Verallgemeinerte Superposition bei binären Automaten

Von M. Gössel und H. D. Modrow

Das große Interesse, das die linearen Automaten innerhalb der Automatentheorie gefunden haben, beruht zu einem erheblichen Teil auf der Gültigkeit des Superpositionsprinzips bezüglich der Addition. Aufgrund der Gültigkeit dieses Prinzips ist z. B. das Input-Output-Verhalten eines linearen Automaten (für den Initialzustand 0) mit eindimensionalem Input schon durch die sog „Impulsantwort" des Automaten vollständig bestimmt, s. z. B. [1].

Ausgehend vom Superpositionsprinzip für lineare Automaten mit eindimensionalem Input und Output über GF(2) wird in der vorliegenden Arbeit untersucht, inwieweit sich dieses Prinzip von der Operation + (Addition modulo 2, Antivalenz) auch auf andere Operationen (Boolesche Funktionen) und Automatenklassen übertragen läßt.

Ein Ansatz für die Übertragung des Superpositionsprinzips auf andere Boolesche Funktionen findet sich in [2]. Dort wird gezeigt, daß für sog. „disjunktive" Automaten, die in Analogie zu den linearen Automaten eingeführt werden, das Superpositionsprinzip für die Disjunktion gilt.

In der vorliegenden Arbeit wird nicht von gegebenen Automatenklassen ausgegangen, sondern es wird für jede zweistellige Boolesche Funktion die Klasse aller Automaten charakterisiert, die dem Superpositionsprinzip bzgl. dieser Booleschen Funktion genügen. Diese Charakterisierung ist nicht explizit zustandsabhängig. Eine derartige Beschreibung auf der Grundlage der hier gegebenen Charakterisierung findet sich in [3].

In dieser Note werden nur initiale vollständig definierte synchrone Automaten $\mathfrak{A}=[X, Y, Z, z_0, \delta, \lambda]$ mit $X=Y=\{0, 1\}$, $z_0\in Z$ betrachtet. Diese Automaten werden *binäre Automaten* genannt. Ist $\mathfrak{A}=[X, Y, Z, z_0, \delta, \lambda]$ ein binärer Automat, so bezeichnen wir den letzten von $\mathfrak{A}$ ausgegebenen Buchstaben (aus $Y=\{0, 1\}$) nach Eingabe eines nicht leeren Wortes $p=x_1\dots x_t$ $(t\geqq 1)$ durch $g_t^{\mathfrak{A}}(x_1, \dots, x_t)$,

$$g_t^{\mathfrak{A}}(x_1, \dots, x_t) =_{Df} \lambda(\delta(z_0, x_1 \dots x_{t-1}), x_t).$$

Damit is $\mathfrak{A}$ ein System $\{g_t^{\mathfrak{A}}|t=1, 2, \dots\}$ von Booleschen Funktionen zugeordnet; $g_t^{\mathfrak{A}}$: $\{0, 1\}^t\to\{0, 1\}$.

Definition. Es bezeichne F eine zweistellige Boolesche Funktion, $F: \{0, 1\}^2 \to \{0, 1\}$. Dann nennen wir einen binären Automaten $\mathfrak{A}$ *F-superponierbar,* wenn für jedes $t \geqq 1$ gilt:

$$g_t^{\mathfrak{A}}(F(x_1, x_1'), \dots, F(x_t, x_t')) = F(g_t^{\mathfrak{A}}(x_1, \dots, x_t), g_t^{\mathfrak{A}}(x_1', \dots, x_t')) \tag{1}$$

$$(x_1, \dots, x_t, x_1', \dots, x_t' \in \{0, 1\}).$$

Unmittelbar einsichtig ist, daß ein binärer Automat $\mathfrak{A}$ F-superponierbar für jede 2-stellige Boolesche Funktion F ist, wenn er die folgende Eigenschaft besitzt: Es gibt eine eindeutige Abbildung $\tau_{\mathfrak{A}}: Nz^+ \to Nz^+$ [1]) mit $\tau_{\mathfrak{A}}(t) \leqq t$, so daß

$$g_t^{\mathfrak{A}}(x_1, \dots, x_t) = x_{\tau_{\mathfrak{A}}(t)} \tag{2}$$

für jedes t, $t \geqq 1$, $x_1, \dots, x_t \in \{0, 1\}$ gilt. Für einen solchen Automaten ist also in jedem Takt t die Funktion $g_t^{\mathfrak{A}}$ die Projektion auf eine (die $\tau_{\mathfrak{A}}(t)$-te) Variable. In jedem Takt t wird von $\mathfrak{A}$ einer der bisher eingegebenen Inputs ausgewählt und als Output direkt ausgegeben.

Automaten, für die (2) gilt, nennen wir *auswählende Automaten;* die Klasse aller dieser Automaten bezeichnen wir durch $\mathscr{A}_{\text{Ausw}}$.

Man zeigt nun umgekehrt auch leicht, daß nur Automaten aus $\mathscr{A}_{\text{Ausw}}$ F-superponierbar für jede 2-stellige Boolesche Funktion sind.

Dazu stellen wir jede Funktion $g_t^{\mathfrak{A}}$ $(t \geqq 1)$ in ihrer antivalenten Normalform dar:

$$g_t^{\mathfrak{A}}(x_1, \dots, x_t) = a_0 + \sum_{1 \leqq i \leqq t} a_i \cdot x_i + \sum_{1 \leqq i < j \leqq t} a_{ij} \cdot x_i \cdot x_j + \dots$$

$$\dots + a_{1 \dots t} \cdot x_1 \cdot \dots \cdot x_t; \tag{3}$$

dabei bezeichnet $+$ die Antivalenz (Addition modulo 2), $\cdot$ die Konjunktion (Multiplikation) — im folgenden wird das Zeichen $\cdot$ nicht geschrieben —, und die $a_0, a_1, \dots, a_t$, $a_{12}, \dots, a_{t-1,t}$ $a_{123}, \dots, a_{1\dots t}$ sind feste Koeffizienten aus $\{0, 1\}$. Die Darstellung (3) einer t-stelligen Booleschen Funktion ist eindeutig; vgl. [5].

Verschwänden nun in (3) alle Koeffizienten, so widerspräche dies der vorausgesetzten $\equiv$-Superponierbarkeit (vgl. Tab. 1) von $\mathfrak{A}$; denn dann wäre

$$\begin{aligned} 0 &= g_t^{\mathfrak{A}}(0, \dots, 0) \\ &= (g_t^{\mathfrak{A}}(0, \dots, 0) \equiv g_t^{\mathfrak{A}}(1, \dots, 1)) \\ &= (0 \equiv 0) \\ &= 1. \end{aligned}$$

Wäre in (3) $a_0 = 1$, so widerspräche dies der vorausgesetzten $+$-Superponierbarkeit von $\mathfrak{A}$; denn dann wäre

$$1 = g_t^{\mathfrak{A}}(0, \dots, 0) = g_t^{\mathfrak{A}}(0, \dots, 0) + g_t^{\mathfrak{A}}(0, \dots, 0) = 1 + 1 = 0.$$

Wir nehmen nun an, es wäre $a_1 = a_2 = \dots = a_t = 0$. Dann muß es einen nicht-verschwindenden Koeffizienten $a_{i_1 \dots i_k}$ mit $1 < k \leqq t$ geben; o.B.d.A. sei k minimal

[1]) $Nz^+ =_{\text{Df}} \{1, 2, 3, \dots\}$

und $a_{1\ldots k}=1$. Wegen der $+$-Superponierbarkeit von $\mathfrak{A}$ gilt aber

$$g_t^{\mathfrak{A}}(\underbrace{1, \ldots, 1}_{k}, 0, \ldots, 0) = g_t^{\mathfrak{A}}(0, \underbrace{1, \ldots, 1}_{k-1}, 0, \ldots, 0) + g_t^{\mathfrak{A}}(1, 0, \ldots, 0).$$

Nach unserer Annahme wäre aber

$$g_t^{\mathfrak{A}}(\underbrace{1, \ldots, 1}_{k}, 0, \ldots, 0) = a_{1\ldots k} \cdot 1^k = 1, \quad g_t^{\mathfrak{A}}(0, \underbrace{1, \ldots, 1}_{k-1}, 0, \ldots, 0) = 0 = g_t^{\mathfrak{A}}(1, 0, \ldots, 0).$$

Aus diesem Widerspruch folgt, daß es mindestens ein τ $(1 \leqq \tau \leqq t)$ mit $a_\tau = 1$ geben muß.

Gäbe es nun zwei verschiedene nicht-verschwindende Koeffizienten mit je einem Index, etwa $a_1 = a_2 = 1$, so folgte wegen der vorausgesetzten $+$-Superponierbarkeit von $\mathfrak{A}$

$$g_t^{\mathfrak{A}}(1, 1, 0, \ldots, 0) = g_t^{\mathfrak{A}}(1, 0, \ldots, 0) + g_t^{\mathfrak{A}}(0, 1, 0, \ldots, 0) = 1 + 1 = 0$$

und damit wegen der $\vee$-Superponierbarkeit von $\mathfrak{A}$

$$0 = g_t^{\mathfrak{A}}(1, 1, 0, \ldots, 0) = g_t^{\mathfrak{A}}(1, 0, \ldots, 0) \vee g_t^{\mathfrak{A}}(0, 1, 0, \ldots, 0) = 1 \vee 1 = 1.$$

Es gibt also höchstens — und damit genau — einen nicht verschwindenden Koeffizienten a_τ mit $1 \leqq \tau \leqq t$ in (3).

Wir nehmen nun an, es gäbe einen nicht-verschwindenden Koeffizienten $a_{i_1 \ldots i_k}$ mit $k \geqq 2$; o.B.d.A. sei k minimal, $a_{1\ldots k} = 1$.

Fall 1. $\tau \leqq k$. O.B.d.A. sei $\tau = 1$, also $a_1 = 1$, $a_{1\ldots k} = 1$. Dann folgt der Widerspruch

$$\begin{aligned} 0 = a_1 + a_{1\ldots k} &= g_t^{\mathfrak{A}}(\underbrace{1, \ldots, 1}_{k}, 0, \ldots, 0) \\ &= g_t^{\mathfrak{A}}(1, 0, \ldots, 0) + g_t^{\mathfrak{A}}(0, \underbrace{1, \ldots, 1}_{k-1}, 0, \ldots, 0) \\ &= a_1 + 0 = 1. \end{aligned}$$

Fall 2. $\tau > k$. O.B.d.A. sei $\tau = t$. Dann folgt der Widerspruch

$$\begin{aligned} 0 = a_{1\ldots k} + a_t &= g_t^{\mathfrak{A}}(\underbrace{1, \ldots, 1}_{k}, 0, \ldots, 0, 1) \\ &= g_t^{\mathfrak{A}}(1, 0, \ldots, 0) + g_t^{\mathfrak{A}}(0, \underbrace{1, \ldots, 1}_{k-1}, 0, \ldots, 0, 1) \\ &= 0 + a_t = 1. \end{aligned}$$

Damit ist gezeigt:

Satz 1. *Ein binärer Automat $\mathfrak{A}$ ist für jede zweistellige Boolesche Funktion F F-superponierbar genau dann, wenn $\mathfrak{A} \in \mathscr{A}_{\mathrm{Ausw}}$ ist.*

Aus dem Beweis folgt sogar:

Korollar. Ist ein binärer Automat $+$-, $\vee$- und $\equiv$-superponierbar, so ist er für jede zweistellige Boolesche Funktion F F-superponierbar.

(Dies ergibt sich auch unmittelbar aus dem unabhängig bewiesenen Satz 6.)

Tabelle 1

Die zweistelligen Booleschen Funktionen

Die Funktionen sind nach den Koeffizienten ihrer antivalenten Normalform geordnet: $F(x_1, x_2) = A_0 + A_1 x_1 + A_2 x_2 + A_{12} x_1 x_2$.

Im unteren Teil sind die Wertetabellen angegeben

	F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}	F_{15}
A_0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
A_1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
A_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
A_{12}	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Zeichen	0	1	x_1	$\bar{x}_1$	x_2	$\bar{x}_2$	$+$	$\equiv$	$\wedge$			$\rightarrow$			$\vee$	
x_1 x_2																
0 0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
1 0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
0 1	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
1 1	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0

Im folgenden soll für jede der 16 zweistelligen Booleschen Funktionen F_i, $i=0, \ldots, 15$ (vgl. Tab. 1), die Klasse derjenigen binären Automaten angegeben werden, die F_i-superponierbar sind.

Zunächst ergibt sich für die nicht echt von zwei Variablen abhängigen Funktionen $F_0, \ldots, F_5$ (s. Tab. 1) der

Satz 2. *Es sei* $\mathfrak{A}$ *ein binärer Automat. Dann gilt:*

1. *Jeder binäre Automat ist* F_2- *und* F_4-*superponierbar.*
2. $\mathfrak{A}$ *ist* F_0-*superponierbar genau dann, wenn für jedes* $t \geqq 1$ $g_t^{\mathfrak{A}}(0, \ldots, 0) = 0$ *gilt.* $\mathfrak{A}$ *ist* F_1-*superponierbar genau dann, wenn für jedes* $t \geqq 1$ *gilt:* $g_t^{\mathfrak{A}}(1, \ldots, 1) = 1$.
3. $\mathfrak{A}$ *ist* F_3- *bzw.* F_5-*superponierbar genau dann, wenn für jedes* $t \geqq 1$ *die Funktion* $g_t^{\mathfrak{A}}$ *selbstdual ist, d.h. wenn für jedes* $x_1, \ldots, x_t \in \{0, 1\}$ *gilt:*

$$\overline{g_t^{\mathfrak{A}}(x_1, \ldots, x_t)} = g_t^{\mathfrak{A}}(\bar{x}_1, \ldots, \bar{x}_t).$$

Um zu Aussagen für die echt von 2 Variablen abhängigen Funktionen $F_6, \ldots, F_{15}$ zu kommen, ordnen wir jeder Funktion $g_t^{\mathfrak{A}}$, jeder (partiellen) Belegung b der t Variablen von $g_t^{\mathfrak{A}}$, $t \geqq 3$, mit $t-2$ fixierten Werten und jedem $F \in \{F_6, \ldots, F_{15}\}$ zwei zweistellige Boolesche Funktionen G^b und H_F^b, folgendermaßen zu.

Ist $b = [x_1, x_2, x_3^0, \ldots, x_t^0]$ mit $x_3^0, \ldots, x_t^0 \in \{0, 1\}$ (o.B.d.A sind hier gerade den letzten $t-2$ Variablen fixierte Werte zugeordnet), so sei

$$G^b(x_1, x_2) =_{\mathrm{Df}} g_t^{\mathfrak{A}}(x_1, x_2, x_3^0, \ldots, x_t^0), \tag{4}$$

$$H_F^b(x_1, x_2) =_{\mathrm{Df}} g_t^{\mathfrak{A}}\big(x_1, x_2, F(x_3^0, x_3^0), \ldots, F(x_t^0, x_t^0)\big). \tag{5}$$

Ist $\mathfrak{A}$ nun F-superponierbar, so muß nach (1) für jede derartige Belegung b und jedes $x_1, x_1', x_2, x_2' \in \{0, 1\}$ gelten:

$$H_F^b(F(x_1, x_1'), F(x_2, x_2')) = F(G^b(x_1, x_2), G^b(x_1', x_2')). \qquad (6)$$

Ausgehend von (6) werden wir die Automatenklassen bestimmen, die F_i-superponierbar sind, $F_i \in \{F_6, \ldots, F_{15}\}$. Wir setzen $G^b = G$, $H_F^b = H$ und stellen, F, G, H in antivalenter Normalform dar.

$$\begin{aligned} F(x_1, x_2) &= A_0 + A_1 x_1 + A_2 x_2 + A_{12} x_1 x_2, \\ G(x_1, x_2) &= B_0 + B_1 x_1 + B_2 x_2 + B_{12} x_1 x_2, \\ H(x_1, x_2) &= b_0 + b_1 x_1 + b_2 x_2 + b_{12} x_1 x_2 \end{aligned} \qquad (7)$$

mit $A_0, A_1, A_2, A_{12}, B_0, B_1, B_2, B_{12}, b_0, b_1, b_2, b_{12} \in \{0, 1\}$. Aus (6) und (7) ergibt sich dann (8):

$$\begin{array}{lcl} F(G(x_1, x_2), G(x_1', x_2')) & = & H(F(x_1, x_1'), F(x_2, x_2')) \\ = A_0 + A_1 B_0 + A_2 B_0 + A_{12} B_0 & & = b_0 + b_1 A_0 + b_2 A_0 + b_{12} A_0 \\ + x_1(A_1 B_1 + A_{12} B_0 B_1) & & + x_1(b_1 A_1 + b_{12} A_0 A_1) \\ + x_2(A_1 B_2 + A_{12} B_0 B_2) & & + x_2(b_2 A_1 + b_{12} A_0 A_1) \\ + x_1'(A_2 B_1 + A_{12} B_0 B_1) & & + x_1'(b_1 A_2 + b_{12} A_0 A_2) \\ + x_2'(A_2 B_2 + A_{12} B_0 B_2) & & + x_2'(b_2 A_2 + b_{12} A_0 A_2) \\ + x_1 x_2(A_1 B_{12} + A_{12} B_0 B_{12}) & & + x_1 x_2(b_{12} A_1) \\ + x_1' x_2'(A_2 B_{12} + A_{12} B_0 B_{12}) & & + x_1' x_2'(b_{12} A_2) \\ + x_1 x_1'(A_{12} B_1) & & + x_1 x_1'(b_1 A_{12} + b_{12} A_0 A_{12}) \\ + x_2 x_1'(A_{12} B_1 B_2) & & + x_2 x_1'(b_{12} A_1 A_2) \\ + x_1 x_2'(A_{12} B_1 B_2) & & + x_1 x_2'(b_{12} A_1 A_2) \\ + x_2 x_2'(A_{12} B_2) & & + x_2 x_2'(b_2 A_{12} + b_{12} A_0 A_{12}) \\ + x_1 x_2 x_1'(A_{12} B_{12} B_1) & & + x_1 x_2 x_1'(b_{12} A_{12} A_1) \\ + x_1 x_2 x_2'(A_{12} B_{12} B_2) & & + x_1 x_2 x_2'(b_{12} A_{12} A_1) \\ + x_1 x_1' x_2'(A_{12} B_{12} B_1) & & + x_1 x_1' x_2'(b_{12} A_{12} A_2) \\ + x_2 x_1' x_2'(A_{12} B_{12} B_2) & & + x_2 x_1' x_2'(b_{12} A_{12} A_2) \\ + x_1 x_2 x_1' x_2'(A_{12} B_{12}). & & + x_1 x_2 x_1' x_2'(A_{12} b_{12}). \end{array} \qquad (8)$$

Jede Funktion $F \in \{F_6, \ldots, F_{15}\}$ ist in (7) und (8) durch Vorgabe der Koeffizienten A_0, A_1, A_2, A_{12} festgelegt.

(8) gilt genau dann, wenn die Koeffizienten an gleichen Variablenkombinationen gleich sind; und aus (8) ergibt sich gleichwertig ein System von 16 Gleichungen

für die Koeffizienten $B_0, B_1, B_2, B_{12}, b_0, b_1, b_2, b_{12}$ der antivalenten Normalform von G und H. Aus (8) bestimmen wir zunächst G und H und schließen dann auf $g_t^{\mathfrak{A}}(x_1, x_2, \ldots, x_t)$ für jedes $t \geqq 1$.

Wir wollen das allgemeine Verfahren am Beispiel der Funktionen F_6 und anschließend F_{14} (vgl. Tab. 1) ausführlich darstellen.

Es gilt $F_6(x_1, x_2) = x_1 + x_2$ und somit $A_0 = A_{12} = 0$, $A_1 = A_2 = 1$. Damit erhalten wir aus (8)

$$b_{12} = 0, \quad B_{12} = 0, \quad B_2 = b_2, \quad B_1 = b_1, \quad b_0 = 0.$$

Lösungen sind somit

$$H(x_1, x_2) = b_1 x_1 + b_2 x_2, \tag{9}$$

$$G^b(x_1, x_2) = B_0 + b_1 x_1 + b_2 x_2. \tag{10}$$

Um auf $g_t^{\mathfrak{A}}(x_1, \ldots, x_t)$ zu schließen, stellen wir $g_t^{\mathfrak{A}}$ wieder in antivalenter Normalform (3) dar:

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = a_0 + \sum_{1 \leqq i \leqq t} a_i x_i + \sum_{1 \leqq i < j \leqq t} a_{ij} x_i x_j + \ldots + a_{1 \ldots t} x_1 \ldots x_t.$$

Mit $F_6(x, x) = x + x = 0$ und (5) gilt

$$H(x_1, x_2) = g_t^{\mathfrak{A}}(x_1, x_2, 0, \ldots, 0). \tag{11}$$

Wegen $H(0, 0) = 0$ (nach (9)) ergibt sich aus (11), (9), (3): $a_0 = 0$.

Wir nehmen nun an, es gäbe einen Koeffizienten $a_{i_1 \ldots i_k} = 1$ mit $k \geqq 2$; k sei minimal. O.B.d.A. sei $a_{12 \ldots k} = 1$. Es gilt dann für die spezielle (partielle) Belegung $b = [x_1, x_2, \underbrace{1, \ldots, 1}_{k-l}, 0, \ldots, 0]$ die Beziehung $g_t^{\mathfrak{A}}(b) = c_1 x_1 + c_2 x_2 + c_0 + x_1 x_2$ mit $c_0, c_1, c_2 \in \{0, 1\}$ im Widerspruch zu (10), (4). Damit hat $g_t^{\mathfrak{A}}$ die Form

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = \sum_{1 \leqq i \leqq t} a_i x_i \quad \text{mit} \quad a_1, \ldots, a_t \in \{0, 1\}. \tag{12}$$

Da man unmittelbar überprüft, daß jeder Automat $\mathfrak{A}$, für den $g_t^{\mathfrak{A}}$ die Bedingung (12) erfüllt, $+$-superponierbar ist (d.h. (1) genügt), ist gezeigt:

Satz 3. *Ein binärer Automat $\mathfrak{A}$ ist $+$-superponierbar genau dann, wenn es für jedes $t \geqq 1$ Koeffizienten $a_1^{(t)}, \ldots, a_t^{(t)} \in \{0, 1\}$ so gibt, daß stets gilt:*

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = \sum_{i=1}^{t} a_i^{(t)} x_i.$$

Wir betrachten jetzt die Disjunktion (F_{14} in Tab. 1). Es gilt

$$F_{14}(x_1, x_2) = x_1 \vee x_2 = x_1 + x_2 + x_1 \cdot x_2;$$
$$A_0 = 0, \quad A_1 = A_2 = A_{12} = 1.$$

Aus (8) ergeben sich für $G(x_1, x_2)$ die 5 Lösungen G_1, G_2, G_3, G_4, G_5:

$$G_1(x_1, x_2) = 0, \quad G_2(x_1, x_2) = 1,$$

$$G_3(x_1, x_2) = x_1, \quad G_4(x_1, x_2) = x_2,$$

$$G_5(x_1, x_2) = x_1 + x_2 + x_1 x_2 \tag{13}$$

und $H=G$. Um auf $g_t^{\mathfrak{A}}(x_1, \ldots, x_t)$ zu schließen, gehen wir wieder von der antivalenten Normalform (3) aus.

Fall 1. $a_0=1$. — Wir nehmen an, es gäbe einen von a_0 verschiedenen nichtverschwindenden Koeffizienten $a_{i_1 \ldots i_k}$, $k \geqq 1$; o.B.d.A. sei k minimal, $a_{1 \ldots k}=1$. Für $k=1$ ergibt sich $g_t^{\mathfrak{A}}(x_1, 0, \ldots, 0)=1+x_1$ und für $k \geqq 2$: $g_t^{\mathfrak{A}}(x_1, x_2, 0, \ldots, 0)=1+x_1x_2$ im Widerspruch zu (13). Im Fall $a_0=1$ verschwinden also alle anderen Koeffizienten.

Fall 2. $a_0=0$. — Es sei o.B.d.A. $a_1=\ldots=a_k=1$, $a_{k+1}=\ldots=a_t=0$, $0 \leqq k \leqq t$. Wir zeigen zunächst:

$$a_{i_1 \ldots i_l}=0, \quad \text{falls} \quad i_l>k \quad (l \geqq 2). \tag{14.1}$$

Wir nehmen, (14.1) gilt nicht und betrachten einen Koeffizienten $a_{i_1 \ldots i_l}$ mit $a_{i_1 \ldots i_l}=1$, $i_l>k$, $l \geqq 2$, l minimal. O.B.d.A. sei $a_{m+1 \ldots m+l}=1$, $l \geqq 2$, $m+l>k$, l minimal. Dann gilt. $g_t^{\mathfrak{A}}(0, \ldots, 0, x_{m+1}, 1, \ldots, 1, x_{m+l}, 0, \ldots, 0)=C_1x_{m+1}+x_{m+1}x_{m+l}+C_2$ mit $C_1, C_2 \in \{0, 1\}$ im Widerspruch zu (13). Damit ist (14.1) nachgewiesen; $g_t^{\mathfrak{A}}$ hängt von den Variablen $x_{k+1}, \ldots, x_t$ nicht ab.

Wir zeigen nun:

$$a_{i_1 \ldots i_l}=1, \quad \text{falls} \quad i_l \leqq k \quad (l \geqq 2). \tag{14.2}$$

Für $k<2$ ist nichts zu zeigen. Es sei jetzt $k \geqq 2$. Wir nehmen an, (14.2) gilt nicht und betrachten einen Koeffizienten $a_{i_1 \ldots i_l}$ mit $l \geqq 2$, $i_l \leqq k$, $a_{i_1 \ldots i_l}=0$, l minimal. O.B.d.A. sei $a_{1 \ldots l}=0$, $2 \leqq l \leqq k$, l minimal. Dann ist im Fall $l=2$ $g_t^{\mathfrak{A}}(x_1, x_2, 0, \ldots, 0)= =x_1+x_2$ im Widerspruch zu (13). Im Fall $l>2$ gilt

$$g_t^{\mathfrak{A}}(x_1, x_2, \underbrace{1, \ldots, 1}_{l-2}, 0, \ldots, 0)=$$

$$=\sum_{i=1}^{l-2}\binom{l-2}{i}+(x_1+x_2)\sum_{i=0}^{l-2}\binom{l-2}{i}+x_1x_2\sum_{i=0}^{l-3}\binom{l-2}{i}=1+x_1x_2$$

wegen $\sum\limits_{i=0}^{l}\binom{l}{i}=2^l=0 \pmod{2}$. Mit diesem Widerspruch zu (13) ist (14.2) verifiziert; Koeffizienten, deren sämtliche Indizes zwischen 1 und k liegen, verschwinden nicht.

Gilt also nicht $g_t^{\mathfrak{A}}=1$, so läßt sich $g_t^{\mathfrak{A}}$ allgemein schreiben in der Form

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t)=\sum_{i \in I} x_i+\sum_{\substack{1 \leqq i<j \leqq t \\ i, j \in I}} x_ix_j+\ldots+\prod_{i \in I} x_i, \tag{15}$$

wobei $I \subseteqq \{1, \ldots, t\}$ ist. Gilt (15), so ist

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t)=\begin{cases} 1, & \text{falls es ein} \quad i \in I \quad \text{mit} \quad x_i=1 \quad \text{gibt,} \\ 0 & \text{sonst;} \end{cases}$$

d.h., (15) läßt sich auch schreiben in der Form

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t)=\bigvee_{i=I} x_i. \tag{16}$$

Man prüft sofort nach, daß die konstanten Funktionen mit dem Wert 1 und die durch (16) festgelegten Funktionen tatsächlich $\vee$-superponierbar sind. Damit haben wir gezeigt:

Satz 4. *Ein binärer Automat $\mathfrak{A}$ ist $\vee$-superponierbar genau dann, wenn für jedes $t \geqq 1$ gilt: $g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = 1$ oder es gibt Koeffizienten $a_1^{(t)}, \ldots, a_t^{(t)} \in \{0, 1\}$ so, daß gilt:*

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = \bigvee_{i=1}^{t} a_i^{(t)} x_i.$$

Mit der Beweismethode zu Satz 3 bzw. Satz 4 zeigt man weiter:

Satz 5. *Ein binärer Automat $\mathfrak{A}$ ist*
a) *F_7-superponierbar ($\equiv$-superponierbar)*
b) *F_8-superponierbar ($\wedge$-superponierbar)*
c) *F_9-superponierbar*
d) *F_{10}-superponierbar*
e) *F_{11}-superponierbar ($\rightarrow$-superponierbar)*
f) *F_{12}-superponierbar*
g) *F_{13}-superponierbar*
h) *F_{15}-superponierbar,*
genau dann, wenn für jedes $t \geqq 1$ gilt:

Für die Koeffizienten $a_0, a_1, \ldots, a_t, a_{12}, \ldots, a_{1\ldots t}$ in der antivalenten Normalform von $g_t^{\mathfrak{A}}$,

$$g_t^{\mathfrak{A}}(x_1, \ldots, x_t) = a_0 + \sum_{i=1}^{t} a_i x_i + \sum_{1 \leqq i_1 < i_2 \leqq t} a_{i_1 i_2} x_{i_1} x_{i_2} + \ldots + a_{1\ldots t} x_1 \ldots x_t,$$

gilt:
a) $a_0 + \sum_{i=1}^{t} a_i = 1$ *und alle Koeffizienten mit mehr als einem Index verschwinden*
b) *Höchstens einer der Koeffizienten verschwindet nicht*
c) *Es verschwindet genau ein Koeffizient nicht, dies ist einer der Koeffizienten $a_1, \ldots, a_t$ (d.h. $\mathfrak{A} \in \mathscr{A}_{\text{Ausw}}$)*
d) *Es verschwindet höchstens ein Koeffizient nicht, dies ist dann einer der Koeffizienten $a_1, \ldots, a_t$*
e) *Es verschwindet genau ein Koeffizient nicht, dies ist einer der Koeffizienten $a_1, \ldots, a_t, a_0$*
f) *wie* d)
g) *wie* e)
h) *wie* c).

Nennen wir einen binären Automaten *wesentlich,* wenn es ein $t \geqq 2$ so gibt, daß die Funktion $g_t^{\mathfrak{A}}(x_1, \ldots, x_t)$ von mindestens 2 Variablen echt abhängt, so gilt:

Satz 6.
1. *Es gibt keine wesentlichen binären Automaten, die F_9-, F_{10}-, F_{11}-, F_{12}-, F_{13}-oder F_{15}-superponierbar sind.*
2. *Ein wesentlicher binärer Automat $\mathfrak{A}$ ist*
   a) *$+$-superponierbar (F_6)*
   b) *$\equiv$-superponierbar (F_7)*
   c) *$\wedge$-superponierbar (F_8) bzw.*
   d) *$\vee$-superponierbar (F_{14})*

genau dann, wenn es für jedes $t \geqq 1$ eine Menge $I_t \subseteqq \{1, \ldots, t\}$ so gibt, daß

a) $g_t^{\mathfrak{A}}(x_1, ..., x_t) = \sum_{i \in I_t} x_i$

b) $g_t^{\mathfrak{A}}(x_1, ..., x_t) = \equiv_{i \in I_t} x_i$

c) $g_t^{\mathfrak{A}}(x_1, ..., x_t) = \bigwedge_{i \in I_t} x_i$ *oder* $g_t^{\mathfrak{A}}(x_1, ..., x_t) = 0$ *bzw.*

d) $g_t^{\mathfrak{A}}(x_1, ..., x_t) = \bigvee_{i \in I_t} x_i$ *oder* $g_t^{\mathfrak{A}}(x_1, ..., x_t) = 1$

gilt (*vgl. Tab.* 1); *dabei ist* $\sum_{i \in \emptyset} x_i = \bigvee_{i \in \emptyset} x_i = 0$, $\equiv_{i \in \emptyset} x_i = \bigwedge_{i \in \emptyset} x_i = 1$.

Die im Satz 6.2 charakterisierten wesentlichen binären Automaten werden in [3, 4] explizit zustandsabhängig charakterisiert.

Kurzfassung

Ausgehend vom Superpositionsprinzip für lineare Automaten mit eindimensionalem Input und Output über GF(2) wird in der vorliegenden Arbeit dieses Prinzip von der Operation + (Addition modulo 2, Antivalenz) auf andere Operationen (Boolesche Funktionen) übertragen. Für jede zweistellige Boolesche Funktion wird die Klasse aller Automaten charakterisiert, die dem Superpositionsprinzip bzgl. dieser Booleschen Funktion genügen.

Generalized Superposition by Binary Automata

In this paper the superposition principle for one-dimensional linear automata over GF(2) is extended from the operation + (addition mod. 2) to other operations (Boolean functions). For every Boolean function of two variables is characterized the class of all automata, for which hold the superposition principle with respect to this Boolean function.

Обобщенный принцип суперпозиции у бинарных автоматов

Исходя с принципа суперпозиции для линейных автоматов с одномерным входом и выходом над полем $GF(2)$ (сложение по модулю 2, антивалентность) обобщается этот принцип на другие операции (булевы функции). Для каждой двухместных булевых функций характеризуется класс всех автоматов, подчиняющихся этому принципу относительно данной булевой функций.

ZENTRALINSTITUT FÜR KYBERNETIK
UND INFORMATIONSPROZESSE DER ADW
DDR-1199 BERLIN-ADLERSHOF
RUDOWER CHAUSSEE 5

Literatur

[1] GILL. A., *Linear sequential circuits*, McGraw Hill, New York, 1966.
[2] REISCHER, C., D. A. SIMOVICI, Linear Boolean automata, *Wiss. Z. Techn. Hochsch. Ilmenau*, v. 17, 1971, pp. 83—96.
[3] GÖSSEL, M., Binäre $+$- und $\equiv$- superponierbare Automaten, *Z. elektr. Inform.- u. Energietechnik*, Leipzig, v. 6, 1976, pp. 225—236.
[4] GÖSSEL, M., Binäre $\vee$- und $\wedge$-superponierbare Automaten, *Z. elektr. Inform.- u. Energietechnik*, Leipzig, v. 6, 1976, pp. 325—330.
[5] Жегалкин, И. И., Арифметизация символической логики. *Мат. сб.* v. 35, 1928, 3/4.

(Eingegangen am 7. August 1974)