Polynomial reducts of modules.I. Rough classification

Bulatov A.A.

Abstract. The lattice of iterative algebras of linear functions is studied in the paper. Any algebra of linear functions can be assigned to one of four types. For definitions of these types properties of coefficients of functions and some special functions are used. We study properties of lattices consisting of algebras of each type. In addition, maximal subalgebras of linear functions are described.

1991 Mathematics Subject Classification: 08A40, 03B50.

§1. Introduction and preliminaries

A set of (finitary) functions on a given finite set A is called *a clone* if it is closed under composition and contains all projection functions (i.e. functions of the form $e_i^n(x_1,\dots,x_n) = x_i$). The set of all functions on A is denoted by $\mathbf{P}_A$. An *iterative algebra* on A is a set of functions on A closed under operations of superposition $\circ, \tau, \xi, \Delta, \nabla$ ([4]). These operations are defined as follows

$$(f \circ g)(x_1,\dots,x_{m+n-1}) \;=\; f(g(x_1,\dots,x_m), x_{m+1},\dots,x_{m+n-1})$$

(*substitution* of a function g instead of the first variable),

$$(\nabla f)(x_1,\dots,x_{n+1}) \;=\; f(x_1,x_2,\dots,x_n)$$ (*adding of a fictitious variable)*

where f is n-ary and g is m-ary;

$$\begin{array}{rcll}(\tau f)(x_1,\ldots,x_n) & = & f(x_2,x_1,x_3,\ldots,x_n) & (\textit{permutations} \\ (\xi f)(x_1,\ldots,x_n) & = & f(x_2,,\ldots,x_n,x_1) & \textit{of variables}), \\ (\Delta f)(x_1,\ldots,x_{n-1}) & = & f(x_1,x_1,x_2,\ldots,x_{n-1}) & (\textit{identification} \\ & & & \textit{of variables})\end{array}$$

if $n \geq 2$;

$$\tau f = \xi f = \Delta f = f$$

if f is unary. So, a clone is an iterative algebra containing all projections. Throughout this paper except Theorems 1,2 we refer iterative algebras rather than clones. The iterative algebra consisting of all projections will be called the algebra of projections and denoted by $\mathbf{J}_A$. For any $C \subseteq \mathbf{P}_A$, we denote by $\langle C \rangle$ the iterative algebra generated by C. The arity of a function f is denoted by $\mathrm{ar} f$ and the set of all n-ary functions from C is denoted by $C^{(n)}$.

Let R be a finite associative commutative ring with an identity element 1 and let M be a finite faithful unitary R-module. A linear function on M is a function of the form

$$\sum \varrho_i x_i + a$$

where $a \in M$ and $\varrho_i \in R$. Thus, a linear function is a polynomial operation of the module M. All linear functions on M formss an iterative algebra which is denoted by $\mathbf{L}_M$; the lattice all of subalgebras of $\mathbf{L}_M$ is denoted by Sub $\mathbf{L}_M$. Note that the least element of Sub $\mathbf{L}_M$ is the empty iterative algebra.

An (universal) algebra $\mathfrak{B}$ is called *a polynomial reduct* of an algebra $\mathfrak{A}$ if each polynomial operation of $\mathfrak{B}$ is a polynomial operation of $\mathfrak{A}$. Clearly, any algebra $(M, \mathbf{C})$ where $\mathbf{C}$ contains all projections and $\mathbf{C} \in$ Sub $\mathbf{L}_M$ is a polynomial reduct of the module M. Most of important properties (for example, subalgebras, congruences, endomorphisms etc.) depend on only clone of term operations of an algebra. So, one may investigate such properties up to term equivalence. One of useful ways of such an investigation is to classify clones of term operations of algebras. Here we deal with clones of polynomial operations of finite modules.

The lattice of iterative algebras of linear functions is one of the oldest objects to study in multiple-valued logic. However, this lattice has been described for some special R-modules only. The first result in this direction is the description of subalgebras of $\mathbf{L}_{\mathbb{Z}_p}$ with p prime where $\mathbb{Z}_p$ is the set of integers modulo p considered as a $\mathbb{Z}_p$-module (Salomaa [7] and independently

Demetrovics and Bagyinszki [1]). Later it was proved that Sub $\mathbf{L}_M$ is denumerable for any M ([10], see also [2]). Moreover, Sub $\mathbf{L}_M$ is finite if and only if R is a direct sum of fields. In this case, the description of Sub $\mathbf{L}_M$ was given ([11, 10, 2]). In more general case some finite sublattices of Sub $\mathbf{L}_M$ were studied. Namely, clones containing the Mal'cev function $x - y + z$ and clones of idempotent functions (a function f is called *idempotent* if it satisfies the condition $f(x, \ldots, x) = x$) were described by A.Szendrei ([8, 9], also, [10], [3]).

In this paper we consider $\mathbf{L}_M$ for an arbitrary finite R-module M where R is associative commutative ring with identity element 1. Any algebra from Sub $\mathbf{L}_M$ can be assigned to one of several types defined below. The definitions of these types use properties of coefficients of functions and, in addition, some special functions. Iterative algebras of each type form an interval or a (set-theoretical) union of intervals of Sub $\mathbf{L}_M$. Algebras of the first type are those containing a function $\varepsilon x + (1 - \varepsilon)y$ where ε is an idempotent of R ($\varepsilon \neq 0, 1$). Similarily, algebras of the second type are those which is not of the first type and containing the function $\varepsilon x + (1 - \varepsilon)b$ where ε is an idempotent of R ($\varepsilon \neq 0, 1$) and $b \in M$. A function $f = \sum_{i=1}^{n} \alpha_i x_i + a$ is called *primitive*, if there exists $j \in \{1, \ldots, n\}$ such that α_j is an invertible element and α_i is a nilpotent element whenever $i \neq j$. Algebras of the third type consist of primitive functions and functions whose coefficients are nilpotent elements. Finally, an algebra belongs to the fourth type if it contains the Mal'cev function $x - y + z$ and is not of the first type.

In §2 we find atoms of Sub $\mathbf{L}_M$ and some covering elements of atoms. We consider a few types of special functions. Then we classify iterative algebras by means of special functions they contain as it was pointed above. Algebras of the first and of the second types are studied in §3. Certain intervals consisting of algebras of the first type can be decomposed into direct product (Theorem 1). Also, we exhibit one special congruence of the lattice of algebras of the second type (Theorem 2). Using Theorems 1,2 we can reduce the study of the structure of algebras of these types to the one for smaller modules. We finish §3 with a description of coatoms of Sub $\mathbf{L}_M$. Algebras of the fourth type are already described by A.Szendrei [11]. Part II of this paper is devoted to study of the algebra of primitive functions and of the lattice of algebras of third type. In particular, we completely describe the lattice of algebras of primitive functions.

Throughout the paper the set $\{1, \ldots, n\}$ is denoted by $\underline{n}$.

§2. Atoms, and types of functions

2.1. Atoms of Sub $\mathbf{L}_M$ and covering elements of the algebra of projections in Sub $\mathbf{L}_M$.

Let us start with description of all atoms of Sub $\mathbf{L}_M$. As usual $\mathrm{E}(R)$ denotes the set of all idempotents of the ring R.

Proposition 1 *Atoms of* Sub $\mathbf{L}_M$ *are exactly the following iterative algebras:*
(1) $\mathbf{J}_M$*;*
(2) $\langle a\rangle$, $a \in M$ *(an algebra generated by a constant function* a*);*
(3) $\langle \varepsilon x + (1-\varepsilon)b\rangle$ *where* $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$, $b \in M$.

The proof of Proposition 1 is an easy exercise. One just needs to calculate linear functions being idempotents of the symmetric semigroup on M.

Our next step is the description of covering elements of $\mathbf{J}_M$ (i.e. atoms of the clone lattice that are contained in Sub $\mathbf{L}_M$). The covering elements of $\mathbf{J}_M$ which consist of idempotent functions were found in [5] and [10]. The following statement completes these results of [5],[10].

As usual, the characteristic of a ring R is denoted by char R. For a linear function $f(x_1,\ldots,x_n) = \sum_{i=1}^n \alpha_i x_i + b$, we use the following notation: $\sigma(f) = \sum_{i=1}^n \alpha_i - 1$ and $\beta(f) = b$. Note that

$$\sigma(f \circ g) = \sigma(f) + \alpha_1\sigma(g), \quad \beta(f \circ g) = \beta(f) + \alpha_1\beta(g)$$

for any $f, g \in \mathbf{L}_M$.

Proposition 2 *The covering elements of the algebra of projections in* Sub $\mathbf{L}_M$ *are*
(i) $\mathbf{J}_M \vee A$ *where* A *is an atom of* Sub $\mathbf{L}_M$ *different from* $\mathbf{J}_M$*;*
(ii) $\langle \varepsilon x + (1-\varepsilon)y\rangle$ *where* $\varepsilon \in \mathrm{E}(R)$, $\varepsilon \neq 0,1$*;*
(iii) $\langle \alpha x + b\rangle$ *where*
either $\alpha \neq 1$ *is such that* $\alpha^p = 1$ *for some prime* p *and an equality* $(1+\alpha+\alpha^2+\ldots+\alpha^{p-1})b = 0$ *holds*
or $\alpha = 1$ *and* b *is of prime additive order;*
(iv) $\langle x - \varrho y + \varrho z\rangle$ *where* $\varrho \neq 0$ *is such that* $\varrho^2 = 0$ *and* ϱ *is of prime additive order;*
(v) $\langle x - y + z\rangle$ *if* char R *is a prime.*

Proof.

First, we show that all listed algebras cover the algebra of projections. Assertion (i) is obvious, (ii), (iv) and (v) are proved in [5]. So, we have to verify (iii) only.

A unary function $g(x)$ generates a covering element of $\mathbf{J}_M$ if and only if this function being considered as a permutation of a set A generates a minimal nontrivial subgroup of the symmetric group on A. Thus we have to prove that $g^p(x) = x$ for a suitable prime p. If $g(x) = \alpha x + b$, then

$$g^p(x) = \alpha^p x + (1 + \alpha + \alpha^2 + \ldots + \alpha^{p-1})b = x.$$

Further, if $g(x) = x + b$ and p is an order of b, then $g^p(x) = x + p \cdot b = x$.

Now we prove that each covering element of $\langle e_1^1 \rangle$ in Sub $\mathbf{L}_M$ is of the form (i)–(v). If an algebra covering the algebra of projections has no one-element generating set, then it contains at least two atoms and, hence, is of the form (i). Suppose that $\mathbf{C}$ covers $\mathbf{J}_M$ and $\mathbf{C} = \langle f \rangle$. Assume that $\sigma(f) \neq 0$ or $\beta(f) \neq 0$. Identifying all variables of f, we get the function $\overline{f} = \alpha x + b$ which generates a minimal subgroup of the symmetric group on A. Hence, $\overline{f}^q = x$ for some prime q. Since $\overline{f}^q = \alpha^q x + (1 + \alpha + \ldots + \alpha^{q-1})b$, we have either $\alpha \neq 1$, α is of prime order q and $(1 + \alpha + \ldots + \alpha^{q-1})b = 0$ or both $\alpha = 1$ and $q \cdot b = 0$. In each case $\mathbf{C}$ is of type (iii).

Finally, the case when $\sigma(f) = 0$, $\beta(f) = 0$, i.e. f is idempotent, was considered in [5]. $\square$

2.2. Types of functions and corresponding "small" algebras.

The statements below answer the following question: what atoms and covering elements of atoms of Sub $\mathbf{L}_M$ are contained in certain algebra from Sub $\mathbf{L}_M$? For any linear function $f = \sum_{i=1}^n \alpha_i x_i + b$, the sequence $(\varepsilon_1, \ldots, \varepsilon_n)$ of idempotents of R such that $\varepsilon_i = \alpha_i^{n_i}$ for some n_i is denoted by $\mathrm{ID}(f)$. We treat the set of idempotents $\mathrm{E}(R)$ as partially ordered with the natural order: $\varepsilon \leq \varepsilon'$ if and only if $\varepsilon\varepsilon' = \varepsilon$. This order is a lattice one and $\varepsilon \wedge \varepsilon' = \varepsilon\varepsilon'$, $\varepsilon \vee \varepsilon' = \varepsilon + (1 - \varepsilon)\varepsilon'$ for any $\varepsilon, \varepsilon' \in \mathrm{E}(R)$. Let R_f be the subring of R generated by $\alpha_1, \ldots, \alpha_n$. The greatest idempotent of R_f is denoted by $\mathrm{Id}(f)$.

Lemma 1 *For a function $f = \sum_{i=1}^n \alpha_i x_i + b$ the equality*

$$\mathrm{Id}(f) = \varepsilon_1 + (1 - \varepsilon_1)\varepsilon_2 + (1 - \varepsilon_1)(1 - \varepsilon_2)\varepsilon_3 + \ldots + (1 - \varepsilon_1) \ldots (1 - \varepsilon_{n-1})\varepsilon_n \quad (1)$$

where $(\varepsilon_1, \ldots, \varepsilon_n) = \mathrm{ID}(f)$ *is valid.*

Proof. We need to prove that the expression in the right side of (1) is an idempotent and, for each i $(1 \le i \le n)$,

$$\varepsilon_i(\varepsilon_1 + (1-\varepsilon_1)\varepsilon_2 + (1-\varepsilon_1)(1-\varepsilon_2)\varepsilon_3 + \ldots + (1-\varepsilon_1)\ldots(1-\varepsilon_{n-1})\varepsilon_n) = \varepsilon_i$$

holds. Both conditions follow from the equations $\varepsilon(1-\varepsilon) = 0$, $(1-\varepsilon)^2 = 1-\varepsilon$, $\varepsilon\varepsilon' + (1-\varepsilon)\varepsilon = \varepsilon$ where $\varepsilon, \varepsilon' \in \mathrm{E}(R)$. □

If $\mathrm{Id}(f) = 1$, then the ideal $R_f R$ generated by $\alpha_1, \ldots, \alpha_n$ is equal to R. Conversely, if $1 \in R_f R$, then there exists an invertible element α in R_f. So we get the following lemma.

Lemma 2 *Let f be a linear function. The equality* $\mathrm{Id}(f) = 1$ *holds if and only if the coefficients of f are not contained in any proper ideal of R.*

Proposition 3 *Let $f \in L_M^{(n)}$ be a function satisfying the conditions:*

(i) $\mathrm{Id}(f) = 1$,

(ii) either $\mathrm{ID}(f)$ *contains a proper idempotent or both* $\mathrm{char}\, R$ *is not prime power and there are at least two occurences of* 1 *in the sequence* $\mathrm{ID}(f)$.

Then there exists $\varepsilon \in \mathrm{E}(R)$, $\varepsilon \neq 0, 1$, such that the function $\varepsilon x + (1-\varepsilon)y$ belongs to $\langle f \rangle$.

Proposition 4 *If* $\mathrm{Id}(f) = \varepsilon$ *holds for a function f where $\varepsilon \neq 0, 1$, then there exists $b \in M$ such that the function $h = \varepsilon x + (1-\varepsilon)b$ belongs to $\langle f \rangle$.*

Proposition 5 *If the sequence* $\mathrm{ID}(f)$ *where f is a nonunary function has at least two occurences of* 1, *then the function $x - y + z$ belongs to $\langle f \rangle$.*

Propositions 3–5 are auxiliary statements and their proof play no role in the sequel, so we prove them in §4.

§3. Types of algebras and corresponding lattices

In this section we construct a partition of Sub $\mathbf{L}_M$ into four parts and study some properties of three of them. The main results concerning the properties of the classes of this partition are Theorems 1 and 2. Besides we illustrate some applications of the partition and describe all coatoms of Sub $\mathbf{L}_M$ (Theorem 3).

3.1. Types of algebras and parts of Sub $\mathbf{L}_M$.

Any function f such that $Id(f) = 1$ and $\mathrm{ID}(f)$ has a unique nonzero member will be called *primitive*. Thus a primitive function has a unique invertible coefficient and the others are nilpotent elements. We denote by $\mathbf{LP}_M$ the set of all primitive functions. By a *nilpotent* function is meant a function whose coefficients are nilpotent elements. So, a nilpotent function f satisfies the condition $\mathrm{Id}(f) = 0$. The set of all nilpotent functions will be denoted by $\mathbf{N}_M$. The following statement is straightforward.

Proposition 6 *$\mathbf{LP}_M$, $\mathbf{N}_M$ and $\mathbf{NP}_M = \mathbf{N}_M \cup \mathbf{LP}_M$ are subalgebras of $\mathbf{L}_M$.*

Further, we write $\mathbf{I}_M$ for the subset of $\mathbf{L}_M$ consisting of all functions f such that all coefficients of f belong to some proper ideal of R and $\mathbf{PI}_M$ for the set $\mathbf{I}_M \cup \mathbf{LP}_M$.

Remark 1 *By Lemma 1, $f \in \mathbf{PI}_M$ if and only if $\mathrm{Id}(f) \neq 1$ or $\mathrm{ID}(f)$ has a unique nonzero element.*

Proposition 7 *(1) $\mathbf{I}_M$ and $\mathbf{PI}_M$ are iterative algebras.*
(2) $\mathbf{PI}_M$ is a coatom of Sub $\mathbf{L}_M$.

Proof.
It is easy to show that $\mathbf{I}_M$ is closed under operations of the iterative algebra. Take $f_1, f_2 \in \mathbf{PI}_M$. Permutations, identification of variables, and adding of fictitious argument preserve $\mathbf{PI}_M$. Since $\mathbf{I}_M$ and $\mathbf{LP}_M$ are algebras, we have to consider two cases only. If $f_1 \in \mathbf{I}_M$ and $f_2 \in \mathbf{LP}_M$, then all coefficients of $f_1 \circ f_2$ belong to the same ideal of R as coefficients of f_1. Hence, $f_1 \circ f_2 \in \mathbf{I}_M$. Assume that $f_1 \in \mathbf{LP}_M$ and $f_2 \in \mathbf{I}_M$, the coefficient of the first variable of f_1 is invertible and I is an ideal containing coefficients of f_2. Then all coefficients of $f_1 \circ f_2$ belong to the ideal generated by I together

with all nilpotent elements of R. So, $f_1 \circ f_2 \in \mathbf{I}_M$. Finally, if $f_1 \in \mathbf{LP}_M$, $f_2 \in \mathbf{I}_M$ and the coefficient of the first variable of f_1 is not invertible, then $f_1 \circ f_2$ is primitive. Thus $\mathbf{PI}_M$ is an iterative algebra.

To prove (2) take a function $f \in \mathbf{L}_M \backslash \mathbf{PI}_M$ and show that any function $g \in \mathbf{L}_M$ belongs to $\langle\{f\} \cup \mathbf{PI}_M\rangle$. Put $n = \mathrm{ar} g$. By Remark 1 and Propositions 3, 5 the algebra $\langle f\rangle$ contains either $\varepsilon x + (1-\varepsilon)y$ for some $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$ or the function $x - y + z$. In both cases $\langle\{f\} \cup \mathbf{PI}_M\rangle$ contains the function $h = x_1 + \ldots + x_n + \beta(g)$. To show this in the former case we substitute the functions $\varepsilon x_1 + \ldots + \varepsilon x_n + \beta(g)$, $(1-\varepsilon)x_1 + \ldots + (1-\varepsilon)x_n + \beta(g) \in \mathbf{PI}_M$ instead of variables x, y of $\varepsilon x + (1-\varepsilon)y$ and then identify some variables. In the latter case we take $x - y_1 - \ldots - y_{n-1} + z_1 + \ldots z_{n-1} \in \langle x - y + z\rangle$ and substitute the constant $0 \in \mathbf{PI}_M$ instead of $y_1, \ldots, y_n$ and the primitive function $x + \beta(g)$ instead of x. Finally, $g(x_1, \ldots, x_n) = h(\alpha_1 x_1, \ldots, \alpha_n x_n)$ where $\alpha_1, \ldots, \alpha_n$ are the coefficients of g. Since the functions $\alpha_i x_i$, $i \in \underline{n}$, either are primitive or belong to $\mathbf{I}_M$, the function g belongs to $\langle\{f\} \cup \mathbf{PI}_M\rangle$. This completes the proof of Proposition 7. $\square$

Now we are ready to introduce the partition of Sub $\mathbf{L}_M$ mentioned above. First we consider the following parts of Sub $\mathbf{L}_M$:

(1) the union of all intervals of the form $[\mathbf{C}, \mathbf{L}_M]$ where $\mathbf{C} = \langle\varepsilon x + (1-\varepsilon)y\rangle$ is a covering element of the algebra of projections of type (ii) for $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$ (such a union is called *upper pseudo-interval*);

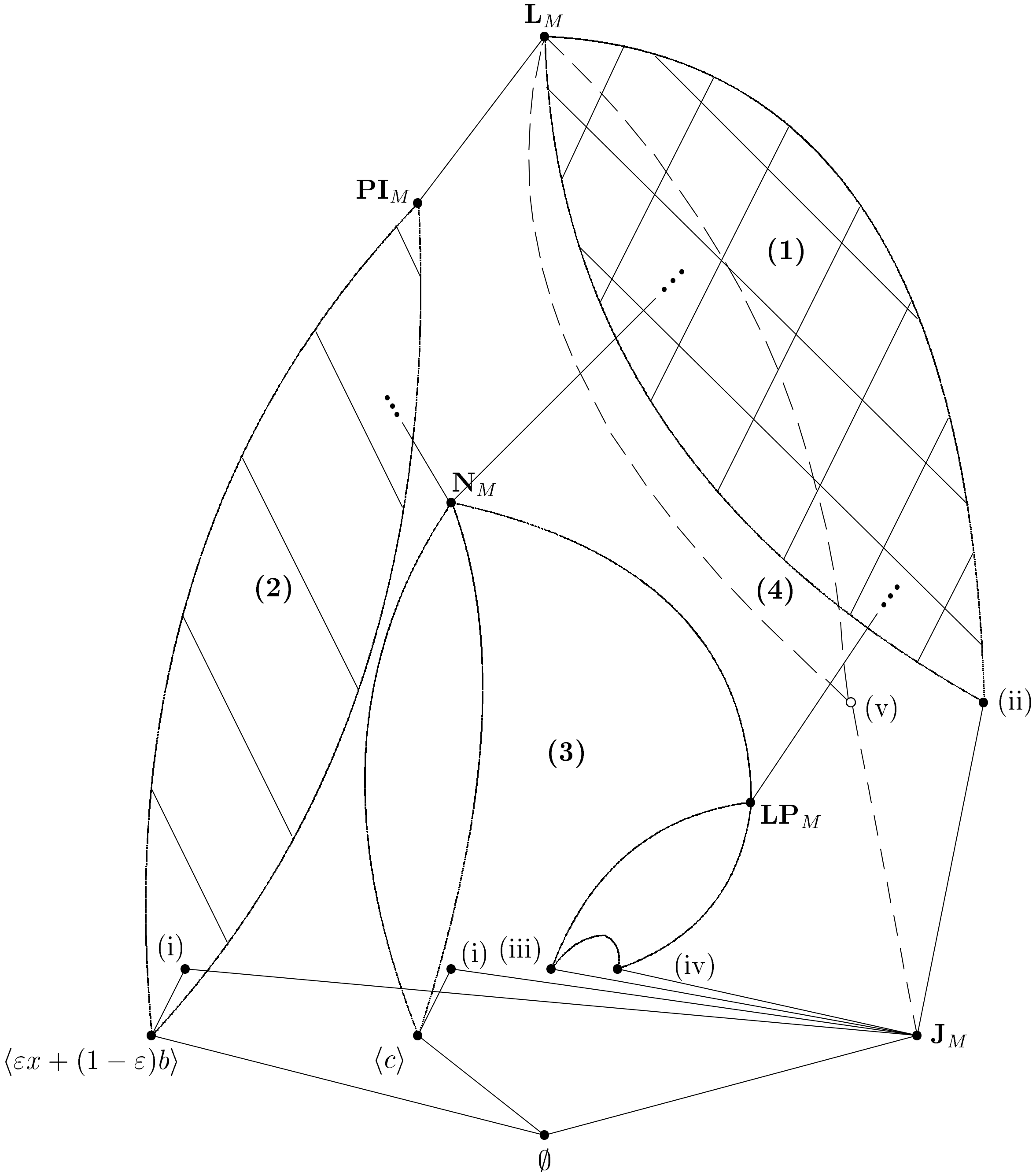
(2) the union of all intervals of the form $[D, \mathbf{L}_M]$ where $D = \langle\varepsilon x + (1-\varepsilon)b\rangle$ is an atom of type (iii) for $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$ and $b \in M$;

(3) the interval $[\emptyset, \mathbf{NP}_M]$;

(4) the interval $[\langle x - y + z\rangle, \mathbf{L}_M]$ (we consider this part only in the case when char R is a prime power).

The parts (1)–(4) cover Sub $\mathbf{L}_M$. Indeed, let $\mathbf{C} \in$ Sub $\mathbf{L}_M$. If there is f in $\mathbf{C}$ such that $\mathrm{Id}(f) = 1$ and f is not primitive, then f satisfies the conditions of Proposition 3 or of Proposition 5. Hence $\mathbf{C}$ belongs to part (1) or to part (4). If $\mathbf{C}$ contains a function f such that $\mathrm{Id}(f) = \varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$, then, by Proposition 4, $\mathbf{C}$ contains an atom of type (iii) and, consequently, $\mathbf{C}$ belongs to part (2). Finally, if $\mathbf{C}$ contains no function of these two kinds, then it consists of nilpotent (i.e. $\mathrm{Id}(f) = 0$) and primitive functions. So, $\mathbf{C} \in [\emptyset, \mathbf{NP}_M]$.

The parts (1)–(4) do not form a partition of Sub $\mathbf{L}_M$. Actually the



$\mathbf{L}_M$
$\mathbf{PI}_M$
(1)
(2)
$\mathbf{N}_M$
(4)
(3)
(v)
(ii)
$\mathbf{LP}_M$
(i)
(i)
(iii)
(iv)
$\langle \varepsilon x + (1-\varepsilon)b \rangle$
$\langle c \rangle$
$\mathbf{J}_M$
$\emptyset$

Fig. 1.

intersection of (1) and (2) as well as the intersection the one of (4) and any of (1)–(3) is not empty. Using the parts (1)–(4) we get a partition of Sub $\mathbf{L}_M$. For this we need description of the lattice $[\langle x-y+z\rangle, \mathbf{L}_M]$ given in [11, 10]. Let us recall it. Each clone from $[\langle x-y+z\rangle, \mathbf{L}_M]$ has a unique representation in the form

$$\mathbf{K}_M(R', M') = \{\sum_{i=1}^{n} \varrho_i x_i + a \mid n \geq 1,\ \varrho_1, \dots, \varrho_n \in R',\ (1 - \sum_{i=1}^{n} \varrho_i, a) \in M'\}$$

where R' is a unitary subring of R and M' is a submodule of R'-module $R' \times M$. Now, to get a partition of Sub $\mathbf{L}_M$ we have to restrict part (2) to the union of all intervals of the form $[\langle \varepsilon x + (1-\varepsilon)b\rangle, \mathbf{PI}_M]$ and replace part (4) by the union of all intervals of the form $[\langle x-y+z\rangle, \mathbf{K}_M(R', R' \times M)]$ where R' is an arbitrary maximal element of the set $\{S|S$ is a unitary subring of R and $\mathrm{E}(S) = \{0,1\}\}$. The upper bounds of intervals in the latter case are the maximal algebras of part (4) which do not belong to parts (1) and (2). In other words, for any element f of such an algebra, the sequence $\mathrm{ID}(f)$ has only trivial idempotents. If there is no ring R' satisfying conditions laid down above, then the algebra $\langle x-y+z\rangle$ belongs to part (1). The whole picture is presented in Fig.1.

3.2. Certain lattice properties of parts (1) and (2).

The complete description of $[\langle x-y+z\rangle, \mathbf{L}_M]$ was given in [11, 10]. In this section we find some properties of intervals of the forms $[\langle \varepsilon x + (1-\varepsilon)y\rangle, \mathbf{L}_M]$ and $[\langle \varepsilon x + (1-\varepsilon)b\rangle, \mathbf{L}_M]$.

In [6], the direct product of functions and iterative algebras was defined in the following way. Let a set A be Cartesian product of the sets A_1 and A_2. The direct product of the functions $f_1 \in \mathbf{P}_{A_1}^{(n)}$ and $f_2 \in \mathbf{P}_{A_2}^{(n)}$ is the function $f \in \mathbf{P}_A^{(n)}$ defined by the equality

$$f((b_1, c_1), \dots, (b_n, c_n)) = (f(b_1, \dots, b_n), f(c_1, \dots, c_n))$$

for arbitrary $b_1, \dots, b_n \in A_1,\ c_1, \dots, c_n \in A_2$. In this case we shall write $f = f_1 \times f_2$. The iterative algebra

$\mathbf{C} = \{f_1 \times f_2 \mid f_1 \in \mathbf{C}_1^{(n)}, f_2 \in \mathbf{C}_2^{(n)}, n \in \mathbb{N}\}$ is the direct product of iterative algebras $\mathbf{C}_1 \in \mathbf{L}_{A_1}$, $\mathbf{C}_2 \in \mathbf{L}_{A_2}$ and is denoted by $\mathbf{C}_1 \times \mathbf{C}_2$. It is easy to see that this notion of direct product of iterative algebras is not identical to their direct product as universal algebras.

It is well known that, for any idempotent ε of R such that $\varepsilon \neq 0, 1$, we can represent the module M as the direct sum of two submodules $\varepsilon M \oplus (1-\varepsilon)M$ (this is the so-called Peirce decomposition). Further, each function $f = \sum_{i=1}^{n} \alpha_i x_i + a \in \mathbf{L}_M$ can be represented as $f = f_1 \times f_2$ where $f_1 = \sum_{i=1}^{n} \alpha_i x_i + \varepsilon a$ and $f_2 = \sum_{i=1}^{n} \alpha_i x_i + (1-\varepsilon)a$ are functions on the sets εM and $(1-\varepsilon)M$, respectively. To show this take $(b_1, c_1), \dots, (b_n, c_n) \in M = \varepsilon M \times (1-\varepsilon)M$. Then

$$\begin{aligned}
& f((b_1, c_1), \dots, (b_n, c_n)) = \\
&= f(b_1 + c_1, \dots, b_n + c_n) = \\
&= \sum_{i=1}^{n} \alpha_i (b_i + c_i) + a = \\
&= \sum_{i=1}^{n} \varepsilon \alpha_i (b_i + c_i) + \varepsilon a + \sum_{i=1}^{n} (1-\varepsilon) \alpha_i (b_i + c_i) + (1-\varepsilon)a = \\
&= \sum_{i=1}^{n} \alpha_i b_i + \varepsilon a + \sum_{i=1}^{n} \alpha_i c_i + (1-\varepsilon)a = \\
&= (f_1(b_1, \dots, b_n), f_2(c_1, \dots, c_n)).
\end{aligned}$$

Conversely, the function $f = f_1 \times f_2 = \sum_{i=1}^{n} (\varepsilon \gamma_i + (1-\varepsilon)\zeta_i) x_i + (b + c)$ corresponds to the given pair of functions $f_1 = \sum_{i=1}^{n} \gamma_i x_i + b \in \mathbf{L}_{\varepsilon M}$, $f_2 = \sum_{i=1}^{n} \zeta_i x_i + c \in \mathbf{L}_{(1-\varepsilon)M}$. The modules εM, $(1-\varepsilon)M$ can be considered as εR- and $(1-\varepsilon)R$-modules, respectively. So, $\mathbf{L}_M = \mathbf{L}_{M_1} \times \mathbf{L}_{M_2}$ where $M_1 = \varepsilon M$ is an εR-module and $M_2 = (1-\varepsilon)M$ is an $(1-\varepsilon)R$-module. Let $\mathbf{C}$ be an algebra of all functions preserving the kernels of projections of A onto A_1 and A_2. In [6](sec.3.3), it was noted that the interval $[\mathbf{J}_{A_1} \times \mathbf{J}_{A_2}, \mathbf{C}]$ can be decomposed into the direct product $[\mathbf{J}_{A_1}, \mathbf{P}_{A_1}] \times [\mathbf{J}_{A_2}, \mathbf{P}_{A_2}]$. Using this decomposition we obtain the next statement.

Theorem 1 *For any* $\varepsilon \in \mathrm{E}(R)$,

(1) if the function $\varepsilon x + (1-\varepsilon)y$ *belongs to an iterative algebra* $\mathbf{L} \in \mathrm{Sub}\, \mathbf{L}_M$, *then* $\mathbf{L} = \mathbf{L}_1 \times \mathbf{L}_2$ *where* $\mathbf{L}_1$, $\mathbf{L}_2$ *are subalgebras of* $\mathbf{L}_{\varepsilon M}$ *and* $\mathbf{L}_{(1-\varepsilon)M}$ *respectively and* $\mathbf{L}_1, \mathbf{L}_2$ *both contain all projections;*

(2) $[\langle \varepsilon x + (1-\varepsilon)y \rangle, \mathbf{L}_M] \cong [\mathbf{J}_{\varepsilon M}, \mathbf{L}_{\varepsilon M}] \times [\mathbf{J}_{(1-\varepsilon)M}, \mathbf{L}_{(1-\varepsilon)M}]$.

Thus the structure of the part (1) of $\mathrm{Sub}\, \mathbf{L}_M$ is completely determined by the structure of lattices $\mathrm{Sub}\, \mathbf{L}_{M'}$ for smaller modules M'.

Now let $\mathfrak{A}$ be a finite (universal) algebra (with the universe A) and $\mathfrak{B}$ be its homomorphic image (with the universe B) under a homomorphism φ. We assume that B is a quotient set of A by the kernel of φ. It is easy to verify that the clone of term operations of $\mathfrak{B}$ (Clo $\mathfrak{B}$ in symbols) is an image of Clo $\mathfrak{A}$ under the clone homomorphism $\overline{\varphi}$ where $\overline{\varphi}$ is defined by the equality

$$(\overline{\varphi}(f))(\varphi(x_1),\dots,\varphi(x_n)) = \varphi(f(x_1,\dots,x_n)).$$

Here we use the notion of a homomorphism of iterative algebras or clones in the common sence, i.e. as a homomorphism of universal algebras. Let t be a function on A that maps each element of a class of the equivalence relation $\ker\varphi$ to a fixed element of the same class. The function t is an idempotent of the symmetric semigroup on A. Suppose $t \in \mathrm{Clo}\ \mathfrak{A}$. Let $\overline{\overline{\varphi}}_t : [\langle t\rangle, \mathrm{Clo}\ \mathfrak{A}] \to [\mathbf{J}_B, \mathrm{Clo}\ \mathfrak{B}]$ be a mapping defined by $\overline{\overline{\varphi}}(\mathbf{C}) = \{\overline{\varphi}(f) \mid f \in \mathbf{C}\}$ for any $\mathbf{C} \in [\langle t\rangle, \mathrm{Clo}\ \mathfrak{A}]$.

Proposition 8 *If $t \in \mathrm{Clo}\ \mathfrak{A}$, then $\overline{\overline{\varphi}}_t$ is a surjective lattice homomorphism.*

Proof.
To show that $\overline{\overline{\varphi}}_t$ is a mapping to $[\mathbf{J}_B, \mathrm{Clo}\ \mathfrak{B}]$ we note that $\overline{\overline{\varphi}}_t(\mathrm{Clo}\ \mathfrak{A}) = \mathrm{Clo}\ \mathfrak{B}$, $\overline{\overline{\varphi}}(\langle t\rangle) = \mathbf{J}_B$ and $\overline{\overline{\varphi}}_t$ is monotone. For any $\overline{\mathbf{C}}\in[\mathbf{J}_B, \mathrm{Clo}\ \mathfrak{B}]$, the set $\mathbf{C} = \{f \mid \overline{\varphi}(f) \in \overline{\mathbf{C}}\}$ is a clone and, since $\overline{\varphi}(t) = e_1^1$, the operation t belongs to $\mathbf{C}$. Thus $\overline{\overline{\varphi}}_t$ is surjective.

Since $\overline{\varphi}$ is a homomorphism, $\overline{\overline{\varphi}}_t(\mathbf{C}_1 \vee \mathbf{C}_2) = \overline{\overline{\varphi}}_t(\mathbf{C}_1) \vee \overline{\overline{\varphi}}_t(\mathbf{C}_2)$ holds for any clones $\mathbf{C}_1, \mathbf{C}_2 \subseteq \mathrm{Clo}\ \mathfrak{A}$ such that $t \in \mathbf{C}_1, \mathbf{C}_2$. Let us prove that the equality $\overline{\overline{\varphi}}_t(\mathbf{C}_1 \wedge \mathbf{C}_2) = \overline{\overline{\varphi}}_t(\mathbf{C}_1) \wedge \overline{\overline{\varphi}}_t(\mathbf{C}_2)$ is valid. The inclusion $\overline{\overline{\varphi}}_t(\mathbf{C}_1 \wedge \mathbf{C}_2) \subseteq \overline{\overline{\varphi}}_t(\mathbf{C}_1) \wedge \overline{\overline{\varphi}}_t(\mathbf{C}_2)$ is obvious. To check the reverse inclusion let us take $f \in \overline{\overline{\varphi}}_t(\mathbf{C}_1) \wedge \overline{\overline{\varphi}}_t(\mathbf{C}_2)$. There exist $f_1 \in \mathbf{C}_1$ and $f_2 \in \mathbf{C}_2$ such that $f = \overline{\varphi}(f_1) = \overline{\varphi}(f_2)$. Hence, $\overline{\varphi}(t(f_1)) = \overline{\varphi}(t(f_2)) = f$. Therefore, for any $\alpha_1,\dots,\alpha_n \in A$, we have $(f_1(\alpha_1,\dots,\alpha_n), f_2(\alpha_1,\dots,\alpha_n)) \in \ker\varphi$ and then $t(f_1(a_1,\dots,a_n)) = t(f_2(a_1,\dots,a_n))$, i.e. $t(f_1) = t(f_2)$. Thus $t(f_1) \in \mathbf{C}_1 \wedge \mathbf{C}_2$ and $f = \overline{\varphi}(t(f_1)) \in \overline{\overline{\varphi}}(\mathbf{C}_1 \wedge \mathbf{C}_2)$. Proposition 8 is proved. □

Let $\varphi_\varepsilon : M \to \varepsilon M$ be a homomorphism which maps an element $a \in M$ to εa and let $t_{\varepsilon,b} = \varepsilon x + (1-\varepsilon)b$ where $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$, $b \in M$. Note that εM can be treated as an εR-module. If $\varepsilon a_1 = \varepsilon a_2$ for $a_1, a_2 \in M$, then $t_{\varepsilon,b}(a_1) = \varepsilon a_1 + (1-\varepsilon)b = \varepsilon a_2 + (1-\varepsilon)b = t_{\varepsilon,b}(a_2)$ and $\varepsilon \cdot t_{\varepsilon,b}(a_1) = \varepsilon^2 a_1 + \varepsilon(1-\varepsilon)b = \varepsilon a_1$. We see that, taking φ_ε as φ, we can take $t_{\varepsilon,b}$ as t in Proposition 8 to obtain the next statement.

Theorem 2 *Let $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$ and $b \in M$.*

(1) If $\mathbf{L} \subseteq \mathbf{L}_M$ is an iterative algebra and $t_{\varepsilon,b} \in \mathbf{L}$, then a mapping $\overline{\varphi}_\varepsilon \colon \mathbf{L} \to \mathbf{L}'$ defined by the formula $\overline{\varphi}_\varepsilon(f) = \varepsilon f$ is a homomorphism onto the subalgebra $\mathbf{L}'$ of $\mathbf{L}_{\varepsilon M}$, and $\mathbf{L}'$ contains all projections;

(2) A mapping $\overline{\overline{\varphi}}_{\varepsilon,b} : [\langle t_{\varepsilon,b}\rangle, \mathbf{L}_M] \to [T_{\varepsilon M}, \mathbf{L}_{\varepsilon M}]$ that takes any $\mathbf{C} \in [\langle t_{\varepsilon,b}\rangle, \mathbf{L}_M]$ to $\{\varepsilon f \mid f \in \mathbf{C}\}$ is a surjective lattice homomorphism.

To illustrate the properties of the parts (1)–(4), let us study a relationship between the properties of R and the cardinalities of (1)–(4). Results of [11, 10] imply that the part (4) is always finite. If R contains no nilpotent element, then R is a direct sum of fields. So by results of [10], Sub $\mathbf{L}_M$ and, hence, the parts (1)–(3) are finite. If R contains a nilpotent element but $\mathrm{E}(R) = \{0,1\}$, then (1) and (2) are empty and the interval $[\emptyset, \mathbf{NP}_M]$ is infinite. Finally, if there exists a proper idempotent and a nilpotent element in R, then, for some $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$ and some nilpotent element ϱ, we have that $\varepsilon\varrho$ is a nilpotent element, but $\varepsilon\varrho \neq 0$. So εR contains a nilpotent element and, by Theorems 1, 2, it follows that the parts (1),(2), for such an idempotent ε and $b \in M$, are infinite.

Theorem 1 shows that one can derive all information about algebras of the part (1) by studying algebras of the parts (2) and (3) for modules which are smaller than M. Thus the structure of the part (1) is completely determined by the structure of lattices of iterative algebras for smaller modules. The information given by Theorem 2 is much poorer. Concerning the homomorphism $\overline{\overline{\varphi}}_{\varepsilon,b}$ pointed in Theorem 2 we see that the classes of its kernel are not necessarily finite. When R contains a nilpotent element it is not very hard to construct an infinite class of such a type. So, the study of the part (2) should be continued.

3.3. Coatoms of Sub $\mathbf{L}_M$.

As an application of established properties of Sub $\mathbf{L}_M$, we give the list of its coatoms. By Remark 1 and Propositions 3, 5 each coatom of Sub $\mathbf{L}_M$ except $\mathbf{PI}_M$ contains a covering element of $\mathbf{J}_M$ of type (ii) or of type (v). The latter case is possible when char R is a prime power, and here the list of coatoms containing the function $x - y + z$ can be derived from results of [11, 10].

Theorem 3 *The set of coatoms of* $\mathrm{Sub}\,\mathbf{L}_M$ *consists exactly of the following clones:*

(1) $\mathbf{PI}_{\varepsilon M} \times \mathbf{L}_{(1-\varepsilon)M}$ *where* $\varepsilon \in \mathrm{E}(R)\backslash\{0\}$*;*

(2) $\mathbf{K}_{\varepsilon M}(R', R' \times \varepsilon M) \times \mathbf{L}_{(1-\varepsilon)M}$ *where* $\varepsilon \in \mathrm{E}(R)\backslash\{0\}$*,* R' *is a maximal unitary subring of* εR *without proper idempotents;*

(3) $\mathbf{K}_{\varepsilon M}(\varepsilon R, M') \times \mathbf{L}_{(1-\varepsilon)M}$ *where* $\varepsilon \in \mathrm{E}(R)\backslash\{0\}$ *is a minimal idempotent and* M' *is a maximal submodule of* $\varepsilon R \times \varepsilon M$*.*

Proof.

First we show that each coatom is of type (1), (2), or (3). We prove this by induction on the number of idempotents of R. If $\mathrm{E}(R) = \{0, 1\}$, then the part (1) is empty and, by Propositions 5, 7, the algebra $\mathbf{PI}_M$ is the only coatom that does not belong to the interval $[\langle x - y + z\rangle, \mathbf{L}_M]$. Using the results of [11, 10], we see that all coatoms are of types (1)–(3) with $\varepsilon = 1$. So, the base of induction is proved.

Induction step. Let R be a finite ring and, for any ring S with $|\mathrm{E}(R)| > |\mathrm{E}(S)|$ and any S-module M', let all coatoms of $\mathrm{Sub}\,\mathbf{L}_{M'}$ be of types (1)–(3). Let $\mathbf{C}$ be a coatom of $\mathrm{Sub}\,\mathbf{L}_M$. We have to consider two cases.

Case 1. There is no $\varepsilon \in \mathrm{E}(R)\backslash\{0, 1\}$ such that the function $\varepsilon x + (1-\varepsilon)y$ belongs to $\mathbf{C}$. Then $\mathbf{C}$ coincides either with $\mathbf{PI}_M$ or with $\mathbf{K}_M(R', R' \times M)$ where R' is a maximal unitary subring of R without proper idempotents. Indeed, since $\varepsilon x + (1 - \varepsilon)y \notin \mathbf{C}$ for all $\varepsilon \in \mathrm{E}(R)$, $\mathbf{C} \neq \mathbf{PI}_M$ implies $x - y + z \in \mathbf{C}$ by Remark 1 and Proposition 5. Hence, $\mathbf{C}$ is either of the form $\mathbf{K}_M(R', R' \times M)$ or of the form $\mathbf{K}_M(R, M')$. Since, for all $\varepsilon \in \mathrm{E}(R)$, the function $\varepsilon x + (1 - \varepsilon)y$ does not belong to $\mathbf{C}$, in the former case R' has no proper idempotent. Similarly, the latter case is impossible. Thus, in Case 1 the algebra $\mathbf{C}$ is of the type (1) or (2) for $\varepsilon = 1$.

Case 2. There is $\varepsilon \in \mathrm{E}(R)\backslash\{0, 1\}$ such that $\varepsilon x + (1 - \varepsilon)y$ belongs to $\mathbf{C}$. Then by Theorem 1 we have $\mathbf{C} = \mathbf{C}_1 \times \mathbf{C}_2$ where $\mathbf{C}_1 \subseteq \mathbf{L}_{\varepsilon M}$, $\mathbf{C}_2 \subseteq \mathbf{L}_{(1-\varepsilon)M}$. Further, since $\mathbf{C}$ is a coatom, either $\mathbf{C}_1 = \mathbf{L}_{\varepsilon M}$ or $\mathbf{C}_2 = \mathbf{L}_{(1-\varepsilon)M}$ holds. Without loss of generality we put $\mathbf{C}_2 = \mathbf{L}_{(1-\varepsilon)M}$. Then $\mathbf{C}_1$ is a coatom of $\mathrm{Sub}\,\mathbf{L}_{\varepsilon M}$ and εR has less number of idempotents than R. By the induction hypotesis $\mathbf{C}_1$ is of type (1)–(3) for some $\varepsilon' \in \mathrm{E}(\varepsilon R)\backslash\{0\}$.Thus, we have $\mathbf{C} = \mathbf{C}' \times \mathbf{L}_{(1-\varepsilon')\varepsilon M} \times \mathbf{L}_{(1-\varepsilon)M}$ where $C' \in \{\mathbf{PI}_{\varepsilon'\varepsilon M}, \mathbf{K}_{\varepsilon'\varepsilon M}(R', R' \times \varepsilon'\varepsilon M), \mathbf{K}_{\varepsilon'\varepsilon M}(\varepsilon'\varepsilon R, M)\}$, and R' and M' satisfy the conditions of types (2), (3) for the ring $\varepsilon'\varepsilon R$ and the module $\varepsilon'\varepsilon R \times \varepsilon'\varepsilon M$. The equality $\mathbf{L}_{(1-\varepsilon')\varepsilon M} \times \mathbf{L}_{(1-\varepsilon)M} = \mathbf{L}_{((1-\varepsilon)+\varepsilon(1-\varepsilon'))M}$ implies that $\mathbf{C}$ is also of one of the types (1)–(3).

Conversely, if $\mathbf{C}$ is of one of the types (1)–(3) for $\varepsilon = 1$, then $\mathbf{C}$ is a coatom by Proposition 7 or by results of [11, 10]. If $\varepsilon \neq 1$, then $\mathbf{C}$ is a coatom in the direct decomposition pointed in Theorem 1. Theorem 3 is proved. $\square$

§4. Proof of Propositions 3–5

To prove Propositions 3–5 we need two lemmas

Lemma 3 *Let $f = \varepsilon x + \alpha y + \sum_{i=1}^{n} \alpha_i z_i + b$ where $\varepsilon \in \mathrm{E}(R)\backslash\{0,1\}$. Then there exist $\gamma \in R$ and $b' \in M$ such that the function $g = \varepsilon x + (1-\varepsilon)\alpha y + \sum_{i=1}^{n} \alpha_i z_i + \gamma z_{n+1} + b'$ belongs to $\langle f \rangle$.*

Proof.
Let t be the additive order of $\varepsilon\alpha$. Put

$$\overline{f} = \underbrace{f \circ f \circ \ldots \circ f}_{t-1 \text{ times}} = \varepsilon x + \sum_{i=1}^{t-1} \varepsilon\alpha y_i + \alpha y + \sum_{i=1}^{n} \alpha_i z_i + \sum_{i=n+1}^{m} \gamma_i z_i + b'$$

for suitable $m \in \mathbb{N}$, $\gamma_i \in R$ $(n+1 \leq i \leq m)$ and $b' \in M$. We identify all y_i $(i \in \underline{t-1})$ with y, and all z_i $(i \in \{n+1, \ldots, m\})$ with z_{n+1}. Since $\alpha = \varepsilon\alpha + (1-\varepsilon)\alpha$, we have

$$g = \varepsilon x + (1-\varepsilon)\alpha y + \sum_{i=1}^{n} \alpha_i z_i + \gamma z_{n+1} + b' \in \langle f \rangle,$$

as desired. $\square$

Lemma 4 *Let $f(x_1, \ldots, x_n) \in \mathbf{L}_M$ and $\mathrm{ID}(f) = (\varepsilon_1, \ldots, \varepsilon_n)$. Then there exist $\gamma \in R$ and $d \in M$ such that the function $\sum_{i=1}^{n} \varepsilon_i x_i + \gamma x_{n+1} + d$ belongs to $\langle f \rangle$.*

Proof.
Let $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \alpha_i x_i + b$. We prove by induction that, for each l $(0 \leq l \leq n)$, a function of the form

$$f_l(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{l} \varepsilon_i x_i + \sum_{i=l+1}^{n} \alpha_i x_i + \gamma_l x_{n+1} + b_l$$

with $\gamma_l \in R$ and $b_l \in M$ belongs to $\langle f \rangle$. For $l = 0$, we can select $f_0 = \nabla f$ ($\gamma_0 = 0$, $b_0 = b$). So suppose that some f_l belongs to $\langle f \rangle$, and show that there exists an f_{l+1} of the required form such that $f_{l+1} \in \langle f \rangle$. For $g \in \mathbf{P}_M^{(n)}$ the symbol $\circ_s$ denote substitution instead of the s-th variable that is

$$(g \circ_s h)(x_1, \ldots, x_{n+m-1}) = g(x_1, \ldots, x_{s-1}, h(x_s, \ldots, x_{s+m-1}), x_{s+1}, \ldots, x_{n+m-1})$$

with $h \in P_M^{(m)}$. Put $\overline{f}_l = \underbrace{f_l \circ_{l+1} f_l \circ \ldots \circ_{l+1} f_l}_{t \text{ times}}$ where t is the order of α_{l+1}, i.e. $\alpha_{l+1}^t = \varepsilon_{l+1}$. For a suitable indexing of variables, we have

$$\begin{aligned}\overline{f}_l(x_1, \ldots, x_{n+1}, y_1, \ldots, y_{nt-n}) &= \sum_{i=1}^{l} \varepsilon_i x_i + \alpha_{l+1}^t x_{l+1} + \sum_{i=l+2}^{n} \alpha_i x_i + \\ &+ \sum_{i=1}^{nt-n} \zeta_i y_i + \gamma_l x_{n+1} + b_{l+1} \in \langle f \rangle.\end{aligned}$$

Now, $f_{l+1} = \sum_{i=1}^{l+1} \varepsilon_i x_i + \sum_{i=l+2}^{n} \alpha_i x_i + \gamma_{l+1} x_{n+1} + b_{l+1}$ is derived from $\overline{f}_l$ by identification of y_i, $i \in \underline{nt-n}$. A function f_n is required. $\square$

Proof of Proposition 3. By Lemma 4 there exists a function $g(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n} \varepsilon_i x_i + \alpha y + b$ where $\mathrm{ID}(f) = (\varepsilon_1, \ldots, \varepsilon_n)$, $\alpha \in R$, $b \in M$ such that $g \in \langle f \rangle$. We prove by induction that, for each l ($1 \leq l \leq n$), a function of the form

$$\begin{aligned} g_l &= \varepsilon_1 x_1 + \ldots + \varepsilon_l x_l + (1 - \varepsilon_l)\varepsilon_{l+1} x_{l+1} + \ldots + \\ &\quad + (1 - \varepsilon_l) \ldots (1 - \varepsilon_{n-1})\varepsilon_n x_n + \alpha_l y + c_l \in \langle f \rangle \end{aligned}$$

with $\alpha_l \in R$ and $c_l \in M$ belongs to $\langle f \rangle$. Put $g_n = g \in \langle f \rangle$. Now suppose that some f_l belongs to $\langle f \rangle$. Applying Lemma 3 $n - l$ times, we get the function

$$\begin{aligned} g_{l-1} &= \varepsilon_1 x_1 + \ldots + \varepsilon_{l-1} x_{l-1} + (1 - \varepsilon_{l-1}) x_{l-1} + \ldots + \\ &+ (1 - \varepsilon_{l-1}) \ldots (1 - \varepsilon_{n-1}) \varepsilon_n x_n + \alpha_{l-1} y + c_{l-1} \end{aligned}$$

for some $\alpha_{l-1} \in R$ and $c_{l-1} \in M$. Thus

$$g_1 = \varepsilon_1 x_1 + (1 - \varepsilon_1)\varepsilon_2 x_2 + \ldots + (1 - \varepsilon_1) \ldots (1 - \varepsilon_{n-1}) \varepsilon_n x_n + \alpha_1 y + b_1$$

belongs to $\langle f \rangle$.

By Lemma 1 the condition $\mathrm{Id}(f) = 1$ implies that $\varepsilon_1 + (1-\varepsilon_1)\varepsilon_2 + \ldots + (1-\varepsilon_1)\ldots(1-\varepsilon_{n-1})\varepsilon_n = 1$. If there exists $\varepsilon_i \in \mathrm{E}(R)$ such that $\varepsilon_i \neq 0, 1$ (without loss of generality we may assume that $i = 1$), then

$$\begin{aligned}\tilde{g} &= \varepsilon_1 x_1 + ((1-\varepsilon_1)\varepsilon_2 + \ldots + (1-\varepsilon_1)\ldots(1-\varepsilon_{n-1})\varepsilon_n)x_2 + \alpha_1 y + b_1 = \\ &= \varepsilon_1 x_1 + (1-\varepsilon_1)x_2 + \alpha_1 y + b_1\end{aligned}$$

belongs to $\langle f \rangle$. Otherwise g is of the form

$$g = x_1 + x_2 + \varepsilon_3 x_3 + \ldots + \varepsilon_n x_n + \alpha y + b.$$

Put $t = \operatorname{char} R$ and $g' = \underbrace{g \circ \ldots \circ g}_{t \text{ times}} = x_1 + x_2 + \ldots + x_{t+1} + \sum_{i=1}^{nt+n-t} \alpha_i y_i + b'$. Since $\operatorname{char} R$ is not a prime power, the element $\varepsilon = \underbrace{1 + \ldots + 1}_{q \text{ times}}$ is an idempotent for some $q < t$ and $\varepsilon \neq 1$. Identifying variables of g' in a suitable way, we produce a function of the form $\tilde{g} = \varepsilon x_1 + (1-\varepsilon)x_2 + \alpha' y + b'$ where $\alpha' \in R$.

In both cases the algebra $\langle f \rangle$ contains a function of the form

$$h_1 = \varepsilon x_1 + (1-\varepsilon)x_2 + \gamma y + d$$

with $\gamma \in R$, $d \in M$. Let r be the least common multiple of the additive orders of γ and d. Now, we shall construct the function h_r inductively. The function h_1 is already defined. Put

$$h_j = h_{j-1}(h_1(x_1, x_2, y), h_1(x_1, x_2, y), y).$$

It is easy to check that $h_j = \varepsilon x_1 + (1-\varepsilon)x_2 + j\gamma y + jd$. Therefore

$$h_r = \varepsilon x_1 + (1-\varepsilon)x_2 + r\gamma y + rd = \varepsilon x_1 + (1-\varepsilon)x_2.$$

Thus $h_r = \varepsilon x_1 + (1-\varepsilon)x_2 \in \langle f \rangle$. The proof is complete. $\square$

Proof of Proposition 4.

Let $\varepsilon_1, \ldots, \varepsilon_n$ be all non-zero elements of the sequence $\mathrm{ID}(f)$. By Lemma 4 a function of the form

$$\overline{f} = \sum_{i=1}^{n} \varepsilon_i x_i + \gamma y + b$$

where $\gamma \in R$ and $b \in M$, belongs to $\langle f\rangle$. Arguing as in the proof of Proposition 3, we have

$$\tilde{h} = \varepsilon_1 x_1 + (1-\varepsilon_1)\varepsilon_2 x_2 + \ldots + (1-\varepsilon_1)\ldots(1-\varepsilon_{n-1})\varepsilon_n x_n + \tilde{\gamma} y + \tilde{b} \in \langle f\rangle$$

for some $\tilde{\gamma} \in R$ and $\tilde{b} \in M$. Since $\varepsilon_1 + (1-\varepsilon_1)\varepsilon_2 + \ldots + (1-\varepsilon_1)\ldots(1-\varepsilon_{n-1})\varepsilon_n = \varepsilon$, by Lemma 1

$$g(x,y) = \tilde{h}(x,\ldots,x,y) = \varepsilon x + \tilde{\gamma} y + \tilde{b}$$

belongs to $\langle f\rangle$. If the element $(1-\varepsilon)\tilde{\gamma}$ is not nilpotent, then $\mathrm{Id}(f) > \varepsilon$. Hence, it is nilpotent; let t be its index. We produce by induction the fuction g_t putting

$$\begin{array}{rcl} g_1(x,y,z) & = & g(x,y) \\ & \vdots & \\ g_{i+1} & = & g_i(x, g(z,y), z) \end{array}$$

for each i $(1 \le i \le t)$. It is not hard to see that g_t is of the form $g_t = \varepsilon x + \tilde{\gamma}^t y + \varepsilon\gamma' z + b'$ for some $\gamma' \in R$ and $b' \in M$. Moreover $\tilde{\gamma}^t = (\varepsilon\tilde{\gamma} + (1-\varepsilon)\tilde{\gamma})^t = \varepsilon\tilde{\gamma}^t + ((1-\varepsilon)\tilde{\gamma})^t = \varepsilon\tilde{\gamma}^t$. Thus $g_t = \varepsilon x + \varepsilon\tilde{\gamma}^t y + \varepsilon\gamma' z + b' \in \langle f\rangle$; identifying y and z, we get $\overline{g} = \varepsilon x + \varepsilon\zeta y + (\varepsilon b' + (1-\varepsilon)b') \in \langle f\rangle$. Let r be the least common multiple of the additive orders of $\varepsilon\zeta$ and $\varepsilon b'$. Put

$$\tilde{g}(x, y_1, \ldots, y_r) = \underbrace{\overline{g} \circ \ldots \circ \overline{g}}_{r-1 \text{ times}} = \varepsilon x + \varepsilon\zeta y_1 + \varepsilon\zeta y_2 + \ldots + \varepsilon\zeta y_r + (r\varepsilon b' + (1-\varepsilon)b').$$

Therefore, the function

$$h(x) = \tilde{g}(x,\ldots,x) = \varepsilon x + (1-\varepsilon)b'$$

belongs to $\langle f\rangle$. This completes the proof. $\square$

Proof of Proposition 5.

By Lemma 4 there exist $\alpha \in R$, $b \in M$ such that the function $h(x,y,z) = x + y + \alpha z + b$ belongs to $\langle f\rangle$. Put $t = \mathrm{char}\, R \cdot |M|$. The sum of coefficients of the function

$$\overline{h} = \underbrace{h(h(\ldots h}_{t \text{ times}}(x,y,z),z,z),\ldots,z,z),z,z) = x + y + \beta z + \overline{b}$$

is equal to $t \cdot \sigma(h) + 1 = 1$, and $\overline{b} = t \cdot b = 0$. Thus $\overline{h}(x, y, z) = x + y - z$ and Proposition 5 is proved. $\square$

The author thanks participants of the seminar "Algebraic systems" under the supervision of Prof. L.N.Shevrin for fruitful discussions and especially A.Krokhin, V.Repnitskiĭ for useful remarks. Special thanks to A.Shur who read the manuscript.

References

[1] Bagyinszki J., Demetrovics J. *The lattice of linear classes in prime-valued logics.* Banach Center Publications, 1982, v.7, p.105–123.

[2] Lau D. *Über die Anzahl von abgeschlossenen Mengen linearer Funktionen der n-vertigen Logik.* EIK, 1978, v.14, no.11, p.561–563.

[3] Lau D. *Über abgeschlossenen Mengen linearer Funktionen in mehrwertigen Logiken.* EIK, 1988, v.24, no.7/8, p.367–381.

[4] Mal'tsev A.I. *Iterative algebras of Post.* Novosibirsk, 1976. (Russian)

[5] Pálfy P.P. *Minimal clones* preprint.

[6] Pöschel R., Kaluznin L.A. *Funktionen- und Relationenalgebren.* Ein Kapitel der diskreten Mathematik, Berlin: VEB DVW, 1979.

[7] Salomaa A.A. *On infinitely generated sets of operations in finite algebras.* Ann. Univ. Turku, Ser.AI 74, 1964, p.1–12.

[8] Szendrei Á. *Idempotent reducts of abelian groups* Acta sci. Math. (Szeged), 1976, v.38, p.171–182.

[9] Szendrei Á. *Idempotent reducts of modules I–II.* In: Universal Algebra (Proc. Conf. Esztergom, 1977), Colloq. Math. Soc. J.Bolyai, v.29, p.753–780.

[10] Szendrei Á. *Clones of linear operations on finite sets.* In: Finite algebra and multiple-valued logic. (Proc. Conf. Szeged (Hungary), 1979), Colloq. Math. Soc. J.Bolyai, v.28, p.693–738.

[11] SZENDREI Á. *On closed classes of quasylinear functions.* Cz̑echoslovak. Math. J., 1980, v.30, p.417–427.

Andrei A. Bulatov

Dept. of Algebra and Discrete Math.

Ural State University

Lenin av. 51

620083 Ekaterinburg

Russia

e-mail: Andrei.Bulatov@usu.ru