e) GUCKI nicht, wohl aber SAUSI.

f) Falls LAUSCHI nicht, dann soll auch PLASMI nicht, wohl aber soll dann GABY verwirklicht werden.

g) Weder GABY noch DENKI.

Den Minister verwirrte dieser Rat sehr: „Das widerspricht sich doch“, klagte er seinem Staatssekretär Grimm. Doch dieser hatte eine rettende Idee. Herr Grimm ging davon aus, daß die sieben Aussagen des Professors abwechselnd wahr und falsch seien (wobei natürlich noch offen war, ob er mit einer wahren oder einer falschen Aussage angefangen hat) und fand so tatsächlich die eindeutige Entscheidung des Gutachtergremiums.
Wie lautet sie?

Die Aufgabe stammt von Zweistein aus der ZEIT.

Aufgabe 18

Nach dem Verfahren von Quine-McCluskey minimalisiere man die folgenden Terme:

a) $(\overline{A} \vee C) \wedge (\overline{B} \vee C) \wedge \overline{\overline{A} \vee B \to C}$;

b) $(A \to B) \to ((B \to C) \to (A \to C))$.

Aufgabe 19

Man wende das Verfahren von Quine-McCluskey auf den Ausdruck

$$(\overline{A} \wedge \overline{B}) \vee ((A \vee B \vee C) \wedge (A \vee B \vee \overline{C})) \vee (A \wedge B \wedge C \wedge D)$$

an.

Aufgabe 20

f aus $\mathbb{R}^{\mathbb{R}}$ heiße monoton wachsend bzw. monoton fallend im Falle

$$\forall x, y \in \mathbb{R}: \; x < y \Rightarrow f(x) \le f(y) \quad \text{bzw.} \quad f(x) \ge f(y)$$

und monoton, falls f monoton wachsend oder monoton fallend ist. Man gebe eine Kennzeichnung von „f ist nicht monoton" an, die kein Negat mehr enthält.

Aufgabe 21

Man minimalisiere nach Quine-McCluskey:

a) $(\overline{A} \wedge \overline{B} \wedge \overline{C} \wedge D) \vee (\overline{A} \wedge \overline{B} \wedge C \wedge \overline{D}) \vee (\overline{A} \wedge B \wedge C \wedge \overline{D}) \vee (A \wedge \overline{B} \wedge \overline{C} \wedge \overline{D}) \vee$
$\vee (A \wedge \overline{B} \wedge \overline{C} \wedge D) \vee (A \wedge \overline{B} \wedge C \wedge \overline{D}) \vee (A \wedge \overline{B} \wedge C \wedge D) \vee (A \wedge B \wedge \overline{C} \wedge \overline{D}) \vee$
$\vee (A \wedge B \wedge \overline{C} \wedge D) \vee (A \wedge B \wedge C \wedge \overline{D}) \vee (A \wedge B \wedge C \wedge D).$

b) $A \vee C \to ((A \wedge \overline{B}) \vee \overline{C} \to B \wedge \overline{C}).$

Aufgabe 22

Für prädikatenlogische Formeln α und β ist zu beweisen:
$\alpha \to \beta$ ist genau dann allgemeingültig, wenn β aus α folgt.

Aufgabe 23

α und β seien Formeln, $\mathcal{M}$ eine Menge von Formeln der Prädikatenlogik und ξ eine Individuenvariable derart, daß ξ in $\mathcal{M} \cup \{\beta\}$ nicht frei vorkomme;
ferner gelte $\mathcal{M} \cup \{\alpha\} \Vdash \beta$.

Man zeige die Gültigkeit von $\mathcal{M} \cup \{\exists \xi \alpha\} \Vdash \beta$.

Aufgabe 24

Gibt es schlichte Graphen der Ordnung n mit den Graden

a) 0, 1, 2, 3 und $n = 4$?

b) 1, 2, 2, 3, 4, 5, 6 und $n = 7$?

c) 4, 4, 4, 4, 4, 4 und $n = 6$?

d) 1, 1, 2, 3, 4, 5 und $n = 6$?

* **Aufgabe 25**

Sei $n \in \mathbb{N}$; man zeige: Es gibt einen kubischen Graphen der Ordnung n genau dann, wenn n gerade und $n \ge 4$ ist.

Aufgabe 26

$A = (a_{\mu\nu})_{\mu,\nu=1,\ldots,n}$ sei Adjazenzmatrix eines Graphen bzw. Digraphen $\mathcal{G}$ mit $\epsilon(\mathcal{G}) = \{E_1, \ldots, E_n\}$ und $n \in \mathbb{N}$. Zu beweisen ist:

$$\sum_{\nu=1}^{n} a_{\mu\nu} = \gamma(E_\mu) \quad \text{und} \quad \sum_{\mu=1}^{n} a_{\mu\nu} = \gamma(E_\nu)$$

bzw.

$$\sum_{\nu=1}^{n} a_{\mu\nu} = \gamma^+(E_\mu) \quad \text{und} \quad \sum_{\mu 1}^{n} a_{\mu\nu} = \gamma^-(E_\nu)$$

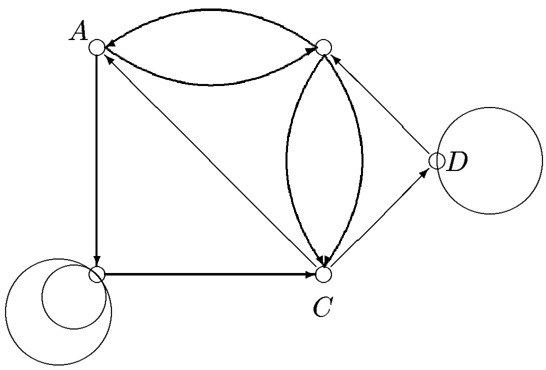
für $\mu, \nu \in \mathbb{A}_n$.

* **Aufgabe 27**

Man entwerfe ein Transitionsdiagramm eines Automaten gemäß Beispiel 38c), der nach geeigneter Wahl von Zuständen die Sprache über $\{a, b\}$ mit $a \neq b$ erkennt, deren Wörter eine gerade Anzahl von a's oder eine ungerade Anzahl von b's enthalten.

Aufgabe 28

Ein Programmablauf kann durch folgenden gerichteten Graphen $\mathcal{G}$ charakterisiert werden.



a) Man stelle eine Adjazenzmatrix von $\mathcal{G}$ auf.

b) Für gewisse Komplexitätsuntersuchungen bestimme man die Zahl der Kantenzüge der Länge 4 von C nach A und die Zahl der Kantenzüge der Länge 8 von A nach D.

Aufgabe 29

Ein Turnier mit $n \in \mathbb{N} \setminus \{1\}$ Teilnehmern (vgl. Beispiel 38b)) sei gegeben. Man beweise den Satz von Rédei [3]: Es gibt einen Weg, der alle Ecken enthält.

[3] Nach dem großen ungarischen Mathematiker László Rédei (⋆15.11.1900 in Rákoskeresztut, †21.11.1980), Professor in Szeged und Budapest, der ihn in seiner Arbeit „Ein kombinatorischer Satz." Acta Sci. Math. (Szeged), 7 (1934), S. 39–43, bewiesen hat.

Aufgabe 30

In einem Unternehmen sollen 3 voneinander vollkommen unabhängige Rechnernetze eingerichtet werden. Wieviele Rechner müssen mindestens installiert werden, um die 600 vorhandenen teuren Verbindungsleitungen auszunutzen?

Aufgabe 31

Der zu einem Graphen $\mathcal{G} = (\mathcal{E}, \mathcal{K})$ mit $\mathcal{K} \subseteq P_2(\mathcal{E})$ <u>komplementäre</u> Graph sei $\overline{\mathcal{G}} \rightleftharpoons (\mathcal{E}, \overline{\mathcal{K}})$ mit $\overline{\mathcal{K}} \rightleftharpoons P_2(\mathcal{E}) \setminus \mathcal{K}$. Ein schlichter Graph $\mathcal{G}$ heiße <u>selbstkomplementär</u> im Falle $\overline{\mathcal{G}} \simeq \mathcal{G}$.

$\mathcal{G} = (\mathcal{E}, \mathcal{K})$ sei ein selbstkomplementärer Graph der Ordnung $n \in \mathbb{N}$ und der Kantenzahl k.

a) Man zeige: Zu jedem A aus $\mathcal{E}$ mit $\gamma(A) = m$ gibt es ein B aus $\mathcal{E}$ mit $\gamma(B) = n - 1 - m$.

b) Für $n > 1$ hat $\mathcal{G}$ keine Ecke E mit $\gamma(E) = 0$ oder $\gamma(E) = n - 1$. Dies ist zu beweisen.

c) Man zeige: $k = \frac{1}{4}n(n-1)$.

d) $n \equiv_4 0$ oder $n \equiv_4 1$ ist nachzuweisen.

e) Man bestimme bis auf Isomorphie alle selbstkomplementären Graphen der Ordnung $n < 8$.

Aufgabe 32

Auf einer Party treffen sich mindestens drei, aber endlich viele, sagen wir genau n Leute. Je zwei Personen, die sich nicht kennen, haben jedoch zusammen mindestens n Bekanntschaften. Ist es möglich, alle Teilnehmer so um einen runden Tisch zu setzen, daß sowohl der linke als auch der rechte Nachbar Bekannter ist?
Begründung!

Aufgabe 33

Man zeige: Die Zahl der Kanten eines dreieckslosen, d. h. keinen Teilgraph aus C_3 enthaltenden schlichten Graphen der Ordnung $n \in \mathbb{N}$ ist höchstens $\left\lfloor \frac{n^2}{4} \right\rfloor$.

Aufgabe 34

a) Ein Algorithmus zur Umwandlung einer in Suffixnotation gegebenen Formel in eine äquivalente in Infixnotation ist zu entwickeln.

b) Man stelle $((a+b) - 3c(4+a))/(5(a-b) - 2d^2)$ in Suffixnotation dar.

Aufgabe 35

Man entwickle ein Petrinetz mit zugehöriger Anfangsmarkierung, das die Addition nichtnegativer ganzer Zahlen x und y bewerkstelligt durch Rückführung auf die Addition und Subtraktion von 1.

Aufgabe 36

Sei $a \in \mathbb{N}_0$ und $a = \sum\limits_{\nu=0}^{n} a_\nu 10^\nu$ mit $a_\nu \in \mathbb{U}_10$ für $\nu = 0, 1, \ldots, n$. Dann heiße

$$W(a) \rightleftharpoons \sum_{\nu=0}^{n} (-1)^{n-\nu} a_\nu$$

Wechselsumme von a.

a) Man zeige: $11 | a \Longleftrightarrow 11 | W(a)$.

b) Die genannten Begriffe und Beziehungen sind auf g-adische Entwicklungen mit $g \in \mathbb{N} \setminus \{1\}$ zu verallgemeinern.

Aufgabe 37

Man zeige für die in der Vorlesung eingeführten Funktionen ν_B und β_B mit den dortigen Bezeichnungen und $\star \in \{+, -, \cdot, /\}$

a) $\qquad \nu_B : \ (\mathbb{R} \times \mathbb{Z}, \star) \overset{\simeq}{\twoheadrightarrow} (N_B, \star)$,

b) $\qquad \beta_B : \ (N_B, \star) \overset{\simeq}{\rightarrowtail\!\!\twoheadrightarrow} (\mathbb{R}, \star)$.

Aufgabe 38

A und B seien Zeichenvorräte mit $|A| = m \in \mathbb{N}$ und $|B| = n \in \mathbb{N}$.

a) Wieviele A-B-Codierungen der Länge $l \in \mathbb{N}$ gibt es?

b) Wieviele Codierungen von $Z = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ in $\mathbb{B}$ der LÄnge 4, 5, 6 und 7 gibt es?

Aufgabe 39

Die zehn Ziffern des Dezimalsystems sollen in $\mathbb{B}^8$ dargestellt werden.

a) Wie groß kann die Hammingzahl eines solchen Codes bei geschickter Wahl mindestens sein?

b) Man gebe einen solchen Code mit möglichst großer Hammingzahl konkret an und erläutere seine Konstruktion.

Aufgabe 40

Man berechne $15 - 19$ in einer ternären Darstellung der Länge 6 durch 2-Komplementation.

Aufgabe 41

Man berechne $15 - 19$ mittels 5-Komplementation in einer Darstellung der Länge 6 zur Basis 5.

Aufgabe 42

Eine Pikosekunde verhält sich zu einer Sekunde wie eine Sekunde zu?
Bitte in Jahren etc. angeben.

Aufgabe 43

Man entwerfe ein Serienparallelmultiplikationswerk für 8-stellige Dualzahlen.

Aufgabe 44

Wie könnte man ein schnelles Quadrierwerk für n-stellige Dualzahlen, also eine Schaltung, die für n-stelliges x schnell x^2 berechnet, zur Konstruktion eines Multiplizierwerkes für n-stellige Dualzahlen benutzen?
Man erläutere die Antwort!

Anhang B

Lösungen

Aufgabe 1

a) Seien $x, y \in \mathbb{N}$ mit $5 \leq x, y \leq 10$ und $z \in \{x, y\}$.

$$s_z \eqqcolon z - 5 \quad \text{(gestreckte Finger)}$$

$$b_z \eqqcolon 5 - s_z \quad \text{(gebeugte Finger)}$$

Der Algorithmus liefert

$$\begin{aligned} b_x \cdot b_y + 10 \cdot (s_x + s_y) &= (5 - s_x) \cdot (5 - s_y) + 10 \cdot (s_x + s_y) \\ &= 25 - 5(s_x + s_y) + s_x \cdot s_y + 10(s_x + s_y) \\ &= 25 + (x - 5)(y - 5) + 5(x - 5 + y - 5) \\ &= 25 + xy - 5(x + y) + 25 + 5(x + y) - 50 \\ &= x \cdot y \end{aligned}$$

b) Betrachte $x, y \in \mathbb{N}$ mit $10 \leq x, y \leq 15$ und $z \in \{x, y\}$. Mit

$$s_z \eqqcolon z - 10 \text{ und } b_z \eqqcolon 15 - z$$

gilt dann

$$\begin{aligned} b_x \cdot b_y &= (15 - x)(15 - y) \\ &= 225 - 15(x + y) + xy \\ &= xy - 15(x - 10 + y - 10) - 300 + 225 \\ &= xy - 15(s_x + s_y) - 75 \end{aligned}$$

Also: $xy = b_x b_y + 15(s_x + s_y) + 75$

$$\begin{aligned} \text{Oder: } s_x s_y &= (x - 10)(y - 10) \\ &= xy - 10(x + y) + 100 \\ &= xy - 10(x - 10 + y - 10) - 200 + 100 \\ &= xy - 10(s_x + s_y) - 100 \end{aligned}$$

Also: $xy = s_x s_y + 10(s_x + s_y) + 100$

Aufgabe 2 (Russische Bauern-Multiplikation)

Beispiel: $37 \cdot 47$

ν	x_ν	y_ν
0	37	47
1	18	~~94~~
2	9	188
3	4	~~376~~
4	2	~~752~~
5	1	1504
		1739

Seien also $x, y \in \mathbb{N}$, $x \leq y$ und

$$x_0 \rightleftharpoons x, \quad y_0 \rightleftharpoons y, x_\nu \rightleftharpoons \left\lfloor \frac{x_{\nu-1}}{2} \right\rfloor \qquad y_\nu \rightleftharpoons 2y_{\nu-1} \qquad \text{für } \nu = 1, \dots, n \text{ und } x_n = 1.$$

Behauptung 1:
Mit

$$d_\nu \rightleftharpoons x_\nu \mathrm{mod} 2$$

gilt

$$(1) \quad \sum_{\nu=0}^{n} d_\nu 2^\nu.$$

Beweis: (Induktion nach n)

IA: Mit $n = 0$ muß $x = x_0 = 1$ gelten und man hat $d_0 = 1$, also

$$x = 1 = d_0 2^0 = \sum_{\nu=0}^{n} d_\nu 2^\nu.$$

IS: (1) sei bereits gezeigt für $n \in \mathbb{N}$.
Damit sind also alle natürlichen Zahlen $x < 2^{n+1}$ erfaßt.
Sei nun $x \in \mathbb{N}$ mit $2^{n+1} \leq x < 2^{n+2}$.
Gilt $x = 2^{n+1}$, so hat man

$$\begin{aligned} x_0 &= x = 2^{n+1} \\ x_1 &= \left\lfloor \frac{x_0}{2} \right\rfloor = \lfloor 2^n \rfloor = 2^n \\ \vdots &\ \ \vdots \\ x_n &= \left\lfloor \frac{x_{n-1}}{2} \right\rfloor = \left\lfloor \frac{2^2}{2} \right\rfloor = 2 \\ x_{n+1} &= \left\lfloor \frac{2}{2} \right\rfloor = 1, \end{aligned}$$

also $d_\nu = 0$ für $\nu = 0, \dots, n$ und $d_{n+1} = 1$, was $x = 2^{n+1} = \sum_{\nu=0}^{n+1} d_\nu 2^\nu$ liefert.

Sei nun $2^{n+1} < x < 2^{n+2}$. Sei $x' \rightleftharpoons x - 2^{n+1}$.
Wegen $1 \leq x' < 2^{n+1}$ gibt es nach Induktionsvoraussetzung ein $m \in \mathbb{N}_0$ mit $m < n+1$ und

$$x' = \sum_{\mu=0}^{m} d'_\mu 2^\mu$$

und wegen $x = x' + 2^{n+1}$ gilt

$$\begin{aligned} x_0 &= x = x'_0 + 2^{n+1} \\ x_1 &= \left\lfloor \frac{x_0}{2} \right\rfloor = \left\lfloor \frac{x'_0}{2} \right\rfloor + 2^n = x'_1 + 2^n \\ x_2 &= \left\lfloor \frac{x_1}{2} \right\rfloor = \left\lfloor \frac{x'_1}{2} \right\rfloor + 2^{n-1} = x'_2 + 2^{n-1} \\ &\vdots \quad \vdots \end{aligned}$$

Allgemein also:

$$(2) \quad x_\mu = x'_\mu + 2^{n+1-\mu} \text{ für } \mu = 0, \ldots, n.$$

Wegen $m < n+1$ hat man für $\mu = 0, \ldots, m$ damit

$$(3) \quad d_\mu = x_\mu \mathrm{mod} 2 = \left(x'_\mu + 2^{n+1-\mu}\right) \mathrm{mod} 2 = x'_\mu \mathrm{mod} 2 = d'_\mu$$

Ferner hat man (2) zufolge

$$x_m = x'_m + 2^{n+1-m} = 1 + 2^{n+1-m}$$

und weiter

$$x_{m+i} = \left\lfloor \frac{x_{m+i-1}}{2} \right\rfloor = 2^{n-m-(i-1)}.$$

Für $m + j = n$ gilt $j = n - m$, also

$$x_n = 2^{n-m-(n-m-1)} = 2, \quad x_{n+1} = \left\lfloor \frac{x_n}{2} \right\rfloor = 1.$$

Das heißt also für $\mu = m+1, \ldots, n$: $d_\mu = 0$ und $d_{n+1} = 1$.
Zusammen mit (3) also:

$$\begin{aligned} x &= x' + 2^{n+1} = 2^{n+1} + \sum_{\mu=0}^{m} d'_\mu 2^\mu \\ &= \sum_{\mu=m+1}^{n+1} d_\mu 2^\mu + \sum_{\mu=0}^{m} d_\mu 2^\mu \\ &= \sum_{\mu=0}^{n+1} d_\mu 2^\mu \end{aligned}$$

BEHAUPTUNG 2:

(4) $y_\nu = 2^\nu y$ für $\nu = 0, \dots, n$

BEWEIS:
Auch hier Induktion nach n.

(1) und (4) liefern nun für ungerade x_ν:

$$\sum_{\nu=0}^{n} y_\nu \overset{(4)}{=} \sum_{\nu=0}^{n} 2^\nu y = \left(\sum_{\nu=0}^{n} d_\nu 2^\nu\right) y \overset{(1)}{=} x \cdot y.$$

Aufgabe 3

a) I. $x \in \mathbb{B}$. Dann ist $x = x^2$ und man hat

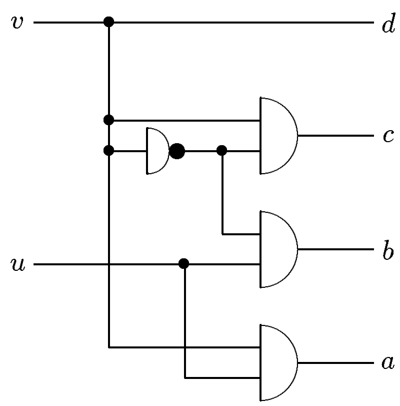
$$x \longrightarrow x^2$$

II. $x = uv$ und $x^2 = abcd$ mit $a, b, c, d, u, v \in \mathbb{B}$. Dann folgt:

u	v	a	b	c	d
0	0	0	0	0	0
0	1	0	0	0	1
1	0	0	1	0	0
1	1	1	0	0	1

, offenbar also

$$\begin{aligned} d &= v \\ c &= 0 \\ b &= u \wedge \overline{v} \\ a &= u \wedge v \end{aligned}.$$



III. $x = uvw$ und $x^2 = abcdef$ mit $a, b, c, d, e, f, u, v, w \in \mathbb{B}$. Dann folgt:

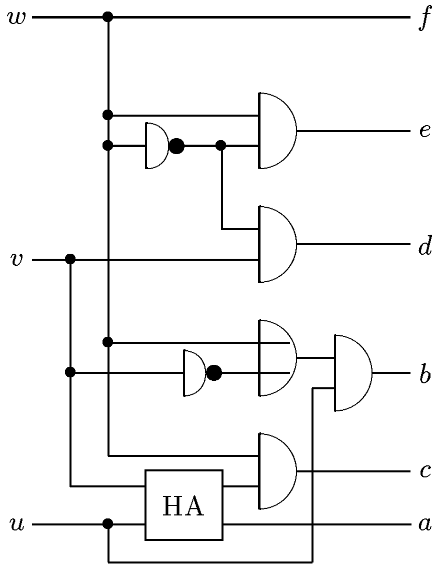
u	v	w	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	1
0	1	0	0	0	0	1	0	0
0	1	1	0	0	1	0	0	1
1	0	0	0	1	0	0	0	0
1	0	1	0	1	1	0	0	1
1	1	0	1	0	0	1	0	0
1	1	1	1	1	0	0	0	1

und somit

$$\begin{aligned} f &= w \\ e &= 0 \\ d &= v \wedge \overline{w} \\ c &= (u \oplus v) \wedge w \\ b &= u \wedge (\overline{v} \vee w) \\ a &= u \wedge v \end{aligned}.$$

Schaltung siehe nächste Seite.

Schaltung zu 3a)III.:



b) Für $x \in \mathbb{N} \setminus \{1\}$:
Gilt $x^2 = \sum_{\nu=0}^{k} a_\nu 2^\nu$ mit $a_\nu \in \mathbb{B}$ für $\nu = 0, \ldots, k$, so ist $a_1 = 0$, oder anders ausgedrückt: beim Teilen durch 4 läßt x^2 nur die Reste 0 und 1. Noch anders:

$$x^2 \equiv_4 0, 1 \qquad (x \in \mathbb{Z}).$$

Beweis:
Es sei x

I. gerade: etwa $x = 2y$ mit $y \in \mathbb{Z}$.
Dann folgt $x^2 = 4y^2$, also $4|x^2$ oder $x^2 \equiv_4 0$.

II. ungerade: etwa $x = 2y + 1$ mit $y \in \mathbb{Z}$.
Das ergibt $x^2 = 4y^2 + 4y + 1 = 4(y^2 + y) + 1$ oder $x^2 \equiv_4 1$.

Aufgabe 4

Durch (9) ist $\overline{}$, also $x \mapsto \overline{x}$ eindeutig bestimmt, denn mit $x \wedge y = 0$ und $x \vee y = 1$ gilt

$$\begin{aligned}
y &\overset{(6)}{=} y \vee 0 \\
&\overset{(9)}{=} y \vee (x \wedge \overline{x}) \\
&\overset{(5)}{=} (y \vee x) \wedge (y \vee \overline{x}) \\
&\overset{(1)}{=} (x \vee y) \wedge (y \vee \overline{x}) \\
&\overset{\text{Vorauss.}}{=} 1 \wedge (y \vee \overline{x}) \\
&\overset{(9)}{=} (x \vee \overline{x}) \wedge (y \vee \overline{x})
\end{aligned}$$

$$
\begin{aligned}
&\overset{(1)}{=} && (\overline{x} \vee x) \wedge (\overline{x} \vee y) \\
&\overset{(5)}{=} && \overline{x} \vee (x \wedge y) \\
&\overset{\text{Vorauss.}}{=} && \overline{x} \vee 0 \\
&\overset{(6)}{=} && \overline{x}
\end{aligned}
$$

Weiter ist

$$(x \wedge y) \wedge (\overline{x} \vee \overline{y}) =^{(5),(1),(2),(9),(7)}_{\cdots} = 0$$

und

$$(x \wedge y) \vee (\overline{x} \vee \overline{y}) =^{(5),(2),(1),(2),(9),(7)}_{\cdots} = 1.$$

Nach dem oben bemerkten folgt $\overline{x} \vee \overline{y} = \overline{x \wedge y}$, was sogleich

$$\overline{x \vee y} \overset{(8)}{=} \overline{\overline{\overline{x}} \vee \overline{\overline{y}}} = \overline{\overline{\overline{x} \wedge \overline{y}}} \overset{(8)}{=} \overline{x} \wedge \overline{y},$$

insgesamt also (10) liefert.

Aufgabe 5

$n \in \mathbb{N}_0$, $m \in \mathbb{N}$.

a) $$|\mathfrak{B}_n^m| = |\mathbb{B}^{m\mathbb{B}^n}| = |\mathbb{B}|^{m|\mathbb{B}|^n} = (2^m)^{(2^n)} = 2^{m \cdot 2^n}$$

b) Mittels a) ergibt sich:

$$
\begin{aligned}
|\bigcup_{\mu=1}^{m} \mathfrak{B}_n^\mu| &= \sum_{\mu=1}^{m} |\mathfrak{B}_m^\mu| = \sum_{\mu=1}^{m} 2^{\mu \cdot 2^n} = \sum_{\mu=0}^{m} \left(2^{2^n}\right)^\mu - 1 \\
&= \frac{\left(2^{2^n}\right)^{m+1} - 1}{2^{2^n} - 1} - 1 = \frac{1}{2^{2^n} - 1}\left(2^{2^n(m+1)} - 1 - 2^{2^n} + 1\right) \\
&= \frac{2^{2^n}\left(2^{2^n m} - 1\right)}{2^{2^n} - 1}.
\end{aligned}
$$

c) Mittels b) hat man für die erfragte Zahl k:

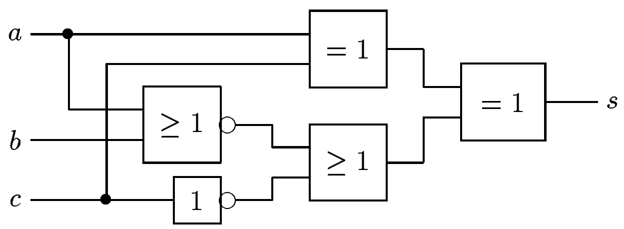
$$
\begin{aligned}
k &= \sum_{\nu=0}^{3} |\bigcup_{\mu=1}^{3} \mathfrak{B}_\nu^\mu| = \sum_{\nu=0}^{3} \frac{2^{2^\nu}}{2^{2^\nu} - 1}\left(2^{2^\nu \cdot 3} - 1\right) \\
&= \frac{2}{1}(8-1) + \frac{4}{3}(2^6 - 1) + \frac{16}{15}(2^{12} - 1) + \frac{256}{255}(2^{24} - 1) = \ldots \\
&= 16\ 847\ 474.
\end{aligned}
$$

Aufgabe 6

s stehe für das gewünschte Steuersignal, das genau dann den Wert 1 hat, falls V geöffnet wird.
Aus den oben genannten Bedingungen ergibt sich für s:

$$s = (a \oplus c) \oplus ((a \vee b) \to \overline{c}) = (a \oplus b) \oplus (\overline{(a \vee b)} \vee \overline{c}).$$

a) Obiges liefert



b) Mit Hilfe der üblichen Umformungen ergibt sich:

$$\begin{aligned}
s &= (a \oplus b) \oplus ((\overline{a} \wedge \overline{b}) \vee \overline{c}) \\
&= ((\overline{a} \vee \overline{c}) \wedge (a \vee c)) \oplus ((\overline{a} \wedge \overline{b}) \vee \overline{c}) \\
&= (\overline{(\overline{a} \vee \overline{c}) \wedge (a \vee c)} \vee \overline{(\overline{a} \wedge \overline{b}) \vee \overline{c}}) \wedge ((\overline{a} \vee \overline{c}) \wedge (a \vee c)) \vee ((\overline{a} \wedge \overline{b}) \vee \overline{c}) \\
&= (\overline{a} \vee \overline{c}) \wedge (\overline{a} \vee c) \wedge ((\overline{a} \vee c) \vee b) \wedge (a \vee b \vee \overline{c}) \\
&= \overline{a} \wedge (b \vee \overline{c}).
\end{aligned}$$

Als adjunktive Normalform erhält man sofort $s = (\overline{a} \wedge b) \vee (\overline{a} \wedge \overline{c})$.

Aufgabe 7

Zu zeigen:

1) Assoziativität von $\wedge$ und $\vee$, denn dann sind $(V, \wedge)$ und $(V, \vee)$ Halbgruppen

2) Kommutativität und Idempotenz von $(V, \wedge)$ und $(V, \vee)$

3) Eigenschaft (12): $x \wedge y = x \Longleftrightarrow x \vee y = y$ für alle $x, y \in V$

Beweis:

1) Seien $s, t, u, v, w, x, y, z \in V$ und $U \subseteq V$.
Wir benutzen $s \leq U \rightleftharpoons \forall u \in U: \; s \leq u$
und damit auch $s \leq U \Leftrightarrow s \leq \inf U$, sofern $\inf U$ existiert.
Zu zeigen ist $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ sowie $(x \vee y) \vee z = x \vee (y \vee z)$.
Es gilt $(x \wedge y) \wedge z = \inf\{x \wedge y, z\} = \inf\{\inf\{x, y\}, z\} \rightleftharpoons s$
und $x \wedge (y \wedge z) = \inf\{x, y \wedge z\} = \inf\{x, \inf\{y, z\}\} \rightleftharpoons t$.
Weil $\inf\{u, v\}$ nach Voraussetzung stets existiert, gilt weiter
$s \leq \inf\{x, y\}$, $s \leq z$
$s \leq \{x, y, z\}$

$s \leq x$, $s \leq \inf\{y, z\}$,
also folgt $s \leq \inf\{x, \inf\{y, z\}\} = t$. Analog erhält man $t \leq s$ und daher $s = t$, also die Assoziativität von $\wedge$.
Entsprechend folgt die von $\vee$.

2) Es gilt $x \wedge y = \inf\{x, y\} = \inf\{y, x\} = y \wedge x$
und $x \vee y = \sup\{x, y\} = \sup\{y, x\} = y \vee x$,
was die Kommutativität zeigt
und $x \wedge x = \inf\{x, x\} = \inf\{x\} = x$
sowie $x \vee x = \sup\{x, x\} = \sup\{x\} = x$,
was die Idempotenz zeigt.

3) Wegen $x = x \wedge y = \inf\{x, y\} \Longleftrightarrow x \leq y \Longleftrightarrow y = \sup\{x, y\} = x \vee y$ gilt auch (12).

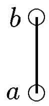
Aufgabe 8

Methode: Etwa gemäß Satz 5 alle möglichen partiellen Ordnungen betrachten und Herausfiltern von denen, die die zwei Elementen stets inf und sup liefern.

$|V| = 1$

$a \leq a$

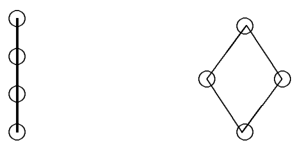
$|V| = 2$



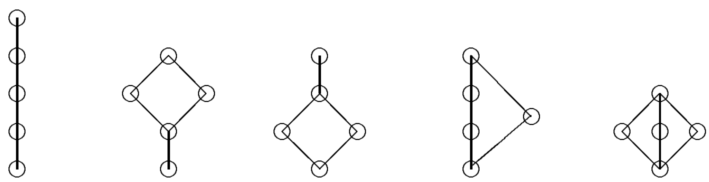
$a \leq a$
$b \leq b$
$a \leq b$

$|V| = 3$

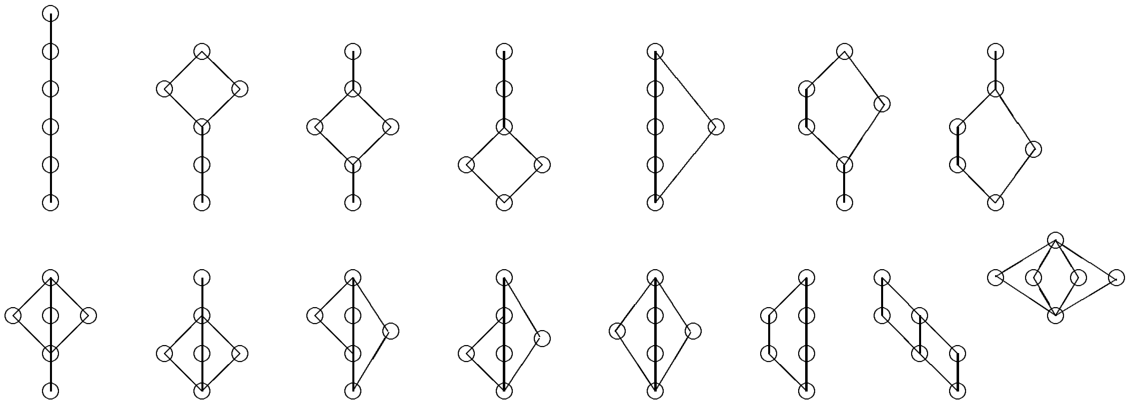
$|V| = 4$



$|V| = 5$



$|V| = 6$



Aufgabe 9

Zu zeigen:
Jede nichtleere Kette $\mathcal{K} = (K, \leq)$ ist ein distributiver Verband.
Nach Satz 7 ist $\mathcal{K}$ ein Verband, es genügt also, die Distributivität zu zeigen, d. h.

$$x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z) \text{ für alle } x, y, z \in K.$$

Beweis:
Seien also $x, y, z \in K$ und

1) $x \leq y$: Dann folgt $x \wedge y = y$ und im Falle

α) $x \leq z$, also $x \wedge z = x$ ergibt sich

$$x \wedge (y \vee z) \leq x \leq x \vee y = y \vee x = (x \wedge y) \vee (x \wedge z),$$

β) $z \leq x$, also $x \wedge z = z$ hat man

$$x \wedge (y \vee z) \leq y \vee z = (x \wedge y) \vee (x \wedge z).$$

Insgesamt folgt also die Distributivität.

Aufgabe 10

Zu zeigen:
In einem distributiven Verband sind die Komplemente jeweils eindeutig bestimmt.
Beweis:
Sei $(V, \wedge, \vee)$ ein distributiver Verband mit 0 und 1 sowie $x \in V$ und y und z Komplemente von x, also

$$x \wedge y = 0 = x \wedge z \quad \text{und} \quad x \vee y = 1 = x \vee z.$$

Dann folgt

$$\begin{array}{lcl} y & = & y \vee 0 = y \vee (x \wedge z) \\ & \overset{\text{Distributivität}}{=} & (y \vee x) \wedge (y \vee z) \\ & \overset{\text{Vorauss.}}{=} & (x \vee z) \wedge (y \vee z) \\ & \overset{\text{Distributivität}}{=} & (x \wedge y) \vee z = 0 \vee z \\ & = & z \end{array}$$

Aufgabe 11

a) BEHAUPTUNG:
$\mathcal{T}_n$ ist genau dann eine Kette, wenn n Primzahlpotenz ist.
BEWEIS

$\Leftarrow$: Sei $n = p^k$ mit $p \in \mathbb{P}$ und $k \in \mathbb{N}_0$. Dann gilt

$$T(n) = \{p^\kappa \mid \kappa \in \mathbb{U}_{k+1}\}$$

und wegen

$$p^0 = 1|p^1|p^2|\cdots|p^{k-1}|p^k$$

ist $(T(n), |)$ Kette.

$\Rightarrow$: Für $n = 1$ gilt $n = p^0$ für jedes $p \in \mathbb{P}$, also ist n Primzahlpotenz.
Sei $n > 1$: Dann existiert ein $p \in \mathbb{P}$ mit $p|n$.
Sei nun $q \in \mathbb{P}$ mit $q|n$. Im Falle $p \neq q$ hätte man also die Unvergleichbarkeit von p und q im Widerspruch zu $\mathcal{T}_n$ als Kette.
Also folgt $p = q$, n ist Primzahlpotenz.

b) BEHAUPTUNG:
$\mathcal{T}_n$ ist genau dann ein Boolescher Verband, wenn n quadratfrei ist, d. h. es gibt kein $k \in \mathbb{N} \setminus \{1\}$ mit $k^2|n$.
BEWEIS:

$\Leftarrow$: Nach Beispiel 10c) ist $\mathcal{T}_n$ ein distributiver Verband.
Wegen $1|x$ und $x|n$ für alle $x \in T(n)$ ist gemäß Satz 13 1 die Null und n die Eins von $\mathcal{T}_n$.
Es gilt zudem $\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = x \cdot y$ für $x, y \in \mathbb{N}$.
n sei quadratfrei und $x \in T(n)$.
BEHAUPTUNG:
$\overline{x} \rightleftharpoons \frac{n}{x}$ ist Komplement von x in $\mathcal{T}_n$.
BEWEIS:
Gäbe es ein $t \in \mathbb{N} \setminus \{1\}$ mit $t|x$ und $t|\frac{n}{x}$, hätte man

$$t^2|x\frac{n}{x} = n$$

im Widerspruch zur Quadratfreiheit von n.
Also gilt

$$\mathrm{ggT}(x, \overline{x}) = \mathrm{ggT}(x, \frac{n}{x}) = 1.$$

Damit folgt

$$\operatorname{kgV}(x,\overline{x}) = \frac{x \cdot \overline{x}}{\operatorname{ggT}(x,\overline{x})} = x \cdot \frac{n}{x} = n.$$

$\Rightarrow$: $\mathcal{T}_n$ sei Boolescher Verband. Wäre n nicht quadratfrei, gäbe es ein $p \in \mathbb{P}$ mit $p^2|n$, also $t \in \mathbb{N}$ mit $n = t \cdot p^2$.
Für das Komplement $\overline{p} \in T(n)$ von $p \in T(n)$ in $\mathcal{T}_n$ gilt dann

$$\operatorname{ggT}(p,\overline{p}) = 1 \text{ sowie } p^2 t = n = \operatorname{kgV}(p,\overline{p}) = \frac{p\overline{p}}{\operatorname{ggT}(p,\overline{p})} = p\overline{p}.$$

Das heißt $\overline{p} = pt$ und ergibt den Widerspruch

$$1 = \operatorname{ggT}(p,\overline{p}) = \operatorname{ggT}(p,pt) = p.$$

Also muß n quadratfrei sein.

Aufgabe 12

BEHAUPTUNG:
$(B, \wedge, \vee, \overline{}, 1, 0)$ ist genau dann eine Boolesche Algebra, wenn (1), (5), (6) und (9) gelten.
BEWEIS:

$\Rightarrow$: Für eine Boolesche Algebra sind die genannten Eigenschaften trivialerweise erfüllt.

$\Leftarrow$: Man hat eine Struktur $\mathcal{B} = (B, \wedge, \vee, \overline{}, 1, 0)$ mit Kommutativität (1), Distributivität (5), 1 und 0 als Neutralelemente (6) und Komplementarität (9).
Um $\mathcal{B}$ als Boolesche Algebra zu zeigen, sind noch Assoziativität und Absorption zu zeigen.
ABSORPTION:
Aus dem Beweis zu Satz 1(11), der nur (5), (6) und (9) benutzt, ergibt sich die Kürzungsregel (11).
Wegen

$$x \wedge x \overset{(6)}{=} (x \wedge x) \vee 0 \overset{(9)}{=} (x \wedge x) \vee (x \wedge \overline{x}) \overset{(5)}{=} x \wedge (x \vee \overline{x}) \overset{(9)}{=} x \wedge 1 \overset{(6)}{=} x$$

und der Dualität steht nun die Idempotenz (3) zur Verfügung.
Die Existenz absorbierender Elemente (7) folgt mit

$$(x \wedge 0) \vee x \overset{(1),(5)}{=} (x \vee x) \wedge (x \vee 0) \overset{(3),(6)}{=} x \wedge x \overset{(3),(6),(1)}{=} 0 \vee x$$

und

$$(x \wedge 0) \vee \overline{x} \overset{(1),(5)}{=} (\overline{x} \vee x) \wedge (\overline{x} \vee 0) \overset{(1),(6)}{=} (x \vee \overline{x}) \wedge \overline{x} \overset{(9),(1)}{=} \overline{x} \wedge 1 \overset{(6),(6),(1)}{=} 0 \vee \overline{x}$$

aus (11) und der Dualität.
Die Absorption (4) ergibt sich nun durch

$$x \wedge (x \vee y) \overset{(6)}{=} (x \vee 0) \wedge (x \vee y) \overset{(5)}{=} x \vee (0 \wedge y) \overset{(1),(7),(6)}{=} x$$

und der Dualität.
ASSOZIATIVITÄT:
Dies folgt nun wie im Beweis zu Satz 1 (2), der nur (1), (4), (5), (6), (9) und (11) benutzt.

Damit ist $\mathcal{B}$ eine Boolesche Algebra.

Aufgabe 13

a) Sei $[a) \rightleftharpoons \{x \in B \mid a \leq x\}$ für $a \in B \setminus \{0\}$.
Nach Definition ist $[a) \subseteq B$ und wegen $a \in [a)$ gilt auch $[a) \neq \emptyset$.
Wegen $0 \leq a$ und $a \neq 0$ hat man $0 \notin [a)$.
Sei nun $x \in [a)$, also $a \leq x$.
Für $y \in [a)$, also $a \leq y$ folgt dann $a \leq \inf\{x, y\} = x \wedge y$, also $x \wedge y \in [a)$.
Für $y \in B$ mit $x \leq y$ ergibt sich $a \leq x \leq y$, $y \in [a)$, da $\leq$ transitiv.
Damit ist gezeigt, daß $[a)$ ein Filter ist.

b) Sei $K = \{X \subseteq \mathbb{N} \mid |\overline{X}| \in \mathbb{N}_0\}$.
Nach Definition ist $K \subseteq B = P(\mathbb{N})$.
Sei $E \rightleftharpoons \mathbb{N} \setminus \{1\}$. Wegen $|\mathbb{N} \setminus E| = |\{1\}| = 1 \in \mathbb{N}_0$ gilt $E \in K$, also $K \neq \emptyset$.
Wegen $|\overline{\emptyset}| = |\mathbb{N}| \notin \mathbb{N}_0$ hat man $\emptyset \notin K$.
Sei $X \in K$, also $|\overline{X}| \in \mathbb{N}_0$.
Für $Y \in K$, also $|\overline{Y}| \in \mathbb{N}_0$ folgt dann

$$|\overline{X \cap Y}| = |\overline{X} \cup \overline{Y}| \leq |\overline{X}| + |\overline{Y}| \in \mathbb{N}_0,$$

d. h. $|\overline{X \cap Y}| \in \mathbb{N}_0$ und daher $X \cap Y \in K$.
Für $Y \in P(\mathbb{N})$ mit $X \subseteq Y$ ergibt sich $\overline{Y} \subseteq \overline{X}$, also $|\overline{Y}| \leq |\overline{X}| \in \mathbb{N}_0$, und somit $|\overline{Y}| \in \mathbb{N}_0$.
Damit ist K ein Filter.

Aufgabe 14

ZU ZEIGEN:

$$A \wedge \overline{B} \prec C,\ A \wedge \overline{B} \prec \overline{C} \Longrightarrow A \prec B$$

BEWEIS:

1	$A \prec A \wedge \top$	(31)
2	$\top \prec \overline{\bot}$	(17)
3	$A \wedge \top \prec A \wedge \overline{\bot}$	(26)
4	$A \prec A \wedge \overline{\bot}$	(15) : 1, 3
5	$A \wedge \overline{B} \prec C$	Vorauss.
6	$A \wedge \overline{B} \prec \overline{C}$	Vorauss.
7	$A \wedge \overline{B} \prec C \wedge \overline{C}$	(19)
8	$C \wedge \overline{C} \prec \bot$	(28)
9	$A \wedge \overline{B} \prec \bot$	(15) : 7, 8

10	$A \wedge \overline{\bot} \prec \overline{\overline{B}}$	(21)
11	$A \prec \overline{\overline{B}}$	$(15):4,10$
12	$\overline{\overline{B}} \prec B$	(16)
13	$A \prec B$	$(15):11,12$

Aufgabe 15

Es symbolisiere

B:	„Benno sagt die Wahrheit“	b:	„Benno hat es getan“
H:	„Hans sagt die Wahrheit“	h:	„Hans hat es getan“
J:	„Jutta sagt die Wahrheit“	j:	„Jutta hat es getan“
O:	„Otto sagt die Wahrheit“	o:	„Otto hat es getan“

Die Aussagen liefern folgende Äquivalenzen:

$$B \prec\!\!\succ h \qquad H \prec\!\!\succ o \qquad J \prec\!\!\succ \overline{j} \qquad O \prec\!\!\succ \overline{H}$$

a) „Genau ein Kind lügt“; es ergibt sich

$$\begin{aligned}
& (B \wedge H \wedge J \wedge \overline{O}) \vee (B \wedge H \wedge \overline{J} \wedge O) \vee (B \wedge \overline{H} \wedge J \wedge O) \vee (\overline{B} \wedge H \wedge J \wedge O) \\
\prec\ & (B \wedge H \wedge J \wedge \overline{\overline{H}}) \vee (B \wedge H \wedge \overline{J} \wedge \overline{H}) \vee (B \wedge \overline{H} \wedge J \wedge \overline{H}) \vee (\overline{B} \wedge H \wedge J \wedge \overline{H}) \\
\prec\ & (B \wedge H \wedge J) \vee \bot \vee (B \wedge \overline{H} \wedge J) \vee \bot \\
\prec\ & (B \wedge J) \wedge (H \vee \overline{H}) \\
\prec\ & B \wedge J \\
\prec\ & h \wedge \overline{j} \\
\prec\ & h,
\end{aligned}$$

also hat Hans es getan.

Sprachlich geht auch: H und O gehen nicht gleichzeitig, d. h. Benno und Jutta sagen die Wahrheit.

b) „Genau ein Kind sagt die Wahrheit“; es ergibt sich

$$\begin{aligned}
& (B \wedge \overline{H} \wedge \overline{J} \wedge \overline{J}) \vee (\overline{B} \wedge H \wedge \overline{J} \wedge \overline{O}) \vee (\overline{B} \wedge \overline{H} \wedge J \wedge \overline{O}) \vee (\overline{B} \wedge \overline{H} \wedge \overline{J} \wedge O) \\
\prec\ & (B \wedge \overline{H} \wedge \overline{J} \wedge H) \vee (\overline{B} \wedge H \wedge \overline{J} \wedge H) \vee (\overline{B} \wedge \overline{H} \wedge J \wedge H) \vee (\overline{B} \wedge \overline{H} \wedge \overline{J} \wedge \overline{H}) \\
\prec\ & \bot \vee (\overline{B} \wedge H \wedge \overline{J}) \vee \bot \vee (\overline{B} \wedge \overline{H} \wedge \overline{J}) \\
\prec\ & (\overline{B} \wedge \overline{J}) \wedge (H \vee \overline{H}) \\
\prec\ & \overline{B} \wedge \overline{J} \\
\prec\ & \overline{h} \wedge j \\
\prec\ & j,
\end{aligned}$$

also hat Jutta es getan.

Aufgabe 16

a) Zu zeigen:

$$A \wedge B \prec C \Longrightarrow A \prec \overline{B} \vee C$$

Beweis:

$$\begin{array}{rcl}
1 & A \prec \overline{\overline{A}} & (16) \\
2 & B \wedge A \prec A \wedge B & (24) \\
3 & A \wedge B \prec C & \text{Vorauss.} \\
4 & B \wedge A \prec C & (15):2,3 \\
5 & B \wedge \overline{C} \prec \overline{A} & (21) \\
6 & \overline{\overline{A}} \prec \overline{B \wedge \overline{C}} & (22) \\
7 & A \prec \overline{B \wedge \overline{C}} & (15):1,6 \\
8 & \overline{B \wedge \overline{C}} \prec \overline{\overline{\overline{B}} \wedge \overline{C}} & \text{Satz31} \\
9 & A \prec \overline{\overline{\overline{B}} \wedge \overline{C}} & (15):7,8 \\
10 & \overline{\overline{\overline{B}} \wedge \overline{C}} \prec \overline{B} \vee C & (36) \\
11 & A \prec \overline{B} \vee C & (15):9,10
\end{array}$$

b) Zu zeigen:

$$A \prec B \vee C \Longrightarrow A \wedge \overline{B} \prec C$$

Beweis:

$$\begin{array}{rcl}
1 & \overline{B} \wedge \overline{C} \prec \overline{\overline{\overline{\overline{B}} \wedge \overline{C}}} & (16) \\
2 & A \wedge \overline{B} \prec \overline{B} \wedge A & (24) \\
3 & A \prec B \vee C & \text{Vorauss.} \\
4 & B \vee C \prec \overline{\overline{B} \wedge \overline{C}} & (36) \\
5 & A \prec \overline{\overline{B} \wedge \overline{C}} & (15):3,4 \\
6 & \overline{\overline{\overline{B} \wedge \overline{C}}} \prec \overline{A} & (22) \\
7 & \overline{B} \wedge \overline{C} \prec \overline{A} & (15):1,6 \\
8 & \overline{B} \wedge \overline{\overline{A}} \prec \overline{\overline{C}} & (21) \\
9 & \overline{B} \wedge A \prec C & \text{Satz31}:8 \\
10 & A \wedge \overline{B} \prec C & (15):2,9
\end{array}$$

Aufgabe 17

Die Aussage a) widerspricht z. B. der Aussage c). Also hat der Professor mit einer falschen Aussage angefangen.
Es folgt nun (mit offensichtlichen Abkürzungen):

a') $\overline{GA \wedge (\overline{SA} \wedge \overline{DE})} = \overline{GA} \vee SA \vee DE$
b) $\overline{LA} \vee \overline{GU}$
c') $\overline{LA \wedge DE \wedge \overline{GU}} = \overline{LA} \vee \overline{DE} \vee GU$
d) $DE \to PL = \overline{DE} \vee PL$
e') $\overline{\overline{GU} \wedge SA} = GU \vee \overline{SA}$
f) $\overline{LA} \to \overline{PL} \wedge GA = LA \vee (\overline{PL} \wedge GA)$
g') $\overline{\overline{GA} \wedge \overline{DE}} = GA \vee DE$

Alle diese Aussagen müssen wahr sein.
Einsetzen von Wahrheitswerten liefert:

$LA = \top$: b)$GU = \bot$
c')$DE = \bot$
e') $SA = \bot$
g')$GA = \top$
a') $DE = \top$ Widerspruch

$LA = \bot$: f)$PL = \bot$, $GA = \top$
d)$DE = \bot$
a')$SA = \top$
e')$GU = \top$
b) $\top$
c') $\top$

Also $LA = PL = DE = \bot$ und $GA = SA = GU = \top$.

Aufgabe 18

a) Umformung in vollständige adjunktive Normalform:

$$
\begin{aligned}
& (\overline{A} \vee C) \wedge (\overline{B} \vee C) \wedge \overline{A \vee B \to C} \\
\dashv\vdash\ & ((\overline{A} \wedge \overline{B}) \vee (C \wedge \overline{B}) \vee (\overline{A} \wedge C) \vee (C \wedge C)) \wedge ((A \vee B) \wedge \overline{C}) \\
\dashv\vdash\ & ((\overline{A} \wedge \overline{B}) \vee (C \wedge \overline{B}) \vee (\overline{A} \wedge C) \vee C) \wedge ((A \wedge \overline{C}) \vee (B \wedge \overline{C})) \\
\dashv\vdash\ & (\overline{A} \wedge \overline{B} \wedge A \wedge \overline{C}) \vee (C \wedge \overline{B} \wedge A \wedge \overline{C}) \vee (\overline{A} \wedge C \wedge A \wedge \overline{C}) \vee (C \wedge A \wedge \overline{C}) \\
& \vee (\overline{A} \wedge \overline{B} \wedge B \wedge \overline{C}) \vee (C \wedge \overline{B} \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge C \wedge B \wedge \overline{C}) \vee (C \wedge B \wedge \overline{C}) \\
\dashv\vdash\ & \bot
\end{aligned}
$$

b) Umformung in vollständige adjunktive Normalform:

$$(A \to B) \to ((B \to C) \to (A \to C))$$

$$
\begin{array}{ll}
\mathrel{-\!\!\ast\!\!-} & (\overline{A} \vee B) \rightarrow ((\overline{B} \vee C) \rightarrow (\overline{A} \vee C)) \\
\mathrel{-\!\!\ast\!\!-} & \overline{\overline{A} \vee B} \vee (\overline{\overline{B} \vee C} \vee (\overline{A} \vee C)) \\
\mathrel{-\!\!\ast\!\!-} & (A \wedge \overline{B}) \vee (B \wedge \overline{C}) \vee \overline{A} \vee C
\end{array}
$$

1. Variante: Es treten in jeder Konjunktion Glieder $X \vee \overline{X}$ auf, also $\mathrel{-\!\!\ast\!\!-} \top$

$$
\begin{array}{ll}
\mathrel{-\!\!\ast\!\!-} & (A \wedge \overline{B} \wedge C) \vee (A \wedge \overline{B} \wedge \overline{C}) \vee (B \wedge \overline{C} \wedge A) \vee (B \wedge \overline{C} \wedge \overline{A}) \\
& \vee(\overline{A} \wedge B \wedge C) \vee (\overline{A} \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge \overline{B} \wedge C) \vee (\overline{A} \wedge \overline{B} \wedge \overline{C}) \\
& \vee(C \wedge A \wedge B) \vee (C \wedge A \wedge \overline{B}) \vee (C \wedge \overline{A} \wedge B) \vee (C \wedge \overline{A} \wedge \overline{B}) \\
\mathrel{-\!\!\ast\!\!-} & (A \wedge B \wedge C) \vee (A \wedge B \wedge \overline{C}) \vee (A \wedge \overline{B} \wedge C) \vee (A \wedge \overline{B} \wedge \overline{C}) \\
& \vee(\overline{A} \wedge B \wedge C) \vee (\overline{A} \wedge B \wedge \overline{C}) \vee (\overline{A} \wedge \overline{B} \wedge C) \vee (\overline{A} \wedge \overline{B} \wedge \overline{C})
\end{array}
$$

2. Variante: Alle möglichen Kombinationsmöglichkeiten sind vorhanden, also $\mathrel{-\!\!\ast\!\!-} \top$

3. Variante: Verfahren nach Quine-McCluskey:

$$
\begin{array}{llcllcl}
ABC & \checkmark & & AB & \checkmark & & A \\
AB\overline{C} & \checkmark & & AC & \checkmark & & B \\
A\overline{B}C & \checkmark & & BC & \checkmark & \Longrightarrow & C \\
A\overline{B}\,\overline{C} & \checkmark & & A\overline{C} & \checkmark & & \overline{A} \\
\overline{A}BC & \checkmark & \Longrightarrow & B\overline{C} & \checkmark & & \overline{B} \\
\overline{A}B\overline{C} & \checkmark & & \overline{B}C & \checkmark & & \overline{C} \\
\overline{A}\,\overline{B}C & \checkmark & & A\overline{B} & \checkmark & & \\
\overline{A}\,\overline{B}\,\overline{C} & \checkmark & & \overline{B}\,\overline{C} & \checkmark & & \\
 & & & \overline{A}B & \checkmark & & \\
 & & & \overline{A}C & \checkmark & & \\
 & & & \overline{A}\,\overline{C} & \checkmark & & \\
 & & & \overline{A}\,\overline{B} & \checkmark & &
\end{array}
$$

$$
\begin{array}{ll}
\mathrel{-\!\!\ast\!\!-} & A \vee B \vee C \vee \overline{A} \vee \overline{B} \vee \overline{C} \\
\mathrel{-\!\!\ast\!\!-} & \top
\end{array}
$$

Aufgabe 19

$$
\begin{array}{ll}
& (\overline{A} \wedge \overline{B}) \vee ((A \vee B \vee C) \wedge (A \vee B \vee \overline{C})) \vee (A \wedge B \wedge C \wedge D) \\
\mathrel{-\!\!\ast\!\!-} & (\overline{A} \wedge \overline{B}) \vee A \vee (A \wedge B) \vee (A \wedge \overline{C}) \vee (A \wedge B) \vee B \\
& \vee(B \wedge \overline{C}) \vee (A \wedge C) \vee (B \wedge C) \vee (C \wedge \overline{C}) \vee (A \wedge B \wedge C \wedge D) \\
\mathrel{-\!\!\ast\!\!-} & \ldots
\end{array}
$$

Es treten alle möglichen Kombinationsmöglichkeiten auf (siehe Aufgabe 18b)), also $\mathrel{-\!\!\ast\!\!-} \top$.

Aufgabe 20

$$
\begin{array}{ll}
 & f \text{ ist nicht monoton} \\
\Leftrightarrow & \neg(f \text{ ist monoton}) \\
\Leftrightarrow & \neg(f \text{ ist monoton wachsend oder monoton fallend}) \\
\Leftrightarrow & \neg\Big((\forall x, y \in \mathbb{R}:\ x < y \Rightarrow f(x) \leq f(y)) \vee (\forall x, y \in \mathbb{R}:\ x < y \Rightarrow f(x) \geq f(y))\Big) \\
\Leftrightarrow & \neg\Big(\forall x, y \in \mathbb{R}:\ x < y \Rightarrow f(x) \leq f(y)\Big) \wedge \neg\Big(\forall x, y \in \mathbb{R}:\ x < y \Rightarrow f(x) \geq f(y)\Big) \\
\Leftrightarrow & \Big(\exists x, y \in \mathbb{R}:\ \neg(x < y \Rightarrow f(x) \leq f(y))\Big) \wedge \Big(\exists x, y \in \mathbb{R}:\ \neg(x < y \Rightarrow f(x) \geq f(y))\Big) \\
\Leftrightarrow & \Big(\exists x, y \in \mathbb{R}:\ \neg(\overline{x < y} \vee f(x) \leq f(y))\Big) \wedge \Big(\exists x, y \in \mathbb{R}:\ \neg(\overline{x < y} \vee f(x) \geq f(y))\Big) \\
\Leftrightarrow & \Big(\exists x, y \in \mathbb{R}:\ x < y \wedge \overline{f(x) \leq f(y)}\Big) \wedge \Big(\exists x, y \in \mathbb{R}:\ x < y \wedge \overline{f(x) \geq f(y)}\Big) \\
\Leftrightarrow & \Big(\exists x, y \in \mathbb{R}:\ x < y \wedge f(x) > f(y)\Big) \wedge \Big(\exists x, y \in \mathbb{R}:\ x < y \wedge f(x) < f(y)\Big)
\end{array}
$$

Aufgabe 21

a)

$$
\begin{array}{llclllcll}
ABCD & \checkmark & & ABC & \checkmark & & AB & \checkmark & \Longrightarrow \quad A \quad * \\
ABC\overline{D} & \checkmark & & ABD & \checkmark & & AC & \checkmark & \\
AB\overline{C}D & \checkmark & & ACD & \checkmark & & AD & \checkmark & \\
AB\overline{CD} & \checkmark & & AB\overline{D} & \checkmark & \Longrightarrow & A\overline{D} & \checkmark & \\
A\overline{B}CD & \checkmark & & AC\overline{D} & \checkmark & & C\overline{D} & * & \\
A\overline{B}C\overline{D} & \checkmark & & BC\overline{D} & \checkmark & & A\overline{C} & \checkmark & \\
A\overline{BC}D & \checkmark & & AB\overline{C} & \checkmark & & A\overline{B} & \checkmark & \\
A\overline{BCD} & \checkmark & \Longrightarrow & A\overline{C}D & \checkmark & & & & \\
\overline{A}BC\overline{D} & \checkmark & & A\overline{CD} & \checkmark & & & & \\
\overline{AB}C\overline{D} & \checkmark & & A\overline{B}C & \checkmark & & & & \\
\overline{ABC}D & \checkmark & & A\overline{B}D & \checkmark & & & & \\
 & & & A\overline{BD} & \checkmark & & & & \\
 & & & \overline{B}C\overline{D} & \checkmark & & & & \\
 & & & A\overline{BC} & \checkmark & & & & \\
 & & & \overline{BC}D & * & & & & \\
 & & & \overline{A}C\overline{D} & \checkmark & & & &
\end{array}
$$

Also: $\ldots \Leftrightarrow A \vee (C \wedge \overline{D}) \vee (\overline{B} \wedge \overline{C} \wedge D)$

b)

$$
\begin{array}{ll}
 & A \vee C \rightarrow ((A \wedge \overline{B}) \vee \overline{C} \rightarrow B \wedge \overline{C}) \\
\Leftrightarrow & \overline{A \vee C} \vee (\overline{(A \wedge B) \vee \overline{C}} \vee (B \wedge \overline{C})) \\
\Leftrightarrow & (\overline{A} \wedge \overline{C}) \vee (\overline{A \wedge \overline{B}} \wedge C) \vee (B \wedge \overline{C}) \\
\Leftrightarrow & (\overline{A} \wedge \overline{C}) \vee ((\overline{A} \vee B) \wedge C) \vee (B \wedge \overline{C})
\end{array}
$$

$$
\begin{aligned}
&\dashv\vdash \quad (\overline{A} \wedge (C \vee \overline{C})) \vee (B \wedge (C \wedge \overline{C}))\\
&\dashv\vdash \quad \overline{A} \vee B
\end{aligned}
$$

Oder nach Quine-McCluskey:

$$\dashv\vdash \quad (\overline{A} \wedge \overline{C}) \vee (\overline{A} \wedge C) \vee (B \wedge C) \vee (B \wedge \overline{C})$$

$$
\begin{array}{llcllcll}
ABC & \checkmark & & AB & \checkmark & \Longrightarrow & \overline{A} & * \\
AB\overline{C} & \checkmark & & BC & \checkmark & & B & * \\
\overline{A}BC & \checkmark & & B\overline{C} & \checkmark & & & \\
\overline{A}B\overline{C} & \checkmark & \Longrightarrow & \overline{A}B & \checkmark & & & \\
\overline{AB}C & \checkmark & & \overline{A}C & \checkmark & & & \\
\overline{ABC} & \checkmark & & \overline{AC} & \checkmark & & & \\
 & & & \overline{AB} & \checkmark & & &
\end{array}
$$

$$\dashv\vdash \quad \overline{A} \vee B$$

Aufgabe 22

Zu zeigen:
$\alpha \to \beta$ ist genau dann allgemeingültig, wenn β aus α folgt.
Beweis:

$$
\begin{aligned}
& \beta \text{ folgt aus } \alpha\\
\overset{\text{Def.32}\gamma)}{\Longleftrightarrow} \quad & \{\alpha\} \Vdash \beta \Longleftrightarrow \emptyset \cup \{\alpha\} \Vdash \beta\\
\overset{\text{Satz51g)}}{\Longleftrightarrow} \quad & \emptyset \Vdash (\alpha \to \beta)\\
\overset{\text{Satz51a)}}{\Longleftrightarrow} \quad & \Vdash (\alpha \to \beta)\\
\overset{\text{Def.32}\beta)}{\Longleftrightarrow} \quad & \alpha \to \beta \text{ ist allgemeingültig.}
\end{aligned}
$$

Aufgabe 23

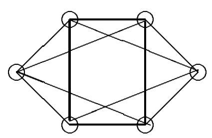
Zu zeigen:
Wenn $\mathcal{M} \cup \{\exists\xi\alpha\}$ bei i gilt, so gilt auch β bei i.
Beweis:
Annahme: $\mathcal{M} \cup \{\exists\xi\alpha\}$ gilt bei i.
Nach Definition 32α) gilt dann insbesondere $\exists\xi\alpha$ bei i.
Mit Satz 50b) folgt: Es gibt ein j mit $i \overset{\xi}{=} j$, bei dem α gilt.
ξ kommt in $\mathcal{M}$ nicht frei vor, nach Definition 33β) also in keinem Element von $\mathcal{M}$.
Da weiterhin $i \overset{\xi}{=} j$ und $\mathcal{M}$ nach Annahme bei i gilt, gilt $\mathcal{M}$ nach Satz 52 auch bei j.
Wegen $\mathcal{M} \cup \{\alpha\} \Vdash \beta$ bedeutet dies nach Definition 32γ): β gilt bei j.
Da ξ nunmehr in β nicht frei vorkommt und $i \overset{\xi}{=} j$ folgt nach Satz 52: β gilt bei i.

Aufgabe 24

a) $n = 4$; Grade: 0, 1, 2, 3
Nein, denn nach Satz 58 muß ein endlicher schlichter Graph mit mindestens 2 Ecken mindestens 2 Ecken gleichen Grades haben.

b) $n = 7$; Grade: 1, 2, 2, 3, 4, 5, 6
Nein, denn nach Korollar B zu Satz 59 muß ein Graph mit endlich vielen Kanten eine gerade Anzahl von Ecken ungeraden Grades haben.

c) $n = 6$; Grade: 4, 4, 4, 4, 4, 4



d) $n = 6$; Grade: 1, 1, 2, 3, 4, 5
Nein: Gäbe es einen schlichten Graphen $\mathcal{G}$ mit $\mathcal{E} = \{A, B, C, D, E, F\}$ und $|\mathcal{E}| = 6$ sowie $\gamma(A) = 5$, $\gamma(B) = 4$, $\gamma(C) = 3$, $\gamma(D) = 2$, $\gamma(E) = 1$, $\gamma(F) = 1$, so wäre $A \sim B, C, D, E, F$ und $B \sim A, C, D, E$ oder $B \sim A, C, D, F$.
Dies widerspricht $\gamma(E) = 1$ bzw. $\gamma(F) = 1$.

Aufgabe 25

$\Rightarrow$: Sei $\mathcal{G}$ kubischer Graph der Ordnung n.
Dann ist n nach Korollar C zu Satz 59 gerade.
Wegen $n \in \mathbb{N}$ gibt es in $\mathcal{G}$ mindestens eine Ecke X. Sie muß wegen $\gamma(X) = 3$ mit 3 weiteren Ecken verbunden sein, was $n \geq 4$ bedingt.

$\Leftarrow$: Sei $n \in 2\mathbb{N}$, etwa $n = 2m$ und $n \geq 4$, also $m \geq 2$.
Induktion nach m:

IA: Für $m = 2$ hat man mit K_4 einen kubischen Graphen.

IS: Sei $\mathcal{G} = (\mathcal{E}, \mathcal{K}, \varphi)$ ein kubischer Graph der Ordnung $2m$ mit $m \geq 2$.
Man konstruiert einen kubischen Graphen $\mathcal{G}' = (\mathcal{E}', \mathcal{K}', \varphi')$ der Ordnung $2(m+1)$ wie folgt:

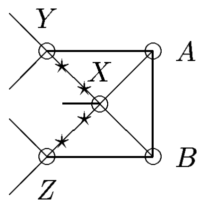
$$\mathcal{E}' :\Leftrightarrow \mathcal{E} \cup \{A, B\} \text{ mit } A, B \notin \mathcal{E} \text{ und } A \neq B.$$

Dann ist $|\mathcal{E}'| = 2m + 2 = 2(m+1)$.
Da $\mathcal{G}$ kubisch ist, gibt es $X, Y \in \mathcal{E}$ mit $X \sim Y$ und $X \neq Y$
und es gibt $Z \in \mathcal{E} \setminus \{X, Y\}$ mit $Z \sim X$.

$$\mathcal{K}' :\Leftrightarrow \Big(\mathcal{K} \setminus \Big\{\{X,Y\}, \{X,Z\}\Big\}\Big) \cup \Big\{\{A,B\}, \{A,X\}, \{A,Z\}, \{B,X\}, \{B,Y\}\Big\},$$

$$\varphi' :\Leftrightarrow 1_{\mathcal{K}'}.$$

Skizze:



Offenbar ist $\gamma(A) = \gamma(B) = 3$ und $\gamma(X) = \gamma(Y) = \gamma(Z) = 3$.
Alle anderen Ecken blieben unverändert, also ist $\mathcal{G}'$ ein kubischer Graph der Ordnung $2(m+1)$.

Aufgabe 26

a) $\mathcal{G}$ sei Graph. Dann gilt für $\mu \in \mathbb{A}_n$

$$\begin{aligned}\sum_{\nu=1}^{n} a_{\mu\nu} &= a_{\mu\mu} + \sum_{\substack{\nu = 1 \\ \nu \neq \mu}}^{n} a_{\mu\nu} \\ &= 2|\varsigma(E_\mu)| + \sum_{\substack{\nu = 1 \\ \nu \neq \mu}}^{n} |\tilde{E_\mu} \cap \tilde{E_\nu}| \\ &= |\varsigma(E_\mu)| + |\tilde{E_\mu}| \\ &= \gamma(E_\mu)\end{aligned}$$

und für $\nu \in \mathbb{A}_n$ nach Satz 60a)

$$\sum_{\mu=1}^{n} a_{\mu\nu} = \sum_{\mu=1}^{n} a_{\nu\mu} = \gamma(E_\nu).$$

b) $\mathcal{G}$ sei Digraph. Für $\mu \in \mathbb{A}_n$ ergibt sich mit $\mathcal{E} = \varepsilon(\mathcal{G})$

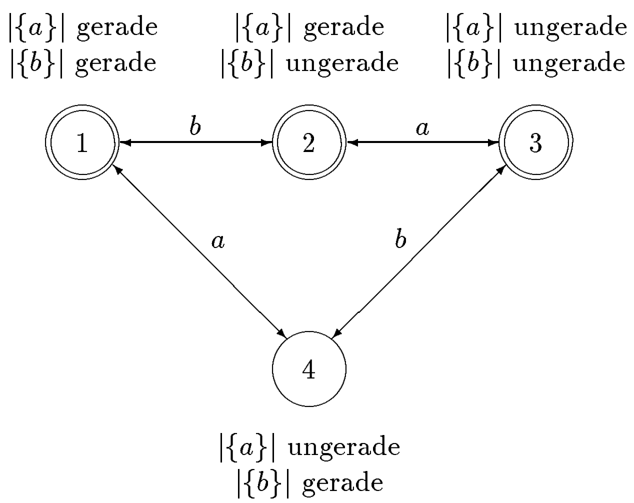
$$\begin{aligned}\sum_{\nu=1}^{n} a_{\mu\nu} &= \sum_{\nu=1}^{n} |\{k \in \mathcal{K} \mid \varphi(k) = (E_\mu, E_\nu)\}| \\ &= |\bigcup_{\nu=1}^{n} \{k \in \mathcal{K} \mid \varphi(k) = (E_\mu, E_\nu)\}| \\ &= |\{k \in \mathcal{K} \mid \exists X \in \mathcal{E} :\ \varphi(k) = (E_\mu, X)\}| \\ &= \gamma^+(E_\mu)\end{aligned}$$

und analog für $\nu \in \mathbb{A}_n$

$$\begin{aligned}\sum_{\mu=1}^{n} a_{\mu\nu} &= \sum_{\mu=1}^{n} |\{k \in \mathcal{K} \mid \varphi(k) = (E_\mu, E_\nu)\}| \\ &= |\bigcup_{\mu=1}^{n} \{k \in \mathcal{K} \mid \varphi(k) = (E_\mu, E_\nu)\}| \\ &= |\{k \in \mathcal{K} \mid \exists X \in \mathcal{E} :\ \varphi(k) = (X, E_\nu)\}| \\ &= \gamma^-(E_\nu).\end{aligned}$$

Aufgabe 27

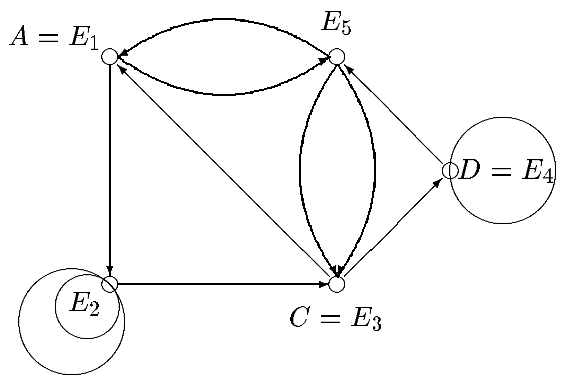
Das gesuchte Transitionsdiagramm könnte so aussehen:



1 ist dabei der Startzustand.

Aufgabe 28

a) Bei der Eckennumerierung



ergibt sich gemäß Definition 42γIIb) die Adjazenzmatrix

$$M \rightleftharpoons \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 2 & 0 & 0 \end{pmatrix}$$

b) I. Mit $\left(m_{\mu\nu}^{(\lambda)}\right)_{\mu,\nu=1,\dots,5} \rightleftharpoons M^{\lambda}$ für $\lambda \in \mathbb{N}$

hat man für die Zahl der Kantenzüge der Länge 4 von $C = E_3$ nach $A = E_1$ Satz

61 zufolge den Wert $m_{3,1}^{(4)}$ zu bestimmen. Dazu reicht es offenbar, die 3. Zeile und 1. Spalte von M^2 zu berechnen. Mit

$$\begin{aligned}
(1,0,0,1,0)\cdot(0,0,1,0,1) &= 0\\
(1,0,0,1,0)\cdot(1,2,0,0,0) &= 1\\
(1,0,0,1,0)\cdot(0,1,0,0,2) &= 0\\
(1,0,0,1,0)\cdot(0,0,1,1,0) &= 1\\
(1,0,0,1,0)\cdot(1,0,0,1,0) &= 2
\end{aligned}$$

und

$$\begin{aligned}
(0,1,0,0,1)\cdot(0,0,1,0,1) &= 1\\
(0,2,1,0,0)\cdot(0,0,1,0,1) &= 1\\
(1,0,0,1,0)\cdot(0,0,1,0,1) &= 0\\
(0,0,0,1,1)\cdot(0,0,1,0,1) &= 1\\
(1,0,2,0,0)\cdot(0,0,1,0,1) &= 2
\end{aligned}$$

erhält man $m_{3,1}^{(4)} = (0,1,0,1,2)\cdot(1,1,0,1,2) = 6$.

II. Analog zu I. ist $m_{1,4}^{(8)}$ zu berechnen und dazu die 1. Zeile und 4. Spalte von M^4, was ganz M^2 erfordert, also

$$M^2 = \begin{pmatrix} 1 & 2 & 3 & 0 & 0\\ 1 & 4 & 2 & 1 & 0\\ 0 & 1 & 0 & 1 & 2\\ 1 & 0 & 2 & 1 & 1\\ 2 & 1 & 0 & 2 & 1 \end{pmatrix}, \qquad M^4 = \begin{pmatrix} 3 & 13 & 7 & 5 & 6\\ \cdot & \cdot & \cdot & 7 & \cdot\\ \cdot & \cdot & \cdot & 6 & \cdot\\ \cdot & \cdot & \cdot & 5 & \cdot\\ \cdot & \cdot & \cdot & 5 & \cdot \end{pmatrix}$$

und damit $m_{4,1}^{(8)} = (3,13,7,5,6)\cdot(5,7,6,5,5) = 203$.

Aufgabe 29

$\mathcal{T}$ sei ein Turnier mit $n \in \mathbb{N}\setminus\{1\}$ Teilnehmern, nach Beispiel 38b) also ein gerichteter Graph $\mathcal{T} = (\mathcal{E}, \mathcal{K}, \varphi)$ mit

$$|\mathcal{E}| = n, \quad \mathcal{K} \subseteq \mathcal{E}\times\mathcal{E}, \quad \varphi \rightleftharpoons 1_{\mathcal{K}}$$

und

$$(*) \quad \forall X, Y \in \mathcal{E}:\ X \neq Y \Longrightarrow |\{(X,Y),(Y,X)\}\cap\mathcal{K}| = 1.$$

BEHAUPTUNG:
In $\mathcal{T}$ gibt es einen gerichteten Weg, der $\mathcal{E}$ enthält.
BEWEIS:
Wir beginnen mit einem beliebigen, wegen $n \geq 2$ und $(*)$ existenten Pfeil $(A,B) \in \mathcal{K}$ und zeigen:
Ist $(A_1,\ldots,A_k)$ ein Weg der Länge $k-1$ mit $\lambda \leq k < n$ in $\mathcal{T}$, kann er zu einem Weg der

Länge k in $\mathcal{T}$ verlängert werden.
Sei also $X \in \mathcal{E} \setminus \{A_\kappa \mid \kappa \in \mathbb{A}_k\}$.
Im Falle $(X, A_1) \in \mathcal{K}$ bilden wir den Weg $(X, A_1, \ldots, A_k)$.
Sei also $(X, A_1) \notin \mathcal{K}$.
Wegen $(*)$ ist dann $(A_1, X) \in \mathcal{K}$, und es sei

$$m \rightleftharpoons \max\{\kappa \in \mathbb{A}_k \mid \forall\lambda \in \mathbb{A}_\kappa : \ (A_\lambda, X) \in \mathcal{K}\},$$

also speziell

$$(**) \quad (A_m, X) \in \mathcal{K}.$$

Im Falle $m = k$ bilden wir daher den Weg $(A_1, \ldots, A_k, X)$.
Sei also $m < k$, dann ist $(X, A_{m+1}) \in \mathcal{K}$, denn sonst wäre $(*)$ zufolge $(A_{m+1}, X) \in \mathcal{K}$ im Widerspruch zur Maximalität von m, und wir können wegen $(**)$ den Weg

$$(A_1, \ldots, A_m, X, A_{m+1}, \ldots, A_k)$$

bilden, womit die Behauptung induktiv bewiesen ist.

Aufgabe 30

Die drei Rechnernetze können als die 3 Komponenten eines endlichen schlichten Graphen der Kantenzahl $n = 600$ aufgefaßt werden. Für die erfragte Minimalzahl m muß also Satz 63 zufolge gelten

$$m \rightleftharpoons \min\left\{\mu \in \mathbb{N} \mid n \leq \binom{\mu - 3 + 1}{2}\right\}$$

und

$$(*) \quad m - 3 \leq n.$$

Aus

$$n \leq \binom{\mu - 2}{2} = \frac{(\mu-2)(\mu-3)}{2}$$

folgt

$$\mu^2 - 5\mu + 6 - 2n \geq 0$$

und weiter

$$\mu \geq \frac{1}{2}\left(5 + \sqrt{D}\right)$$

mit

$$D \rightleftharpoons 25 - 4(6 - 2n) = 8n + 1 = 4801,$$

wegen

$$69^2 = 4671 < 4801 < 4900 = 70^2$$

also

$$\mu \geq \frac{1}{2}(5 + 69, \ldots) > \frac{74}{2} = 37,$$

was $m = 38$ bedingt und auch $(*)$ genügt.

Aufgabe 31

a) Da $\mathcal{G}$ schlicht ist, gibt es zu jedem $A \in \mathcal{E}$ mit $\gamma(A) = m$ genau $n-1-m$ Ecken, die nicht mit A verbunden sind. A hat also in $\overline{\mathcal{G}}$ den Grad $n-1-m$. Wegen $\mathcal{G} \simeq \overline{\mathcal{G}}$ existiert folglich in $\mathcal{G}$ eine Ecke B mit $\gamma(B) = n-1-m$.

b) Sei $n > 1$ und es gebe in $\mathcal{G}$ eine Ecke E mit $\gamma(E) = 0$. Nach a) existiert dann $F \in \mathcal{E}$ mit $\gamma(F) = n-1$. Da F mit jeder anderen Ecke verbunden ist und wegen $n > 1$ jedoch $E \neq F$ gilt, folgt ein Widerspruch zu $\gamma(E) = 0$, also zur Annahme.
Der Fall $\gamma(E) = 1$ ist analog zu einem Widerspruch zu führen.

c) Mit $\overline{k} \rightleftharpoons |\overline{\mathcal{K}}|$ hat man wegen $\mathcal{K} \cap \overline{\mathcal{K}} = \emptyset$

$$k + \overline{k} = |\mathcal{K}| + |\overline{\mathcal{K}}| = |\mathcal{K} \cup \overline{\mathcal{K}}| = |P_2(\mathcal{E})| = \binom{n}{2}.$$

Wegen $\mathcal{G} \simeq \overline{\mathcal{G}}$ hat man zudem $k = \overline{k}$ und somit

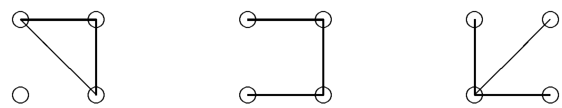
$$2k = \binom{n}{2}, \text{ also } k = \frac{1}{2}\frac{n(n-1)}{2} = \frac{n}{4}(n-1).$$

d) Nach c) hat man $n(n-1) = 4k$.
Für gerades n ist $(n-1)$ ungerade und man hat $4|n$.
Für ungerades n ist $(n-1)$ gerade und man hat $4|(n-1)$.
Insgesamt folgt also $n \equiv_4 0, 1$.

e) Der leere Graph ist selbstkomplementär.
Sei $\mathcal{G} = (\mathcal{E}, \mathcal{K})$ ein selbstkomplementärer Graph der Ordnung $n \in \mathbb{A}_7$ und k seine Kantenzahl.
Nach d) folgt $n \in \{1, 4, 5\}$. Sei

$n = 1$: Nach c) erhält man $k = 0$, also $\mathcal{G} \in N_1$, und $\mathcal{G}$ ist in der Tat selbstkomplementär.

$n = 4$: Mit c) folgt $k = 3$.
Für einen schlichten Graphen der Ordnung 4 mit 3 Kanten existieren genau die folgenden nichtisomorphen Möglichkeiten:



1 2 3

Wegen b) scheiden 1 und 3 aus. 2 ist selbstkomplementär.

$n = 5$: c) liefert $k = 5$.
Satz 59 ergibt $\sum \gamma(E) = 2k = 10$, was unter Berücksichtigung von b), also von $\forall E \in \mathcal{E}: \ 1 \leq \gamma(E) \leq 3$ auf folgende Gradfolgen führt:

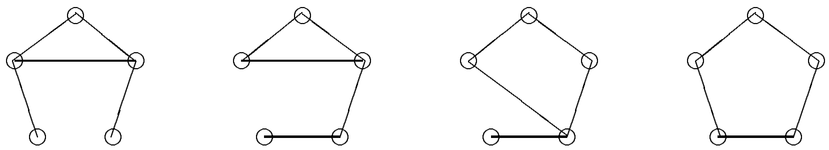
$(1, 1, 2, 3, 3)$
$(1, 2, 2, 2, 3)$
$(2, 2, 2, 2, 2)$.

Die zugehörigen Gradfolgen in $\overline{\mathcal{G}}$ ergeben sich zu

$$\begin{array}{l}(3,3,2,1,1)\\(3,2,2,2,1)\\(2,2,2,2,2).\end{array}$$

Sie stimmen also nach Umordnen mit den ursprünglichen überein.
Es ergeben sich bis auf Isomorphie folgende mögliche Graphen:

$(1,1,2,3,3)$ $(1,2,2,2,3)$ $(2,2,2,2,2)$



1 2 3 4

1 und 4 sind dabei selbstkomplementär, 2 und 3 jedoch nicht.

Aufgabe 32

Die Situation kann durch einen schlichten Graphen $\mathcal{G} = (\mathcal{E}, \mathcal{K})$ der Ordnung $n \in \mathbb{N} \setminus \mathbb{A}_2$ modelliert werden.
Die Menge der Personen wird durch $\mathcal{E}$ dargestellt und $A \in \mathcal{E}$ mit $B \in \mathcal{E}$ genau dann verbunden, falls sie miteinander bekannt sind.
Die gestellte Frage ist die nach der Existenz eines Hamiltonschen Kreises in $\mathcal{G}$.
Es sind alle Voraussetzungen von Satz 68 erfüllt und es gilt

$$\Big(\forall A, B \in \mathcal{E} : \; A \not\sim B \Rightarrow \gamma(A) + \gamma(B) \geq n\Big) \Longrightarrow \; \mathcal{G} \text{ ist Hamiltonscher Graph.}$$

Die geforderte Plazierung ist also möglich.

Aufgabe 33

Beweis mittels Induktion nach n, wobei von n auf $n+2$ geschlossen wird.

IA: $n = 1 : \; k = 0 \leq \left\lfloor \frac{1^2}{4} \right\rfloor$

$n = 2 : \; k \leq 1 = \left\lfloor \frac{2^2}{4} \right\rfloor$

IS: Sei $n \in \mathbb{N}$ und die Behauptung für alle schlichten Graphen der Ordnung $\leq n$ bewiesen.
Sei $\mathcal{G}$ ein dreiecksloser schlichter Graph der Ordnung $n+2$, oBdA. $\mathcal{G} \notin N_{n+2}$.
Dann existiert $A, B \in \varepsilon(\mathcal{G})$ mit $A \neq B$ und $A \sim B$.
Der Graph $\mathcal{H}$, der durch Entfernen von A und B samt adjazenter Kanten aus $\mathcal{G}$ entsteht, hat die Ordnung n und ist ebenfalls dreieckslos. Es folgt

$$(*) \quad |\kappa(\mathcal{H})| \leq \left\lfloor \frac{n^2}{4} \right\rfloor \text{ nach Induktionsvoraussetzung.}$$

Es existiert kein $C \in \varepsilon(\mathcal{H})$ mit $A \sim C \sim B$ in $\mathcal{G}$, da $\mathcal{G}$ dreieckslos.
Ist somit A mit genau m Ecken von $\mathcal{H}$ verbunden, so B mit höchstens $n - m$ Ecken.
Wegen $(*)$ gilt

$$k \leq \left\lfloor \frac{n^2}{4} \right\rfloor + m + n - m + 1 \leq \frac{n^2}{4} + n + 1 = \frac{n^2 + 4n + 4}{4} = \frac{(n+2)^2}{4}.$$

Aufgabe 34

a) Der folgende Algorithmus wandelt eine in Suffixnotation gegebene Formel F in eine äquivalente Formel G in Infixnotation um. Dabei sei F als Zeichenkette gegeben, und jedes Zeichen von F erkennbar als Variable oder Konstante (kurz als Atom) oder als binärer Operator. Andere Zeuichen sollen nicht vorkommen.

   A) Man erzeuge aus F einen Kantorowitschbaum B, indem man F wie auf Seite 175 von rechts nach links abarbeitet, wobei z das jeweilige Zeichen sei.

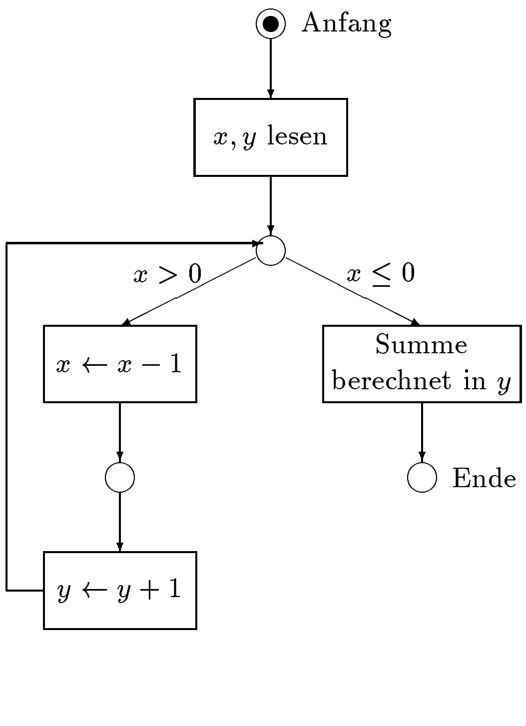
   B) Man durchwandere den Baum B mit der Wurzel W nach dem Algorithmus auf Seite 176 (linker Teilbaum, Wurzel, rechter Teilbaum), wobei E die jeweils aktuelle Ecke sei.

b) Man erhält einen Kantorowitschbaum wie auf Seite 176 und damit

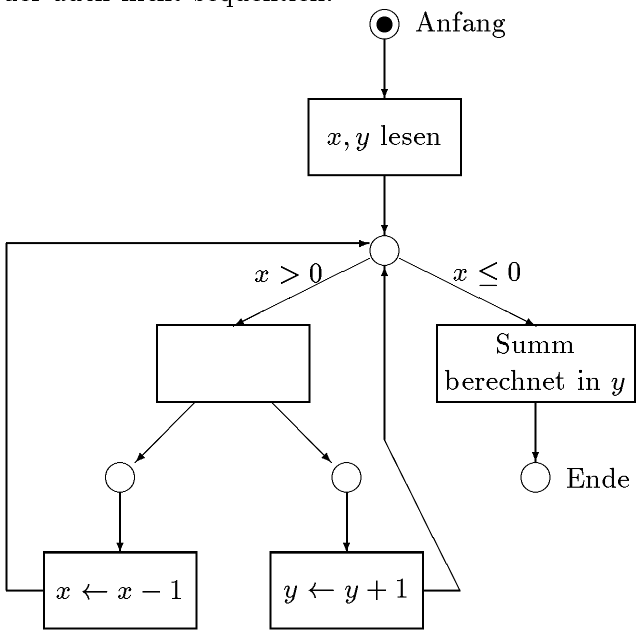
$$ab + 3c \cdot 4a + \cdot - 5ab - \cdot 2dd \cdot \cdot - /.$$

Aufgabe 35

Üblichr Flußdiagramme können unmittelbar in Petrinetze umgesetzt werden, wobei im weiteren Anweisungen als Ereignisse und mögliche Programmzustände als Zustände aufgefaßt werden:



oder auch nicht sequentiell:



Aufgabe 36

a) Mit

$$b_\nu \rightleftharpoons \sum_{\lambda=0}^{\nu-1} \binom{\nu}{\lambda} 11^{\nu-1-\lambda}(-1)^\lambda \text{ für } \nu \in \mathbb{N}$$

hat man

$$\begin{aligned} 10^\nu &= (11-1)^\nu = \sum_{\lambda=0}^{\nu} 11^{\nu-\lambda}(-1)^\lambda \\ &= 11b_\nu + (-1)^\nu \end{aligned}$$

und mit

$$c_\nu \rightleftharpoons \sum_{\nu=1}^{n} a_\nu b_\nu \in \mathbb{N}_0$$

daher

$$\begin{aligned} a &= \sum_{\nu=0}^{n} a_\nu 10^\nu = \sum_{\nu=1}^{n} a_\nu (11b_\nu + (-1)^\nu) + a_0 \\ &= 11\sum_{\nu=1}^{n} a_\nu b_\nu + (-1)^{\lambda n} \sum_{\nu=0}^{n}((-1)^\nu a_\nu (-1)^{-\lambda\nu}) \\ &= 11c + (-1)^n \sum_{\nu=0}^{n} (-1)^{n-\nu} a_\nu \\ &= 11c + (-1)^n W(a), \end{aligned}$$

gilt also $11|a$, so auch $11|W(a)$ und umgekehrt.

b) Für

$$a = \sum_{\nu=0}^{n} a_\nu g^\nu$$

mit $a \in \mathbb{N}_0$, $g \in \mathbb{N} \setminus \{1\}$ und $a_\nu \in \mathbb{U}_g$ für $\nu = 0, \ldots, n$ definiere man

$$W(a) \rightleftharpoons \sum_{\nu=0}^{n} (-1)^{n-\nu} a_\nu$$

und erhält analog zu a) damit

$$(g+1)|a \Longleftrightarrow (g+1)|W(a).$$

Aufgabe 37

Wir beginnen zunächst mit b).

b) Satz 75 besagt $\beta: \ N \rightarrowtail\!\!\!\twoheadrightarrow \mathbb{R}$.
Zu zeigen:
β ist bezüglich $\star \in \{+, -, \cdot, /\}$ homomorph.
Beweis:
Wegen $g_{\lceil N} = \beta$ hat man $\nu_{\lceil N} = \beta^{-1} g_{\lceil N} = \beta^{-1}\beta = 1_N$.
Mit (m, e) und (m', e') aus N ergibt sich

I.

$$\begin{aligned}
\beta((m,e)\cdot(m',e')) &= \beta(\nu(mm', e+e')) \\
&= \beta(\beta^{-1}(g(mm', e+e'))) = \beta\beta^{-1}(mm'B^{e+e'}) \\
&= mB^e \cdot m'B^{e'} = g(m,e)\cdot g(m',e') \\
&= \beta(\beta^{-1}(g(m,e)))\cdot\beta(\beta^{-1}(g(m',e'))) \\
&= \beta(\nu(m,e)) + \beta(\nu(m',e')) \\
&= \beta(m,e) + \beta(m',e')
\end{aligned}$$

II.

$$\begin{aligned}
\beta((m,e)+(m',e')) &= g(m + m'B^{e'-e}) = (m + m'B^{e'-e})B^e \\
&= mB^e + m'B^{e'} = g(m,e) + g(m',e') \\
&= \beta(\nu(m,e)) + \beta(\nu(m',e')) \\
&= \beta(m,e) + \beta(m',e')
\end{aligned}$$

III.

$$\begin{aligned}
\beta((m,e)-(m',e')) &= (m - m'B^{e'-e})B^e = mB^e - m'B^{e'} \\
&= \beta(m,e) - \beta(m'-e')
\end{aligned}$$

IV. für $m' \neq 0$:

$$\begin{aligned}\beta((m,e)/(m',e')) &= g(\frac{m}{m'}m, e-e') = \frac{m}{m'}B^{e-e'} \\ &= \frac{mB^e}{m'B^{e'}} \\ &= \beta(m,e)/\beta(m',e')\end{aligned}$$

a) Satz 76 besagt $\nu:\ \mathbb{R}\times\mathbb{Z} \twoheadrightarrow N$.
ZU ZEIGEN:
ν ist bezüglich $\star \in \{+,-,\cdot,/\}$ homomorph.
BEWEIS:
Da β laut b) ein Isomorphismus von $(N,\star)$ auf $(\mathbb{R},\star)$ ist, gilt auch

$$(*)\quad \beta^{-1}:\ (\mathbb{R},\star) \overset{\simeq}{\rightarrowtail\!\!\twoheadrightarrow} (N,\star).$$

Es gilt:

$$\begin{aligned}\nu((m,e\cdot(m',e')) &= \nu(\nu(mm',e+e')) \overset{\text{Satz76c)}}{=} \nu(mm'm,e+e') \\ &= \beta^{-1}(g(mm',e+e')) = \beta^{-1}(mm'B^{e+e'}) = \beta^{-1}(mB^e\cdot m'B^{e'}) \\ &\overset{(*)}{=} \beta^{-1}(mB^e)\cdot\beta^{-1}(m'B^{e'}) = \beta^{-1}(g(m,e))\cdot\beta^{-1}(g(m',e')) \\ &= \nu(m,e)\cdot\nu(m',e')\end{aligned}$$

Für $\star \in \{+,-,/\}$ analog.

Aufgabe 38

a) Gefragt ist nach der Anzahl k der Injektionen von A in B^l,
d. h. $k = |C|$ mit $C \rightleftharpoons \{\varphi \mid \varphi:\ A \rightarrowtail B^l\}$.
Für injektive φ hat man

$$(*)\quad |\varphi(A)| = |A| = m.$$

Wieviele verschiedene $\psi \in C$ mit dem gleichen Bildbereich gibt es für ein festes φ?

$$(**)\quad |C_\varphi| = |\{\psi\in C \mid \psi(A) = \varphi(A)\}| \overset{(*)}{=} m!.$$

Es ist

$$(***)\quad |B^l| = |B|^l = n^l.$$

Damit folgt

$$\begin{aligned}k &= |C| = |\bigcup_{\varphi\in C} C_\varphi| \overset{(**)}{=} |\{X\subseteq B^l \mid |X| = m\}|\cdot m! \\ &= \binom{n^l}{m}\cdot m! = \frac{n^l!}{m!(n^l-m)!}m! \\ &= \frac{n^l!}{(n^l-m)!}.\end{aligned}$$

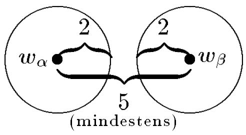
b) $|Z| = 10$, $|\mathbb{B}| = 2$. Mit a) erhält man

$$\begin{array}{ll}
\text{I.} & \dfrac{2^4!}{(2^4-10)!} = \dfrac{16!}{6!} = 29\,059\,430\,400 \\
\text{II.} & \dfrac{2^5!}{(2^5-10)!} = \dfrac{32!}{22!} = 234\,102\,016\,512\,000 \\
\text{III.} & \dfrac{2^6!}{(2^6-10)!} = \dfrac{64!}{54!} = 549\,666\,001\,924\,300\,800 \\
\text{IV.} & \dfrac{2^7!}{(2^7-10)!} = \dfrac{128!}{118!} = 823\,179\,324\,291\,287\,040\,000
\end{array}$$

Aufgabe 39

Die Codewörter aus $\mathbb{B}^8$ seien Elemente des 8-dimensionalen Vektorraumes über dem Galois-Feld $GF(2)$.

a) ANNAHME:
Es gibt einen Code C der Länge 8 über $\mathbb{B}$ mit $|C| = 10$ und $h_C \geq 5$.
WIDERSPRUCH:
Man betrachte die Kugeln vom Radius 2 um jedes Codewort.

Skizze: 

Wegen $2 \cdot 2 = 4 < 5 \leq h_C$ berühren sich diese Kugeln nicht.

Wir bestimmen die Anzahl der Wörter, die in einer solchen Kugel (und auf dem Rand), etwa um $w_\alpha \in C$ liegen.
Abstand 1: Alle Wörter, die sich an genau einer Stelle von w_α unterscheiden:

$$\binom{8}{1} = 8$$

Abstand 2: Alle Wörter, die sich an genau zwei Stellen von w_α unterscheiden:

$$\binom{8}{2} = 28$$

Die gesuchte Anzahl ist also $1 + 8 + 28 = 37$.
Da es mindestens zehn solcher Kugeln geben muß um $h_C \geq 5$ zu gewährleisten, erhält man den Widerspruch

$$10 \cdot 37 = 370 \leq |\mathbb{B}^8| = |\mathbb{B}|^8 = 2^8 = 256.$$

Es gilt also $h_C < 5$.

b) Für die Konstruktion eines solchen Codes C mit $h_C = 4$ könnte man mit 00000000 beginnen.
Durch Halbieren von 0000 000 und „kippen" jeweils einer Hälfte entstehen drei weitere

Wörter.
Durch Vierteln von 00 00 00 00 und „kippen“ jeweils zweier Viertel entstehen vier weitere Wörter.
Das Verfahren mittels Achteln von 0 0 0 0 0 0 0 0 erbringt noch einmal vier Wörter.
Offensichtlich gilt für diesen Code $h_C = 4$.

1:	00000000
2:	00001111
3:	11110000
4:	11110000
5:	00110011
6:	00111100
7:	11000011
8:	11001100
9:	01010101
10:	01011010
11:	10100101
12:	10101010

Es sind zehn beliebige Codewörter auszuwählen.

Aufgabe 40

$$
\begin{array}{cr}
- & 000201 \\ \hline
 & 222021 \\
+ & 000120 \\ \hline
+ & 222211 \\ \hline
- & 000011 \\ \hline\hline
\end{array}
$$

Aufgabe 41

$$
\begin{array}{cr}
- & 000034 \\ \hline
 & 444410 \\
+ & 1 \\ \hline
 & 444411 \\
+ & 000030 \\ \hline
 & 444441 \\
+ & 000003 \\
+ & 1 \\ \hline
- & 000004 \\ \hline\hline
\end{array}
$$

Aufgabe 42

- 10^{12} Sekunden
- $1,6 \cdot 10^{10}$ Minuten
- $2,7 \cdot 10^{8}$ Stunden
- 11 574 074 Tage
- 31 688,... Jahre

Aufgabe 43 Hier gibt es meherere Varianten der Lösung:

a) Multiplikation durch wiederholte Addition, Realisierung also in einem Serienparallelen Addierwerk.

b) Multiplikation durch Shiften (Schieben) und Addieren entsprechend der schriftlichen Multiplikation.

c) Multiplikation durch vermischte Addition und Subtraktion:

III. Man durchsucht den Multiplikator nach ununterbrochenen Folgen von Nullen und Einsen

III. Für n hintereinanderstehende Nullen n-mal nach rechts shiften.

III. Für n hintereinanderstehende Einsen zunächst einmal subtrahieren, dann n-mal nach rechts shiften, dann addieren entsprechend dem Grundgedanken $(2^n - 1)b = 2^n b - b$.

Eine solche Multiplikation läßt sich durch die Formel

$$A \cdot B = \sum_{i=1}^{n} B_i \cdot A \cdot 2^{i-1}.$$

Aufgabe 44

Eine Möglichkeit ist die Anwendung binomischer Formeln:

$$(a+b)^2 = a^2 + 2 \cdot a \cdot b + b^2 \quad \text{oder} \quad (a-b)^2 = a^2 - 2 \cdot a \cdot b + b^2,$$

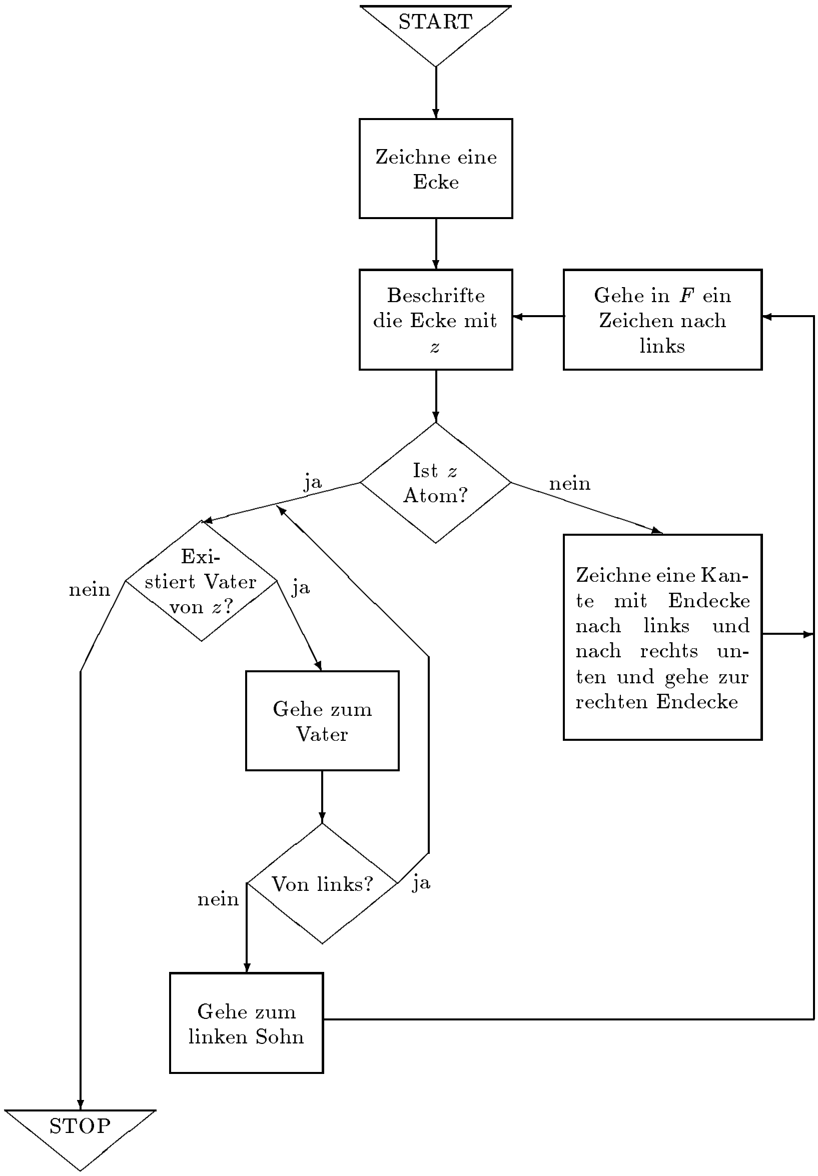
womit sich

$$a \cdot b = \frac{1}{2}\left((a+b)^2 - a^2 - b^2\right) \quad \text{oder} \quad a \cdot b = \frac{1}{2}\left(a^2 + b^2 - (a-b)^2\right).$$

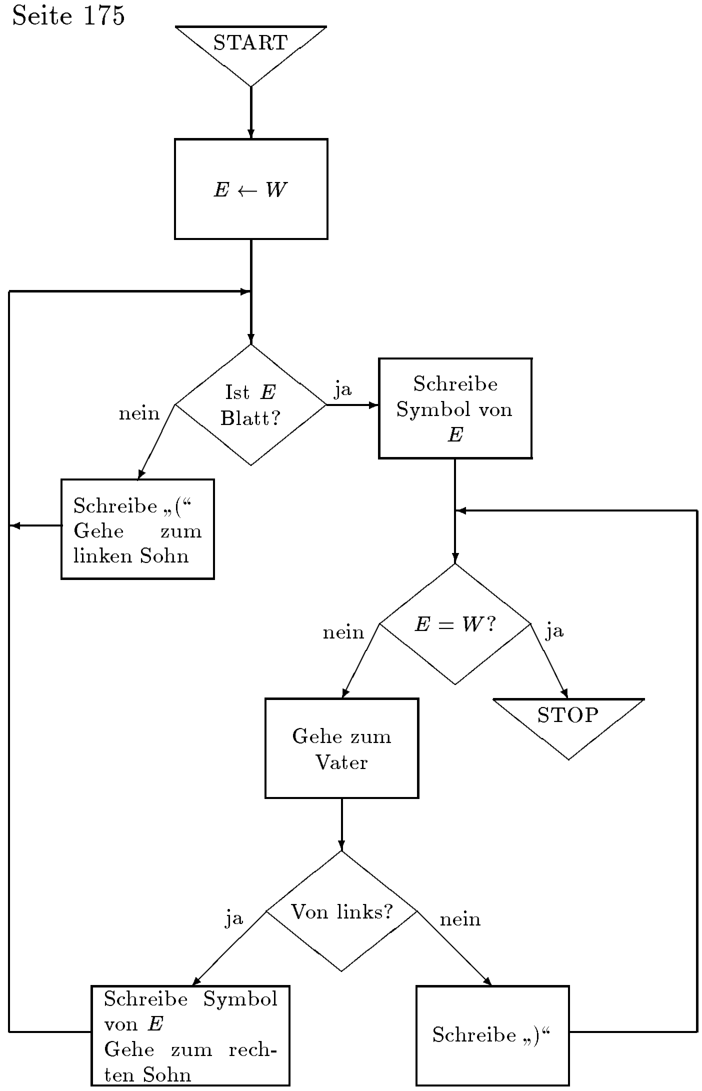
ergibt. Die Benutzung beider Formeln führt auf

$$a \cdot b = \frac{1}{4}\left((a+b)^2 - (a-b)^2\right).$$

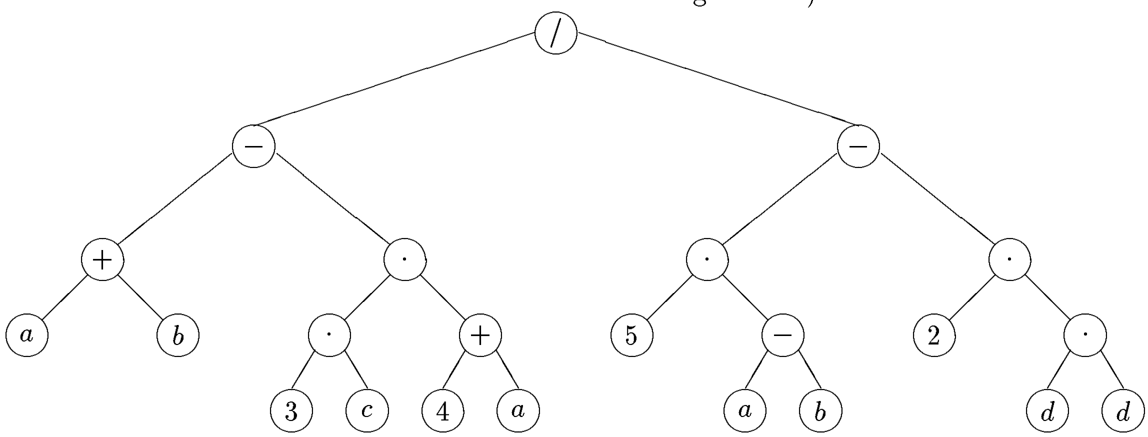
Erstellung eines Kantorowitschbaumes zu Aufgabe 11a)



Erstellen einer Formel mittels Kantorowitschbaum von Seite 175

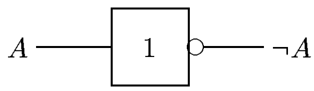
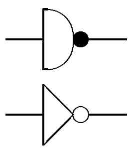
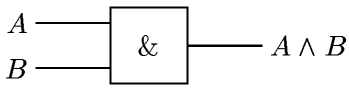
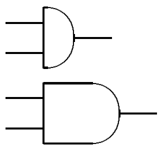
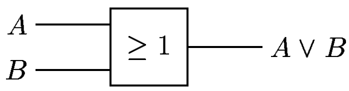
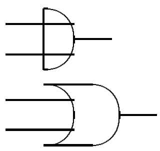


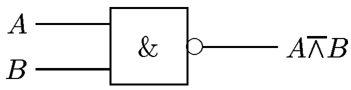
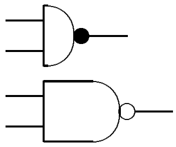
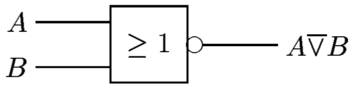
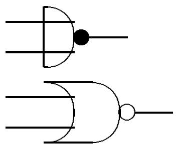
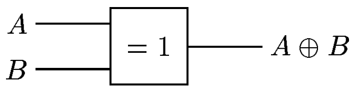
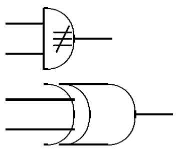
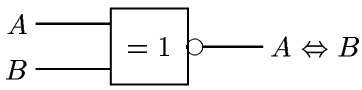
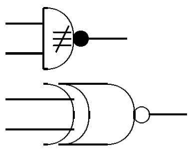
Kantorowitschbaum zur Aufgabe 11b)



Anhang C

Schaltungen

Gatter	alternativ	math	DIN-Norm	veraltet
NON	Inverter, Negator	$\overline{A}$, $\neg A$, $\sim A$		
AND	Konjunktor	$A \wedge B$, $A \& B$, $A \bullet B$, AB		
OR	Adjunktor, Disjunktor, Alternator, Valenz	$A \vee B$, $A + B$		

Gatter	alternativ	math	DIN-Norm	veraltet
NAND	Negatadjunktor, Sheffer-Strich	$\overline{A \wedge B}$, $A \overline{\wedge} B$, $A \vert B$, $A \uparrow B$, $A \sqcup B$, $A - B$		
NOR	Negatkonjunktor, Antialternator, Peirce-Pfeil, Nicod-Funktor, „weder, noch“	$\overline{A \vee B}$, $A \overline{\vee} B$, $A \downarrow B$, $A \sqcap B$, $A \bigtriangledown B$		
EXOR	Exklusiv-Oder, vollständige Adjunktion, vollständige Disjunktion „entweder, oder“	$A \dot{\vee} B$, $A \triangle B$, $A \oplus B$, $A \not\leftrightarrow B$, $A \not\Leftrightarrow B$, $A \curlyvee B$		
EXNOR	NEXOR-Gatter, Exklusiv-NOR, (Materiale) Äquivalenz, „genau dann, wenn“	$A \equiv B$, $A \leftrightarrow B$, $A \Leftrightarrow B$, $A \curlywedge B$, $A \sim B$		

Anhang D

Personenverzeichnis

Baudot Jean Maurice, (1845–1903); seit 1882 Ingénieur-inspecteur des französischen Telegraphensystems. Einheit der Telegraphiergeschwindigkeit, allgemeiner der Datenübertragung: 1 Bd=1 Baud=1 bps (bit per second) siehe S. 106

Birkhoff Gerrett, (⋆1911); Professor an der Harvard University, nebenbei Industrietätigkeit.
siehe S. 33

Boole George, (2.11.1815–8.12.1864), Professor in Cork; mit seinem 1847 erschienenen Werk „The mathematical analysis of logic" leitete er eine Algebraisierung der Logik ein und wurde damit einer der Mitbegründer der modernen Logik siehe S. 7

Caramuel Juan y Lobkowitz, (1606–1682); Generalvikar der Zisterzienser, Bischof von Campania und Vigurano, Darstellung des dualen Systems in „Mathesis biceps vetus et nova", Campania 1670.
siehe S. 95

Euler Leonhard, (1707–1783); Professor in St. Petersburg und Berlin
siehe S. 42, 63, 70, 88

Frege Friedrich Ludwig Gottlob, (1848–1925); Professor in Jena. Die heutige Schreibweise der Subjunktion geht auf seine „Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens", Halle 1879 zurück.
siehe S. 45

Gauß Carl Friedrich, (1777–1855); Prof. in Göttingen. Telegraphierversuche zusammen mit Weber.
siehe S. 110

Gentzen Gerhard Karl, (1909–1945); Dozent in Prag
siehe S. 62

Gödel Kurt, (1906–1978); Dozent in Wien und Princeton, ab 1953 dort Professor. Dissertation „Die Vollständigkeit der Axiome des logischen Funktionalkalküls", Monatshefte für Mathematik und Physik 37/1930, S. 349–360.
siehe S. 60

Gray Frank, (†1969); amerikanischer Physiker. Gray-Code in US Patent Office 26 32 058, 1953.
siehe S. 109

Hamilton Sir Williams Rowan, (1805–1865); Professor in Dublin
siehe S. 64, 88

Hamming Richard Wesley, (⋆ 11.01.1915); amerikanischer Mathematiker bei den Bell Telephone Laboratories, ab 1976 Prof. für Informatik in Monterey, Cal. Die Hamming-Abstand, -Zahl entstanden 1948–50.
siehe S. 107

Harriot Thomas, (ca. 1560–1621); engl. Mathematiker, Physiker und Astronom. In seinem unveröffentlichten Manuskript (ca. 1605) taucht zum ersten Mal das duale Zahlensystem auf.
siehe S. 95

Hasse Helmut, (1898–1979); Professor in Halle, Marburg, Göttingen, Berlin und Hamburg; algebraischer Zahlentheoretiker
siehe S. 22

Horner William George, (1786–1837); Darstellung des nach ihm benannten Schemas in „A new method of solving numerical equations of all orders, by continous approximation", Phil. Trans. RSL, 1819, S. 308–335
siehe S. 100

Kantorowitsch Leonid Witaljewitsch, (1912–1986); Mathematiker und Wirtschaftswissenschaftler; Professor in Leningrad und Moskau; arbeitete an den Grundlagen des linearen Programmierens, führte 1955 den Kantorowitsch-Baum ein; Nobelpreis 1975
siehe S. 86

Kuratowski Kazimir, (1896–1980); Professor in Lemberg und Warschau
siehe S. 68

Leibniz Gottfried Wilhelm; Darstellung des dualen Systems in „Explication de l'arithmétique binaire", Paris 1703, S. 110–116.
siehe S. 95

Łukasiewicz Jan, (1878–1956); Logiker und Philosoph; Professor in Warschau und Dublin, Kultusminister; Mitbegründer der Warschauer Logikerschule; entwickelte die polnische Notation um 1925
siehe S. 86

Morgan Augustus de, (27.6.1806–18.3.1871); britischer Mathematiker und Logiker, Professor in London, Mitbegründer der modernen Logik (Algebra der Logik), bedeutendes Werk „Formel Logic"
siehe S. 9, 64

Peirce Charles Sonders-Peirce, (10.9.1839–19.4.1914), amerikanischer Philosoph und Mathematiker, Sohn von Benjamin Peirce (4.IV.1809–6.X.1880), Mathematiker und Astronom, Professor an der Harvard University, Cambridge, Mass siehe S. 7

Quine Willard von Orman, ($\star$1908); Mathematiker, Logiker, Philosoph; Professor an der Harvard University. Entwickelte mit McCluskey das nach ihnen benannte Verfahren.
siehe S. 52

Ruffini Paolo, (1765–1822); Arzt, Prof. der Medizin und Mathematik in Modena.
siehe S. 100

Russel Bertrand Arthur William, 3. Earl , Duke of Bertford, (1872–1970); Professor in Cambridge et. al., fand die Antinomie 1901 in Freges „Grundgesetze der Arithmetik“ 1893
siehe S. 42

Sheffer Henry Maurice, (1883–1964), amerikanischer Logiker siehe S. 7

Stibitz George Robert; konstruierte ab 1937 Relais-Rechner. Stibitz-Code in „Computer Memorandum“, Bell Telephone Laboratories 1940.
siehe S. 109

Stone Marshall Harvey, (1903–1989); Professor an der Harvard University, Columbia University, Yale University, University of Chicago, Cambridge, University of Massachusetts.
siehe S. 32

Veblen Oswald, (1880–1960); Professor in Chicago und Princeton
siehe S. 88

Venn John, (1834–1923); Professor (Moralphilosophie) in Cambridge
siehe S. 42

Weber Wilhelm Eduard, (1804–1891); Prof. in Göttingen und Leipzig, bedeutender Physiker, einer der Göttinger Sieben. Telegraphierversuche mit Gauß.
siehe S. 110

Anhang E

Literaturverzeichnis

Stichwortverzeichnis