CONTRIBUTIONS TO GENERAL ALGEBRA 13
Proceedings of the Dresden Conference 2000
and the Summer School 1999
Verlag Johannes Heyn, Klagenfurt 2000

ON THE NUMBER OF FINITE MAL'TSEV ALGEBRAS

ANDREI BULATOV

Abstract. We study the problem: How many term (polynomially) inequivalent Mal'tsev algebras are there on a given base set? The answer is known for small base sets and for E-minimal Mal'tsev algebras.

AMS Mathematics Subject Classification: 08A40, 03B50.

1. Introduction and preliminaries

A *clone* on a finite set A is a set of operations on A closed under superposition and containing all projection operations. The well-known result of E.L.Post [15] gives a complete description of clones on a two-element set. There are countably infinitely many such clones. If A containes three or more elements, there exist uncountably many clones on A, as it was shown by Yu. Yanov and A. A. Muchnik in [16] and independently by A. Hulanicki and S. Świerczkowski in [10]. This fact leaves no hope of obtaining an acceptable classification of clones in this case. The gap between the numbers of clones on two- and three-element sets is much greater if we consider *polynomial* clones, that is clones containing all constant operations. Post's result shows that there are only 7 polynomial clones on a two-element set. On the other hand I.Ágoston, L.Demetrovics and L.Hannák [1] constructed uncountably many polynomial clones on a three-element set.

By $\mathsf{Clo}\ \mathbb{A}$ [$\mathsf{Pol}\ \mathbb{A}$] we denote the clone of all term [polynomial] operations of an algebra $\mathbb{A}$. Algebras $\mathbb{A}$ and $\mathbb{B}$ with the same universe are said to be *term* [*polynomially*] *equivalent* if $\mathsf{Clo}\ \mathbb{A} = \mathsf{Clo}\ \mathbb{B}$ [$\mathsf{Pol}\ \mathbb{A} = \mathsf{Pol}\ \mathbb{B}$]. Thus, the number of clones [polynomial clones] of a certain kind on a set A is equal to the number of term [polynomial] unequivalent algebras of that kind with the universe A. Moreover, many important properties of an algebra (subalgebras, automorphisms etc.) depend only on its clone of term or (congruences, stable orderings etc.) of polynomial operations and therefore are the same for term [polynomial] equivalent algebras.

In this paper we restrict ourselves to such clones that the corresponding algebras generate congruence permutable varieties. They need to contain a ternary operation $\mathbf{d}(x, y, z)$ satisfying $\mathbf{d}(x, x, y) = y = \mathbf{d}(y, x, x)$. Such an operation $\mathbf{d}$ is called a *Mal'tsev operation*. A clone containing at least one Mal'tsev operation is to be called a *Mal'tsev clone*. We are going to deal with both types of clones, of term and of polynomial operations. In the first case we will assume that an algebra has a Mal'tsev *term* and in the second a Mal'tsev *polynomial*. So, in the latter case the algebra should not generate a congruence-permutable variety.

In the following table we summarize our present knowledge of the number of clones satisfying the most famous Mal'tsev conditions. The number of inequivalent algebras with a finite universe can be treated as a measure of rigour of a condition. Thus by this table we may compare rigour of different Mal'tsev conditions. For a fixed number of elements in A the first row shows the number of all clones on A with a given Mal'tsev condition, while the second row shows the number of polynomial clones of this type.

$\lvert A\rvert$	all	CD	CD and C3P	CP	CP and E-min	CD and CP
2	ω	ω	ω	11	11	6
	7	2	1	2	2	1
3	2^ω	2^ω	2^ω	1167	6	fin
	2^ω	2^ω	2^ω	14	1	4
4	2^ω	2^ω	2^ω	$\geq \omega$	$\geq \omega$	fin
	2^ω	2^ω	2^ω	ω	ω	fin
5	2^ω	2^ω	2^ω	$\geq \omega$	$\geq \omega$	fin
	2^ω	2^ω	2^ω	$\geq \omega$	ω	fin
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The symbols CD, CP and C3P denote congruence distributivity, congruence permutability and congruence 3-permutability. (Recall that an algebra $\mathbb{A}$ is called *congruence 3-permutable* if $\alpha \circ \beta \circ \alpha = \beta \circ \alpha \circ \beta$ holds, for any congruences α, β of $\mathbb{A}$.) The column labelled "CP and E-min." gives the number of Mal'tsev E-minimal algebras.

The entries for $|A| = 2$ follow from Post's classification. The results of [16] and [10] give the number of all clones while the results of [1] give the number of all polynomial clones. M. Porębska [14] constructed an uncountable set of three-element polynomially inequivalent algebras that generate congruence-distributive and congruence-3-permutable varieties. This result allows us to fill up columns "CD" and "CD and C3P". Further, as it follows from results of [2], there are finitely many term [polynomially] inequivalent finite congruence distributive and congruence permutable algebras. We discuss the entries from "CP" and "CP and E-min" in following sections.

2. Types, commutators and polynomial equivalence

The numbers of polynomially inequivalent Mal'tsev algebras for cases $|A| = 3, 4$ were obtained in [11],[6]. The most remarkable fact is that in these cases of small universes an algebra is uniquely determined by those of its properties that can be expressed in the language of commutator theory.

Recall that tame congruence theory [9] allows us to label all prime quotients in the congruence lattice of a finite algebra by one of the types $\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}$. These types describe in some sense the local structure of the algebra, and corresponding forms of the local structure are the following: **1.** a finite set with a group action on it, **2.** a finite vector space over a finite field, **3.** a two-element Boolean algebra, **4.** a two-element lattice, **5.** a two-element semilattice. The type of the prime quotient $\alpha \prec \beta$ in the congruence lattice $\mathsf{Con}\ \mathbb{A}$ is to be denoted by $\mathsf{typ}_{\mathbb{A}}(\alpha, \beta)$, or simply $\mathsf{typ}(\alpha, \beta)$ if $\mathbb{A}$ is clear from the context.

If $\mathbb{A}$ is a Mal'tsev algebra, prime quotients of its congruence lattice may have only types $\mathbf{2}$ and $\mathbf{3}$. We will use the notion of polynomially rich algebra introduced in [12]. This notion captures our informal idea of an algebra having as many polynomials as possible whilst keeping the congruence lattice and labels (in the sense of tame congruence theory) of its prime quotients.

Definition 1. *Let $\mathbb{A} = (A, F)$ be a finite algebra. An operation $f : A^s \to A$ is called* $\mathbb{A}$-admissible *if* $\mathsf{Con}\ (A; F \cup \{f\}) = \mathsf{Con}\ \mathbb{A}$ *and for $\alpha, \beta \in \mathsf{Con}\ \mathbb{A}$ with $\alpha \prec \beta$ we have $\mathsf{typ}_{(A;F\cup\{f\})}(\alpha, \beta) = \mathsf{typ}_{\mathbb{A}}(\alpha, \beta)$.*

A finite algebra $\mathbb{A}$ is said to be polynomially rich *if every $\mathbb{A}$–admissible operation is a polynomial of $\mathbb{A}$. It is* hereditarily polynomially rich *if all its homomorphic images are so.*

The next theorem follows immediately from results of [11].

Theorem 1. *Every two- and three-element Mal'tsev algebra is hereditarily polynomially rich.*

We may refomulate this theorem making use commutator theory [8]. Recall that by the *commutator* of congruences α, β of an algebra $\mathbb{A}$ we mean the smallest congruence $\gamma = [\alpha, \beta]_{\mathbb{A}}$ such that for any polynomial operation $f(x_1, \ldots, x_n)$ of $\mathbb{A}$ and any $a \stackrel{\beta}{\equiv} b$, $a_2 \stackrel{\alpha}{\equiv} b_2, \ldots, a_n \stackrel{\alpha}{\equiv} b_n$,

$$f(a, a_2, \ldots, a_n) \stackrel{\gamma}{\equiv} f(b, a_2, \ldots, a_n)$$

implies

$$f(a, b_2, \ldots, b_n) \stackrel{\gamma}{\equiv} f(b, b_2, \ldots, b_n).$$

If the algebra is clear from the context we shall write $[\alpha,\beta]$ instead of $[\alpha,\beta]_{\mathbb{A}}$. In fact, the commutator is uniquely determined by binary operations of an algebra. As is well known, in a congruence-modular variety the commutator is a commutative monotone operation on congruence lattices of algebras from the variety.

Let $\mathbf{L}$ be a lattice of permutable equivalence relations on a finite set A and $\mathbf{d}$ be a Mal'tsev operation such that $\mathbf{d}$ preserves all relations from $\mathbf{L}$. (Such a Mal'tsev operation does not necessarily exist, see [7].) Denote $\mathbb{A} = (A; \mathbf{d})$ and define on $\mathbf{L}$ a binary operation $[\cdot,\cdot]$ satisfying all properties of modular commutator and such that $[\alpha,\beta] \geq [\alpha,\beta]_{\mathbb{A}}$ for all $\alpha,\beta \in \mathbf{L}$. An operation f on A is said to be $(\mathbf{L},\mathbf{d})$-*admissible* if it preserves all equivalence relations from $\mathbf{L}$ and for any $\alpha,\beta \in \mathbf{L}$, $[\alpha,\beta]_{(A;\{\mathbf{d},f\})} \leq [\alpha,\beta]$.

Further, for any $\alpha,\beta,\gamma \in \mathbf{L}$ satisfying $[\alpha,\beta] \leq \gamma \leq \alpha,\beta$, we define the 4–ary relation $R_{\alpha,\beta,\gamma} \subseteq A^4$ by

$$R_{\alpha,\beta,\gamma} = \left\{ (a,b,c,u) \in A^4 : a \stackrel{\alpha}{\equiv} b \stackrel{\beta}{\equiv} c \text{ and } u \stackrel{\gamma}{\equiv} \mathbf{d}(a,b,c) \right\}.$$

Results of [6] imply the following:

Lemma 1. *An operation f preserves $R_{\alpha,\beta,\gamma}$ for all $\alpha,\beta,\gamma \in \mathbf{L}$, $[\alpha,\beta] \leq \gamma \leq \alpha,\beta$, if and only if f is $(\mathbf{d},\mathbf{L})$-admissible.*

This means that all $(\mathbf{d},\mathbf{L})$-admissible operations form a clone. Therefore every pair consisting of a Mal'tsev operation and a lattice of permutable equivalence relations preserved by the operation determines a clone.

Now let $\mathbb{A}$ be an algebra, $\alpha,\beta \in \mathsf{Con}\ \mathbb{A}$ with $\alpha \prec \beta$. The type $\mathsf{typ}(\alpha,\beta)$ of this prime quotient is obviously determined by the commutator square $[\beta,\beta]$:

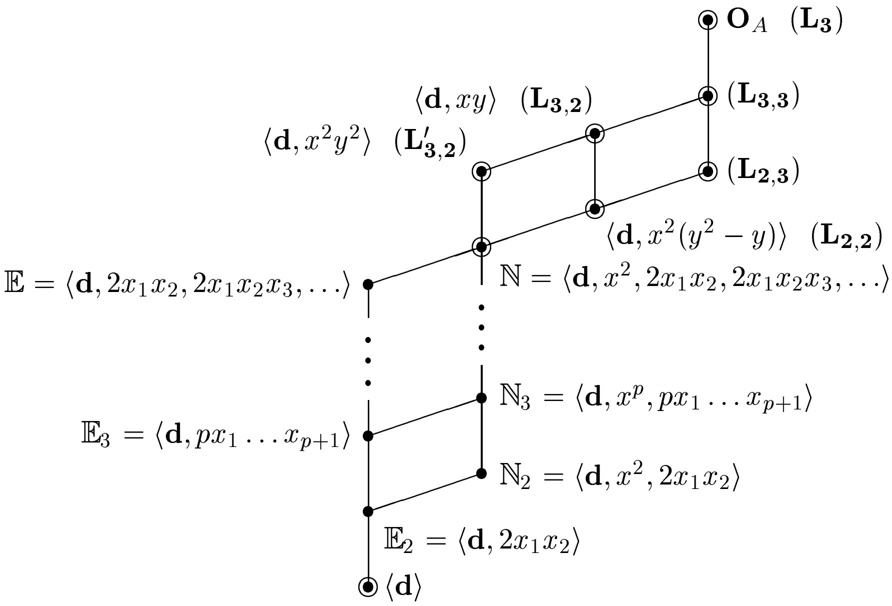
$$\mathsf{typ}(\alpha,\beta) = \begin{cases} \mathbf{2}, & \text{if } [\beta,\beta] \leq \alpha, \\ \mathbf{3}, & \text{if } [\beta,\beta] \not\leq \alpha. \end{cases}$$

Let $\mathbf{d}$ be a Mal'tsev operation and $\mathbf{L}$ be a lattice of equivalence relations such that $\mathbf{d}$ preserves $\mathbf{L}$ and each prime quotient (α,β) of $\mathbf{L}$ is labelled with type $\mathsf{typ}_{\mathbf{L}}(\alpha,\beta) \in \{\mathbf{2},\mathbf{3}\}$. Then, there exists at most one polynomially rich algebra $\mathbb{A}$ with $\mathsf{Con}\ \mathbb{A} = \mathbf{L}$ and $\mathsf{typ}_{\mathbb{A}}(\alpha,\beta) = \mathsf{typ}_{\mathbf{L}}(\alpha,\beta)$, for each prime quotient.

Corollary 1. *Up to polynomial equivalence, there exist finitely many three-element Mal'tsev algebras.*

Corollary 1 does not provide a description of three-element Mal'tsev algebras, because many pairs $\mathbf{d},\mathbf{L}$ give the same polynomially rich algebras. To reach a complete description a great deal of additional work is required. This work has been done in [11] where it was proved that there are 14 polynomially inequivalent three-element Mal'tsev algebras.

As was shown in [11] (see also [6],[13]), there are infinitely many polynomially inequivalent four-element Mal'tsev algebras. They therefore cannot be determined by congruence lattice and commutator operation. The picture below presents the lattice of those clones on a four-element set which contain the Mal'tsev operation $\mathbf{d} = x - y + z$ of the group $\mathbb{Z}_4$. Encircled clones are those which are determined by the congruence lattice and the commutator operation of the corresponding algebra. Also generating sets (constant operations should be added) for some clones are given. The notation xy means multiplication modulo 4. $\mathbf{L_{ij}}$ denotes the clone such that the corresponding algebra has three congruences $\underline{0} < \mu < \underline{1}$ and $\mathsf{typ}(\underline{0}, \mu) = \mathbf{i}$, $\mathsf{typ}(\mu, \underline{1}) = \mathbf{j}$; $\mathbf{L'_{2,3}}$ is the clone determined by $\mathsf{typ}(\underline{0}, \mu) = \mathbf{2}, \mathsf{typ}(\mu, \underline{1}) = \mathbf{3}$ and $[\underline{1}, \mu] = \underline{0}$; $\mathbb{N}$ is determined by $[\underline{1}, \underline{1}] = \mu, [\underline{1}, \mu] = \underline{0}$, and $\langle \mathbf{d} \rangle$ is determined by $[\underline{1}, \underline{1}] = \underline{0}$.



So, commutator operation cannot distinguish clones from two infinte ascending chains. The left chain is formed by clones of E-minimal algebras. An algebra is called *E-minimal* if each of its unary idempotent polynomials (that is, polynomials f satisfying $f^2 = f$) is either the identity mapping or a constant operation. We introduce here a commutator-like operations that allow us to distinguish these clones. By boldface letters we denote tuples of elements or variables.

Definition 2. *Let $\mathbb{A}$ be an algebra, $\alpha_1, \ldots, \alpha_n, \beta, \delta$ be congruences of $\mathbb{A}$, $f(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y})$ be a polynomial and $\mathbf{a}_1, \mathbf{b}_1, \ldots, \mathbf{a}_n, \mathbf{b}_n, \mathbf{c}, \mathbf{d}$ be such that*

$$\mathbf{a}_1 \stackrel{\alpha_1}{\equiv} \mathbf{b}_1, \ldots, \mathbf{a}_n \stackrel{\alpha_n}{\equiv} \mathbf{b}_n, \mathbf{c} \stackrel{\beta}{\equiv} \mathbf{d}.$$

We say that $\alpha_1,\dots,\alpha_n$ centralize β *modulo* δ *if*

$$f(\mathbf{x}_1,\dots,\mathbf{x}_n,\mathbf{c}) \stackrel{\delta}{\equiv} f(\mathbf{x}_1,\dots,\mathbf{x}_n,\mathbf{d}),$$

for any $(\mathbf{x}_1,\dots,\mathbf{x}_n) \in (\{\mathbf{a}_1,\mathbf{b}_1\} \times \dots \times \{\mathbf{a}_n,\mathbf{b}_n\} - \{(\mathbf{b}_1,\dots,\mathbf{b}_n)\}$, *implies*

$$f(\mathbf{b}_1,\dots,\mathbf{b}_n,\mathbf{c}) \stackrel{\delta}{\equiv} f(\mathbf{b}_1,\dots,\mathbf{b}_n,\mathbf{d}).$$

It is written as $C(\alpha_1,\dots,\alpha_n,\beta;\delta)$.

It follows immediately from the definition that for any congruences $\alpha_1,\dots,\alpha_n,\beta,\delta_i, i\in I$, if $C(\alpha_1,\dots,\alpha_n,\beta;\delta_i)$ for each $i \in I$, then

$$C(\alpha_1,\dots,\alpha_n,\beta;\bigwedge_{i\in I}\delta_i).$$

This justifies the following definition.

Definition 3. *For congruences* $\alpha_1,\dots,\alpha_n$*, the smallest congruence* δ *such that* $C(\alpha_1,\dots,\alpha_n;\delta)$ *is called the (*n-ary*)* commutator *of* $\alpha_1,\dots,\alpha_n$*. We write it* $[\alpha_1,\dots,\alpha_n]$.

It can be shown [4] that multi-placed commutators satisfy most properties of the usual (binary) commutator, e.g. monotonicity and commutativity.

Multi-placed commutators allow us to distinguish E-minimal algebras in our example. Actually, one may easily check that, for the algebra $(\{0,1,2,3\};\mathbb{E}_n)$, the equality $[\underbrace{\underline{1},\dots,\underline{1}}_{k\text{ times}}] = \underline{0}$ holds if and only if $k > n$. Moreover, it follows from the results of [6], that the analogous property holds for all four-element Mal'tsev algebras.

Theorem 2. *Up to polynomial equivalence, every four-element Mal'tsev algebra is uniquely determined by its congruence lattice, multi-placed commutators and set of unary polynomials.*

Corollary 2. *There exist countably many polynomially inequivalent four-element Mal'tsev algebras.*

It was proved in [4],[5] that the theorem above can be generalized for larger E-minimal algebras.

Theorem 3. *Let* $\mathbb{A}$ *be a Mal'tsev* E*-minimal algebra. Then, up to polynomial equivalence,*
1) if $|\mathbb{A}| = p^2$ *then* $\mathbb{A}$ *is uniquely determined by its congruence lattice and multi-placed commutators;*
2) if $|\mathbb{A}| = p^3$ *then there are finitely many* E*-minimal algebras having the same congruence lattice and multi-placed commutators;*
3) otherwise there are countably many E*-minimal algebras having the same congruence lattice and multi-placed commutators.*

Corollary 3. *There exist countably many polynomially inequivalent finite E-minimal Mal'tsev algebras.*

3. Subalgebras, automorphisms and term equivalence

One would expect, looking at Post's classification that there are many more term inequivalent Mal'tsev algebras than polynomially inequivalent ones. Fortunately, it seems this is not the case. Moreover, small Mal'tsev algebras can be determined up to term equivalence by their simple properties. First, examine carefully Post's description.

Theorem 4. *Up to term equivalence every two-element Mal'tsev algebra is uniquely determined by the type of the sole prime quotient of its congruence lattice, subalgebras and automorphisms.*

In total, there are 11 term inequivalent two-element Mal'tsev algebras.
Five of them are polynomially equivalent to an Abelian group (that is of type **2**): one having 2 one-element subalgebras and the non-identity automorphism, one having the automorphism and no subalgebras, two having a subalgebra and no non-identical automorphisms, one without proper subalgebras and non-identical automorphisms;
the six others are functionally complete two-element Mal'tsev algebras (of type **3**), five of them are determined in the same way and the remaining one one has 2 one-element subalgebras and no non-identity automorphism.

To classify three-element algebras we have to consider more complicated structures. Let $\mathbb{B}$, $\mathbb{C}$ be subalgebras of $\mathbb{A}$. A homomorphism $\mathbb{B}$ onto $\mathbb{C}$ is called an *inner homomorphism* of $\mathbb{A}$. Let $A = \{a, b, c\}$. We define a ternary relation as follows

$$S_{a,b} = \begin{pmatrix} a & b & c & a & b & c \\ a & a & b & b & b & a \\ a & a & a & b & b & b \end{pmatrix}.$$

Theorem 5 ([3])**.** *If a three-element Mal'tsev algebra $\mathbb{A}$ has a non-trivial congruence μ and $\mathsf{typ}(\mu, \underline{1}) = \mathbf{2}$, then it is determined up to term equivalence by its subalgebras, inner homomorphisms and subuniverses of $\mathbb{A}^3$ of the form $S_{a,b}$ where $\{a, b\}$ is the only non-trivial block of μ. Otherwise a three-element Mal'tsev algebra is determined by its subalgebras, inner homomorphisms, congruences and types of prime quotients of the congruence lattice.*

By careful examination of all possible combinations of these parameters one may get the total number of all term inequivalent three-element Mal'tsev algebras.

Corollary 4. *Up to term equivalence, there exist 1167 three-element Mal'tsev algebras.*

4. Concluding remarks

The main purpose of this investigation is to prove (or disprove) the following conjectures.

Conjecture 1. *Up to polynomial equivalence, there are countably many finite Mal'tsev algebras.*

Conjecture 2. *Up to term equivalence, there are countably many finite Mal'tsev algebras.*

We believe that the first conjecture can be proved by generalizing Theorem 3, which, perhaps, can be done by reduction of the structure of an arbitrary Mal'tsev algebra to the structure of its E-minimal (or, more generally, nilpotent) parts. The second conjecture seems much harder, because in this case we lose many tools that work succesfully in the case of E-minimal algebras. The first important step towards this conjecture would be an answer to the following problem.

Problem 1. *Up to term equivalence, how many four-element Mal'tsev algebras are there?*

References

[1] I. Ágoston, L. Demetrovic and L. Hannák. On the number of clones containing all constants. in: *Lectures in Universal Algebra*, Coll. Math. Soc. János Bolyai, vol. 43, 1983, pp. 21–25.

[2] K. A. Baker and A. Pixley. Polynomial interpolation and the Chinese remainder theorem for algebraic systems. *Math. Z.*, **143**(1975), 165–174.

[3] A. A. Bulatov. Three-element Mal'tsev algebras. manuscript.

[4] A. A. Bulatov. Multi-placed commutators and E-minimal algebras. manuscript.

[5] A. A. Bulatov. The number of finite Mal'cev E-minimal algebras. manuscript.

[6] A.A.Bulatov, P.M.Idziak. Counting Mal'tsev clones on small sets. *International Journal of Algebra and Computing* (submitted).

[7] I. Chajda, G. Czédli. Mal'tsev functions on small algebras. *Studia Sci. Math. Hungar.*, **28**(1993), no. 3-4, 339–348.

[8] R. Freese and R. McKenzie. Commutator Theory for Congruence Modular Varieties, *London Math. Soc. Lecture Notes*, 125, 1987.

[9] D. Hobby and R. McKenzie. The Structure of Finite Algebras. *Amer. Math. Soc., Contemporary Mathematics*, vol. 76, Providence Rhode Island 1988.

[10] A. Hulanicki and S. Świerczkowski. Number of algebras with a given set of elements. *Bull. Acad. Sci. Polon., Ser. Sci., math. Phys. et Astron.*, **8**(1960), 283–284.

[11] P. M. Idziak. Clones with Malcev operations. *International Journal of Algebra and Computation*, **9**(1999), 213–226.

[12] P. M. Idziak and K. Słomczyńska. Polynomially rich algebras to appear in: *Journal of Pure and Applied Algebra*.

[13] A. A. Krokhin, K. L. Safin and E. V. Sukhanov. On the structure of the lattice of closed classes of polynomials. *Diskretnaja Matematika*, **9**(1997), 24–40, (Russian).

[14] M. Porębska. Interpolation for fragments of intermediate logics *Reports on Mathematical Logic*, **21**(1987), 9–14.

[15] E. L. Post. The two-valued iterative systems of mathematical logic. *Annals of Math. Studies*, no.5, Princeton University Press, N.J., 1941.
[16] Yu. Yanov and A. A. Muchnik. On existence of k-valued closed classes without finite basis. *Dokl. AN SSSR*, **127**(1959), 44 – 46, (Russian).

Dept. of Algebra and Discrete Math., Ural State University, 51 Lenina ave., 620083 Ekaterinburg, Russia

E-mail address: `Andrei.Bulatov@usu.ru`