Josef Metelka

Vektorielles Modell der endlichen Booleschen Algebren

Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica-Physica-Chemica, Vol. 7 (1966), No. 1, 33--43

Persistent URL: http://dml.cz/dmlcz/119857

1966 — ACTA UNIVERSITATIS PALACKIANAE OLOMUCENSIS.
FACULTAS RERUM NATURALIUM. TOM 21.

Katedra algebry a geometrie přírodovědecké fakulty
Vedoucí katedry: prof. RNDr. Josef Metelka

VEKTORIELLES MODELL DER ENDLICHEN BOOLESCHEN ALGEBREN

JOSEF METELKA

(Eingelangt am 13. September 1965)

Man konstruiert ein vektorielles Modell für die endlichen Booleschen Algebren. Es zeigt sich, daß bei der Benützung des Modells manche Betrachtungen sehr einfach aussehen. Das gilt z. B. von der Homomorphie (No. 4) und besonders von der Booleschen Abhängigkeit, welche in No. 5 definiert wird. Man findet ein Kriterium für die Abhängigkeit oder Unabhängigkeit gegebener Elemente einer Booleschen Algebra (Satz 5.3.), sowie auch ein Mittel für das Aussuchen aller Bindungsfunktionen. Der angeschlossene Begriff der erzwungenen Abhängigkeit findet seine Anwendung in der Aussagenlogik mit vorgeschriebenen logischen Bedingungen (No.6).

1. Es sei $M_0 = \{\alpha, \beta\}$ eine Menge mit zwei Elementen, für welche die Operationen

$$V_0\colon\ \alpha + \alpha = \alpha,\ \alpha + \beta = \beta + \alpha = \beta,\ \beta + \beta = \beta; \qquad (1.1)$$
$$S_0\colon\ \alpha \,.\, \alpha = \alpha,\ \alpha \,.\, \beta = \beta \,.\, \alpha = \alpha,\ \beta \,.\, \beta = \beta$$

definiert sind. Die Menge M_0 ist also eine Boolesche Algebra (weiter nur B-Algebra), wie man sofort sieht.

Definition 1.1. *Ein Element des m-fachen kartesischen Produktes* $M_0 \times M_0 \times \ldots \times M_0$ *heisst ein Vektor über* M_0 *und es wird wie* $\mathrm{a} = (a_1, \ldots, a_m)$, $a_i \in M_0$, $1 \leqq i \leqq m$ *bezeichnet. Die Menge* $\mathfrak{M}_m$ *aller Vektoren über* M_0 *heisst der vektorielle m-dimensionale Raum über* M_0.

Wir definieren für zwei Vektoren $\mathrm{a} = (a_1, \ldots a_m)$, $\mathrm{b} = (b_1, \ldots, b_m)$ wie üblich die Gleichheitsrelation

$$G\colon\ \mathrm{a} = \mathrm{b} \Leftrightarrow a_i = b_i,\ 1 \leqq i \leqq m. \qquad (1.2)$$

Dann enthält die Menge $\mathfrak{M}_m$ genau 2^m verschiedene Vektoren.

Mit Hilfe von (1.1) und (1.2) definieren wir weiter in $\mathfrak{M}_m$ zwei binäre Operationen

$$V\colon\ \mathrm{a} + \mathrm{b} = \mathrm{c} \Leftrightarrow a_i + b_i = c_i,\ 1 \leqq i \leqq m; \qquad (1.3)$$
$$S\colon\ \mathrm{a} \,.\, \mathrm{b} = \mathrm{d} \Leftrightarrow a_i b_i = d_i,\ 1 \leqq i \leqq m,$$

wo $\mathrm{c} \in \mathfrak{M}_m$, $\mathrm{d} \in \mathfrak{M}_m$ und $\mathrm{c} = (c_1, \ldots, c_m)$, $\mathrm{d} = (d_1, \ldots, d_m)$, $c_i, d_i \in M_0$.

Offenbar ist jetzt $\mathfrak{M}_m$ ein distributiver Verband. Wenn wir weiter die vorigen Operationen zur Definition der Teilanordnung in $\mathfrak{M}_m$ in dem Sinne benützen, dass wir

$$\mathfrak{a} \leqq \mathfrak{b} \Leftrightarrow \mathfrak{a} + \mathfrak{b} = \mathfrak{b} \tag{1.4}$$

legen, so existiert in $\mathfrak{M}_m$ *das kleinste Element* O und *das grösste Element* I

$$\mathrm{O} = (\alpha, \ldots, \alpha), \quad \mathrm{I} = (\beta, \ldots, \beta); \tag{1.5}$$

jedem Vektor $\mathfrak{a} = (a_1, \ldots, a_m)$ ist eindeutig *ein Komplement* $\mathfrak{a}' = (a_1', \ldots, a_m')$ zugeordnet, wo $a_i' = \alpha$, wenn $a_i = \beta$, und $a_i' = \beta$, wenn $a_i = \alpha$. Es gilt

$$\mathfrak{a} + \mathfrak{a}' = \mathrm{I}, \quad \mathfrak{a} \,.\, \mathfrak{a}' = \mathrm{O}. \tag{1.6}$$

Der Vektorraum $\mathfrak{M}_m$ ist also eine B-Algebra mit 2^m Elementen.

Anmerkung 1. Man könnte auch die dualle Teilanordnung zu (1.4) durch die Definition $\mathfrak{a} \leqq \mathfrak{b} \Leftrightarrow \mathfrak{a} + \mathfrak{b} = \mathfrak{a}$ einführen. Auch in diesem Falle entsteht eine B-Algebra, die zu der vorigen isomorph ist, das Element $(\alpha, \ldots, \alpha)$ wird jetzt das grösste und $(\beta, \ldots, \beta)$ das kleinste Element von $\mathfrak{M}_m$. Wir werden weiter nur die Relation (1.4) und also auch die Zuordnung (1.5) benützen.

Anmerkung 2. Wir können auch eine neue Operation, die wir *Adition* nennen wollen, einführen

$$A\colon\ a \dot{+} b = a \,.\, b' + a' \,.\, b, \tag{1.7}$$

d. h. für $\mathfrak{a} = (a_1, \ldots, a_m)$, $\mathfrak{b} = (b_1, \ldots, b_m)$, $\mathfrak{c} = (c_1, \ldots, c_m)$ $\mathfrak{a} \dot{+} \mathfrak{b} = \mathfrak{c}$, wo c_i aus a_i und b_i, $1 \leqq i \leqq m$, nach den Regeln gerechnet wird

$$\alpha \dot{+} \alpha = \alpha, \quad \alpha \dot{+} \beta = \beta \dot{+} \alpha = \beta, \quad \beta \dot{+} \beta = \alpha. \tag{1.7a}$$

Es ist klar, dass die so eingeführte Adition mit der gewöhnlicher Adition nach dem Modul 2 isomorph ist. Weil noch die Operation S die Eigenschaften der Multiplikation hat und A und S distributiv sind, was man leicht bestätigt, ist der Vektorraum $\mathfrak{M}_m$ mit Rücksicht auf die Operationen A und S *ein kommutativer, idempotenter Ring von der Charakteristik zwei.* O ist das neutrale Element für die Adition A und I das neutrale Element für die Multiplikation S (Vergl. [3], S. 193).

2. Definition 2.1. *Die Multiplikation des Vektors $a \in \mathfrak{M}_m$ mit einem Elemente $\varepsilon \in M_0$ wird durch die Relationen*

$$M\colon\ \varepsilon \,.\, \mathfrak{a} = \mathfrak{a} \,.\, \varepsilon = \begin{cases} \mathrm{O}, \text{wenn } \varepsilon = \alpha \\ \mathfrak{a}, \text{ wenn } \varepsilon = \beta \end{cases} \tag{2.1}$$

gegeben.

Für die Multiplikation (2.1) gelten offensichtlich die folgenden Gesetze

$$\varepsilon(\mathfrak{a} + \mathfrak{b}) = \varepsilon\mathfrak{a} + \varepsilon\mathfrak{b}, \quad (\varepsilon_1 + \varepsilon_2)\,\mathfrak{a} = \varepsilon_1\mathfrak{a} + \varepsilon_2\mathfrak{a},$$
$$\varepsilon(\mathfrak{a}\mathfrak{b}) = (\varepsilon\mathfrak{a})\,\mathfrak{b} = (\varepsilon\mathfrak{a})\,\mathfrak{b} = \mathfrak{a}(\varepsilon\mathfrak{b}) = (\varepsilon\mathfrak{a}) \,.\, (\varepsilon\mathfrak{b}),$$
$$(\varepsilon_1\varepsilon_2)\,\mathfrak{a} = (\varepsilon_2\varepsilon_1)\,\mathfrak{a} = \varepsilon_1(\varepsilon_2\mathfrak{a}) = \varepsilon_2(\varepsilon_1\mathfrak{a}) \text{ usw.}$$

Diese Gesetze können leicht durch Induktion für beliebige Anzahl von Vektoren, sowie auch für beliebige Anzahl der Elemente aus M_0 verallgemeinert werden.

Definition 2.2. *Als lineare Kombination von Vektoren* $\mathfrak{a}^{(j)} \in \mathfrak{M}_m$ *über* M_0, $1 \leqq j \leqq s$, *bezeichnen wir den Vektor*

$$\mathfrak{c} = \varepsilon_1 \mathfrak{a}^{(1)} + \ldots + \varepsilon_s \mathfrak{a}^{(s)} = \sum_{i=1}^{m} \varepsilon_i \mathfrak{a}^{(j)}, \qquad \varepsilon_j \in M_0.$$

Speziell kann jeder Vektor $\mathfrak{a} = (a_1, \ldots, a_m) \in \mathfrak{M}_m$ in der Form

$$\mathfrak{a} = \sum_{j=1}^{m} a_j \mathfrak{e}^{(j)} \tag{2.2}$$

als lineare Kombination der *Basisvektoren in* $\mathfrak{M}_m$

$$\begin{aligned} \mathfrak{e}^{(1)} &= (\beta, \alpha, \ldots, \alpha) \\ &\ldots\ldots\ldots\ldots \\ \mathfrak{e}^{(m)} &= (\alpha, \alpha, \ldots, \beta) \end{aligned} \tag{2.3}$$

ausgedrückt werden. Die Menge $\{\mathfrak{e}^{(1)}, \ldots, \mathfrak{e}^{(m)}\}$, wollen wir *Basis in* $\mathfrak{M}_m$ nennen und mit E bezeichnen. Die Elemente $a_1, \ldots, a_m \in M_0$ sind dann *die Koordinaten des Vektors* a *in der Basis* E.

Allgemeiner möchten wir als Basis in $\mathfrak{M}_m$ jede Menge von r Vektoren $\mathfrak{f}^{(k)} \in \mathfrak{M}_m$, $1 \leqq k \leqq r$, bezeichnen, wenn es für $\mathfrak{f}^{(k)}$ gilt

$$\begin{aligned} &\text{a)}\ \mathfrak{f}^{(k)} \neq \mathfrak{O},\ 1 \leqq k \leqq r; \\ &\text{b)}\ \mathfrak{f}^{(j)} \cdot \mathfrak{f}^{(k)} = \mathfrak{O},\ 1 \leqq j < k \leqq r; \\ &\text{c)}\ \mathfrak{a} = \sum_{k=1}^{r} \varepsilon_k \mathfrak{f}^{(k)},\ \varepsilon_k \in M_0, \text{ für jeden vektor } \mathfrak{a} \in \mathfrak{M}_m. \end{aligned} \tag{2.4}$$

Die Eigenschaften (2.4) gehören offenbar der Basis E zu. Es gilt aber auch umgekehrt.

Satz 2.1. *Die Basis* E *mit den Vektoren* (2.3) *ist — von der Reihenfolge der Vektoren* $\mathfrak{e}^{(j)}$ *abgesehen — die einzige Basis in* $\mathfrak{M}_m$.

Beweis: Sei $\mathrm{H} = \{\mathfrak{f}^{(1)}, \ldots, \mathfrak{f}^{(r)}\}$ eine Basis in m-dimensionalem Vektorraum $\mathfrak{M}_m$. Wir schreiben die Koordinaten der Vektoren $\mathfrak{f}^{(k)}$ in der Basis E als Elemente einer Matrix A von r Zeilen und m Spalten und bezeichnen mit s die Gesamtanzahl der Elemente β in der Matrix A. Mit Rücksicht auf die Eigenschaft (2.4) a) muss die Ungleichung $s \geqq r$ gelten. Wegen der Eigenschaft (2.4) b) befindet sich höchstens ein Element β in jeder Spalte der Matrix A, also $m \geqq s$. Endlich muss es $r \geqq m$ sein, denn anders könnten wir nicht die 2^m verschiedenen Vektoren des Raumes $\mathfrak{M}_m$ in der Form der Kombinationen $\sum_{k=1}^{r} \varepsilon_k \mathfrak{f}^{(k)}$ bekommen. Es ist also $m = s = r$, die Matrix A ist quadratisch und hat genau ein Element β in jeder Zeile und Spalte. Die Basis H ist also bis auf die Reihenfolge ihrer Vektoren mit der Basis E identisch.

3. Sei B_m eine abstrakte endliche B-algebra mit 2^m Elementen. Es ist gut bekannt, dass jede andere B-Algebra gleicher Elementenanzahl mit B_m isomorph ist. Wir können deswegen den Vektorraum $\mathfrak{M}_m$ als Modell für jede endliche B-Algebra annehmen. Obwohl auch die Fragen der isomorphen Zuordnung schon längst bekannt sind, wollen wir nun hier von ihnen das angehender studieren, was wir später brauchen werden.

Definition 3.1. *Als Atome bezeichnen wir die Elemente* x_i, $1 \leqq i \leqq r$, *der* B-*Algebra* B_m, *mit den Eigenschaften*

a) $x_i \neq \mathrm{O}$, $1 \leqq i \leqq r$;

b) $x_i \cap y$ *ist gleich entweder* O *oder* x_i *für jedes Element* $y \in B_m$ *und für alle* x_i; (3.1)

c) $x_1 \cup \ldots \cup x_r = \mathrm{I}$,

wo O *das kleinste und* I *das grösste Element in* B_m *bedeutet.*

Anmerkung: Die Eigenschaften (3.1) sind charakteristisch für die Menge der Atome sogar in jedem komplementären modulären Verbande (Vergl. [2], Kap. § 1).

Satz 3.1. *Es existieren genau* 2. $m!$ *isomorphe Abbildungen von zwei* B-*Algebren mit* 2^m *Elementen aufeinander.*

Beweis: Wir wollen zuerst als bekannt annehmen, dass es immer mindestens eine isomorphe Abbildung der abstrakten B-Algebra B_m auf jede andere B-Algebra mit derselben Elementenanzahl gibt. Sei σ solche Abbildung von B_m auf den Vektorraum $\mathfrak{M}_m$, wo

$$\mathrm{a} = \sigma(y),\ \mathrm{b} = \sigma(z),\ \mathrm{a} + \mathrm{b} = \sigma(y \cup z),\ \mathrm{ab} = \sigma(y \cap z),\ y, z \in B_m.$$

Dann gilt auch $\mathrm{O} = \sigma(\mathrm{O})$, $\mathrm{I} = \sigma(\mathrm{I})$. Sind x_i, $1 \leqq i \leqq r$, die Atome in B_m, so haben wir weiter $\mathrm{f}^{(i)} = \sigma(x_i)$. Aus (3.1) folgt a) $\mathrm{f}^{(i)} \neq \mathrm{O}$; b) $\mathrm{f}^{(i)} \,.\, \mathrm{f}^{(j)} = \mathrm{O}$, $1 \leqq i < j \leqq r$; c) $\sum_{i=1}^{s} \mathrm{f}^{(i)} = \mathrm{I}$ und weiter für beliebigen Vektor $\mathrm{a} \in \mathfrak{M}_m$

$$\mathrm{a} = \mathrm{a} \,.\, \mathrm{I} = \mathrm{a} \sum_{i=1}^{r} \mathrm{f}^{(i)} = \sum_{i=1}^{r} \mathrm{a} \,.\, \mathrm{f}^{(i)} = \sum_{i=1}^{r} \varepsilon_i \mathrm{f}^{(i)},\ \varepsilon_i \in M_0,$$

denn es ist nach (3.1) b) entweder $\mathrm{a} \,.\, \mathrm{f}^{(i)} = \alpha \mathrm{f}^{(i)}$ oder $\mathrm{a} \,.\, \mathrm{f}^{(i)} = \beta \mathrm{f}^{(i)}$. Die Vektoren $\mathrm{f}^{(j)}$ bilden also eine Basis in $\mathfrak{M}_m$ nach (2.4) und sind (von der Reihenfolge abgesehen) mit den Vektoren $\mathrm{e}^{(j)}$, $1 \leqq j \leqq m$, identisch. Es gibt also mindestens $m!$ verschiedene isomorphe Abbildungen von Typus σ. Zu jeder von diesen Abbildungen σ existiert aber eine duale Abbildung ϱ, in der $\mathrm{a} + \mathrm{b} = \varrho(y \cap z)$, $\mathrm{ab} = \varrho(y \cup z)$, was zu der Gesamtanzahl 2. $m!$ führt. Dass es nicht mehr als 2. $m!$ Isomorphismen geben kann, folgt aus der Eindeutigkeit des Ausdruckes der Vektoren in der Basis E.

4. Definition 4.1. *Es sei* $K = \{1, \ldots, m\}$ *die Menge der* m *ersten natürlichen Zahlen,* L *eine beliebige (eventuell leere) Untermenge von* K, $\overline{L}$ *die zu* L *komplementäre Untermenge in* K, *d. i.* $L \cup \overline{L} = K$, $L \cap \overline{L} = 0$. *Ein zu der Untermenge* L *gehörender Unterraum* $\mathfrak{M}(L)$ *in* $\mathfrak{M}_m$ *heisst die Menge der Vektoren* $\mathrm{a} \in \mathfrak{M}_m$, $\mathrm{a} = \sum_{i=1}^{r} a_j \mathrm{e}^{(j)}$, *für welche* $a_j = \alpha$, *wenn* $j \in \overline{L}$, *während die anderen Koordinaten* a_i, $i \in L$ *ganz beliebige Elemente aus* M_0 *sind.*

Wenn $L = K$, also $\overline{L} = 0$, ist $\mathfrak{M}(L) = \mathfrak{M}_m$, für $L = 0$ ist $\mathfrak{M}(L) = \{O\}$. In diesen zwei Fällen wollen wir die entsprechenden Unterräume *unecht* in $\mathfrak{M}_m$ nennen. In allen übrigen Fällen handelt es sich um *echte* Unterräume $\mathfrak{M}(L)$ in $\mathfrak{M}_m$.

Hat L r Elemente, $0 < r < m$, so ist es offenbar möglich den Unterraum $\mathfrak{M}(L)$ auf den Vektorraum $\mathfrak{M}_r$ mit 2^r Vektoren isomorph abzubilden. Jeder echte Unterraum in $\mathfrak{M}_m$ ist also eine B-Unteralgebra in $\mathfrak{M}_m$. Das gilt auch für $\mathfrak{M}(K) = \mathfrak{M}_m$ und wir werden durch Extension auch den einzigen Vektor O des Unterraumes $\mathfrak{M}(O)$ für eine B-Unteralgebra in $\mathfrak{M}_m$ halten.

Anmerkung: Die Unterräume $\mathfrak{M}(L)$ von der Definition 4.1 kann man mit mehr Bestimmtheit als *untere* Unterräume in $\mathfrak{M}_m$ bezeichnen. Dual existieren auch *obere* Unterräume, deren Vektoren $a = \sum_{j=1}^{m} a_j e^{(j)}$ alle ihre Koordinaten $a_j = \beta$ haben für $j \in \overline{L}$, während die übrigen Koordinaten a_i, $i \in L$, ganz beliebige Elemente aus M_0 bleiben. Weiter werden wir als Unterräume nur die unteren Unterräume benützen.

Definition 4.2. *Ein (unteres) Ideal der B-Algebra B_m ist eine Untermenge R von Elementen aus B_m, für welche die zwei Bedingungen gelten*

$$\begin{aligned} &\text{a)}\ a \in R,\ b \in R \to a \cup b \in R; \\ &\text{b)}\ a \in R,\ t \in B_m \to a \cap t \in R. \end{aligned} \tag{4.1}$$

Anmerkung 2: Dual kann man das *obere* Ideal in B_m definieren. Weiter werden wir als Ideal immer nur unteres Ideal verstehen. Als Unterlage zur Definition der Ideale braucht man nicht bis zu den B-Algebren greifen; das untere sowie auch das obere Ideal kann in jedem Verbande definiert werden.

Satz 4.1. *Alle Unterräume $\mathfrak{M}(L)$ in $\mathfrak{M}_m$ und nur diese Untermengen von $\mathfrak{M}_m$ sind Ideale in $\mathfrak{M}_m$. Jedes Ideal in $\mathfrak{M}_m$ ist durch sein grösstes Element eindeutig bestimmt.*

Beweis: Es folgt unmittelbar aus der Definition, dass jeder Unterraum $\mathfrak{M}(L)$ in $\mathfrak{M}_m$ ein Ideal in $\mathfrak{M}_m$ ist. Umgekehrt, es sei R ein Ideal in $\mathfrak{M}_m$ und u sein grösster Vektor. Ist $u = I$, so ist nach (4.1) b) $R = \mathfrak{M}_m$. Wir können also $u \neq I$ und $u = \sum_{j=1}^{m} u_j e^{(j)}$ annehmen, wo nicht alle Koordinaten $u_j = \beta$. Es sei L die Menge der Indexe j, für welche $u_j = \beta$. Jetzt ist nach der Definition 4.1 ein Unterraum $\mathfrak{M}(L)$ definiert, worin wir einen beliebigen Vektor a wählen. Es gilt $a \,.\, u = a$ und anderseits nach (4.1) b) $a \in R$, d. h. $\mathfrak{M}(L) \subset R$. Es sei weiter b ein beliebiger Vektor aus R. Wir setzen voraus, dass in dem Ausdrucke $b = \sum_{j=1}^{m} b_j e^{(j)}$ mindestens eine Koordinate $b_j = \beta$ mit $j \notin L$. In diesem Falle wäre $u + b = c \neq u$ und der Vektor u wäre nicht das grösste Element in R. Die Voraussetzung über b ist also falsch, alle Koordinaten $b_j = \alpha$ für $j \in L$ und $b \in \mathfrak{M}(L)$. Es ist also $R \subset \mathfrak{M}(L)$ und der Satz ist bewiesen.

Wir können zusammenfassen: In der B-Algebra $\mathfrak{M}_m$ mit 2^m Elementen gibt es genau 2^m (untere) Ideale, welche eindeuting den Untermengen der Menge $K = \{1, \ldots, m\}$, sowie auch den einzelnen Elementen $u \in \mathfrak{M}_m$ zugeordnet sind.

Man kann also anstatt $R = \mathfrak{M}(L)$ auch $R = \mathfrak{M}(u)$ schreiben, wo u das grösste Element von R ist. Ganz analoge Behauptungen können wir durch Dualisation auch für die oberen Ideale in $\mathfrak{M}_m$ bekommen.

Anmerkung 3: Wenn man $\mathfrak{M}_m$ als Ring von der Charakteristik zwei mit den Operationen A (1.7) und S (1.3) betrachtet (vergl. Anmerkung 2. von No 1), bestätigt man sofort, dass jedes Ideal $\mathfrak{M}(L)$ auch ein Ideal im gewöhnlichen Sinne im Ringe $\mathfrak{M}_m$ ist. Umgekehrt ist jedes gewöhnliche Ideal $\mathfrak{N}$ von $\mathfrak{M}_m$ auch ein Ideal $\mathfrak{M}(L)$ im Sinne der Definition 4.2. Ist nähmlich $a \in \mathfrak{N}$, $b \in \mathfrak{N}$, so ist es auch $a \,.\, b' \in \mathfrak{N}$ und $b \dotplus a \,.\, b' \in \mathfrak{N}$. Es gilt aber $b \dotplus a \,.\, b' = a + b$, wie man leicht nachprüft. Mit den oberen Idealen stimmt es nicht, denn diese enthalten allgemein nicht das Element O. Für die oberen Ideale müsste man die Operationen A und S dual definieren.

Jetzt wollen wir nur im Kurzen einige weitere gut bekannte Tatsachen von der Theorie der Ideale in den B-Algebren andeuten, welche in dem Vektormodell sehr durchsichtig ausgehen.

Jedes Ideal $\mathfrak{M}(L) \subset \mathfrak{M}_m$ induziert in $\mathfrak{M}_m$ eine *Zerlegung in Klassen (Restklassen mod* $\mathfrak{M}(L)$*)*. Zwei Vektoren $x = \sum_{j=1}^{m} x_j e^{(j)}$, $y = \sum_{j=1}^{m} y_j e^{(j)}$ gehören in dieselbe Klasse, was wir in der Form $x \equiv y$ (mod $\mathfrak{M}(L)$) schreiben, dann und nur dann, wenn $x_j = y_j$ für jeden Index $j \in L$. Die reflexive, symmetrische und transitive Eigenschaft dieser Äquivalenzrelation ist evident; in anderen, nicht vektoriellen Auffassungen ist es nicht so einfach. Wenn die Untermenge $L \subset K\,r$ Elemente enthält, $0 \leqq r \leqq m$, so ist jede Klasse eine B-Algebra mit 2^r Elementen, welche mit dem Ideale $\mathfrak{M}(L)$ isomorph ist. Es gibt insgesammt 2^{m-r} Klassen, denn jede Klasse ist eineindeutig einer Untermenge von L zugeordnet. Daraus folgt auch unmittelbar, dass die Menge der Restklassen mod $\mathfrak{M}(L)$ eine B-Algebra bildet, welche dem Ideale $\mathfrak{M}(\bar{L})$ isomorph ist. Die B-Algebra der Restklassen mod $\mathfrak{M}(L)$ heisst die *Faktor-B-Algebra der B-Algebra* $\mathfrak{M}_m$ *mod* $\mathfrak{M}(L)$ und wird durch $\mathfrak{M}_m/\mathfrak{M}(L)$ bezeichnet.

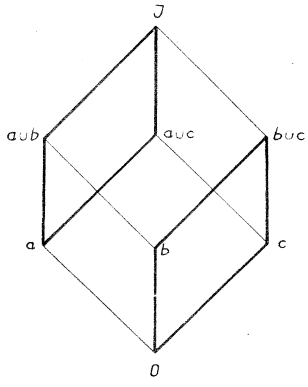

Abb. 1

Jede Restklasse $(X) \in \mathfrak{M}_m/\mathfrak{M}(L)$ kann durch ihren beliebigen Repräsentanten gegeben werden. Es ist jedoch sehr zweckmässig als Repräsentanten das kleinste Element aus (X) zu wählen, d. h. das Element $(X) \cap \mathfrak{M}(\bar{L})$. Dieses Element wollen wir die *Projektion der Klasse* (X) *in den Unterraum* $\mathfrak{M}(\bar{L})$ nennen. Das Ideal $\mathfrak{M}(\bar{L})$ wird dann als *Projektion der Faktor-B-Algebra* $\mathfrak{M}_m/\mathfrak{M}(L)$ *in* $\mathfrak{M}(\bar{L})$ oder auch als *Projektion des Vektorraumes* $\mathfrak{M}_m$ *nach der Richtung* $\mathfrak{M}(L)$ *in* $\mathfrak{M}(\bar{L})$ bezeichnet.

Als Beispiel werden wir die B-Algebra mit 8 Elementen betrachten, deren Hasse-Diagramm in Abb. 1 wiedergegeben ist. Das Vektormodell $\mathfrak{M}_3$ hat acht Vektoren

$$\mathrm{O} = (\alpha, \alpha, \alpha),\ \mathrm{a} = (\beta, \alpha, \alpha),\ \mathrm{b} = (\alpha, \beta, \alpha),\ \mathrm{c} = (\alpha, \alpha, \beta),$$

$$\mathrm{a} + \mathrm{b} = (\beta, \beta, \alpha),\ \mathrm{a} + \mathrm{c} = (\beta, \alpha, \beta),\ \mathrm{b} + \mathrm{c} = (\alpha, \beta, \beta),\ \mathrm{I} = (\beta, \beta, \beta).$$

$K = \{1, 2, 3\}$. Wählen wir $L = \{2, 3\}$, d. h. $\bar{L} = \{1\}$, so ist $\mathfrak{M}(L) = \{\mathrm{O}, \mathrm{b}, \mathrm{c}, \mathrm{b} + \mathrm{c}\}$, $\mathfrak{M}(\bar{L}) = \{\mathrm{O}, \mathrm{a}\}$. Die beiden Restklassen mod $\mathfrak{M}(L)$ sind $\{\mathrm{O}, \mathrm{b}, \mathrm{c}, \mathrm{b} + \mathrm{c}\}$ und $\{\mathrm{a}, \mathrm{a} + \mathrm{b}, \mathrm{a} + \mathrm{c}, \mathrm{I}\}$, ihre Projektionen in $\mathfrak{M}(\bar{L})$ die Elemente O und a. Das Ideal $\mathfrak{M}(\bar{L}) = \{\mathrm{O}, \mathrm{a}\}$ ist die Projektion des Raumes $\mathfrak{M}_3$ nach der Richtung $\{\mathrm{O}, \mathrm{b}, \mathrm{c}, \mathrm{b} + \mathrm{c}\}$ in $\mathfrak{M}(\bar{L})$.

5. **Definition 5.1.** *Es sei $\{a_1, \ldots, a_r\}$ eine Menge von r Elementen aus der abstrakten B-Algebra B_m mit 2^m Elementen. Wir nennen die Elemente $a_1, \ldots, a_r$ B-abhängig, wenn es mindestens eine Boolesche Funktion (weiter B-Funktion) $G(X_1, \ldots, X_r)$ gibt, die nicht dem kleinsten Elemente* O *gleich ist, die aber nach der Einsetzung $G(a_1, \ldots, a_r) = \mathrm{O}$. Die B-Funktionen $G(X_1, \ldots, X_r)$ mit dieser Eigenschaft heissen die B-Bindungsfunktionen für die Menge $\{a_1, \ldots, a_r\}$.*

Man könnte die oben definierte B-Abhängigkeit auch *untere* B-Abhängigkeit nennen und dual noch die *obere* B-Abhängigkeit einführen. Diese Unterscheidung ist jedoch überflüssig, denn man sieht sofort, dass die Elemente, welche *unter* B-abhängig sind, auch durch die *obere* B-Abhängigkeit verbunden sind und umgekehrt. Aus $G(X_1, \ldots, X_r) \neq \mathrm{O}$ und $G(a_1, \ldots, a_r) = \mathrm{O}$ folgt nähmlich unmittelbar $[G(X_1, \ldots, X_r)]' \neq \mathrm{I}$, $[G(a_1, \ldots, a_r)]' = \mathrm{I}$ und umgekehrt.

Jetzt enstehen die natürlichen Probleme die B-Abhängigkeit oder B-Unabhängigkeit der gegebenen Elemente zu erkennen und im positiven Falle alle B-Bindungsfunktionen zu finden. Zur Lösung verwenden wir das Vektormodell, indem wir die B-Algebra B_m mittels einer beliebigen Isomorphie σ auf den Vektorraum $\mathfrak{M}_m$ abbilden.

In dieser Abbildung möchten $\mathrm{a}_i = \sum_{j=1}^{m} a_{ij}\mathrm{e}^{(j)}$ die Bilder der Elemente a_i, $1 \leqq i \leqq r$ sein und A die Matrix von r Zeilen und m Spalten mit den Elementen a_{ij}, d. i. $A = (a_{ij})$.

Definition 5.2. *Als Rang der Matrix A bezeichnen wir die natürliche Zahl h, welche die Anzahl von verschiedenen Spalten der Matrix A angibt.*

Aus der Definition sieht man sofort, dass der Rang weder von der Reihenfolge der Vektoren noch von der Reihenfolge der Koordinaten, d. h. von der gewählten Isomorphie, abhängt. Man kann also h auch als *Rang der Vektormenge* $\{\mathrm{a}_i\}$ *oder der Elemente* $\{a_i\}$ bezeichnen.

Leicht überprüft man auch die folgenden Behauptungen:

(A) Der Rang der Matrix ist $h = 1$ dann und nur dann, wenn in der Menge der Vektoren nur die Vektoren O und I vorkommen. Die Menge $\{a_1, \ldots, a_r\}$ hat den Rang $h = 1$ dann und nur dann, wenn sie keine andere Elemente als nur das grösste und das kleinste enthält.

(B) Ist r die Anzahl der Vektoren a_i, so ist der maximale Rang der Matrix A gleich $h = \min(2^r, m)$. Es ist leicht die Beispiele anzugeben, wo der Rang wirklich den Grenzwert erreicht.

Satz 5.1. *Der Rang der Vektorenmenge* $\{a_i\}$, $1 \leqq i \leq r$, *ändert sich nicht, wenn man der Menge einen Vektor* a_k *anschliesst oder von ihr einen Vektor* a_k *abnimmt (für* $r > 1$*), der sich als B-Funktion der übrigen Vektoren schreiben lässt.*

Beweis: Durch das Anschliessen eines beliebigen Vektors kann der Rang h nur zunehmen, denn die Spalten, welche vorher verschieden waren, können nicht gleich werden. Wir wollen nun annehmen, dass sich in der Menge die Vektoren a_i und a_j befanden, und schliessen die Vektoren a'_i, bzw. $a_i + a_j$, bzw. $a_i a_j$ an. Wenn sich vorher die Spalten mit Indexen s und t glichen, gab es auch $a_{is} = a_{it}$, $a_{js} = a_{jt}$. Dann ist aber nach dem Anschliessen $a'_{is} = a'_{it}$, bzw. $a_{is} + a_{js} = a_{it} + a_{jt}$, bzw. $a_{is} \cdot a_{js} = a_{jt} \cdot a_{jt}$. Die Anzahl der gleichen Spalten wird also nicht kleiner, d. h. der Rang bleibt derselbe wie vorher. Jede B-Funktion $a_k = F(a_1, \ldots, a_r)$ der Vektoren a_i, $1 \leqq i \leq r$, ensteht durch die Operationen der Komplementation, bzw. V, bezw. S (1.3) aus den Vektoren a_i oder aus den Vektoren, welche durch dieselbe Operationen aus a_i konstruiert wurden. Damit ist der Satz bewiesen, was das Anschliessen des Vektors a_k betrifft. Dass sich der Rang auch beim Abnehmen des Vektors a_k nicht ändern kann, ist nur eine Folgerung, denn anders müsste er sich bei der inversen Operation, d. h. bei dem Rückanschliessen des Vektors a_k ändern.

Folgerung: *Der Rang einer Menge von r Vektoren ändert sich nicht, wenn man den Vektor* O *oder* I *anschliesst oder (für* $r > 1$*) abnimmt.*

Die Behauptung ist klar, denn man kann immer die Vektoren O oder I als B-Funktionen der beliebigen Vektoren a_i schreiben.

Satz 5.2. *Es sei* $B_n(X)$, $n = 2^r$, *die B-Algebra aller* 2^n *B-Funktionen von r Unbestimmten* $X_1, \ldots, X_r$. *Der Rang der Menge* $\{X_1, \ldots, X_r\}$ *ist* $h = n = 2^r$.

Beweis: Wir konstruieren ein vektorielles Modell der B-Algebra $B_n(X)$. Der Rang der Menge der Unbestimmten $\{X_1, \ldots, X_r\}$ kann nicht grösser sein als 2^r, denn es in der zugehörigen Matrix überhaupt nicht mehr als $n = 2^r$ Spalten gibt. Schliessen wir jetzt zu der Menge $\{X_1, \ldots, X_r\}$ eine beliebige weitere B-Funktion aus $B_n(X)$ an, so ändert sich der Rang nicht nach dem Satze 5.1. Das bedeutet, dass der Rang der Menge aller 2^n B-Funktionen aus $B_n(X)$ derselbe ist, wie der Rang der Menge $\{X_1, \ldots, X_r\}$. Der Rang der Menge aller B-Funtionen von r Unbestimmten ist aber offenbar nicht kleiner als 2^r, denn es ist leicht eine Matrix von n Spalten anzugeben, welche alle ihre Spalten verschieden hat.

Jetzt können wir schon ein Kriterium für die B-Abhängigkeit oder B-Unabhängigkeit gegebener Menge von Elementen einer B-Algebra aussprechen.

Satz 5.3. *Es sei* B_m *die B-Algebra und* $\{a_1, \ldots, a_r\}$ *eine Menge von Elementen aus* B_m, *welche den Rang h haben. Die Elemente* a_i *sind B-unabhängig dann und nur dann, wenn* $h = 2^r$. *Ist* $h < 2^r$, *so existieren genau* $2^{2^r - h} - 1$ *B-Bindungsfunktionen für die Menge* $\{a_1, \ldots, a_r\}$.

Beweis: Wir konstruieren ein vektorielles Modell der B-Algebra B_m und die Matrix A, welche den Elementen a_i zugehört. Nach der Voraussetzung befinden sich h verschiedene Spalten in A. Betrachten wir weiter die B-Algebra $B_n(X)$, $n = 2^r$, aller 2^n B-Funktionen von r Unbestimmten $X_1, \ldots, X_r$ und konstruieren auch zu ihr ein vektorielles Modell $\mathfrak{M}_n$, so hat die Matrix A, welche zu den Unbestimmten $X_1, \ldots, X_r$ gehört, den Rang $\bar{h} = 2^r$ nach dem Satze 5.2. Das bedeutet, dass man unter den Spalten der Matrix A alle h verschiedenen Spalten der Matrix A und ausserdem möglicherweise noch $2^r - h$

andere Spalten finden kann. Es seien $j_1, \ldots, j_h$ die Indexe der erstgenannten h Spalten in der Mattrix A. Wir wollen die Menge $\{j_1, \ldots, j_h\}$ mit L bezeichnen und mit $\overline{L}$ — ähnlich wie in No 4. — die komplementäre Menge zu L in $K = \{1, \ldots, 2^r\}$. (Für $h = 2^r$ ist $\overline{L}$ leer.) Jetzt konstruieren wir das Ideal $\mathfrak{M}_n(\overline{L}) \subset \mathfrak{M}_n$ (Def. 4. 1.,Satz. 4.1.). Für $h = 2^r$ ist $\mathfrak{M}_n(\overline{L}) = \{O\}$, für $h < 2^r$ hat $\mathfrak{M}_n(\overline{L})$ insgesammt $\nu = 2^{2^r - h}$ Elemente, unter welchen sich natürlich auch der Vektor O befindet. Wir bezeichnen $G_1, \ldots, G_\nu$ die B-Funktionen aus $B_n(X)$, welche den Vektoren aus $\mathfrak{M}_n(\overline{L})$ entsprechen, wobei G_ν dem Vektor O zugeordnet werden soll. Es gilt $G_j(X_1, \ldots, X_r) \neq O$ für $1 \leqq j < \nu$ und anderseits $G_j(a_1, \ldots, a_r) = O$ nach der Konstruktion des Ideals. Für $\nu > 1$, d. h. für $h < 2^r$, sind also die Elemente $a_i \in B_m$ B-abhängig und wir kennen schon $\nu - 1 = 2^{2^r - h} - 1$ B-Bindungsfunktionen für sie. Andere B-Bindungsfunktionen für $\{a_1, \ldots, a_r\}$ können aber nicht existieren, denn jede B-Funktion $G_s(X_1, \ldots, X_r)$, für welche $G_s(a_1, \ldots, a_r) = 0$, bildet sich in $\mathfrak{M}_n$ in einen Vektor g_s ab, der alle Koordinaten mit den indexen $j_1, \ldots, j_h$ gleich α hat, d. h. $g_s \in \mathfrak{M}_n(\overline{L})$.

Aus dem Beweise des Satzes folgt auch ein Hinweis, wie man alle B-Bindungsfunktionen für eine gegebene Menge von Elementen findet.

Folgerung: *In der B-Algebra B_m mit 2^m Elementen kann man höchstens $[\log_2 m]$ B-unabhängige Elemente finden; unter diesen darf weder das kleinste noch das grösste Element vorkommen. Für $m > 1$ wird die angegebene Höchstanzahl wirklich erreicht.*

Beweis: Die ersten zwei Behauptungen sind klar. Die letzte folgt daraus, dass man immer eine Matrix mit $[\log_2 m]$ Zeilen und m verschiedenen Spalten konstruieren kann.

Die vorige Folgerung kann auch so ausgesprochen werden: *Wenn es in einer B-Algebra n B-unabhängige Elemente gibt, so hat die B-Algebra mindestes 2^{2^n} Elemente.*

6. Es sei B_m eine abstrakte B-Algebra und σ ihre homomorphe Abbildung auf die B-Algebra B_n. Dadurch entsteht in B_m eine Klassenzerlegung und auch eine neue Gleichheit, welche von der alten verschieden ist, sofern σ nicht eine Isomorphie ist. Wir schreiben diese Gleichheit $a_1 \equiv a_2 \pmod{\mathfrak{R}}$, $a_1, a_2 \in B_m$, wo $\mathfrak{R}$ ein Ideal ist, die Menge der Urbilder für das kleinste Element $O^* \in B_n$. Es sei $a^* = \sigma(a)$, $b^* = \sigma(b)$, $a^*, b^* \in B_n$. Die Elemente a^*, b^* mögen B-abhängig sein, d. h. es existiere eine B-Funktion $G(X_1, X_2) \neq O$, für welche $G(a^*, b^*) = O^*$. Die Beziehung $G(a, b) \equiv O$ in B_m gilt nur mod $\mathfrak{R}$, braucht aber keineswegs in der ursprünglichen Gleichheit zu gelten.

Durch eine Homomorphie, d. h. durch eine Klassenzerlegung nach einem Ideal $\mathfrak{R}$, enstehen also allgemein neue B-Abhängigkeiten mod $\mathfrak{R}$ in der B-Algebra B_m.

Man kann diese Betrachtungen gewissermassen umkehren. Es seien $a_1, \ldots, a_r$ B-unabhängige Elemente aus B_m und $G(X_1, \ldots, X_r) \neq O$ eine B-Funktion von r Unbestimmten. Dann gilt auch $G(a_1, \ldots, a_r) \neq O$. Wir fragen, ob es möglich ist doch eine Beziehung $G(a_1, \ldots, a_r) \equiv O$ zu verlangen, wo wir mit $\equiv$ eine neu definierte Gleichheit in B_m bezeichneten. Die so entstandene B-Abhängigkeit der Elemente $a_1, \ldots, a_r$ werden wir die *erzwungene B-Abhängigkeit der Elemente, $a_1, \ldots, a_r$ mittels der B-Funtion $G(X_1, \ldots, X_r) \neq 0$* nennen. Allgemeiner können wir verlangen $G_1(a_1, \ldots, a_r) \equiv O, \ldots, G_s(a_1, \ldots, a_r) \equiv O$. Wenn mindestens für ein Index k urpsrünglich $G_k(a_1, \ldots, a_r) \neq O$ war, handelt

es sich um die *erzwungene B-Abhängigkeit der Elemente* $a_1, \ldots, a_r$ *mittels der Menge* $M_G = \{G_1(X_1, \ldots, X_r), \ldots, G_s(X_1, \ldots, X_r)\}$ der B-Funktionen.

Wir bezeichnen $G_i(a_1, \ldots, a_r) = b_i \in B_m$, $1 \leqq i \leqq s$. In der neuen Gleichheit müssen alle Elemente b_i in das Ideal $\mathfrak{R}$ gehören, welches die Klassenzerlegung induziert. Dann gilt auch $b_1 \cup \ldots \cup b_s = u \in \mathfrak{R}$ und u ist das grösste Element von $\mathfrak{R}$, welches $\mathfrak{R}$ eindeutig bestimmt nach dem Satze 4.1. Wenn die Menge M_G der B-Bindungsfunktionen nicht schon von Anfang an eine B-Algebra ist, so treten noch weitere B-Bindungsfunktionen zu, welche die Menge M_G zu einer zum Ideal $\mathfrak{R}$ isomorphen B-Algebra ergänzen.

In dem Vektormodell sind alle diese Verhältnisse leicht übersichtlich. Den Elementen $b_i \in B_m$ mögen die Vektoren $\mathrm{b}_i = \sum_{j=1}^{m} b_{ij}\mathrm{e}^{(j)}$ entsprechen. Wir bezeichnen mit L_i die Menge der Indexe j, für welche $b_{ij} = \beta$ und mit $L = L_1 \cup \cup \ldots \cup L_s$ die wohlbestimmte Untermenge von $K = \{1, \ldots, m\}$. Der Unterraum $\mathfrak{M}(L)$ führt in B_m zu der Faktor-B-Algebra $B_m/\mathfrak{M}(L)$; die Gleichheit ihrer Elemente stellt die neue Gleichheit mod $\mathfrak{M}(L) = \mathfrak{R}$ vor.

Als Anwendung haben wir ein einfaches Beispiel aus der Aussagenlogik mit erzwungener B-Abhängigkeit gewählt. Es seien p und q zwei Aussagen, von denen man durch die Operationen der Negation, Disjunktion und Konjunktion eine B-Algebra mit insgesammt 16 Elementen bilden kann. In Ihrem Vektormodell müssen wir also die Vektoren mit vier Koordinaten benützen. Bezeichnen wir die Vektoren, die den Aussagen p und q entsprechen, mit p und q, so können wir z. B.

$$\mathrm{p} = (\alpha, \beta, \alpha, \beta), \qquad \mathrm{q} = (\alpha, \alpha, \beta, \beta)$$

wählen. Durch diese Wahl haben wir schon die Tatsache ausgedrückt, dass die beiden Aussagen p und q zuerst unabhängig sein sollen. Jetzt werden aber alle 16 Elemente des Raumes $\mathfrak{M}_4$ schon eindeutig bestimmt, d. h. die isomorphe Abbildung der Aussagenlogik auf den Vektorraum ist festgelegt.

Die erzwungene B-Abhängigkeit soll durch die B-Funktion $X_1' \cap X_2'$ gegeben werden, d. i. wir verlangen, dass non $p \wedge$ non $q \equiv 0$. In Worten: Von den beiden Aussagen soll mindestens eine immer wahrhaft sein.

In unserem Vektormodell entspricht der eingeführten B-Bindungsfunktion der Vektor $p' \,.\, q' = (\beta, \alpha, \alpha, \alpha)$. Es ist also $L = \{1\}$, $\mathfrak{M}(L) = \{(\alpha, \alpha, \alpha, \alpha), (\beta, \alpha, \alpha, \alpha)\}$. Die 16 Aussagen grupieren sich mod $\mathfrak{M}(L)$ zu zwei in acht Äquivalenzklassen (deren Elemente auch im Sinne der Aussagenlogik äquivalent sind). In jede Klasse gehören die zwei Aussagen, deren zugeordnete Vektoren sich nun in der ersten Koordinate unterscheiden.

So ist es z. B. $p = (\alpha, \beta, \alpha, \beta)$, $p + q' = (\beta, \beta, \alpha, \beta)$. Wir können also eine logische Äquivalenz schreiben

$$p \equiv q \to p \ (\mathrm{mod\ non}\ p \wedge \mathrm{non}\ q \equiv 0),$$

wo das Zeichen $\to$ die logische Implikation bedeutet. Der Leser möge versuchen die Richtigkeit dieser Äquivalent durch die Mittel der Aussagenlogik zu bestätigen. Er wird sofort erkennen, dass die Benützung des Vektormodells viel behaglicher ist.

LITERATUR

[1] *Birkhoff, G.:* Lattice Theory, American Mathem. Society, New York, 1940.
[2] *Ore, O.:* On the Foundations of abstract Algebra, Annals of Math., 37 (1936).
[3] *Dubreil, P.—Dubreil, M. L.—Jacotin:* Leçons d'algèbre moderne, Paris Dunod, 1964.

SHRNUTÍ

VEKTOROVÝ MODEL KONEČNÝCH BOOLOVÝCH ALGEBER

JOSEF METELKA

Vektorový m-rozměrný prostor, v němž jsou účelně zavedeny operace sčítání a násobení, může sloužit jako univerzální model ke studiu konečných Booleových algeber o 2^m členech. Ukazuje se, že mnohá vyšetřování jsou při použití tohoto modelu přehlednější. Týká se to např. pojmu homomorfismu a faktorové Booleovy algebry, kde ke zjednodušení studia přispívá pojem podprostoru příslušného k jisté vybrané posloupnosti. Tento podprostor je vždy ideálem a rozklad na třídy jím způsobený lze bez násilí popsat jako promítání z jednoho podprostoru do jiného komplementárního podprostoru. Zvláště užitečný se vektorový model ukázal při studiu Booleovské závislosti a nezávislosti funkcí. Tento pojem je v článku zaveden jako přirozené rozšíření algebraické nezávislosti a závislosti. Pomocí vektorového modelu je možno definovat důležitý celočíselný charakter množiny Booleových funkcí, který byl nazván hodností této množiny. Hodnost má některé vlastnosti obdobné vlastnostem hodnosti matice, zejména souvisí s Booleovskou závislostí a nezávislostí funkcí takto: Množina n Booleových funkcí je nezávislá právě tehdy, je-li její hodnost $h = 2^n$. Je-li $h < 2^n$, existuje přesně $2^{2^n - h} - 1$ Booleových funkcí (v článku se nazývají „vazební"), jež zprostředkují netriviálním způsobem Booleovskou závislost funkcí množiny. Vektorový model umožňuje okamžité vyhledání všech vazebních funkcí. V posledním oddílu článku se studuje tzv. vynucená Booleovská závislost funkcí, která vede na zobecněnou rovnost, tím na rozklad množiny funkcí na třídy, tj. na jistý endomorfismus této množiny. Aplikabilita zavedených pojmů i metod se předvádí na jednoduchém příkladě z výrokové logiky s vynucenou logickou závislostí.