Acta Math. Univ. Comenianae
Vol. LX, 2(1991), pp. 225–231

ON VARIETIES GENERATED BY BOOLEAN CLONES

K. DENECKE

Clones are collections of functions defined on the same set A which are closed under superposition and contain all projections. One of the applications of clones is the composition of switching circuits. The combination of switching circuits to logical networks can be regarded as a technical realization of the superposition of Boolean functions, i.e. functions defined on the set $\{0,1\}$. In [**5**] A. I. Mal'cev described clones as carriers of algebras of the type $(2,1,1,1,0)$. W. Taylor ([**6**]) showed that the identities of such clone algebras (for short also clones) correspond to so-called hyperidentities. Hyperidentities are special formulas in a second order language. To the differences between clones of Boolean functions and clones of functions defined on sets with more than two elements belongs the following fact ([**2**]): Every clone of Boolean functions is (up to isomorphisms) uniquely determined by the sets of its hyperidentities. In this sense, Boolean clones can be "separated" by hyperidentities. This is not longer true for clones of functions defined on sets with more than two elements. There are non-isomorphic clones of functions defined on the same set A with $|A| > 2$ satisfying the same hyperidentities. Using these results we characterize that part of a variety generated by a clone of Boolean functions which consists only of clones of Boolean functions and describe all homomorphic images of clones of Boolean functions.

1. Basic Concepts

Let A be a finite nonempty set and let $O_n(A)$ be the set of all n-ary functions $f\colon A^n \to A$. We set $O(A) = \cup_{n=1}^{\infty} O_n(A)$ and define the following operations on $O(A) : *, \xi, \tau, \Delta, e_1^2$:

$$(f * g)(x_1, \dots, x_{m+n-1}) := f(g(x_1, \dots, x_m), x_{m+1}, \dots, x_{m+n-1}),$$
$$f \in O_n(A),\ g \in O_m(A),$$
$$(\tau f)(x_1, \dots, x_n) := f(x_2, x_3, \dots, x_n, x_1),$$
$$(\xi f)(x_1, \dots, x_n) := f(x_2, x_1, x_3, \dots, x_n),$$
$$(\Delta f)(x_1, \dots, x_n) := f(x_1, x_1, \dots, x_{n-1}) \quad \text{if } f \in O_n(A) \text{ with } n > 1 \text{ and}$$

Received January 10, 1991; revised September 2, 1991.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 08A40, 08B15.

$$(\tau f)(x_1) = (\xi f)(x_1) = (\Delta f)(x_1) = f(x_1) \quad \text{if } f \text{ is a unary function.}$$

As a nullary operation we add the binary projection on the first component $(e_1(x_1, x_2) = x_1)$.

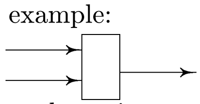
In this manner we get an algebra $\mathbb{O}(A) := (O(A); *, \xi, \tau, \Delta, e_1^2)$ of the type $(2, 1, 1, 1, 0)$. Each subalgebra of $\mathbb{O}(A)$ (or its carrier) is called a clone. In case that $A = \{0, 1\}$ by $\mathcal{L}_2$ we denote the lattice of all subclones of $\mathbb{O}(\mathbb{A})$. The lattice $\mathcal{L}_2$ is atomic and dually atomic, the cardinality of $\mathcal{L}_2$ is countably infinite and each clone from $\mathcal{L}_2$ is finitely generated ([**6**]). For $|A| > 2$ the lattice $\mathcal{L}_{|A|}$ of all subclones of $\mathbb{O}(A)$ has the cardinality of the continuum and there are clones which are not finitely generated. If $\mathbb{C}$ is a clone then under $\operatorname{Id}\mathbb{C}$ we understand the set of all identities of $\mathbb{C}$. For instance, $e_1^2 * X = X$ is an identity satisfied by every clone $\mathbb{C} = (C; *, \xi, \tau, \Delta, e_1^2)$, where X is a variable for any function of C. For an algebra $\mathbb{A} = (A; \Omega)$ the set of all its derived operations is the clone generated by Ω and is called clone of all term functions of the algebra $\mathbb{A}$. Conversely, if a clone $\mathbb{C}$ of functions (defined on A) is given, it can be regarded as the clone of term functions of an algebra with the carrier A. Clearly, an algebra is not uniquely determined by the clone of its term functions. For terms w_1, w_2 which are constructed in the usual way from individual variables and from the elements of a set of operation variables (each of them is endowed with an arity) we define:

Definition 1.1. Let w_1, w_2 be terms built from operation symbols ω_i of the arity n_i, $(i = 1, \dots, k)$. $w_1 = w_2$ is called a hyperidentity of the algebra $\mathbb{A} = (A; \omega)$ (in symbols $\mathbb{A} \vdash w_1 = w_2$ or $T(\mathbb{A}) \vdash w_1 = w_2$) if for all choices of n_i-ary functions f_i $(i = 1, \dots, k)$ from $T(\mathbb{A})$ the two term functions w_1^A, w_2^A obtained from w_1 and w_2 by replacing the n_i-ary operation symbols ω_i by f_i $(i = 1, \dots, k)$ are identical.

In [**7**] W. Taylor recognized the equivalence between identities for clones and hyperidentities (see also [**4**]).

As an example we mention that the equation $F(F(x, y), y) = F(x, y)$ is a hyperidentity satisfied by any lattice. That means: substituting any binary term function of the lattice for the binary operation symbol F one obtains a lattice identity.

Hyperidentities can be applied in the theory of logical nets. Consider the following example:

Let  be a symbol for an arbitrary switching circuit with one output and two inputs. Then the composed network (Fig. 1) can be substituted by the elementary switching circuit since $F(x, F(x, F(x, y))) = F(x, y)$ is a hyperidentity of the two-element Boolean algebra $\mathbb{2} = (\{0, 1\}; \wedge, N)$ ($\wedge$ conjunction, N negation) and since the term $F(x, F(x, F(x, y)))$ describes the composed circuit.

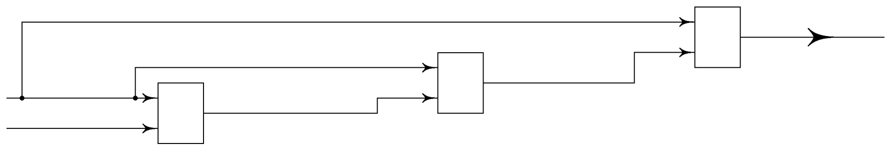


Fig. 1.

2. Separation of Clones of Boolean Functions by Hyperidentities

Under the separation of two clones via hyperidentities we understand the following problem: Are the sets $\operatorname{Id}\mathbb{C}$ and $\operatorname{Id}\mathbb{C}'$ of all identities of two non-isomorphic clones $\mathbb{C}$ and $\mathbb{C}'$ (written as hyperidentities) of functions defined on the same set A equal or not?

In [**1**] the following result is given:

Lemma 2.1 ([1]). *Let $\mathbb{C}$ and $\mathbb{C}'$ be two clones of Boolean functions with $\mathbb{C} \subset \mathbb{C}'$. Then $\operatorname{Id}\mathbb{C} \supset \operatorname{Id}\mathbb{C}'$, where $\operatorname{Id}\mathbb{C}$ and $\operatorname{Id}\mathbb{C}'$ are the sets of all identities of the clones $\mathbb{C}$ and $\mathbb{C}'$, respectively.*

To prove Lemma 2.1 the identities of $\mathbb{C}$ (of $\mathbb{C}'$) are written equivalently as hyperidentities of certain two-element algebras. For clones of functions defined on sets with more than two elements Lemma 2.1 is not valid. We will give an example for $A = \{0, 1, \ldots, k-1\}$, $k \geq 3$. Consider the functions c, h_1, h_2 defined by

$$c(x) = \begin{cases} 0, & \text{if } x = 1,2 \\ x, & \text{otherwise} \end{cases}, \quad h_1(x) = \begin{cases} 0, & \text{if } x = 2 \\ x, & \text{otherwise} \end{cases}, \quad h_2(x) = \begin{cases} 0, & \text{if } x = 1 \\ x, & \text{otherwise} \end{cases}$$

and the clones $\mathbb{C} = \langle\{id, c\}\rangle$ (id is the identity function on A) where $C_1 = \{id, c\}$ is the set of all unary functions of $\mathbb{C}$ and $\mathbb{C}' = \langle\{id, c, h_1, h_2\}\rangle$ where $C_1' = \{id, c, h_1, h_2\}$ are the unary functions of $\mathbb{C}'$. It is easy to see that the monoid $\mathbb{C}_1' = (\{id, c, h_1, h_2\}; *, id)$ is isomorphic to a direct power of $\mathbb{C}_1 = (\{id, c\}; *, id)$. It follows that $\operatorname{Id}\mathbb{C}_1' = \operatorname{Id}\mathbb{C}_1$. Because of $\mathbb{C} = \langle C_1\rangle$ and $\mathbb{C}' = \langle C_1'\rangle$ we have $\operatorname{Id}\mathbb{C} = \operatorname{Id}\mathbb{C}'$, but $\mathbb{C} \subset \mathbb{C}'$.

Further for clones of Boolean functions we have ([**2**]):

Lemma 2.2 ([2]). *Let $\mathbb{C}$ and $\mathbb{C}'$ be two non-isomorphic clones of Boolean functions with $\mathbb{C} \nsubseteq \mathbb{C}'$ and $\mathbb{C}' \nsubseteq \mathbb{C}$ and assume that there is no clone $\mathbb{C}'' \cong C'$ with $\mathbb{C} \subseteq \mathbb{C}''$ and no clone $\mathbb{C}^* \cong \mathbb{C}$ with $\mathbb{C}' \subseteq \mathbb{C}^*$. Then there holds $\operatorname{Id}\mathbb{C} \nsubseteq \operatorname{Id}\mathbb{C}'$ and $\operatorname{Id}\mathbb{C}' \nsubseteq \operatorname{Id}\mathbb{C}$.*

Remark. From Lemma 2.1 and Lemma 2.2 it follows that for any two non-isomorphic clones of Boolean functions $\mathbb{C}$ and $\mathbb{C}'$ there holds $\operatorname{Id}\mathbb{C} \neq \operatorname{Id}\mathbb{C}'$, i.e. $\mathbb{C}$ and $\mathbb{C}'$ can be separated by hyperidentities.

3. Varieties Generated by Boolean Clones

We can now state and prove an easy but useful corollary of Lemma 2.1 and Lemma 2.2.

Corollary 3.1. *Let $\mathbb{C}$ and $\mathbb{C}'$ be two clones of Boolean functions with* $\operatorname{Id}\mathbb{C} \supset \operatorname{Id}\mathbb{C}'$. *Then there is a Boolean clone $\mathbb{C}''$ with $\mathbb{C} \subset \mathbb{C}''$ and $\mathbb{C}' \cong \mathbb{C}''$.*

Proof. Assume that for all $\mathbb{C}'' \in \mathcal{L}_2$ we have: if $\mathbb{C}'' \cong \mathbb{C}'$ then $\mathbb{C} \subset \mathbb{C}''$. If $\mathbb{C}' \cong \mathbb{C}'' \subseteq \mathbb{C}$ we get $\operatorname{Id}\mathbb{C}' = \operatorname{Id}\mathbb{C}'' \supseteq \operatorname{Id}\mathbb{C}$. This contradicts the presumption. Further there exists no clone $\mathbb{C}^*$ with $\mathbb{C}'' \subseteq C^* \cong \mathbb{C}$ since otherwise $\operatorname{Id}\mathbb{C}'' \supseteq \operatorname{Id}\mathbb{C}^* = \operatorname{Id}\mathbb{C}$ and $\operatorname{Id}\mathbb{C}'' = \operatorname{Id}\mathbb{C}'$. $\operatorname{Id}\mathbb{C}' \supseteq \operatorname{Id}\mathbb{C}$ contradicts the presumption. Moreover, there exists no clone $\mathbb{C}^+$ with $\mathbb{C} \subseteq \mathbb{C}^+ \cong \mathbb{C}'' \cong \mathbb{C}'$ since by $C^+ \cong \mathbb{C}'$ we would have $\mathbb{C} \subset \mathbb{C}^+$ and $\mathbb{C} = \mathbb{C}^+ \cong \mathbb{C}'' \cong \mathbb{C}'$ would mean $\operatorname{Id}\mathbb{C} = \operatorname{Id}\mathbb{C}'$ which contradicts the presumption. Therefore, if $\mathbb{C}''$ and $\mathbb{C}$ are incomparable, i.e. if $\mathbb{C}'' \nsubseteq \mathbb{C}$ and $\mathbb{C} \nsubseteq \mathbb{C}''$ by Lemma 2.2 we get $\operatorname{Id}\mathbb{C}'' \nsubseteq \operatorname{Id}\mathbb{C}$ and $\operatorname{Id}\mathbb{C} \nsubseteq \operatorname{Id}\mathbb{C}'' = \operatorname{Id}\mathbb{C}'$ in contradiction to the presumption. □

A consequence of Corollary 3.1 and Lemma 2.1 is

Theorem 3.2. *Let $\mathbb{C}$ and $\mathbb{C}'$ be two clones of Boolean functions. Then* $\operatorname{Id}\mathbb{C} \supset \operatorname{Id}\mathbb{C}'$ *if and only if there is a Boolean clone $\mathbb{C}''$ with $\mathbb{C} \subset \mathbb{C}''$ and $\mathbb{C}'' \cong \mathbb{C}'$.*

Further we get

Corollary 3.3. *Let $\mathbb{C}$ and $\mathbb{C}'$ be two clones of Boolean functions. Then* $\operatorname{Id}\mathbb{C} = \operatorname{Id}\mathbb{C}'$ *if and only if $\mathbb{C} \cong \mathbb{C}'$.*

Proof. $\mathbb{C} \cong \mathbb{C}'$ implies $\operatorname{Id}\mathbb{C} = \operatorname{Id}\mathbb{C}'$. If conversely, $\operatorname{Id}\mathbb{C} = \operatorname{Id}\mathbb{C}'$ then $\mathbb{C} \subset \mathbb{C}'$ and $\mathbb{C}' \subset \mathbb{C}$ are impossible because of Lemma 2.1. Assume $\mathbb{C}$ and $\mathbb{C}'$ are incomparable, i.e. $\mathbb{C} \nsubseteq \mathbb{C}'$ and $\mathbb{C}' \nsubseteq \mathbb{C}$. There are clones $\mathbb{C}^*, \mathbb{C}^+$ with $\mathbb{C} \subseteq \mathbb{C}^* \cong \mathbb{C}'$ and $\mathbb{C}' \subseteq \mathbb{C}^+ \cong \mathbb{C}$. Otherwise by Lemma 2.2 it would be follow $\operatorname{Id}\mathbb{C} \neq \operatorname{Id}\mathbb{C}'$. Since from $\mathbb{C} \subset \mathbb{C}^+ \cong \mathbb{C}$ it would be follow $\operatorname{Id}\mathbb{C}' \supset \operatorname{Id}\mathbb{C}$, we get $\mathbb{C} = \mathbb{C}^* \cong \mathbb{C}'$ or $\mathbb{C}' = \mathbb{C}^+ \cong \mathbb{C}$. In both cases we have $\mathbb{C} \cong \mathbb{C}'$. □

Let $\mathcal{V}(\mathbb{C})$ be the variety (of algebras of the same type $(2,1,1,1,0)$) generated by $\mathbb{C}$. Clearly, every subalgebra of $\mathbb{C}$ is a Boolean clone. The only isomorphism of a Boolean clone $\mathbb{C}'$ is given by the mapping $\mathbb{C}' \to \mathbb{C}'^d \cong \mathbb{C}$ with $\mathbb{C}^d = \{f^d \mid f \in C\}$ and $f^d(x_1, \ldots, x_n) = Nf(Nx_1, \ldots, Nx_n)$, where N is the negation. $\mathbb{C}'^d$ is a Boolean clone. There arises the question whether all algebras of $\mathcal{V}(\mathbb{C})$ which are Boolean clones are subclones or isomorphic images of subclones of $\mathbb{C}$.

Definition 3.4. $\mathcal{V}_2(C) := \mathcal{V}(\mathbb{C}) \cap \mathcal{L}_2$.

Clearly, $\mathcal{V}_2(\mathbb{C}) = \{\mathbb{C}' \mid \operatorname{Id}\mathbb{C}' \supseteq \operatorname{Id}\mathbb{C} \ \wedge \ \mathbb{C}' \in \mathcal{L}_2\}$. We get the following characterization of $\mathcal{V}_2(\mathbb{C})$:

Theorem 3.5. *Let $\mathbb{C}$ be a clone of Boolean functions. Then we get $\mathcal{V}_2(\mathbb{C}) = IS(\mathbb{C})$ where I, S denote operators for the formation of isomorphic images and subalgebras.*

Proof. Clearly, $IS(\mathbb{C}) \subseteq \mathcal{V}_2(\mathbb{C})$. If $\mathbb{C}' \in \mathcal{V}_2(\mathbb{C})$ and $\mathrm{Id}\,(\mathbb{C}) = \mathrm{Id}\,(\mathbb{C}')$, then we get $\mathbb{C} \cong \mathbb{C}'$ by Corollary 3.3 and therefore $\mathbb{C}' \in IS(\mathbb{C})$. If $\mathrm{Id}\,\mathbb{C}' \supset \mathrm{Id}\,\mathbb{C}$ then by Theorem 3.2 there exists a Boolean clone $\mathbb{C}''$ with $\mathbb{C}' \subset \mathbb{C}''$ and $\mathbb{C}'' \cong \mathbb{C}$. Under this isomorphism there exists a subalgebra of $\mathbb{C}$ which is isomorphic to $\mathbb{C}'$, i.e. $\mathbb{C}' \in IS(\mathbb{C})$. Altogether we have $\mathcal{V}_2(\mathbb{C}) \subseteq IS(\mathbb{C})$. □

In a natural way there arises the question whether any homomorphic image of a Boolean clone is again a Boolean clone (i.e. by Theorem 3.5 a subalgebra or an isomorphic image of a subalgebra). Factorization of a clone by each of its congruence relations leads to all homomorphic images of this clone. On every clone $\mathbb{C}$ there are the following congruence relations $\varkappa_0$, $\varkappa_a$, $\varkappa_1$ defined by

$$
\begin{aligned}
&(f,g) \in \varkappa_0 \iff \{f,g\} \subseteq \mathbb{C} \text{ and } f = g,\\
&(f,g) \in \varkappa_a \iff \{f,g\} \subseteq \mathbb{C} \text{ and } arf = arg \quad (arf = arity \text{ of } f)\\
&(f,g) \in \varkappa_1 \iff \{f,g\} \subseteq \mathbb{C}.
\end{aligned}
$$

As usual $\mathbb{C}/\varkappa_0 = \mathbb{C}$ and $\mathbb{C}/\varkappa_1 = \mathbb{I}$, where $\mathbb{I}$ is a one-element algebra of the type $(2,1,1,1,0)$. The carrier of $\mathbb{C}/\varkappa_a$ consists of exactly one function of each arity. Therefore, $\mathbb{C}/\varkappa_a = \mathbb{O}(\{0,1\})$.

(Remark that for the algebra $\mathbb{C}/\varkappa_1$ there is no set such that $\mathbb{C}/\varkappa_1$ is isomorphic to a clone of functions on this set.) Gorlov ([**3**]) determined the congruence lattices of all Boolean clones.

We introduce the following notations:

$+$ for the addition modulo 2 on $\{0,1\}$,

N for the negation,

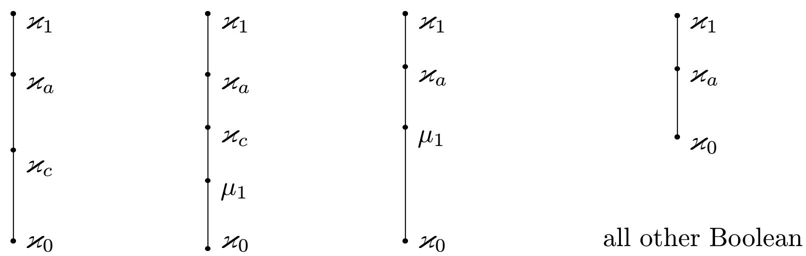
$c_0^n, c_1^n, n \in \mathbb{N}$, for the n-ary constant operations with the value 0 and 1, respectively,

$$
\begin{aligned}
&\mathbb{L}_1 := \left\langle \{+, N, c_0^1, c_1^1\} \right\rangle \text{ (linear functions)},\\
&\mathbb{L}_3 := \left\langle \{+, c_0^1\} \right\rangle \text{ linear } \{0\}\text{-preserving functions)},\\
&\mathbb{L}_4 := \langle \{x+y+z\} \rangle\,,\ \mathbb{L}_5 := \langle \{x+y+z, N\} \rangle\,,\\
&\mathbb{O}_4 := \langle \{N\} \rangle\,,\ \mathbb{O}_9 := \left\langle \{N, c_0^1\} \right\rangle,\\
&\mathbb{O}_8 := \left\langle \{id, c_0^1, c_1^1\} \right\rangle,\ \mathbb{O}_6 := \left\langle \{id, c_0^1\} \right\rangle,\\
&\mathbb{O}_1 := \langle \{id\} \rangle\,.
\end{aligned}
$$

Further we define congruences $\varkappa_c$ and μ_1 by

$$(f,g) \in \varkappa_c :\Longleftrightarrow \quad \{f,g\} \in C \text{ and } arf = arg \text{ and there is an element } c \in \{0,1\}$$
$$\text{with } f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n) + c.$$
$$(f,g) \in \mu_1 :\Longleftrightarrow \quad \{f,g\} \in C \text{ and } f = g \text{ or there is an element } n \in \mathbb{N}$$
$$\text{with } \{f,g\} = \{c_0^n, c_1^n\}.$$

Then the congruence lattices of all Boolean clones have the following form:



$\mathbb{L}_1, \mathbb{L}_5, \mathbb{O}_4$ $\quad$ $\mathbb{O}_9$ $\quad$ $\mathbb{O}_8$ $\quad$ clones

These congruences lead to the following factor algebras: $\mathbb{L}_1/\varkappa_c \cong \mathbb{L}_3 \subset \mathbb{L}_1$, $\mathbb{L}_5/\varkappa_c \cong \mathbb{L}_4 \subset \mathbb{L}_5$, $\mathbb{O}_4/\varkappa_c \cong \mathbb{O}_1$, $\mathbb{O}_9/\varkappa_c \cong \mathbb{O}_6 \subset \mathbb{O}_9$, $\mathbb{O}_8/\mu_1 \cong \mathbb{O}_6 \subset \mathbb{O}_8$.

Further, it is easy to see that the carrier of $\mathbb{O}_9/\mu_1$ contains exactly three unary functions f_1, f_2, f_3 with

$*$	f_1	f_2	f_3
f_1	f_1	f_2	f_3
f_2	f_2	f_1	f_3
f_3	f_3	f_3	f_3

Therefore, $\mathbb{O}_9/\mu_1 = \langle\{f_1, f_2, f_3\}\rangle$ is not a clone of Boolean functions. $\mathbb{O}_9/\mu_1$ can be interpreted as a clone of functions defined on $\{0,1,2\}$ with $f_1 = id$, $f_2 = (12)$, $f_3 = c_0^1$.

We mention that an algebra is subdirectly irreducible if its congruence lattice has a uniquely determined atom. Using Gorlov's result we get:

Lemma 3.6. *Every Boolean clone is subdirectly irreducible.*

Altogether we obtain

Theorem 3.7. *Let $\mathbb{C}$ be a clone of Boolean functions and $\mathbb{C} \neq \mathbb{O}_9$. Then $\mathcal{V}_2(\mathbb{C}) = HS(\mathbb{C}) \setminus \{\mathbb{I}, \mathbb{O}(\{0\})\}$ ($\mathbb{I} =$ one-element algebra).*

For $\mathbb{O}_9$ we have $\mathcal{V}_2(\mathbb{O}_9) = HS(\mathbb{O}_9) \setminus \{\mathbb{I}, \mathbb{O}(\{0\}, \langle\{id, (12), c_0^1\}\rangle\}$.

References

1. Denecke K., *Boolean clones and hyperidentities in Universal Algebras, Universal and Applied Algebra*, Proceedings of the V. Universal algebra Symposium, Turawa, Poland, 3-7 May, 1988, World Scientific, Singapore, New Yersey, London, Honkong, 1989.

2. Denecke K., Mal'cev I. A. and Reschke M., *Separation of clones by hyperidentities*, Preprint, 1990.

3. Gorlov V. V., *On congruences on closed Post classes*, Mat. Zametki **13** (1973), 725–734. (Russian)

4. Hoehnke H. J., *Superposition partieller Funktionen (Studien zur Algebra und ihre Anwendungen)*, Berlin, 1972.

5. Mal'cev A. I., *Iterative Post algebras and varieties*, Algebra i Logika **5** (1966), 5–24. (Russian)

6. Post E. L., *Introduction to a general theory of elementary propositions*, Amer. J. Math. **43** (1921), 163–185.

7. Taylor W., *Hyperidentities and hypervarieties*, Aequat. Math. **23** (1981), 30–49.

K. Denecke, FB Matematik, Brandenburgische Landeshochschule Am Neuen Palais, D-1571 Potsdam, Germany