Inhaltsverzeichnis

Darstellung von Schaltfunktionen unter Ausnutzung von Symmetrien boolescher Algebren

G. Hotz

1 Einleitung

Ein zentrales Problem der Computerentwicklung besteht in dem Entwurf von Schaltkreisen, die vorgegebene boolesche Funktionen, d.h. Abbildungen $f : \mathbb{B}^n \to \mathbb{B}^m$, $\mathbb{B} = \{0, 1\}$ realisieren. Natürlich hat man den Wunsch, ein Programm zu entwickeln, das aufgrund der Spezifikationen einer solchen Funktion f automatisch einen optimalen Schaltkreis erzeugt, der f darstellt. Sobald man näher hinschaut, wird schon dieser Wunsch problematisch: In welcher Sprache soll f definiert werden? Was soll optimal heißen? Und in der Tat ist man von der Lösung der Aufgabe noch weit entfernt, wenn man auch sehr beachtliche Fortschritte auf diesem Weg gemacht hat.

Wir wollen uns hier mit der Frage befassen, wie man die Invarianz von f unter Automorphismengruppen boolescher Algebren zur Konstruktion von Darstellungen von f durch boolesche Netze ausnutzen kann. *McCluskey* ist 1956 in seinem Artikel *Minimization of Boolean Functions* [McC56] auf die Ausnutzung von Variablensymmetrien bei der Berechnung von Primimplikanten boolescher Funktionen $f : \mathbb{B}^n \to \mathbb{B}$ eingegangen. In einem etwas weitergehenden systematischen Ansatz wird in [Hot61], [Hot74] eine Verbindung zwischen dem Verband boolescher Algebren und Automorphismengruppen auszunutzen versucht, um zu allgemeineren Darstellungen boolescher Funktionen zu gelangen.

Grundlegend war die Beobachtung, daß Schnitte durch das boolesche Netz, das f darstellt, Erzeugendensysteme boolescher Algebren definieren und daß eine Folge von *parallelen* Schnitten zu einer Folge absteigender boolescher Algebren führt, die sich auf die durch $f = [f_1, \dots, f_m]$ erzeugte boolesche Algebra $\langle f_1, \dots, f_n \rangle$ zusammenziehen. Zu der absteigenden Folge boolescher

Algebren gehört eine aufsteigende Folge von ineinander enthaltenen Automorphismengruppen, die eine korrespondierende boolesche Algebra elementweise festlassen. Diese Verbindung führte im Zusammenhang mit der Addition zu einfachen Addierwerken.

E. Engeler hat in [Eng75] den Aspekt der Ausnutzung von Symmetrien im Zusammenhang mit Fragen nach der Lösbarkeit algorithmischer Probleme behandelt, ohne aber auf ihre Anwendung im Bereich der booleschen Schaltnetze einzugehen. In einem etwas weiteren Sinne gehört auch die von *T. Beth* in [Bet84] entwickelte Theorie der schnellen Fourier-Transformation in Restklassenringen hier hin. Wir verwenden dieses Konzept in dieser Vorlesung zur Herleitung eines neuen effizienten Multipliziernetzwerkes der Tiefe $0(\log n)$ und der Größe $0(n \cdot \log n)$ für n-stellige Dualzahlen.

Mit Erfolg wurden unter Ausnutzung von Symmetrien von *B. Becker und R. Kolla* [BK87] effiziente Darstellungen für Addierer angegeben. Schließlich ist es *C. Scholl* in seiner Dissertation [Sch97] gelungen, das Konzept der Symmetrien in Verbindung mit den speziellen Darstellungen boolescher Funktionen durch binäre Entscheidungsdisgramme (BDDs) so auf den Rechner zu bringen, daß er automatisch eine etwas verbesserte Version des c.s.–Addierers für 64-stellige Dualzahlen in weniger als einer Stunde Rechenzeit erzeugen konnte.

Somit war es an der Zeit, den Versuch zu machen die Theorie der booleschen Netze unter Ausnutzung von Symmetrien einmal systematisch darzustellen. Diesem Ziel war das erste Kapitel meiner Vorlesung „VLSI–Entwurf“ im SS 1997 und die ganze Vorlesung „Schaltkreistheorie“ im WS 1997/98 gewidmet.

Das vorliegende Manuskript ist die Ausarbeitung dieser Vorlesung. Meinen Hörern A. Gamkrelidze, B. Schieffer, J.-B. Son und B. Zhu bin ich für kritische Fragen und J.-B. Son und M. Melchior zusätzlich für die kritische Durchsicht von Teilen des Manuskiptes zu Dank verpflichtet. Frau K. Klose danke ich für das Schreiben des Textes und die Konstruktion der Figuren und Diagramme.

2 Grundlagen der endlichen booleschen Algebren

2.1 Grundlegende Definitionen

2.1.1 Definition der booleschen Algebren

$(M, \cup, \cdot, -)$ heißt boolesche Algebra: $\Longleftrightarrow$ Es ist $M \neq \emptyset$ und es gelten für alle $a, b \in M$ die Axiome (A1) bis (A5).

(A1) $\quad a \cup b = b \cup a, \quad a \cdot b = b \cdot a$

(A2) $\quad a \cup (b \cup c) = (a \cup b) \cup c, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(A3) $\quad a \cup (a \cdot b) = a, \quad a \cdot (a \cup b) = a$

(A4) $\quad a \cup (b \cdot c) = (a \cup b) \cdot (a \cup c), \quad a \cdot (b \cup c) = (a \cdot b) \cup (a \cdot c)$

(A5) $\quad a \cup (b \cdot \overline{b}) = a, \quad a \cdot (b \cup \overline{b}) = a$

2.1.2 Das Dualitätsprinzip

Eine Aussage ist ein Satz der booleschen Algebra, wenn sie aus der Definition der booleschen Algebra logisch folgt. Jeder Satz der booleschen Algebra geht durch die Vertauschung von „$\cup$“ und „$\cdot$“ in einen Satz der booleschen Algebra über, was daraus folgt, daß die Definition der booleschen Algebra unter diesen Vertauschungen der Operationen invariant ist.

Beobachtung 2.1.

1. Jede boolesche Algebra besitzt genau eine 0 und eine 1.

2. Zu jedem $a \in M$ gibt es genau ein Element $\overline{a} \in M$ mit $a \cup \overline{a} = 1$ und $a \cdot \overline{a} = 0$. Hieraus folgt $a = \overline{\overline{a}}$.

3. $a \cdot a = a, \quad a \cup a = a \quad$ für $\quad a \in M$

Wir setzen $a \leq b :\Longleftrightarrow a \cdot b = a$ und beweisen leicht

4. $0 \leq a \leq 1, \quad a \leq b \Longleftrightarrow \overline{b} \leq \bar{a}$

5. $a \leq b$ und $b \leq a \Longrightarrow a = b$

6. $a \leq b$ und $b \leq c \Longrightarrow a \leq c$.

Wir schreiben $a < b$, genau dann, wenn $a \leq b$ und $a \neq b$ gelten.

7. Aus $a < b$ und $b \leq c$ folgt $a < c$.

8. Hat M mehr als ein Element, dann gilt $0 < 1$.

Die folgenden Beispiele zeigen, daß es boolesche Algebren gibt.

Beispiel 1. Sei $\mathbb{B} = \{0, 1\}$ und seien $\vee, \cdot, -$ wie folgt definiert.

$$\begin{aligned}
0 \vee 0 &:= 0 \\
0 \vee 1 &:= 1 \vee 0 := 1 \vee 1 := 1 \\
1 \cdot 1 &:= 1 \\
1 \cdot 0 &:= 0 \cdot 1 := 0 \cdot 0 := 0 \\
\overline{0} &:= 1 \\
\overline{1} &:= 0
\end{aligned}$$

Hat man einmal eine boolesche Algebra, dann kann man aus ihr leicht viele weitere boolesche Algebren erzeugen, wie das folgende Beispiel zeigt.

Beispiel 2. Sei D Menge und $\mathcal{B}$ eine boolesche Algebra. Wir setzen

$$S(D, \mathcal{B}) := \{f : D \to \mathcal{B}\}$$

und definieren für

$$f, g \in S(D, \mathcal{B})$$

die Operationen $\vee, \cdot, -$ wie folgt:

$$\begin{aligned}
(f \vee g)(\xi) &:= f(\xi) \vee g(\xi), \\
(f \cdot g)(\xi) &:= f(\xi) \cdot g(\xi), \\
\bar{f}(\xi) &:= \overline{f(\xi)}.
\end{aligned}$$

Man prüft leicht nach, daß $(S(D, \mathcal{B}), \cup, \cdot, -)$ eine boolesche Algebra ist.

Wir setzen abkürzend

$$S(D) = S(D, \mathbb{B})$$

und

$$S_n := S(\mathbb{B}^n).$$

Beispiel 3. Sei $(\mathbb{B}^n, \cup, \cdot, -)$ durch die komponentenweise Übertragung der Operationen von $\mathbb{B}$ auf $\mathbb{B}^n$ definiert; d.h. es gelten

$$\begin{aligned}
(\alpha_1, \ldots, \alpha_n) \cup (\beta_1, \ldots, \beta_n) &= (\alpha_1 \cup \beta_1, \ldots, \alpha_n \cup \beta_n), \\
(\alpha_1, \ldots, \alpha_n) \cdot (\beta_1, \ldots, \beta_n) &= (\alpha_1 \beta_1, \ldots, \alpha_n \beta_n), \\
\overline{(\alpha_1, \ldots, \alpha_n)} &:= (\overline{\alpha_1}, \ldots, \overline{\alpha_n}).
\end{aligned}$$

Offensichtlich ist $(\mathbb{B}^n, \cup, \cdot, -)$ eine boolesche Algebra.

An sich folgt das schon aus dem Beispiel 2, wenn man dort $D = [1:n] := \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$ setzt.

Die hier betrachteten booleschen Algebren sind alle endlich. Wir haben

$$\sharp\mathbb{B} = 2, \quad \sharp\mathbb{B}^n = 2^n, \quad \sharp S_n = 2^{2^n}, \quad \sharp S(D, \mathbb{B}) = 2^{\sharp D};$$

hierin bezeichnet $\sharp D$ die Anzahl der Elemente der Menge D, falls D endlich ist. Ist D nicht endlich, dann setzen wir

$$\sharp D = \infty.$$

2.2 Unteralgebren, Erzeugendensysteme und Atome

Sei $\mathcal{B}$ eine boolesche Algebra und $\mathcal{B}'$ eine Teilmenge von $\mathcal{B}$. $\mathcal{B}'$ heißt genau dann *Unteralgebra* von $\mathcal{B}$, wenn für alle Elemente $a, b \in \mathcal{B}'$

$$a \vee b \in \mathcal{B}', \; a \cdot b \in \mathcal{B}', \; \overline{a} \in \mathcal{B}'$$

gilt.

Wir betrachten hierzu das

Beispiel 4. Sei $\mathcal{B} = S_4$ und

$$\mathcal{B}' = \{f : \mathbb{B}^4 \to \mathbb{B} \mid f(\xi) = f(\eta) \\ \text{für } \xi_2 + \xi_4 + 2(\xi_1 + \xi_3) = \eta_2 + \eta_4 + 2(\eta_1 + \eta_3)\}$$

Wir zeigen, daß $\mathcal{B}'$ eine Unteralgebra von S_4 ist.

Seien $f, g \in \mathcal{B}'$ und

$$h = f \vee g.$$

Wir haben dann

$$h(\xi) = f(\xi) \vee g(\xi).$$

Aufgrund der Voraussetzung über f, g gilt für $\xi, \eta \in \mathbb{B}^4$ und

$$2 \cdot (\xi_1 + \xi_3) + \xi_2 + \xi_4 = 2(\eta_1 + \eta_3) + \eta_2 + \eta_4,$$

daß $f(\xi) = f(\eta)$ und $g(\xi) = g(\eta)$ ist.

Hieraus folgt

$$f(\xi) \vee g(\xi) = f(\eta) \vee g(\eta), \; f(\xi) \cdot g(\xi) = f(\eta) \cdot g(\eta), \; \overline{f}(\xi) = \overline{f}(\eta).$$

Also ist $\mathcal{B}'$ unter den Operationen von $\mathcal{B}$ abgeschlossen, d.h. $\mathcal{B}'$ ist eine Unteralgebra von $\mathcal{B}$.

Sind $\mathcal{B}_1$ und $\mathcal{B}_2$ Unteralgebren der booleschen Algebra $\mathcal{B}$, dann ist auch $\mathcal{B}_1 \cap \mathcal{B}_2$ eine Unteralgebra von $\mathcal{B}$.
Sind $f, g \in \mathcal{B}_1 \cap \mathcal{B}_2$, dann gilt nämlich

$$f * g \in \mathcal{B}_1 \text{ und } f * g \in \mathcal{B}_2 \text{ für } * \in \{\vee, \cdot\}$$

und $\overline{f} \in \mathcal{B}_1,\ \overline{f} \in \mathcal{B}_2$.

Für $\mathcal{B}_1 \cup \mathcal{B}_2$ gilt das nicht, wie man an dem Beispiel

$$\mathcal{B}_1 = \{(\alpha, 0) \mid \alpha \in \mathbb{B}\},\ \mathcal{B}_2 = \{(0, \beta) \mid \beta \in \mathbb{B}\}$$

erkennt. Es ist $(1,1) \notin \mathcal{B}_1 \cup \mathcal{B}_2$, aber mit $(1,0) \in \mathcal{B}_1$ und $(0,1) \in \mathcal{B}_2$ liegt (1,1) in jeder booleschen Algebra, die sowohl $\mathcal{B}_1$ als auch $\mathcal{B}_2$ enthält.

Wir nehmen diese Tatsache nun als Anlaß für die folgende

Definition 1. Ist $E \subset \mathcal{B}$, dann definieren wir

$$\langle E \rangle_{\mathcal{B}} := \bigcap_{E \subset \mathcal{B}'} \mathcal{B}'$$

$\mathcal{B}'$ ist hierin Unteralgebra von $\mathcal{B}$. E heißt *Erzeugendensystem* von $\langle E \rangle_{\mathcal{B}}$. Falls der Bezug offensichtlich ist, schreiben wir $\langle E \rangle$ anstelle von $\langle E \rangle_{\mathcal{B}}$.

Lemma 1. $\langle E \rangle_{\mathcal{B}}$ ist eine Unteralgebra von $\mathcal{B}$.

Beweis. Seien $f, g \in \langle E \rangle_{\mathcal{B}}$ und $* \in \{\vee, \cdot\}$, dann gilt aufgrund der Definition von $\langle E \rangle_{\mathcal{B}}$: Ist $\mathcal{B}'$ eine Unteralgebra von $\mathcal{B}$, und gilt $E \subset \mathcal{B}'$, dann ist $f, g \in \mathcal{B}'$. Hieraus folgt $f * g \in \mathcal{B}'$, $\overline{f} \in \mathcal{B}'$. Es gilt also auch $\overline{f}, f * g \in \langle E \rangle_{\mathcal{B}}$. □

Man erkennt, daß

$$A = \{(\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0) \mid i = 1, \ldots, n\}$$

ein Erzeugendensystem von $\mathbb{B}^n$ ist. Das Erzeugendensystem A ist von sehr spezieller Natur. Die Elemente von A sind nämlich die kleinsten Elemente von $\mathbb{B}^n$, die ungleich 0 sind. Diese Erzeugendensysteme spielen eine besondere Rolle, so daß sie einen speziellen Namen erhalten.

Definition 2. Sei $\mathcal{B}$ eine boolesche Algebra und $a \in \mathcal{B}$. a heißt *Atom* von $\mathcal{B}$: $\Longleftrightarrow$ Es gilt $a \neq 0$, und für alle $b \in \mathcal{B}$ gilt $a \cdot b = a$ oder $a \cdot b = 0$.

Lemma 2. Jede endliche boolesche Algebra mit mindestens zwei Elementen besitzt Atome. Ist $f \neq 0$ Element der Algebra, dann gibt es ein Atom a der Algebra mit $a \leq f$.

Beweis. $\mathcal{B}$ enthält mindestens zwei Elemente. Es gibt daher ein Element $a \in \mathcal{B}$, so daß $a \neq 0$ ist.

Gilt für alle $b \in \mathcal{B} : a \cdot b = 0$ oder $a \cdot b = a$, dann ist a Atom. Ist das nicht der Fall, dann gibt es b_1 mit $a \neq a \cdot b_1 \neq 0$.

Nun betrachten wir $a_1 = a \cdot b_1$. Ist a_1 Atom, dann sind wir fertig. Im anderen Fall wählen wir b_2, so daß $a_1 \neq a_1 \cdot b_2 \neq 0$ ist und haben

$$a \cdot b_1 \cdot b_2 < ab_1 < a.$$

Indem wir das Verfahren fortsetzen, erhalten wir eine Kette

$$a_1 > a_2 > \ldots > a_k > 0.$$

Da $\mathcal{B}$ endlich ist, bricht das Verfahren ab. Das tritt aber nur dann ein, wenn wir ein Atom gefunden haben. Damit ist der erste Teil des Satzes bewiesen. Auf die gleiche Weise zeigt man auch: Zu jedem $f \in \mathcal{B}$ mit $f \neq 0$ gibt es ein Atom $a \leq f$. □

Lemma 3. Ist A die Menge der Atome von $\mathcal{B}$, dann ist $\langle A \rangle = \mathcal{B}$. Weiter gilt für jedes $f \in \mathcal{B}$

$$f = \bigvee_{a \in A} f \cdot a.$$

Beweis. Seien $a_1, \ldots, a_m$ die Atome von $\mathcal{B}$. Wir bilden

$$x = a_1 \vee \ldots \vee a_m.$$

Ist $\overline{x} \neq 0$, dann gibt es aufgrund von Lemma 2 ein Atom $a \leq \overline{x}$.
Hieraus folgt

$$ax = a = a \cdot \overline{x}$$

Wegen $x \cdot \overline{x} = 0$ gilt

$$0 = a(x\overline{x}) = (ax)\overline{x} = a \cdot \overline{x} = a \quad \textit{Widerspruch!}$$

Also haben wir

$$\bar{x} = 0 \quad \text{d.h.} \quad x = 1$$

Ist $f \in \mathcal{B}$, dann gilt

$$f = f \cdot 1 = f \cdot a_1 \cup \ldots \cup f \cdot a_m,$$

womit Lemma 3 bewiesen ist. □

Also jedes f ist Summe von Atomen. Setzen wir

$$\alpha_i = \begin{cases} 1 & \text{für} \quad a_i \cdot f = a_i \\ 0 & \text{für} \quad a_i \cdot f = 0, \end{cases}$$

dann können wir auch

$$f = \alpha_1 \cdot a_1 \cup \ldots \cup \alpha_m \cdot a_m, \quad \alpha_i \in \{0, 1\}.$$

schreiben. Die Darstellung ist eindeutig. Ist nämlich

$$\alpha_1 \cdot a_1 \cup \ldots \cup \alpha_m a_m = \beta_1 \cdot a_1 \cup \ldots \cup \beta_m \cdot a_m,$$

dann erhält man durch Multiplikation mit a_l

$$\alpha_l \cdot a_l = \beta_l \cdot a_l$$

d.h. es gilt für alle l

$$\alpha_l = \beta_l.$$

Hieraus ergibt sich, daß $\sharp\mathcal{B}$ eine Zweierpotenz ist.

Wir fassen die Resultate in dem folgenden Satz zusammen.

Satz 1. *Jede endliche boolesche Algebra $\mathcal{B}$ besitzt Atome. Ist A die Menge der Atome von $\mathcal{B}$, dann läßt sich jedes Element $f \in \mathcal{B}$ auf genau eine Weise als Summe von Elementen von A darstellen. Weiter gilt*

$$\sharp\mathcal{B} = 2^{\sharp A}.$$

Dieser Satz ist Teil des weitergehenden Satzes von Stone, den wir etwas später beweisen werden. Zunächst betrachten wir zwei für uns wichtige Beispiele. Hierzu verabreden wir die folgende Bezeichnung:

Wir setzen für $f \in \mathcal{B}$ und $\varepsilon \in \{0, 1\}$

$$f^\varepsilon := \begin{cases} \overline{f} & \text{für} \quad \varepsilon = 0 \\ f & \text{für} \quad \varepsilon = 1. \end{cases}$$

Weiter definieren wir $x_i \in S_n$ durch

$$x_i(\xi) = \xi_i \text{ für } \xi = (\xi_1, \ldots, \xi_n) \in \mathbb{B}^n.$$

x_i ist also die Projektion von $\mathbb{B}^n$ auf die i-te Komponente. Wir setzen weiter

$$x^\varepsilon := x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n} \text{ für } \varepsilon \in \mathbb{B}^n.$$

Lemma 4.

$$A = \{x^\varepsilon \mid \varepsilon \in \mathbb{B}^n\}$$

ist die Menge der Atome von S_n.

Beweis. Ist $f \in S_n$, dann gilt $x^\varepsilon(\xi) \Leftrightarrow \xi = \varepsilon$ und

$$(x^\varepsilon \cdot f)(\varepsilon) = x^\varepsilon(\varepsilon) \cdot f(\varepsilon) = \begin{cases} 0 & \text{für} \quad f(\varepsilon) = 0 \\ 1 & \phantom{\text{für}} \quad f(\varepsilon) = 1. \end{cases}$$

Also gilt $f \cdot x^\varepsilon = x^\varepsilon \quad \text{oder} \quad = 0$, d.h. x^ε ist Atom.

$A = \{x^\varepsilon \mid \varepsilon \in \mathbb{B}^n\}$ ist die Menge aller Atome von S_n, da

$$f = \bigcup_{\varepsilon \in \mathbb{B}^n} f(\varepsilon) \cdot x^\varepsilon$$

gilt. □

Lemma 5. Sei $D \subset \mathbb{B}^n$ und $\tilde{x}_i$ die Einschränkung von x_i auf D. Dann gilt

$$\begin{aligned} &\tilde{x}^\varepsilon \quad \text{Atom von} \quad S(D) \Longleftrightarrow \varepsilon \in D, \\ &x^\varepsilon(\xi) = 0 \quad \text{für} \quad \xi \in D \quad \text{und} \quad \varepsilon \notin D; \quad \text{d.h.} \quad x^\varepsilon = 0 \end{aligned}$$

Beweis. Es gilt

$$\tilde{x}^\varepsilon(\xi) = \begin{cases} 1 & \text{für} \quad \xi = \varepsilon \in D \\ 0 & \qquad\qquad \text{sonst.} \end{cases}$$

Also ist $\tilde{x}^\varepsilon \neq 0$ für $\varepsilon \in D$. $\tilde{x}^\varepsilon$ ist Atom in $S(D)$ für $\varepsilon \in D$, da $\tilde{x}^\varepsilon$ nur an einer Stelle gleich 1 ist. Für $\varepsilon \notin D$ gilt für alle $\xi \in D$, daß $\xi \neq \varepsilon$ ist, woraus $x^\varepsilon = 0$ folgt. □

Korollar 1. *$\tilde{x}_1, \ldots, \tilde{x}_n$ ist ein Erzeugendensystem von $S(D)$ und es gilt*

$$\sharp S(D) = 2^{\sharp D}.$$

Korollar 2. *$x_1, \ldots, x_n$ ist ein Erzeugendensystem von S_n und es gilt*

$$\sharp S_n = 2^{2^n}.$$

Es stellt sich nun die Frage, wieviele verschiedene Erzeugendensysteme es gibt und wie man sie klassifizieren kann. Bevor wir diese Frage angehen können, benötigen wir den Begriff des Homomorphismus.

2.3 Homomorphismen

Definition 3. Die Abbildung $h : \mathcal{B} \to \mathcal{B}'$ heißt Homomorphismus genau dann, wenn 1 - 3 gelten:

$$\begin{aligned} h(f \vee g) &= h(f) \vee h(g), && (1)\\ h(f \cdot g) &= h(f) \cdot h(g), && (2)\\ h(\overline{f}) &= \overline{h(f)}. && (3) \end{aligned}$$

Lemma 6. Sind $\mathcal{B}$ und $\mathcal{B}'$ boolesche Algebren, sind $a, b \in \mathcal{B}$ und ist $h : \mathcal{B} \to \mathcal{B}'$ ein Homomorphismus, dann gelten 1, 2, 3, 4.

1. $a \leq b \Longrightarrow h(a) \leq h(b)$,   h(0) = 0,   h(1) = 1,
2. $h(\mathcal{B})$ ist eine boolesche Algebra,
3. h ist injektiv $\Longleftrightarrow h^{-1}(0) = 0$,
4. Ist a Atom von $\mathcal{B}$, dann ist entweder $h(a)$ Atom von $h(\mathcal{B})$, oder es ist $h(a) = 0$.

Beweis. 1 und 2 folgen unmittelbar. Der Beweis zu 3 ergibt sich aus 1 und 2.

Ad 3: Es ist für alle a

$$0 = a \cdot \overline{a}.$$

Also gilt

$$h(0) = h(a \cdot \overline{a}) = h(a) \cdot h(\overline{a}) = h(a) \cdot \overline{h(a)} = 0.$$

Da h injektiv ist, gilt also

$$h^{-1}(0) = 0.$$

Sind a, b Atome und ist $h(a) = h(b)$, dann gilt

$$0 = h(a) \cdot \overline{h(b)} = h(a\overline{b}).$$

Aus $h^{-1}(0) = 0$ folgt $a \cdot \overline{b} = 0$ und daraus $a = b$.

Also ist h injektiv auf der Menge der Atome von $\mathcal{B}$. Hieraus folgt weiter über den Darstellungssatz, daß h injektiv auf ganz $\mathcal{B}$ ist.

Ad 4: Ist a Atom von $\mathcal{B}$, dann gilt entweder $a \cdot b = a$ oder $a \cdot b = 0$. Im ersteren Fall ergibt sich $h(a) \cdot h(b) = h(a)$. Im letzteren Fall, $h(a) \cdot h(b) = 0$. Wir haben also für alle $b : h(a) \cdot h(b) = h(a)$ oder $= 0$. Ist also $h(a) \neq 0$, dann ist $h(a)$ Atom in $h(\mathcal{B})$.

$\square$

Satz 2. Satz von Stone *Jede boolesche Algebra $\mathcal{B}$ mit 2^N Elementen ist isomorph zu $\mathbb{B}^N$.*

Beweis. Sei $A = \{a_1, \ldots, a_n\}$ die Menge der Atome von $\mathcal{B}$. Wegen $\#\mathcal{B} = 2^N$ ist $n = N$. Nun definieren wir $h'(a_i) = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$ für $i = 1, \ldots, N$. h' bildet die Menge der Atome von $\mathcal{B}$ bijektiv auf die Menge der Atome von $\mathbb{B}^n$ ab. Wir setzen h' zu einem Homomorphismus $h : \mathcal{B} \to B^n$ fort, indem wir

$$h\left(\bigvee_{i=1}^{N} (f \cdot a_i)\right) = \bigvee_{i=1}^{N} h'\,(f \cdot a_i)$$

und $h(0) := 0$ definieren. h ist ein Homomorphismus, wie man nachrechnet. h ist injektiv nach Lemma 6. h ist surjektiv, da $\mathcal{B}$ und $\mathbb{B}^n$ gleichviele Elemente besitzen. Also ist h ein Isomorphismus. $\square$

Definition 4.

1. E heißt *freies* Erzeugendensystem von $\mathcal{B}$ $:\Longleftrightarrow$ Ist $h' : E \to \mathcal{B}'$ eine Abbildung, dann gibt es eine eindeutig bestimmte homomorphe Fortsetzung $h : \mathcal{B} \to \mathcal{B}'$ von h' auf $\mathcal{B}$.

2. $\mathcal{B}$ heißt frei $:\Longleftrightarrow$ $\mathcal{B}$ besitzt ein freies Erzeugendensystem.

Satz 3. *Ist $\mathcal{B}$ endlich und frei, dann gibt es ein $n \in \mathbb{N}$, so daß $\mathcal{B}$* isomorph *zu S_n ist.*

Beweis. Sei $e_1, \ldots, e_n$ ein freies Erzeugendensystem von $\mathcal{B}$. Setze $h'(e_i) = x_i$ für $i = 1, \ldots, n$ und setze h' homomorph zu h fort. Es folgt: $h(e_1^{\varepsilon_1} \cdot \ldots \cdot e_n^{\varepsilon_n}) = x^\varepsilon \neq 0$.

Sei $\mathcal{B}' = \langle\{e^\varepsilon \mid \varepsilon \in \mathbb{B}^n\}\rangle$. $\mathcal{B}'$ ist eine Unteralgebra von $\mathcal{B}$. Da $E \subset \mathcal{B}'$ ist und $\langle E \rangle = \mathcal{B}$ gilt, ist $\mathcal{B} = \mathcal{B}'$. Nun enthält $A = \{e^\varepsilon \mid \varepsilon \in \mathbb{B}^n\}$ offensichtlich die Menge der Atome von $\mathcal{B}'$. Da $0 \notin h(A)$, ist h injektiv; da $\langle\{x_1, \ldots, x_n\}\rangle = S_n$ ist, ist h surjektiv. Also ist h ein Isomorphismus. $\square$

Korollar 3. *Ist $\mathcal{B}$ eine endliche freie boolesche Algebra, dann gilt für ein geeignetes $n \in \mathbb{N}$ $\sharp\mathcal{B} = 2^{2^n}$.*

Beweis. Ist $\mathcal{B}$ endlich und frei, dann ist $\mathcal{B}$ isomorph zu S_n. Aus Korollar 2 folgt nun die Behauptung. □

Korollar 4. *Ist $f : \mathbb{B}^n \to \mathbb{B}^n$ bijektiv und ist $x_i : \mathbb{B}^n \to \mathbb{B}$ die Projektion von $\mathbb{B}^n$ auf die i-te Komponente, dann ist $\{f_i = x_i \circ f \mid i = 1, \ldots, n\}$ ein freies Erzeugendensystem von S_n.*

Beweis. Wir betrachten $\langle\{x_i | i = 1, \ldots, n\}\rangle = S_n$. Wir definieren $h : S_n \to S_n$ durch $h(g) := g \circ f$. Der Beweis ergibt sich aus 1, 2 und 3.

1. *h ist ein Homomorphismus.*

   Für $\xi \in \mathbb{B}^n$ gilt

$$((g_1 \cup g_2) \circ f)(\xi) = g_1(f(\xi)) \cup g_2(f(\xi)) \tag{4}$$
$$= (g_1 \circ f)(\xi) \cup (g_2 \circ f)(\xi) = ((g_1 \circ f) \cup (g_2 \circ f))(\xi). \tag{5}$$

   Ebenso beweist man die Homomorphie für „·“ und „$^-$“

2. *h ist ein Isomorphismus.*

$$\forall \xi : (g \circ f)(\xi) = 0 \Longleftrightarrow \forall \xi : g(\xi) = 0,$$

   da f bijektiv ist.

   Also gilt

$$h(g) = 0 \Longleftrightarrow g = 0,$$

   woraus die Behauptung 2 folgt.

3. *$f_1, \ldots, f_n$ ist ein freies Erzeugendensystem*

   Aus dem Beweis des Satzes von Stone ergibt sich, daß $\{x_1, \ldots, x_n\}$ ein freies Erzeugendensystem von S_n ist. Nun ist h ein Isomorphismus. Also ist $f_i := h(x_i), i = 1, \ldots, n$ ein freies Erzeugendensystem.

□

Korollar 5. *S_n besitzt $\frac{2^n!}{n!}$ freie Erzeugendensysteme.*

Beweis. Ist $h : S_n \to S_n$ ein Isomorphismus, dann liefert die Einschränkung von h auf die Menge der Atome x^ε eine Permutation. Diese Permutation überträgt man auf $\mathbb{B}^n$: Geht x^ε in x^η über, dann setze man $f(\eta) = \varepsilon$. Man erhält $h(x^\varepsilon) = x^\varepsilon \circ f$. Also kann man jeden Automorphismus von S_n durch eine Bijektion auf $\mathbb{B}^n$ erzeugen.

Die Anzahl der Automorphismen von S_n ist gleich der Anzahl der Permutationen der Atome von S_n. Da es auf die Reihenfolge der freien Erzeugenden nicht ankommt, ist diese Anzahl gleich $2^n! \cdot \frac{1}{n!}$. □

In freien booleschen Algebren besitzt man nur die Rechenregeln, die sich aus den Axiomen der booleschen Algebra ableiten lassen. In nicht freien booleschen Algebren $S(D)$ gelten zusätzlich die Relationen

$$x^\varepsilon = 0 \quad \text{für} \quad \varepsilon \in \mathbb{B}^n - D,$$

was man zur Vereinfachung der Darstellung boolescher Funktionen ausnutzen kann.

Aufgabe: Man verallgemeinere das Korollar 5 auf nicht freie boolesche Algebren $S(D)$.

2.4 Quotienten boolescher Algebren

Seien $\mathcal{B}, \mathcal{B}'$ boolesche Algebren und sei $h : \mathcal{B} \to \mathcal{B}'$ ein Homomorphismus. Sind $f_1, f_2 \in h^{-1}(0)$ und ist $f \in \mathcal{B}$, dann gilt

$$f_1 \cup f_2 \in h^{-1}(0) \textit{ und } f \cdot f_1 \in h^{-1}(0).$$

$h^{-1}(0)$ ist also abgeschlossen unter der Vereinigung und der Multiplikation mit beliebigen Elementen aus $\mathcal{B}$. Diese Eigenschaft von $h^{-1}(0)$ nehmen wir zum Anlaß für die folgende

Definition 5. Eine Teilmenge $\Im \subset \mathcal{B}$ heißt Ideal von $\mathcal{B}$, wenn 1 und 2 gelten.

1. $\Im$ ist abgeschlossen unter $\cup$.
2. Für $f \in \mathcal{B}$ und $g \in \Im$ gilt $f \cdot g \in 0$.

Wir haben oben gesehen, daß $h^{-1}(0)$ ein Ideal ist. Bildet man zu dem Ideal $\Im$ das Element

$$g := \bigcup_{f \in \Im} f,$$

dann gilt $g \geq f$ für alle $f \in \Im$. Wir gewinnen damit eine zweite Charakterisierung der Ideale.

Lemma 7. Zu jedem Ideal $\Im$ gibt es ein Element g, so daß $\Im = g \cdot \mathcal{B}$ ist. Umgekehrt gilt: Für jedes g ist $g \cdot \mathcal{B}$ ein Ideal von $\mathcal{B}$.

Beweis. Zunächst sieht man leicht, daß $g \cdot \mathcal{B}$ ein Ideal ist. Wegen $g \cdot 1 \geq g \cdot f$ für jedes $f \in \mathcal{B}$ folgt auch, daß g größtes Element in $g \cdot \mathcal{B}$ ist. Darüberhinaus enthält $g \cdot \mathcal{B}$ auch jedes Element $f \in \mathcal{B}$, für das $f \leq g$ gilt; denn es folgt aus $f \leq g$, daß $f = f \cdot g$ gilt, d.h., daß $f \in g \cdot \mathcal{B}$ ist. Ist $\Im$ ein Ideal aus $\mathcal{B}$ und g das maximale Element von $\Im$, dann gilt $g \cdot \mathcal{B} \subset \Im$ und wegen $1 \in \mathcal{B}$ gilt nun auch $g \cdot \mathcal{B} = \Im$. □

Da sich jedes Ideal $\Im$ von $\mathcal{B}$ durch ein Element $g \in \mathcal{B}$ erzeugen läßt, schreiben wir anstelle von $\Im$ meist (r), wenn r das maximale Element von $\Im$ ist.

Wir zeigen nun, daß es zu jedem Ideal (r) von $\mathcal{B}$ eine boolesche Algebra $\mathcal{B}'$ und einen Homomorphismus $h : \mathcal{B} \to \mathcal{B}'$ gibt, so daß $h^{-1}(0) = (r)$ ist. Hierzu definieren wir die folgende Kongruenzrelation:

$$g_1 \text{ heißt kongruent } g_2 \textit{ modulo } (r)$$

genau dann, wenn $g_1 \cdot \overline{r} = g_2 \cdot \overline{r}$ ist. Hierfür schreiben wir $g_1 \equiv g_2(r)$. Nun setzen wir weiter

$$[g]_r := \{f \in \mathcal{B} | f \equiv g(r)\}$$

und definieren für $f, g \in \mathcal{B}$ und $* \in \{\cup, \cdot\}$

$$[f]_r * [g]_r := [f * g]_r \text{ und } \overline{[f]}_r = [\overline{f}]_r.$$

Sind $f_1, f_2 \in [f]_r$, dann gilt wegen

$$(f_1 * g) \cdot \overline{r} = (f_1 \cdot \overline{r}) * (g \cdot \overline{r}) = (f_2 \cdot \overline{r}) * (g \cdot \overline{r}) = (f_2 * g) \cdot \overline{r},$$

daß die Operation „$*$“ von der Auswahl der Repräsentanten der Klasse unabhängig ist.

Wegen

$$1 \cdot \overline{r} = (f_1 \cup \overline{f}_1) \cdot \overline{r} = f_1 \cdot \overline{r} \cup \overline{f}_1 \cdot \overline{r} = f_2 \cdot \overline{r} \cup \overline{f}_1 \cdot \overline{r}$$

folgt

$$\overline{r} \cdot \overline{f}_2 = \overline{f}_1 \cdot \overline{f}_2 \cdot \overline{r}.$$

Ebenso folgt

$$\overline{r} \cdot \overline{f}_1 = \overline{f}_1 \cdot \overline{f}_2 \cdot \overline{r}.$$

Aus beiden Beziehungen folgt $\overline{r} \cdot \overline{f}_1 = \overline{r} \cdot \overline{f}_2$, d.h. $\overline{f}_1 \equiv \overline{f}_2(r)$.

Wir setzen $\mathcal{B}/r := \{[g]_r | g \in \mathcal{B}\}$ und haben damit eine Algebra $(\mathcal{B}/r, \cup, \cdot, -)$ auf eindeutige Weise definiert. Die Abbildung $h : \mathcal{B} \to \mathcal{B}/r$, die durch $h(f) := [f]_r$ definiert wird, ist ein Homomorphismus, wie die vorausgegangenen Rechnungen zeigen. Also ist $\mathcal{B}/r$ eine boolesche Algebra.

Nun sieht man, daß $h^{-1}(0) = \{g \in \mathcal{B} | g \cdot \overline{r} = 0\}$ ist. Also ist $g \leq r$ für $g \in h^{-1}(0)$, was äquivalent ist zu $h^{-1}(0) = (r)$. Wir fassen unser Resultat in dem folgenden Satz zusammen:

Satz 4. *Ist $\mathcal{B}$ eine boolesche Algebra und ist $r \in \mathcal{B}$, dann ist $\mathcal{B}/r$ eine boolesche Algebra. Die Abbildung $f \to [f]_r$ definiert einen Homomorphismus $h : \mathcal{B} \to \mathcal{B}/r$ und es gilt $h^{-1}(0) = (r)$. Ist $h : \mathcal{B} \to \mathcal{B}'$ ein Homomorphismus, dann ist $h^{-1}(0)$ ein Ideal. Ist $(r) = h^{-1}(0)$ und ist h surjektiv, dann ist $\mathcal{B}/r$ isomorph zu $\mathcal{B}'$.*

Wir veranschaulichen diesen Sachverhalt, indem wir ihn für $\mathcal{B} = S_n$ interpretieren. In diesem Fall ist $f : \mathbb{B}^n \to \mathbb{B}$. Das Ideal $\{f \in S_n | f \leq r\}$ besteht aus der Menge der Abbildungen $f \in S_n$, für die $f(\xi) = 0$ für $r(\xi) = 0$ gilt. Setzen wir $D_r := r^{-1}(0)$, dann gilt für $f_1 \cdot \overline{r} = f_2 \cdot \overline{r}$, daß $f_1 | D_r = f_2 | D_r$. Somit ergibt sich

$$S_n/r \cong S(D_r).$$

Man erhält also den Quotienten S_n/r, indem man $D = \mathbb{B}^n - r^{-1}(1)$ bildet und die Funktionen aus S_n auf D einschränkt. Diesen Sachverhalt werden wir bei der Behandlung spezieller Funktionen verwenden.

2.5 Prüfung boolescher Operationen

Zur Rechenkontrolle beim Rechnen mit ganzen rationalen Zahlen verwendet man bei Dezimaldarstellungen die Neuner- oder Elferprobe. Es handelt sich dabei um eine Wiederholung der Rechnung in den Restklassen modulo 9 bzw. modulo 11.

Das dahinterstehende allgemeine Prinzip kann man wie folgt definieren:

Sei $\mathcal{A} = (A, \tau_1, \ldots, \tau_k)$ eine Algebra mit den Operationen $\tau_i : A^{n_i} \to A$, und ist $\mathcal{A}' = (A', \tau_1', \ldots, \tau_k')$ eine zweite solche Algebra und ist

$$h : A \to A'$$

ein Homomorphismus, d.h. gilt

$$h(\tau_i(a_1, \ldots, a_{n_i})) = \tau_i'(h(a_1), \ldots, h(a_{n_i})),$$

dann kann man die korrekte Ausführung von τ_i testen, indem man $h(a_1)$, $\dots$, $h(a_{n_i})$, $h(\tau_i(a_1, \dots, a_{n_i}))$ und $\tau_i'(h(a_1), \dots, h(a_{n_i}))$ berechnet und prüft, ob die obige Relation erfüllt ist. Eine solche Prüfung ist besonders dann interessant, wenn

1. A' kleiner als A ist (man kann o.B.d.A. annehmen, daß $h(A) = A'$ ist).

   und

2. die Prüfung für alle $(a_1, \dots, a_{n_i})$ gleich gut ist.

Im Beispiel der ganzen Zahlen wird das durch Homomorphismen von $\mathbb{Z}$ auf den Ring $\mathbb{Z}_m$ geleistet. Im Falle der booleschen Algebra erfüllen diese Prüfungen die Forderung 2 nicht, wenn $\sharp A' \lneq \sharp A$ ist. Das folgt daraus, daß für Atome $a \neq b$ entweder $h(a) \neq h(b)$ oder $h(a) = h(b) = 0$ folgt.

Ist also $h : S(D) \to S(D')$ ein surjektiver Homomorphismus, dann wird eine Teilmenge der Atome von $S(D)$ bijektiv auf $A(S(D'))$ abgebildet und der Rest auf die 0. Also werden einige Atome spezifisch getestet und andere so gut wie gar nicht.

3 Ausnutzung von Symmetrien boolescher Algebren zur Schaltkreissynthese

Wir entwickeln in diesem Abschnitt die Verbindung zwischen dem Verband boolescher Unteralgebren und dem Verband von Gruppen, die die Unteralgebren elementweise festlassen. Anschließend behandeln wir als Beispiele die Addition, Multiplikation und die total symmetrischen Funktionen.

3.1 Grundlegende Definitionen

Sei $\mathcal{B}$ eine boolesche Algebra und

$$G(\mathcal{B}) := \{h : \mathcal{B} \to \mathcal{B} \mid h \quad \text{Automorphismus}\}.$$

$G(\mathcal{B})$ ist eine Gruppe bezüglich der Hintereinanderausführung der Abbildungen.

Lemma 8. Es gilt für endliche boolesche Algebren $\mathcal{B}$:
$h \in G(\mathcal{B}) \Longleftrightarrow$ für alle Atome a von $\mathcal{B}$ gilt: $h(a)$ ist Atom von $\mathcal{B}$

Beweis. Da h ein Homomorphismus ist, gilt $h(0) = 0$ und $(h(a) \leq h(f)$ für $a \leq f$.

(1) Da h injektiv ist, ist $h^{-1}(0) = 0$ und also $h(a)$ Atom von $\mathcal{B}$. Da h surjektiv ist, permutiert h die Atome von $\mathcal{B}$.

(2) Ist $h(a) \neq 0$ für alle Atome von $\mathcal{B}$, dann ist $h^{-1}(0) = 0$. Nach Lemma 6 ist h injektiv.

□

Sei nun $A(\mathcal{B})$ die Menge der Atome von $\mathcal{B}$ und $\mathfrak{S}(A(\mathcal{B}))$ die Permutationsgruppe von $A(\mathcal{B})$. $\cong$ bezeichne die Isomorphie von Gruppen und Algebren.

Lemma 9. Es gilt $G(\mathcal{B}) \cong \mathfrak{S}(A(\mathcal{B}))$.

Beweis.

1. Ist h bijektiv und $h(A(\mathcal{B})) = A(\mathcal{B})$, dann ist die Einschränkung $h|A(\mathcal{B})$ von h auf $\mathcal{A}(\mathcal{B})$ eine Permutation; es gilt also

$$h|A(\mathcal{B}) \in \mathfrak{S}(A(\mathcal{B})).$$

2. Ist $h|A(\mathcal{B}) = g|A(\mathcal{B})$ für $h, g \in G(\mathcal{B})$, dann gilt aufgrund des Darstellungssatzes

$$f = \bigcup_{a \in A(\mathcal{B})} (f \cdot a)$$

$h = g$.

3. Für $h, g \in G(\mathcal{B})$ gilt $(h \circ g)|A(\mathcal{B}) = (h|A(\mathcal{B})) \circ (g|A(\mathcal{B}))$.

Aus 1, 2 und 3 folgt, daß $h|A(\mathcal{B})$ einen Isomorphismus zwischen $G(\mathcal{B})$ und $\mathfrak{S}(A(\mathcal{B}))$ definiert. □

Wir betrachten nun Untergruppen von $G(\mathcal{B})$, die dadurch charakterisiert sind, daß ihre Elemente vorgegebene Elemente von $\mathcal{B}$ festlassen.

Definition 6. Für $E \subset \mathcal{B}$ definieren wir

$$G(\mathcal{B}, E) := \{h \in G(\mathcal{B}) | h(e) = e \text{ für } e \in E\}.$$

Lemma 10.

1. $G(\mathcal{B}, E)$ ist eine Untergruppe von $G(\mathcal{B})$.

2. $G(\mathcal{B}) = G(\mathcal{B}, \{0\})$.

3. Für $E \subset \mathcal{B}$ gilt $G(\mathcal{B}, E) = G(\mathcal{B}, \langle E \rangle)$.

Beweis. 1 und 2 gelten offensichtlich. Der Beweis für 3 ergibt sich wie folgt: Aufgrund des Darstellungssatzes haben wir

$$f \in \langle E \rangle \Longrightarrow f = \bigcup_{a \in A(\langle E \rangle)} f \cdot a.$$

Nun gilt: Zu jedem $a \in A(\langle E \rangle)$ gibt es $\varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}$, so daß $a = e_1^{\varepsilon_1} \cdot \ldots \cdot e_k^{\varepsilon_k}$ für $E = \{e_1, \dots, e_k\}$ gilt.

Für $h \in G(\mathcal{B}, E)$ gilt nun

$$\begin{aligned} h(a) &= h(e_1^{\varepsilon_1}) \cdot \ldots \cdot h(e_k^{\varepsilon_k}) \\ &= h(e_1)^{\varepsilon_1} \cdot \ldots \cdot h(e_k)^{\varepsilon_k} = e_1^{\varepsilon_1} \cdot \ldots \cdot e_k^{\varepsilon_k}. \end{aligned}$$

Also die Atome bleiben fest unter den Abbildungen aus $h \in G(\mathcal{B}, E)$.

Hieraus folgt nun

$$h(f) = h(\bigcup_{A(\langle E \rangle)} (f \cdot a)) = \bigcup_{A(\langle E \rangle)} h(f \cdot a) = \bigcup_{A(\langle E \rangle)} f \cdot a = f.$$

Damit gilt also $G(\mathcal{B}, E) \subset G(\mathcal{B}, \langle E \rangle)$.

Die Inklusion in umgekehrter Richtung

$$h \in G(\mathcal{B}, \langle E \rangle) \Longrightarrow h \in G(\mathcal{B}, E)$$

gilt wegen $E \subset \langle E \rangle$. $\square$

Satz 5. *Sind $\mathcal{B}'$ und $\mathcal{B}''$ Unteralgebren von $\mathcal{B}$ und ist $\mathcal{B}' \neq \mathcal{B}''$, dann gilt*

$$\Longrightarrow G(\mathcal{B}, \mathcal{B}') \neq G(\mathcal{B}, \mathcal{B}'').$$

Beweis. Wegen $\mathcal{B}' \neq \mathcal{B}''$ gibt es $f \in \mathcal{B}', f \notin \mathcal{B}''$ oder $f \in \mathcal{B}'', f \notin \mathcal{B}'$.

O.E.d.A. nehmen wir die letztere Alternative an. Nun ist

$$\bigcup_{a \in A(\mathcal{B}')} a = 1.$$

Es gibt also ein $a \in A(\mathcal{B}')$ mit $a \cdot f \neq 0$, aber auch mit $a \cdot f \neq a$, da sonst $f \in \mathcal{B}'$ gelten würde.

Also gibt es $a_1, a_2 \in A(\mathcal{B})$ mit

$$a_1 \leq a \cdot f, \ a_2 \leq a \cdot \overline{f}.$$

Nun definieren wir die Permutation $\tilde{h} : A(\mathcal{B}) \to A(\mathcal{B})$ durch

$$\tilde{h}(a) = \begin{cases} a & \text{für} \quad a \neq a_1, a \neq a_2 \\ a_2 & \text{für} \quad a = a_1 \\ a_1 & \text{für} \quad a = a_2. \end{cases}$$

Es gilt:

$$\tilde{h}(f) = f \quad \text{für} \quad f \in \mathcal{B}',$$

da $h(a) = a$ ist für alle Atome aus $\mathcal{B}'$.

Also haben wir

$$\tilde{h} \in G(\mathcal{B}, \mathcal{B}').$$

Es ist aber $\tilde{h}(f) \neq f'$, da $a_1 \leq f$, aber $\tilde{h}(a_1) = a_2 \leq \overline{f}$. Also ist $\tilde{h} \notin G(\mathcal{B}, \mathcal{B}'')$. Also gilt $G(\mathcal{B}, \mathcal{B}') \neq G(\mathcal{B}, \mathcal{B}'')$. $\square$

Interpretation des Satzes:
Wir bezeichnen mit $G(\mathcal{B}, -)$ die Abbildung, die $\mathcal{B}' \subset \mathcal{B}$ die Gruppe $G(\mathcal{B}, \mathcal{B}')$ zuordnet. Wir haben gezeigt, daß $G(\mathcal{B}, -)$ die Menge der Unteralgebren $\mathcal{B}' \subset \mathcal{B}$ injektiv in die Menge der Untergruppen von $G(\mathcal{B})$ abbildet.

Wir untersuchen $G(\mathcal{B}, \mathcal{B}')$ etwas näher. Hierzu betrachten wir zunächst

$$E_{(a')} := \{a'\} \cup \{a \in A(\mathcal{B}) \mid a \cdot a' = 0\} \quad \text{für} \quad a' \in A(\mathcal{B}')$$

und

$$G_{a'} := G(\mathcal{B}, E_{(a')}).$$

$G_{a'}$ ist die Automorphismengruppe von $\mathcal{B}$, die a' fest läßt und jedes Atom a von $\mathcal{B}$, das nicht von a' überdeckt wird. D.h., daß $G_{a'}$ eingeschränkt auf $A(\mathcal{B})$ gerade die symmetrische Gruppe $\mathfrak{S}(\{a \in A(\mathcal{B}) \mid a \cdot a' = a\})$ ist. Hieraus ergibt sich der

Satz 6. $G(\mathcal{B}, \mathcal{B}') \cong X_{a' \in A(\mathcal{B}')} G_{a'}$;
hierin bezeichnet „X“ das direkte Produkt der Gruppen.

Beweis. Ist $h \in G(\mathcal{B}, \mathcal{B}')$, dann gilt für alle $f \in \mathcal{B}' : h(f) = f$. Also gilt für $a < f$ auch $h(a) < f$. Also permutiert h die Atome von $\mathcal{B}$, die unter Elementen von $\mathcal{B}'$ liegen, untereinander. Insbesondere gilt das für die Atome von $\mathcal{B}'$.

Umgekehrt induziert jede Permutation, die nur solche Atome von $\mathcal{B}$ permutiert, die unter dem gleichen Atom von $\mathcal{B}'$ liegen, einen Automorphismus auf $G(\mathcal{B}, \mathcal{B}')$. □

Hieraus ergibt sich, daß nicht alle Untergruppen von $G(\mathcal{B})$ als Gruppen $G(\mathcal{B}, \mathcal{B}')$ auftreten. $G(\mathcal{B}, -)$ ist also nicht surjektiv.

Wir drehen nun die Betrachtungsweise um, indem wir jeder Untergruppe $G' \subset G(\mathcal{B})$ eine Unteralgebra von $\mathcal{B}$ zuweisen.

Definition 7. $\mathcal{B}(G') := \{f \in \mathcal{B} \mid h(f) = f \quad \text{für alle} \quad h \in G'\}$

Satz 7. *$\mathcal{B}(G')$ ist Unteralgebra von $\mathcal{B}$.*

Beweis. Seien $f, g \in \mathcal{B}(G')$, dann gilt für $h \in G(\mathcal{B})$:

$$\begin{aligned} h(f \cup g) &= h(f) \cup h(g), \\ h(f \cdot g) &= h(f) \cdot h(g), \\ h(\overline{f}) &= \overline{h(f)}, \end{aligned}$$

woraus $h(f \cup g) = f \cup g$, $h(f \cdot g) = f \cdot g$, $h(\overline{f}) = \overline{f}$ folgt. Also ist $\mathcal{B}(G')$ abgeschlossen unter den Anwendungen der Operationen der booleschen Algebra. □

Satz 8. $\mathcal{B}(G(\mathcal{B},\mathcal{B}')) = \mathcal{B}'$.

Beweis. 1. Aus der Definition von $G(\mathcal{B},\mathcal{B}')$ folgt $\mathcal{B}' \subset \mathcal{B}(G(\mathcal{B},\mathcal{B}'))$.
2. Aus der Injektivität der Abbildung $G(\mathcal{B},-)$ folgt $\mathcal{B}' = \mathcal{B}(G(\mathcal{B},\mathcal{B}'))$. $\square$

Offensichtlich gilt der

Satz 9.

$$\begin{aligned} \mathcal{B}',\mathcal{B}'' \subset \mathcal{B} \textit{ und } \mathcal{B}' \subsetneq \mathcal{B}'' &\implies G(\mathcal{B},\mathcal{B}') \supsetneq G(\mathcal{B},\mathcal{B}'') && (6)\\ G',G'' \subset G, G' \subset G'' &\implies \mathcal{B}(G'') \subset \mathcal{B}(G'). && (7)\end{aligned}$$

Die Mengen der Unteralgebren und Untergruppen von $\mathcal{B}$ bzw. G bilden Verbände. $\mathcal{B}'(-)$ bildet den Untergruppenverband *surjektiv* auf den Unteralgebrenverband von $\mathcal{B}$ ab. $G(\mathcal{B},-)$ bildet den Algebrenverband auf den Untergruppenverband injektiv ab. Diese Abbildungen sind antihomomorph bezüglich der Verbandsstrukturen.

Definition 8. Für $\mathcal{B}',\mathcal{B}'' \subset \mathcal{B}$ und $G',G'' \subset G$ definieren wir

$$\mathcal{B}' + \mathcal{B}'' := \langle \mathcal{B}' \cup \mathcal{B}'' \rangle,\ G' + G'' := \langle G' \cup G'' \rangle.$$

Satz 10. *Es gelten die Aussagen 8, 9, 10 und 11.*

$$G(\mathcal{B},\mathcal{B}'+\mathcal{B}'') = G(\mathcal{B},\mathcal{B}) \cap (\mathcal{B},\mathcal{B}''), \qquad (8)$$

$$\mathcal{B}(G'+G'') = \mathcal{B}(G') \cap \mathcal{B}(G''). \qquad (9)$$

$$\begin{aligned} G(\mathcal{B},\mathcal{B}' \cap \mathcal{B}'') &\supset G(\mathcal{B},\mathcal{B}') + G(\mathcal{B},\mathcal{B}''); && (10)\\ \textit{es gibt } \mathcal{B},\mathcal{B}',\mathcal{B}'', \textit{so daß } G(\mathcal{B},\mathcal{B}' \cap \mathcal{B}'') &\neq G(\mathcal{B},\mathcal{B}') + G(\mathcal{B},\mathcal{B}'') \textit{ gilt.} \end{aligned}$$

$$\begin{aligned} \mathcal{B}(G' \cap G'') &\supset \mathcal{B}(G') + \mathcal{B}(G''); && (11)\\ \textit{es gibt } G',G'', \textit{so daß } \mathcal{B}(G' \cap G'') &\neq \mathcal{B}(G') + \mathcal{B}(G'') \textit{ ist.} \end{aligned}$$

Beweis.

Ad 8: Ist $g \in G(\mathcal{B},\mathcal{B}'+\mathcal{B}'')$, dann ist jedes Element von $\mathcal{B}'$ und jedes Element von $\mathcal{B}''$ invariant unter g. Also gilt $g \in G(\mathcal{B},\mathcal{B}') \cap G(\mathcal{B},\mathcal{B}'')$. Ist umgekehrt g Element dieses Durchschnittes, dann ist jedes Element von $\mathcal{B}' \cup \mathcal{B}''$ invariant unter g und damit nach Beobachtung 10 auch jedes Element aus $\langle \mathcal{B}' \cup \mathcal{B}'' \rangle = \mathcal{B}' + \mathcal{B}''$. Aus beiden Feststellungen folgt die Behauptung 8.

Ad 9: Aus $f \in \mathcal{B}(G'+G'')$ folgt $f \in \mathcal{B}(G'')$ und $f \in \mathcal{B}(G')$. Ist umgekehrt $f \in \mathcal{B}(G') \cap \mathcal{B}(G'')$, dann ist f sowohl unter G' als auch G'' invariant, sodaß f auch unter der durch G' und G'' erzeugten Gruppe $G' + G'$ invariant ist.

Ad 10: $h \in G(\mathcal{B}, \mathcal{B}') + G(\mathcal{B}, \mathcal{B}'')$ läßt jedes Element $f \in \mathcal{B}' \cap \mathcal{B}''$ fest. Also ist $h \in G(\mathcal{B}, \mathcal{B}' \cap \mathcal{B}'')$.

Zum Beweis des zweiten Teiles der Behauptung betrachten wir $\mathcal{B} = S_{2n} = \langle x_1, \ldots, x_n, y_1, \ldots, y_n \rangle, \mathcal{B}' = \langle x_1, \ldots, x_n \rangle$ und $\mathcal{B}'' = \langle y_1, \ldots, y_n \rangle$. Es ist $\mathcal{B}' \cap \mathcal{B}'' = \{0, 1\}$, d.h. es gilt $G(\mathcal{B}, \mathcal{B}' \cap \mathcal{B}'') = G(\mathcal{B})$.

Nun gilt weiter $G(\mathcal{B}, \mathcal{B}') \cong G(\mathcal{B}'')$ und $G(\mathcal{B}, \mathcal{B}'') \cong G(\mathcal{B}')$. Hieraus folgt $G(\mathcal{B}, \mathcal{B}') + G(\mathcal{B}, \mathcal{B}'') \cong G(\mathcal{B}') \times G(\mathcal{B}'') \neq G(\mathcal{B})$, was zu zeigen war.

Ad 11: $f \in \mathcal{B}(G') + \mathcal{B}(G'')$ ist invariant unter allen Transformationen, die sowohl in G' als auch in G'' liegen. Also gilt $f \in \mathcal{B}(G' \cap G'')$. Zum Beweis des zweiten Teiles des Satzes 10, 11 betrachten wir die durch die Atome a_1, a_2, a_3, a_4, a_5 erzeugte boolesche Algebra $\mathcal{B}$. Wir definieren zwei zyklische Gruppen $G' = \langle s_1 \rangle, G'' = \langle s_2 \rangle; s_1$ und s_2 werden durch die folgenden Diagramme definiert

$$s_1 : a_1 \to a_2 \to a_3 \to a_4 \to a_1, \quad a_5 \to a_5;$$

$$s_2 : a_1 \to a_3 \to a_2 \to a_4 \to a_1, \quad a_5 \to a_5.$$

Man erhält

$$\mathcal{B}(G') = \langle a_1 \vee a_2 \vee a_3 \vee a_4 \rangle = \mathcal{B}(G'').$$

Also ist $\mathcal{B}(G') + \mathcal{B}(G'') = \mathcal{B}(G') \neq \mathcal{B}$.

Aber es gilt $\mathcal{B}(G' \cap G'') = \mathcal{B}(id) = \mathcal{B}$.

□

Wir werden im folgenden zeigen, daß sich aufgrund dieser Beziehung aus der Kenntnis des Untergruppenverbandes $G(\mathcal{B})$ einfache Darstellungen boolescher Funktionen aus $\mathcal{B}'$ gewinnen lassen, wie wir das bereits in der Einleitung zu diesem Kapitel beschrieben haben.

3.2 Berechnung von Erzeugendensystemen für $\mathcal{B}(G')$

Wir gehen davon aus, daß uns ein Erzeugendensystem E von $\mathcal{B}$ gegeben ist. Wir suchen ein Erzeugendensystem für $\mathcal{B}' = \mathcal{B}(G')$, wenn $G' \subset G(\mathcal{B})$ ist.

Hierzu definieren wir für $f \in \mathcal{B}$:

Definition 9. $G'(f) := \bigcup_{h \in G'} h(f)$ heißt *Abschluß* von f unter G'.

Es ist $f' := G'(f)$ invariant unter G'.

Beweis. Ist nämlich $h_1 \in G'$, dann gilt

$$h_1(f') = \bigcup_{h \in G'} (h_1 \circ h)(f) = \bigcup_{h \in G'} h(f) = f'.$$

□

Satz 11. *Ist $A = A(\mathcal{B})$ die Menge der Atome von $\mathcal{B}$ und $\mathcal{B}' = \mathcal{B}(G')$, dann ist*

$$A'(\mathcal{B}') := \{G'(a) \mid a \in A(\mathcal{B})\} = A(\mathcal{B}').$$

Man erhält also die Atome von $\mathcal{B}'$, indem man den Abschluß der Atome von $\mathcal{B}$ unter G' bildet.

Beweis. Ist $f \in \mathcal{B}'$, dann gilt

$$f = \bigcup_{a \in A} f \cdot a = \bigcup_{a \in A} \alpha_a \cdot a \text{ mit } \alpha_a = \begin{cases} 0 & \text{für } f \cdot a = 0 \\ 1 & \text{sonst.} \end{cases}$$

Nun gilt

$$\begin{aligned} f &= G'(f) = \bigcup_{a \in A} \bigcup_{h \in G'} \alpha_a \cdot h(a) \\ &= \bigcup_{a \in A} \alpha_a \cdot \bigcup_{h \in G'} h(a) = \bigcup_{a \in A} \alpha_a G'(a) \\ &= \bigcup_{a \in A'} \alpha_{a'} \cdot a' \qquad \text{mit } \alpha_{a'} = \bigcup_{a \cdot a' \neq 0} \alpha_a. \qquad (*) \end{aligned}$$

Also ist A' ein Erzeugendensystem von $\mathcal{B}'$. Sind $a' \neq a'' \in A'$, dann gilt $a' \cdot a'' = 0$.
Hieraus und aus $(*)$ folgt, daß $A' = A(\mathcal{B}')$ gilt, was wir behauptet haben.

□

3.3 G-invariante Fortsetzungen von Funktionen

Wir betrachten die Frage, ob $f \in S(D)$ zu einer G-invarianten Abbildung $f' \in S_n$ fortgesetzt werden kann. Die Motivation dieser Frage ergibt sich aus der Tatsache, daß jede Realisierung einer booleschen Funktion $f \in S(D), D \subset \mathbb{B}^n$ stets Realisierung einer Funktion $f' \in S_n$ ist. Allgemeiner handelt es sich nicht um die Realisierung *einer* solchen Funktion, sondern der simultanen Realisierung von mehreren Funktionen, sodaß der Übergang zu der von diesen Funktionen erzeugten Unteralgebra angemessen ist.

Wir gehen also von einer Unteralgebra $\mathcal{B}' \subset S(D)$ aus und fragen zunächst nach einer Gruppe, die $\mathcal{B}'$ elementweise fest läßt. Es mag sein, daß es eine solche nichtriviale Gruppe $G' = G(S(D), \mathcal{B}')$ gibt. Es kann aber auch sein, daß es Fortsetzungen f^* der Funktionen $f \in S(D)$ auf ganz $\mathbb{B}^n$ gibt, so daß die zu der von diesen Funktionen erzeugten Algebra $\mathcal{B}^*$ gehörige Gruppe $G^* = G(S_n, \mathcal{B}^*)$ wesentlich größer als G' ist. Im Interesse, das die gesamte Untersuchung der Invarianzgruppen bestimmt, sind wir daran interessiert G^* möglichst groß zu machen.

Zur Konstruktion solcher maximalen Gruppen G^* verfolgen wir die Idee, aus kleineren, uns bereits bekannten Gruppen G_1, G_2, für die wir geeignete Fortsetzungen kennen, größere solche Gruppen zu konstruieren. Hierbei denken wir natürlich sofort an $G_1 + G_2$. Im allgemeinen wird aber $G_1 + G_2$ zu groß geraten, so daß man in $G_1 + G_2$ geeignete maximale Untergruppen G^* wird finden wollen.

Wir gehen zunächst von $S(D), D \subset \mathbb{B}^n, D \neq \mathbb{B}^n$ und einer Gruppe $G' \subset G(S_n)$ aus. Man erinnere sich hier an Lemma 9, das es uns erlaubt, zwischen Automorphismen und Invarianzgruppen zu wechseln.

Definition 10. $f \in S(D)$ heißt G'-invariant fortsetzbar genau dann, wenn für jedes $\xi \in D$ und jedes $g \in G'$ $f(\xi) = f(g(\xi))$ gilt, falls $g(\xi) \in D$ ist.

Lemma 11. Ist $f \in S(D)$ G'-invariant fortsetzbar und ist $G'(D) = \{\xi | \text{Es gibt } g \in G' \text{ mit } g(\xi) \in D\}$, dann gibt es eine Fortsetzung f' von f auf $G'(D)$, die G'-invariant ist.

Beweis. Definiere

$$f'(\xi) := \begin{cases} f(\xi) & \text{für} \quad \xi \in D \\ f(\xi') & \text{für} \quad \xi \notin D \text{ und } \exists g \in G \text{ mit } g(\xi) = \xi' \in D \end{cases}$$

f' ist wohldefiniert. Gibt es nämlich zwei Automorphismen $g_1, g_2 \in G'$ mit $g_1(\xi) = \xi_1 \in D$ und $g_2(\xi) = \xi_2 \in D$, dann gilt $g_2(g_1^{-1}(\xi_1)) = \xi_2$. Hieraus folgt $f(\xi_1) = f(\xi_2)$, da wir vorausgesetzt haben, daß f G'-invariant fortsetzbar ist. □

Korollar 6. *Unter den Voraussetzungen von Lemma 11 ist f auf ganz $\mathbb{B}^n$ G'-invariant fortsetzbar.*

Beweis. Setze zunächst f wie im Beweis zu Lemma 11 auf $G'(D)$ fort. Dann definiere $f'(\xi) = 1$ für $\xi \in \mathbb{B}^n - G'(D)$. □

Satz 12. *Sei $h : S_n \to S(D)$ der natürliche Homomorphismus und sei G' Untergruppe der Permutationsgruppe vom $\mathbb{B}^n$. Die Elemente einer Unteralgebra $\mathcal{B}' \subset S(D)$ sind genau dann G'-invariant auf $\mathbb{B}^n$ fortsetzbar, wenn $h(\mathcal{B}^*) = \mathcal{B}'$ für $\mathcal{B}^* = S_n(G')$ gilt.*

Beweis. Ist $h(\mathcal{B}^*) = \mathcal{B}'$, dann gibt es zu jedem $f \in \mathcal{B}'$ ein $f^* \in \mathcal{B}^*$ mit $h(f^*) = f$. Da f^* G'-invariant ist, folgt, daß f G'-invariant fortsetzbar ist. Sei nun umgekehrt $\mathcal{B}'$ gegeben. Wir definieren $\mathcal{B}^* = \{f' \in S_n | f'$ ist G'-invariante Fortsetzung von $f\}$. $\mathcal{B}^*$ bildet eine Boolesche Algebra von G'-invarianten Funktionen. Es ist $h(\mathcal{B}^*) = \mathcal{B}'$, wie aus Korollar 6 folgt. Da $\mathcal{B}^*$ auch jede G'-invariante Funktion von S_n enthält, ist $\mathcal{B}^* = S_n(G')$. □

Sei nun $\mathcal{B}'$ G_1- und G_2-invariant fortsetzbar. Aus Satz 10 folgt

$$S_n(G_1 + G_2) = S_n(G_1) \cap S_n(G_2).$$

Es ist also unklar, ob $h(S_n(G_1 + G_2)) = \mathcal{B}'$ ist. Besteht Gleichheit, dann haben wir eine größere Gruppe $\tilde{G}$ gefunden, die eine $\tilde{G}$-invariante Fortsetzung gestattet. Besteht Ungleichheit, dann stellt sich die Aufgabe maximale Untergruppen $\tilde{G} \subset G_1 + G_2$ zu finden, so daß $\mathcal{B}'$ $\tilde{G}$-invariant fortsetzbar ist. Wir setzen uns hier nicht mit der Klassifikation der Komplexität dieser Frage auseinander. *C. Scholl* hat gezeigt, daß dieses Problem NP-vollständig ist, so daß es sich also um ein schwieriges Problem handelt.

Satz 13. *Sind $\mathcal{B}_1, \mathcal{B}_2$ boolesche Unteralgebren von $\mathcal{B}$ mit $\mathcal{B}_1 \cap \mathcal{B}_2 = \{0,1\}$ und $\mathcal{B}_i' \subset \mathcal{B}_i$ und ist $A(\mathcal{B}_i) \leq A(\mathcal{B}_i')$ für $i = 1, 2$, dann gilt*

$$G(\mathcal{B}_1 + \mathcal{B}_2, \mathcal{B}_1' + \mathcal{B}_2') = G(\mathcal{B}_1, \mathcal{B}_1') + G(\mathcal{B}_2, \mathcal{B}_2').$$

Beweis. Aus Satz 10 folgt

$$\begin{aligned} G(\mathcal{B}_1 + \mathcal{B}_2, \mathcal{B}_1' + \mathcal{B}_2') &= G(\mathcal{B}_1 + \mathcal{B}_2, \mathcal{B}_1') \cap G(\mathcal{B}_1 + \mathcal{B}_2, \mathcal{B}_2') && (12) \\ &= (G(\mathcal{B}_1, \mathcal{B}_1') + G(\mathcal{B}_2)) \cap (G(\mathcal{B}_2, \mathcal{B}_2') + G(\mathcal{B}_1)) && (13) \end{aligned}$$

13 folgt aus 12 aufgrund der Voraussetzung über die Atome.
Offensichtlich ist $G(\mathcal{B}_1, \mathcal{B}_1') + G(\mathcal{B}_2, \mathcal{B}_2')$ in (13) enthalten. Ist nun umgekehrt g Element von (13) dann gilt

$$g \in G(\mathcal{B}_1, \mathcal{B}_1') + G(\mathcal{B}_2) \text{ und } g \in G(\mathcal{B}_2, \mathcal{B}_2') + G(\mathcal{B}_1).$$

Also läßt g die Elemente von $\mathcal{B}_1'$ fest und führt $\mathcal{B}_2$ in sich über. Ebenso folgt, daß g $\mathcal{B}_2'$ fest läßt und die Elemente von $\mathcal{B}_1$ in sich überführt. Also läßt g, soweit es auf $\mathcal{B}_1$ wirkt, $\mathcal{B}_1'$ fest und soweit es auf $\mathcal{B}_2$ wirkt, die Elemente von $\mathcal{B}_2'$. Also läßt sich g durch $G(\mathcal{B}_1, \mathcal{B}_1')$ und $G(\mathcal{B}_2, \mathcal{B}_2')$ erzeugen. □

Wir wenden die entwickelten Konzepte an, um Darstellungen für einige spezielle Funktionen zu berechnen.

4 Spezielle Funktionen

4.1 Addition n-stelliger Dualzahlen

Es soll also eine Funktion

$$ad_n : \mathbb{B}^{2n} \to \mathbb{B}^{n+1}$$

dargestellt werden, die zwei n-stelligen Dualzahlen $[\xi]$ und $[\eta]$ ihre Summe $[\zeta]$ zuordnet; hierin verwenden wir die Bezeichnung

$$[\xi] := \sum_{i=1}^{n} \xi_i 2^{n-i}.$$

Wir haben also

$$ad_n(\xi, \eta) = [\xi] + [\eta].$$

Sind $P_i : \mathbb{B}^{n-1} \longrightarrow \mathbb{B}$ für $i = 0, \ldots, n$ die Projektionen auf die i-te Komponente, dann setzen wir

$$e_i := P_i \circ ad_n \qquad \text{für } i = 0, \ldots, n.$$

Anstelle von e_0 schreiben wir manchmal auch c, das sich von „carry" ableitet. Wir setzen weiter

$$\Delta_n := \langle e_0, e_1, \ldots, e_n \rangle \text{ und } \Gamma_n := \langle e_1, \ldots, e_n \rangle.$$

Es ist also $\Delta_n = \langle e_0 \rangle + \Gamma_n$.

$$G_n := \{g : \mathbb{B}^{2n} \longrightarrow \mathbb{B}^{2n} \mid [ad_n(g(\xi, \eta)] = [\xi] + [\eta]\}$$

ist eine Gruppe von Abbildungen, die Δ_n elementweise fest läßt.

Unter Verwendung des in Lemma 9 definierten *natürlichen* Isomorphismus zwischen $G(\mathcal{B})$ und der Permutationsgruppe auf $A(\mathcal{B})$ identifizieren wir G_n mit der dadurch bestimmten Untergruppe in $G(S_{2n})$. In diesem Sinne gilt $G_n \subset G(S_{2n}, \Delta_n)$, da jeder Automorphismus $g \in G_n$ jedes Element aus Δ_n fest läßt. Es gilt auch $G(S_{2n}, \Delta_n) \subset G_n$, da G_n jeden Automorphismus enthält, der $[\xi] + [\eta]$ fest läßt. Also haben wir $G_n = G(S_{2n}, \Delta_n)$.

4.1.1 Die Atome von Δ_n

Wir definieren nun

$$a_i := G_n(\xi, \eta) \quad \text{für } [\xi] + [\eta] = i$$

und $i = 0, \ldots, 2^{n+1} - 2$. Aufgrund der den Erläuterungen nach Satz 21 folgenden geometrischen Veranschaulichung Abbildung 13. bezeichnen wir die a_i auch als zu Δ_n gehörige *Diagonalen.* Nach Satz 11 ist $A(\Delta_n) = \{a_i \mid i = 0, \ldots, 2^{n+1} - 2\}$ die Menge der Atome von Δ_n.
Führen wir die analoge Konstruktion für Γ_n durch, dann erhalten wir

$$G'_n = G(S_{2n}, \Gamma_n) = \{g \in \Delta_n \mid [ad_n(g(\xi, \eta))] = [\xi] + [\eta] \textit{ modulo } 2^n\}.$$

Man erhält für die Atome $A(\Gamma_n) = \{b_0, \ldots, b_{2^n-1}\}$

$$b_i = a_i \vee a_{i+2^n} \quad \text{für } i = 0, \ldots, 2^n - 1,$$

wenn man $a_{2^{n+1}-1} = 0$ setzt. Das folgt aus $(\xi', \eta') \in G'_n(\xi, \eta)$ für $[\xi'] + [\eta'] = [\xi] + [\eta]$ *modulo* 2^n.

Seien nun $x' := (x_1, \ldots, x_n)$, $y' := (y_1, \ldots, y_n)$, $\tilde{x} := (x_{n+1}, \ldots, x_{n+m})$, $\tilde{y} = (y_{n+1}, \ldots, y_{n+m})$. Weiter setzen wir $x := (x', \tilde{x})$ und $y := (y', \tilde{y})$. $\Delta(x', y')$, $\Delta(\tilde{x}, \tilde{y})$ und $\Delta(x, y) = \Delta_{n+m}$ beziehen sich auf die Algebren $\langle x, y\rangle, \langle x', y'\rangle$ bzw. $\langle \tilde{x}, \tilde{y}\rangle$. Vermöge der durch die Bezeichnung beschriebenen Einbettung können wir annehmen, daß $\Delta(x', y') \subset \Delta(x, y)$ und $\Delta(\tilde{x}, \tilde{y}) \subset \Delta(x, y)$ gilt. Für $\Delta(x, y)$, $\Delta(x', y')$ und $\Delta(\tilde{x}, \tilde{y})$ schreiben wir auch Δ, Δ' bzw. $\tilde{\Delta}$.

Satz 14. *Unter Verwendung der oben eingeführten Bezeichnung gelten (14) und (15).*

$$\Delta(x, y) \subset \Delta(x', y') + \Delta(\tilde{x}, \tilde{y}), \tag{14}$$

$$\Gamma(x, y) \subset \Gamma(x', y') + \Delta(\tilde{x}, \tilde{y}). \tag{15}$$

Beweis.

Ad (14): Wir führen den Beweis, indem wir zeigen, daß diese Relationen für die Atome der links stehenden Algebren gelten.

Sei also $a_i \in A\left(\Delta(x, y)\right)$, d.h.

$$a_i = \{(\xi, \eta) \mid [\xi] + [\eta] = i\},$$

worin (ξ, η) abkürzend für das Atom $a(\xi, \eta) \in S_{2n}$ steht, das genau für (ξ, η) gleich 1 wird. Nun gilt für $\xi = (\xi', \tilde{\xi})$ und $\eta = (\eta', \tilde{\eta})$

$$[\xi] = [\xi'] \cdot 2^m + [\tilde{\xi}], \quad [\eta] = [\eta'] \cdot 2^m + [\tilde{\eta}]$$

und

$$i = [\xi] + [\eta] = ([\xi'] + [\eta']) \cdot 2^m + [\tilde{\xi}] + [\tilde{\eta}].$$

Setzen wir

$$i' := [\xi'] + [\eta'] \quad \text{und } \tilde{\imath} := [\tilde{\xi}] + [\tilde{\eta}],$$

dann erhalten wir für $2^m - 1 < i < 2^{n+m+1} - 2^m - 1$ die folgenden Möglichkeiten für i' und $\tilde{\imath}$:

Fall 1: $\tilde{\imath} < 2^m - 1 \Longrightarrow i = i' \cdot 2^m + \tilde{\imath},$

Fall 2: $\tilde{\imath} > 2^m - 1 \Longrightarrow i = (i' + 1) \cdot 2^m + \tilde{\imath} - 2^m.$

Fall 3: $\tilde{\imath} = 2^m - 1 \Longrightarrow i = i' \cdot 2^m + 2^m - 1$

Hieraus ergibt sich für die Standarddarstellung $i := i_1 \cdot 2^m + i_2,\ i_2 < 2^m$

$$i_1 = i',\ i_2 = \tilde{\imath} \quad \text{oder} \quad i_1 = i' + 1,\ i_2 = \tilde{\imath} - 2^m,$$

falls $\tilde{\imath} \neq 2^m - 1$. Im Falle $\tilde{\imath} = 2^m - 1$ haben wir nur eine Darstellung.

Wir erhalten also für die Atome $a_i \in \Delta,\ a'_i \in \Delta'$ und $\tilde{a}_i \in \tilde{\Delta}$

$$a_i = a'_{i_1} \cdot \tilde{a}_{i_2} \vee a'_{i_1 - 1} \cdot \tilde{a}_{i_2 + 2^m},$$

wenn wir die Bezeichnung so wählen, daß stets $i_2 < 2^m - 1$ gilt. In dem *Fall 3* und den Fällen $i < 2^m - 1$ und $i > 2^{n+m+1} - 1 - 2^m$ erhalten wir jeweils nur einen Fall. In diesen Fällen ergibt sich also

$$a_i = a'_{i_1} \cdot \tilde{a}_{i_2}.$$

Also liegt a_i für alle i in $\Delta' + \tilde{\Delta}$, woraus $\Delta \subset \Delta' + \tilde{\Delta}$ folgt.

Ad (15): Sei $b_i \in A(\Gamma)$. Wie wir oben bereits eingesehen haben, gilt $b_i = a_i \vee a_{i+2^{n+m}}$. Verwenden wir die im ersten Teil des Beweises eingeführte Bezeichnung, dann haben wir

$$a_i = a'_{i_1} \cdot \tilde{a}_{i_2} \vee a'_{i_1 - 1} \cdot \tilde{a}_{i_2 + 2^m} \quad \text{für } i_2 < 2^m,\ i < 2^{n+m}.$$

Wir erhalten mit dieser Bezeichnung

$$\begin{aligned} i + 2^{n+m} &= j_1 \cdot 2^m + j_2 \\ &\quad \text{mit } j_2 < 2^m,\ 2^{n+m} \leq i + 2^{n+m} < 2^{n+m+1} - 1 \\ &= i_1 \cdot 2^m + i_2 + 2^{n+m} = (i_1 + 2^n) \cdot 2^m + i_2 \end{aligned}$$

Für die zweite Lösung ergibt sich somit

$$i + 2^{n+m} = (j_1 - 1) \cdot 2^m + j_2 + 2^m$$

und also

$$a_{i+2^{n+m}} = a'_{i_1+2^n} \cdot \tilde{a}_{i_2} \vee a'_{i_1-1+2^n} \cdot \tilde{a}_{i_2+2^m}.$$

Hieraus folgt

$$\begin{aligned} a_i \vee a_{i+2^{n+m}} &= (a'_{i_1} \vee a'_{i_1+2^n}) \cdot \tilde{a}_{i_2} \vee (a'_{i_1-1} \vee a'_{i_1-1+2^n}) \cdot \tilde{a}_{i_2+2^m} \\ &= b'_{i_1} \cdot \tilde{a}_{i_2} \vee b'_{i_1-1} \cdot \tilde{a}_{i_2+2^m} \in \Gamma' + \tilde{\Delta}. \end{aligned}$$

Die Diskussion der restlichen Fälle verläuft nach dem gleichen Schema. Also ergibt sich $\Gamma \subset \Gamma' + \tilde{\Delta}$.

□

Korollar 7. *Jedes Atom von Δ_n oder Γ_n läßt sich für $n = 2^k$ in Tiefe $\leq 2 \cdot (1 + \log n)$ mit Kosten $\leq 4 \cdot n^2 - 1$ erzeugen.*

Beweis. Aus der Konstruktion in dem Beweis zu Satz 14 ergibt sich für $n = m$ als Kosten C_{2n} des Atomes $a_i \in \Delta_{2n}$ oder $b_i \in \Delta_{2n}$

$$C_{2n} \leq 4 \cdot C_n + 3, \quad C_1 \leq 3.$$

Für die Tiefe T_{2n} erhalten wir

$$T_{2n} \leq T_n + 2, \quad T_1 \leq 2.$$

Beschränken wir uns auf $n = 2^k,\ k \in \mathbb{N}$, und schreiben wir $\tilde{C}_k$ für C_{2^k}, dann folgt

$$\tilde{C}_k \leq 4 \cdot \tilde{C}_{k-1} + 3, \quad \tilde{C}_0 \leq 3$$

und

$$\tilde{T}_k \leq \tilde{T}_{k-1} + 2, \quad \tilde{T}_0 \leq 2,$$

und weiter

$$\tilde{C}_k \leq 4^k \cdot \tilde{C}_0 + 3 \cdot \sum_{l=0}^{k-1} 4^l = 4 \cdot n^2 - 1 \text{ und } \tilde{T}_k = 2 \cdot (k+1)$$

□

Korollar 8. *Ist* $k_i = x_i \cdot y_i$ *und* $d_i = x_i \vee y_i$ *für* $i = 1, \ldots, n$, *dann gilt* $\Delta_n \subset \langle k_1, d_1, \ldots, k_n, d_n \rangle$.

Beweis. Aus Satz 14 folgt

$$\Delta(x, y) \subset \Delta(x_1, y_1) + \Delta(x_{n-1}, \ldots, x_1, y_{n-1}, \ldots, y_1)$$

und daraus induktiv

$$\Delta(x, y) \subset \Delta(x_1, y_1) + \ldots + \Delta(x_n, y_n).$$

Nun erzeugt k_i, d_i die Algebra $\Delta(x_i, y_i)$. Also ist

$$\Delta(x_1, y_1) + \ldots + \Delta(x_n, y_n) = \langle k_1, d_1, \ldots, k_n, d_n \rangle,$$

woraus die Behauptung folgt. $\square$

Die rekursive Beschreibung der Darstellung der Atome, wie sie sich aus Satz 14 ergibt, hat uns Realisierungen der Atome mit quadratisch in n wachsenden Kosten geliefert. Wir geben nun eine iterative Beschreibung der gleichen Funktionen an, die zeigt, daß sich die Atome mit linear ansteigenden Kosten realisieren lassen. Zur Vereinfachung der Notation und Vermeidung von Fallunterscheidungen erweitern wir die Algebren Δ zu freien Algebren und ersetzen die Indexrechnungen durch Automorphismen auf diesen Algebren.

Δ_n besitzt $2^{n+1}-1$ Atome und ist also nicht frei. Wir adjungieren ein weiteres Atom $a_{2^{n+1}-1}$ zu Δ_n und erhalten so eine freie boolesche Algebra, die wieder mit Δ_n bezeichnet werde.

Nun definieren wir auf $A(\Delta_{n+m}) = \{a_0, \ldots, a_{2^{n+m+1}-1}\}$ die Abbildungen σ und τ, indem wir

$$\sigma(a_i) = a_j \quad \text{für } j + 1 = i \; mod \; 2^{n+m+1}$$

und

$$\tau(a_i) = a_j \quad \text{für } i + 2^m = j \; mod \; 2^{n+m+1}$$

setzen. Offensichtlich sind σ und τ Permutationen der Atome und es gilt $\tau(a) = \sigma^N(a)$ für $N = -2^m$. Die von σ und τ erzeugte Gruppe ist also zyklisch, so daß $\sigma \circ \tau = \tau \circ \sigma$ ist. σ und τ besitzen eine eindeutig bestimmte homomorphe Fortsetzung auf Δ, die wir ebenso bezeichnen.

Weiter schreiben wir $[a] = [\xi] + [\eta]$ für $a(\xi, \eta) = 1$ und $[a_{2^n-1}] = 2^n - 1$.

Wir verwenden diese Notation, um die im Beweis zu Satz 14 abgeleiteten Darstellungen der Atome von Δ_{n+m} umzuschreiben. Zunächst betrachten wir den Fall $2^m - 1 < [a] < 2^{n+m+1} - 2^m - 1$. Wir haben in diesen Fällen

$$a = a' \cdot \tilde{a} \vee \sigma(a') \cdot \tau(\tilde{a}) \quad \text{für } [\tilde{a}] < 2^m - 1$$

und

$$a = a' \cdot \tilde{a} \vee \sigma(a') \cdot \tilde{a}_{2^{m+1}-1} \quad \text{für } [\tilde{a}] = 2^m - 1.$$

Da $\tau(a_{2^m-1}) = a_{2^{m+1}-1}$ ist, haben wir in beiden Fällen formal die gleiche Darstellung.

Wir betrachten nun die beiden restlichen Fälle.

$$a = a' \cdot \tilde{a} \vee a'_{2^{n+1}-1} \cdot \tau(\tilde{a}) \quad \text{für } [a'] = 0,\ [\tilde{a}] < 2^m - 1$$

und

$$a = a_{2^{n+1}-1} \cdot \tau^{-1}(\tilde{a}) \vee a' \cdot \tilde{a} \quad \text{für } [a'] = 2^{n+1} - 2,\ [\tilde{a}] > 2^m - 1.$$

Wir sehen, daß auch diese beiden Fälle in den durch ein Atom erweiterten Algebren die gleiche Darstellung besitzen.

Wir bemerken weiter, daß $\tau^2(a) = a$ gilt, da $i + 2^{m+1} = i \; mod \; 2^{m+1}$ ist.

Um a effizient berechnen zu können, benötigen wir auch eine effiziente Berechnung von $\sigma(a')$ und $\tau(\tilde{a})$. Wir erhalten aus obiger Darstellung von a

$$\sigma(a) = a' \cdot \sigma(\tilde{a}) \vee \sigma(a') \cdot \tau(\sigma(\tilde{a}))$$

und

$$\tau(a) = \tau(a') \cdot \tilde{a} \vee \sigma(a') \cdot \tau(\tilde{a}).$$

Die simultane Berechnung von $a, \sigma(a), \tau(a)$ aus den entsprechenden Atomen Δ_m und Δ_n erfordert also für ein fest vorgegebenes Atom $a \in \Delta_{n+m}$ 9 Gatteroperationen.

Sei nun $a \in \Delta_N, N = 2^k$ vorgegeben. Es gibt in jeder Algebra $\Delta_i^0 = \Delta(x_i, y_i)$ genau ein Atom a_i^0, so daß

$$a \cdot a_l^0 \neq 0 \quad \text{und } a \cdot \sigma(a_l^0) \neq 0$$

ist. Wir setzen

$$x_j^l = (x_{j \cdot 2^l + 1}, \ldots, x_{j \cdot 2^l + 2^l}) \quad \text{für } j = 0, 1, \ldots, 2^{k-l} - 1.$$

Entsprechend ist y_j^l zu verstehen.

In $\Delta_j^l := \Delta(x_j^l, y_j^l)$ gibt es zu a höchstens ein Tripel $a_j^l, \sigma(a_j^l), \tau(a_j^l)$, mit

$$a \cdot a_j^l \neq 0,\ a \cdot \sigma(a_j^l) \neq 0,\ a \cdot \tau(a_j^l) \neq 0.$$

Indem wir nun $\Delta_j^{l+1} \subset \Delta_{2j-1}^l + \Delta_{2j}^l$ verwenden, können wir $a_j^{l+1}, \sigma(a_j^{l+1})$ und $\tau(a_j^{l+1})$ auf der Basis von $a_{2j-1}^l,\ \sigma(a_{2j-1}^l),\ \tau(a_{2j-1}^l),\ a_{2j}^l,\ \sigma(a_{2j}^l),\ \tau(a_{2j}^l)$ ausdrücken.

Der Übergang von der Menge von $A^l = \{a_{2j-1}^l,\ \sigma(a_{2j-1}^l),\ \tau(a_{2j-1}^l)\}$ von Atomen von Δ_j^l zu den Atomen A^{l+1} erfordert also höchstens $9 \cdot 2^{k-l-1}$ Gatter. Die Kosten für die Darstellung von A^0 auf Basis von x, y erfordert $5 \cdot 2^k$ Gatter. Also ergeben sich für die Kosten $C_k(a)$, $a \in \Delta_{2^k}$, wenn wir stets $n = m$ wählen:

$$\begin{aligned} C_k(a) &= 5 \cdot 2^k + 9 \cdot 2^{k-1} + \ldots + 9 \cdot 1 && (16)\\ &= 9(2^{k+1} - 1) - 4 \cdot 2^k && (17)\\ &= 7 \cdot 2^{k+1} - 9 && (18)\\ &= 14 \cdot N - 9. && (19) \end{aligned}$$

Wir fassen das Resultat in dem folgenden Satz zusammen:

Satz 15. *Die Atome der Algebra Δ_N lassen sich iterativ mit Kosten $C_N(a) \leq 14 \cdot N - 9$ in Tiefe $T_N \leq 2 \cdot \log N$ berechnen.*

Beweis. Den Beweis haben wir vorher geführt. Es bleibt nur noch zu bemerken, daß der Übergang von der Erweiterung von Δ durch ein Atom durch einen Homomorphismus rückgängig gemacht werden kann, der das hinzugefügte Element löscht und die Darstellungen der Atome erhält. □

Diskussion der Ergebnisse

In der rein rekursiven Betrachtung wird nicht berücksichtigt, daß $a, \sigma(a)$ und $\tau(a)$ die gleichen Variablen betreffen. Das wirkt sich so aus, daß bei der hierarchischen Expansion die gleichen Schaltkreise mehrfach erzeugt werden. Das Beispiel der Atome zeigt, daß dabei ein im iterativen Fall lineares Wachstum in ein quadratisches Wachstum der Kosten übergehen kann. Es sollte allerdings möglich sein, hierarchische Entwurfssysteme so zu ergänzen, daß eine bottom-up-Analyse der Resultate zu einer automatischen Faltung der Teilnetze gleicher Funktion verwendet werden kann. Dies hätte den Vorteil, daß man die Einfachheit des hierarchischen Entwurfs mit der Effizienz des iterativen Entwurfs verbinden kann.

4.1.2 Darstellungen von ad_n

Wir übertragen nun die für Atome erprobte Konstruktion auf andere Erzeugendensysteme. Seien $E' = \{e'_0, \ldots, e'_n\}$, $\tilde{E} = \{\tilde{e}_0, \ldots, \tilde{e}_m\}$ und $E = \{e_0, \ldots, e_{n+m}\}$ die zu Beginn des Kapitels definierten Erzeugendensysteme von $\Delta', \tilde{\Delta}$ bzw. Δ. Nehmen wir an, daß wir E' und $\tilde{E}$ bereits konstruiert haben, dann stellt sich die Aufgabe E auf Basis von E' und $\tilde{E}$ zu erzeugen. Offensichtlich gilt

$$e_{n+i} = \tilde{e}_i \quad \text{für } i = 1, \ldots, m,$$

so daß wir uns nur mit der Konstruktion von $e_0, \ldots, e_n$ befassen müssen. Wir setzen $c := \tilde{e}_0$. Es bezeichnet c also den durch $ad(\tilde{x}, \tilde{y})$ erzeugten Übertrag. Wir beweisen, daß

$$e_1 = e'_1 \cdot \overline{c} \vee \sigma(e'_1) \cdot c$$

und

$$e_0 = e'_0 \vee \sigma(e'_0) \cdot c$$

gelten. Anschließend zeigen wir, daß daraus folgt, daß die erste Gleichung für $1 \leq i \leq n$ gilt.

Wie wir in Satz 14 gezeigt haben, lassen sich die Atome $b \in \Gamma$ in der Form $b = b' \cdot \tilde{a} \vee \sigma(b') \cdot \tau(\tilde{a})$ und $b = a \vee \tau(a)$ schreiben.

Nun gilt

$$e_1 b = b \Longleftrightarrow 2^{n+m-1} \leq [a] < 2^{n+m}.$$

Aus der Darstellung

$$b = b' \cdot \tilde{a} \vee \sigma(b') \cdot \tau(\tilde{a})$$

erhalten wir für $b' = a' \vee \tau(a')$

$$2^{n-1} \leq [a'] < 2^n.$$

Damit ergibt sich

$$e_1 = \bigcup_{e_1 \cdot b = b} b = \bigcup b' \cdot \tilde{a} \vee \bigcup \sigma(b') \cdot \tau(\tilde{a}),$$

worin die Vereinigung über $[\tilde{a}] < 2^m$ und $2^{n-1} \leq [a'] < 2^n$ zu nehmen ist. Wegen

$$\bigcup \tilde{a} = \overline{c} \quad \text{und} \quad \bigcup(\tau(\tilde{a})) = c$$

erhalten wir

$$e_1 = e_1' \cdot \overline{c} \vee \sigma(e_1') \cdot c.$$

Ebenso findet man

$$e_0 = e_0' \cdot \overline{c} \vee \sigma(e_0') \cdot c.$$

Wegen $e_0' < \sigma(e_0')$ (hierbei kommt die Adjunktion von $a_{2^{n+1}-1}$ zum tragen) gilt auch $e_0 = e_0' \vee \sigma(e_0') \cdot c$, was wir behauptet haben.

Indem wir diese Konstruktion sukzessive für $i = 1, 2, \ldots, n$ durchführen, erhalten wir

$$e_i = e_i' \cdot \overline{c} \vee \sigma(e_i') \cdot c \quad \text{für } i = 1, \ldots, n \tag{20}$$
$$e_0 = e_0' \vee \sigma(e_0') \cdot c. \tag{21}$$

Zur rekursiven Berechnung von E aus E' und $\tilde{E}, \sigma(E')$ und $\sigma(\tilde{E})$ benötigen wir auch die Darstellung von $\sigma(E)$ auf der gleichen Basis. Zunächst betrachten wir den Fall $i = 0$. Wir erhalten

$$\sigma(e_0) = \bigcup_{a \cdot e_0 = a} \sigma(a) \vee a_{2^{n+m+1}-2} = \sigma(a_{2^{n+m}}) \vee e_0 = e_0 \vee a_{2^{n+m}-1}.$$

Aus der Darstellung der Atome erhalten wir

$$a_{2^{n+m}-1} = a'_{2^n-1} \cdot \tilde{a}_{2^m-1}.$$

Hieraus folgt, wenn wir diese Zerlegung und die Darstellung von e_0 oben einsetzen

$$\sigma(e_0) = e_0' \vee \sigma(e_0') \cdot c \vee a' \cdot \tilde{a}.$$

Hierin haben wir die Indizes von a' und $\tilde{a}$ unterschlagen. Wir erhalten durch einfache Umformungen

$$\begin{aligned}
\sigma(e_0) &= e_0' \vee (\sigma(e_0') \vee a') \cdot c \vee a' \cdot \tilde{a} && (22)\\
&= e_0' \vee \sigma(e_0') \cdot c \vee a' \cdot \sigma(c) && (23)\\
&= e_0' \vee e_0' \cdot \sigma(c) \vee \sigma(e_0') \cdot c \vee a' \cdot \sigma(c) && (24)\\
&= e_0' \vee \sigma(e_0') \cdot c \vee (e_0' \vee a') \cdot \sigma(c) && (25)\\
&= e_0' \vee \sigma(e_0') \cdot \sigma(c). && (26)
\end{aligned}$$

Durch die gleichen Schlüsse wie im Fall der Darstellung von e_i erhält man aus der für die Atome abgeleiteten Darstellung $\sigma(a) = a' \cdot \sigma(\tilde{a}) \vee \sigma(a') \cdot \tau(\sigma(\tilde{a}))$

unter Verwendung von $\sigma \circ \tau = \tau \circ \sigma$, $\sigma(\overline{c}) = \overline{\sigma(c)}$ und $\tau(\sigma(\overline{c})) = \sigma(c)$ die Darstellung

$$\sigma(e_i) = e'_i \cdot \overline{\sigma(c)} \vee \sigma(e'_i) \cdot \sigma(c)$$

für $i = 1, \dots, n$. Wir fassen unsere Ergebnisse in dem folgenden Lemma zusammen:

Lemma 12. $E, \sigma(E)$ und a lassen sich aus $E', \sigma(E'), a'$ und $\tilde{E}, \sigma(\tilde{E}), \tilde{a}$ durch die folgenden Operationen berechnen:

$$\begin{aligned} e_i &= e'_i \cdot \overline{c} \vee \sigma(e'_i) \cdot c, & (27)\\ e_{n+i} &= \tilde{e}_i, & (28)\\ \sigma(e_i) &= e'_i \cdot \overline{\sigma(c)} \vee \sigma(e'_i) \cdot \sigma(c), & (29)\\ e_0 &= e'_0 \vee \sigma(e'_0) \cdot c, & (30)\\ \sigma(e_0) &= e'_0 \vee \sigma(e'_0) \cdot \sigma(c) & (31) \end{aligned}$$

für $i = 1, \dots, n$ und $c = \tilde{e}_0$.

Wir verwenden diese Operationen um E aus x, y auf zwei verschiedene Weisen zu berechnen. Hierzu definieren wir die beiden Bausteine F_0 und F_1, die in Abbildung 1 dargestellt sind.
Aus diesen Bausteinen bauen wir nun zu der Konstruktion von E aus E' und $\tilde{E}$ den Schaltkreis, der in Abbildung 2 dargestellt wird.
Der Übergang von $E', \tilde{E}$ zu E ergibt sich also durch die Hinzufügung des linken unteren Schaltkreises zu den linken oberen und dem rechten, die beide in dem vorhergegangenen Schritt konstruiert wurden.

Ist T^n bzw. T^m die Gattertiefe des Schaltkreises für E' bzw. $\tilde{E}$, dann gilt also $T^{n+m} = \max\{T_n, T_m\} + 2$. Ist C^n bzw. C^m die Anzahl der Gatter, die für die Konstruktion von E' bzw. $\tilde{E}$ verbraucht wurden, dann gilt $C^{n+m} = C^n + C^m + n \cdot 6 + 4$.

Für die erste Schicht erhält man

$$e_0 = x \cdot y, \ \sigma(e_0) = x \vee y, \ e_1 = x\overline{y} \vee \overline{x}y, \ \sigma(e_1) = \overline{e}_1.$$

Wählen wir $N = 2^k$ und in der Konstruktion stets $n = m$, dann erhalten wir für die Tiefe T_N des Schaltkreises $T_N \leq 2 \cdot (1 + \log N)$. Wir setzen C_i für die

Abbildung 1:

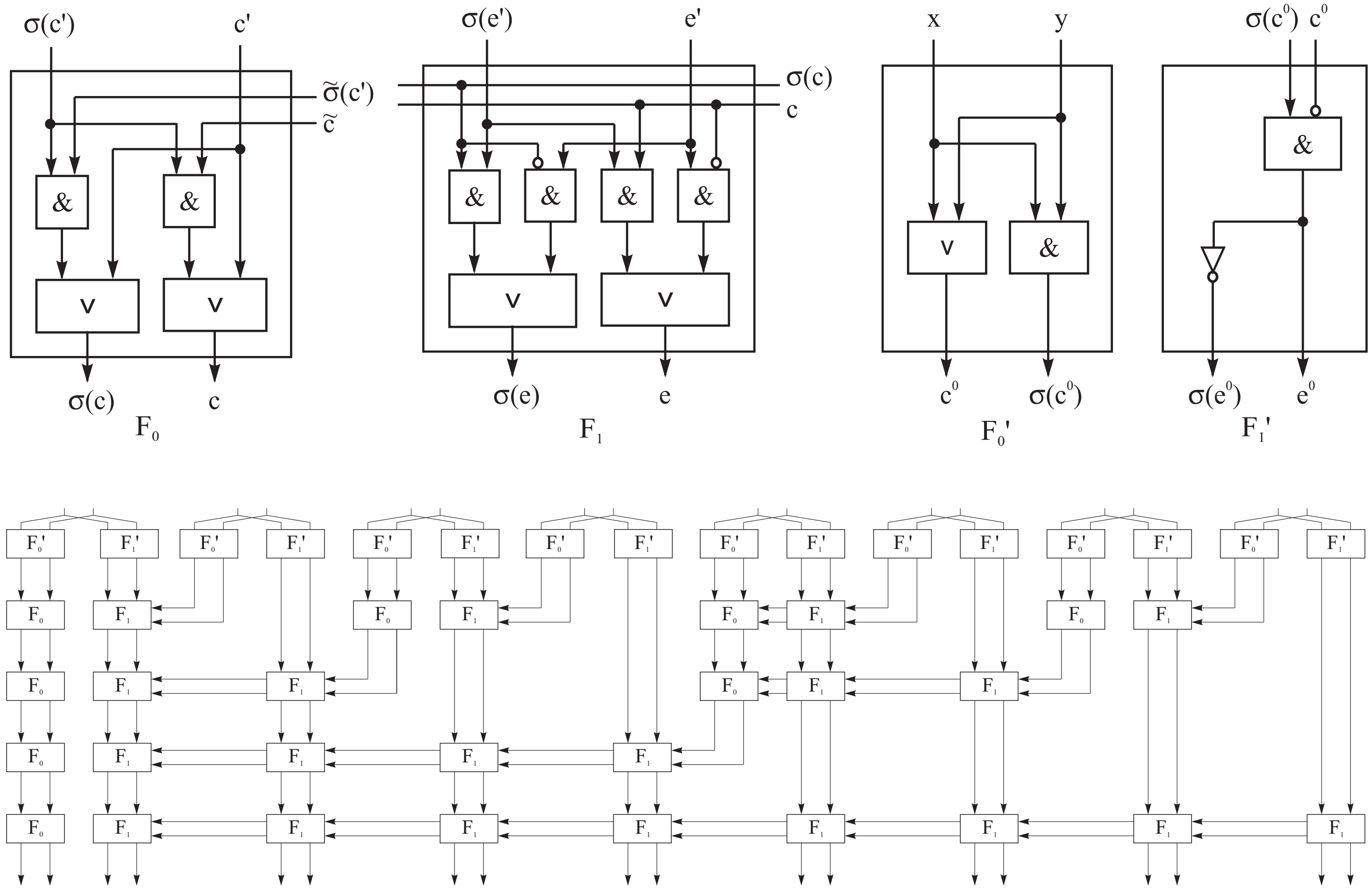
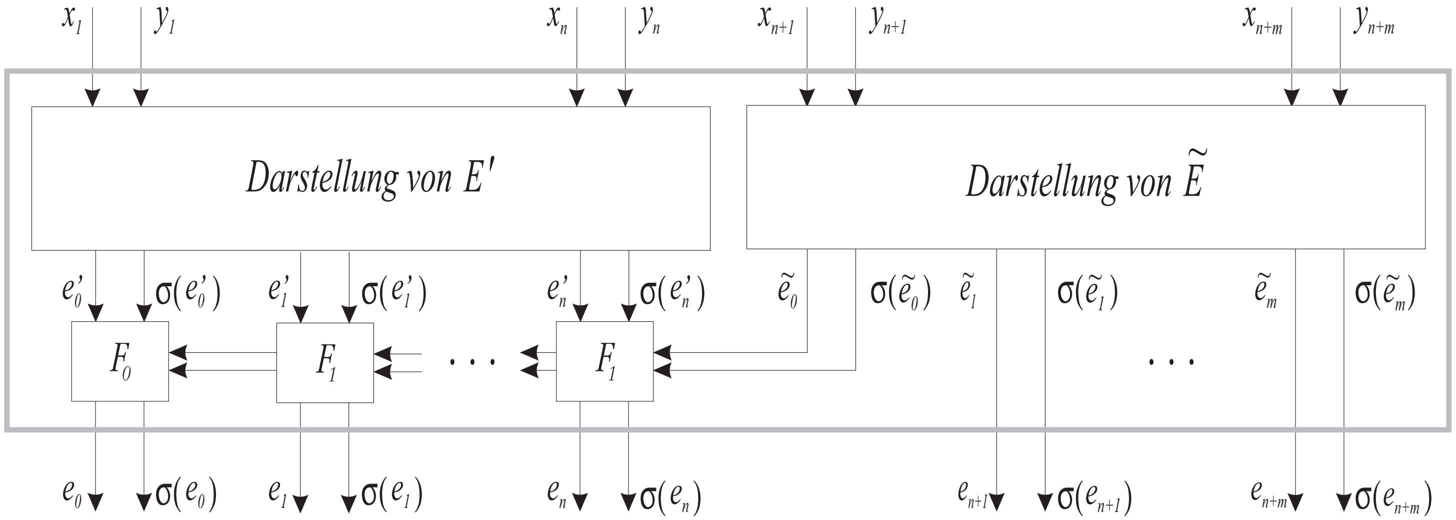


Abbildung 2:



Figur 2

Kosten nach der i-ten Iteration und erhalten

$$\begin{aligned}
C_k &\leq 2 \cdot C_{k-1} + |F_1| \cdot 2^{k-1} + |F_0| && (32)\\
&= 2 \cdot (2 \cdot C_{k-2} + |F_1| \cdot 2^{k-2} + |F_0|) + |F_1| \cdot 2^{k-1} + |F_0| && (33)\\
&= 2^2 \cdot C_{k-2} + 2 \cdot |F1| \cdot 2^{k-1} + (2+1) \cdot |F_0| && (34)\\
&= 2^k \cdot C_0 + |F_1| \cdot k \cdot 2^{k-1} + |F_0| \cdot \sum_{i=0}^{k-1} 2^i && (35)\\
&= \frac{|F_1|}{2} \cdot N \log N + N \cdot (C_0 + |F_0|) - |F_0| && (36)
\end{aligned}$$

Wir haben $C_0 = |F_0'| + |F_1'| = 3$, $|F_1| = 6$ und $|F_0| = 4$. Somit erhält man bei dieser Wahl der Bausteine den

Satz 16. *Die Addition ad_N läßt sich für $N = 2^k$ mittels der Bausteine F_0, F_1, F_0', F_1' rekursiv in Tiefe $2 \cdot (1 + \log N)$ mittels $\leq 3 \cdot N \cdot \log N + 7 \cdot N - 4$ $\{\vee, \&\}$-Gattern konstruieren.*

Das soweit geschilderte Verfahren beschreibt im wesentlichen den conditional sum-Addierer. Läßt man auch $\oplus$ als Grundbaustein zu, dann reduziert sich die Tiefe um 1, so daß wir damit die in Satz 3.4.3 in [Weg96] angegebene Tiefe dieses Addierers, allerdings mit einem um $3 \cdot N - 2$ geringeren Aufwand, erhalten.

Der Baustein F_0 läßt sich noch vereinfachen, wenn man $\sigma(e_0) = e_0 \vee a_{2^{n+m}-1}$ und die Darstellung $a_{2^{n+m}-1} = a'_{2^n-1} \cdot \tilde{a}_{2^m-1}$ heranzieht. Lassen wir wieder die Indizes weg und bezeichnen wir den „carry“ e_0 wie üblich mit c, dann erhalten wir

$$\begin{aligned}
c = c' \vee \sigma(c') \cdot \tilde{c} &= c' \vee (c' \vee a') \cdot \tilde{c} && (37)\\
&= c' \vee a' \cdot \tilde{c} && (38)
\end{aligned}$$

und

$$\begin{aligned}
\sigma(c) = c' \vee \sigma(c') \cdot \sigma(\tilde{c}) &= c' \vee (c' \vee a') \cdot (\tilde{c} \vee \tilde{a}) && (39)\\
&= c' \vee a' \cdot \tilde{c} \vee a' \cdot \tilde{a} && (40)\\
&= c \vee a. && (41)
\end{aligned}$$

Wir haben weiter

$$\begin{aligned}
e &= e' \cdot \bar{\tilde{c}} \vee \sigma(e') \cdot \tilde{c}\\
&= e' \cdot \bar{\tilde{c}} \vee (e' \vee a') \cdot \tilde{c} = e' \vee a' \cdot \tilde{c}.
\end{aligned}$$

Es genügt also zur Berechnung von e die Funktion e', a' und $\tilde{a}, \tilde{c}$ bereitzustellen. Somit erhalten wir als Rekursionsformel zur Berechnung von e

$$a = a' \cdot \tilde{a}, \;\; c = c' \vee a' \cdot \tilde{c}, \;\; e = e' \vee a' \cdot \tilde{c} \tag{42}$$

und damit als neue Version unserer Bausteine $\tilde{F}_0, \tilde{F}_1$

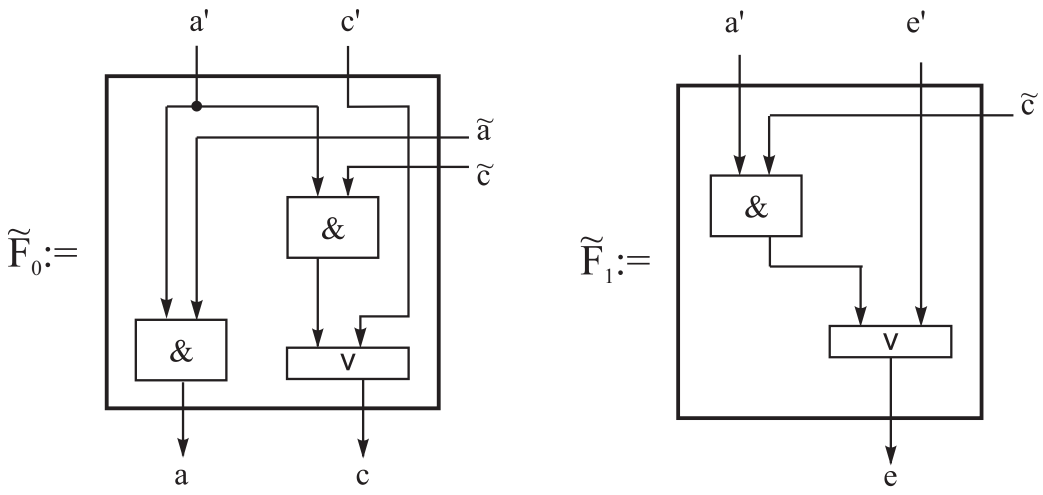


Abbildung 3:

Daraus ergibt sich Tiefe $(\tilde{F}_0) = 2$, $Tiefe(\tilde{F}_1) = 2$, $|\tilde{F}_0| = 2$, $|\tilde{F}_1| = 2$.
Für die oberste Schicht erhalten wir

$$c = x \cdot y, \quad a = x \oplus y = d \cdot \overline{c}, \quad d = x \vee y$$

Wir fassen F_0' und F_1' in einem Baustein $\tilde{F}$ zusammen, der in Abbildung 4 beschrieben wird.
Wir haben Tiefe $(\tilde{F}) = 2$ und $|\tilde{F}| = 3$. Setzen wir die Kosten anstelle von $|F_0|, |F_0', |F_1|$ und $|F_1'|$ in unsere Formeln ein, dann erhalten wir nun die gleiche Tiefe $T_N = 2 \cdot (1 + \log N)$ und die Kosten

$$\tilde{C}_k = \frac{3}{2} N \cdot \log N + 6 \cdot N - 3.$$

Die Tiefe T_N kann man allerdings noch um 1 niedriger abschätzen indem man die Tiefe von $c = x \cdot y$ mit 1 anstelle von 2 in Rechnung stellt. Wir erhalten somit zu Satz 16 das

Korollar 9. *Die Addition von Dualzahlen der Länge $N = 2^k$ läßt sich in $(\&, \vee)$-Gattertiefe $2 \cdot \log N - 1$ in Größe $\leq \frac{3}{2} N \log N + 6 \cdot N - 3$ realisieren.*

Das Netz enthält N Negationen in der ersten Schicht und ist sonst monoton.

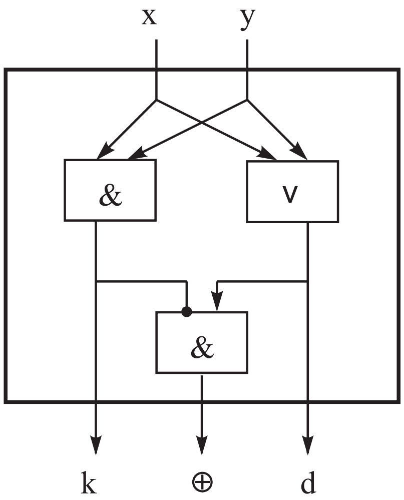


Abbildung 4:

Eine Darstellung von ad_n mit linearem Aufwand

Fischer und Ladner [LF80] und *Slansky* [Sla60] andererseits verdankt man die Beobachtung, daß im Conditional-Sum-Addierer gewisse Unterschaltkreise überflüssig sind. Sie haben von dieser Beobachtung ausgehend zunächst nur die Übertragsfunktion berechnet und danach die Funktionen $e_1, \ldots, e_n$. In diesem Zusammenhang entwickelten sie das schöne Konzept der parallelen Präfixberechnung in Monoiden. *Becker und Kolla* [BK87] haben anknüpfend an [LF80] und [Hot61] gezeigt, daß man unter Ausnutzung der Symmetrien sieben verschiedene, im wesentlichen äquivalente Realisierungen der Addition angeben kann. Wir geben hier eine etwas andere Herleitung dieser Ergebnisse.

Wir betrachten zunächst einmal einen 8-stelligen Abschnitt des oben definierten Addierers, der zu (x_j^3, y_j^3) für ein geeignetes j gehört. Hierzu sehe man Abbildung 2. Wir beobachten, daß die in einer Spalte liegenden Bausteine vom Typ F_1 wiederholt einen „Übertrag“ von rechts erhalten und das daraus berechnete Resultat an den tiefer liegenden Baustein F_1 der gleichen Spalte weitergeben. Die Übertragssignale $c, \sigma(c)$ werden unverändert nach links weitergeleitet. Löschen wir die Bausteine von Typ F_1, dann bleibt ein baumartiger Schaltkreis zurück, dessen Knoten Bausteine vom Typ F_0 sind. Indem wir die parallelen Leitungen vom 2-wertigen Typ *boolean* durch eine 4-wertige Leitung vom Typ *boolean*^{2} ersetzen, erhalten wir den Baum, der in Abbildung 5 durch die stark ausgezogenen Kanten markiert wird. Die Knoten des Baumes repräsentieren die Bausteine vom Typ F_0. Dieser Baum

erfaßt einen 32-stelligen Abschnitt. Er beschreibt den Schaltkreis, der $x_i \oplus y_i$ erzeugt und die Überträge zu allen diesen Stellen.
Nun ist Tiefe $(F_0) = 2$ und Tiefe $(F_0') = 1$, so daß sich daraus für die Tiefe T_k des Schaltkreises mit 2^k Eingängen $T_k \leq 4 \cdot k - 3$ ergibt.

Die Kosten C_k, die zur Realisierung von ad_n erforderlich sind, schätzen wir wie folgt ab: Die Kosten C_k' des *tragenden* (stark ausgezogenen) Baumes in Abbildung 5 lassen sich durch die Rekursion

$$\begin{aligned} C_k' &\leq 2 \cdot C_{k-1}' + |\tilde{F}_0| \\ &\vdots \\ &= 2^k \cdot C_0 + |\tilde{F}_0| \cdot \sum_{i=0}^{k-1} 2^i = 2^k \cdot |F_0'| + (2^k - 1) \cdot |\tilde{F}_0| \end{aligned}$$

abschätzen. Setzen wir $N = 2^k$, dann erhalten wir also

$$C_k' = N \cdot (|\tilde{F}_0'| + |\tilde{F}_0|) - |\tilde{F}_0|.$$

Zur Realisierung des Baumes aus Abbildung 5 insgesamt benötigen wir zur Erzeugung der Überträge, die der tragende Baum nicht liefert, zusätzlich $(N - 3)$ mal den Baustein $\tilde{F}_0$. Die -3 rührt daher, daß der Übertrag der beiden letzten Stellen und der ersten Stelle bereits durch den tragenden Baum berechnet werden. Somit erhalten wir als Abschätzung der Kosten $\tilde{C}_n$ des Gesamtbaumes, wenn wir $|\tilde{F}_0| = 3$ und $|F_0'| = 2$ einsetzen

$$\tilde{C}_N \leq 8 \cdot N - 12.$$

Für die Realisierung von ad_N kommen wir aufgrund der angegebenen Rekursion zu der Abschätzung

$$C_N \leq \tilde{C}_N + 4 \cdot N - 3 = 12 \cdot N - 15;$$

hierbei haben wir verwendet, daß sich die Addition $mod 2$ durch $\overline{k} \cdot d$ darstellen läßt und daß das &-Gatter k und das $\vee$-Gatter d in F_0' vorhanden sind. Die zusätzliche Addition $mod 2$ des jeweiligen Übertrages zu $x_i \oplus y_i$ erfordert zusätzlich die Kosten 3 pro Stelle.

Wir fassen zusammen:

Satz 17. *Die angegebene Realisierung von ad_N erfordert bei einer Tiefe $T_N \leq 4 \cdot \log N - 1$ an $\{\vee, \&\}$-Kosten $C_N \leq 12 \cdot N - 15$. Hierin ist $N = 2^k$ und $k \in \mathbb{N}$.*

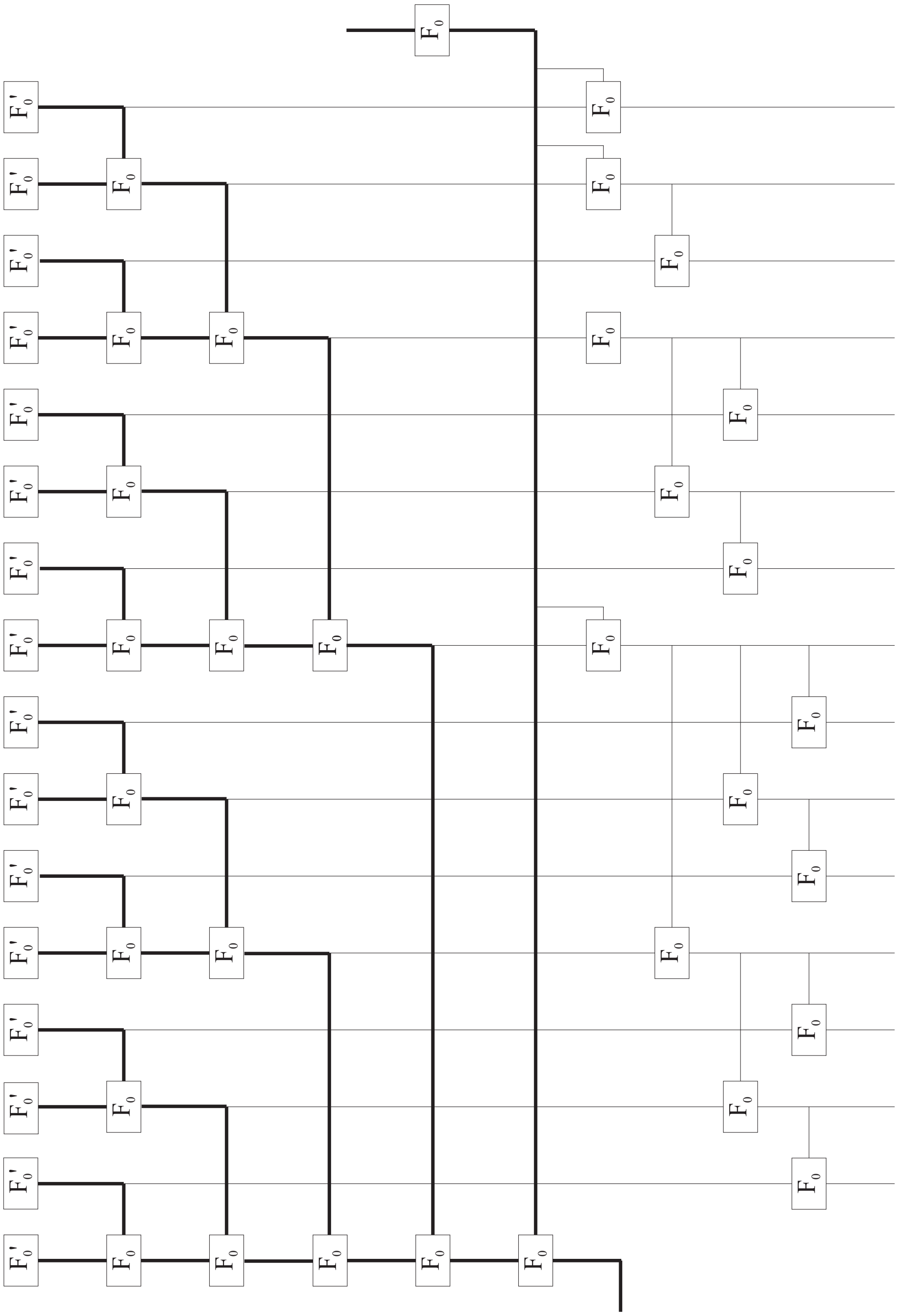


Abbildung 5:

Nimmt man zu den Operationen $\{\vee, \&\}$ noch $\oplus$, die Addition *modulo*2, hinzu, dann erhält man für die erste Stufe nur die Kosten 2 anstelle von 3 und für die letzte Stufe die Kosten 1 anstelle von 3. Somit verbilligen sich die Gesamtkosten in diesem Fall um $3 \cdot N$. Man beobachtet weiter, daß man in der Hälfte der terminalen Bausteine F_0 den Ausgang a nicht braucht, was zu einer weiteren Verbilligung von $\frac{N}{2}$ &-Gattern führt. Wir fassen dieses Resultat zusammen in

Korollar 10. *Die Addition von zwei N-stelligen Dualzahlen läßt sich mittels der Bausteine $\vee, \&, \oplus$ in Tiefe $4 \cdot \log N$ mit Kosten $C_N \leq 8,5 \cdot N$ realisieren.*

Realisiert man die drei Funktionen (42) durch den Baustein $\tilde{F}$

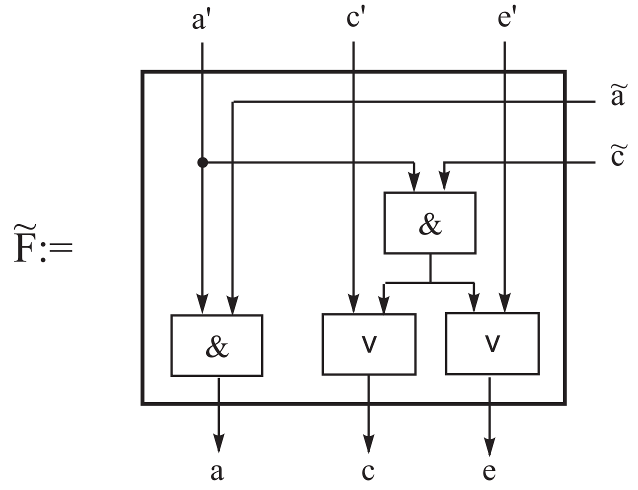


Abbildung 6:

und ersetzt man in dem Graphen Figur 3 überall F_0' durch $\tilde{F}'$ und F_0 durch $\tilde{F}$, dann erhält man eine Realisierung von ad_N. Die Hälfte der terminalen Bausteine erzuegt a und c überflüssigerweise. Kappt man diese Ausgänge und berücksichtigt man die dadurch induzierte Reduktion von $\tilde{F}$ um zwei Gatter, dann erhält man für die $\{\vee, \&\}$-Kosten dieser Realisierung die Abschätzung

$$\begin{aligned} C_k &\leq N \cdot |\tilde{F}'| + (N-1)|\tilde{F}| + N \cdot |\tilde{F}| - N && (43) \\ &= 3N + 4(N-1) + 4 \cdot N - N && (44) \\ &= 10 \cdot N - 4. && (45) \end{aligned}$$

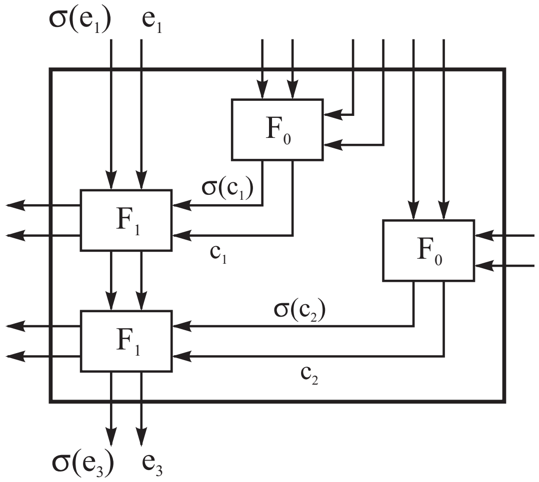
Die Tiefe des Netzes ändert sich durch diese Substitution nicht. Wir fassen zusammen:

Korollar 11. *ad_N $(N = 2^k)$ läßt sich in der Tiefe $4 \cdot \log N$ mit $\{\vee, \&\}$-Kosten $\leq 10 \cdot N - 4$ realisieren.*

Eine weitere Realisierung von ad_n

Wir beschreiben eine weitere Realisierung von ad_N, die interessant ist, da sie einen anderen Zugang zur Herleitung der Realisierung verwendet. Die Basis dazu bilden die beiden folgenden Lemmas.

Lemma 13. Für die durch die beiden folgenden Netze definierten Funktionen gilt $(\sigma(e_3), e_3) = (\sigma(e_3'), e_3')$



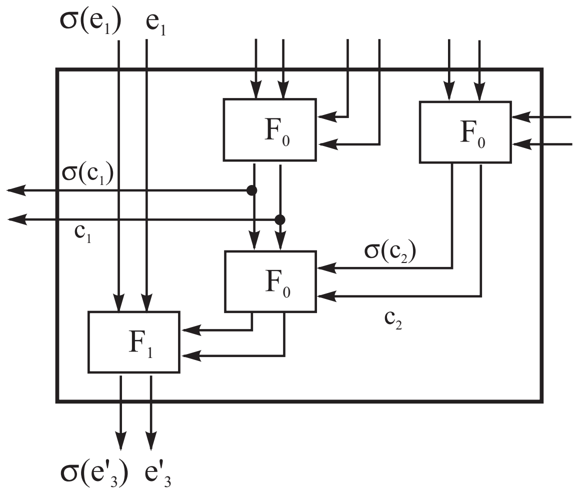


Abbildung 7:

Beweis. Wir haben nach Voraussetzung

$$e_2 = e_1 \cdot \overline{c_1} \vee \sigma(e_1) \cdot c_1 \,, \qquad \sigma(e_2) = e_1 \cdot \overline{\sigma(c_1)} \vee \sigma(e_1) \cdot \sigma(c_1)$$
$$e_3 = e_2 \cdot \overline{c_2} \vee \sigma(e_2) \cdot c_2 \,, \qquad \sigma(e_3) = e_2 \cdot \overline{\sigma(c_2)} \vee \sigma(e_2) \cdot \sigma(c_2).$$

Durch Einsetzen der Definition von e_2 und $\sigma(e_2)$ in die Definition von e_3 erhalten wir

$$\begin{aligned} e_3 &= e_1 \cdot \overline{c_1} \cdot \overline{c_2} \vee \sigma(e_1) \cdot c_1 \cdot \overline{c_2} \vee e_1 \overline{\sigma(c_1)} \cdot c_2 \vee \sigma(e_1) \cdot \sigma(c_1) \cdot c_2 &(46)\\ &= e_1 \cdot (\overline{c_1} \cdot \overline{c_2}) \vee \overline{\sigma(c_1)} \cdot \overline{c_2} \vee \sigma(e_1) \cdot (c_1 \cdot \overline{c_2} \vee \sigma(c_1) \cdot c_2). &(47)\end{aligned}$$

Nun ist

$$\begin{aligned} \overline{\overline{c_1} \cdot \overline{c_2} \vee \overline{\sigma(c_1)} \cdot c_2} &= (c_1 \vee c_2) \cdot (\sigma(c_1) \vee \overline{c_2}) &(48)\\ &= c_1 \cdot \sigma(c_1) \vee c_2 \cdot \sigma(c_1) \vee c_1 \cdot \overline{c_2} &(49)\\ &= c_1 \vee c_1 \cdot \overline{c_2} \vee \sigma(c_1) \cdot c_2 &(50)\\ &= c_1 \vee \sigma(c_1)\overline{c_2}. &(51)\end{aligned}$$

Also haben wir wegen $\overline{c_2'} = \overline{c_1} \cdot \overline{c_2} \vee \overline{\sigma(c_1)} \cdot c_2$, wie behauptet $e_3 = e_3'$. Die entsprechende Berechnung für $\sigma(e_3)$ ergibt

$$\sigma(e_3) = e_1 \cdot \left(\underbrace{\overline{c_1} \cdot \overline{\sigma(c_2)} \vee \overline{\sigma(c_1)} \cdot \sigma(c_2')}_{\overline{\sigma(c_2')}} \vee \sigma(e_1) \cdot (\underbrace{c_1 \cdot \overline{\sigma(c_2)} \vee \sigma(c_1) \cdot \sigma(c_2)}_{\sigma(c_2')} \right).$$

Also gilt auch $\sigma(e_3) = \sigma(e_3')$. □

Wir geben zunächst eine Erläuterung, die diese Transformation übersichtlicher erscheinen läßt. Dazu fassen wir das Paar der Leitungen $(e, \sigma(e))$ und $(c, \sigma(c))$ bzw. (a, c) stets zu einer Verbindung vom Typ *boolean*^{2} zusammen. Der an der Transformation beteiligte Teil der Netze faßt sich zusammen zu Hierin verwenden wir $*$ als Infixnotation für F_1 und $\circ$ als Infixnotation für F_0 Unser Lemma besagt also

$$(\alpha * \beta) * \gamma = \alpha * (\beta \circ \gamma).$$

Wir beweisen ein zweites Lemma dieser Art.

Lemma 14. Die beiden Funktionen, die durch die Netze in Abbildung 9 definiert werden, sind gleich.

Beweis. Man rechnet in beiden Fällen nach, daß $(a, c) = (a' \cdot \tilde{a} \cdot \vec{a}, c' \vee a' \cdot \tilde{c} \vee a' \cdot \tilde{a} \cdot \vec{c})$ gilt; hierin ist $\alpha = (a', c')$, $\beta = (\tilde{a}, \tilde{c})$ und $\gamma = (\vec{a}, \vec{c})$. □

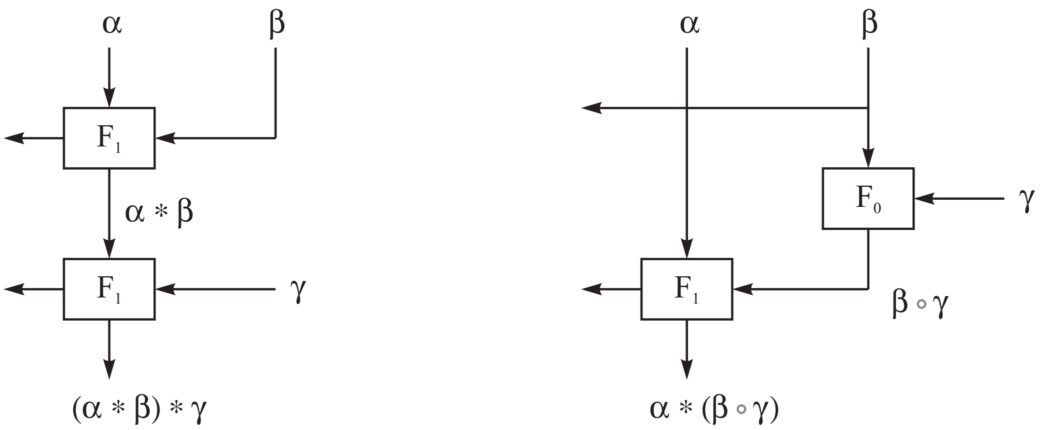


Abbildung 8:

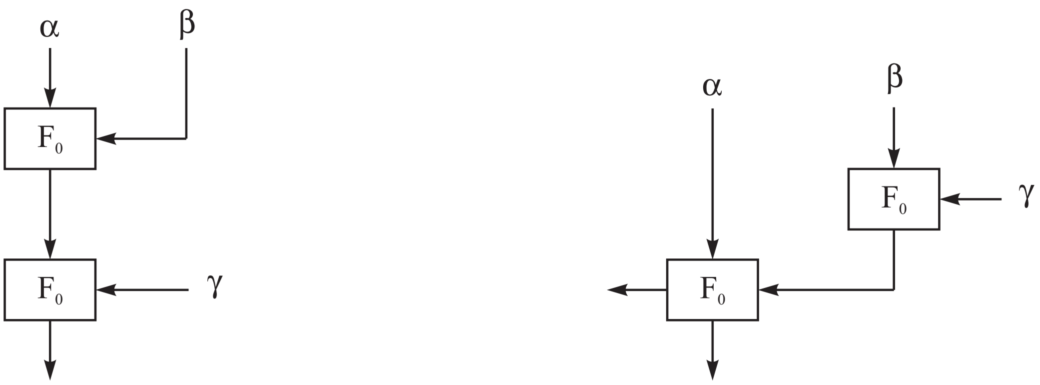


Abbildung 9:

Schreiben wir für die von F_0 definierte Operation wieder $\circ$, dann besagt das Lemma

$$(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma).$$

Lemma 14 drückt also die Assoziativität der Operation $\circ$ aus. Diese Operation wurde in [LF80] verwendet um die parallele Präfixberechnung für die Realisierung der Addition anzuwenden.

Wir verwenden nun beide Transformationsregeln, um den C. S.-Addierer in einen Addierer zu transformieren, dessen Tiefe sich nur um 1 erhöht, dabei aber nur linear in N wachsende Kosten erfordert.

Wir wenden die Identität $(\alpha * \beta) * \gamma = \alpha * (\beta \circ \gamma)$ auf jedes F_1 in dem C. S. - Addierer in Abbildung 10 an. Wir erhalten so eine die Transformation, die

Abbildung 10 in Abbildung 11 überführt.

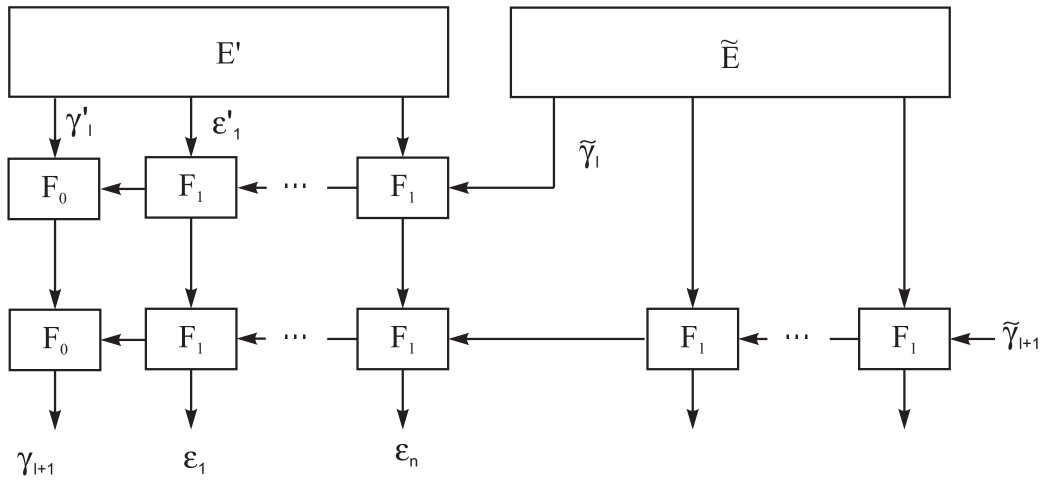


Abbildung 10:

Man entnimmt aus den Abbildungen

$$\varepsilon_i = (\varepsilon_i' * \tilde{\gamma}_l) * \gamma_{l+1} \text{ und } \vec{\varepsilon_i} = \varepsilon_i' * (\tilde{\gamma}_l \circ \gamma_{l+1}) \quad \text{für } i = 1, \ldots, n.$$

Also ist $\varepsilon_i = \vec{\varepsilon_i}$. Wir stellen weiter fest, daß sich bei dieser Transformation die Tiefe der Netze über γ_l' und $\tilde{\gamma}_l$ nicht verändert hat. Die Tiefe über γ_{l+1} hat hingegen um 1 zugenommen. Nicht zugenommen hat die Tiefe von γ_{l+1} und Tiefe $\tilde{\gamma}_l$ ist die gleiche wie die γ_{l+1}.

Wir erhalten auf diese Weise ein Netz, das man aus dem c. s. - Addierer durch die Ersetzung der F_1-Bausteine durch F_0-Bausteine erhält, wenn man von der terminalen Zeile aus F_1-Bausteinen absieht. Auf den ersten Blick haben wir nichts gewonnen. Die Kosten sind gleich geblieben und die Tiefe hat sich um 1 erhöht. Nun kann man aber diese Matrix durch die Anwendung der Asssoziativität von F_0 vereinfachen, indem man die durch Abbildung 12 beschriebene Transformation anwendet.
Hierfür können wir auch

$$(\alpha \circ \gamma_1 \circ \gamma_2, \beta \circ \gamma_1 \circ \gamma_2) = (\alpha, \beta) \circ (\gamma_1 \circ \gamma_2),$$

schreiben. Man erhält auf diese Weise eine ähnliche Realisierung wie wir sie in Satz 17 angegeben haben.

Das Konzept der „semantikerhaltenden" Transformationen von Netzen, das wir hier angedeutet haben, wird im zweiten Teil der Vorlesung eine wesentliche Rolle spielen und dort grundsätzlich behandelt [HZ97].

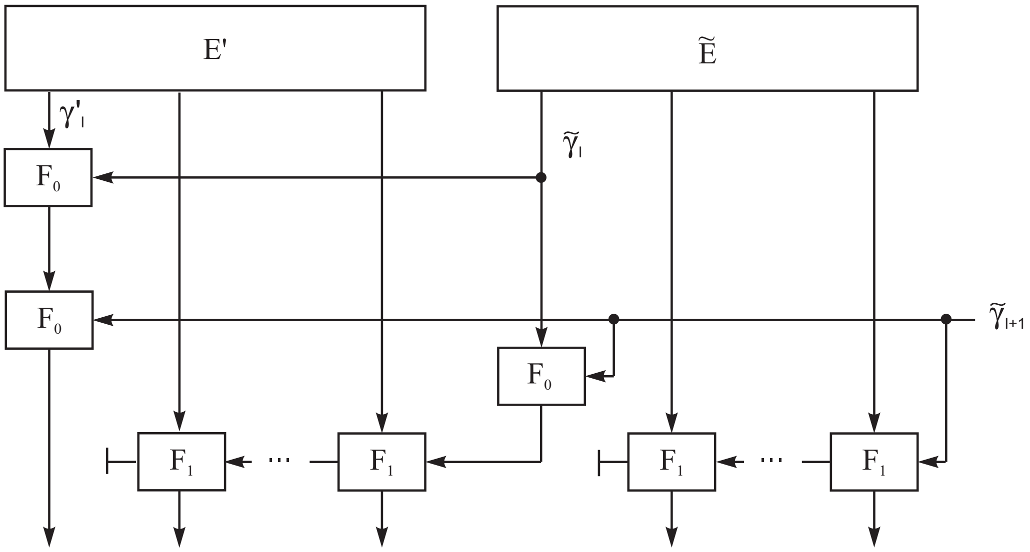


Abbildung 11:

Ohne Beweis geben wir zum Abschluß des Paragraphen den

Satz 18. *Die angegebenen Transformationen*

$$
\begin{aligned}
(\alpha \circ \beta) \circ \gamma &= \alpha \circ (\beta \circ \gamma), && (52)\\
(\alpha * \beta) * \gamma &= \alpha * (\beta \circ \gamma), && (53)\\
(\alpha, \beta) \circ \gamma &= (\alpha \circ \gamma, \beta \circ \gamma), && (54)\\
(\alpha, \beta) * \gamma &= (\alpha * \gamma, \beta * \gamma) && (55)
\end{aligned}
$$

genügen, um die Schulmethode der Addition in die in diesem Paragraphen

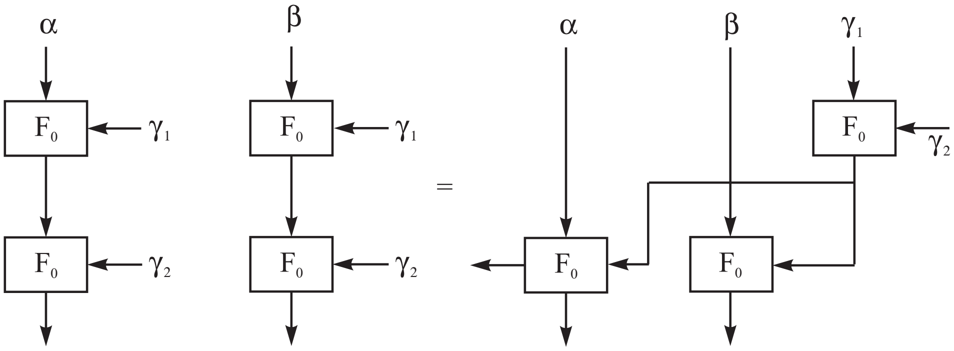


Abbildung 12:

angegebenen Additionsnetze zu transformieren.

Es bleibt noch zu bemerken, daß die Tiefen- und Kostenabschätzungen für die Additionsnetze für N-stellige Zahlen zwar nur für $N = 2^k, k \in \mathbb{N}$ angegeben wurden, daß sie trivialerweise aber auch für $N \in \mathbb{N}$ gelten, wenn man $\log N$ durch $\lceil \log N \rceil$ in der Tiefenabschätzung und N durch $N' = 2^{\lceil \log N \rceil}$ in der Kostenabschätzung ersetzt. Die Kostenabschätzung kann man verbessern, da man von dem Addiernetz die überflüssigen führenden Stellen wegschneiden kann.

4.1.3 Die Algebra $\langle k_1, d_1, \ldots, k_n, d_n \rangle$

Offensichtlich gilt

$$\begin{aligned} & ad_n(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n,\ y_1, \ldots, y_{i-1}, y_i, y_{i+1}, \ldots, y_n) \\ = \ & ad_n(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n,\ y_1, \ldots, y_{i-1}, x_i, y_{i+1}, \ldots, y_n). \end{aligned}$$

Also ad_n ist invariant unter der durch

$$x_i \longleftrightarrow y_i \text{ für } i = 1, \ldots, n$$

erzeugten Gruppe G.

Setzen wir

$$G_i := \langle x_i \longleftrightarrow y_i \rangle,$$

dann gilt

$$G = G_1 + G_2 + \cdots + G_n = G_1 \times G_2 \times \cdots \times G_n,$$

da $x_i \leftrightarrow y_i$ und $x_j \leftrightarrow y_j$ in der Reihenfolge ihrer Anwendung vertauschbar sind.
Wir konstruieren nach dem Schema von Satz 11 die Atome der Unteralgebra von $\mathcal{B}_i$ von $\langle x_i, y_i \rangle$, der unter G_i invarianten Funktionen, und erhalten dafür

$$\overline{x}_i \overline{y}_i,\ x_i \overline{y}_i \ \vee \ \overline{x}_i y_i,\ x_i y_i$$

Hieraus erhalten wir ein minimales Erzeugendensystem für $\mathcal{B}_i := \langle x_i, y_i \rangle (G_i)$ in Gestalt von

$$k_i := x_i y_i,\ d_i := x_i \vee y_i \text{ für } i = 1, \ldots, n.$$

Wir setzen $\mathcal{B} := \langle x_1, \cdots, x_n, y_1, \cdots, y_n \rangle$, $\tilde{\mathcal{B}}_i := \mathcal{B}(G_i)$ und $\tilde{\mathcal{B}} := \mathcal{B}(G)$. Aufgrund von Satz 10 (9) erhalten wir

$$\tilde{\mathcal{B}} = \tilde{\mathcal{B}}_1 \cap \tilde{\mathcal{B}}_2 \cap \ldots \cap \tilde{\mathcal{B}}_n.$$

Nun ist

$$\tilde{\mathcal{B}}_i = \mathcal{B}_i + \langle x_l, y_l | l \in [1:n], l \neq i\rangle.$$

Offensichtlich gilt $\mathcal{B}_i \subset \tilde{\mathcal{B}}$, woraus $\mathcal{B}_1 + \ldots + \mathcal{B}_n \subset \tilde{\mathcal{B}}$ folgt.

Wir beweisen nun, daß die Inklusion auch in der umgekehrten Richtung gilt. Dazu betrachten wir ein Atom $a \in \tilde{\mathcal{B}}_i$. Dieses Atom läßt sich als Produkt der Atome $a_i \in \mathcal{B}_i$ und der Atome $a_l \in \langle x_l, y_l\rangle,\ l \neq i$ schreiben. Wir bilden nun

$$G(a) = G_1(a_1) \cdot G_2(a_2) \cdot \ldots \cdot G_n(a_n)$$

Da $G_i(a_i)$ in $\mathcal{B}_i$ liegt, gilt $G(a) \in \mathcal{B}_1 + \ldots + \mathcal{B}_n$. Hieraus folgt, daß das für $f \in \tilde{\mathcal{B}}_i$ und für jedes i gilt. Also gilt auch für $f \in \bigcap \mathcal{B}_i$, daß $G(f) \in \mathcal{B}_1 + \ldots + \mathcal{B}_n$ ist, woraus $\tilde{\mathcal{B}} \subset \mathcal{B}_1 + \ldots \mathcal{B}_n$ folgt. Also gilt

$$\tilde{\mathcal{B}} = \mathcal{B}_1 + \ldots + \mathcal{B}_n.$$

Wir geben einen zweiten unmittelbaren Beweis für diese Beziehung. Hierbei verwenden wir Induktion über n. Für $n = 1$ ist die Aussage offenbar richtig. Wir nehmen an, daß sie für $l < n$ bewiesen ist.

Es gilt also

$$\langle x_1, \ldots, x_l, y_1, \ldots, y_l\rangle(G_1 \times \ldots \times G_l) = \mathcal{B}_1 + \ldots + \mathcal{B}_l$$

Für

$$f \in \langle x_1, \ldots, x_{l+1}, y_1, \ldots, y_{l+1}\rangle(G_1 \times \ldots \times G_{l+1})$$

erhalten wir aufgrund der Shannon-Entwicklung die Zerlegung

$$\begin{aligned} f = {} & x_{l+1}y_{l+1}f_{11}(x_1, \ldots, x_l, y_1, \ldots, y_l) \\ & \cup \overline{x}_{l+1}y_{l+1}f_{01} \cup x_{l+1}\overline{y}_{l+1}f_{10} \cup \overline{x}_{l+1}\overline{y}_{l+1}f_{00} \end{aligned}$$

Aufgrund der Invarianz von f unter $G_1 \times \ldots \times G_l$ ergibt sich die Invarianz von $f_{11}, f_{01}, f_{10}, f_{00}$ unter $G_1 \times \ldots \times G_l$ und damit nach Induktionsannahme, daß diese Funktionen aus $\mathcal{B}_1 + \ldots + \mathcal{B}_l$ sind.

Nun folgt aus der Invarianz unter G_{l+1}, daß $f_{01} = f_{10}$ ist. Damit haben wir $f = k_{l+1} \cdot f_{11} \vee \overline{k}_{l+1} \cdot d_{l+1}f_{01} \vee \overline{d}_{l+1}f_{00}$.

Also liegt f in $\mathcal{B}_1 + \ldots + \mathcal{B}_{l+1}$. Die Inklusion in der anderen Richtung ist trivial. Induktiv folgt also unsere Behauptung $\tilde{\mathcal{B}} = \mathcal{B}_1 + \ldots + \mathcal{B}_n$. Hieraus ergibt sich der

Satz 19. *Jede der unter den Symmetrien* $(x_i \longleftrightarrow y_i), \quad i = 1, \dots, n$ *invarianten Abbildungen* $f \in S_n$ *läßt sich mittels*

$$k_i, d_i, \; i = 1, \dots, n$$

erzeugen.

Wir wenden Lemma 11 nun auf den Sonderfall der Addition an.

Korollar 12. *Ist* $f \in S(D)$ *und* $D \subset \mathbb{B}^{2 \cdot n}$ *und ist* f *invariant unter* G*, soweit die Anwendung von* G *nicht aus* D *herausführt, dann läßt sich* f *mittels*

$$\{k'_i, d'_i \mid i = 1, \dots, n\}$$

erzeugen, wenn sich k'_i *und* d'_i *durch die Einschränkung von* k_i *bzw.* d_i *auf* D *ergeben.*

Beweis. Ist f' die in dem Beweis von Lemma 11 definierte Fortsetzung von f auf $\mathbb{B}^{2 \cdot n}$, dann ist f invariant unter G. Also läßt sich f' aufgrund von Satz 19 durch $\{k_i, d_i\}$ erzeugen. Hieraus folgt die Behauptung, wenn wir uns daran erinnern, daß die Einschränkung $f \mid D$ einen Homomorphismus von S_n auf $S(D)$ definiert. □

Korollar 13. *Ersetzt man in* $\{k_i, d_i \mid i = 1, \dots, n\}$ *eines oder mehrere der* k_i *oder* d_i *durch* $(x_i \oplus y_i)$*, dann erhält man ein äquivalentes Erzeugendensystem.*

Beweis. Es gilt $\overline{k_i} \cdot d_i = (x_i \oplus y_i)$ und $d_i = k_i \cup (x_i \oplus y_i)$. □

Wir haben die Hierarchie

$$\Delta_{2^k} \subset \Delta'_{2^{k-1}} + \tilde{\Delta}_{2^{k-1}} \subset \dots \subset \sum_{l=1}^{n} \Delta(x_i, y_i)$$

verwendet um einfache Darstellungen für Erzeugende von Δ_{2^k} zu berechnen. Wir haben bei unseren Umformungen Relationen zwischen verschiedenen Funktionen verwendet, ohne uns aber Rechenschaft darüber abzulegen, welche Relationen in welcher Stufe der Darstellungen gelten. Wenn man die betrachteten Verfahren automatisch verwenden will, dann muß man solche Relationen auch automatisch erkennen. Aus diesem Grund gehen wir hier auf diese Relationen kurz grundsätzlich ein. Wir knüpfen hier an 3.4 an:

Fassen wir z.B. $\{k_i, d_i \mid i = 1, \dots, n\}$ als freies Erzeugendensystem auf, dann stehen uns genau die Rechenregeln der booleschen Algebra zur Verfügung. Es gilt aber $k_i \cdot \overline{d_i} = 0$ als zusätzliche Relation. Wir fragen uns, wie die Menge aller dieser zusätzlichen Rechenregeln aussieht. Dazu sei $u = (u_1, \dots, u_n)$, $v = (v_1, \dots, v_n)$ ein freies Erzeugendensystem. Es gilt dann der

Satz 20. *Sei $S_2n = \langle u_1, \ldots, u_n, v_1, \ldots, v_n\rangle$ und $\mathcal{B} = \langle k_1, d_1, \ldots, k_n, d_n\rangle$ wie oben definiert. Ist $r = v_1\ \overline{u}_1 \vee \ldots \vee v_n\ \overline{u}_n$, dann ist $\mathcal{B} \cong S_n/r$.*

Beweis. Wir betrachten den durch $h(u_i) = k_i, h(v_i) = d_i$ für $i = 1, \ldots, n$ definierten Homomorphismus $h : S_n \longrightarrow \mathcal{B}$. Wie man leicht sieht, gelten die folgenden Relationen.

$$\begin{aligned} h(u_1 \cdot v_1) &= k_1, & h(\overline{u}_1 \cdot v_1) &= \overline{k}_1 \cdot d_1, \\ h(u_1 \cdot \overline{v}_1) &= 0, & h(\overline{u}_1, \overline{v}_1) &= \overline{k}_1 \cdot \overline{d}_1. \end{aligned}$$

Es liegt also $r = u_1\overline{v}_1 \vee \ldots \vee u_n\overline{v}_n$ in $h^{-1}(0)$ und damit gilt auch $(r) \subset h^{-1}(0)$. Wir zeigen, daß auch $h^{-1}(0) \subset (r)$ gilt. Dazu betrachten wir ein Atom $a \in S_n$ mit $h(a) = 0$. Wir können jedes Atom in der Form $a = u_1^{\varepsilon_1} \cdot v_1^{\delta_1} \cdot \ldots \cdot u_n^{\varepsilon_n} \cdot v_n^{\delta_n}$ darstellen. Damit gilt

$$h(a) = k_1^{\varepsilon_1} \cdot d_1^{\delta_1} \cdot \ldots \cdot k_n^{\varepsilon_n} \cdot d_n^{\delta_n}.$$

Ist $(\varepsilon_i, \delta_i) \neq (1, 0)$, dann gibt es eine Einsetzung (ξ_i, η_i) mit $k_1^{\varepsilon_i} \cdot d_1^{\delta_i}(\xi_i, \eta_i) = 1$. Aus $h(a) = 0$ folgt, daß es für mindestens ein i keine solche Einsetzung gibt. Also gilt für ein i $(\varepsilon_i, \delta_i) = (1, 0)$. Nun ist $u_i\overline{v}_i < r$ und also $u_i \cdot \overline{v}_i \in (r)$. Hieraus folgt $a \in (r)$. Da für jedes Atom a aus $h(a) = 0$ $a \in (r)$ folgt, ergibt sich auch für jedes f mit $h(f) = 0$, daß $f \in (r)$ ist. Also ist $(r) = h^{-1}(0)$, was zu zeigen war. □

Wenn auch, wie Satz 20 zeigt, Δ_n nicht frei ist über 2^n Variablen, so könnte doch $S_m \cong \sum_{i=1}^{n} \langle k_i, d_i\rangle$ für ein $m < n$ gelten. Der Satz 21 besagt, daß das nicht so ist.

Satz 21. *$\mathcal{B} = \langle k_1, d_1, k_2, d_2, \ldots, k_n, d_n\rangle$ ist nicht frei. Minimale Erzeugendensysteme von $\mathcal{B}$ besitzen $\lceil n \cdot \log 3\rceil$ Erzeugende.*

Beweis. Wir setzen $\mathcal{B} = \langle k_1, d_1\rangle + \langle k_2, d_2\rangle + \ldots + \langle k_n, d_n\rangle$. $\langle k_i, d_i\rangle$ enthält die drei Atome $x_i \cdot y_i$, $\overline{x}_i \cdot y_i \vee x_i \cdot \overline{y}_i$, $\overline{x}_i \cdot \overline{y}_i$. Ist $\mathcal{B}_1, \mathcal{B}_2 \subset \mathcal{B}$ und ist $\mathcal{B}_1 \cap \mathcal{B}_2 = \{0, 1\}$, dann ist $A(\mathcal{B}_1 + \mathcal{B}_2) = A(\mathcal{B}_1) \cdot A(\mathcal{B}_2)$. Also hat $\mathcal{B}$ 3^n Atome. Es ist also $\sharp\mathcal{B} = 2^{3^n}$, woraus die Behauptung folgt. □

Erläuterungen: Faßt man $k_1, \ldots, k_n, d_1, \ldots, d_n$ als freie Erzeugende einer booleschen Algebra auf und faktorisiert man diese Algebra nach den Relationen $k_i \cdot \overline{d_i}$, dann erhält man $\mathcal{B}$ als Quotienten.

Wir stellen in Abbildung 13 Figur 1 das Atom a_2 von Δ_2 in einer 2-dimensionalen Tabelle dar. Die Kästchen ohne Eintrag repräsentieren den Eintrag 0.

In der Abbildung 13 Figur 2 und 3 stellen wir die Einbettungen $a_2^{(4)}$ und $b_4^{(4)}$ von a_2 bzw. a von Δ_2 in S_4 dar. Abbildung 13 Figur 4 stellt das Produkt $a_2^{(4)} \cdot b_4^{(4)}$ dar.

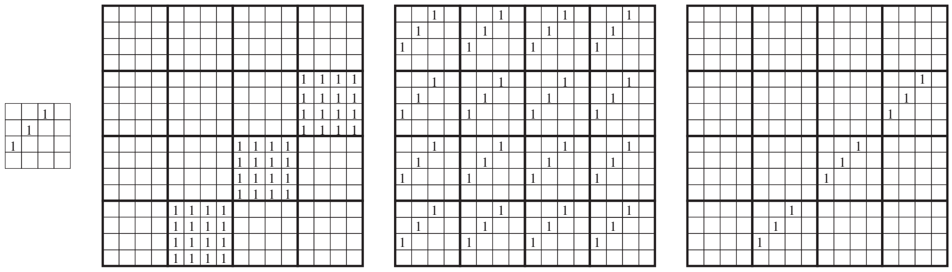


Fig. 1 Fig. 2 Fig. 3 Fig. 4

Abbildung 13:

Wenn man in Abbildung 13 Figur 4 die Diagonale vervollständigen will, dann kann man das tun, indem man die eine Nachbardiagonale von $b_4^{(4)}$, in unserem Fall $b_3^{(4)}$ wählt, und zu $a_2^{(4)}$ die Diagonale $a_6^{(4)}$, so daß man für das Atom a_{18} aus Δ_4

$$a_{18} = a_2^{(4)} \cdot b_4^{(4)} \cup b_3^{(4)} \cdot a_6^{(4)}$$

erhält.

Schön wäre es, wenn man mit Variablensymmetrien allein auskäme.
Wir haben diesen Abschnitt mit der Beobachtung begonnen, daß ad_n invariant ist unter der Vertauschung $x_i \longleftrightarrow y_i$ für $i = 1, \ldots, n$, und haben hieraus als Basis für die Algebra, die unter der hierdurch erzeugten Gruppe invariant ist, $E_d = \{d_i, k_i \mid i = 1, \ldots, n\}$ abgeleitet. Das legt es nahe, sich zunächst einmal auf Untergruppen der Permutationsgruppe der *Erzeugenden* der Algebra zu beschränken. Folgen wir dieser Idee, dann müssen wir im zweiten Schritt ad_n über E_d oder $E_e := \{e_i, k_i \mid i = 1, \ldots, n\}$ darstellen und anschließend untersuchen, welche Invarianzeigenschaften diese Funktion hat. Nun sind E_d und E_e keine freien Erzeugendensysteme, wie wir in Satz 20 gesehen haben. Das bedeutet, daß wir unter Anwendung der zugehörigen Relationen (r) Symmetrien erhalten können, die sich sonst nicht ergeben würden (siehe 3.4). Wir wollen das etwas näher erläutern.

Wir betrachten die durch E_e definierte Abbildung

$$[e] := [e_1, e_2, \ldots, e_n, k_1, k_2, \ldots, k_n] \; : \; \mathbb{B}^{2n} \to \mathbb{B}^{2n}.$$

Da E_e nicht frei ist, gilt

$$D := [e](\mathbb{B}^{2n}) \subsetneq \mathbb{B}^{2n}.$$

$$\begin{tikzcd} \mathbb{B}^{2n} \arrow[rr, "ad_n"] \arrow[d, "{[e]}"'] & & \mathbb{B}^{n+1} \\ D \arrow[urr, dashed, "F"] & & \end{tikzcd}$$

Wenn wir $[e]$ als eine erste Stufe zur Realisierung einer Darstellung verwenden wollen, dann müssen wir eine Funktion F finden, die das nebenstehende Diagramm erfüllt. Jede Darstellung definiert, wenn wir sie durch boolesche Ausdrücke beschreiben, aber eine Funktion $F' : \mathbb{B}^{2n} \to \mathbb{B}^{n+1}$. Das heißt, daß wir bei allen Darstellungen Fortsetzungen von F auf ganz $\mathbb{B}^{2n}$ realisieren.

$$\begin{tikzcd} \mathbb{B}^{2n} \arrow[rr, "ad_n"] \arrow[d, "{[e]}"'] & & \mathbb{B}^{n+1} \\ D \arrow[urr, "F"] \arrow[rr, "inclusion"] & & \mathbb{B}^{2n} \arrow[u, "F'"'] \end{tikzcd}$$

Die Situation ist also wie sie durch das nebenstehende Diagramm beschrieben wird. Die Symmetrien in den Variablen hängen ganz offensichtlich von der Fortsetzung ab. D wird i.allg. nicht unter der Symmetriegruppe von F' abgeschlossen sein. Es genügt also nicht, wenn man alle Möglichkeiten ausschöpfen will, sich auf die Symmetrien der Funktion F zu beschränken, sondern man muß alle möglichen Symmetrien unter dem Aspekt der Fortsetzbarkeit von F diskutieren. *Ch. Scholl* hat in seiner Dissertation zur Lösung dieses Problems eine Heuristik entwickelt und in ein erstaunlich effizientes Programm umgesetzt [Sch97]. Um aber zu erfolgreichen Anwendungen zu gelangen, genügte dieser Schritt nicht, wie wir jetzt erläutern werden.

Betrachten wir E_e, dann entdecken wir, daß sich F zu einer Abbildung F' fortsetzen läßt, die unter den Vertauschungen

$$e_{i-1} \longleftrightarrow k_i \text{ für } i = 1, \dots, n-1$$

invariant ist. Man sieht das sofort ein, wenn man sich erinnert, daß $e_i = x_i \oplus y_i$ und $k_i = x_i \cdot y_i$ der Übertrag ist, der in der Schule unter e_{i-1} geschrieben wird. Wir verdeutlichen das in dem folgenden Diagramm, das die zweite Stelle von ad_2 als Funktion von e_1, k_1, e_2, k_2 darstellt. Man beachte, daß die Reihenfolge von e_1, k_1 und e_2, k_2 auf den beiden Seiten verschieden ist.

Wir finden wie früher als mögliche Basis für die zugehörige Algebra der unter dieser Gruppe invarianten Funktionen

$$\begin{aligned} & e_0^2 := k_1, e_1^2 := e_1 \oplus k_2, k_1^2 := e_1 \cdot k_2, \\ \dots, \quad & e_{n-1}^2 := e_{n-1} \oplus k_n, k_{n-1}^2 := e_{n-1} \cdot k_n, e_n^2 = e_n \end{aligned}$$

Diesen Schritt kann man wiederholt anwenden. Man erhält so schließlich

$$e_0^n, e_1^n, e_2^{n-1}, \dots, e_{n-2}^3, e_{n-1}^2, e_n$$

als Basis für Δ_n. Allerdings besitzt diese Konstruktion die Tiefe n. Daran ändert sich auch nichts, wenn wir diese Basen zunächst für $\Delta_{1,n}$ und $\Delta_{n+1,n+m}$ berechnen, um daraus die Basis für Δ_{n+m} zu konstruieren, da sich der Übertrag in $\Delta_{1,n}$ über n Stellen hinweg fortpflanzen muß. Man benötigt hier eine weitere Idee. Diese Idee besteht darin auszunutzen, daß die Funktion ad_n in gewissem Sinne schwach zusammenhängend ist. Dieser schwache Zusammenhang ist für $h(x_1, \dots, x_n, z_1, \dots, z_m)$ z.B. gegeben, wenn es Funktionen $g : \mathbb{B}^m \to \mathbb{B}$ und $f : \mathbb{B}^{n+1} \to \mathbb{B}$ gibt, so daß $h(x, z) = f(g(x), z)$ ist. Man spricht hier von einer Ashenhurst-Zerlegung [A]. In diesem Fall der Shannon-Zerlegung [Sha49] (Abbildung 14)

$$f(z_0, z) = z_0 \cdot f(1, z) \vee \overline{z}_0 \cdot f(0, z)$$

erhält man die Realisierung

$$h(x, z) = g(x) \cdot f(1, z) \vee \overline{g(x)} \cdot f(0, z).$$

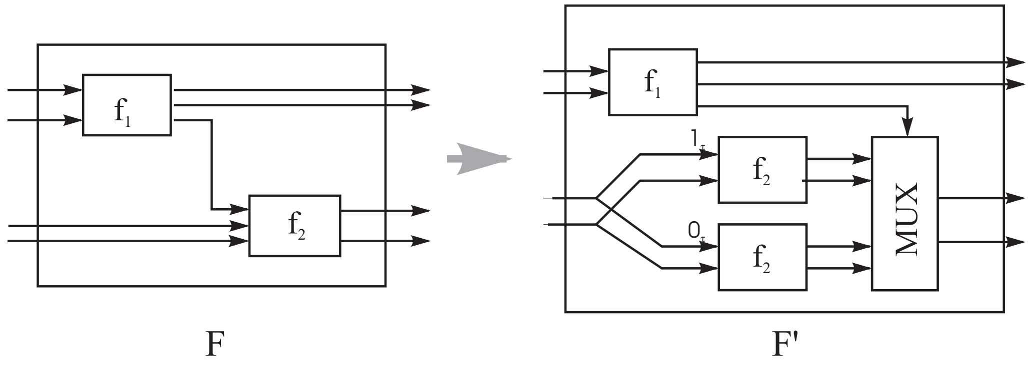


Abbildung 14:

Die Transformation, die die erste Darstellung von h in die zweite überführt, reduziert die Tiefe. Es gilt nämlich, wenn wir mit F, G zu den Funktionen f, g gehörige Darstellungen und mit H_1, H_2 die zu der ersten bzw. zweiten Zerlegung von h gehörigen Darstellungen bezeichnen,

$$\text{Tiefe } (H_1) \leq \text{Tiefe } (F) + \text{ Tiefe } (G)$$

und

$$\text{Tiefe } (H_2) \leq \max\{ \text{ Tiefe } (F), \text{ Tiefe } (G)\} + 2.$$

Man hat also die Chance, durch diese Zerlegungen die Tiefe der Netze zu reduzieren. Man bezahlt i.allg. mit einem erhöhten Aufwand hinsichtlich der Realisierung von f. Iteriert man die Shannon-Zerlegung, so erhält man ja exponentiell mit der Anzahl der Variablen wachsende Kosten.

Es stellt sich die Frage, wie man Ashenhurst-Zerlegungen finden kann. Haben wir eine Invarianz von h unter der Gruppe G von Variablenpermutationen, dann zeigen unsere Sätze, daß sich h durch Erzeugendensysteme von $\mathcal{B}(G)$ darstellen läßt. Ist G auf der Menge der Variablen nicht transitiv, dann erzeugt G Äquivalenzklassen von Variablen („Cliquen" von Variablen), die zu Basisfunktionen von $\mathcal{B}(G)$ führen, die nur von diesen Variablen abhängen. Diese Basisfunktionen führen zu Ashenhurst-Zerlegungen von h.

Haben wir umgekehrt eine solche Zerlegung von h, dann ist h invariant unter jeder Gruppe G von Permutationen auf $\mathbb{B}^n$, die g invariant lassen. Also ist G eine Untergruppe von $G(\mathcal{B}, h)$. Das zeigt, daß unser Ansatz einer Galois-Theorie der booleschen Funktionen die Ashenhurst-Shannon-Zerlegung (AS-Zerlegung) mit liefert. Die Schwierigkeit besteht darin, geeignete Gruppen zu bestimmen.

Gehen wir davon aus, daß wir eine Variablen-Symmetriegruppe G gefunden haben, dann stellt sich die Frage, wie man zugehörige AS-Zerlegungen findet. Hierbei ist es hilfreich, wenn man Funktionen durch binäre Entscheidungsdiagramme (BDDs) repräsentiert, die so ausgewählt sind, daß die oben erwähnten Äquivalenzklassen von Variablen benachbart gruppiert sind.

Damit haben wir die drei Konzepte genannt, die den Kern der Scholl'schen Heuristik ausmachen.

1. Repräsentation der Funktionen durch BDDs.

2. Bestimmung von Variablensymmetrien von Funktionen $f : D \to \mathbb{B}$ mit $D \subsetneq \mathbb{B}^n$.

3. Konstruktion der zur Symmetrie gehörigen AS-Zerlegung.

Die Addition ist ein Beispiel dafür, daß man mit der iterativen Anwendung dieses Konzeptes sehr gute Resultate erzielen kann. Es ist Ch. Scholl gelungen, mit seinem universell angelegten Programm für ad_N, $N \leq 64$ eine Version des c.s.–Addierers auf Basis einer allgemeinen Spezifikation der Addition zu berechnen.

4.2 Total symmetrische Funktionen

Eine Abbildung $f : \mathbb{B}^n \to \mathbb{B}$ heißt total symmetrisch, wenn sie invariant ist unter jeder Permutation der Variablen, d.h. ist

$$\xi = (\xi_1, \dots, \xi_n) \in \mathbb{B}^n \text{ und ist } \xi' = (\xi_{i_1}, \dots, \xi_{i_n}),$$

dann gilt$f(\xi) = f(\xi')$ für jede Permutation $\pi = \binom{1 \ \dots \ n}{i_1 \ \dots \ i_n}$. Die Gruppe der Permutationen von n Elementen bezeichnen wir mit $\mathfrak{S}_n$.

Wir betrachten einige Beispiele:

4.2.1 Sortierfunktion

Ist M eine Menge auf der eine Ordnungsrelation $\leq$ definiert ist, dann heißt $s : M^n \to M^n$ *Sortierfunktion* genau dann, wenn für jedes $\xi \in M^n$ die beiden folgenden Bedingungen gelten.

(1) ξ und $s(\xi)$ enthalten jedes Element in der gleichen Vielfachheit.

(2) Ist $s(\xi) = (\eta_1, \dots, \eta_n)$, dann gilt

$$\eta_i \geq \eta_{i+1} \text{ für } i = 1, \dots, n-1.$$

Offensichtlich gilt

$$s(\xi) = s(\pi(\xi))$$

für jede Permutation $\pi : [1:n] \to [1:n]$, wenn wir $\pi(\xi)$ für $(\xi_{i_1}, \dots, \xi_{i_n})$ schreiben.

Das Sortierproblem besteht in der Aufgabe eine der Sortierfunktionen s effizient zu berechnen. Zwei Grenzfälle verdienen ein besonderes Interesse.

- Die Länge n der zu sortierenden Folge ist groß gegenüber der Anzahl der Elemente von M. Also $n \gg \#M$.
- $\#M \gg n$. Es liegt stets nur eine Teilmenge von M als zu sortierende Folge vor.

Man kann diese Unterscheidung noch verfeinern, indem man die Repräsentation der Elemente von M z.B. durch Folgen über einem vorgegebenen Alphabet heranzieht. Wir wollen annehmen, daß $M = \mathbb{B}^m$ ist. Der erste Fall ist erfüllt, wenn $n \gg 2^m$ ist. Der zweite Fall gilt z.B., wenn $n \ll m$ ist. Der zweite Fall läßt sich leicht auf den ersten Fall zurückführen, wenn die Auswahl der Elemente aus M zufällig ist, d.h. wenn die Elemente der zu sortierenden

Folge mit gleicher Wahrscheinlichkeit gezogen werden. In diesem Fall genügt es, nach den ersten $2 \cdot \lceil \log n \rceil$ Stellen der Elemente der Folgen zu sortieren, um mit hoher Wahrscheinlichkeit das Sortierproblem zu lösen. Dieser Fall tritt aber nur selten auf. Große Objekte, die in Sortierproblemen auftreten, sind nicht zufällig erzeugt. Man denke dabei etwa an Bilder, die so abgelegt werden sollen, daß man sie leicht wiederfindet. Die einfachste Annahme, die den praktisch auftretenden Problemen etwas näher kommt, besteht in der Betrachtung von Markovprozessen, die diese Objekte erzeugen. Sind diese Prozesse nicht zu „träge“ , dann kann man an die Stelle der ersten $c \cdot \lceil \log n \rceil$ Stellen „zufällig“ ausgewählte $\lceil \log n \rceil$ Stellen aus den Objekten auswählen und so verfahren wie vorher. Wir setzen uns hier nur mit dem im ersten Punkt beschriebenen Fall auseinander. Im übrigen verweisen wir auf die für das Sortieren einschlägige Literatur. Den Aspekt des Sortierens bei Quellen mit Gedächtnis findet man in [HZ97] ausgeführt.
Wir betrachten hier den Fall $M = \mathbb{B}$ ausführlich und skizzieren die Verallgemeinerung auf den Fall $m > 1$.

4.2.2 Elementarsymmetrische Funktionen

Ein Polynom in den Variablen $x_1, \ldots, x_n$ und mit Koeffizienten aus einem Ring heißt elementarsymmetrisch, wenn es die Form

$$\sigma_l(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \ldots < i_n \leq n} x_{i_1} \cdot \ldots \cdot x_{i_l}, \; l = 0, \ldots, n$$

hat; l heißt der Grad von σ_l. Offensichtlich ist $\sigma_l(x) = \sigma_l(\pi(x))$ für jede Permutation π der Variablen $x = (x_1, \ldots, x_n)$.

Jede totalsymmetrische Funktion läßt sich aus den elementarsymmetrischen erzeugen. Wir betrachten hier nur den Fall der booleschen Algebra, indem einiges einfacher ist und in dem auch einige Besonderheiten gelten.

Zunächst bemerken wir die enge Verwandtschaft zwischen der Sortierfunktion und den elementarsymmetrischen Funktionen.

Satz 22. *Unter der Verwendung der eben eingeführten Bezeichnung gilt für* $\xi \in \mathbb{B}^n$

$$s(\xi) = (\sigma_1(\xi), \sigma_2(\xi), \ldots, \sigma_n(\xi)).$$

Der Satz besagt, daß sich im Falle der booleschen Algebra durch Anwendung der elementarsymmetrischen Polynome sortieren läßt und daß sich umgekehrt die elementarsymmetrischen Polynome simultan durch Sortieren berechnen lassen.

Beweis. Man erkennt, daß

$$\sigma_l(\xi) = 1 \iff \sum_{i=1}^{n} \xi_i \geq l$$

gilt. Hieraus folgt $s(\xi)_l = 1$ und umgekehrt folgt daraus auch $\sum \xi_i \geq l$. $\square$

Da man das Sortierproblem auf Computern in $n \cdot \log n$ Zeit lösen kann, kann man damit auch $\sigma_1, \ldots, \sigma_n$ simultan in dieser Zeit berechnen. Uns geht es hier aber um das Berechnen in der booleschen Algebra, so daß wir das Problem etwas genauer anschauen.

Zunächst zeigen wir:

Satz 23. *Ist $\Sigma_n = \{f \in S_n \mid f$ total symmetrisch$\}$, dann gilt*

$$\Sigma_n = \langle \sigma_1, \ldots, \sigma_n \rangle.$$

Beweis. Wir müssen zeigen, daß sich jede Abbildung f aus der booleschen Algebra der totalsymmetrischen Abbildungen mittels $\sigma_1, \ldots, \sigma_n$ erzeugen läßt.

Sei $a \in S_n$ ein Atom, $f \in \Sigma_n$ und $f \cdot a \neq 0$. Dann ist $\mathfrak{S}(a)$ Atom von Σ_n (Satz 11) und $\mathfrak{S}(a) \cdot f \neq 0$. Da wir f als Vereinigung von Atomen von Σ_n darstellen können, genügt es zu zeigen, daß sich jedes Atom von Σ_n mittels $\sigma_1, \ldots, \sigma_n$ erzeugen läßt.

Ist $a = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ mit $\alpha_1 + \alpha_2 + \ldots + \alpha_n = l$, dann gilt $x_1 \cdot \ldots \cdot x_l \cdot \overline{x}_{l+1} \cdot \ldots \cdot \overline{x}_n \leq \mathfrak{S}(a)$. Nun gilt weiter

$$x_1 \cdot \ldots \cdot x_l \cdot \overline{x}_{l+1} \cdot \ldots \cdot \overline{x}_n \leq \sigma_l \cdot \overline{\sigma}_{l+1}.$$

Da σ_l und σ_{l+1} in Σ_n liegen, gilt auch

$$\mathfrak{S}(a) \leq \sigma_l \cdot \overline{\sigma}_{l+1}.$$

Gilt für $\xi \in \mathbb{B}^n$ $\sigma_l \cdot \overline{\sigma}_{l+1}(\xi) = 1$, dann ist

$$l \geq \sum_{i=1}^{n} \xi_i < l + 1, \text{ so daß wir } \sum_{i=1}^{n} \xi_i = l$$

haben. Hieraus folgt

$$\mathfrak{S}(a)(\xi) = 1.$$

Da das für alle solchen ξ gilt, haben wir

$$\sigma_l \cdot \overline{\sigma}_{l+1} \leq \mathfrak{S}(a),$$

woraus nun

$$\mathfrak{S}(a) = \sigma_l \cdot \overline{\sigma}_{l+1}$$

folgt. Also erzeugen $\sigma_1, \ldots, \sigma_n$ ganz Σ_n, was zu zeigen war. $\square$

Korollar 14. *Jede Abbildung $f \in \Sigma_n$ läßt sich mit Kosten*

$$C(f) \leq C(\sigma_1, \ldots, \sigma_n) + 2 \cdot n - 1$$

in Tiefe

$$T(f) \leq T(\sigma_1, \ldots, \sigma_n) + \lceil \log n \rceil + 1$$

erzeugen.

Beweis. Σ_n besitzt $n+1$ Atome, die sich simultan je mit Kosten 1 darstellen lassen. Jedes $f \in \Sigma_n$ läßt sich als Vereinigung von höchstens n der Atome darstellen. Hieraus folgt die Behauptung. $\square$

Es bleibt die Frage nach einer effizienten Darstellung der σ_i zu beantworten. Hierzu ziehen wir die Relation

$$\sigma_l(\xi) = 1 \iff \Sigma\, \xi_i \geq l$$

heran. Wir erhalten hierdurch Zugang zu einem anderen, kleineren Erzeugendensystem von Σ_n:

Sei also

$$sum\ :\ \mathbb{B}^n \to \mathbb{B}^k,\ k = \lceil \log n \rceil$$

und

$$\sum_{i=1}^{n} \xi_i = [sum(\xi)].$$

Wir setzen

$$\mu_l(\xi) = sum(\xi)_l \text{ für } \xi \in \mathbb{B}^n,\ l \in [1:k];$$

μ_l gibt also die l-te Komponente der Darstellung der Summe der Komponenten von ξ im Dualsystem an.

Satz 24.

$$\langle \mu_1, \dots, \mu_k \rangle = \Sigma_n.$$

Beweis. Es genügt zu zeigen, daß sich die Atome von Σ_n in den $\mu_1, \dots, \mu_k$ darstellen lassen. Ist $l = [\varepsilon_1, \dots, \varepsilon_k]$, $\varepsilon_i \in \mathbb{B}$, dann gilt

$$\mu_1^{\varepsilon_1} \cdot \ldots \cdot \mu_k^{\varepsilon_k} = \sigma_l \cdot \overline{\sigma}_{l+1}.$$

Hieraus folgt die Aussage des Satzes. □

Um zu einer ersten Abschätzung des Sortierens zu gelangen, geben wir eine Darstellung von σ_l auf Basis von μ. Es gilt

$$[\mu(\xi)] \geq l \quad \leftrightarrow \quad \sigma_l(\xi) = 1.$$

Es genügt also, $[\mu(\xi)] \geq l$ darzustellen. Wir tun das, indem wir simultan die Funktionen $[\xi] > [\eta]$ und $[\xi] = [\eta]$ für $\xi, \eta \in \mathbb{B}^k$ darstellen. Hierbei nehmen wir an, daß $m = 2^k$ ist. Beide Funktionen fassen wir zu einem Baustein zusammen und bezeichnen den Baustein mit $>_k$. Offensichtlich gilt

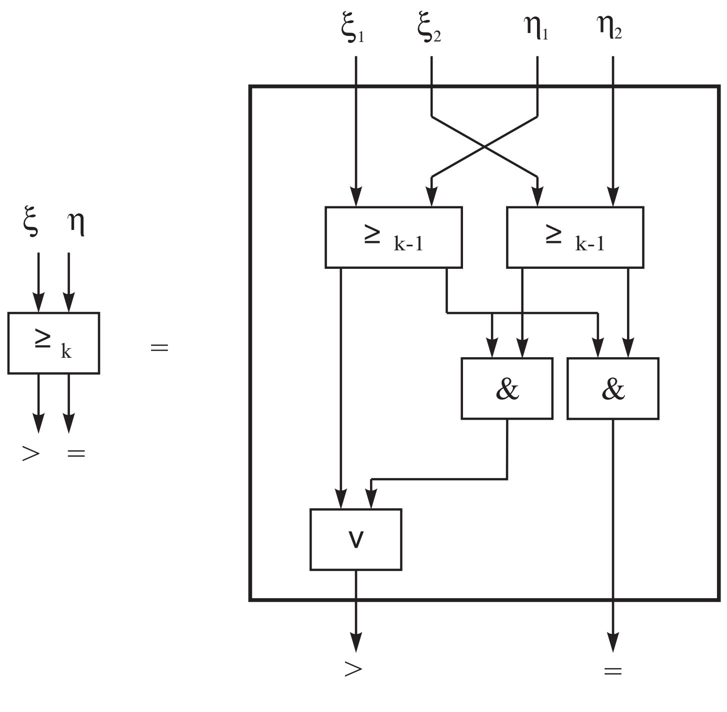


Abbildung 15:

wenn wir $\xi = (\xi_1, \xi_2)$, $\eta = (\eta_1, \eta_2)$ und $\xi_i, \eta_i \in \mathbb{B}^{\frac{k}{2}}$ verwenden. Weiter gilt

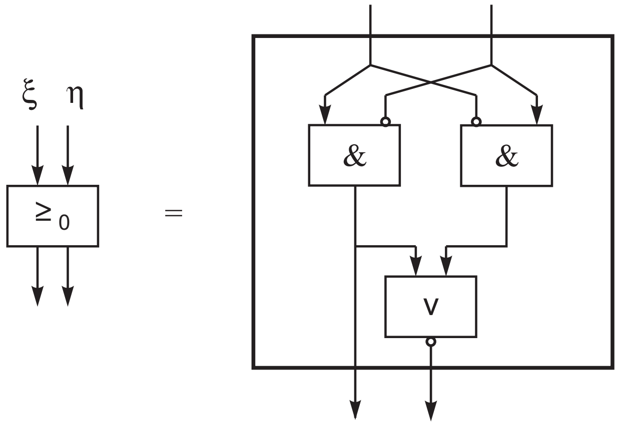


Abbildung 16:

für $\xi, \eta \in \mathbb{B}$.

Bezeichnen wir mit C_k die $\{\&, \vee\}$-Gattergröße des Schaltkreises, dann gilt

$$C_k = 2 \cdot C_{k-1} + 3 \quad \text{und} \quad C_0 = 3.$$

Hieraus erhält man $C_k = 6 \cdot m - 3$.

Wir fassen das Resultat zusammen in

Lemma 15. Die Vergleichsfunktionen $>$ und $=$ für $\xi, \eta \in \mathbb{B}^m$, $m = 2^k$ lassen sich simultan durch ein Netz der Größe $6 \cdot m - 3$ und der Tiefe $2 \cdot \log m + 2$ realisieren.

Beweis. Zum vollständigen Beweis fehlt nur noch die Abschätzung der Tiefe. Wir haben, wenn T_k die Tiefe des Netzes bezeichnet

$$T_k = T_{k-1} + 2 \quad \text{und} \quad T_0 = 2$$

Hieraus ergibt sich $T_k = 2 \cdot (k + 1)$, woraus die Behauptung des Lemmas folgt. □

Wir kehren zurück zur Darstellung von σ_l. Wir erhalten diese Darstellung, indem wir als Eingänge von $<_k$ die variable Eingabe ξ und für die zweite Eingabe $[\eta_l] = l$ fixieren. Wir erhalten damit die Darstellung in Abbildung 17 für σ_l.
Legen wir für η nun konstante Werte an, dann erhalten wir im Falle $k = 0$ für den Parameter $\eta = 0 : \sigma_0^0(\xi) = 1$ und $\sigma_1^0(\xi) = \xi$ für $\eta = 1$.

Wir erhalten durch eine einfache Reduktion Abbildung 18.

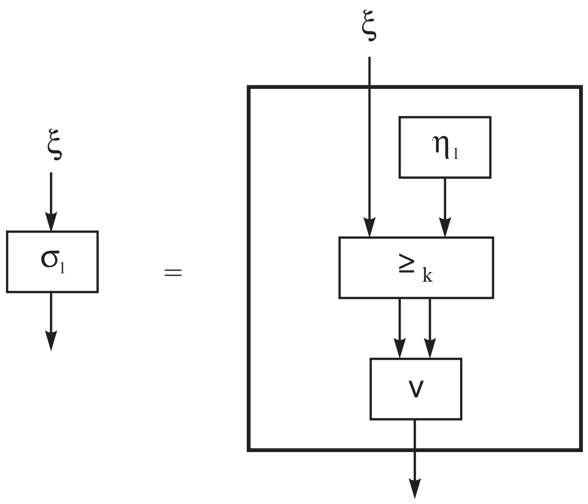


Abbildung 17:

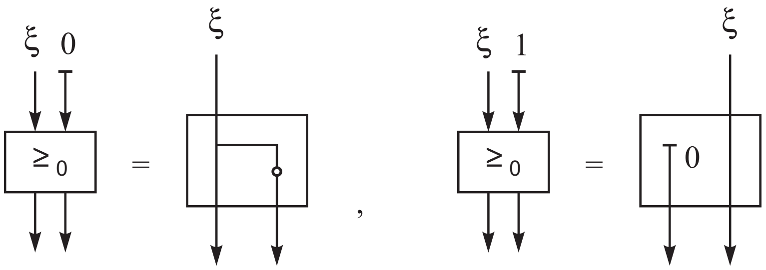


Abbildung 18:

Die Gatterkosten für $\geq_0$ sind also 0. Damit erhalten wir für die Darstellung der Kosten C'_k des in Abhängigkeit von der Konstanten η_l realisierten Schaltkreises

$$C'_k \leq 2 \cdot C'_{k-1} + 3 \quad \text{und} \quad C'_0 = 0.$$

Hieraus ergibt sich $C'_k \leq 3 \cdot m - 3$.

Unsere Konstruktion liefert uns also für die simultane Berechnung aller σ_l im Falle $m = 2^k$ ein Netz mit Kosten $\leq 3 \cdot m \cdot \log m - 3m$ und Tiefe $\leq 2 \cdot \log m$. Wir fassen das Resultat zusammen in

Korollar 15. *Die Sortierfunktion* $s \ : \ \mathbb{B}^m \rightarrow \mathbb{B}^m$ *läßt sich auf Basis von* $\mu_1, \ldots, \mu_k$, $m = 2^k$ *mit Kosten* $< 3 \cdot m \cdot \log m - 3m$ *in Tiefe* $2 \log m$ *realisieren.*

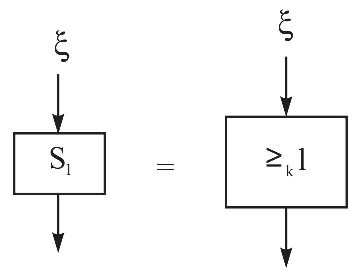


Abbildung 19:

Eine effizientere Lösung

Das Sortieren über der Basis $\{\mu_1, \ldots, \mu_k\}$ läßt sich allerdings wesentlich effizienter realisieren. Wir beschreiben ein solches Verfahren rekursiv für die Fälle $N = 2^k - 1,\ k \in \mathbb{N}$.
Wir konstruieren also ein Netz mit den Eingängen $\mu_1, \mu_2, \ldots, \mu_k$ und $2^k - 1$ Ausgängen. Hierzu definieren wir induktiv Netze S_j für $j = 1, \ldots, k$. S_j besitzt $\mu_{k-j+1}, \ldots, \mu_k$ als Eingänge und $2^j - 1$ Ausgänge. Wir setzen $S_1 = \mu_k$ und definieren S_{j+1} durch Abbildungen 19 und 20.

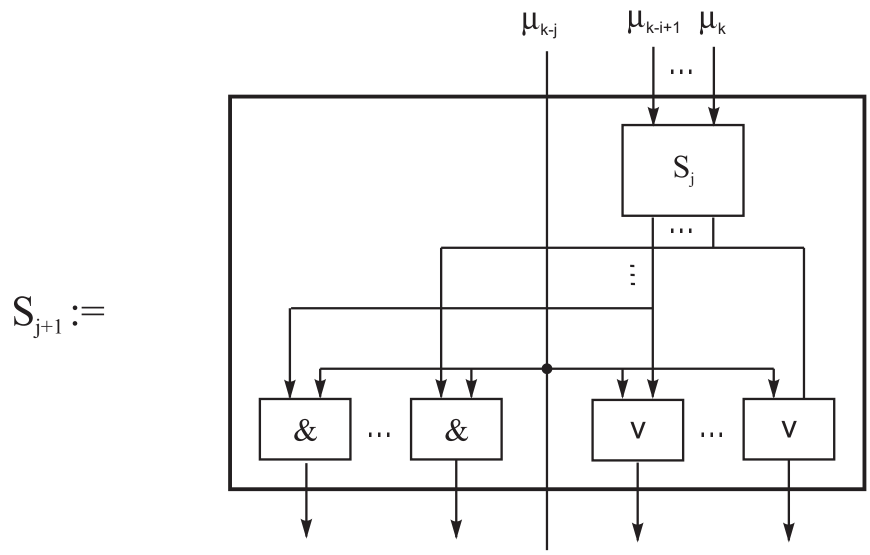


Abbildung 20:

Wir zeigen, daß S_k das Sortierproblem löst, indem es an den Ausgängen $l = [\mu(\xi)], l+1, \ldots, 2^k - 1$ eine 1 und für $j < l$ eine 0 ausgibt.
Den Beweis führen wir in zwei Schritten.

1. Falls der Ausgang j von S_k eine 1 liefert, dann gilt das auch für die Ausgänge $j' \geq j$.

2. Das Netz liefert an dem Ausgang $\mu(\xi) - 1$ eine 0.

Beweis. Ad 1: Wir beweisen diese Eigenschaft für alle Netze S_j. Für $j = 1$ ist die Behauptung richtig, da S_1 nur einen Ausgang besitzt.

Wir nehmen an, daß die Eigenschaft für S_j zutrifft. In dem Fall $\mu_{k-j}(\xi) = 1$ sind alle Ausgänge mit den Positionen $2^j, \ldots, 2^{j+1} - 1$ gleich 1, wie sich aus der Definition von S_{j+1} unmittelbar ergibt. Da die Ausgänge $1, \ldots, 2^j - 1$ von S_{j+1} wegen $\mu_{k-j}(\xi) = 1$ die gleichen Werte haben wie die entsprechenden Ausgänge von S_j, gilt unsere Behauptung 1 in dem Fall $\mu_{k-j}(\xi) = 1$ allgemein.

In dem anderen Fall, $\mu_{k-j}(\xi) = 0$, haben aufgrund der Konstruktion von S_{j+1} die Ausgänge $1, \ldots, 2^j$ den Wert 0. Die Ausgänge $l = 2^j + m$ haben die gleichen Werte wie die Ausgänge $m = 1, \ldots, 2^j - 1$ von S_j. Also gilt die Behauptung 1 auch in diesem Fall.

Ad 2: Aus den Ausführungen unter Ad 1 folgt, daß der i-te Eingang genau $\mu_{k-j}(\xi) \cdot 2^j$ Einsen an den Ausgängen beiträgt. Also liefert das Netz bei der Eingabe $(\mu_1(\xi), \ldots, \mu_k(\xi))$ genau $\sum_{j=1}^{k} \mu_{k-j}(\xi) \cdot 2^j$ Einsen an den Ausgängen. Da die Einsen in einem Block rechts auftreten, folgt die Behauptung.

□

Wir schätzen die Tiefe und die Größe von S_k ab. Offensichtlich gilt Tiefe $(S_1) = 0$ und Tiefe (S_{j+1}) = Tiefe $(S_j) + 1$. Hieraus erhalten wir Tiefe $(S_k) = k - 1$.
Sei $C(S_j)$ die Anzahl der $\{\&, \vee\}$-Gatter. Es gilt dann $C(S_1) = 0$ und $C(S_{j+1}) = C(S_j) + 2 \cdot (2^j - 1)$. Hieraus erhalten wir

$$C(S_k) = 2^k + 2^{k-1} + \ldots + 2 - 2 \cdot k = 2 \cdot (N - \log(N + 1)).$$

Wir fassen das Ergebnis zusammen in dem

Satz 25. *Ist $\xi \in \mathbb{B}^N$, $N = 2^k - 1$ und ist $\mu(\xi) = |\xi|$, dann berechnet das Netz S_k die sortierte Folge $s(\xi)$. Es gilt Tiefe $(S_k) = k - 1$ und $C(S_k) = 2 \cdot (N - k)$.*

Wir skizzieren die Verallgemeinerung von $\mathbb{B}$ auf $\mathbb{B}^m$ für $m > 1$. Wir zählen nun analog zu dem Vorgehen im Fall $m = 1$ die Frequenz ν_η des Vorkommens von η in der Folge $\xi = (\eta_1, \eta_2, \ldots, \eta_n)$. Das kann man auf einfache

Weise mit einem Netz tun, dessen Größe linear mit n und exponentiell mit m wächst. Hält man m fest, dann hat man also eine in ihrer Komplexität linear wachsende Lösung. Nun konstruiert man auf Basis der Frequenzen ν_η nach Vorbild des Falles $m = 1$ ein Netz, das die sortierte Folge ausgibt. Natürlich ist das Verfahren nur für kleine m interessant.
Hardware-Realisierungen des Sortierens spielen bei der Organisation des Rechnens auf Rechnernetzen eine große Rolle. Einen hierarchischen Entwurf eines Sortierchips mittels des Entwurfssystem CADIC findet man in [BG98].
Die Kosten des Sortierens und der total symmetrischen Funktion relativ zu den Variablen $x_1, \dots, x_n$ behandeln wir im Zusammenhang mit der Addition von m k-stelligen Dualzahlen. Letztere verwenden wir auch im Zusammenhang mit der Multiplikation.

4.3 Addition von m k-stelligen Dualzahlen

Die Addition von m 1-stelligen Dualzahlen ist eine total symmetrische Funktion. Wir wenden uns aber zunächst dem allgemeinen Fall, der Addition von m k-stelligen Dualzahlen zu, erhalten $k = 1$ als Sonderfall und hieraus eine zweite Realisierung des allgemeinen Falles.

Der Einfachheit halber nehmen wir an, daß $m = 2^n$ ist. Wir addieren die m Zahlen, indem wir die Summe von je vier Zahlen, der Idee von *Wallace* [Wal64] folgend, auf die Summe von zwei Zahlen zurückführen. Das Schema wird durch das folgende Diagramm für $i = 1, \dots, k$ beschrieben.
In diesem Schema sind z^1, z^2, z^3, z^4 die zu addierenden Dualzahlen und sum^1, sum^2 die beiden sich nach diesem Schema ergebenden Zahlen. Für $i = k+1$ setzen wir $sum^2_{k+1} = r_k$.

Offensichtlich gilt

$$[z_1] + [z_2] + [z_3] + [z_4] = [sum^1] + 2[sum^2].$$

Indem wir in jedem Schritt die Summe von vier Zahlen auf die Summe von zwei Zahlen reduzieren, erhalten wir nach $n-1$ Schritten eine Reduktion der Addition von 2^n auf die Summe von zwei Zahlen. Allerdings wächst bei jedem Schritt die Breite der Summanden um 1, so daß wir nach $n-1$ Schritten zwei $k + (n-1)$ stellige Zahlen zu addieren haben.

Wir schätzen nun die Kosten $\tilde{C}_{m,k}$ der Reduktion und die Tiefe des Netzwerkes ab. Die Tiefe ergibt sich als $(n-1) \cdot 2 \cdot$ Tiefe $(FA) = 2 \cdot 4 \cdot (n-1)$, wenn wir FA in Tiefe 4 mit Kosten 10 realisieren.

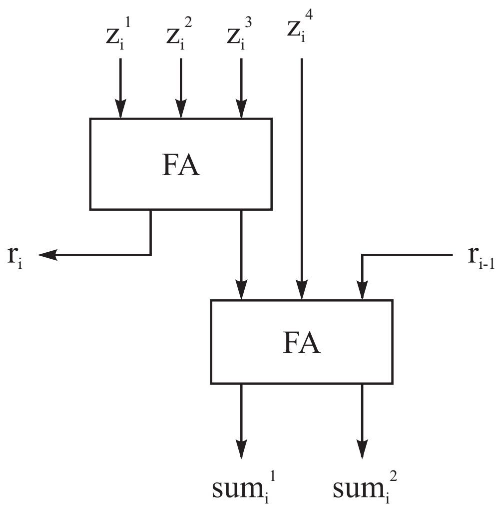


Abbildung 21:

Wir erhalten also für die Kosten $\tilde{C}_{m,k},\ m = 2^n$:

$$\begin{aligned}\tilde{C}_{m,k} &= 2 \cdot 10 \cdot 2^{n-2}k + 2 \cdot 10 \cdot 2^{n-3}(k+1) + \ldots + 2 \cdot 10 \cdot 2(k + (n-1)) \\ &\leq 20 \cdot (k + (n-1)) \cdot \sum_{i=1}^{n-2} 2^i \leq 10 \cdot 2^n \cdot (k + (n-1))\end{aligned}$$

d.h.

$$\tilde{C}_{m,k} < 10 \cdot m \cdot (k + \log m).$$

Aus diesen Resultaten und aus Satz 17 ergibt sich

$$C_{m,k} < 10 \cdot m \cdot (k + \lceil \log m \rceil) + 12 \cdot (k + \lceil \log m \rceil) - 15$$

und

$$\begin{aligned}T_{m,k} &< 8 \cdot (\lceil \log m \rceil - 1) + 4 \cdot \lceil \log(k + 2 \cdot \lceil \log m \rceil) \rceil + 2 \\ &< 12 \cdot \log m + 4 \log k - 4 \quad \text{für} \quad k > 2 \quad \text{und} \quad m > 4.\end{aligned}$$

Satz 26. *Die Addition von m k-stelligen Dualzahlen läßt sich durch ein Netz der Größe*

$$C_{m,k} < 12 \cdot m \cdot (k + \log m)$$

und der Tiefe

$$T_{m,k} < 12 \cdot \log m + 4 \log k$$

für $m \geq 7$ und $k \geq 6$ realisieren.

Korollar 16. *Die Funktion sum* $: \mathbb{B}^m \to \mathbb{B}$, $m = 2^l$, $l \in \mathbb{N}$ *läßt sich durch ein Netz mit Kosten*

$$C_{m,1} \leq 12 \cdot m \log m$$

und der Tiefe

$$T_{m,1} < 9 \cdot \log m$$

für $m > 128$ *realisieren.*

Aufgrund von Satz 25 erhalten wir weiter das

Korollar 17. *Das Sortieren binärer Folgen läßt sich für* $m = 2^l$ *durch ein Netz der Größe*

$$C_m \leq 14 \cdot m \cdot \log m$$

und der Tiefe

$$T_m \leq 10 \cdot \log m$$

realisieren.

Im Falle $m = 1024$ erhalten wir also $C_m \approx 100000$ und $T_m < 100$. Man muß also die logarithmische Tiefe mit einem sehr hohen Aufwand an $\{\&, \vee\}$-Gattern bezahlen.

4.3.1 Eine effiziente Version

Wir betrachten die rekursive Berechnung von $sum(\xi)$ nicht als Sonderfall des Wallace-Tree Verfahrens, sondern wenden unsere Idee zunächst $sum(\xi)$ zu berechnen konsequent auch auf die Berechnung von $sum(\xi)$ selbst rekursiv an.

Seien

$$\zeta^i = (\xi_{i1}, \dots, \xi_{ik}),\ \ i = 1, \dots, m$$

die zu addierenden Dualzahlen und

$$\xi^j = (\xi_{1j}, \dots, \xi_{mj})$$

die j-te Spalte der Matrix (ξ_{ij}) dieser Zahlen. $Sum(\xi^j)$ sei die als Dualzahl geschriebene Summe der Zahlen ξ^j. Um die folgenden Ausdrücke formal nicht zu überlasten, fassen wir binäre Folgen mal als die durch sie dargestellte

Zahl, mal nur als Folge auf, ohne das wie früher durch die Klammer [ ] zu markieren. Wir haben dann

$$ad(\zeta_1, \ldots, \zeta_m) = \sum_{i=1}^{k} sum(\xi^i) \cdot 2^{k-i}.$$

Nun setzen wir $i = l + j \cdot \lambda$ mit $\lambda = \lceil \log m \rceil$ und $0 \leq l < \lambda$. Damit werden l und j durch i eindeutig bestimmt. Wir erhalten, wenn wir $k_l := \frac{k-l}{\lambda}$ setzen,

$$\begin{aligned} ad(\zeta_1, \ldots, \zeta_m) &= \sum_{0 \leq l < \lambda} \sum_{0 \leq j \leq k_l} sum(\xi^{l+j\cdot\lambda}) \cdot 2^{k-(l+j\cdot\lambda)} \\ &= \sum_{0 \leq l < \lambda} \left(\sum_{0 \leq j \leq k_l} sum(\xi^{l+j\cdot\lambda}) \cdot 2^{(k-l)-(l+j\cdot\lambda)} \right) \cdot 2^l. \end{aligned}$$

Damit haben wir die Berechnung der Summe von m Zahlen auf die Berechnung der Summe von λ Zahlen reduziert, da sich die innere Summe gerade zu einer binären Folge

$$sum(\xi^l), sum(\xi^{l+\lambda}), sum(\xi^{l+2\lambda}), \ldots, sum(\xi^{l+j_e\cdot\lambda})$$

zusammensetzt, die diese Summe als Dualzahl definiert.

Iteriert man das Verfahren, bis man auf zwei Zahlen herabkommt, dann kann man die endgültige Summe mit dem in Korollar 11 vorkommenden Addierer berechnen.

Diese Reduktion von m auf zwei Summanden ist nach spätestens s Schritten beendet, wenn

$$\left.2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\right\}{\scriptstyle s\ mal} > m$$

gilt. Bezeichnen wir, wie üblich, die Umkehrfunktion dieser Funktion durch $\log^*(m)$, dann erfordert diese Reduktion höchstens $s = \lceil \log^*(m) \rceil$ Schritte.
Wir untersuchen nun den einzelnen Reduktionsschritt. Jeder dieser Schritte gliedert sich selbst wieder in Reduktionen, die das folgende Schema beschreibt.
Die Folge ν_0^1 enthält die in der ersten Stufe erzeugten Überträge, die Folge ν_1^1 die Summen $mod 2$. Nun iterieren wir das Verfahren, indem wir es auf ν_0^1 und ν_1^1 getrennt anwenden.

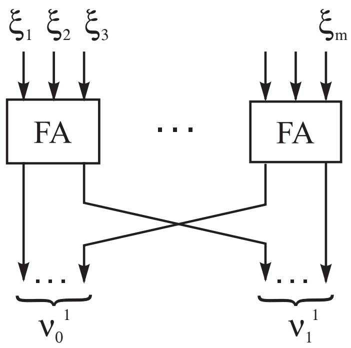


Abbildung 22:

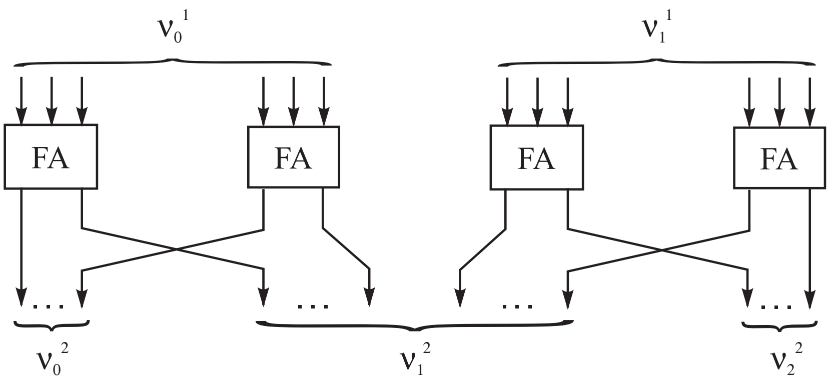


Abbildung 23:

Wir erhalten für die Längen, wenn wir einmal Rundungen auf benachbarte ganze Zahlen vernachlässigen

$$\begin{aligned} \left|\nu_0^1\right| &= \left|\nu_1^1\right| = \frac{m}{3} \\ \left|\nu_0^2\right| &= \left|\nu_2^2\right| = \frac{m}{3^2}, \qquad \left|\nu_1^2\right| = \frac{2}{3^2} \cdot m. \end{aligned}$$

Setzt man das Schema weiter fort, so erhält man nach l Schritten die Folgen

$$\nu_0^l, \nu_1^l, \dots, \nu_l^l.$$

Man beobachtet

$$\left|\nu_0^{l+1}\right| = \frac{1}{3}\left|\nu_0^l\right|, \quad \left|\nu_{l+1}^{l+1}\right| = \frac{1}{3}\left|\nu_l^l\right|$$

und

$$\left|\nu_i^{l+1}\right| = \frac{1}{3}(\left|\nu_{l-1}^l\right| + \left|\nu_l^l\right| \quad \text{für } i = 1, \dots, l.$$

Wir erkennen darin das Schema einer Binomialkoeffizientenberechnung und erhalten

$$\left|\nu_i^l\right| = \frac{1}{3^l} \cdot \binom{l}{i} \cdot m \quad \text{für } i = 0, \ldots, l.$$

Das Verfahren bricht ab, wenn zum erstenmal

$$m \cdot \frac{1}{3^t} \cdot \binom{t}{i} \leq 1 \quad \text{für } i = 0, \ldots, t$$

gilt. Wir verwenden die Abschätzung

$$\binom{t}{i} \leq \left(\frac{e \cdot t}{i}\right)^i,$$

die sich aus der Stirling-Formel herleitet; e ist hierin die Basis des natürlichen Logarithmus. Wir überschätzen t, wenn wir diese Ungleichung anwenden und erhalten

$$3^t \geq m \cdot \left(\frac{e \cdot t}{i}\right)^i$$

oder

$$t \cdot \log 3 \geq \log m + i(\log e + \log t - \log i).$$

Die rechte Seite nimmt ihr Maximum an für

$$\log i = \log t - 1.$$

Wir vergröbern unsere Ungleichungen durch eine Ungleichung, nämlich

$$t \cdot \log 3 \geq \log m + \frac{1}{2} \cdot \log t \cdot (1 + \log e)\,.$$

Hieraus folgt

$$t \geq \frac{1}{\log 3} \cdot \log m + \frac{1 + \log e}{2 \cdot \log 3} \cdot \log t$$

Setzen wir $m = 2^n$ und machen wir den Ansatz $t = n$, dann erhalten wir

$$t \geq \frac{1}{\log 3} \cdot t + \frac{1 + \log e}{2 \cdot \log 3} \cdot \log t$$

und weiter

$$\frac{t}{\log t} \geq 2,1$$

als hinreichende Bedingung für t. Diese Ungleichung ist für $t = n \geq 5$ stets erfüllt. Da jede Stufe aus 2^n Summanden für $n \geq 5$ in Tiefe n berechnet werden kann, erhalten wir durch Summation der Tiefe der $\log^*(m)$ Stufen des Gesamtschaltkreises die folgende Abschätzung. Die Reduktion auf fünf Summanden kann in Tiefe

$$t_1 = \sum_{i=1}^{i_0} \log^i(m) \quad \text{mit } \log^{i_0}(m) = 5$$

erfolgen. Die Reduktion der restlichen fünf Summanden auf die Summe zweier Zahlen kann in drei FA-Stufen erfolgen. Da $Tief(FA) = 4$ ist, ergibt sich als Gattertiefe des Gesamtschaltkreises $t = 4 \cdot (t_1 + 3)$. Wegen

$$\frac{1}{\log m} \cdot \sum_{i=1}^{i_0} \log^i(m) \to 1$$

erhalten wir

Lemma 16. Die Reduktion der Summe von m k-stelligen Dualzahlen auf die Summe zweier Dualzahlen läßt sich in Tiefe $t = 4 \cdot \log m + 12$ asymptotisch in Größe $k \cdot m$ durchführen. Hierbei sind diese Maße in Vielfachen von Full-Adder-Größen zu nehmen.

Beweis. Wir schätzen nun die Gesamtkosten des Verfahrens ab. Das tun wir, indem wir zunächst die Kosten für die Berechnung der Dualdarstellung der Summe von m i-stelligen Zahlen abschätzen.

Wir haben in den Stufen dieser Berechnung die folgenden Kosten in Vielfachen von FA's ausgedrückt.

Stufe	1	2	3	$\cdots$
Kosten	$\frac{1}{3}m$	$\frac{2}{9}m$	$(\frac{2}{g})^2 m$	$\cdots$

Also erhalten wir als Kosten $C_{1,m}$ über alle diese Stufen

$$C_{1,m} < \frac{m}{3} \sum_{i=0}^{\infty} \left(\frac{2}{3}\right)^i = m.$$

Für die Gesamtkosten C_k der Reduktion von m k-stelligen Summanden auf $\lceil \log m \rceil$ Summanden gilt also

$$C_{k,m} < k \cdot m.$$

Die Gesamtkosten C^m über alle Großstufen lassen sich also abschätzen durch

$$C_k^m < C_{k,m} + C_{k_1,m_1} + C_{k_2,m_2} + \cdots$$

mit $m_1 = \lceil \log m \rceil$ und $m_{i+1} = \lceil \log m_i \rceil$
und mit

$$k_0 = k, \quad k_i = k_{i-1} + \lceil \log m_{i-1} \rceil$$

für $i = 1, 2, \ldots$
Hieraus erhalten wir

$$\begin{aligned} C_k^m &< k \cdot m + k_1 \cdot m_1 + \cdots && (56) \\ &= k \cdot m \cdot \left(1 + \frac{k_1}{k} \cdot \frac{m_1}{m} + \frac{k_2}{k} \cdot \frac{m_2}{k} + \cdots \right). && (57) \end{aligned}$$

Für $k < 32$ erhalten wir daraus

$$C_k^m < k \cdot m \left(1 + 2\frac{m_1}{m}\right).$$

Mit groß werdendem m erhalten wir asymptotisch die Kosten $k \cdot m$. □

Die folgende Tabelle zeigt, wie C_k^m relativ zu festem k wächst.

m	32	64	128	···
$\frac{1}{k}C_k^m <$	32,5	32,25	32,11	···

Wir fassen unsere Resultate in Satz 27 zusammen. Dabei setzen wir als Kosten für den Full Adder 10 boolesche Gatter an und als Tiefe 4. Weiter verwenden wir zur Addition der restlichen beiden Dualzahlen das Addierwerk aus Korollar 10 für die Stellenzahl $N = k + \log m$. Damit ergibt sich durch elementare Umformungen der

Satz 27. *Die Summe von m k-stelligen Dualzahlen läßt sich durch ein boolesches Netz der Tiefe $16 \cdot \log m + 4 \log k + o(\log m + \log k)$ in Größe $10 \cdot k \cdot m + o(k \cdot m)$ realisieren.*

Indem wir dieses Resultat auf das Sortieren von einstelligen Dualzahlen in Verbindung mit Satz 25 anwenden, erhalten wir

Satz 28. *Binäre Folgen der Länge m lassen sich durch boolesche Netze der Tiefe $17 \cdot m + o[m]$ und der Größe $12 \cdot m + o(m)$ sortieren.*