Zusammenfalten des Postschen Verbandes mittels Operationen aus binären Booleschen Funktionen

Christian Reitwießner

Report No. 386 Juni 2006

Preprint-Reihe
Fakultät für Mathematik und Informatik
Universität Würzburg

Zusammenfalten des Postschen Verbandes mittels Operationen aus binären Booleschen Funktionen

Christian Reitwießner

Theoretische Informatik
Bayerische Julius-Maximilians-Universität Würzburg
Am Hubland, D-97074 Würzburg
christian@reitwiessner.de

Zusammenfassung

Die Mengen Boolescher Funktionen, die bezüglich der Superposition abgeschlossen sind, wurden schon 1941 von Post analysiert. In der vorliegenden Arbeit betrachten wir die Mengen Boolescher Funktionen, die bezüglich der Superposition und einer Operation Q_g abgeschlossen sind. Dabei ist Q_g für eine zweistellige Boolesche Funktion g wie folgt definiert: $Q_g(f)(x_1, \ldots, x_{n-1}) \stackrel{\text{def}}{=} g(f(x_1, \ldots, x_{n-1}, 0), f(x_1, \ldots, x_{n-1}, 1))$ für eine n-stellige Boolesche Funktion f. Insgesamt ergeben sich also 16 verschiedene Operationen. Diese werden wir in fünf Gruppen von sich gleichartig verhaltenden Operationen unterteilen, wobei sich diese durch Dualitätsbetrachtungen noch auf drei Gruppen reduzieren lassen.

1 Einleitung

Boolesche Funktionen haben in der Informatik eine große Bedeutung, denn sie sind die Funktionen auf der einfachsten Menge der Informatik, der Menge aus der Null und der Eins. Mit ihnen kann man das Verhalten von digitalen Schaltkreisen beschreiben. Komplexe digitale Schaltkreise werden oft durch Kombination von einheitlichen, einfacheren Schaltkreisen erzeugt. In der Welt der Booleschen Funktionen wird dieser Vorgang durch die *Superposition* von Funktionen modelliert, im Wesentlichen das Einsetzen von Funktionen in andere. Schon 1941 analysierte Post [Pos41], welche Mengen von Booleschen Funktionen unter Superposition *abgeschlossen* sind, das heißt welche Mengen unter Anwendung der Superposition keine neuen Funktionen hervorbringen können.

Die Booleschen Funktionen sind jedoch nicht nur für Schaltkreise relevant, sie modellieren zum Beispiel auch aussagenlogische Formeln. Mit ihnen kann man atomare Wahrheitsaussagen logisch verknüpfen. (Zum Beispiel „Die Sonne scheint *und* es ist warm“ oder „Die Sonne scheint, und *daraus folgt*, dass es warm ist“.) Um mehr Ausdrucksstärke zu gewinnen, werden oft *Quantoren* (der Existenz- und den Allquantor) hinzugenommen. Mit dem Existenzquantor kann man dann zum Beispiel folgendes ausdrücken: „*Es gibt* eine Stellung des Lichtschalters, *so dass* das Licht leuchtet.“ Abstrakter formuliert: Für die Variable x existiert eine Belegung, so dass die Formel wahr wird. Quantoren kann man natürlich auch mischen: Für alle Belegungen von x existiert eine Belegung von y, so dass x den gleichen Wert wie y hat.

Da diese beiden Quantoren nur eine spezielle Art von allgemeineren Operationen auf Booleschen Funktionen sind, die alle eine ähnliche Struktur aufweisen, wird der Begriff der Quantoren-Operation noch verallgemeinert. Manche Mengen, die unter Superposition abgeschlossen sind, sind dies nicht mehr, wenn man die Superposition mit solch einer Operation erweitert. Schließlich ergeben sich fünf Gruppen von erweiterten Quantoren, die auf die abgeschlossenen Mengen jeweils unterschiedlich wirken.

Über die allgemeine Theorie der abgeschlossenen Mengen (sogenannte *clones*) kann man in einem Lehrbuch von Cohn [Coh65] genaueres nachlesen. Jablonski, Gawrilow und Kudrjawzew [JGK70] geben eine Beschreibung des Postschen Graphen zusammen mit den Resultaten von Post. Im Gegensatz zur rein algebraischen Analyse des Postschen Graphen im vorliegenden Text behandeln Böhler, Creignou, Reith und Vollmer [BCRV03] Fragen der Komplexitätstheorie, die sich mit Hilfe der Resultate von Post leichter lösen lassen.

2 Definitionen

Eine *n-stellige Boolesche Funktion* ist eine totale Funktion $f : \{0,1\}^n \to \{0,1\}$ mit $n \geq 1$. Die Menge aller Booleschen Funktionen sei bezeichnet mit BF. Eine Variable x_i einer Booleschen Funktion f heißt *fiktiv*, wenn sie keinerlei Auswirkung auf den Funktionswert hat, falls also für alle $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in \{0,1\}$ gilt:

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = f(a_1, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n)$$

Die Superposition wird durch die folgenden algebraischen Operationen modelliert. Dabei seien f, g und h Boolesche Funktionen der Stelligkeiten $n \geq 1$, $m \geq 2$ und $k \geq 1$.

- $\mathrm{VI}()(x_1) \stackrel{\text{def}}{=} x_1$, das Vorhandensein der Identität.
- $\mathrm{ZV}(g)(x_1, \ldots, x_{m-1}, x_m) \stackrel{\text{def}}{=} g(x_2, \ldots, x_{m-1}, x_m, x_1)$, die zyklische Vertauschung von Variablen.
- $\mathrm{LV}(g)(x_1, \ldots, x_{m-2}, x_{m-1}, x_m) \stackrel{\text{def}}{=} g(x_1, \ldots, x_{m-2}, x_m, x_{m-1})$, die Vertauschung der letzten beiden Variablen.
- $\mathrm{FV}(f)(x_1, \ldots, x_n, x_{n+1}) \stackrel{\text{def}}{=} f(x_1, \ldots, x_n)$, die Einführung einer fiktiven Variablen.
- $\mathrm{ID}(g)(x_1, \ldots, x_{m-2}, x_{m-1}) \stackrel{\text{def}}{=} g(x_1, \ldots, x_{m-2}, x_{m-1}, x_{m-1})$, die Identifizierung der letzten beiden Variablen.
- $\mathrm{SUB}(g,h)(x_1, \ldots, x_{m-1}, y_1, \ldots, y_k) \stackrel{\text{def}}{=} g(x_1, \ldots, x_{m-1}, h(y_1, \ldots, y_k))$, die Substitution an der letzten Stelle.

Wir verwenden als Abkürzung $\mathrm{SUP} \stackrel{\text{def}}{=} \{\mathrm{VI}, \mathrm{ZV}, \mathrm{LV}, \mathrm{FV}, \mathrm{ID}, \mathrm{SUB}\}$.

Im Folgenden bezeichnen wir mit *Operation* immer nur eine Operation auf Booleschen Funktionen. Definieren wir nun die Quantoren-Operationen, die die Superposition erweitern sollen; dabei sei f eine n-stellige Boolesche Funktion mit $n \geq 2$.

$$\mathrm{EX}(f)(x_1, \ldots, x_n) \stackrel{\text{def}}{=} f(x_1, \ldots, x_{n-1}, 0) \vee f(x_1, \ldots, x_{n-1}, 1)$$

$$\mathrm{FA}(f)(x_1, \ldots, x_n) \stackrel{\text{def}}{=} f(x_1, \ldots, x_{n-1}, 0) \wedge f(x_1, \ldots, x_{n-1}, 1)$$

Außerdem sei für jede zweistellige Boolesche Funktion g die erweiterte Quantoren-Operation Q_g definiert (im Folgenden einfach ebenfalls *Quantoren-Operation genannt*):

$$Q_g(f)(x_1, \ldots, x_{n-1}) \stackrel{\text{def}}{=} g(f(x_1, \ldots, x_{n-1}, 0), f(x_1, \ldots, x_{n-1}, 1))$$

Es gilt also $\mathrm{EX} = Q_{\mathrm{vel}}$ und $\mathrm{EX} = Q_{\mathrm{et}}$. Wir definieren noch die Abkürzung $\mathrm{SUP}_{Q_g} \stackrel{\mathrm{def}}{=} \mathrm{SUP} \cup \{Q_g\}$.

Eine Menge $A \subseteq \mathrm{BF}$ heißt *abgeschlossen* unter einer Operation $O : \mathrm{BF}^n \to \mathrm{BF}$ für $n \geq 0$, falls mit allen $f_1, \ldots, f_n \in A$ auch $O(f_1, \ldots, f_n) \in A$ ist. Sie heißt abgeschlossen unter einer Menge von Operationen, falls sie unter jeder einzelnen Operation der Menge abgeschlossen ist. Weiterhin ist für eine Menge von Operationen O der Abschluss einer Menge $A \subseteq \mathrm{BF}$ definiert als $[A]_O \stackrel{\mathrm{def}}{=} \bigcap\{M \subseteq \mathrm{BF} \mid A \subseteq M \text{ und } M \text{ ist abgeschlossen unter } O\}$. $A \subseteq \mathrm{BF}$ ist also genau dann unter O abgeschlossen, wenn $[A]_O = A$ gilt.

Lemma 1. *Sei O eine Menge von Operationen und A und B Mengen Boolescher Funktionen, die unter O abgeschlossen sind. Dann gilt: $A \cap B = [A \cap B]_O$.*

Beweis. Sei M_0 definiert als $M_0 \stackrel{\mathrm{def}}{=} \{M \subseteq \mathrm{BF} \mid A \cap B \subseteq M \text{ und } M \text{ ist abgeschlossen unter } O\}$. Dann sind $A, B \in M_0$ und für alle $M \in M_0$ gilt $A \cap B \in M$. Weil der Abschluss definiert ist als $[A \cap B]_O = \bigcap M_0$ gilt schließlich $A \cap B = [A \cap B]_O$. □

Nun wollen wir einige Boolesche Funktionen und die abgeschlossenen Mengen Boolescher Funktionen definieren. Eine komplette Liste der abgeschlossenen Mengen ist in Tabelle 1 gegeben. Diese Mengen bilden mit der Inklusion einen Verband; das zugehörige Hasse-Diagramm ist in Abbildung 1 angegeben. Bei der Bezeichnungen der Mengen folgen wir der von Wagner [RW00] verwendeten Notation, die sich von der ursprünglichen, von Post [Pos41] verwendeten unterscheidet.

Die beiden (einstelligen) *Konstanten* sind $c_0(x) \stackrel{\mathrm{def}}{=} 0$ und $c_1(x) \stackrel{\mathrm{def}}{=} 1$, wobei wir sie in Formeln oft einfach durch „0“ oder „1“ ersetzen werden. Die n-stelligen Konstanten bezeichnen wir mit c_0^n und c_1^n. Die beiden nicht-konstanten einstelligen Funktionen sind die *Identität* $id(x) \stackrel{\mathrm{def}}{=} x$ und die *Negation*: $\mathrm{non}(x) \stackrel{\mathrm{def}}{=} 1$ gdw. $x = 0$. In Formeln werden wir $\neg x$ oder $\overline{x}$ für $\mathrm{non}(x)$ verwenden. Für $n \geq 1$ und $1 \leq i \leq n$ sei die *n-stellige Identität der i-ten Stelle* definiert als $\mathrm{id}_i^n(x_1, \ldots, x_n) \stackrel{\mathrm{def}}{=} x_i$. Oft gebrauchte zweistellige Funktionen sind:

- $\mathrm{et}(x, y) \stackrel{\mathrm{def}}{=} 1$ genau dann, wenn $x = y = 1$. (In Formeln: $x \wedge y$, beziehungsweise einfach xy)
- $\mathrm{vel}(x, y) \stackrel{\mathrm{def}}{=} 0$ genau dann, wenn $x = y = 0$. (In Formeln: $x \vee y$)
- $\mathrm{aut}(x, y) \stackrel{\mathrm{def}}{=} 1$ genau dann, wenn $x \neq y$. (In Formeln: $x \oplus y$)

Nun zu den abgeschlossenen Mengen Boolescher Funktionen. Im Folgenden sei f eine n-stellige Boolesche Funktion. f heißt *a-reproduzierend* für $a \in$

$\{0,1\}$, wenn $f(a,\ldots,a) = a$ gilt. R_a ist die Menge aller a-reproduzierenden Booleschen Funktionen. f heißt *monoton*, falls für alle $a_1,\ldots,a_n,b_1,\ldots,b_n \in \{0,1\}$ mit $a_i \leq b_i$ für $1 \leq i \leq n$ gilt: $f(a_1,\ldots,a_n) \leq f(b_1,\ldots,b_n)$. Die Menge der monotonen Booleschen Funktionen sei bezeichnet mit M. f wird *selbstdual* genannt, wenn für alle $a_1,\ldots,a_n \in \{0,1\}$ gilt: $f(a_1,\ldots,a_n) = \neg f(\overline{a_1},\ldots,\overline{a_n})$. Die Menge aller selbstdualen Funktionen sei bezeichnet mit D. f heißt *linear*, wenn es Konstanten $k_0,\ldots,k_n \in \{0,1\}$ gibt, so dass f beschrieben werden kann durch $f(x_1,\ldots,x_n) = k_0 \oplus k_1x_1 \oplus \cdots \oplus k_nx_n$. L ist die Menge aller linearen Booleschen Funktionen. Für $T \subseteq \{0,1\}^n$ und $a \in \{0,1\}$ heißt T *a-separierbar*, wenn es ein i mit $1 \leq i \leq n$ gibt, so dass für alle $(b_1,\ldots,b_n) \in T$ gilt: $b_i = a$. f heißt *a-separierend*, wenn $f^{-1}(\{a\})$ a-separierbar ist. f heißt *a-separierend vom Grad k*, wenn jede k-elementige Teilmenge von $f^{-1}(\{a\})$ a-separierbar ist. Die Menge aller a-separierenden Booleschen Funktionen sei bezeichnet mit S_a, und die Menge der a-separierenden Booleschen Funktionen vom Grad k mit S_a^k. E ist die Menge der et-Funktionen, das heißt die Menge aller Funktionen, die durch Formeln über $0,1$ und $\wedge$ darstellbar sind. Also $\mathrm{E} \stackrel{\text{def}}{=} \{f \mid \exists\, n \in \mathbb{N}$ und $\exists\, k_0,\ldots,x_n \in \{0,1\}$ mit $f(x_1,\ldots,x_n) = k_0 \wedge (k_1 \vee x_1) \wedge \cdots \wedge (k_n \vee x_n)\}$. Analog ist die Menge der vel-Funktionen, V, definiert als Menge der Booleschen Funktionen, die durch Formeln über $0,1$ und $\vee$ darstellbar sind. Die Menge I enthält alle Identitäten und Konstanten: $\mathrm{I} \stackrel{\text{def}}{=} \{\mathrm{id}_i^n \mid n \geq 1, 1 \leq i \leq n\} \cup \{c_a^n \mid n \geq 1, a \in \{0,1\}\}$. Und schließlich enthält die Menge N zusätzlich zu den Funktionen aus I noch alle Negationen der Identitäten: $\mathrm{N} \stackrel{\text{def}}{=} \mathrm{I} \cup \{\neg f \mid f \in \mathrm{I}\}$

Die restlichen abgeschlossenen Mengen aus Tabelle 1 ergeben sich mittels Durchschnitt der obigen Mengen (siehe Lemma 1).

Ein wichtiges Hilfsmittel zur Analyse von Mengen Boolescher Funktionen ist der Begriff der *Dualität*. Zu einer n-stelligen Booleschen Funktion f ist die ebenfalls n-stellige duale Funktion wie folgt definiert:

$$\mathrm{dual}(f)(x_1,\ldots,x_n) \stackrel{\text{def}}{=} \neg f(\overline{x_1},\ldots,\overline{x_n})$$

(Eine Funktion f ist selbstdual, wenn $\mathrm{dual}(f) = f$ gilt.) Für eine Menge $A \subseteq \mathrm{BF}$ ist $\mathrm{dual}(A) \stackrel{\text{def}}{=} \{\mathrm{dual}(f) \mid f \in A\}$. Im Verband der abgeschlossenen Mengen (Abbildung 1) erhält man die duale Menge mittels Spiegelung an der Symmetrieachse durch BF und I_2. Für Quantoren-Operationen wird der Begriff der Dualität etwas anders definiert. Seien g eine zweistellige Boolesche Funktion, dann ist die *duale Operation* der Operation Q_g definiert durch $\mathrm{dualOp}(Q_g) \stackrel{\text{def}}{=} Q_{\mathrm{dual}(\mathrm{ZV}(g))}$. Die Vertauschung der Variablen wird durch das folgende Lemma gerechtfertigt.

Menge	**Definition**
BF	alle Booleschen Funktionen
R_0	$\{f \in \mathrm{BF} \mid f$ ist 0-reproduzierend$\}$
R_1	$\{f \in \mathrm{BF} \mid f$ ist 1-reproduzierend$\}$
R_2	$\mathrm{R}_1 \cap \mathrm{R}_0$
M	$\{f \in \mathrm{BF} \mid f$ ist monoton$\}$
M_i	$\mathrm{M} \cap \mathrm{R}_i$ für $i = 0, 1, 2$
S_1^n	$\{f \in \mathrm{BF} \mid f$ ist 1-separierend vom Grad $n\}$
S_1	$\{f \in \mathrm{BF} \mid f$ ist 1-separierend$\}$
S_{12}^n	$\mathrm{S}_1^n \cap \mathrm{R}_2$
S_{12}	$\mathrm{S}_1 \cap \mathrm{R}_2$
S_{11}^n	$\mathrm{S}_1^n \cap \mathrm{M}$
S_{11}	$\mathrm{S}_1 \cap \mathrm{M}$
S_{10}^n	$\mathrm{S}_1^n \cap \mathrm{R}_2 \cap \mathrm{M}$
S_{10}	$\mathrm{S}_1 \cap \mathrm{R}_2 \cap \mathrm{M}$
S_0^n	$\{f \in \mathrm{BF} \mid f$ ist 0-separierend vom Grad $n\}$
S_0	$\{f \in \mathrm{BF} \mid f$ ist 0-separierend$\}$
S_{02}^n	$\mathrm{S}_0^n \cap \mathrm{R}_2$
S_{02}	$\mathrm{S}_0 \cap \mathrm{R}_2$
S_{01}^n	$\mathrm{S}_0^n \cap \mathrm{M}$
S_{01}	$\mathrm{S}_0 \cap \mathrm{M}$
S_{00}^n	$\mathrm{S}_0^n \cap \mathrm{R}_2 \cap \mathrm{M}$
S_{00}	$\mathrm{S}_0 \cap \mathrm{R}_2 \cap \mathrm{M}$
D	$\{f \in \mathrm{BF} \mid f$ ist selbstdual$\}$
D_1	$\mathrm{D} \cap \mathrm{R}_2$
D_2	$\mathrm{D} \cap \mathrm{M}$
L	$\{f \in \mathrm{BF} \mid f$ ist linear$\}$
L_i	$\mathrm{L} \cap \mathrm{R}_i$ für $i = 0, 1, 2$
L_3	$\mathrm{L} \cap \mathrm{D}$
V	$\{f \in \mathrm{BF} \mid f$ ist eine vel-Funktion$\}$
V_i	$\mathrm{V} \cap \mathrm{R}_i$ für $i = 0, 1, 2$
E	$\{f \in \mathrm{BF} \mid f$ ist eine et-Funktion$\}$
E_i	$\mathrm{E} \cap \mathrm{R}_i$ für $i = 0, 1, 2$
N	$[\{\mathrm{non}\}] \cup [\{c_0\}] \cup [\{c_1\}]$
N_2	$[\{\mathrm{non}\}]$
I	$[\{\mathrm{id}\}] \cup [\{c_0\}] \cup [\{c_1\}]$
I_0	$[\{\mathrm{id}\}] \cup [\{c_0\}]$
I_1	$[\{\mathrm{id}\}] \cup [\{c_1\}]$
I_2	$[\{\mathrm{id}\}]$

Tabelle 1: Die abgeschlossenen Mengen Boolescher Funktionen [BCRV03]

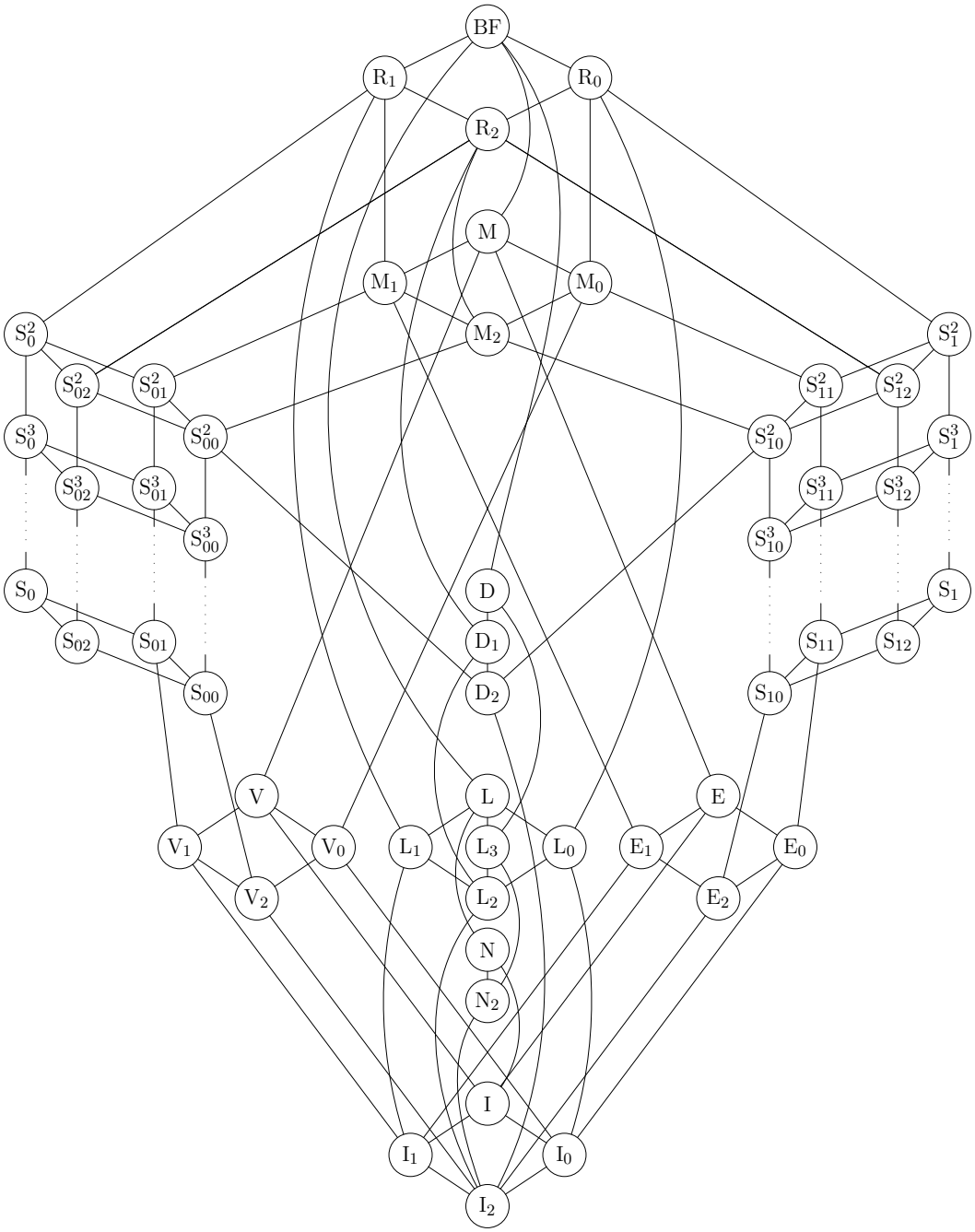


Abbildung 1: Verband der abgeschlossenen Mengen Boolescher Funktionen [BCRV03]

Lemma 2. *Die Funktion* dual *ist ein Isomorphismus zwischen den algebraischen Strukturen* (BF, Q_g) *und* $(\mathrm{BF}, \mathrm{dualOp}(Q_g))$.

Beweis. dual ist bijektiv, da dual $\circ$ dual die Identität ist. Außerdem ist sie ein Homomorphismus, denn es gilt:

$$\begin{aligned}
&\mathrm{dual}(Q_g(f))(x_1,\ldots,x_{n-1}) = \neg g(f(\overline{x_1},\ldots,\overline{x_{n-1}},0), f(\overline{x_1},\ldots,\overline{x_{n-1}},1))\\
&\quad= \mathrm{dual}(g)(\neg f(\overline{x_1},\ldots,\overline{x_{n-1}},0), \neg f(\overline{x_1},\ldots,\overline{x_{n-1}},1))\\
&\quad= \mathrm{dual}(g)(\mathrm{dual}(f)(x_1,\ldots,x_{n-1},1), \mathrm{dual}(f)(x_1,\ldots,x_{n-1},0))\\
&\quad= Q_{\mathrm{dual}(\mathrm{ZV}(g))}(\mathrm{dual}(f))(x_1,\ldots,x_{n-1})\\
&\quad= \mathrm{dualOp}(Q_g)(\mathrm{dual}(f))(x_1,\ldots,x_{n-1})
\end{aligned}$$

Also ist $\mathrm{dual}(Q_g(f)) = \mathrm{dualOp}(Q_g)(\mathrm{dual}(f))$. □

Wie man leicht sieht, sind die Superpositions-Operationen aus SUP alle „selbstdual“, das heißt, für jede Operation $O \in \mathrm{SUP}$ ist (BF, O) mittels dual isomorph zu sich selbst. Das folgende Lemma zeigt schließlich noch eine Anwendungsmöglichkeit dieser Isomorphie.

Lemma 3. *Sei M eine Menge Boolescher Funktionen und O eine Menge von Operationen. M ist genau dann unter O abgeschlossen, wenn* $\mathrm{dual}(M)$ *unter* $\mathrm{dualOp}(O)$ *abgeschlossen ist, wobei hier* $\mathrm{dualOp}(S) = S$ *für* $S \in \mathrm{SUP}$ *gilt.*

Beweis. Da dual und dualOp selbstinvers sind, müssen wir nur eine Richtung zeigen. Sei M abgeschlossen unter O, das heißt für eine beliebige n-stellige Operation $O_1 \in O$ und beliebige Funktionen $f_1,\ldots,f_n \in M$ ist auch $O_1(f_1,\ldots,f_n) \in M$. Seien nun $g_1,\ldots,g_n \in \mathrm{dual}(M)$ und $f_i = \mathrm{dual}(g_i)$ für $i = 1,\ldots,n$. Dann gilt mit Lemma 2:

$$\begin{aligned}
\mathrm{dualOp}(O)(g_1,\ldots,g_n) &= \mathrm{dualOp}(O)(\mathrm{dual}(f_1),\ldots,\mathrm{dual}(f_n))\\
&= \mathrm{dual}(O(f_1,\ldots,f_n)) \in \mathrm{dual}(M)
\end{aligned}$$

□

3 Die Gruppen der Quantoren-Operationen

Nun wollen wir uns den Quantoren-Operationen selbst zuwenden. Wir werden feststellen, dass es bezüglich ihrer Auswirkungen auf den Postschen Graphen nur fünf verschiedene Arten von Quantoren-Operationen gibt, von denen sich zwei auch noch dual zu zwei anderen Arten verhalten. Insofern gibt es also nur drei Arten, wie eine Quantoren-Operation auf den Postschen Graphen wirken kann.

Zuerst wollen wir feststellen, was die kleinste Menge ist, die unter der Superposition und gleichzeitig unter einer Quantoren-Operation Q_g abgeschlossen ist, also der Abschluss der leeren Menge unter SUP_{Q_g}. Wir nennen diese Menge μ_{Q_g}:

$$\mu_{Q_g} \stackrel{\text{def}}{=} [\emptyset]_{\mathrm{SUP}_{Q_g}}$$

Dazu zunächst ein Hilfssatz, der uns die Beweise erleichtern soll.

Lemma 4. *Sei f eine n-stellige ($n \geq 2$) Boolesche Funktion, deren letzte Variable x_n fiktiv ist, dann ist $Q_g(f) \in [\{f, Q_g(\mathrm{id}_1^2)\}]_{\mathrm{SUP}}$.*

Beweis. Wegen $Q_g(\mathrm{id}_1^2)(x) = g(\mathrm{id}_1^2(x,0), \mathrm{id}_1^2(x,1)) = g(x,x)$ gilt:

$$\begin{aligned} Q_g(f)(x_1,\ldots,x_{n-1}) &= g(f(x_1,\ldots,x_{n-1},0), f(x_1,\ldots,x_{n-1},1)) \\ &= g(f(x_1,\ldots,x_{n-1},x_{n-1}), f(x_1,\ldots,x_{n-1},x_{n-1})) \\ &= Q_g(\mathrm{id}_1^2)(f(x_1,\ldots,x_{n-1},x_{n-1})) \\ &= Q_g(\mathrm{id}_1^2)(\mathrm{ID}(f)(x_1,\ldots,x_{n-1})) \\ &= \mathrm{SUB}(Q_g(\mathrm{id}_1^2), \mathrm{ID}(f))(x_1,\ldots,x_{n-1}) \end{aligned}$$

□

Dieses Lemma hilft uns folgendermaßen: Die Funktion id_1^2 ist in jeder unter Superposition abgeschlossenen Menge vorhanden, also sind sowohl id_1^2 als auch $Q_g(\mathrm{id}_1^2)$ in μ_{Q_g}. Sei M eine unter Superposition abgeschlossene Menge Boolescher Funktionen mit $\mu_{Q_g} \subseteq M$. Wenn wir zeigen wollen, dass M auch unter Q_g abgeschlossen ist, müssen wir für eine beliebige Funktion $f \in M$ zeigen, dass auch $Q_g(f) \in M$ ist. Wegen Lemma 4 können wir jedoch annehmen, dass die letzte Variable von f nicht fiktiv ist.

Lemma 5. *Für eine zweistellige Boolesche Funktion g sei $g_1(x) \stackrel{def}{=} g(0,1)$ und $g_2(x) \stackrel{def}{=} g(x,x)$. Dann gilt*

$$\mu_{Q_g} = [\{g_1, g_2\}]_{\mathrm{SUP}} \in \{\mathrm{I}_1, \mathrm{I}_0, \mathrm{I}, \mathrm{N}\}.$$

Beweis. Wir beweisen zunächst $[\{g_1, g_2\}]_{\mathrm{SUP}} \in \{\mathrm{I}_1, \mathrm{I}_0, \mathrm{I}, \mathrm{N}\}$:
Für beliebige g ist $g_1 \in \{c_0, c_1\}$ und $g_2 \in \{c_0, c_1, \mathrm{id}, \mathrm{non}\}$. Mit Blick auf Tabelle 1 sieht man, dass die abgeschlossene Menge $[\{g_1, g_2\}]_{\mathrm{SUP}}$ nur eine der Mengen I_1, I_0, I oder N sein kann.

Nun zur Gleichung $\mu_{Q_g} = [\{g_1, g_2\}]_{\mathrm{SUP}}$:
Mit den Operationen VI, FV und ZV sind $\mathrm{id}_2^2, \mathrm{id}_1^2 \in \mu_{Q_g}$. Die Anwendung der Quantoren-Operation ergibt $Q_g(\mathrm{id}_2^2) = g_1$ und $Q_g(\mathrm{id}_1^2) = g_2$, also gilt $\mu_{Q_g} \supseteq \{g_1, g_2\}$. Wegen den Eigenschaften des algebraischen Abschlusses ist folglich $\mu_{Q_g} \supseteq [\{g_1, g_2\}]_{\mathrm{SUP}}$.

Offensichtlich ist $[\emptyset]_{\mathrm{SUP}_{Q_g}} \subseteq [\{g_1, g_2\}]_{\mathrm{SUP}_{Q_g}}$. Für die andere Inklusion genügt also zu zeigen, dass $[\{g_1, g_2\}]_{\mathrm{SUP}_{Q_g}} = [\{g_1, g_2\}]_{\mathrm{SUP}}$ gilt. Sei $f \in [\{g_1, g_2\}]_{\mathrm{SUP}}$ eine beliebige n-stellige Funktion. Wir zeigen nun, dass auch $Q_g(f) \in [\{g_1, g_2\}]_{\mathrm{SUP}}$ ist. Da $Q_g(\mathrm{id}_1^2) = g_2 \in [\{g_1, g_2\}]_{\mathrm{SUP}}$ ist, können wir Lemma 4 benutzen: Ist die letzte Variable von f fiktiv, so ist $Q_g(f) \in [\{g_1, g_2\}]_{\mathrm{SUP}}$. Im Folgenden sei also die letzte Variable von f nicht fiktiv.

Im Fall $[\{g_1, g_2\}]_{\mathrm{SUP}} \neq \mathrm{N}$ kann nur $f = \mathrm{id}_n^n$ gelten. Damit stimmt $Q_g(f)$ bis auf fiktive Variablen mit g_1 überein und damit aus $[\{g_1, g_2\}]_{\mathrm{SUP}}$.

Ist andernfalls $[\{g_1, g_2\}]_{\mathrm{SUP}} = \mathrm{N}$, so gilt für f entweder wieder $f = \mathrm{id}_n^n$ oder $f(x_1, \ldots, x_n) = \overline{x_n}$. Für letzteres ist dann $Q_g(f)(x_1, \ldots, x_{n-1}) = g(1, 0)$. Dies ist eine Konstante und da in N alle Konstanten vorhanden sind, gilt ebenfalls $Q_g(f) \in [\{g_1, g_2\}]_{\mathrm{SUP}}$.

Es ist also $Q_g(f) \in [\{g_1, g_2\}]_{\mathrm{SUP}}$ für eine beliebige Funktion $f \in [\{g_1, g_2\}]_{\mathrm{SUP}}$, und damit $[\{g_1, g_2\}]_{\mathrm{SUP}_{Q_g}} = [\{g_1, g_2\}]_{\mathrm{SUP}}$. □

Die Resultate dieses Lemmas sind nahezu alles, was man wissen muss, um Quantoren-Operationen zu klassifizieren. Wir werden sehen, dass das Verhalten auf den zweistelligen Identitäten eine Quantoren-Operation eindeutig kennzeichnet, der Wert $g(1, 0)$ ist also irrelevant für ihr Verhalten. Fast alle Operationen erzeugen auch keine weiteren Funktionen, als die in μ_{Q_g}. Wir wollen dafür einen Begriff einführen: Eine Operation Q_g heißt *homogen*, wenn für alle $M \subseteq \mathrm{BF}$ mit $M = [M]_{\mathrm{SUP}_{Q_g}}$ gilt:

$$\mu_{Q_g} \subseteq M \Longrightarrow M = [M]_{\mathrm{SUP}_{Q_g}}$$

Eine homogene Operation ist also auf jeder Menge genauso mächtig wie auf der leeren Menge.

3.1 Die All- und Existenzquantoren-Gruppen

Wir definieren zwei Gruppen von Quantoren-Operationen: Die *Allquantoren-Gruppe* $\mathrm{ALL} \stackrel{\text{def}}{=} \{Q_g \mid g(0,0) = g(0,1) = 0\}$ und die *Existenzquantoren-Gruppe* $\mathrm{EXISTS} \stackrel{\text{def}}{=} \{Q_g \mid \mathrm{dualOp}(Q_g) \in \mathrm{ALL}\} = \{Q_g \mid g(0,1) = g(1,1) = 1\}$.

Der Existenzquantor EX liegt in EXISTS und FA in ALL. Die Existenzquantoren-Gruppe ist das duale Gegenstück zur Allquantoren-Gruppe. Dies sind die beiden schwächsten Gruppen von Quantoren-Operationen, weil Ihre Hinzunahme zu den Operationen den Postschen Graphen am wenigsten verändert. Für alle Q_g aus ALL und EXISTS sind die Wertetabellen der Funktionen g in den Abbildungen 2(a) und 2(b) aufgeführt. Außerdem sind ihre definierenden Werte grau markiert.

Wir werden zunächst nur ALL behandeln, die Resultate für EXISTS erhalten wir dann durch Dualität.

Beobachtung 6. *Für $Q_g \in \mathrm{ALL}$ ist $\mu_{Q_g} = \mathrm{I}_0$.*

Beweis. Wir benutzen Lemma 5. Für die Funktionen g_1 und g_2 aus Lemma 5 gilt $g_1 = c_0$ und $g_2 \in \{c_0, \mathrm{id}\}$. Damit ist $\mu_{Q_g} = [\{c_0\}]_{\mathrm{SUP}} = \mathrm{I}_0$ (siehe Tabelle 1). □

Da jede unter Superposition und Q_g abgeschlossene Menge μ_{Q_g} enthalten muss, können, wie man aus dem Postschen Graphen leicht entnehmen kann, höchstens die Mengen aus Abbildungen 2(c) abgeschlossen sein. In der Tat sind auch genau diese Mengen abgeschlossen. Die All- und Existenzquantoren-Gruppen sind also homogen. Wir werden nun für jede dieser Mengen die Abgeschlossenheit zeigen. Die Beweise werden wir sehr allgemein halten und sie für die anderen Gruppen von Operationen teilweise wiederverwenden. Es sei noch gesagt, dass eine ALL-Operation die Voraussetzungen der in diesem Abschnitt folgenden Lemmata immer erfüllt.

Lemma 7. *Für eine beliebige Quantoren-Operation Q_g ist eine unter Superposition abgeschlossene Menge M mit $\mu_{Q_g} \subseteq M \subseteq \mathrm{L}$ auch unter Q_g abgeschlossen.*

Beweis. Sei $f \in M$ eine beliebige n-stellige Funktion mit $n \geq 2$. Wegen Lemma 4 nehmen wir an, dass x_n nicht fiktiv ist. Da außerdem f linear ist, gilt $f(x_1, \ldots, x_{n-1}, 1) = \overline{f(x_1, \ldots, x_{n-1}, 0)}$. Damit ist

$$\begin{aligned} Q_g(f)(x_1, \ldots, x_{n-1}) &= g(f(x_1, \ldots, x_{n-1}, 0), \overline{f(x_1, \ldots, x_{n-1}, 0)}) \\ &= g(1,0) f(x_1, \ldots, x_{n-1}, 0) \vee g(0,1) \overline{f(x_1, \ldots, x_{n-1}, 0)} \end{aligned}$$

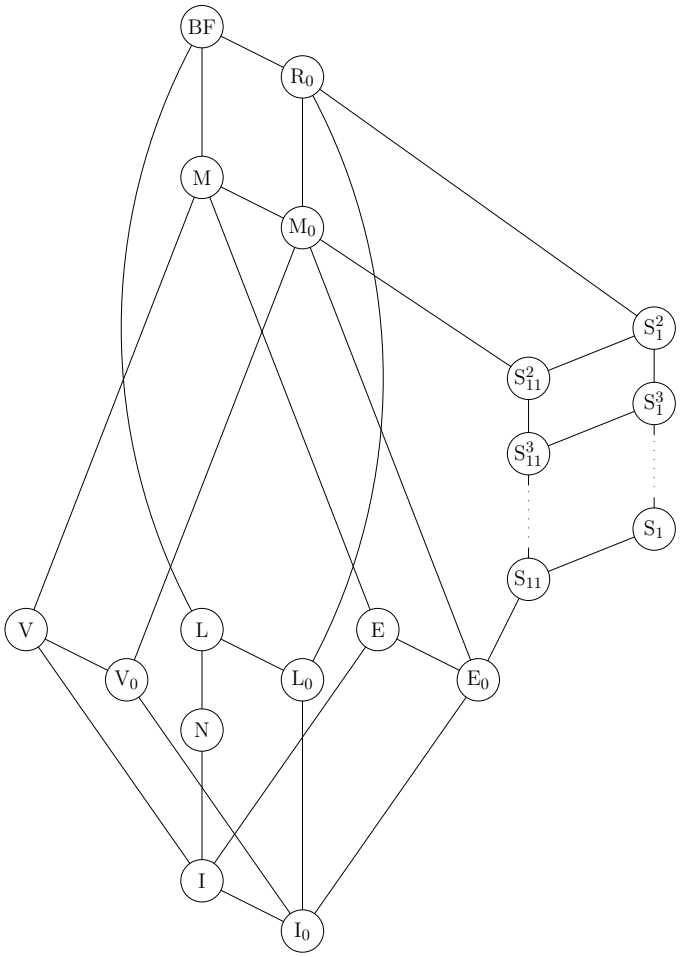
Gilt $g(1,0) = g(0,1)$, so ist $Q_g(f) = g(0,1) \in \mu_{Q_g} \subseteq M$. Andernfalls ist $Q_g(f)(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, g(0,1)) \in M$. □

x_1	x_2	$g(x_1, x_2)$			
0	0	0	0	0	0
0	1	0	0	0	0
1	0	0	0	1	1
1	1	0	1	0	1

(a) g für alle Q_g aus der Allquantoren-Gruppe

x_1	x_2	$g(x_1, x_2)$			
0	0	0	0	1	1
0	1	1	1	1	1
1	0	0	1	0	1
1	1	1	1	1	1

(b) g für alle Q_g aus der Existenzquantoren-Gruppe



(c) Verband der unter Superposition und einer Allquantor-Operation abgeschlossenen Mengen Boolescher Funktionen

Abbildung 2: Die All- und Existenzquantoren-Gruppen

Lemma 8. *Sei Q_g eine beliebige Quantoren-Operation, so dass $\mu_{Q_g} \subseteq \mathrm{V}$. Dann ist $[\mathrm{V}]_{\mathrm{SUP}_{Q_g}} = \mathrm{V}$ genau dann, wenn $g(1,1) = 1$ oder $g(0,1) = 0$ ist.*

Beweis. Sei $f \in \mathrm{V}$ eine n-stellige Boolesche Funktion mit $n \geq 2$. Zur Erleichterung der Lesbarkeit nehmen wir hier an, dass f keine fiktiven Variablen besitzt, es ist also $f(x_1, \ldots, x_n) = x_1 \vee \cdots \vee x_n$. Dann gilt:

$$\begin{aligned} Q_g(f)(x_1, \ldots, x_{n-1}) &= g(x_1 \vee \cdots \vee x_{n-1}, 1) \\ &= g(0,1)(\overline{x_1 \vee \cdots \vee x_{n-1}}) \vee g(1,1)(x_1 \vee \cdots \vee x_{n-1}) \end{aligned}$$

Im Falle $g(0,1) = g(1,1)$ ist wieder $Q_g(f) = g(0,1) \in \mu_{Q_g} \subseteq V$. Ist $g(0,1) = 0$ und $g(1,1) = 1$, so liegt $Q_g(f)$ in V. Falls jedoch $g(0,1) = 1$ und $g(1,1) = 0$ ist, so gilt $Q_g(x_1 \vee x_2) = \overline{x_1} \notin \mathrm{V}$. □

Korollar 9. *Sei Q_g eine beliebige Quantoren-Operation, so dass $\mu_{Q_g} \subseteq \mathrm{E}$ gilt. Dann ist $[\mathrm{E}]_{\mathrm{SUP}_{Q_g}} = \mathrm{E}$ genau dann, wenn $g(0,0) = 0$ oder $g(0,1) = 1$ ist.*

Beweis. Man erhält dieses Korollar, wenn man Lemma 8 mit der Abbildung dual in die duale Algebra überträgt, denn es ist dual(V) = E. Die Bedingungen an g erhält man, weil in der dualen Algebra auch die duale Operation benutzt werden muss, und es gilt $\mathrm{dualOp}(Q_g) \stackrel{\mathrm{def}}{=} Q_{\mathrm{dual}(\mathrm{ZV}(g))}$. □

Lemma 10. *Für eine beliebige Quantoren-Operation Q_g und $k \geq 2$ gilt:*

$$\mu_{Q_g} \subseteq S_1^k \iff [S_1^k]_{\mathrm{SUP}_{Q_g}} = S_1^k$$

Ist S_1^k für jedes $k \geq 2$ abgeschlossen unter SUP_{Q_g}, so ist es auch S_1.

Beweis. Für ein beliebiges $k \geq 2$ zeigen wir zuerst die Äquivalenz, und davon zunächst die Richtung „⇐“. Sei also $[S_1^k]_{\mathrm{SUP}_{Q_g}} = S_1^k$. Offensichtlich gilt $\emptyset \subseteq S_1^k$ und damit $\mu_{Q_g} = [\emptyset]_{\mathrm{SUP}_{Q_g}} \subseteq [S_1^k]_{\mathrm{SUP}_{Q_g}} = S_1^k$.

Nun zu „⇒“: Laut Lemma 5 gibt es für μ_{Q_g} nur die Möglichkeiten I_0, I_1, I oder N. Da $\mu_{Q_g} \subseteq S_1^k$ ist, bleiben noch I_2 und I_0 (siehe Abbildung 1). Für g bedeutet dies, dass $g(0,1) = 0$ und $g(x,x) \in \{\mathrm{id}, c_0\}$ ist (siehe Lemma 5), beziehungsweise $g(0,0) = g(0,1) = 0$.

Sei nun $f \in S_1^k$ eine n-stellige Boolesche Funktion und $a_1, \ldots, a_{n-1} \in \{0,1\}$. Dann gilt die Implikation:

$$f(a_1, \ldots, a_{n-1}, 0) = 0 \Longrightarrow Q_g(f)(a_1, \ldots, a_{n-1}) = g(0, f(a_1, \ldots, a_{n-1}, 1)) = 0$$

Umgekehrt folgt also aus $Q_g(f)(a_1, \ldots, a_{n-1}) = 1$, dass $f(a_1, \ldots, a_{n-1}, 0) = 1$ sein muss. Für die Urbilder der Eins bedeutet dies:

$$Q_g(f)^{-1}(\{1\}) \times \{0\} \subseteq f^{-1}(\{1\})$$

Da $f \in S_1^k$ ist, ist jede Menge $M \subseteq f^{-1}(\{1\})$ mit $|M| = k$ Eins-separierbar. Das heißt es existiert ein j mit $1 \leq j \leq n$, so dass $M \subseteq \{0,1\}^{j-1} \times \{1\} \times \{0,1\}^{n-j}$. Sei $M \subseteq Q_g(f)^{-1}(\{1\})$ mit $|M| = k$. Dann ist $M \times \{0\}$ eine k-elementige Teilmenge von $f^{-1}(\{1\})$ und damit Eins-separierbar. Für die in der Definition genannte Stelle j kann jedoch nicht $j = n$ gelten, da die n-te Stelle von $M \times \{0\}$ immer Null ist. Also ist $j \leq n-1$, M ist Eins-separierbar und damit $Q_g(f)$ Eins-separierend.

Die Aussage über S_1 gilt offensichtlich wegen der Definition von S_1. □

Lemma 11. *Sei Q_g eine beliebige Quantoren-Operation, so dass $\mu_{Q_g} \subseteq \mathrm{M}$ gilt. Dann ist $[\mathrm{M}]_{\mathrm{SUP}_{Q_g}} = \mathrm{M}$ genau dann, wenn $g(0,0) \leq g(0,1) \leq g(1,1)$ ist.*

Beweis. Wir zeigen zunächst die Richtung „⇒“. Ist $1 = g(0,0) > g(0,1) = 0$, dann gilt mit der monotonen Funktion et:

$$Q_g(\mathrm{et})(0) = g(0 \wedge 0, 0 \wedge 1) = g(0,0) = 1$$

und

$$Q_g(\mathrm{et})(1) = g(1 \wedge 0, 1 \wedge 1) = g(0,1) = 0.$$

Also ist $Q_g(\mathrm{et}) \notin \mathrm{M}$.

Für den Fall $1 = g(0,1) > g(1,1) = 0$ und mit der monotonen Funktion vel gilt:

$$Q_g(\mathrm{vel})(0) = g(0 \vee 0, 0 \vee 1) = g(0,1) = 1$$

und

$$Q_g(\mathrm{vel})(1) = g(1 \vee 0, 1 \vee 1) = g(1,1) = 0$$

und damit ist $Q_g(\mathrm{vel})$ ebenfalls nicht monoton.

Für „⇐“ sei $n \geq 2$ und $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \{0,1\}^n$ mit $a_i \leq b_i$ für $1 \leq i \leq n$. Dann gilt für eine beliebige, n-stellige und monotone Funktion f: $f(a_1, \ldots, a_n) \leq f(b_1, \ldots, b_n)$. Betrachten wir nun

$$Q_g(f)(a_1, \ldots, a_{n-1}) = g(\underbrace{f(a_1, \ldots, a_{n-1}, 0)}_{\stackrel{\mathrm{def}}{=} a}, \underbrace{f(a_1, \ldots, a_{n-1}, 1)}_{\stackrel{\mathrm{def}}{=} b})$$

und

$$Q_g(f)(b_1, \ldots, b_{n-1}) = g(\underbrace{f(b_1, \ldots, b_{n-1}, 0)}_{\stackrel{\mathrm{def}}{=} c}, \underbrace{f(b_1, \ldots, b_{n-1}, 1)}_{\stackrel{\mathrm{def}}{=} d}).$$

Wegen der Monotonie von f ist $a \leq b$, $c \leq d$ aber auch $a \leq c$ und $b \leq d$. Da nach Voraussetzung $g(0,0) \leq g(0,1) \leq g(1,1)$ gilt, ist $g(a,b) \leq g(c,d)$ für alle solchen a, b, c, d. Damit ist $Q_g(f)$ monoton. □

Wie schon erwähnt, ist auch hier der Wert $g(1,0)$ nicht relevant.

Lemma 12. *Sei Q_g eine beliebige Quantoren-Operation. R_1 ist genau dann unter SUP_{Q_g} abgeschlossen, wenn $\mu_{Q_g} \subseteq R_1$ gilt.*

Beweis. Ist $\mu_{Q_g} \not\subseteq R_1$, so ist R_1 offenbar nicht abgeschlossen unter SUP_{Q_g}. Ist umgekehrt $\mu_{Q_g} \subseteq R_1$, so muss $c_0 \notin \mu_{Q_g}$ gelten. Für die in Lemma 5 definierten Funktionen g_1 und g_2 gilt dann: $c_0 \neq g_1(x) = g(0,1)$, also $g(0,1) = 1$ und $g_2 \notin \{c_0, \mathrm{non}\}$, also $g(1,1) = 1$. Sei schließlich $f \in R_1$ eine n-stellige Funktion mit $n \geq 2$. Dann gilt:

$$Q_g(f)(1,\ldots,1) = g(f(1,\ldots,1,0), f(1,\ldots,1,1)) = g(f(1,\ldots,1,0),1) = 1$$

Und damit ist $Q_g(f) \in R_1$. □

Die Voraussetzungen aller dieser Lemmata sind für eine Allquantoren-Operation erfüllt. Da die restlichen Mengen aus Abbildung 2(c) über Durchschnitte definiert sind, haben wir mit Lemma 1 folgendes Resultat:

Satz 13. *Für $Q_g \in$ ALL sind die Mengen* BF, R_0, M, M_0, $\mathrm{S}_1^{\mathrm{k}}$, $\mathrm{S}_{11}^{\mathrm{k}}$, S_1, S_{11}, V, V_0, L, L_0, E, E_0, N, I *und I_0 für $k \geq 2$ (siehe Abbildung 2(c)) genau die unter SUP_{Q_g} abgeschlossenen Mengen.*

Beweis. Lemma 5 zeigt, dass andere Mengen als diese nicht abgeschlossen sein können, und die vorangegangenen Lemmata zeigen mit Lemma 1, dass sie in der Tat alle abgeschlossen sind. □

Korollar 14. *Für $Q_g \in$ EXISTS sind genau die Mengen* BF, R_1, M, M_1, $\mathrm{S}_0^{\mathrm{k}}$, $\mathrm{S}_{01}^{\mathrm{k}}$, S_0, S_{01}, V, V_1, L, L_1, E, E_1, N, I *und I_1 für $k \geq 2$ unter SUP_{Q_g} abgeschlossenen.*

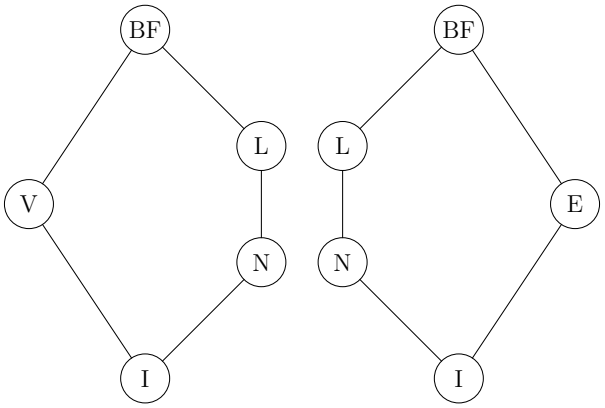
Beweis. Dieses Korollar folgt durch Dualität aus Satz 13. Die angegebenen Mengen und Operationen sind die dualen Gegenstücke zu denen aus Satz 13. Da die Abgeschlossenheit bei Übergang zur dualen Algebra erhalten bleibt (Lemma 3), gilt dieses Korollar. □

x_1	x_2	$g(x_1, x_2)$	
0	0	1	1
0	1	0	0
1	0	0	1
1	1	1	1

(a) g für alle Q_g aus EVEN

x_1	x_2	$g(x_1, x_2)$	
0	0	0	0
0	1	1	1
1	0	0	1
1	1	0	0

(b) g für alle Q_g aus ODD



(c) Verband der unter Superposition und einer EVEN-Operation abgeschlossenen Mengen Boolescher Funktionen

(d) Verband der unter Superposition und einer ODD-Operation abgeschlossenen Mengen Boolescher Funktionen

Abbildung 3: Die Gruppen EVEN und ODD

3.2 Die Gruppen EVEN und ODD

Die Gruppe EVEN $\stackrel{\text{def}}{=} \{Q_g \mid g(0,0) = g(1,1) = 1, g(0,1) = 0\}$ und die dazu duale Gruppe ODD $\stackrel{\text{def}}{=} \{Q_g \mid g(0,0) = g(1,1) = 0, g(0,1) = 1\}$ haben gravierendere Auswirkungen auf den Postschen Graphen. Die Wertetabellen der Funktionen g sind in den Abbildungen 3(a) und 3(b) angegeben. Wie schon bei den Allquantoren werden wir nur EVEN behandeln. Der Verband der abgeschlossenen Mengen ist, um die Ergebnisse der Sätze 16 und 17 vorwegzunehmen, in den Abbildungen 3(c) beziehungsweise 3(d) dargestellt. Die Namensgebung ist motiviert durch die Tatsache, dass in den relevanten Teilen der Wertetabelle (grau hinterlegte Zeilen) bei einer EVEN-Operation eine gerade Anzahl Einsen vorkommt und bei einer ODD-Operation eine ungerade Anzahl.

Beobachtung 15. *Für* $Q_g \in$ EVEN *ist* $\mu_{Q_g} = \mathrm{I}$.

Beweis. Wir benutzen Lemma 5. Für die Funktionen g_1 und g_2 aus Lemma 5 gilt $g_1 = c_0$ und $g_2 = c_1$. Damit ist $\mu_{Q_g} = [\{c_0, c_1\}]_{\mathrm{SUP}} = \mathrm{I}$ (siehe Tabelle 1). □

Satz 16. *Die unter Superposition und* $Q_g \in$ EVEN *abgeschlossenen Mengen Boolescher Funktionen sind genau die Mengen* BF*,* V*,* N*,* L *und* I*.*

Beweis. Aus Beobachtung 15 ergibt sich, dass höchstens die Mengen I, V, N, E, L, M und BF abgeschlossen sein können. Lemma 7 ist auch für EVEN gültig, also sind L und N abgeschlossen. V ist abgeschlossen, da $g(1,1) = 1$ gilt (siehe Lemma 8). Aus Korollar 9 sieht man jedoch, dass E nicht abgeschlossen ist (Es gilt weder $g(0,0) = 0$ noch $g(0,1) = 1$). M ist ebenfalls nicht abgeschlossen (Lemma 11), da $g(0,0) = 1 \not\leq g(0,1) = 0$. □

Korollar 17. *Die unter Superposition und* $Q_g \in$ ODD *abgeschlossenen Mengen Boolescher Funktionen sind genau die Mengen* BF*,* E*,* N*,* L *und* I*.*

Beweis. Dieses Korollar folgt durch Dualität aus Satz 16. Die angegebenen Mengen und Operationen sind die dualen Gegenstücke zu denen aus Satz 16. Da die Abgeschlossenheit bei Übergang zur dualen Algebra erhalten bleibt (Lemma 3), gilt dieses Korollar. □

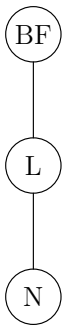
Wie man sieht, sind die EVEN-Operationen nicht homogen, da eine EVEN-Operation auf E stärker ist als auf der leeren Menge: Auf E erzeugt sie die Negation und die Konstanten, wobei sie auf der leeren Menge nur die Konstanten erzeugt.

3.3 Die Gruppe NOT

Die Gruppe NOT $\stackrel{\text{def}}{=} \{Q_g \mid g(0,0) = 1, g(1,1) = 0\}$ ist eine „selbstduale“ Gruppe, denn für jede Operation $Q_g \in \text{NOT}$ ist $\text{dualOp}(Q_g) = Q_g$. Die Wertetabellen der Funktionen g sind in Abbildung 4(a) aufgeführt. Der Verband der abgeschlossenen Mengen ist in Abbildung 4(b) angegeben.

x_1	x_2	$g(x_1, x_2)$			
0	0	1	1	1	1
0	1	0	0	1	1
1	0	0	1	0	1
1	1	0	0	0	0

(a) g für alle Q_g aus NOT



(b) Verband der unter Superposition und einer NOT-Operation abgeschlossenen Mengen Boolescher Funktionen

Abbildung 4: Die Gruppe NOT

Beobachtung 18. *Für* $Q_g \in \text{NOT}$ *ist* $\mu_{Q_g} = N$.

Beweis. Wir benutzen wiederum Lemma 5. Für die Funktionen g_1 und g_2 aus Lemma 5 gilt $g_1 \in \{c_0, c_1\}$ und $g_2 = \text{non}$. Damit ist, wie man an Tabelle 1 sieht, $\mu_{Q_g} = [\{c_0, \text{non}\}]_{\text{SUP}} = [\{c_1, \text{non}\}]_{\text{SUP}} = \text{N}$. □

Dadurch bleiben nicht mehr viele Mengen übrig, die abgeschlossen sein können.

Satz 19. *Die unter Superposition und* $Q_g \in \text{NOT}$ *abgeschlossenen Mengen Boolescher Funktionen sind genau die Mengen* BF*,* L *und* N*.*

Beweis. Wie man an Abbildung 1 mit Beobachtung 18 sieht, können nur BF, L und N abgeschlossen sein, da sie die einzigen unter Superposition abgeschlossenen Mengen sind, die $\mu_{Q_g} = \text{N}$ enthalten. Lemma 7 zeigt, dass sie wirklich abgeschlossen sind (BF ist trivialerweise abgschlossen.). □

Bei NOT handelt es sich also wieder um eine Gruppe von homogenen Operationen, wobei der Begriff „homogen“ natürlich immer weniger aussagekräftig wird, je größer die kleinste abgeschlossene Menge ist.

4 Ausblick

Eine der noch offenen Fragen dieser Arbeit ist, warum für die Auswirkungen einer Operation Q_g der Wert $g(1,0)$ irrelevant ist. Natürlich tritt dieser Wert nur in Erscheinung, wenn man Q_g auf eine Negation oder eine ähnliche Funktion anwendet. In jeder unter SUP_{Q_g} abgeschlossenen Menge ist jedoch eine Konstante vorhanden. Wenn nun auch noch die Negation vorhanden ist, sind sogar beide Konstanten erzeugbar. Dann könnte es sein, dass nicht mehr genug Differezierungsmöglichkeiten durch die Unterscheidung bei $g(1,0)$ vorhanden sind, denn die Operation ist sowieso schon sehr stark.

Man könnte die Quantoren-Operationen folgendermaßen auf mehrstellige Funktionen erweitern:

Für eine vierstellige Boolesche Funktion g sei Q_g^2 definiert als

$$Q_g^2(f)(x_1,\ldots,x_{n-2}) \stackrel{\text{def}}{=} g(f(x_1,\ldots,x_{n-2},0,0),f(x_1,\ldots,x_{n-2},0,1),\\ f(x_1,\ldots,x_{n-2},1,0),f(x_1,\ldots,x_{n-2},1,1)).$$

Hier wäre es interessant zu erfahren, welche Werte von g irrelevant für das Verhalten der Operation sind.

Außerdem bleibt noch die Frage wie sich die Inhomogenität einer Operation ergibt. Natürlich kann man beliebige inhomogene Operationen definieren, jedoch ist die Definition dann recht unnatürlich. Zum Beispiel ist

$$O : \mathrm{BF}^n \to \mathrm{BF}, f \mapsto \begin{cases} \mathrm{vel}, & \text{falls } f \in \mathrm{S}_1^2 \setminus (\mathrm{S}_{11}^2 \cup \mathrm{S}_{12}^2 \cup \mathrm{S}_1^3) \\ f, & \text{sonst} \end{cases}$$

eine inhomogene Operation mit etwas seltsamen Auswirkungen auf den Postschen Verband. Wenn man einfache Definitionen von Operationen fordert, wird sich die Inhomogenität wohl auf das Erzeugen der Negation beschränken, wie das bei EVEN der Fall ist.

Literatur

[BCRV03] E. Böhler, N. Creignou, S. Reith, H. Vollmer. Playing with Boolean blocks, Part I: Post's lattice with applications to complexity theory. *ACM-SIGACT Newsletter*, 34(4):38-52, 2003.

[Coh65] P. M. Cohn *Universal Algebra.* Harper & Row, 1965.

[JGK70] S. W. Jablonski, G. P. Gawrilow, W. B. Kudrjawzew. *Boolesche Funktionen und Postsche Klassen.* Akademie-Verlag, 1970.

[Pos41] E. L. Post. The two-valued iterative systems of mathematical logic. *Annals of Mathematical Studies*, 5:1-122, 1941.

[RW00] S. Reith, K. W. Wagner. The complexity of problems defined by Boolean circuits. Forschungsbericht 255, Institut für Informatik, Universität Würzburg, 2000.